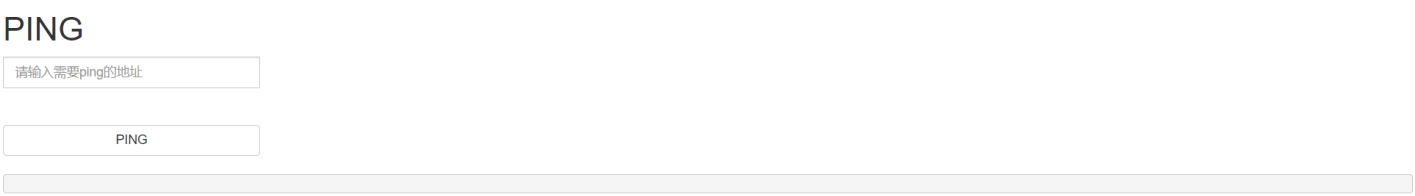
# Buuctf Exec

原创

Dexret 于 2021-12-06 20:14:23 发布 1470 收藏 1
分类专栏： buuctf Web 文章标签： buuctf web 安全




打开该靶机，发现该页面为一个ping页面





输入127.0.0.1测试，发现和电脑cmd上ping的结果差不多

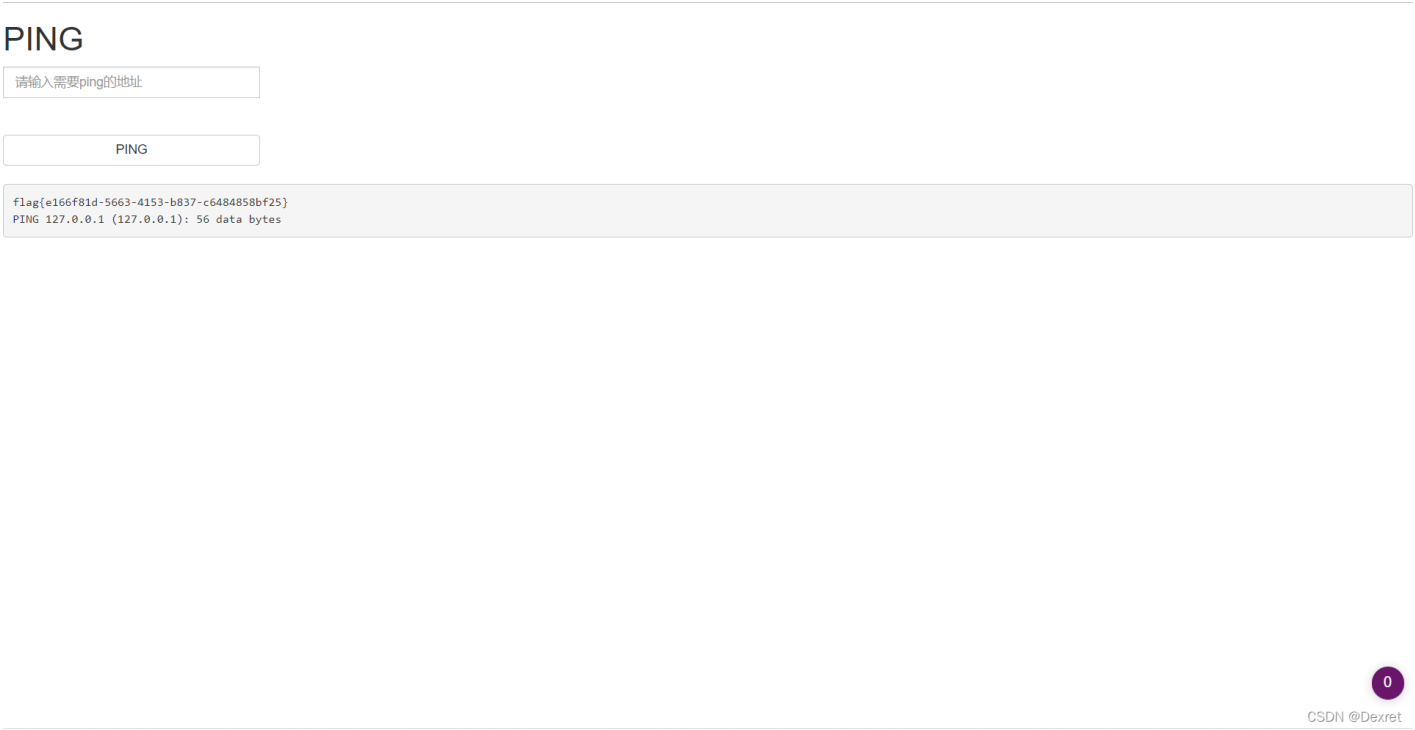
分析一下**ping**小技巧

&，&&，|，|| 的区别：

- A&B：简单的拼接，A、B之间无制约关系
- A&&B：A执行成功，然后才会执行B
- A|B：A的输出，作为B的输入
- A||B：A执行失败，然后才会执行B

构造payload

```
127.0.0.1&cat /flag
```




得到该题的flag

```
flag{e166f81d-5663-4153-b837-c6484858bf25}
```