攻防世界 WEB 新手练习区 writeup 001-006



 ChaoYue_miku
 ● ± 2021-09-01 23:40:58 发布
 ● 102 ℃ 收藏

 分类专栏:
 # 攻防世界 CTF # Web 文章标签:
 html BurpSuite

 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/ChaoYue_miku/article/details/120051290

 版权



6篇文章0订阅



127 篇文章 5 订阅 订阅专栏



4 篇文章 0 订阅 订阅专栏

攻防世界 WEB 新手练习区 题目解答

浏览器: Firefox(火狐浏览器)

文章目录

- 001 view source
- 002 robots
- 003 backup
- 004 cookie
- 005 disabled_button
- 006 weak_auth

001 view source



难度系数: 1.0

题目来源: Cyberpeace-n3k0

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。

0x01打开网页

$\leftarrow \rightarrow$	C D	0 1	11.200.241.244:54345					☆		ی ع	4	0	IP	0	≡
🗋 收藏夹	□ 密码工具	CSDN - 专业开发者社	⊕ CSDN - 专业开发者社	⊕ 签到 - 鱼C论坛 - Pow	😪 个人中心	闷 BugkuCTF - 练习平台	🚼 吾爱破解 -	LCG - LSG	🚳 w3cschool -	编程狮…			» (_ 其他∹	书签

FLAG is not here

CSDN @ChaoYue_miku

网页中显示FLAG is not here

0x02 按F12键打开开发者工具

🔊 編藏文章 - Halo Dashboard 🗙 🛞 题目 🛛 🗙 🗙	Where is the FLAG \times	http://111.200.241.244:54345/ ×	D 京东(JD.COM)-正品低价、品》	× 🤨 新标签页	× +	-	ð	×
← → C 🙆 ○ 🏖 111.200.241.244:54	4345			☆	🗲 🖂 🌾	IP	0	=
🗋 收藏夹 🗋 密码工具 🢽 CSDN - 专业开发者社 💮 CSDN - 专业开发	者社 💮 PTA 程序设计类实验	💮 签到 - 鱼C论坛 - Pow (个人中心	闷 BugkuCTF - 练习平台 🛗 吾爱	破解 - LCG - LSG (🔯 w3cschool - 编程狮	»	口其	也书签

FLAG is not here



或者使用快捷键Ctrl+U打开源代码

```
1 <! DOCTYPE html>
2 <html lang="en">
3 <head>
      <meta charset="UTF-8">
4
      <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>
14 <h1>FLAG is not here</h1>
17 <!-- cyberpeace{4dda626c173a3bea3af8cd8512f79211} -->
19 </body>
                                          CSDN @ChaoYue_miku
20 </html>
```

0x03 得到flag: cyberpeace{4dda626c173a3bea3af8cd8512f79211}

002 robots



难度系数: 1.0

题目来源: Cyberpeace-n3k0

题目描述: 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。

0x01 打开网页,根据题目提示,查看robots.txt文件



0x02 继续打开f1ag_1s_h3re.php文件



0x03 得到flag: cyberpeace{4a64d1a8d56ab95f9bbacd50d6877395}

003 backup



难度系数: 1.0

题目来源: Cyberpeace-n3k0

题目描述: 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!

0x01打开网页

 く
 〇
 込
 111.200.241.244:63032
 □

 □ 收藏夹
 □ 密码工具
 C CSDN - 专业开发者社... ④ CSDN - 专业开发者社... ④ PTA | 程序设计类实验... ④ 签到 - 鱼C论坛 - Pow... ⑤ 个人中心 Ø BugkuCTF - 练习平台 醫 音報

网页中显示:你知道index.php的备份文件名吗? 通常备份文件的后缀名为.bak 所以index.php的备份文件名为index.php.bak

0x02 打开index.php.bak文件



0x03 得到flag: cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

004 cookie



难度系数: 1.0

题目来源: Cyberpeace-n3k0

题目描述: 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?'

0x01打开网页



你知道什么是cookie吗?

