

攻防世界(Xctf)web题新手练习区writeup

原创

秋风瑟瑟...  于 2020-02-19 00:29:31 发布  3232  收藏 5

分类专栏: [笔记](#) 文章标签: [web 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/qq_45628145/article/details/104385452

版权



[笔记 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

攻防世界(Xctf)web题新手练习区Writeup

这里是攻防世(Xctf)平台上面新手练习区web题的writeup, 我也是个新手, 如果有什么不对的地方, 欢迎大家指出, 如果大家觉得写的不错的话, 别忘了点个赞哦!

1.view_source

返回 本题用时: 1分41秒

view_source 38 最佳Writeup由Healer_aptx • Anchorite提供

难度系数: ★ 1.0

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://111.198.29.45:37846

删除场景

倒计时: 03:59:48 延时

题目附件: 暂无

https://blog.csdn.net/qq_45628145

进入之后, 根据题目给的提示view_source和鼠标右键好像坏了, 进入之后, 是这样的界面。

111.198.29.45:37846

火狐官方网站 新手上路 常用网址 CTF

FLAG is not here

于是按f12, 查看源码, 发现flag。

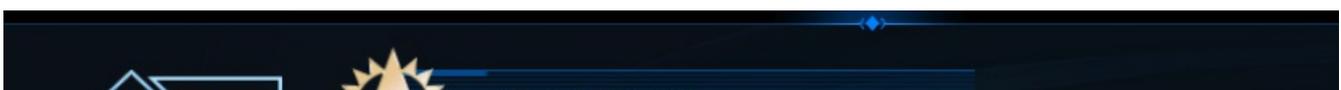
查看器 控制台 调试器 网络 样式编辑器 性能 内存

搜索 HTML

```
<!DOCTYPE html>
<html lang="en">
  <head>
  </head>
  <body>
    <script>
      <h1>FLAG is not here</h1>
      <!--cyberpeace{bb781a16c77edca52df8c403f5d2381d}-->
    </body>
  </html>
```

https://blog.csdn.net/qq_45628145

2.robots





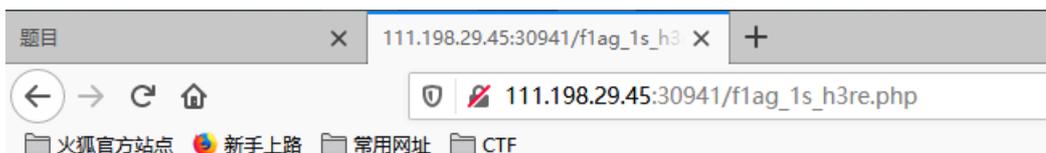
进入页面之后，什么都没有，根据题目提示，去搜索robots协议，下图来源于百度百科。



于是进入robots.txt，看到这样的界面。



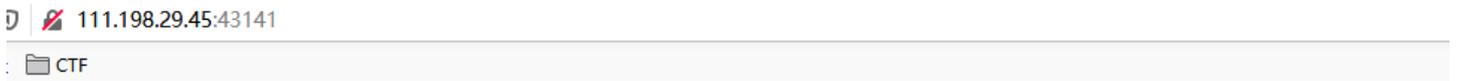
根据网上查询到的有关robots协议知识点，进入flag_1s_h3re.php，得到flag。



3.backup

The screenshot shows a CTF challenge interface for a challenge named 'backup'. It includes a difficulty coefficient of 1.0, a source of 'Cyberpeace-n3k0', and a description: '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!'. The challenge scene is 'http://111.198.29.45:43141' with a '删除场景' (Delete Scene) button. A timer shows '03:59:40' with a '延时' (Extend) button. The challenge has 14 likes and is a '最佳Writeup' (Best Writeup) by '话求·樱宁提供'. The URL 'https://blog.csdn.net/qq_45628145' is visible at the bottom right.

