[ACTF2020 新生赛]Exec

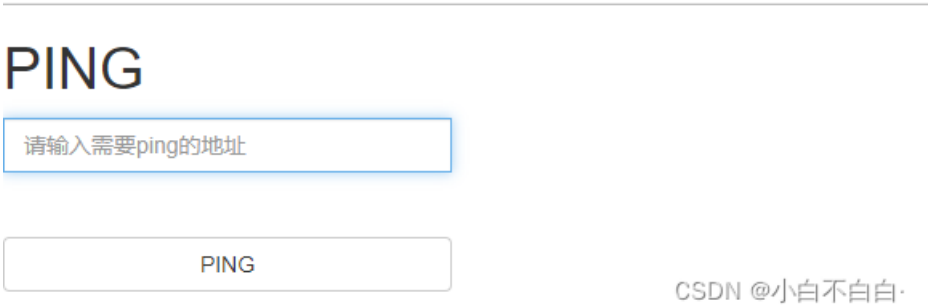
原创

小白不白白· 于 2022-01-24 15:16:28 发布 2006 收藏
分类专栏： BUUCTF 命令执行 文章标签： linux 运维 服务器 系统安全 web安全

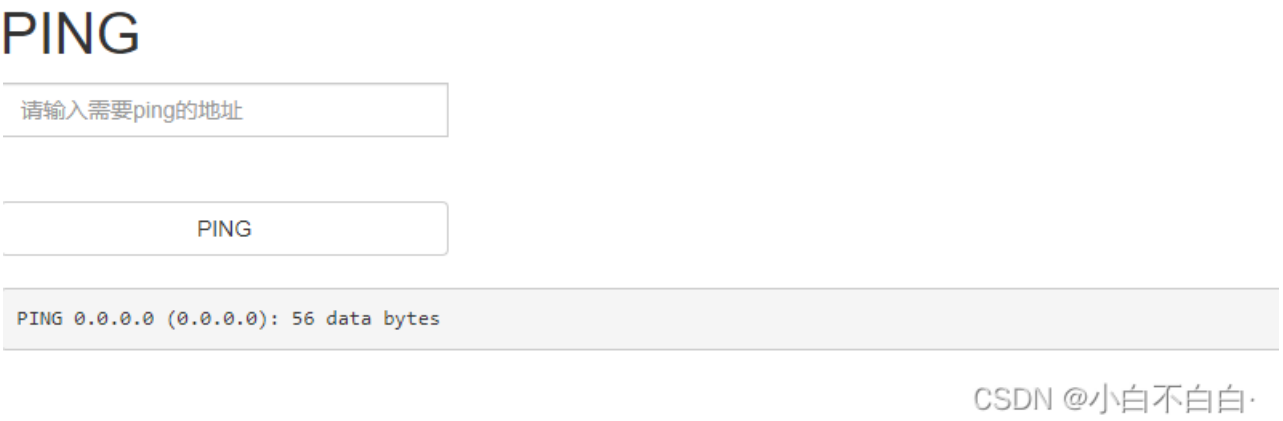

BUUCTF 同时被 2 个专栏收录
7 篇文章 0 订阅
订阅专栏


命令执行
1 篇文章 0 订阅
订阅专栏

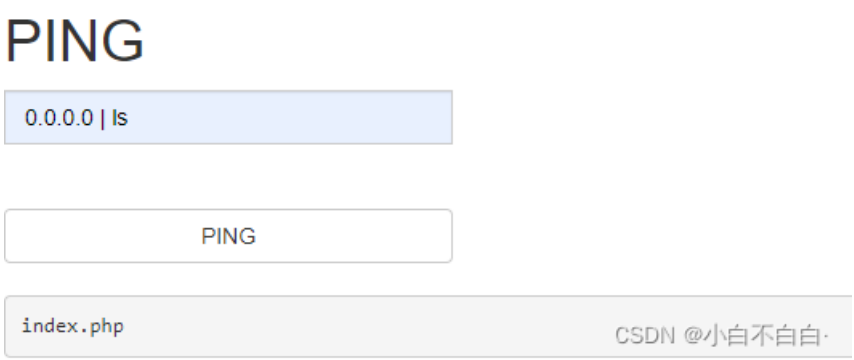
1.打开环境是一个ping的输入框



