xctf_web区题解(入门区1--6)

原创

Imc職 ● 于 2021-12-13 10:42:17 发布 ● 2482 ℃ 收藏 分类专栏: ctf web刷题记录 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/weixin_52185973/article/details/121900100 版权



ctf web刷题记录 专栏收录该内容

1篇文章0订阅 订阅专栏

xctf_web区题解(新手区1—6)

ps:说明一下,这次这个题解可能是比较是比较low的,因为前一段时间在玩学校的**vhdl**来实现eda的大作业,花了我一段比较长 的时间,另外之前一段时间再刷**密码学**的相关知识,也没这么去了解这个web这个方向的,对于小组内的blog我也就只能写写题 解了,以后可能做了一些项目会写一些其他有意思的东西

1.view_source

据题目描述,这道题的flag应该是在网页的源代码中的,但是鼠标右键点不了。那么这里有其他的解决方法,我在这里主要说两个解决方法:1.就是在网址上直接输入view-source:URL;2.就是按F12进入开发者模式,这里可以直接看见网页的源代码的(个人感觉这个很好用,接下来的题我好像都用到了这个开发者模式)

1.直接输入view-source:URL

如下图:

🗖 🛛 😂 题目	×	▶ view-source:111.200.241.244:653 ×
\leftarrow \rightarrow (▲ 不安全 view-	source:111.200.241.244:65352

换行 🗆

```
1
2 <html lang="en">
3 <head>
       \texttt{Kmeta charset="UTF-8"}
4
5
       <title>Where is the FLAG</title>
6 </head>
7 <body>
8 <script>
9 document.oncontextmenu=new Function("return false")
10 document.onselectstart=new Function("return false")
11 </script>
12
13
14 <h1>FLAG is not here</h1>
15
16
17 <!-- cyberpeace {22b0e1ed5dbc9de7bb4f8941ce8fc8c1} -->
18
19 </body>
20 </html>
```

2.直接在开发者模式查看

如下图:

										—	D	Х
		аљ	τœ	MK	v	ж	¢		౯ౖ≡	Ē		
	」 欢迎		元素	控制台	源代码	>>	+		9 1	ණ	°°	×
DU</td <td>CIYPE htm.</td> <td>1></td> <td></td>	CIYPE htm.	1>										
Knu	ni iang= e nead> <td>en ></td> <td></td>	en >										
• • <	ody> == 3	50										
•	<script></script>											

这个应该就是一个简单的签到题,就不过多细讲了。

2.robots

对于这个题目我简单的说一下**robots**,首先我简单的说一下什么是*Robots*协议,简单的来说robots协议就是一个存放在网站根目录下的ASCII编码的文本文件,所以也叫*robots.txt*,它的作用就是来告诉网络搜索引擎的漫游器(又叫网络蜘蛛),哪些地方是可以获取的,哪些地方是不能够获取的。

解题思路:本题很明显就是让你查看网站的robots.txt这个东西,所以查看就可以得到flag了,而对于查看网站的robots.txt, 其实很简单就是在*URL中输入robots.txt*就看以查看网站的robots.txt了。

如下图:



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

然后你会发现**"f1ag_1s_h3re.php"** 的字样在这个txt文档中,我们可以抱着试一试的态度将这个东西输入到URL中,然后就可以看见flag了

如图:

cyberpeace{e15b85bd4554677e4f0e0cb96be9df7d}

3. backup

据题目的描述就是要我们找出网页的备份,而且在题目给出的网站中你会发现是有关**index.php的备份文件名**,而对于网站的 备份文件的后缀大多都是**".git"、".svn"、" .swp"".~"、".bak"、".bash_history"、".bkf**放在URL的后面。

所以解题思路为:在URL后输入index.php.xx后缀名,然后就可以看到flag了

在URL中输入index.php.bak之后就可以看见下载了一个名为index.php.bak的文件,然后打开即可看见本题的flag

如下图

🧮 index.php.bak - 记事本 F 文件(F) 编辑(E) 格式(O) 视图(V) 帮助(H) **t**京 <html> <head> <meta charset="UTF-8"> <title>备份文件</title> k href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" /> 字 <style> body{ margin-left:auto; margin-right:auto; margin-TOP:200PX; width:20em; } </style> </head> <body> 鈋 <h3>你知道index.php的备份文件名吗? </h3> }3 <?php • ", \$flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}" ?> </body> . </html> 見 Ŧ (年1 万111 100% Windows (CPLE) LITE 9

4.cookie

很明显就是一个flag放在cookie中的问题,看到cookie就可以得到这个flag。

首先简单的聊一下什么是cookie。cookie是某些网站为了辨别用户身份,进行Session跟踪而储存在用户本地终端上的数据 (通常经过加密),由用户客户端计算机暂时或永久保存的信息,简单的来说就是储存在用户本地终端的数据,详细参 考cookie(储存在用户本地终端上的数据)_百度百科 (baidu.com))

那么对于这道题目而言的话,就是查看cookie,但是如何查看?很简单就是打开开发者模式就可以了,然后选中"网络"这个选项就可以了,然后就开始监听网页的一些活动了,刷新一下网页即可,然后点击下面的*cookie*就可以看见响应的cookie是啥了,这个很明显就是那个cookie.php这个东西,然后将其输入到URL中去。此时再观察开发者的那个界面,就会发现出现了一个 cookie.php的东西,然后在响应头就可以看见那个flag了

如图:

名称	× 标头 预览 响应 发起程序 计时								
🗋 cookie.php	 ▼ 响应头 查看源 								
bootstrap.min.css	Content-Encoding: gzip								
	Content-Length: 253								
	Content-Type: text/html								
	Date: Mon, 13 Dec 2021 01:32:53 GMT								
	<pre>flag: cyberpeace{e07c8edeef67c2efea98012d7b6beff0}</pre>								
	Server: Apache/2.4.7 (Ubuntu)								
	Vary: Accept-Encoding								
	X-Powered-By: PHP/5.5.9-1ubuntu4.26								
	▼ 请求标头 查看源								
	Upgrade-Insecure-Requests: 1								
	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl								
	eWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.55 Sa								
2 次请求 已传输0 B 1	fari/537.36 Edg/96.0.1054.43								

5.disabled_button

对于这题,应该就是改一下**html**的代码即可,将那个button的按键改为可以按下即可。那么如何改,同样还是打开开发者选项, 查看网站的源代码,你会发现在有个disable的单词,就英文意思而言也是"不能的意思",那么改一下捡起改为**able**,然后你就会 发现,那个button就可以使用了,点击一下,就可以发现那个flag就会自己跳出来,提交即可。

结果如图:

	□□ ☆迎 元素 控制台 源代码 ≫ 十 ■ 8 ☆ ピ ··· >				
$\Lambda \tau$ 45+244-44	<pre> <html> == 50</html></pre>				
一个个形式在时发出	html				
flag	样式 已计算 布局 事件侦听器 DOM 断点 雇性 辅助功能 AdGuard				
	筛选器 :hov .cls + €				
cyberpeace{1d58825172de60c11b5cbd7d02d12010}	element.style {				
	html { font-size: 62.5%; -uebkit-tap-highlight-color: ⊡rgba(θ,θ,θ,θ); }				
	<pre>html { font-family: sans-serif; webkit-text-size-adjust: 100%; "ms-text-size-adjust: 100%; }</pre>				
	<pre>*, *:before, *:after {</pre>				
	控制台问题十				
	▶ 🖉 top ▼ ● m选器 默认级别 ▼ ● 8 €				
	net::ERR_UNKNOWU_URL_SCHEME ▲ DevTools 无法加载源映射: 无法加载c <u>hrome-extension://gnnbmcifkkjgjdbkilfglp</u> <u>dpmidkgefn/scripts/content-script.js.map</u> 的內容:HTTP 错误: 状态代码 404, net::ERR_UNKNOWU RL_SCHEME				
	>				

6.weak_auth

嗯,对于这题呢。其实非常的nice。从这个网页不难看出,这个就是需要将这个网页成功登陆后就可以得到相关的flag了。然后 我就试了一两次,然后就登陆进去了(*好吧,这是个1星题,密码也不会太难,但是直接输入"123456"就让我进去了是不是太草 率了*)。

下面我说一下,常规的破解方法,没错就是**爆破**(反正我是目前想不出来有啥好的方法)。对于这个的爆破有一个好的工具, 那就是**burp suite**,我也是前几天才接触到这个东西的,用的还不是很习惯。首先好像要和浏览器搞一个代理,(推荐用Firefox 似乎好搞一些,Microsoft edge好像不太好搞)至于如何建立我推荐一篇文章读者可以自己去阅读解决,本文就过多赘述了.

链接: BurpSuite-代理和浏览器设置

在配置完之后,打开burp suite,然后在proxy将intercept打开,然后再题目的容器中输入相关的信息,然后你就会发现在burp suite中会收到数据包。在点击intruder,进入爆破界面。首先输入攻击的ip,以及相应的port;然后再positions中将一开始发过来 的数据包copy过来,通过add, clear操作选择爆破的对象。这里我们选择password,然后payload中添加字典,然后开始可以 爆破了。爆破之后,然后点击123456的那条密码,然后就可以看见response中有一个flag。ok,破解成功。(*因为事先就知道 了密码,所以就是验证一下,至于burp suite这个软件,个人还是不怎么怎么会用*)

附爆破图:

Results	Target Position	s Payloa	ds Resource	Pool Op	tions			
Filter: Show	ing all items							?
Request \land	Payload		Status Error	Timeout	Length	Comment		
0	Sesult 1 Intruder	attack					>	<
	Payload: 123456 Status: 200 Length: 437 Timer: 32						Previous Next	
	Request Respo	nse						
	Pretty Raw Hex	Render 🚍	\n ≡					
Request	<pre>11 (nemi lang en 12 <head> 13 <meta 14="" <title="" char=""/> weak aut 15 </head></pre>	set="UTF-8" h	*>					
Pretty Ra 1 HTTP/1. 2 Date: 5	16 body> 17 18 cyberpeace	{f45181e04}	d37c16d843b75	507a9509c}	maybe you</td <td>need a dictiona</td> <td>ry></td> <td></td>	need a dictiona	ry>	
3 Server: 4 X-Power 5 Vary: A 6 Content	19 20 21 22							
7 Connect 8 Content 9	?\$\$\$ ← → Sea	arch					0 match	es
10 DOCTY<br 11 <html 1<br="">12 <head< td=""><td>TPE html> Lang="en"> i></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></head<></html>	TPE html> Lang="en"> i>							
13 <me< td=""><td>ta charset="UTF-8</td><td>"></td><td></td><td></td><td></td><td></td><td></td><td></td></me<>	ta charset="UTF-8	">						
am								