BUU 命令执行漏洞-[ACTF2020 新生赛]Exec

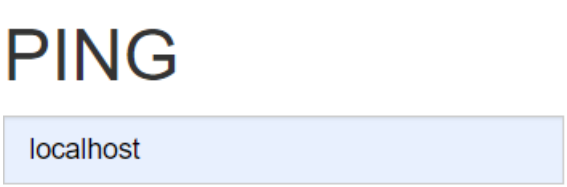
原创

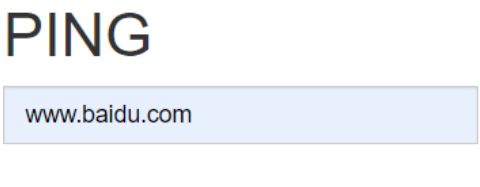
1vyyyyyy 于 2021-10-17 19:12:26 发布 2249 收藏
分类专栏： BUUCTF writeup 文章标签： linux web安全

一、题目

点开页面，经典的命令执行表单

先输入几个玩玩





都是正常回显，没啥怪东西

二、解题

1. 这里会用到 管道符 有关的知识点

① | : 即按位或，会直接执行管道符之后的语句

② || : 即逻辑或，若管道符前语句为true则只执行前一句，否则只执行后一句

③ & : 即按位与，会直接执行前后两个语句

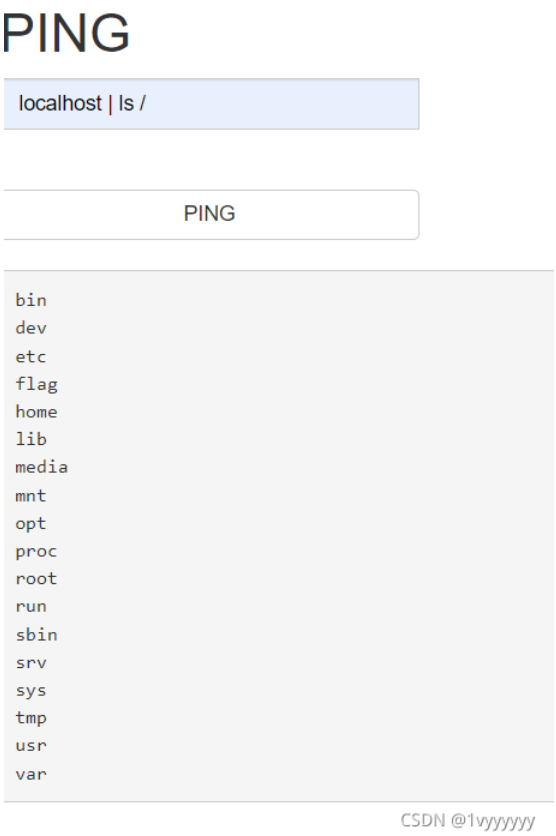
④ && : 即逻辑与，若管道符前语句为true则执行两个语句，反之都不执行

2. 在Linux命令中， ls 用于列出目录条目

那么我们输入

```
localhost | ls /
```

会显示根目录下所有条目



看到flag在根目录下，直接cat出来

payload:

```
localhost | cat /flag
```

三、总结

涉及Linux命令的题可以结合几个管道符进行操作，有时需要猜测后台的语句找合适的方法来构造输入