BUUCTF Web [ACTF2020 新生赛]Exec

原创

士别三日wyx 于 2021-10-27 16:39:29 发布 10459 收藏 9

分类专栏： 靶场通关教程 文章标签： 运维 网络安全 python java linux

> 「作者主页」：士别三日wyx
> 此文章已录入专栏《网络攻防》，持续更新热门靶场的通关教程
> 「未知攻，焉知收」，在一个个孤独的夜晚，你完成了几百个攻防实验，回过头来才发现，已经击败了百分之九十九的同期选手。

[ACTF2020 新生赛]Exec

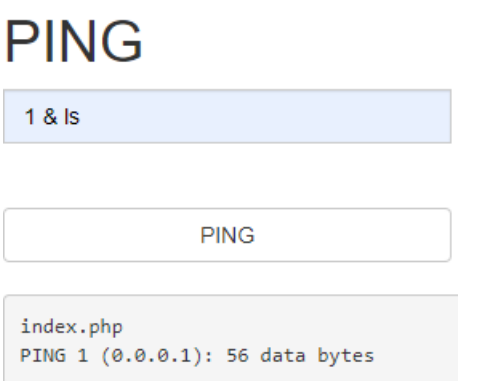
一、题目简介

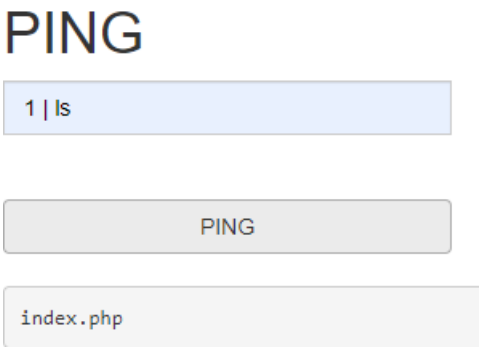
进入题目连接后，是一个ping的「功能」，我们输入ip地址或域名后可以使用ping命令「测试」网络的连通性

二、思路分析

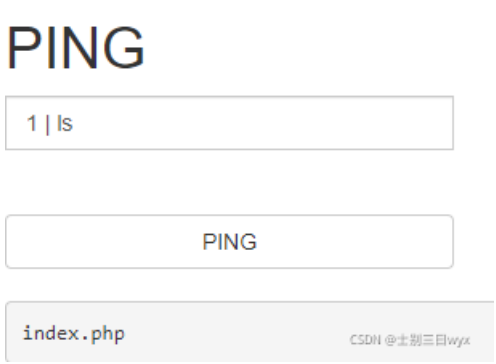
这一关是一个「命令执行」漏洞，推荐使用「逻辑运算符」执行多条命令

可以使用的逻辑运算符有很多，比如 `&` `|` `;`

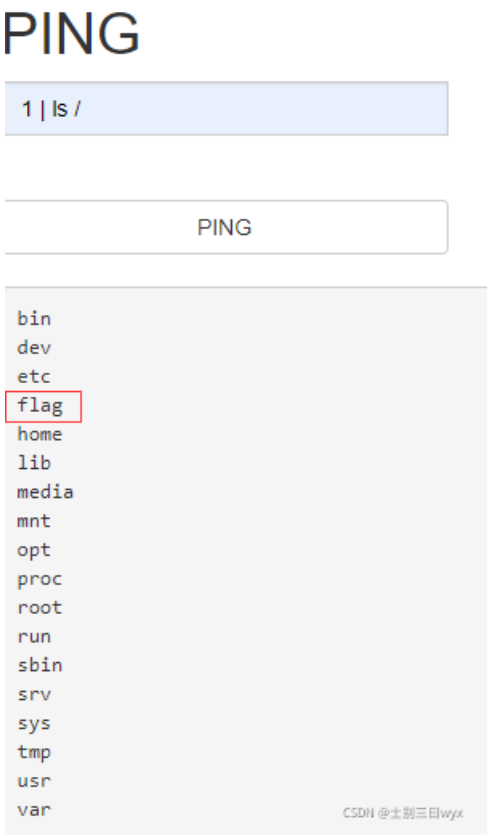




这里我们使用「逻辑或」 `|`，先查看当前路径下的文件，很明显flag不在这里。



接下来我们从「根目录」开始遍历目录。



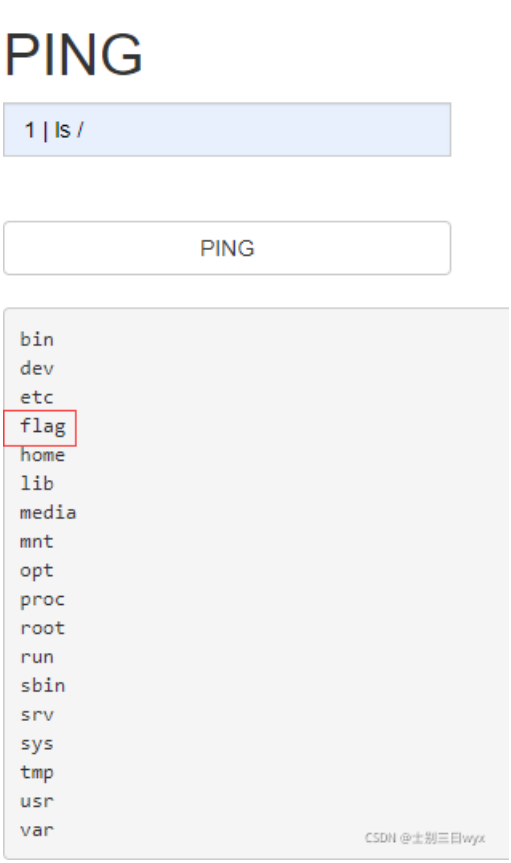
发现了flag文件，接下来「查看」这个文件就可以了

三、解题步骤

1）遍历目录

查看「根目录」，发现flag文件，payload如下

```
1 | ls /
```



2）查看文件内容

「查看」flag文件，获取flag，payload如下

```
1 | cat /flag
```

四、总结

> 喜欢一个东西首先要先学会「尊重」，虽然网络安全的圈子不乏各种灰产，以及高调宣传自己是黑客的脚本小子，但不可否认，这个圈子仍有不少人保持着「举世皆浊我独清，众人皆醉我独醒」的心态，努力磨砺技术，提升自身修养，让互联网变得更加安全