CSDN @ChaoYue_miku

网页中显示:你知道什么是cookie吗?

0x02 按F12进入开发者工具,在"网络"中查看

▼ 请	求头 (487 字节)	原始 ●
?	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0).8
?	Accept-Encoding: gzip, deflate	
?	Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2	
?	Cache-Control: max-age=0	
?	Connection: keep-alive	
?	Cookie: look-here=cookie.php	
?	Host: 111.200.241.244:53710	
?	Upgrade-Insecure-Requests: 1	
?	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0	CEDN @ChaoYua miku
?	X-Forwarded-For: 123.51.163.163	

▼ 响	应头 (307 字节)	原始 ● ^
?	Connection: Keep-Alive	
?	Content-Encoding: gzip	
?	Content-Length: 276	
?	Content-Type: text/html	
?	Date: Mon, 30 Aug 2021 05:21:50 GMT	
?	Keep-Alive: timeout=5, max=100	
?	Server: Apache/2.4.7 (Ubuntu)	
?	Set-Cookie: look-here=cookie.php	
?	Vary: Accept-Encoding	SDN @ChaoYue miku
	X-Powered-Rv: DHD/5.5.9-1ubuntu4.26	

请求头和响应头均有cookie

0x03 打开http://111.200.241.244:53710/cookie.php

	♥	<u>ី</u>
□ 收藏夹 □ 密码工具 C CSDN - 专	业开发者社 💮 CSDN - 专业开发者社 💮 PTA 程序设计类实验 💮 签到 - 鱼C论坛 - Pow 🔡 吾爱破解 - LCG - LSG 😂	个人中心

See the http response

CSDN @ChaoYue_miku

网页中显示: See the http response

直接查看响应头,发现flag

_										
⊡ €	○ 查看器	控制台	调试器 ↑↓ 网络 {}	样式編編器 📿 性能	① 内存 目存	储 🕇 🦻	无障碍环境 🛛 闘 应	用程序	HackBar Max HacKBar 9 9 1 ···· 1	×
⑪									🔍 🛇 所有 HTML CSS JS XHR 字体 图像 媒体 WS 其他 📕 萘用缓存 不节流 🗧 🕇	¥
状态	方法	域名	文件		发起者	类型	传输		同 消息头 Cookie 请求 响应 耗时 浅跟踪	
200	GET	🔏 111.200.241	cookie.php		BrowserTabChil	html	578 字节		♀ 过速消息头 拦截 重数	2≎
404									▼ 响应头 (325 字节)	
									O Connection: Keep-Alive Content-Encoding: gzip Content-Length: 253 O Content-Type: text/html Date: Mon, 30 Aug 2021 05:25:35 GMT flag: cyberpeace(cf1040003192113ce1279c221c6316ea) Keep-Alive: timeout=5, max=100 Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding	
Ō	2 个请求	已传输 703 字节 / 57	78 字节 完成: 538 毫秒	DOMContentLoaded: 3	41 窒秒 🛛 load: 35	58 室秒			X-Powered-By: PHP/5.5.9-1ubuntu4.26 CSDN @ChaoYue_mikt	ļ,

0x04 得到flag: cyberpeace{c1f040003192113ce1279c221c63f6ea}

005 disabled_button



难度系数: 1.0

题目来源: Cyberpeace-n3k0

题目描述: 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?

0x01打开网页



一个不能按的按钮

flag

CSDN @ChaoYue_miku

页面中显示: 一个不能按的按钮

下方是一个Button按钮,内容为flag,显示为灰色且不能按下。

0x02 按F12进入开发者工具,修改页面源代码



Q 捜索 HTML	+ 🎢
<html> [event]</html>	
<pre><script id="allow-copy_script"></script></pre>	

