初试ctf

原创

Tangthr 于 2019-02-19 15:52:09 发布 1392 收藏 33

分类专栏： ctf 文章标签： ctf

本文链接：https://blog.csdn.net/c1042503039/article/details/87657391

ctf 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

初试CTF

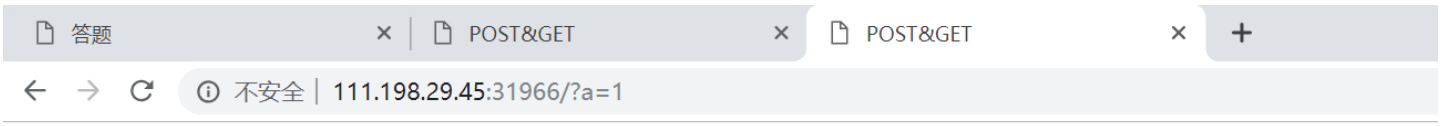
在朋友的推荐下，在攻防世界里练ctf，借博客总结加深记忆。

1、当不能用右键打开源代码时，在url前输入view-source: 即可看到网页源代码

2、以get和post方式提交参数

请用GET方式提交一个名为a,值为1的变量

按照提示，用get方式提交参数，直接在url后面加上/?a=1(?应该是统一格式吧)，我在这犯了一个错误，符号不小心用了中文形式的。



请用GET方式提交一个名为a,值为1的变量

请再以POST方式随便提交一个名为b,值为2的变量

再以post方式提交b=2，此时要用到火狐里的hackbar插件

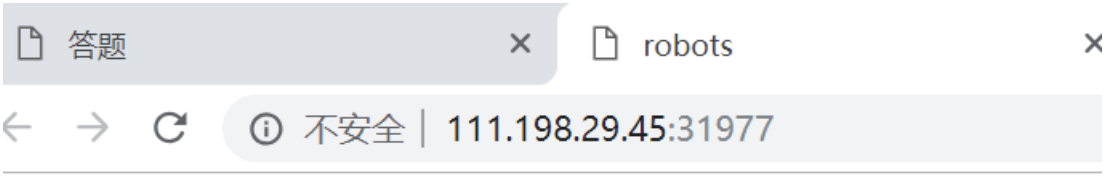
请用GET方式提交一个名为a,值为1的变量

请再以POST方式随便提交一个名为b,值为2的变量

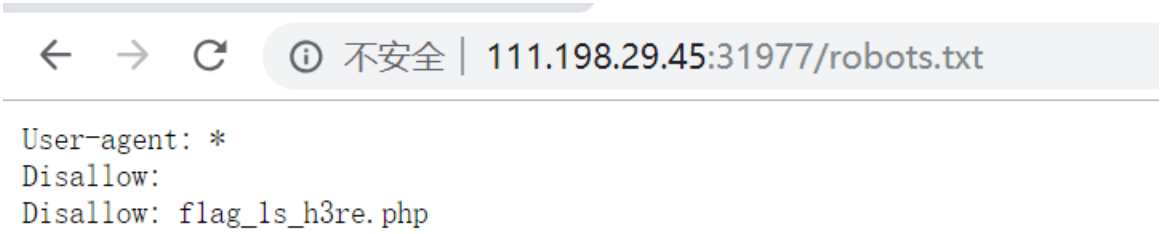
xctf{f0f453f4cf9833d4338d1853b2fa3322}

flag就出现了

3、robots协议



可以根据经验，直接在url后面加上/robots.txt

