

XCTF刷题笔记

原创

419xs 于 2021-09-28 00:05:14 发布 1141 收藏

分类专栏: [XCTF](#) 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_43323728/article/details/120520084

版权



[XCTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

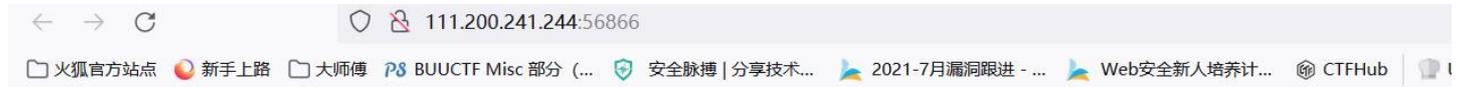
XCTF刷题笔记

1.view_source

难度: 1.0

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。

打开题目, 提示FLAG不在此处

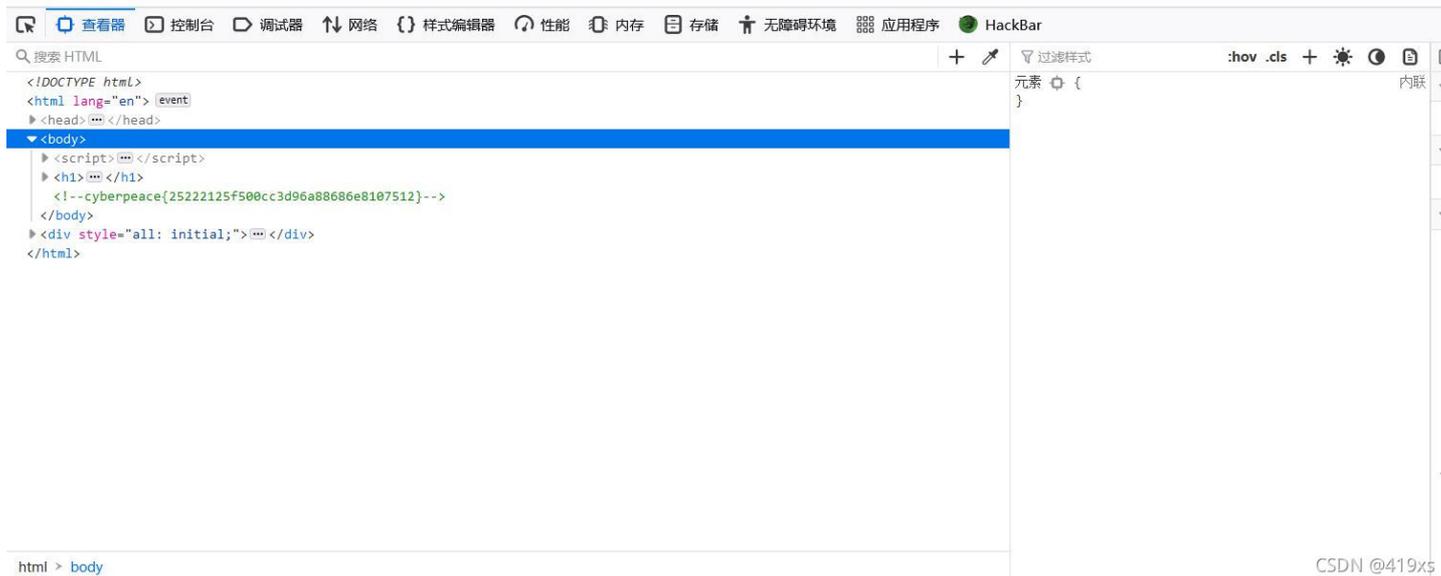


FLAG 不在此处

CSDN @419xs

按F12查看源代码

FLAG 不在这里



知识点: F12查看源码

FLAG: cyberpeace{25222125f500cc3d96a88686e8107512}

2.robots

难度: 1.0

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。

打开题目, 发现是空白页



访问url/robots.txt,发现Disallow: f1ag_1s_h3re.php



访问url/f1ag_1s_h3re.php,获得FLAG



知识点: robots协议

FLAG:cyberpeace{8a444833ca561069c252f1dc3f24ab3f}

3.backup

难度: 1.0

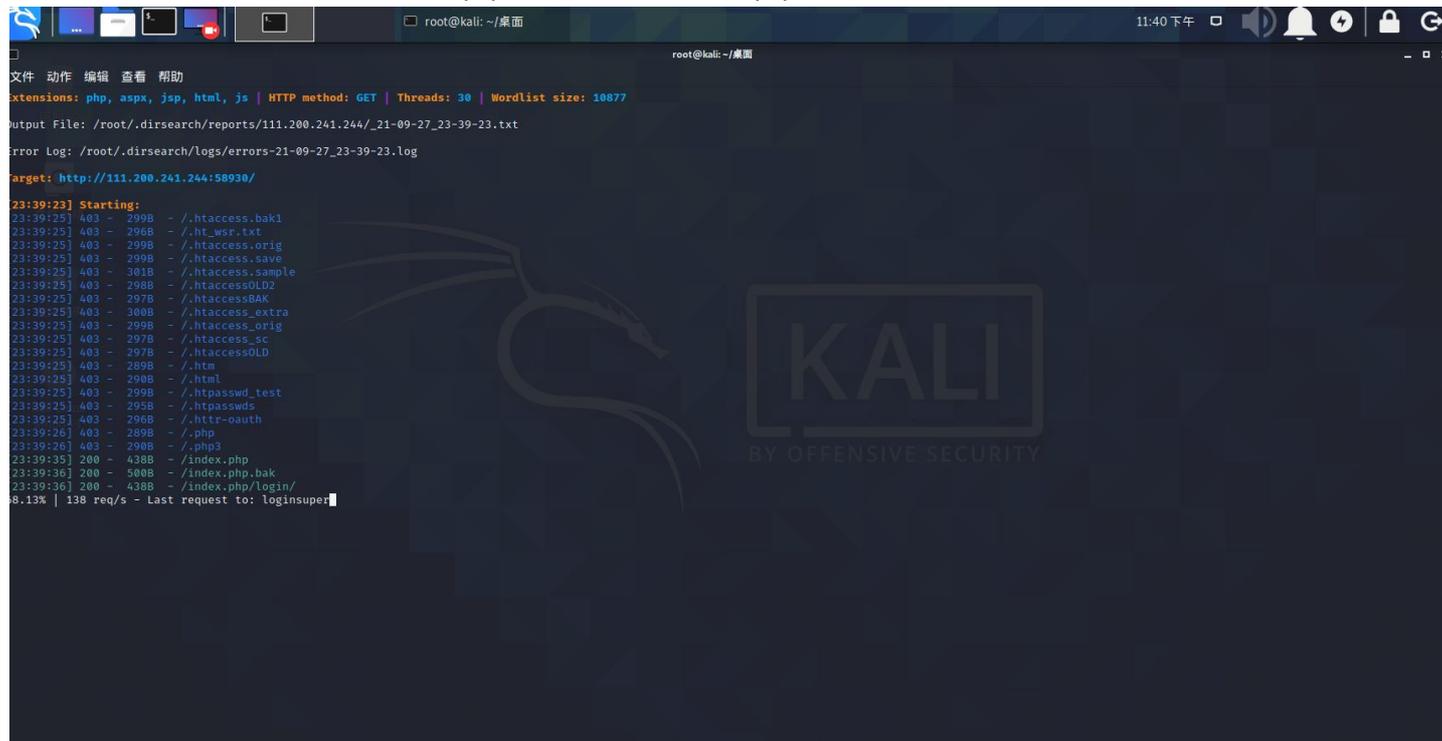
题目描述: X老师忘记删除备份文件, 他派小宁同学去把备份文件找出来,一起来帮小宁同学吧!

打开题目，提示，你知道index.php的备份文件名吗？

你知道index.php的备份文件名吗？

CSDN @419x5

使用dirsearch进行目录扫描，发现index.php.bak,此文件就是index.php的备份文件



```
extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10877
