week4-writeup

wuerror

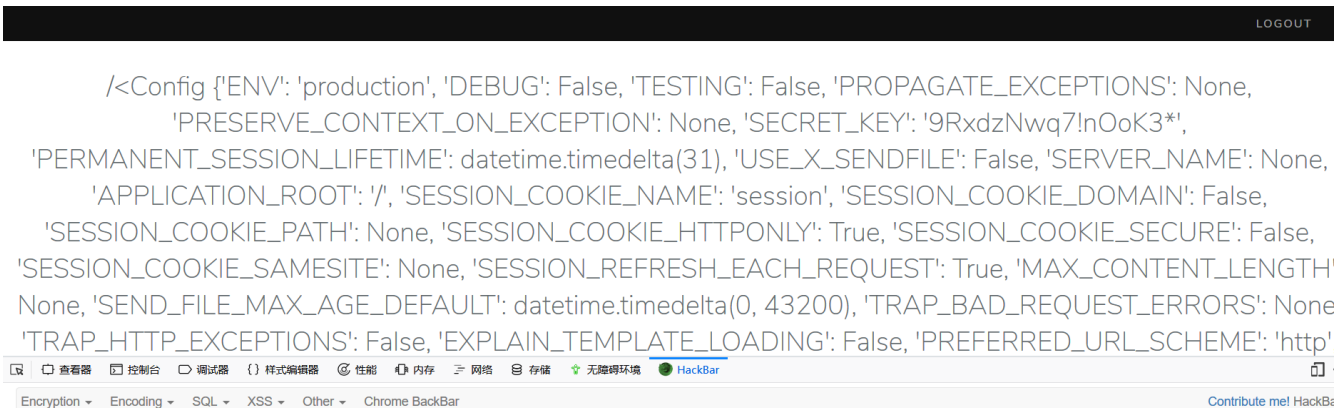
web

happy python

{u'csrf_token': u'a844480fd5e2cd4c8e3107765aa25923572cd2df', u'*fresh': True, u'user_id': u'admin', u'*id': u'051101fca32cbd279dfd6e96892ec55881e06fcb6a52872d04c920c74efacf9e245536486635b70ed6ecc6c446f0b431600fbaa9626a2089b2ca45ae7b8dc2eb'}

这题首先百度发现应该是flask/jinjia2模板注入，

```
http://118.25.18.223:3001/{{1+1}} //输出hello 2，确定是模板注入
http://118.25.18.223:3001/{{config}}
```

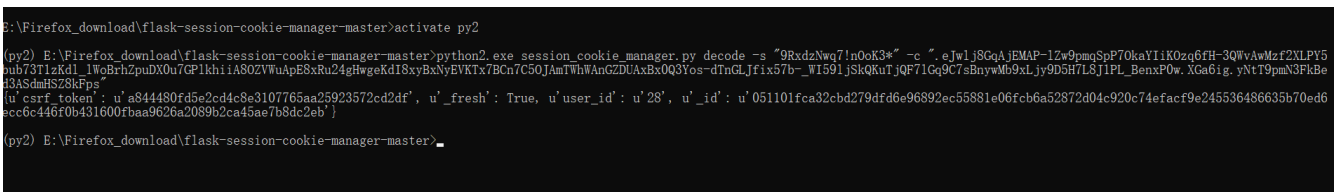


看文章继续试验注入

```
{{''.__class__.__mro__}}
```

发现可以，觉得大概是沙箱逃逸了，但努力两天继续下去发现()似乎被过滤了无法像文章说的那样找到file这些基本类。于是转向另一篇hctf的博文试验伪造session登陆的思路。

在之前注入{{config}}时我们已经得到了secret_key，抓取session利用GitHub的session_cookie_manager.py解密session，发现user_id是个数字，把它改成admin加密后访问失败。又注册两个新账号whd1/whd2发现其user_id为164/165，猜测admin的user_id为01.成功得到flag



资料：https://www.cnblogs.com/apossin/p/10083937.html

https://www.freebuf.com/articles/web/98928.html