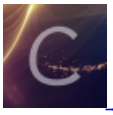
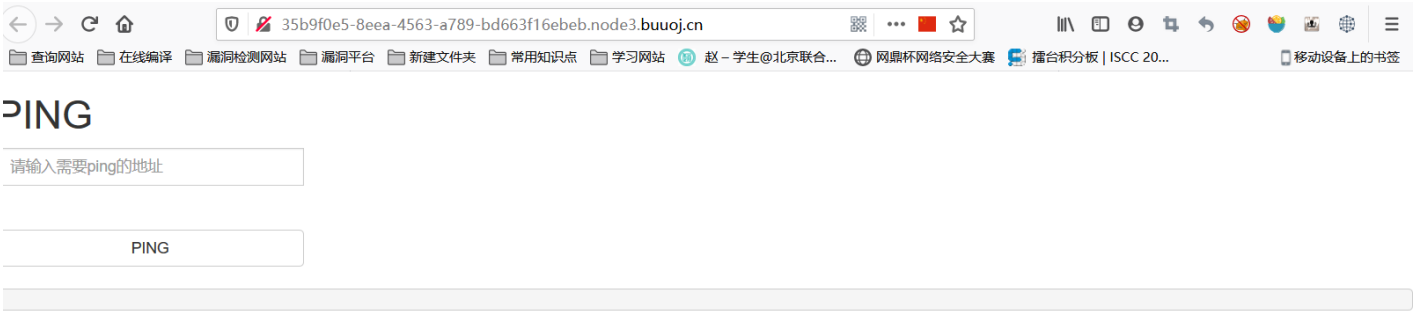
【学习笔记6】 buu [ACTF2020 新生赛]Exec

原创

Noslpum 于 2020-05-07 15:44:38 发布 148 收藏
分类专栏： 学习笔记 ctf 文章标签： linux java ubuntu 安全 python


学习笔记 同时被 2 个专栏收录
50 篇文章 0 订阅
订阅专栏


ctf
47 篇文章 1 订阅
订阅专栏



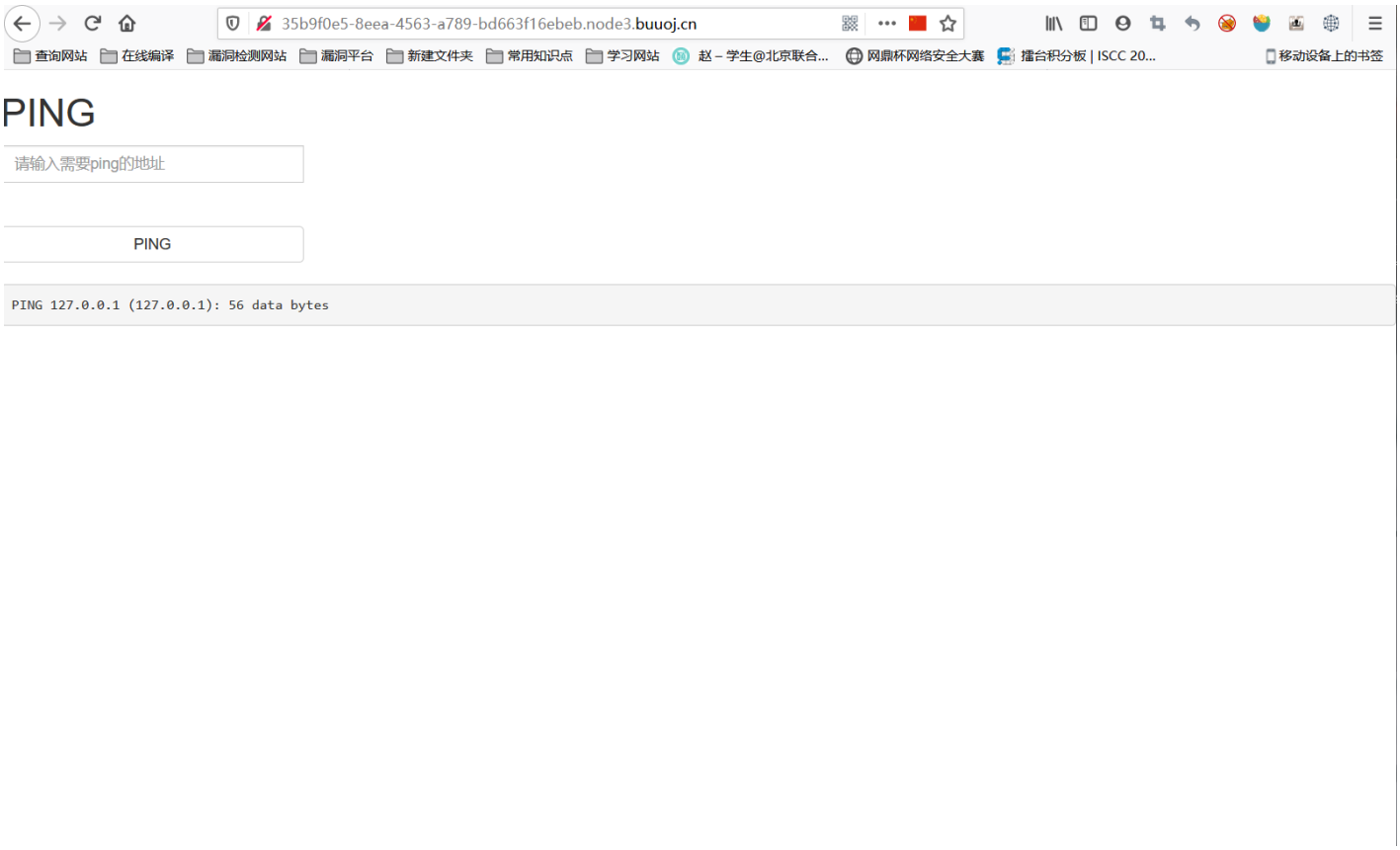
打开看到这样一个界面，根据做题经验，这应该是一道考察命令执行的题，但是老套路，先看看源码里有什么

