# 第二届华为武研119网络安全大赛misc部分wp

原创

Ank1e 于 2021-11-02 15:30:00 发布 3532 收藏

分类专栏： CTF Writeup 文章标签： 华为 web安全 安全





## 华为武研119网络安全大赛

> 报名就是线下赛。武研所得一个比赛。题目不错。有点小难。最后4秒第一被冲了。最后亚军。麻了。

## MISC

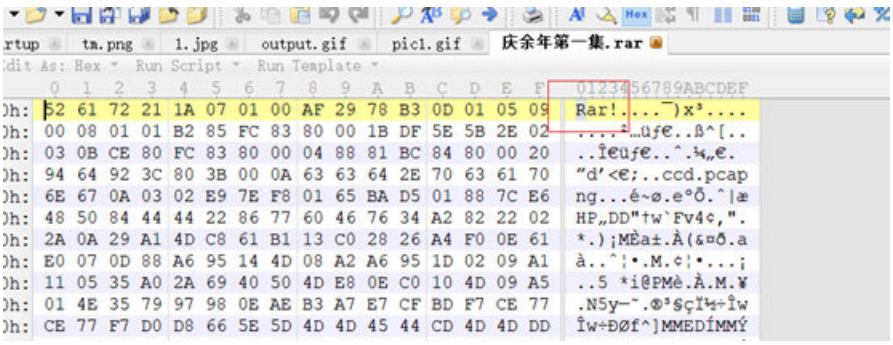
misc只做出来一道题。其他的等官方wp

### 神秘的视频

#### 核心技术点：python字节码嵌入payload、gif异或加密

#### 解题思路（附截图）：

下载附件发现是个mp4，但是打不开。使用十六进制工具打开发现Rar头




更改后缀为.rar解压缩。得到一个流量包和一个pyc文件。首先反编译pyc文件。发现在上面有一行注释。

```
#!/usr/bin/env python
# visit https://tool.lu/pyc/ for more information
'''Example carrier file to embed our payload in.
'''
from math import sqrt

def fib_v1(n):
    if n == 0 or n == 1:
        return n
```

网上搜索发现一种用于在Python字节码中嵌入Payload的隐写工具 – Stegosaurus。下载相关工具，进行解密，得到前半段flag

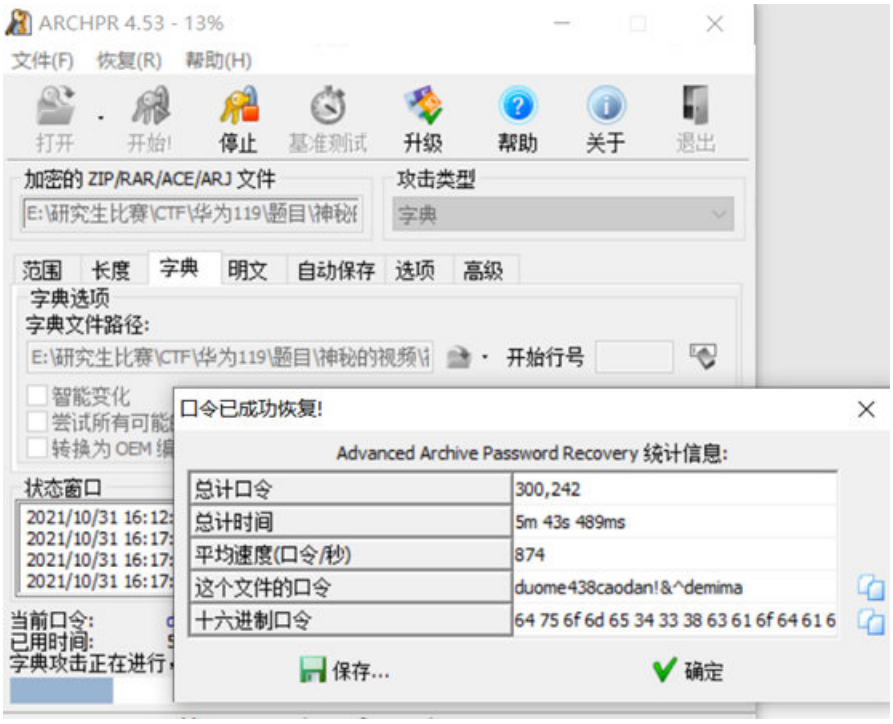
```
(fanyi) D:\Program_Files\InformationSafety\tools\misc\tools\stegosaurus>python stegosaurus.py -x flag.pyc
Extracted payload: flag{6754997a
```