删除disabled属性后flag按钮就可以按下

← → C @	0 111.200.241.244:53877			一 公	
□ 收藏夹 □ 密码工具 С С	SDN - 专业开发者社 💮 CSDN - 专业开发者社	. 💮 PTA 程序设计类实验 💮 签到 - 鱼C论坛 - Pc	w 🧱 吾爱破解 - LCG - LSG 🧯	👌 个人中心 🌾 BugkuCT	F - 练习平台

一个不能按的按钮

flag

cyberpeace{1137d28f4f0cc032202bcdb6e3c185b8}

0x03 得到flag: cyberpeace{1137d28f4f0cc032202bcdb6e3c185b8}

006 weak_auth



难度系数: 1.0 题目来源: Cyberpeace-n3k0 题目描述: 小宁写了一个登陆验证页面,随手就设了一个密码。

0x01 打开网页,页面中出现一个登录界面

	O 111.200.241.244:61608	二 公
□ 收藏夹 □ 密码工具 C CSDN - ⁴	专业开发者社	人中心 闷 Bugku

Login	
username	
	1
password	
login	
login	
reset	CSDN @ChaoYue_miku
	CDDN @Chabhae_hika

根据题目以及题目描述,估计密码是一个弱口令,可以进行爆破

0x02 输入任意用户名和密码,查看回显

⊕ 111.200.241.244:58706	
please login as admin	
	确定

提示我们要用admin账户登录

0x03 用户名输入admin 密码随意输入(这里输入123456)

← → C @	🗟 🔿 111.200.241.244:58706/check.php										
🗋 收藏夹 📄 密码工具 🦲 CSDN - 专业开发者社 💮 CSDN - 专业开发者社 💮 PTA 程序设计类实验 💮 签到 - 鱼C论坛 - Pow 🔡 吾爱破解 - LCG - LSG 🛞 个人											
cyberpeace {f7901dfd2bdff62eb2dd7cd62d2120d9}											

直接登录成功,的确是最为常见的一个弱口令,其实这里也是有些巧合,接下来介绍密码输入错误的情况

0x04 用户名输入admin 密码随意输入(这里输入123)



提示密码错误,说明用户名输入正确

0x05 使用BurpSuite进行抓包,准备爆破

<mark>5</mark> Burp Pr	Burp Project Intruder Repeater Window Help Burp Suite Professional v2021.8.2 - Temporary Project - licensed to Uncia																
Dashboard	Target Proxy	Intruder	Repeater	Sequencer	Decoder	Compar		gger E	xtender	Project op	otions	User options	Learn				
Intercept	HTTP history We	oSockets hist	ory Options														
Filter: Hiding CSS, image and general binary content														?			
# 2 http://		Method 6 POST	/check.php							MIME typa HTML							
Request																	
Pretty Raw																	
5 Accept-Lar 6 Accept-Enc 7 Referer: H 8 Content-Ty 9 Content-Le 10 Origin: ht 11 Connection 2 Upgrade-Ir 13 X-Forwarde 14 Pragma: nc 15 Cache-Cont 16 17 username=2	nguage: zh-CN,zh;q= coding: gzip, defla http://11.200.241.2 ype: application/x-n ength: 27 ttp://11.200.241.2 h: close secure-Requests: 1 secure-Requests: 1 sd-For: 123.51.163. cache trol: no-cache admin&password=132).8,zh-TW;q ⁻ :e :44:58706/ ww-form-ur 14:58706 63	=0. 7, zh-HK;q=0 lencoded	. 5, en−US;q=C). 3, en;q=0.												SPECTOR
-→\$?	→ Search														SDN @Ohae¥	uheളmil	