Output File: /root/.dirsearch/reports/111.200.241.244/_21-09-27_23-39-23.txt
Error Log: /root/.dirsearch/logs/errors-21-09-27_23-39-23.log
target: http://111.200.241.244:58930/

23:39:23] Starting:
23:39:25] 403 - 299B - /.htaccess.bak1
23:39:25] 403 - 296B - /.ht_wsr.txt
23:39:25] 403 - 299B - /.htaccess.orig
23:39:25] 403 - 299B - /.htaccess.save
23:39:25] 403 - 301B - /.htaccess.sample
23:39:25] 403 - 298B - /.htaccessOLD2
23:39:25] 403 - 297B - /.htaccessBAK
23:39:25] 403 - 300B - /.htaccess_extra
23:39:25] 403 - 299B - /.htaccess_orig
23:39:25] 403 - 297B - /.htaccess_sc
23:39:25] 403 - 297B - /.htaccessOLD
23:39:25] 403 - 289B - /.htm
23:39:25] 403 - 290B - /.html
23:39:25] 403 - 299B - /.htpasswd_test
23:39:25] 403 - 295B - /.htpasswd
23:39:25] 403 - 296B - /.httr-oauth
23:39:26] 403 - 289B - /.php
23:39:26] 403 - 290B - /.php3
23:39:35] 200 - 438B - /index.php
23:39:36] 200 - 500B - /index.php.bak
23:39:36] 200 - 438B - /index.php/login/
8.13% | 138 req/s - Last request to: login:super
```

