

【学习笔记6】 buu [ACTF2020 新生赛]Exec

原创

Noslpum 于 2020-05-07 15:44:38 发布 148 收藏

分类专栏: [学习笔记](#) [ctf](#) 文章标签: [linux](#) [java](#) [ubuntu](#) [安全](#) [python](#)

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/weixin_43553654/article/details/107686921

版权



[学习笔记](#) 同时被 2 个专栏收录

50 篇文章 0 订阅

订阅专栏



[ctf](#)

47 篇文章 1 订阅

订阅专栏



PING

请输入需要ping的地址

PING

打开看到这样一个界面, 根据做题经验, 这应该是一道考察命令执行的题, 但是老套路, 先看看源码里有什么

```
view-source:http://35b9f0e5-8eea-4563-a789-bd663f16ebef.node3.buuoj.cn/
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <title>command execution</title>
6   <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
7
8
9 </head>
10 <body>
11
12 <h1>PING</h1>
13 <form class="form-inline" method="post">
14
15   <div class="input-group">
16     <input style="width:280px;" id="target" type="text" class="form-control" placeholder="请输入需要ping的地址" aria-describedby="basic-addon1" name=
17   </div>
18   <br/>
19   <br/>
20
21   <button style="width:280px;" class="btn btn-default">PING</button>
22
23
24 </form>
25 <br /><pre>
26 </pre></body>
27 </html>
```

通过查看源码发现什么否没有

那什么都说了，直接开始尝试

首先因为是让你ping一个地址，这里我们尝试

127.0.0.1

← → ↻ 🏠 35b9f0e5-8eea-4563-a789-bd663f16ebeb.node3.buuoj.cn

查询网站 在线编译 漏洞检测网站 漏洞平台 新建文件夹 常用知识点 学习网站 赵-学生@北京联合... 网鼎杯网络安全大赛 擂台积分榜 | ISCC 20... 移动设备上的书签

PING

请输入需要ping的地址

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

显示给127.0.0.1发送了对应数据包，说明ping命令执行成功了，那么我们是不是就可以利用“|”来连接另外一个命令来执行从而得到flag，所以构造payload如下

```
127.0.0.1|cat /flag
```

← → ↻ 🏠 35b9f0e5-8eea-4563-a789-bd663f16ebeb.node3.buuoj.cn

查询网站 在线编译 漏洞检测网站 漏洞平台 新建文件夹 常用知识点 学习网站 赵-学生@北京联合... 网鼎杯网络安全大赛 擂台积分榜 | ISCC 20... 移动设备上的书签

PING

请输入需要ping的地址

PING

flag{31966a89-ec5a-4415-935b-225c16cbe07c}

可以看到直接给出了flag，这是一道没有任何过滤的命令执行题

在这里补充一些相关的管道符

- 1、|（就是按位或），直接执行|后面的语句
- 2、||（就是逻辑或），如果前面命令是错的那么就执行后面的语句，否则只执行前面的语句
- 3、&（就是按位与），&前面和后面命令都要执行，无论前面真假
- 4、&&（就是逻辑与），如果前面为假，后面的命令也不执行，如果前面为真则执行两条命令
- 5、;（linux下有的，和&一样的作用）