CTF | CTF-Web 捉迷藏



<u>大青呐</u> 于 2019-07-10 13:52:41 发布 ◎ 867 ※ 收藏 2 分类专栏: <u>CTF-Web实验</u> <u>CTF-Web实验</u> 文章标签: <u>CTF-Web</u> 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/qq_42646885/article/details/95321970</u> 版权



 CTF-Web实验
 同时被2个专栏收录

 9 篇文章 0 订阅
 10 订阅



CTF-Web实验

4篇文章0订阅 订阅专栏 打开网址,看到如下页面。



先查看源代码,发现页面还有一个表格和一个链接。

 Cbody style= "margin:auto;padding=top:50pz;background:black;color:#0F0;">	
<pre>(div align="center")</pre>	
<pre class="logo" style="font=size:bpr;"></pre>	
Can you see the hidden flag?	
$\langle t_2 \rangle \langle t_4 \rangle \langle t_$	
$(\tau_1 \land \tau_1 \land \tau_2) = 0 \land (\tau_1 \land \tau_2 \land \tau_2) \land (\tau_1 \land \tau_2) \land $	
$(t_1)(t_1)(t_2)(t_2)(t_1)(t_1)(t_2)(t_2)(t_2)(t_2)(t_2)(t_2)(t_2)(t_2$	
<pre>(tr><td< th=""></td<></pre>	
<td class<="" th=""></td>	
ctr> <td c<="" th=""></td>	
$\langle tr \rangle \langle td \ class="b" \rangle \langle td \rangle \langle td$	
$\langle tr \rangle \langle td class= w \rangle \langle td \rangle \langle td class= w \rangle \langle td \rangle \langle td class= b \rangle \langle td \rangle \langle td class= b \rangle \langle td \rangle \langle td class= w \rangle \langle td \rangle \langle td class= w \rangle \langle td \rangle \langle td class= b \rangle \langle td \rangle \langle td \rangle \langle td class= b \rangle \langle td \rangle \langle td \rangle \langle td class= b \rangle \langle td \rangle \langle td \rangle \langle td \rangle \langle td class= b \rangle \langle td \rangle \langle td \rangle \langle td class= b \rangle \langle td $	
$\langle t_T \rangle \langle t_d \rangle \langle t_$	
(r) ($r)$	
$\frac{1}{1} \frac{1}{1} \frac{1}$	
(tr)(td_class="b")(td)(td)(td)(td)(td)(td)(td)(td)(td)(td	
<pre>class="b">class="w"><td <="" class="w" th=""></td></pre>	
ctr> <td b"<="" class="b</th></tr><tr><th><td class</th></tr><tr><th><td class=" th=""></td>	
ctr> <td_class="b"><td_class="w"><td_class="w"><td_class="w"><td_class="w"><td_class="w"><td_class="w"><td_class="w"><td_class="w"><td_class="w"><td_class="w"><</td_class="w"></td_class="w"></td_class="w"></td_class="w"></td_class="w"></td_class="w"></td_class="w"></td_class="w"></td_class="w"></td_class="w"></td_class="b">	
<pre>(tr><td< th=""></td<></pre>	
(/tbody)	
APAR HERE HORE DU ALANT COLOR DIRCK ANDRALARAADA	
<pre></pre> (/body)	

在样式将背景颜色改为红色后看到页面如下:



点击index链接,发现页面闪现出了绿色的字符,随机一闪而逝,好像看到了flag信息。尝试用burpsuite抓包,看下Index.php页面的信息。

burpsuite端口已默认设置好。

Burp Intruder Repeater Window Help												
Targe	t Proxy	Spide	r Scanne	r Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts	
Intercept History Option												
Proxy Listeners												
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.												
	Add	R	unning	Interface	Inv	isible Re	edirect		Certificate			
	Edit		V	127.0.0.1:8080	30				Per-host			-
	Remove	•									•	
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.												
CA certificate https://blog.csdn.net/qq_42646885												

配置访问国际互联网的 (C)不使用代理(X)	代理							
日初短期に内容的代理で直通し								
() 使用承载代理设置 (1)								
· 于动配置代理: (U)								
HTTP 代理: (Z)	127.0 0.1	端口:① 8080 🕂						
	□ 为所有协议使用相同代理(2)							
SSL 代理:		端口: (0) 0 🚔						
<u>F</u> TP 代理:		端口:(B) 0 🕂						
SO <u>C</u> KS 主机:		端口: ① 0 🛨						
	C SOCKS v4 G SOCKS v5 [注程 DNS							
不使用代理: (1)								
localhost, 127.0.0.1								
例如:.mozills.org, .net.nz, 192.188.1.0/24 〇 自动代理配置(PAC):								
重新載入(2)								
厂 如果密码已保存,不提示身份验证 (I)								
	商定	TO SHE APPH OD						

点击确定后,打开burpsuite,在Proxy-Intercept-点击Intercept on。

在浏览器访问10.1.1.219:20111/Index.php,再查看History,打开详细看到flag的信息。



除此之外,开始的时候检查中间table有什么东西,找到控制table颜色的样改为白色:



看到table变成了一个二维码。



用微信扫描二维码后出现Key。

ăii "inii 🖘 🛎 🔒 🛬	🕸 🛈 84% 📧 12:09					
×						
flag{htm!_qrc0d3}						

不过这个flag是个幌子。。。

实验总结:该实验比较简单,主要是要会使用burpsuite抓包。

burpsuit使用参考:工具 | Burpsuite简介及使用