通过查看源码发现什么否没有

那什么都说了，直接开始尝试

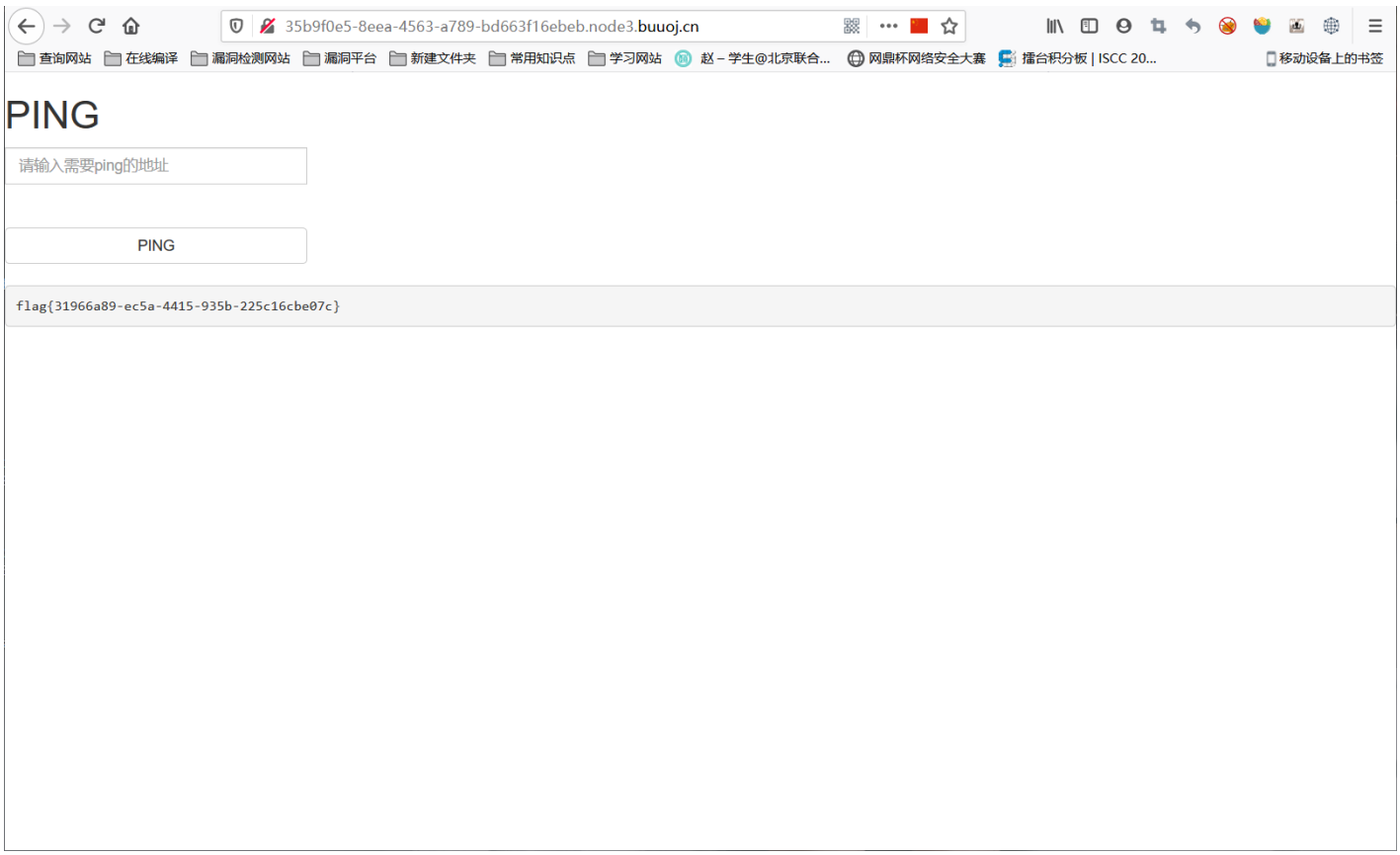
首先因为是让你ping一个地址，这里我们尝试

> **127.0.0.1**



显示给127.0.0.1发送了对应数据包，说明ping命令执行成功了，那么我们是不是就可以利用“|”来连接另外一个命令来执行从而得到flag，所以构造payload如下

> 127.0.0.1|cat /flag



可以看到直接给出了flag，这是一道没有任何过滤的命令执行题

在这里补充一些相关的管道符

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

3、&（就是按位与），&前面和后面命令都要执行，无论前面真假

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

5、;（linux下有的，和&一样的作用）