抓包后发送给Intruder模块

0x06 使用Intruder模块进行爆破

我们可以寻找弱口令字典进行爆破,密码正确时的响应长度与密码错误时不同,以此找出正确的密码

🛐 Burp Project Intruder Repeater Window Help 🛛 Burp Suite Professional v2021.8.2 - Temporary Project - licensed to Uncia												
Dashboard Target Proxy Intruder Repea	ater Sequencer Deco	der Comparer	Logger	Extender	Project options	User options	Learn					
Target Positions Payloads Resource Pool Options												
Payload Positions												
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.												
Attack type: Sniper												
1 POST /check.php HTTP/1.1								Add §				
2 Host: 111.200.241.244:58706 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0												
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2												
6 Accept-Encoding: gzip, deflate												
8 Content-Type: application/x-www-form-urle	encoded											
9 Content-Length: 27												
11 Connection: close												
12 Upgrade-Insecure-Requests: 1 13 X-Forwarded-For: 123 51 163 163												
14 Pragma: no-cache												
15 Cache-Control : no-cache 16												
17 username=admin&password= <mark>§132§</mark>												
$(?)\{\mathfrak{G}\} \leftarrow \rightarrow Search$												
1 payload position							Length: 655 CSDN	@ChaoYue_miku				

Burp Project Intruder Repeater Window Help Burp Suite Professional v2021.8.2 - Temporary Project - licensed to Uncia													
Dashboard Targe	t Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extender	Project options	User options	Learn		
	Payloads		Pool Opt										
Payload Sets												Start	attack
You can define or type can be custo	ne or more pa omized in diffe	yload sets. T erent ways.	he number of	payload sets d	epends on th	e attack type d	efined in the	Positions tab	o. Various payload ty	/pes are available	for each payload se	t, and each p	
Payload set: 1			Payload o	ount: 1,000,00									
Payload type: Numbers V Request count: 1,000,000													
Payload Option	ns [Number:	s]											
This payload type	e generates nu		ads within a g	iven range and	l in a specifie	d format.							
Number range													
	💿 Seque												
How many:													
Number format													
	💿 Decim												
Min integer digit													
Max integer digit													
Min fraction digit													
Max fraction digi													
Examples 1.1											C	SDN @Chao'	Yue_miku

3	Attack	k Save Columns 4. Intruder attack of 111.200.241.244 - Temporary attack - Not saved to project file — 🗆 🗙											
Re	sults	Target	Positions	Payloads	Reso	ource Pool	Options						
Filte	er: Showi	ing all iter											?
Re	quest		Payload		Status	Error	Timeout	Length ~		omment			
7		123456		20	0			437					
0				2(0			434					
2		123451		20	0			434					
3		123452		20	0			434					
4		123453		20	0			434					
5		123454		20	0			434					
6		123455		20	0			434					
8		123457		20	0			434					
10		123459		20	0			434					
11		123460		20	0			434					
14		123463		20	0			434					
16		123465		20	0			434					
18		123467		20	0			434					
20		123469		2(0			434					
Re	quest	Respon	ise										
Pre	tty Rav	w Hex											
1 P	0ST /ch	eck. php	HTTP/1.1										
2 H	ost: 11	1.200.24	1.244:58706										
3 U	ser-Age	nt: Mozi	lla/5.0 (Windo	ows NT 10.	0; Winć	04; x64; rv	:92.0) Ge	cko/20100101	1 Firefox/92	2.0			
4 A	ccept:	text/htm	1, application/	xhtml+xm	l, applic	ation/xml;	q=0.9, ima	ge/avit, imag	ge/webp,*/*;	q=0.8			
A C	ccept-L	anguage:	zn-UN, zn;q-U.	8, zn-1W;0	1=0. 7, zn	I−HK;q=0. ⊃,	en-05;q=0	. 3, en;q=0. 2					
	eferer.	http://	'111 200 241 24	; 14·58706/									
8 0	ontent-	Tvpe: ap	plication/x-ww	w-form-u	lencode	d							
9 C	ontent-	Length:	30										
10 0	rigin:	http://1	11. 200. 241. 244	1:58706									
11 C	onnecti	on: clos											
12 U	pgrade-	Insecure	-Requests: 1										
13 X	-Forwar	ded-For:	123. 51. 163. 16	53									
(?)		→ Sea	orch									0 mato	hes
109	of 151										CSDN @Chao	oYue_m	niku



0x07 得到flag: cyberpeace{f7901dfd2bdff62eb2dd7cd62d2120d9}