

robots-xctf攻防世界

原创

H3CFly 于 2021-11-19 11:52:48 发布 916 收藏

分类专栏: [CTF 网络安全](#) 文章标签: [前端](#) [网络安全](#)

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/weixin_46168073/article/details/121419236

版权



[CTF 同时被 2 个专栏收录](#)

12 篇文章 0 订阅

订阅专栏



[网络安全](#)

34 篇文章 0 订阅

订阅专栏

一、解析

可以看到

The screenshot shows a CTF challenge interface. At the top, there is a '返回' (Return) button and a star icon with the text '本题用时: 42秒'. Below this, the challenge title 'robots' is displayed with a thumbs-up icon and '276' likes, and a note '最佳Writeup由MOLLMY提供'. The difficulty coefficient is shown as '★ 1.0'. The source is 'Cyberpeace-n3k0'. The description reads: 'X老师上课讲了Robots协议, 小宁同学却上课打了瞌睡, 赶紧来教教小宁Robots协议是什么吧。'. There is a button '点击获取在线场景' under the '题目场景:' label. The '题目附件:' section shows '暂无'. In the bottom right corner, it says 'CSDN @H3CFly'.

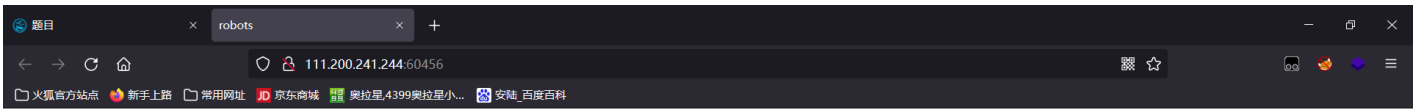
这是一个对robots协议的利用。

robots协议, 基本上在渗透别人的时候是算是重要的, 这个决定了爬虫能爬那些东西, 那些东西不能爬取。

二、做题

点击进入题目。

可以看到进去之后一片空白。



CSDN @H3CFly

我们在URL的后面输入robots.txt



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

CSDN @H3CFly

然后他就出来了东西。

可以看到他说：不允许爬取flag_1s_h3re.php

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

那我们直接在URL后面打上flag_1s_h3re.php



CSDN @H3CFly

然后我们就得到了flag，复制粘贴到记事本，提交就行。



CSDN @H3CFly