攻防世界web解题

原创

 sevenlob

 于 2020-01-25 16:03:49 发布

 2268 % 收藏 2
 文章 收藏 2
 分类专栏: <u>笔记</u>文章标签: <u>web 信息安全 php html</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/sevenlob/article/details/104083301</u>
 版权



笔记 专栏收录该内容

15 篇文章 1 订阅 订阅专栏

robots

robots协议(robots.txt)

Robots协议用来告知搜索引擎哪些页面能被抓取,哪些页面不能被抓取;可以屏蔽一些网站中比较大的文件,如:图片,音 乐,视频等,节省服务器带宽;可以屏蔽站点的一些死链接。方便搜索引擎抓取网站内容;设置网站地图连接,方便引导蜘蛛爬 取页面。(来自百度百科)

** 置于网页上的robots.txt,指定了搜索引擎和网络爬虫可以可以访问和禁止访问的页面 **

题目分析

进入答题页面后,在网址上直接进入robots.txt



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

就可以查看答案



cyberpeace{f82d773922e5d5b2267cff15bb83183a}

backup

你知道index.php的备份文 件名吗?

index.php的备份文件是index.php.bax,直接访问下载,再打开查看文件,就可以找到flag

1	P <html></html>
2	⊨ <head></head>
3	<meta charset="utf-8"/>
4	<title>备份文件</title>
5	<pre><link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet"/></pre>
6	e <style></th></tr><tr><th>7</th><th>body {</th></tr><tr><td>8</td><td>margin-left:auto;</td></tr><tr><td>9</td><td>margin-right: auto;</td></tr><tr><td>10</td><td>margin-TOP:200PX;</td></tr><tr><td>11</td><td>width:20em;</td></tr><tr><td>12</td><td>}</td></tr><tr><td>13</td><td>- </style>
14	-
15	⊨ <body></body>
16	<h3>你知道index.php的备份文件名吗? </h3>
17	⊨ php</td
18	\$flag= "Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"
19	-?>
20	-
21	L
22	
1	
Hyper 1	Text Markup La length : 500 lines : 22 Ln : 22 Col : 1 Sel : 0 0 Windows (CR LF) UTF-8 UTF-8

cookic(储存在用户本地终端上的数据)

cookic,类型为"小型文本文件",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(源自百度百科)

客户机保存的用于服务器识别的一小段文本信息

题目分析



进入cookie.php查看cookie

🔏 111.198.29.45:44266/cookie.php

See the http response

https://blog.csdn.net/sevenlob

提示"查看网页响应",刷新一下网页就可以在网站消息头当中找到flag

R	○ 査者器	▶ 控制台 □ 调试器	▶ 网络 {}样式编辑器 ⑦ 性能 ⑧ 内存	🗄 存储 肯 无障碍环境	🔒 Max Had	KBar			0 … ×
Û	▼ 过滤 UF	IL.				11 Q O	所有 HT	ML CSS JS XHR 字体图像像媒体WS 其他 目持续日志 目 禁用缓存	不节流 \$ HAR \$
状态	方法	域名	文件	触发源头	类型	传输	大小	I 消息头 Cookie 参数 响应 耗时 堆栈跟踪	
200	GET	💋 111.198.29.45:44266	5 cookie.php	document	html	578 字节	411 字节	版本: HTTP/1.1	编辑和重发 ^
200	GET	🔏 libs.baidu.com	bootstrap.min.css	stylesheet	CSS	16.89 KB	97.22 KB	▼ 过滤消息头	
404	GET	🔏 111.198.29.45:44266	5 favicon.ico	img	html	已缓存	290 字节	▼ 响应头 (325 字节)	原始头
								○ Connection: Keep-Alive ○ Content-Encoding: gzip ○ Content-Length: 253 ○ Content-Type: text/html ○ Date: Sat, 25 Jan 2020 07:34:16 GMT flag: cyberpeace(d1b6a994d346/f7047409/22ae784b40) ○ Server: Apache/2.4.7 (Ubuntu) ○ Vary: Accept-Encoding ×-Powered-By: PHP/5.59-1ubuntu4.26	TEMAN,
								▼ 南水大 (421 子口) ③ Accent: tout (html application (whtml ym, mlra=0.0 image/webp t //ra=0.0	Inter C
Ō	3 个请求	已传输 97.91 KB / 17.45 KB	完成: 345 室秒 DOMContentLoaded: 123 室秒	load: 357 室砂				Accept-Encoding: gzip, deflate https://blog.ci	sdn.net/sevenloo