指针从虚拟机中移出或按 Ctrl+Alt,

CSDN @419x5

访问url/index.php.bak,下载备份文件,记事本打开,发现FLAG



```
index.php.bak - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<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>
<body>
<h3>你知道index.php的备份文件名吗? </h3>
<?php
flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"
'>
</body>
</html>
```

第 18 行, 第 52 列 100% Windows (CRLF) UTF-8 @419x5

知识点: .bak备份文件

FLAG: Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

4.cookie

难度: 1.0

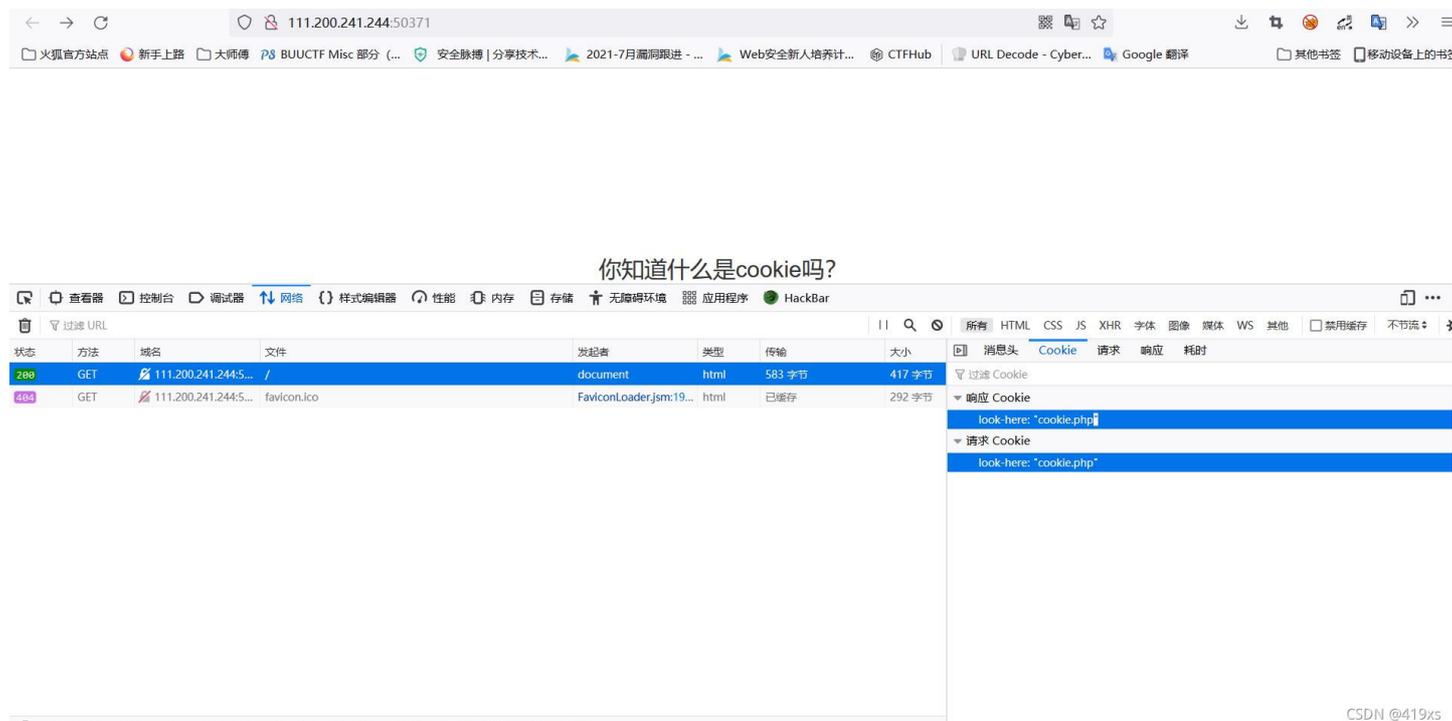
题目描述: X老师告诉小宁他在cookie里放了些东西,小宁疑惑地想:“这是夹心饼干的意思吗?”