再来看流量包。打开流量包，搜索http，发现了三个蚁剑流量。追踪返回包，发现第一个是查看目录，

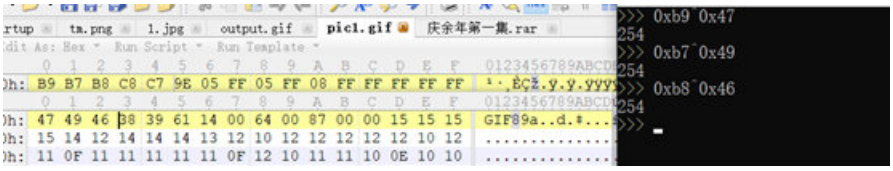
```
 D:\phpstudy_pro\WWW 的目录

2019/12/24  22:09    <DIR>          .
2019/12/24  22:09    <DIR>          ..
2019/12/24  22:08                33 1.php
2019/11/09  11:02               864 11.php
2019/12/03  08:59             1,172 12.php
2019/12/12  10:16             1,145 a.php
2019/11/14  11:38             2,389 backdoor.txt
2019/11/15  11:15               668 dd.py
2019/11/09  13:22               215 evil.pl
2019/11/08  09:08             4,281 exploit.php
2019/11/09  13:01             2,294 http.pm
2019/11/18  10:19                44 index.html
2019/11/08  09:02            86,661 jquery.js
2019/11/09  14:08                85 koa.pm
2018/08/13  22:09            81,920 nc.exe
2019/09/25  11:26    <DIR>          ook-master
2019/09/25  11:25            34,337 ook-master（解码ook，但需要php环境
2019/12/24  22:05         8,012,461 passwords.rar
2019/10/16  14:52    <DIR>          phpMyAdmin4.8.5
2019/12/24  22:02             4,828 pic1.zip
2019/11/09  14:07             2,294 pr0ph3t.pm
2019/11/08  10:46                 0 step1_prefix
2019/11/08  10:46                 0 step2_prefix
              19 个文件      8,235,691 字节
               4 个目录 103,121,678,336 可用字节
[S]
```

后两个是访问压缩包文件。直接全部导出。发现一个passwords.txt文件

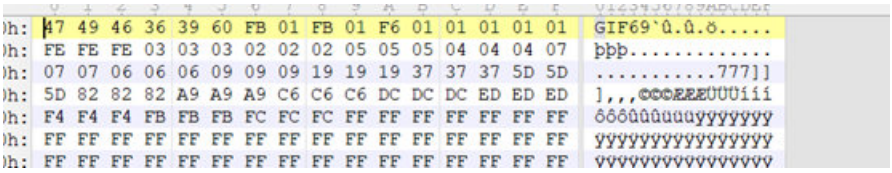

还有一个加密的pic1.zip。使用passwords.txt对压缩包进行爆破。得到密码：duome438caodan!&^demima



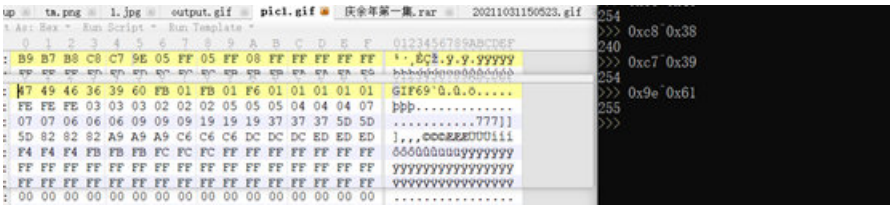

解压出来发现gif文件打不开，用十六进制工具打开什么都没发现。猜测可能经过某种加密，最常见的是异或。就用gif的头去试了一下。最开始以为是跟254异或得到gif的头




发现还是太年轻了。异或出来是gif69-。还是打不开。




又往下猜了几个。发现只有240和255，就两个都试了一下。




发现在跟255异或后把文件头改为gif89a可以还原成gif图片。分离gif图片得到后半段flag


Flag：flag{6754997a44ofd5f4}

### 解题脚本代码（可选）：

```
#-*- coding: utf-8 -*-

f= open("./pic1.gif")

f_1= open("./test1.gif","rb+")

data= f.read()

dec = ""

forx in range(len(data)):

  dec += chr(ord(data[x])^255)

#print f_1

f_1.write(dec)
```