暂时还不知道怎么在Google中查看

disable button

题目分析

一个不能按的按钮

flag

F12发现,form有一个disable属性,直接删除就可以点了,点出来就有答案



HTML表单的disabled属性

HTML中的input元素、button元素、option元素等可附加disabled属性。 当赋予该属性时该元素将变得不可交互 创建一个可以按的按键



浏览器显示如下,这个按键是可以点击的



falg

html
<html></html>
<body></body>
<h1>disable<h1></h1></h1>
<form action=""></form>
<input disabled="" type="button" value="falg"/>

浏览器显示如下,这个按键是不可以点击的



falg

weak auth

题目如下,是一个无需登陆验证和不限登录次数的登陆界面,这种就可以使用暴力破解获得这个弱密码:

Login	
username	
password	
	login
	reset

https://blog.csdn.net/sevenlob

随便输入一个用户名,提示用户名为admin,就使用admin作为用户名进行爆破。 我在虚拟机上使用Buipsuit进行爆破

1. 先在浏览器中设置代理



Auto-detect proxy settings for this net <u>w</u> ork		
Jse system proxy settings		
danual proxy configuration		
HTTP Proxy 127.0.0.1	Port	8080
\checkmark Use this proxy server for all protocols		
SS <u>L</u> Proxy 127.0.0.1	P <u>o</u> rt	8080
FTD Drovy 127 0 0 1	Dort	2020
Help	Cancel	OK

2. 之后再浏览器中输入username为admin, password随便输入一个数(刚好输入的是123456,直接出答案了。。。但为了 爆破一次,换成了111111), Burpsuit就会拦截,就可以开始具体的爆破步骤

3. Action —> Sent to Intruder

	burp suite community Euronvz	1.07 - Temporary	Project		~
Burp Project Intruder Repeater Window Help		~			
Dashboard Target Proxy Intruder Repeater Seq	uencer Decoder Comparer Exte	nder Project option	ns User options		
Intercept HTTP history WebSockets history Options]				
Request to http://111.198.29.45:51410					
Forward Drop Intercept is on	Action	20		Comment this item	🤍 🦇 💽
Raw Params Headers Hex	Scan [Pro version only]				
POST /check.php HTTP/1.1	Send to Intruder	Ctrl+l			
Host: 111.198.29.45:51410	Send to Repeater	Ctrl+R			- n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0)	Send to Sequencer				
Accept: text/ntml,application/xntml+xml,applicatio	Send to Comparer				
Accept-Encoding: gzip, deflate	Send to Decoder				
Referer: http://111.198.29.45:51410/	Request in browser	•			
Content-length: 30	Engagement tools [Pro version only]	•			
Connection: close	Change request method				
Upgrade-Insecure-Requests: 1	Change body encoding				
username-admin£passuord-111111	Copy URL				
user hunce-uum intepussion u-iiiiii	Copy as curl command				
	Copy to file				
	Paste from file				
	Save item				
	Don't intercept requests	•			
	Do intercept	•			
	Convert selection	•			
	URL-encode as you type				
	Cut	Ctrl+X			
	Сору	Ctrl+C			
	Paste	Ctrl+V			
	Message editor documentation				
	Proxy interception documentation				
		10			

4. Intruder —> Positions, 清理变量后选定password为变量

Burp Project Intruder Repeater Window Help	
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options	
Target Positions Payloads Options	
(?) Payload Positions	t attack
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.	
åttark tune: Sniner 4	

