云演CTF web题型 ping

原创

静默开水 于 2022-01-19 10:34:16 发布 794 收藏

分类专栏： 命令执行漏洞 web题解题思路 CTF 文章标签： 安全 经验分享 linux unctf

本文链接：https://blog.csdn.net/cadandme/article/details/122575292

命令执行漏洞 同时被 3 个专栏收录

2 篇文章 0 订阅

订阅专栏

web题解题思路

7 篇文章 0 订阅

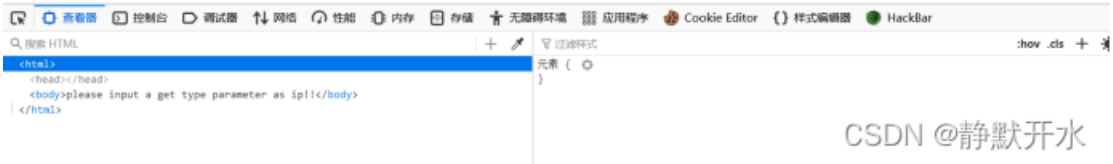
订阅专栏

CTF

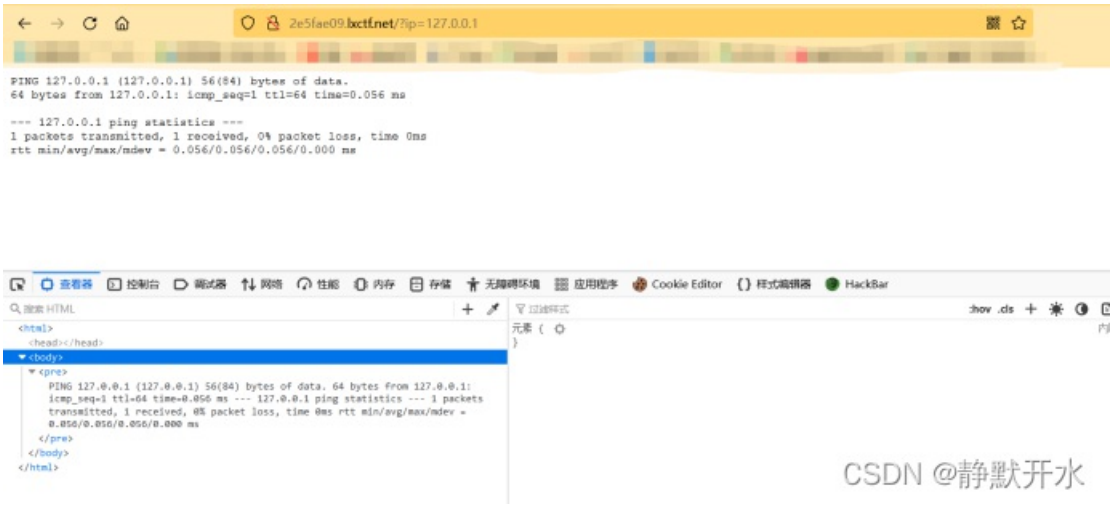
14 篇文章 0 订阅

订阅专栏

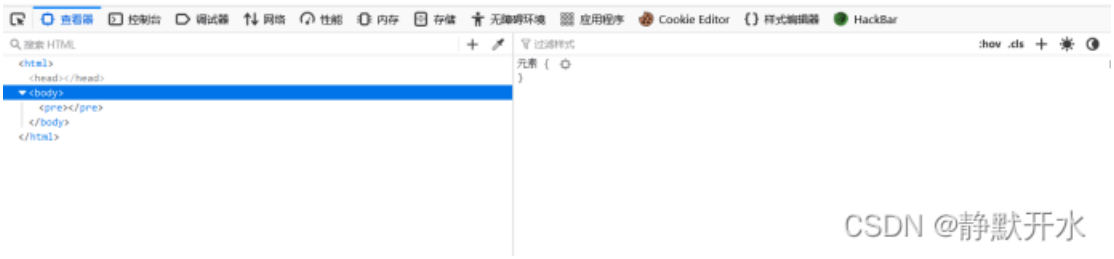
ping



打开页面提示用GET方式提交ip



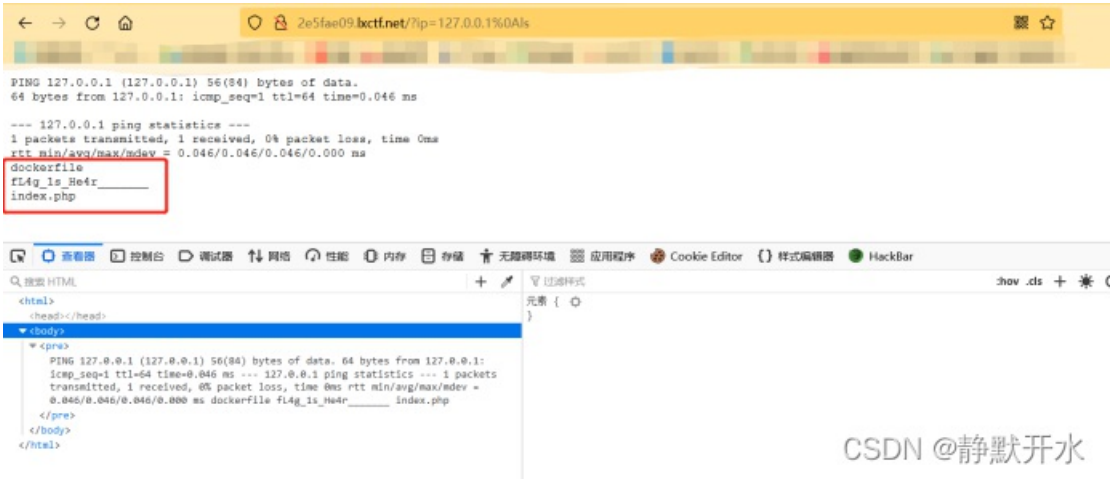
尝试管道符分隔命令查看目录，没回显，被禁用



在这里我尝试了好久，忘记有哪些命令分隔符可以代替了，查找后才知道
Linux下一般的命令分隔符有这几个

```
|   ||   &   &&   .   ;   -   <>   $   %0a   %0d   `
```

逐个尝试，%0a可以使用



到这一步，我们就可以看出flag就在fL4g_1s_He4r_____中了，直接查看，得到flag