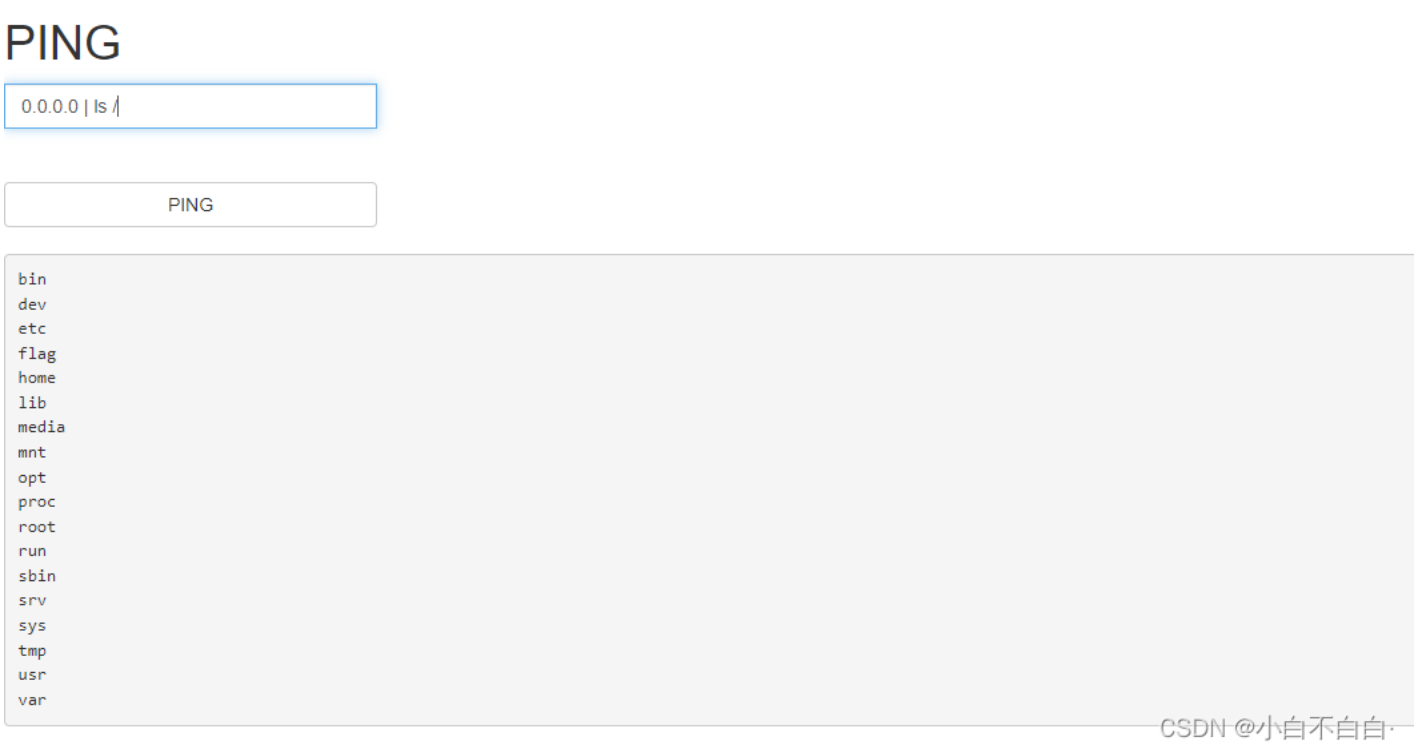
2.随便输入一个ip试试



3.回显内容，我们用管道符试试命令执行，先试试Linux的ls



4.看到了index.php,试试ls根目录，



5.看到了flag，直接cat他

6.本题考查 命令执行漏洞，说说常见管道符：

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

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、；（&一样的作用）在linux下用

本题用别的运算符一样可以的