DAGT /shark she UTD/1 1		
Host 11 108 20 45-51410	Add	5
nost. 111.190.29.49.91410 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 Accent: text/html.application/xhtml+xml.application/xml:a=0.9.*/*:a=0.8	Clear	-§
Accept-Language: zh,en-US;g=0.7,en;g=0.3	2	
Accept-Encoding: gzip, deflate	Z Auto	§
Referer: http://111.198.29.45:51410/		_
Content-Type: application/x-www-form-urlencoded	Refre	sh
Content-Length: 30		-
Connection: close		
Upgrade-Insecure-Requests: 1		
username=admin&password=§111111§		
	https://blog.esdn.net/sev	

5. 选定爆破模式为Cluster bomb

_
sevenlop
-//

6. Payloads中的Payloads set和Payloads type选为默认,此外还可以使用自己的字典

			Burp Suite (communit	y Edition v2	2.1.07 - Tei	mporary Proje	ct		
irp Project Intru	uder Repeater Window	Help								
ashboard Tar	rget Proxy Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project option	us User optio	ns	
. × 4 ×										
arget Position	ns Payloads Options	,								
) Payload S	ets									Start attack
You can defir	ne one or more payload s	ets. The num	nber of payloa	d sets depe	ends on the at	ttack type de	fined in the Pos	tions tab. Vario	us payload type:	sare
available for	each payload set, and ea	ich payload ty	ype can be cu	stomized in	different way	's.				
Payload set:	[1	Pag	yload count: (5						
Pavload type	· Simple list	Rei Rei	quest countr (n						
i dylodd lype			queer count.							
		on pie noce	r strings that	are used as	s payloads.					
Paste Load Remove Clear	可自3	主选择	字典	▶	s payloads.					
Paste Load Remove Clear Add	可自 :	主选择	字典	are used as	s payloads.					
Paste Load Remove Clear Add Add from lis	可自己 Enter a new item st [Pro version only]	主选择	字典		s payloads.					
Paste Load Remove Clear Add Add from lie	可自己 Enter a new item st [Pro version only]	主选择	字典		s payloads.					
Paste Load Remove Clear Add Add from lis	可自己 Enter a new item st [Pro version only] rocessing ne rules to perform variou	主选择	字典 g tasks on ear	ch payload l	before it is us	sed.				

7. 选择线程等

xff referer

现在浏览器中设置代理ip,再用burpsuite,我在虚拟机上完成 现在burp suite上抓包

Burp Project Intruder Repeater Window Help							
Dashboard Target Proxy Intruder Repeater Seq	uencer	Decoder	Comparer	Extender	Project options	User options	•
Intercept HTTP history WebSockets history Options]				KI .	**	
Request to http://111.198.29.45:33752							
Forward Drop Intercept is on	Actio	n			Comment th	is item	🛯 🦇 🕐
Raw Headers Hex	Scan [Send t	Pro versior o Intruder	only]	c	trl+1		17
GET / HTTP/1.1 Host: 111.198.29.45:33752	Send t	o Repeater	;	trl+R			
User-Agent: Mozilla/5.0(X11;Linux x86_64;rv:60.0)	Send t	o Sequenci	er				
Accept: text/html,application/xhtml+xml,applicatio	Send t	o Compare	r				
Accept-Language: zn,en-US;q=U./,en;q=U.3 Accept-Encoding:gzip.deflate	Send t	o Decoder					
Connection: close	Reque	st in brows	er		•		
Upgrade-Insecure-Requests: 1	Engag	ement tool:	s (Pro version	•			
Cache-Control: max-age=0	Chang	e request r	nethod				
	Chang	ie body enc	oding		hiigs://blog		evenios