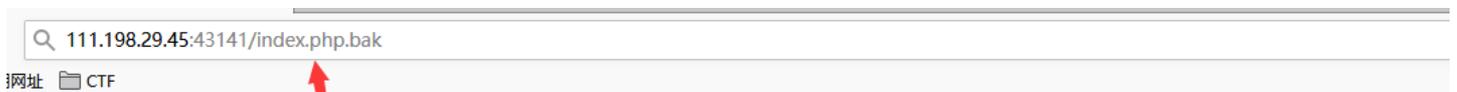
进入之后，发现问我们知不知道index.php的备份文件吗？



你知道index.php的备份文件名吗？

https://blog.csdn.net/qq_45628145

于是进入index.php.bak。



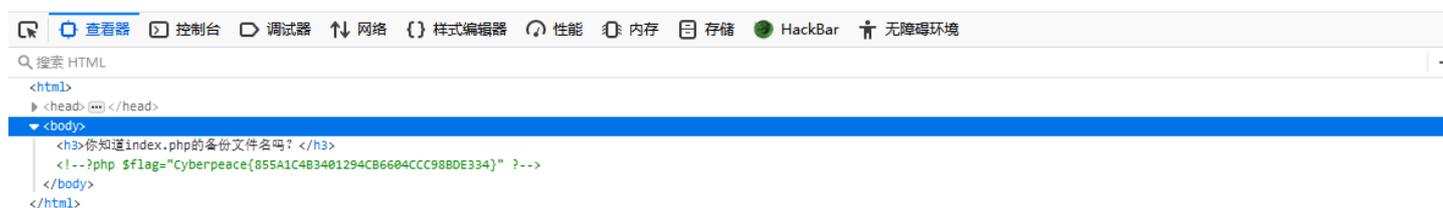
你知道index.php的备份文件名吗?



https://blog.csdn.net/qq_45628145

打开之后，查看源码，得到flag。

你知道index.php的备份文件名吗?



https://blog.csdn.net/qq_45628145

4.cookie

cookie 最佳Writeup由神秘人·孔雀翎提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

题目描述: X老师告诉小宁他在cookie里放了东西,小宁疑惑地想:‘这是夹心饼干的意思吗?’

题目场景: 0%

进入之后, 发现问我们知不知道cookie吗。

111.198.29.45:54758

CTF

你知道什么是cookie吗?

https://blog.csdn.net/qq_45628145

于是查看cookie, 发现线索。

The screenshot shows the 'Cookie' tab in a browser's developer tools. The 'Response' pane is expanded to show the 'Response Headers' section. The 'Set-Cookie' header is highlighted with a red arrow, indicating the value 'look-here=cookie.php'. Other headers include 'Connection: Keep-Alive', 'Content-Encoding: gzip', 'Content-Length: 276', 'Content-Type: text/html', 'Date: Tue, 18 Feb 2020 16:02:38 GMT', 'Keep-Alive: timeout=5, max=100', 'Server: Apache/2.4.7 (Ubuntu)', 'Vary: Accept-Encoding', and 'X-Powered-By: PHP/5.5.9-1ubuntu4.26'. The 'Request Headers' section is also visible, showing 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8'.

根据线索进入cookie.php, 得到这样的页面。

111.198.29.45:54758/cookie.php

CTF

See the http response

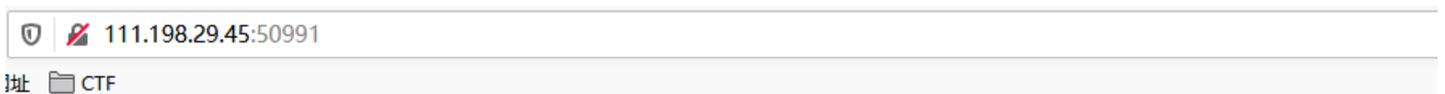
于是查看http的response，得到flag。



5.disabled_button

The image shows a CTF challenge page for 'disabled_button'. It has a difficulty coefficient of 1.0 (indicated by a star icon) and 13 likes. The source is 'Cyberpeace-n3k0'. The description reads: 'x老师今天上课讲了前端知识，然后给大家一个不能按的按钮，小宁惊奇地发现这个按钮按不下去，到底怎么才能按下去呢？'. The progress bar shows 4% completion. The page footer includes the URL 'https://blog.csdn.net/qq_45628145'.

