

# 攻防世界web入门writeup

原创

shallon6 于 2022-02-27 17:38:06 发布 385 收藏

分类专栏: [信安之路](#) 文章标签: [爬虫](#) [pycharm](#) [ide](#)

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/u012839564/article/details/123049216>

版权



[信安之路](#) 专栏收录该内容

3 篇文章 2 订阅

订阅专栏

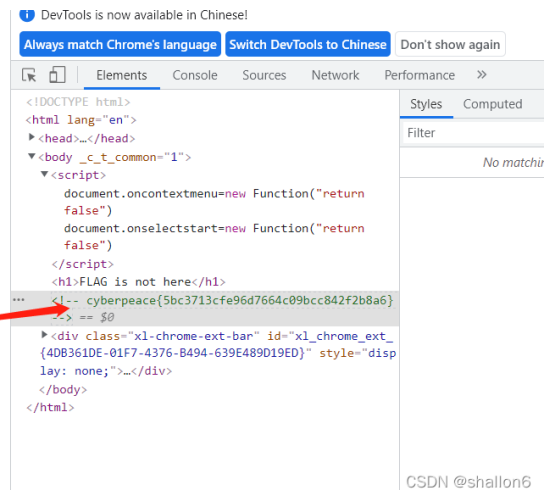
1.view\_source

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。

打开网址后发现无法右键查看源代码, 禁用了右键, 所以我们采用按下F12查看源代码

直接获取flag `cyberpeace{5bc3713cfe96d7664c09bcc842f2b8a6}`

## FLAG is not here



## 2.robots

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。

打开网址发现是空白页面, 于是根据题目提示robots.txt 据我所理解就是禁止爬虫爬取信息的一个文件, 文件内的东西爬虫不会进行爬取, 于是我们在网址后面加上/robots.txt

← → ↻ ⚠ 不安全 | 111.200.241.244:58847/robots.txt

```
User-agent: *  
Disallow:  
Disallow: flag_ls_h3re.php
```

CSDN @shallon6

得知禁止爬取flag\_ls\_h3re.php这个文件，于是我们访问顺利的到  
flag cyberpeace{a7d28e5084a603f2ed351244c45e962b}

← → ↻ ⚠ 不安全 | 111.200.241.244:58847/flag\_ls\_h3re.php

cyberpeace{a7d28e5084a603f2ed351244c45e962b}

CSDN @shallon6

3.backup

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！

⚠ 不安全 | 111.200.241.244:60139

你知道index.php的备份文  
文件名吗？

CSDN @shallon6

php的备份文件一般是 xxx.php.bak 于是我们访问看看，下载得到一个index.php.bak

你知道index.php的备份文件名吗?

```
index.php.bak - 记事本
文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)
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>
```

CSDN @shallon6

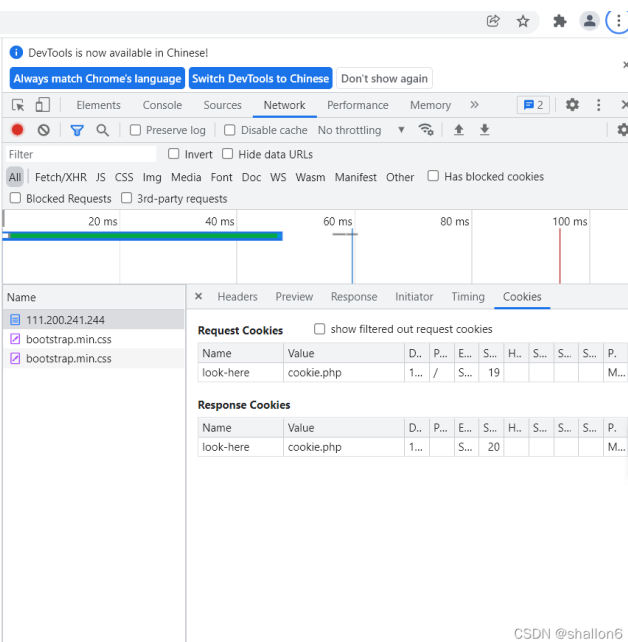
顺利得到flag Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

#### 4.cookie

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？’

我们摁下F12查看网页cookie

你知道什么是cookie吗?



Name	Value	D...	P...	E...	S...	H...	S...	S...	P...
look-here	cookie.php	1...	/	S...	19				M...

Name	Value	D...	P...	E...	S...	H...	S...	S...	P...
look-here	cookie.php	1...		S...	20				M...

CSDN @shallon6

提示我们打开cookie.php

See the http response

DevTools is now available in Chinese!