打开题目,“你知道什么是cookei吗”

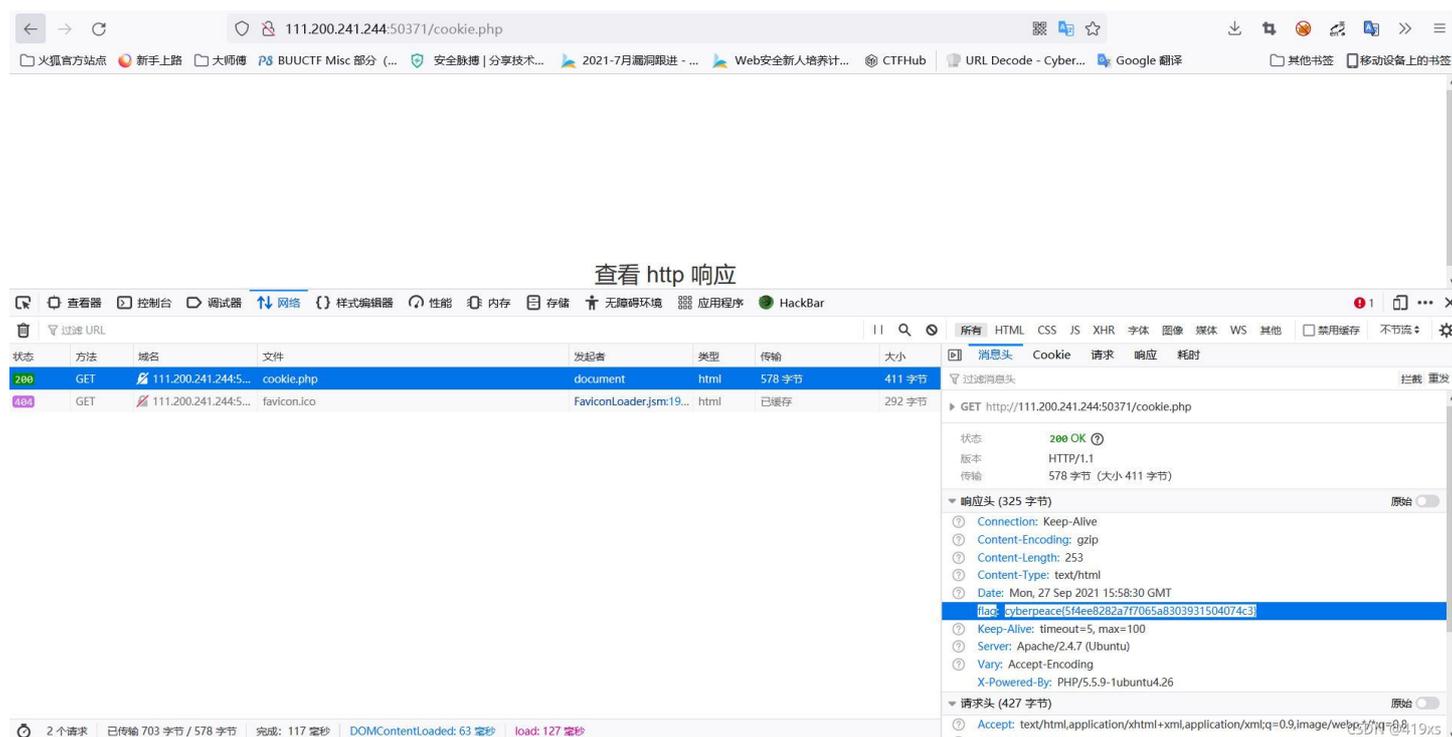


你知道什么是cookie吗?

F12查看cookie, 提示cookie.php



访问cookie.php,提示查看http响应, F12查看, 响应头flag字段得到FLAG



知识点: cookie

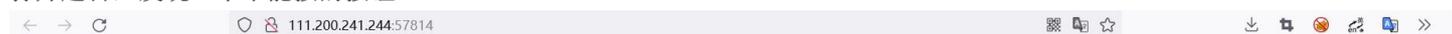
FLAG:cyberpeace{5f4ee8282a7f7065a8303931504074c3}

5.disabled_button

难度: 1.0

题目描述: 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?

打开题目, 发现一个不能按的按钮



知识点: disabled属性

FLAG:cyberpeace{10d1c43f393fff927e8304de5e46541a}