

XCTF web刷题

原创

Assass1n- 于 2022-01-23 16:50:33 发布 17 收藏

分类专栏: [ctf](#) 文章标签: [前端](#) [蓝桥杯](#) [职场和发展](#)

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_63685461/article/details/122653360

版权



[ctf](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

1.view_source

FLAG is not here

进入题目所给环境出现

CSDN @Assass1n-

题目来源: [Cyberpeace-n3k0](#)

题目描述: X老师让小宁同学查看一个网页的源代码, 但小宁同学发现鼠标右键好像不管用了。

CSDN @Assass1n-

```
body> == $0
<script>...</script>
<h1>FLAG is not here</h1>
```

提示鼠 标右键不管用 就F12查看网页源代码

直接找到flag

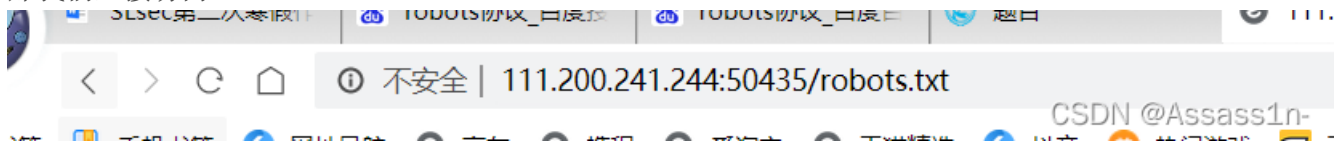
2.robots

根据题目搜索robots协议

robots协议也叫**robots.txt** (统一小写) 是一种存放于**网站**根目录下的**ASCII**编码的**文本文件**, 它通常告诉网络**搜索引擎**的漫游器 (又称**网络蜘蛛**), 此网站中的哪些内容是不应被搜索引擎的漫游器获取的, 哪些是可以被漫游器获取的。因为一些系统中的URL是大小写敏感的, 所以robots.txt的文件名应统一为小写。robots.txt应放置于网站的根目录下。如果想单独定义搜索引擎的漫游器访问子目录时的行为, 那么可以将自定的设置合并到根目录下的robots.txt, 或者使用**robots元数据** (Metadata, 又称元数据)。

robots协议并不是一个规范, 而只是约定俗成的, 所以并不能保证网站的隐私

那我们直接访问



```
User-agent: *
Disallow:
Disallow: flag_1s_h3re.php
```

CSDN @Assass1n-

出现这个东西我们直接访问第二个在原来环境网站后面加上

`flag_1s_h3re.php`

得到flag `cyberpeace{e0802351a7dd0ada52f9032dcb9f5ed2}`

3.backup

进入题目环境

你知道index.php的备份文件名吗?

CSDN @Assass1n-

给出提示 百度

常见的备份文件后缀名有：“.git”、“.svn”、“.swp”、“.”、“.bak”、“.bash_history”、“.bkf”

那我们在 url后面加上index.php 并查找备份文件根据题目 可以得知是bak文件

新建下载任务 ×

地址

文件名

保存到 浏览

开启静默下载，下载时不弹出下载框。

下载并打开 下载 取消

CSDN @Assass1n-

会弹出一个文件下载 下载后打开就能得到flag