

XCTF-WEB-view_source-解题思路

原创

RedTeam  于 2019-11-06 11:27:26 发布  222  收藏

文章标签: [CTF](#) [XCTF](#)

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_36304918/article/details/102931733

版权

题目介绍



The screenshot shows a CTF challenge interface for a challenge named 'view_source'. At the top, it has a title 'view_source' and a badge indicating it is the 'Best Writeup' by 'Healer_aptx' and 'Anchorite' with 15 likes. Below the title, the difficulty is '1.0' (indicated by a star icon). The source is 'Cyberpeace-n3k0'. The description states: '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。' (X teacher asks Little Ning to view the source code of a webpage, but Little Ning finds that the right mouse button doesn't seem to work). The challenge scenario is 'http://111.198.29.45:57858'. There is a progress bar and a '删除场景' (Delete Scenario) button. A timer shows '倒计时: 03:59:42' with a '延时' (Extend) button. At the bottom, it says '题目附件: 暂无' (No attachments).

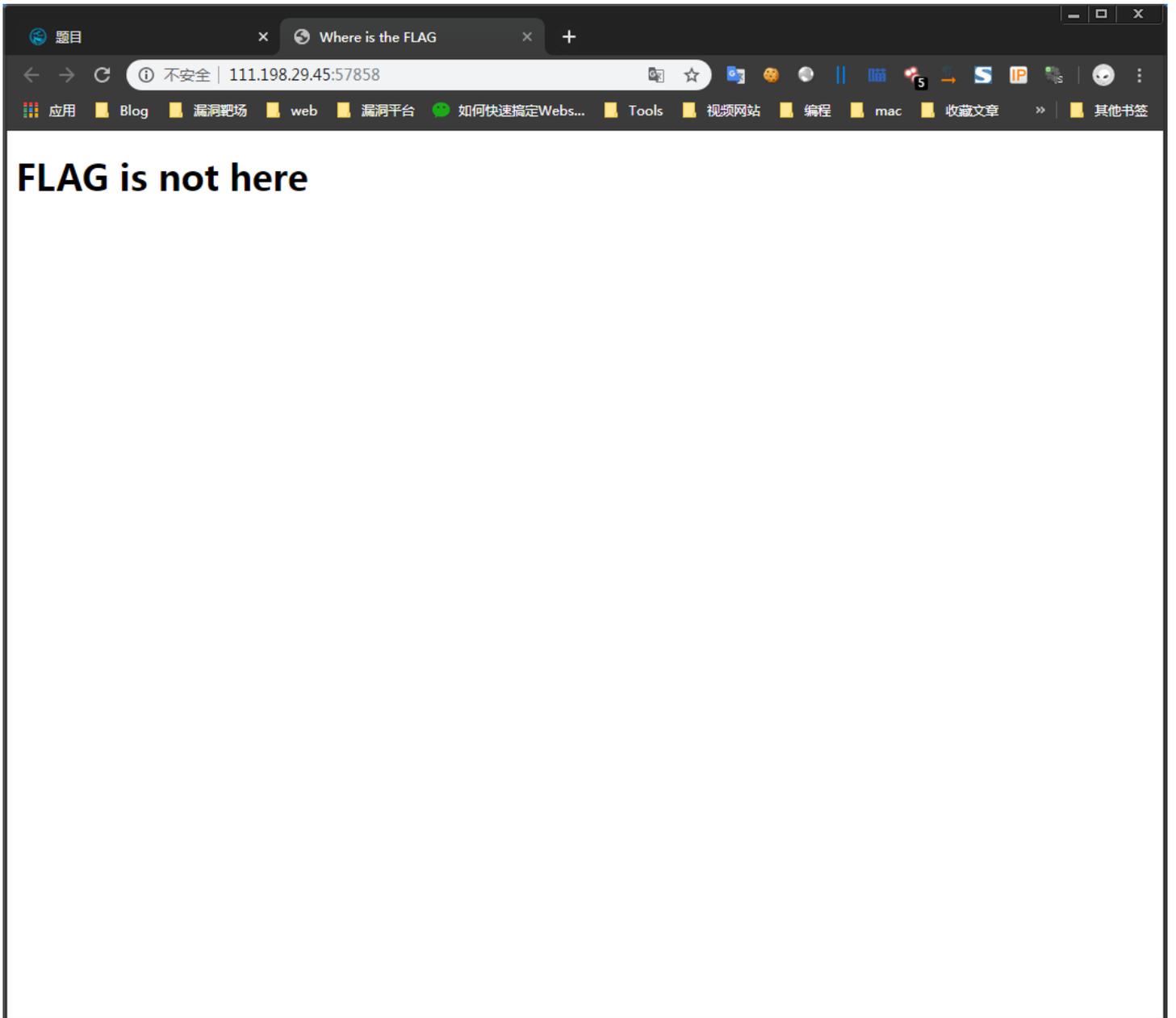
题目描述

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

解题过程

方法一

打开题目给到的是这样一个页面:

