HAGAME_Week1_WriteUp

Author: H41eyC Date: 26, Jan. 2021

######忘截图了 就凑合下

Misc

1.欢迎欢迎！热烈欢迎

关注“奇安信技术研究院”微信公众号，发送 HelloHGAME2022 获得flag

2.这个压缩包，它真的可以打开吗?

下载附件，打开可看到提示信息`Pure numeric passwords within 6 digits are not safe!`，利用`AZPR`6位纯数字爆破得到第一层密码`483279`。

第二层提示信息`I don't know if it's a good idea to write down all the passwords.`直接导入字典爆破`password-note.txt`
，得到密码`&-`;qpCKliw2yTR\`。

第三层，提示信息`If you don't like to spend time compressing files, just stores them.`，一开始以为是伪加密，把`14000100`改为`14000000`
提示文件损坏，说明是有加密的。

然后，我就卡壳了。之后观察了好久 发现当前目录的`README.MD`和`flag.zip/README.TXT`的crc值相同，遂想到明文加密。但是加密方式死活不对。

之后我查阅了`zip`的参数， 发现`zip -0  store only`， 和提示信息对上了，压缩完两个`README.TXT`的大小一样，遂判定为同种加密方式。之后使用`AZPR`明文攻击得到`UnEncrypted.zip`。

得到`README.TXT`和`flag.jpg`。之后就是常规流程，`binwalk`一跑得到`4FC5.zip`， 伪加密把`14000100`改为`14000900`得到flag。

3.好康的流量

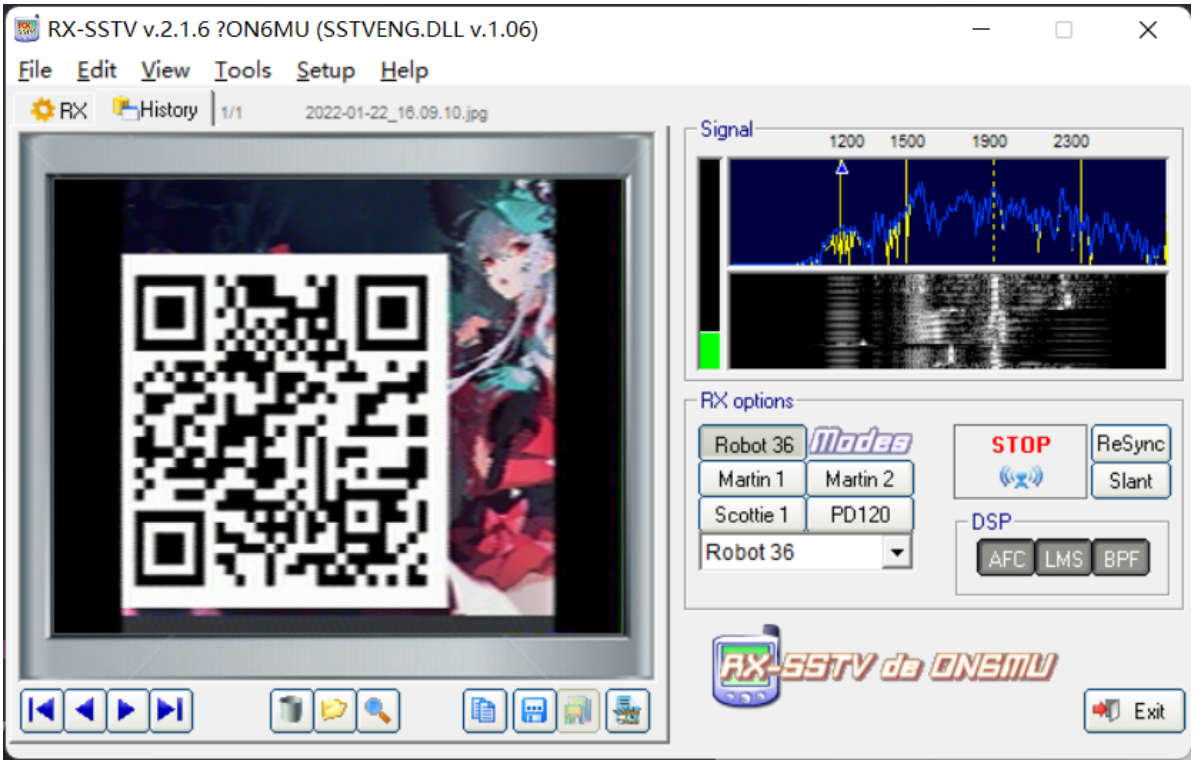
下载附件，在`wireshark`里打开， 先看`http`流， 没有有效信息。 继续观察流量包， 发现`SMTP`协议， 遂跟踪tcp流。发现2小串`BASE64`和一大串文字。 Decode一下:`涩图.png`
和`我知道你是LSB，快来看涩图`（好像是这样的，忘了），总之很明显就是LSB隐写。 然后先在那一大串文字前加上``复制到浏览器中打开，
能看到上半张图片，估计数据有损坏。先去掉所有换行符，再过滤其他非法字符。 由于是在`IDEA`里处理， 没有保留代码。 接下来通过脚本转码输出得到以下图片:

