Hgame week1 Write up—FAD18

1. web

1.1 谁吃了我的 flag

打开乍一看是一段很皮的话，但是最后的一个单词却指明了方向，disclosure，然后直接百度尝试了一些，没有结果。后来更新了 hint，跟 vim 有关。百度后，是 vim 备份问题，构造 http://118.25.111.31:10086/.index.html.swp，下载 swp，直接用记事本打开也能找到 flag hgame{3eek_diScl0Sure_fRom+wEbsit@}

1.2 换头大作战

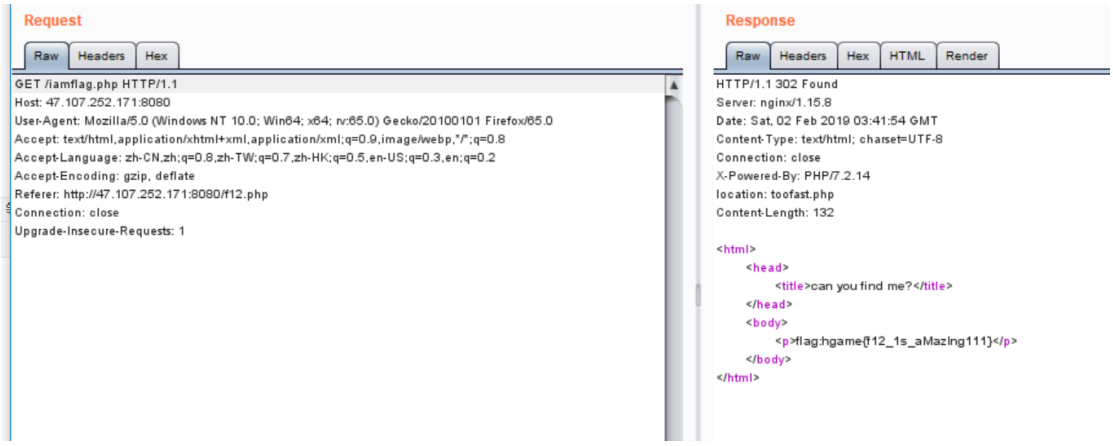
先随便输入一个值 submit，然后提示 post，F12 更改源码方法为 post，再随便尝试一个值，提示用 x-forwarded-for 伪造，x-forwarded-for: 127.0.0.1，接着网页提示要用 Waterfox/50.0，在请求头里更改 user-agent，接着网页提示要更改 referer，更改 referer 重新发送，最后根据提示改 admin=1，得到 flag hgame{hTTp_HeaDeR_iS_Ez}

1.3 very easy web

审计 php 代码，发现是典型的 strpos 绕过问题，首先想到数组绕过，然后发现失败了。原来是 === 全等，决定用两次 url 编码绕过，构造 ?id=%2576idar 得到 flag hgame{urlDecode_Is_GoOd}

1.4 can u find me?

提示 12 姑娘，直接 F12，发现 f12.php，前往。提示要 post 密码，在消息头里找到密码，post 过去，然后根据提示点击链接，在 f12 网络里看到 302 页面，然后根据提示想到抓包，抓到包，go 一下，得到 flag hgame{f12_1s_aMazIng111}



2. Re

2.1 HelloRe

这题直接下载附件，记事本打开就可看到 flag hgame{Welc0m3_t0_R3_World!}

2.2 Pro 的 python 教室（一）

查看源码，直接 base 解密，得到 flag hgame{Here_1s_3asy_Pyth0n}，这题可能只是叫我们认识一下 python 语言？

3. Misc

3.1Hidden Image in LSB

根据提示使用神器 stegsolve，一直点，点出 flag

3.2 打字机

一开始没有思路，然后尝试着百度识图，然后发现是新番紫罗兰永恒花园里的，想到了 violet，然后根据{}前面的肯定是 hgame，对应出 flag hgame{My_vi0let_tyPewRiter}

3.3Broken Chest

直接打开失败，先放到 winHex 里瞧瞧，发现开头固定格式被改了，改完后得到 flag（密码就是注释） hgame{Cra2y_D1aM0nd}

4. Crypto

4.1Mix

一看是摩斯密码，先解密得到 744B735F6D6F7944716B7B6251663430657D，发现只有 0~9，A~F,然后尝试 Hex 解密得到 tKs_moyDqk{bQf40e},想到了栅栏，尝试栏数到 9，解密 tsmyq{Q4eK_oDkbf0}，最后凯撒解密，得到 flag hgame{E4sY_cRypt0}

4.2Base 全家

查看页面，发现字符量很庞大，直接写 python 脚本

```
import base64
import requests
url='http://plir4axuz.bkt.clouddn.com/hgame2019/enc.txt'
s=requests.Session()
r=s.get(url).text
r=r.encode('utf-8')
def decode(a):
    b=a
    flag1=0
    flag2=0
    flag3=0
    for i in range(100):
     try:
        c=base64.b64decode(b)
        b=str(c,'utf-8')
        print("64 成功")
        print(b)
        continue
     except:
         flag1=1
         pass

     try:
        c=base64.b32decode(b)
        b = str(c, 'utf-8')
        print("32 成功")
        print(b)
        continue
     except:
        flag2=1
        pass;

     try:
        c=base64.b16decode(b)
        b = str(c, 'utf-8')
        print("16 成功")
        print(b)
        continue
     except:
        flag3=1
        pass

     if flag1==1&flag2==1&flag3==1:
```

```
            print("不能 base 解密")
            break

    print(b)
decode(r)
```

得到提示 base58：2BAja2VqXoHi9Lo5kfQZBPjq1EmZHGEudM5JyDPREPmS3CxrpB8BnC，用在线解密得到 flag hgame{40ca78cde14458da697066eb4cc7daf6}