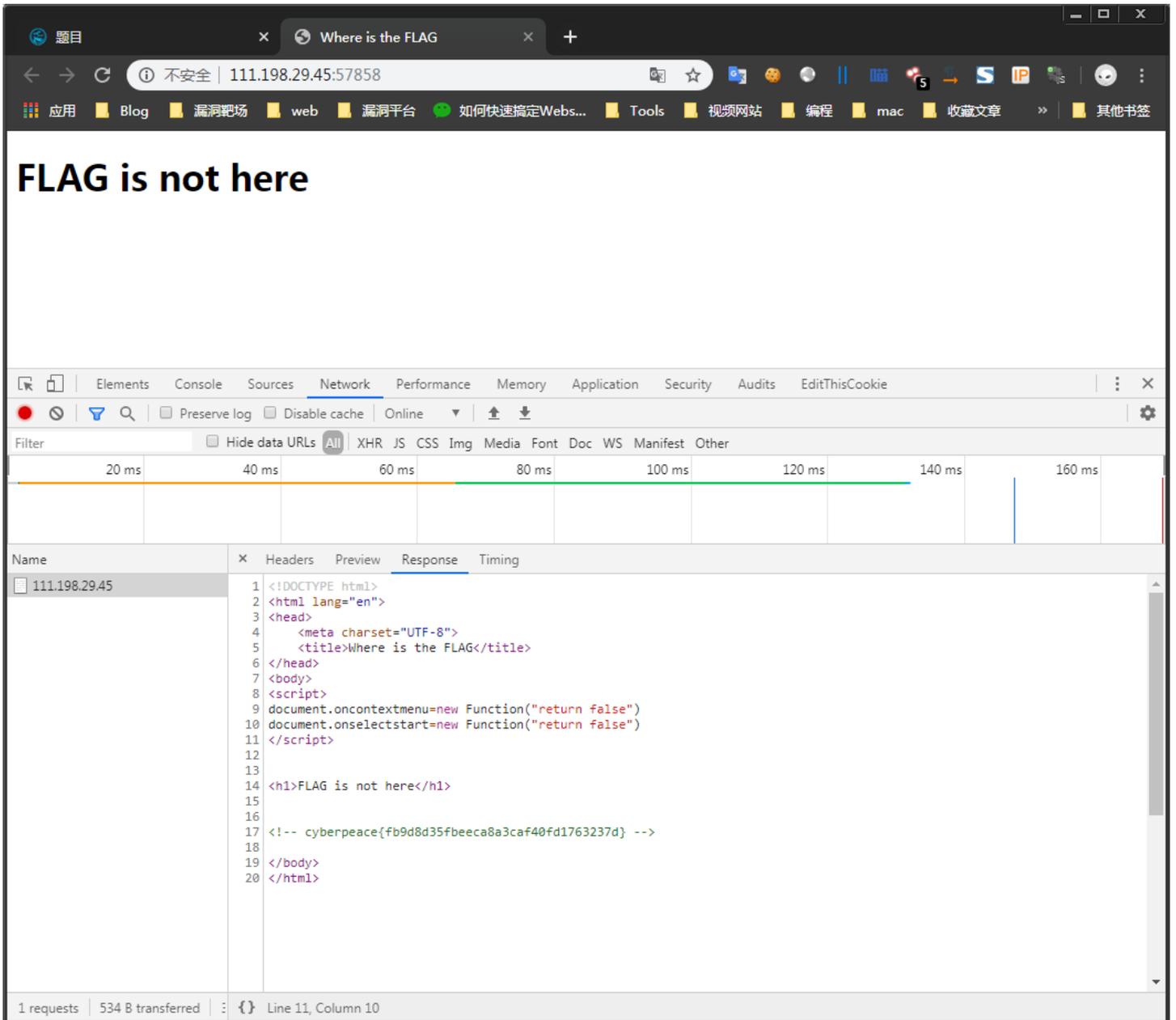


试着鼠标右键去点击页面，毫无反应！

但是在页面上输出一个：FLAG is not here：

然后想到了一个方法，它应该是使用了某些标签上的属性禁止我们点击鼠标右键和禁止选择！

那么就可以按下 F12 来打开开发者工具：



这个时候就可以看到网页的整个源码以及 **FLAG**：

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Where is the FLAG</title>
</head>
<body>
<script>
document.oncontextmenu=new Function("return false")
document.onselectstart=new Function("return false")
</script>

<h1>FLAG is not here</h1>

<!-- cyberpeace{fb9d8d35fbeecca8a3caf40fd1763237d} -->

</body>
</html>
```

果然是使用了一些属性:

```
禁止鼠标右键
document.oncontextmenu=new Function("return false")

禁止选择
document.onselectstart=new Function("return false")
```

方法二

如果在比赛中给到的浏览器不是火狐跟Google浏览器，那么只能通过 [BurpSuite](#) 来抓包查看源码:

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

4 x 5 x 6 x 7 x 8 x 9 x 10 x ...

Go Cancel < >

Target: http://111.198.29.45:57858

Request

Raw Headers Hex

```
GET / HTTP/1.1
Host: 111.198.29.45:57858
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
x-forwarded-for: 127.0.0.1
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Thu, 03 Oct 2019 02:26:43 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Vary: Accept-Encoding
Content-Length: 345
Connection: close
Content-Type: text/html

<!--DOCTYPE html-->
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Where is the FLAG</title>
</head>
<body>
<script>
document.oncontextmenu=new Function("return false")
document.onselectstart=new Function("return false")
</script>

<h1>FLAG is not here</h1>

<!-- cyberpeace{fb9d8d35fbeecca8a3caf40fd1763237d} -->
</body>
</html>
```

Done 557 bytes | 64 millis

这样就拿到了FLAG