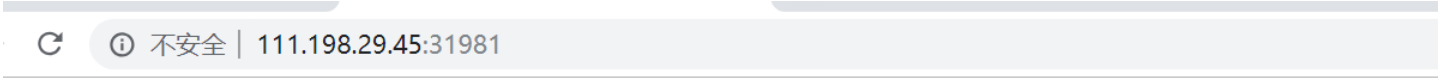


之前到这就不会了，在朋友的提示下。访问f1ag_1s_h3re.php文件，即把robots.txt换成f1ag_1s_h3re.php。

xctf{9e8499d961a52914a15b54516651320b}

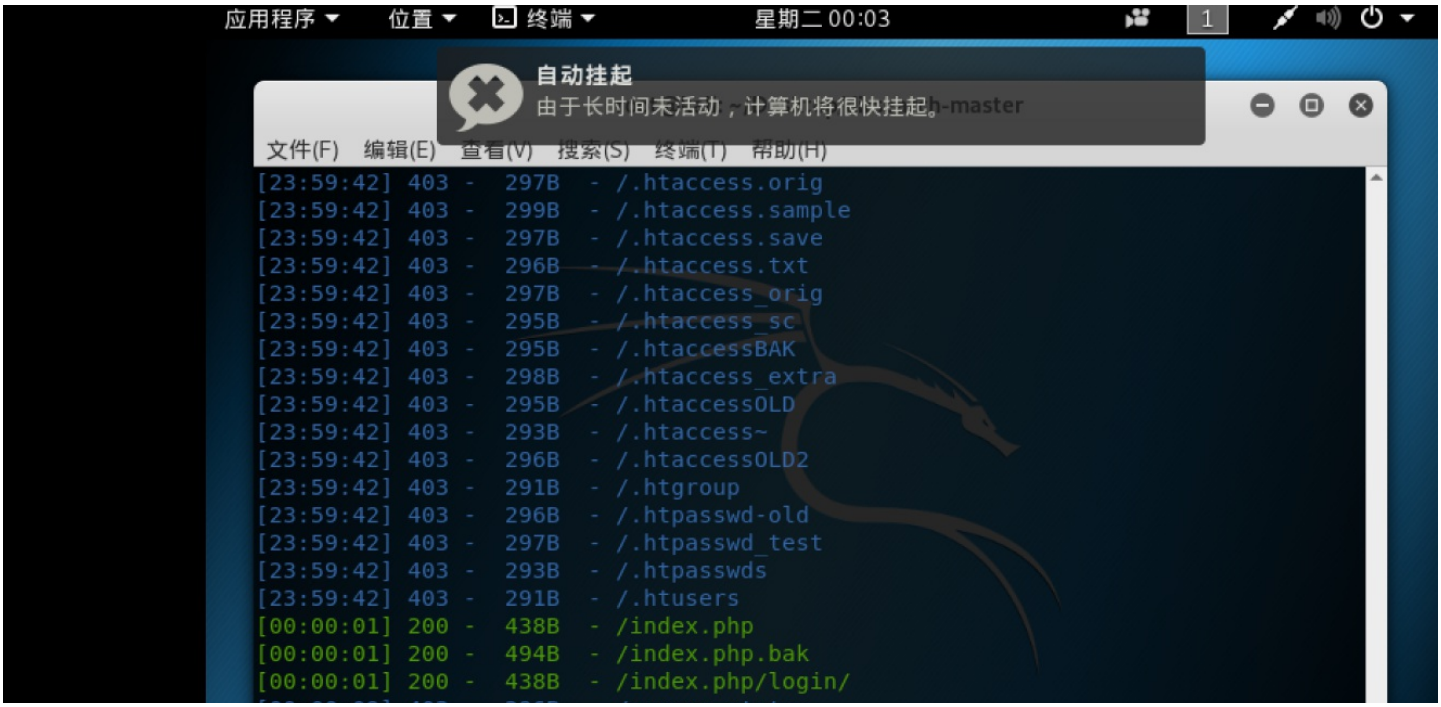
这里要介绍一个神器，dirsearch，扫目录脚本，通过dirsearch也可以发现robots.txt

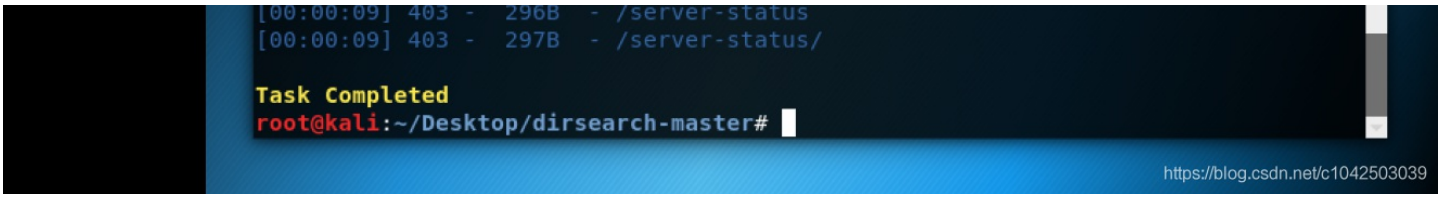
4、备份文件



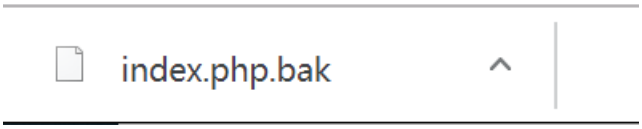
你知道index.php的备份文件名吗?

不知道没关系，用dirsearch可以扫描出来



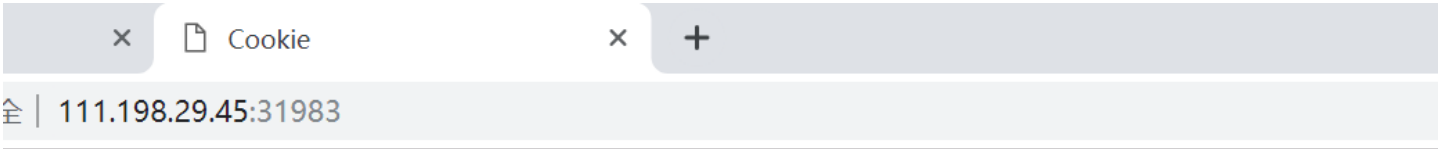


在url后面输入/index.php.bak,输入完后它会下载一个文件



打开即可

5、cookie



你知道什么是cookie吗?

老方法，先用dirsearch扫描一波（有经验的人应该都不用扫描了），在url后输入cookie.php

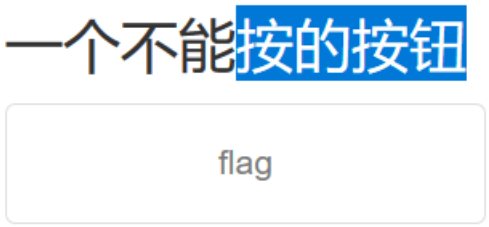
111.198.29.45:31983/cookie.php

See the http response

之后根据提示，打开开发者工具看响应头，即可发现flag

See the http response

6、如图



f12，查看器，吧disabled=""删喽，即可