但是在导入`Stegsolve`时提示文件已损坏， 跑了下`CRC32`发现是`CRC32`有问题， 于是使用`Pillow`忽视损坏数据复制了一张。 使用`data extrat`， 勾选`extract by column`，
选择红绿蓝的`0`平面， 得到flag后半部分。在`GREEN plane 2`得到一串条形码， 解码得到前半部分。拼接得到flag。

4.群青(其实是幽灵东京)

这题应该是除了签到最简单的， 但是因为我脑瘫（SilentEye密码那两个框都要填我只填了一个）， 花了一下午。

下载下来， 丢进`Adobe Audition 2021`在频谱图里找到`Yoasobi`字样。`WinHex`打开在文件末尾找到提示`Why not try try SilentEye`（后来发现文件属性里直接能看）。
输入密码`Yoasobi`，decode得到一串`url`，下载下来是`S_S_T_V.mp3`。 然后我傻乎乎的自己写脚本在分析它是啥编码， 分析了好久好久才想到文件名（主要之前没做过音频Misc题） 一查发现下载`Rx-SSTV`
装上虚拟声卡就能解码。解出来一张二维码：



解码得到flag。

至此misc方向结束

Web

1.easy_auth

看到注册界面这么简陋一开始以为是二次注入。。。找了半天没找到注入点， 放弃。

第二天再次随手输入用户名`admin' or 1 = 1 #`发现用户名还是被注册，意识到站点没有定期清空后台，这说明肯定不是二次注入。
于是登录， 看到`app.js`点开发现它从`/v1/todo/`请求数据。盲猜Django后台（虽然没啥用），BP抓包， `Ctrl R`丢进
`repeater`， 发现他会传入一串token比
如:`eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJRCI6NjMzOSwiVXNlck5hbWUiOiIyNCByMnYzNXYycSAzdjUiLCJQaG9uZSI6IiIsIkVtYWlsIjoiIiwiZXhwIjoxNjQzMjI1MjA1LCJpc3MiOiJNSmNsb3VkcyJ9.xvvZKMJ7wJb_XLCdV9frErN_pbdY2SB8Beow82HOQKs`

以小数点分割， 对第一段解码得到`{"alg":"HS256","typ":"JWT"}`， 是`JWT`加密。 百度以后， 用`JWT_tool`爆破口令
`jwt_tool.py eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJRCI6NjMzOSwiVXNlck5hbWUiOiIyNCByMnYzNXYycSAzdjUiLCJQaG9uZSI6IiIsIkVtYWlsIjoiIiwiZXhwIjoxNjQzMjI1MjA1LCJpc3MiOiJNSmNsb3VkcyJ9.xvvZKMJ7wJb_XLCdV9frErN_pbdY2SB8Beow82HOQKs -C -d /usr/share/wordlists/dirb/common.txt`
发现根本没有设口令。

那就直接构造了, 在这里我在`jwt.io`上构造，将`id`改为`1`将`username`改成`admin`，不设置口令，得到
payload`eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJRCI6MSwiVXNlck5hbWUiOiJhZG1pbiIsIlBob25lIjoiIiwiRW1haWwiOiIiLCJleHAiOjE2NDMyMjUyMDUsImlzcyI6Ik1KY2xvdWRzIn0.e8uFStuvzuOt2WFWlYvLCfXzMmjl3heCQTwYSJ63KfA`

使用BP发送token， 返回flag。

2.蛛蛛...嘿嘿♥我的蛛蛛

爬虫， 直接爬到99关， 在header里有flag。
就放段代码吧。

```
from bs4 import BeautifulSoup as Soup
import requests


def next_page(href):
    print(href)
    a_s = Soup(requests.get(r"https://hgame-spider.vidar.club/974257a916" +
href).content, "lxml").find_all("a")
    for a in a_s:
        if a["href"] is not None and a["href"] != "":
            next_page(a["href"])


next_page("")
```

3.Tetris plus

玩到3000分弹了个弹窗让我找flag。

慢慢看js， 首先发现了一个显示中文base64的js， 说明刚刚的弹窗肯定是编码的， 不能直接查找，base64加密再查or慢慢看吧。
懒得去加密，于是直接看代码。 盲猜在`main.js`或者`checking.js`， 果然 在`checking.js`里看到了一串`JS Fuck`还是叫啥的?
反正丢到`console`就行了。 话说这不是misc?