Always match Chrome's language Switch DevTools to Chinese Don't show again

Elements Console Sources Network Performance Memory

Filter: [x] Invert [x] Hide data URLs

All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other [x] Has blocked cookies

[x] Blocked Requests [x] 3rd-party requests

20 ms 40 ms 60 ms 80 ms 100 ms

Name: cookie.php, bootstrap.min.css, bootstrap.min.css

General

Request URL: http://111.200.241.244:51350/cookie.php

Request Method: GET

Status Code: 200 OK

Remote Address: 111.200.241.244:51350

Referrer Policy: strict-origin-when-cross-origin

Response Headers

Connection: Keep-Alive

Content-Encoding: gzip

Content-Length: 253

Content-Type: text/html

Date: Mon, 21 Feb 2022 08:12:13 GMT

flag: cyberpeace{3d33571d082ea9819c000e573533db0a}

Keep-Alive: timeout=5, max=100

Server: Apache/2.4.7 (Ubuntu)

Vary: Accept-Encoding

CSDN @shallon6

根据提示打开http头得到flag cyberpeace{3d33571d082ea9819c000e573533db0a}

## 5.disabled\_button

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？

打开网址，我们摁下f12找到对应按钮的代码，删去disabled 再次摁下flag得到

cyberpeace{7f42256b1e79b4e5f7659352d831bf6a}

→ C 不安全 | 111.200.241.244:52448

DevTools is now available in Chinese!

Always match Chrome's language Switch DevTools to Chinese

Elements Console Sources Network Pe

<html>

><head>...</head>

><body \_c\_t\_common="1">

><h3>一个不能按的按钮</h3>

><form action method="post">

>><input disabled class="btn btn-default" style="height:50px;width:200px;" type="submit" value="flag" name="auth"> == \$0

></form>

>><div class="xl-chrome-ext-bar" id="xl\_chrome\_ext\_{40B361DE-01F7-4376-B494-639E489D19ED}" style="display: none;">...</div>

></body>

></html>

CSDN @shallon6

一个不能按的按钮

flag

## 6.weak\_auth

小宁写了一个登陆验证页面，随手就设了一个密码。

## Login

CSDN @shallon6

假设随便登录就会报这样的错

**please login as admin**

所以我们就登陆admin

密码就admin 123456等弱密码试一下然后就通关了

得到flag cyberpeace{fce97ad34b590ad7e9c26b4c515a6ca2}

### 7.simple\_php

小宁听说php是最好的语言,于是她简单学习之后写了几行php代码。

```
<?php
show_source( FILE );
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0 and $a){
    echo $flag1;
}
if(is_numeric($b)){
    exit();
}
if($b>1234){
    echo $flag2;
}
?>
```

CSDN @shallon6

打开之后我也看不是很懂,所以就去百度搜索每一句的意思,

第一行看起来像是php默认的首位都需要的类似于c语言的花括号

## 第二行百度说是高亮函数

### 例子

"test.php":

```
<html>
<body>
<?php
show_source("test.php");
?>
</body>
</html>
```

输出:

```
<html>
<body>
<?php
show_source("test.php");
?>
</body>
</html>
```

在浏览器中查看的结果类似这样:

CSDN @shallon6

第三行是一个php的include函数，感觉类似于c语言引入库函数的感觉



The screenshot shows a web browser interface. On the left, the source code is displayed with syntax highlighting. It includes a DOCTYPE declaration, HTML tags, and PHP code that uses the `include` function to load 'footer.php'. On the right, the rendered page content is shown, featuring a large heading, two paragraphs, and a copyright notice.

```
<!DOCTYPE html>
<html>
<body>

<h1>欢迎访问我的首页! </h1>
<p>这是一个段落。</p>
<p>这是另一个段落。</p>
<?php include 'footer.php';?>

</body>
</html>
```

# 欢迎访问我的首页!

这是一个段落。

这是另一个段落。

Copyright © 2006-2022 W3School.com.cn

CSDN @shallon6

第四行是个get函数的样子

## PHP \$\_GET 变量

在 PHP 中，预定义的 \$\_GET 变量用于收集来自 method="get" 的表单中的值。

### \$\_GET 变量

预定义的 \$\_GET 变量用于收集来自 method="get" 的表单中的值。

从带有 GET 方法的表单发送的信息，对任何人都是可见的（会显示在浏览器的地址栏），并且对发送信息的量也有限制。

### 实例

form.html 文件代码如下：

```
<html>
<head>
<meta charset="utf-8">
<title>菜鸟教程(runoob.com)</title>
</head>
<body>

<form action="welcome.php" method="get">
名字: <input type="text" name="fname">
年龄: <input type="text" name="age">
<input type="submit" value="提交">
</form>

</body>
</html>
```

当用户点击 "Submit" 按钮时，发送到服务器的 URL 如下所示：

```
http://www.runoob.com/welcome.php?fname=Runoob&age=3
```

CSDN @shallon6

后面很明显就类似于c语言的if判断分支了,根据所学过的c, c++猜测到是get一个a的值和b的值  
查资料后发现差不多 是这样那网页上怎么get呢? 地址后面直接加/?a=\*\*\* &b=\*\*\*传参即可综上所述, 我们  
尝试的给其页面传递数据

最后得到:

get a和b的值

如果a和0比较返回为true而且a为真

而且b不是纯数字

而且b要大于1234

满足这些条件则返回flag

根据分析, a可以=abcd (以0开头会认为是八进制数字)

因为b不能是纯数字而且要大于1234 (很明显提醒你了, 可以在数字后面加字母表示非纯数字)

则b可以=12345b

然后把a=abcd,b=12345b写进去即可

得到flag

### 8.get\_post

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?

使用get提交a=1在网址后面加上/? a=1

而后在使用插件hackbar插件 F12 postdata b=2

## 得到flag

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

cyberpeace{3c540695f681a0ffbda07659381e7254}