进入之后，发现一个按不了的按钮。



一个不能按的按钮



https://blog.csdn.net/qq_45628145

于是查看源码，发现了一点东西。

```
<html>
  <head> ... </head>
  <body>
    <h3>一个不能按的按钮</h3>
    <form action="" method="post">
      <input class="btn btn-default" disabled="" style="height:50px;width:200px;" type="submit" value="flag" name="auth">
    </form>
  </body>
</html>
```

这是disabled属性的介绍，来源于w3school。

定义和用法

disabled 属性规定应该禁用 input 元素。

被禁用的 input 元素既不可用，也不可点击。可以设置 disabled 属性，直到满足某些其他的条件为止（比如选择了一个复选框等等）。然后，就需要通过 JavaScript 来删除 disabled 值，将 input 元素的值切换为可用。

注释： disabled 属性无法与 <input type="hidden"> 一起使用。

于是我们删去该属性。

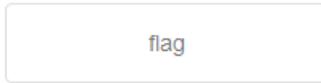
一个不能按的按钮



```
查看器 控制台 调试器 网络 {} 样式编辑器 性能 内存 存储 HackBar 无障碍环境
. 搜索 HTML
<html>
  <head> ... </head>
  <body>
    <h3>一个不能按的按钮</h3>
    <form action="" method="post">
      <input class="btn btn-default" style="height:50px;width:200px;" type="submit" value="flag" name="auth">
    </form>
  </body>
</html>
```

flag按钮就可以按了，点击按钮，得到flag。

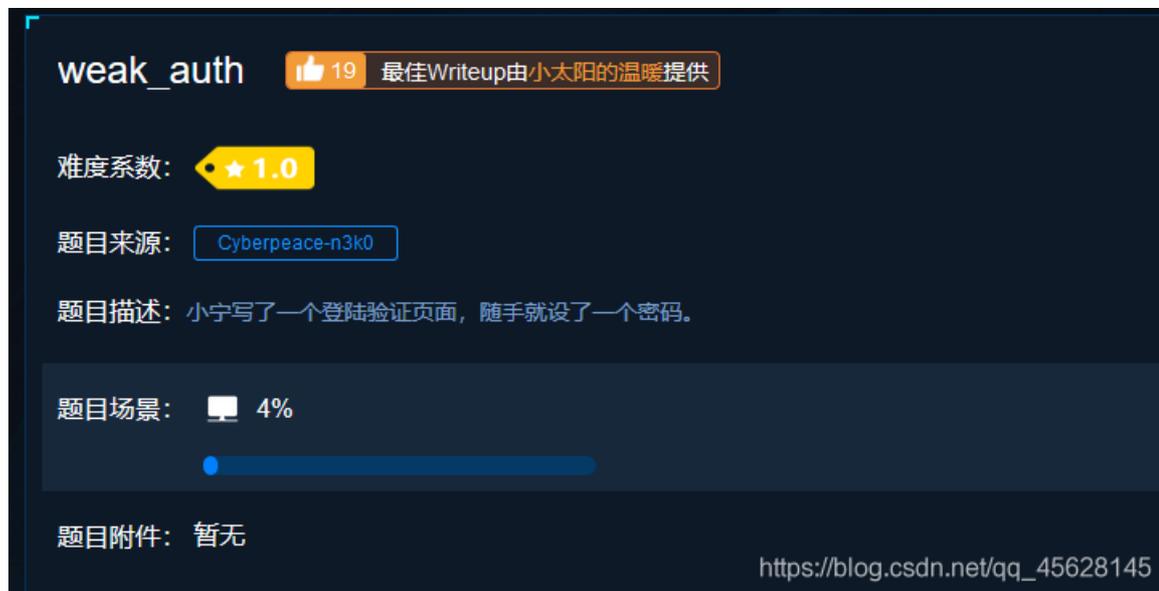
一个不能按的按钮



cyberpeace{032cf8f4977d2a4edf0728d0323bbbb8}

https://blog.csdn.net/qq_45628145

6.weak_auth



weak_auth 👍 19 最佳Writeup由小太阳的温暖提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

题目描述: 小宁写了一个登陆验证页面，随手就设了一个密码。

题目场景: 🖥️ 4%

题目附件: 暂无

https://blog.csdn.net/qq_45628145

进入之后，是一个登录页面。

Login

https://blog.csdn.net/qq_45628145

根据题名以及题目描述的提示，进行弱口令登录，admin，密码我先试的123456，还真对了，登陆进去之后，得到flag。

Login

https://blog.csdn.net/qq_45628145

cyberpeace{c22d00f91291d31a704e6073ce53d65a}