4。Fujiwara Tofu Shop

点进去， 提示`想成为车神，你需要先去一趟秋名山（qiumingshan.net）`

那就是`referer`改成`qiumingshan.net`

再次访问， 提示`只有借助AE-86才能拿到车神通行证(Hachi-Roku)`

那就把`User-Agent`改成`Hachi-Roku`

再次访问， 提示`86的副驾上应该放一盒树莓（Raspberry）味的曲奇`

观察返回的headers可以看到：`'Set-Cookie': 'flavor=Strawberry; ...`

如下设置cookie:`cookie:flavor=Raspberry; Path=/; Domain=localhost; Max-Age=3600; HttpOnly`

再次访问， 提示`汽油都不加，还想去秋名山？请加满至100`， 联想到返回headers里有`'Gasoline': '0'`

改为`100`继续访问， 得到`哪怕成了车神，也得让请求从本地发出来才能拿到 flag ！`

胜利在望， 把`x-forwarded-for`设置为`127.0.0.1`

访问，提示`大黑阔也想当车神？`说明大方向对了， 研究了一下， 把`x-forwarded-for`改为`127.0.0.1,127.0.0.1,127.0.0.1`
得到flag。
代码如下

```
import requests

url = "http://shop.summ3r.top/"
h = {}
h["User-Agent"] = 'Hachi-Roku'
h["Referer"] = 'qiumingshan.net'
h["Cookie"] = 'flavor=Raspberry; Path=/; Domain=localhost; Max-Age=3600;
HttpOnly'
h["Gasoline"] = "100"
h["x-forwarded-for"] = "127.0.0.1,127.0.0.1,127.0.0.1"
print(requests.get(url, headers=h).text)
```

至此web方向结束

crypto

1.Easy RSA

就是一道简单的rsa，（人生第一次做出rsa，太简单了）。
直接上代码。

```
import gmpy2


def de(l):
    e, p, q, c = l
    s = (p - 1) * (q - 1)
    d = gmpy2.invert(e, s)
    return pow(c, d, p * q)


if __name__ == '__main__':
    ls = [(12433, 149, 197, 104), (8147, 131, 167, 6633), (10687, 211, 197,
35594), (19681, 131, 211, 15710),
          (33577, 251, 211, 38798), (30241, 157, 251, 35973), (293, 211, 157,
31548), (26459, 179, 149, 4778),
          (27479, 149, 223, 32728), (9029, 223, 137, 20696), (4649, 149, 151,
13418), (11783, 223, 251, 14239),
          (13537, 179, 137, 11702), (3835, 167, 139, 20051), (30983, 149, 227,
23928), (17581, 157, 131, 5855),
          (35381, 223, 179, 37774), (2357, 151, 223, 1849), (22649, 211, 229,
7348), (1151, 179, 223, 17982),
          (8431, 251, 163, 30226), (38501, 193, 211, 30559), (14549, 211, 151,
21143), (24781, 239, 241, 45604),
          (8051, 179, 131, 7994), (863, 181, 131, 11493), (1117, 239, 157,
12579), (7561, 149, 199, 8960),
          (19813, 239, 229, 53463), (4943, 131, 157, 14606), (29077, 191, 181,
33446), (18583, 211, 163, 31800),
          (30643, 173, 191, 27293), (11617, 223, 251, 13448), (19051, 191, 151,
21676), (18367, 179, 157, 14139),
          (18861, 149, 191, 5139), (9581, 211, 193, 25595)]
    out_list = ""
    for l in ls:
        o = de(l)
```

```
        print(chr(o))
        out_list += chr(o)
    print(out_list)
```

至此crypto方向结束

Pwn

1.test_your_nc

直接`nc`然后`ls`接着`cat flag`。

至此Pwn方向结束

至此WriteUp结束

写在最后

一学期没打ctf了， 寒假娱乐一下， 之前学ctf的初衷是想让自己的代码能够更加健全， 这样就够了。 懒得冲榜， 学学web
防止被日站， 学学misc藏藏涩图（bushi) 娱乐娱乐， 对我而言足矣。