【buuCTF】[ACTF2020 新生赛]Exec1

原创

Gariakov 于 2021-10-11 20:29:02 发布 1841 收藏
分类专栏： writeup BUUCTF 文章标签： web安全

其实嘛，这篇wp主要写给自己看的，本人也是三天打鱼两天晒网的菜鸟，自己写wp才能验证真的学会了嘛。想要和我一起学习的朋友也拜托指出1我的不足啊！

这道题CSDN和其他博客上已经有很多wp了，每道wp的解法都不尽相同，所以这里本人在学习了解法后还总结归纳了一下其他大佬们所用的一些解法。

这道题是属于非常基础的命令执行题了，连空格和分号都没有过滤→_→。

方法一：常用的管道符

包括：|，||，&，&&，；

其中：

| ：按或位，直接执行管道符后的语句。

|| ：逻辑或，判断前后语句，前面语句错误则执行后面语句，否则执行前面语句。

& ：按位与，无论&前后语句错误，前后语句均要执行。

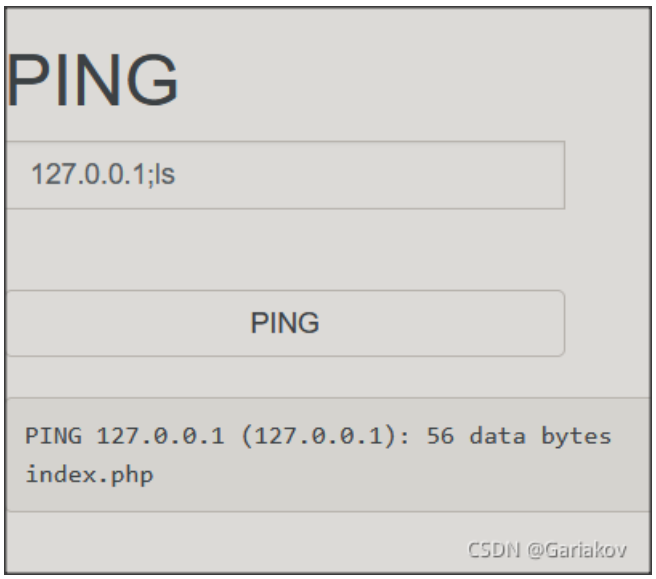
&&：逻辑与，前面语句错误则前后语句均不执行，前面语句正确则执行前后语句。

； ：在linux下使用，与&相同。

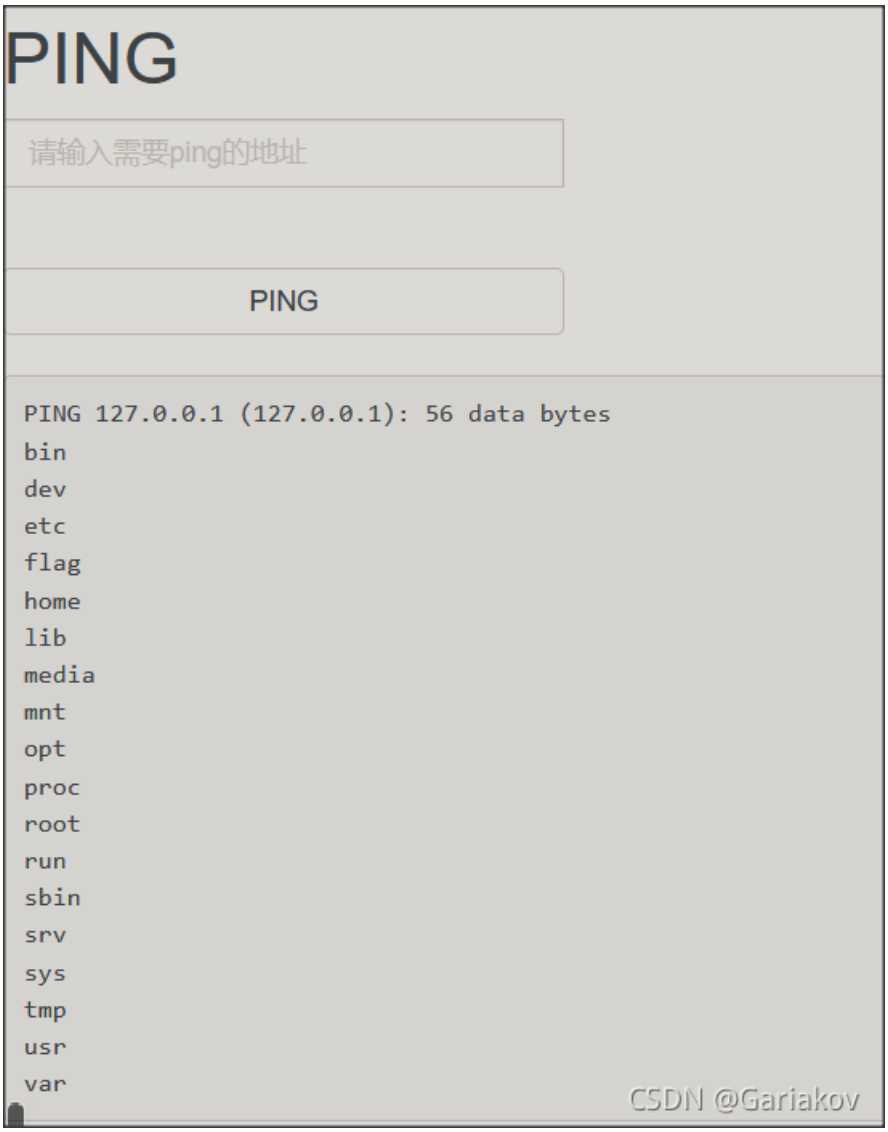
下面上图：

&和&&同理。

方法二：尝试路径访问

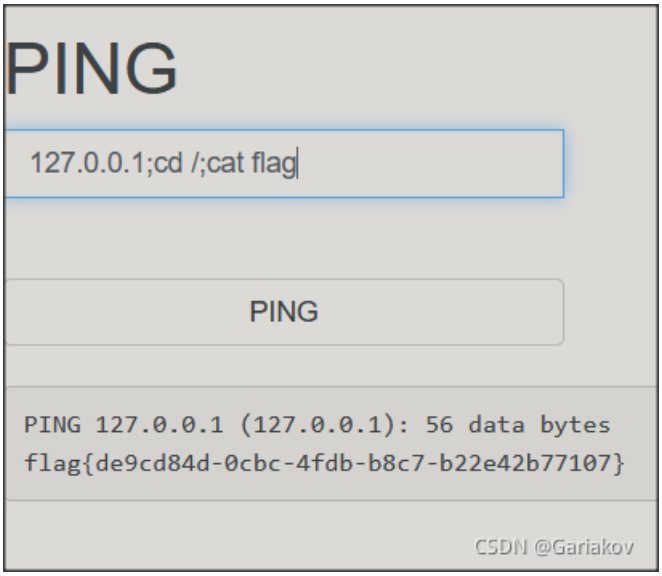


`127.0.0.1;cd /;ls`　　回到根目录



找到flag目录，访问。

127.0.0.1;cd /;cat flag



flag到手。

还有其他大佬的更厉害更高深的办法了，因为这道题比较简单所以我觉得杀鸡不用牛刀，后面有更难的命令执行漏洞的题可以再一起学习(゜∀。)