

XCTF新手区Web解题Writeup

原创

[Harvey丶北极熊](#)



于 2019-10-27 12:40:13 发布



858



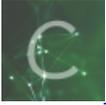
收藏 3

分类专栏: [CTF](#) 文章标签: [ctf](#)

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_38867330/article/details/102765463

版权



[CTF 专栏收录该内容](#)

20 篇文章 3 订阅

订阅专栏

[view_source](#)

view_source



最佳Writeup由Healer_aptx • Anchorite提供

难度系数:



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。

题目场景:

http://111.198.29.45:56060

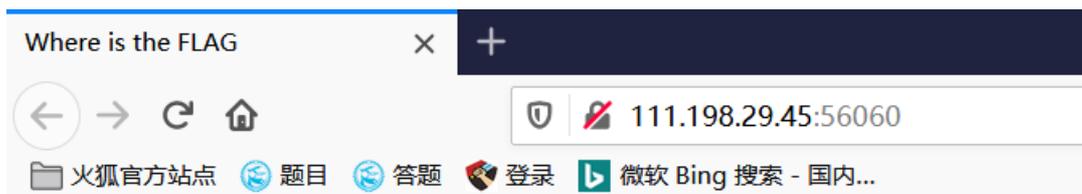
删除场景

倒计时: 03:59:27

延时

题目附件: 暂无

https://blog.csdn.net/qq_38867330



FLAG is not here

https://blog.csdn.net/qq_38867330

打开题目后显示FLAG is not here, 而且题目描述提示鼠标右键不管用了。这时想到F12键打开开发者工具, 查看器可以查看页面源代码。F12 —— 查看器直接得到答案。



https://blog.csdn.net/qq_38867330

get_post

get_post

👍 12

最佳Writeup由神秘人·柒爷提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

题目描述: X老师告诉小宁同学HTTP通常使用两种请求方法,你知道是哪两种吗?

题目场景:  http://111.198.29.45:45651

删除场景

倒计时: 03:59:47

题目附件: 暂无

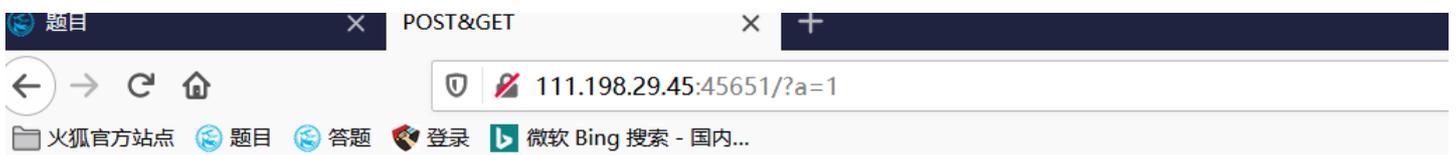
https://blog.csdn.net/qq_38867330



请用GET方式提交一个名为a,值为1的变量

https://blog.csdn.net/qq_38867330

看一下题目,要求“请用GET方式提交一个名为a,值为1的变量”,GET方式一般为在url后拼接参数,只能以文本的方式传递参数。因此直接在http://111.198.29.45:39706/后进行拼接http://111.198.29.45:39706/?a=1,输出结果为

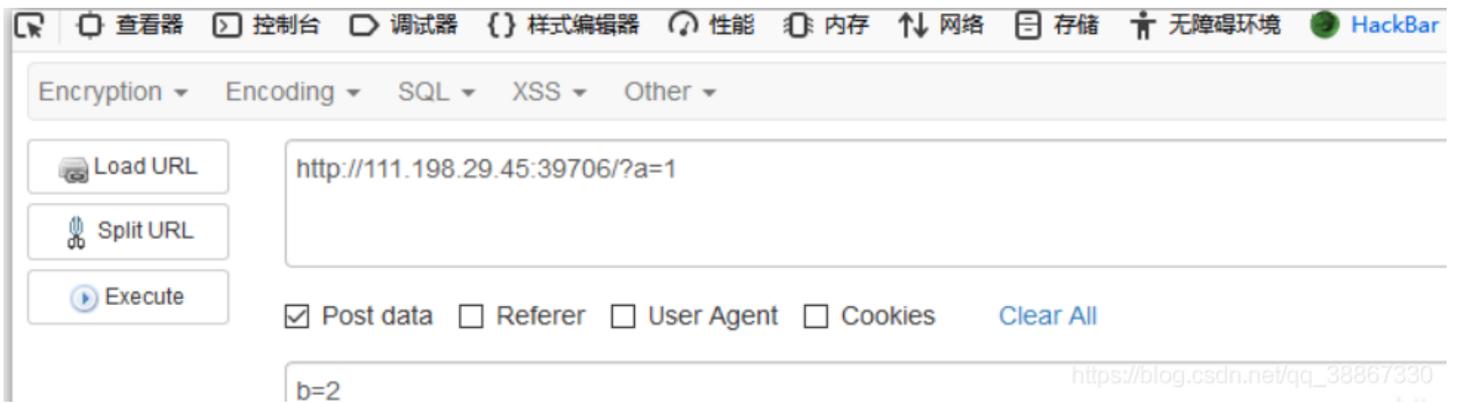


请用GET方式提交一个名为a,值为1的变量

请再以POST方式随便提交一个名为b,值为2的变量

https://blog.csdn.net/qq_38867330

以get方式提交参数后,然后要求“请再以POST方式随便提交一个名为b,值为2的变量”,提交post请求用火狐插件hackbar(增加组件找扩展)



执行后输出cyberpeace{xxxxxxxxxxxxxxxxxxxxxxxxxxxx}



robots

robots



最佳Writeup由MOLLMY提供

难度系数:



题目来源:

Cyberpeace-n3k0

题目描述: 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。

题目场景:

http://111.198.29.45:38353

删除场景

倒计时: 03:59:54

延时

题目附件: 暂无

https://blog.csdn.net/qq_38867330

熟悉一下Robots协议

Robots协议 (也称为爬虫协议、机器人协议等) 的全称是“网络爬虫排除标准”(Robots Exclusion Protocol), 网站通过Robots协议告诉搜索引擎哪些页面可以抓取, 哪些页面不能抓取。

robots协议通常以robots.txt存在, robots.txt文件是一个文本文件, robots.txt是一个协议, 而不是一个命令。robots.txt是搜索引擎中访问网站的时候要查看的第一个文件。robots.txt文件告诉蜘蛛程序在服务器上什么文件是可以被查看的。

robots.txt文件写法:

User-agent: * 这里的代表的所有的搜索引擎种类, 是一个通配符

Disallow: /admin/ 这里定义是禁止爬寻admin目录下面的目录

Disallow: /require/ 这里定义是禁止爬寻require目录下面的目录

Disallow: /ABC/ 这里定义是禁止爬寻ABC目录下面的目录

Disallow: /cgi-bin/.htm 禁止访问/cgi-bin/目录下的所有以".htm"为后缀的URL(包含子目录)。

Disallow: /* 禁止访问网站中所有包含问号(?)的网址

Disallow: /.jpg\$ 禁止抓取网页所有的.jpg格式的图片

Disallow:/ab/adc.html 禁止爬取ab文件夹下面的adc.html文件。

Allow: /cgi-bin/ 这里定义是允许爬寻cgi-bin目录下面的目录

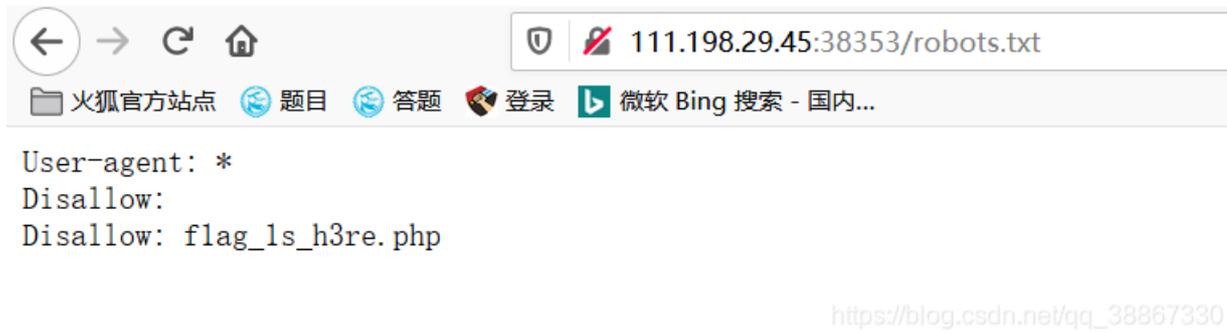
Allow: /tmp 这里定义是允许爬寻tmp的整个目录

Allow: .htm\$ 仅允许访问以".htm"为后缀的URL。

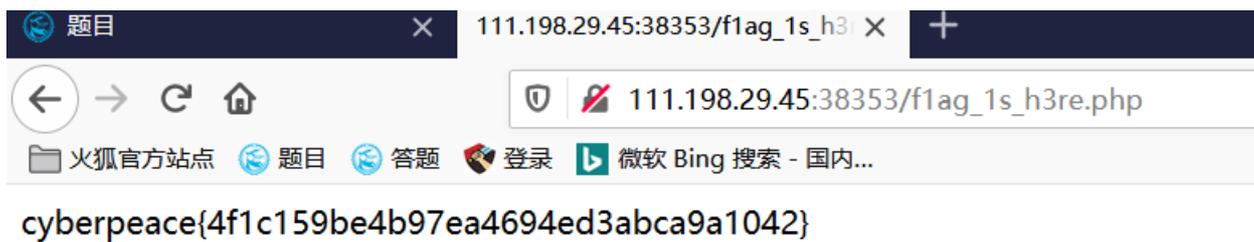
Allow: .gif\$ 允许抓取网页和gif格式图片

Sitemap: 网站地图 告诉爬虫这个页面是网站地图

看一下题目，在题目给出的URL后输入/robots.txt即http://111.198.29.45:49905/robots.txt后显示



flag_1s_h3re.php表示这个页面不允许被爬取，接下来查看一下flag_1s_h3re.php页面得到正确答案



backup

backup 👍 7 最佳Writeup由话求·樱宁提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

题目描述: X老师忘记删除备份文件，他派小宁同学去把备份文件找出来，一起来帮小宁同学吧!

题目场景: 🖥️ http://111.198.29.45:43201

删除场景

倒计时: 03:59:46 延时

题目附件: 暂无

https://blog.csdn.net/qq_38867330



你知道index.php的备份文件名吗?

https://blog.csdn.net/qq_38867330

打开题目后提示“你知道index.php的备份文件”，备份文件通常为文件名+.bak。输入后提示下载

111.198.29.45:43201/index.php.bak

微软 Bing 搜索 - 国内...



https://blog.csdn.net/qq_38867330

```
aos.py x index.php.bak x
<html>
<head>
<meta charset="UTF-8">
<title>备份文件</title>
<link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
<style>
  body{
    margin-left:auto;
    margin-right:auto;
    margin-TOP:200PX;
    width:20em;
  }
</style>
</head>
</html>
```

```
    </style>
</head>
<body>
<h3>你知道index.php的备份文件名吗? </h3>
<?php
$flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"
?>
</body>
</html>
```

https://blog.csdn.net/qq_38867330

就先分享四道题的Writeup，剩下的请听下回分解。