再将X-Forwarded-For:123.123.123.123添加到反应头当中

Burp Project Intruder Repeater Window Help							
Dashboard Target Proxy Intruder Repeater Sequencer Decoder	Comparer	Extender	Project options	User option	rs		
Send Cancel < Y > Y				Targ	et: http://11	1.198.29.45:33	1752 🖉 🕐
Request		Res	ponse				
Raw Headers Hex		Rav	W Headers He	× HTML	Render		
<pre>GET / HTTP/1.1 Host: 111.198.29.45:33752 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0 Accept-Language: zh,en-US;q=0.7,en;q=0.3 Accept-Encoding: gzip, deflate X-Forwarded-For: 123.123.123.123 Connection: close Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0</pre>	0.8	Conte <htm <head <me <ti <li href= .min. <st; bo } </st; </li </ti </me </head <scri https </scri </htm 	<pre>sht-Type: text/h ll> ls ta charset="UTF- tle>index ody{ margin-left:au margin-right:au margin-TOP:2000 width:20em; tyle> ds s ="demo">ip地址必 pt:/document.get tyle></pre>	tml -8"> .e> aidu.com/bd sheet"/> to; uto; PX; 须为123.123 tElementByJ com"; <td>.123.123</td> <td>.0.3/css/boo /p> .innerHTML="</td> <td>w √ w 须来自</td>	.123.123	.0.3/css/boo /p> .innerHTML="	w √ w 须来自
Type a search term	0 matches	?	< + :	> Type a	search terr	n	0 matches
Done						log.csc/37 by	tes 49 millis

回复显示"必须来自https://www.google.com",就再将Referer:https://www.google.com添加到反应头当中,可以得出答案

Dashboard Target	Proxy Intru	uder Repeater	Sequencer	Decoder	[]				
	and the second sec	ACCORD TO A CONTRACTOR	and actives.	Decoder	Comparer	Extender	Project options	User options	
1 ×									

Send Cancel < > *	Target: http://111.198.29.45:33752 🖉 ?
Request	Response
Raw Headers Hex	Raw Headers Hex HTML Render
GET / HTTP/1.1 Host: 111.198.29.45:33752 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0 Accept-Language: zh,en-US;q=0.7,en;q=0.3 Accept-Encoding: gzip, deflate X-Forwarded-For: 123.123.123.123 Connection: close Referer: https://www.google.com Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0	<pre></pre> -0.8 -0.8 -0.8 -0.8 -o.8 -o.8 -o.8 -o.9
Type a search term	0 matches ⑦ < + > Type a search term 0 matches
Done	https://blog.co/843 bytes 64 millis

command_execution

ping是操作系统常用的网络诊断工具,可以用来判断连接是否建立。是利用IP地址的唯一性,发送一个数据包,以反馈的数据包 和反馈时间判断连接是否建立的方法。

首先判断链接是否建立,ping127.0.0.1是可以连接的。

PING

127.0.0.1

PING

```
ping -c 3 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.059 ms
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.050/0.054/0.059/0.003 msoc.esdn.na/savanlob
```

再在127.0.0.1当中寻找flag的文档,在ping当中注入命令使用&&逻辑符号,可以看到在/home中有一个flag.txt文件

PING

```
127.0.0.1 && find / -name "flag.*"
```

PING ping -c 3 127.0.0.1 && find / -name "flag.*" PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.072 ms 64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.063 ms 64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.062 ms --- 127.0.0.1 ping statistics ---3 packets transmitted, 3 received, 0% packet loss, time 1999ms rtt min/avg/max/mdev = 0.062/0.065/0.072/0.010 ms /home/flag.txt

打开这个文件就可以看到flag了。

PING

127.0.0.1 && cat /home/flag.txt

PING

```
ping -c 3 127.0.0.1 && cat /home/flag.txt
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.047 ms
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.044/0.048/0.054/0.007 ms
cyberpeace{a0bfec0a6f61c3fbcca747b3d92ab839}; /blog.csdn.nel/sevenlob
```

simple_js

这个不太清楚为什么这样就是答案,如果有大佬看到可以帮我解答一下吗

Ctrl+u查看源码

```
<title>JS</title>
function dechiffre(pass_enc){
    var tab = pass_enc.split(',');
            var tab2 = pass.split(',');var i,j,k,l=0,m,n,o,p = "";i = 0;j = tab.length;
                    n = tab2.length;
                    for(i = (o=0); i < (k = j = n); i++ ){o = tab[i-1];p += String.fromCharCode((o = tab2[i]))</pre>
                            if(i == 5)break;}
                                    p += String.fromCharCode((o = tab2[i]));
    p += String.fromCharCode(tab2[17]);
    pass = p;return pass;
String["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x
h = window.prompt('Enter password');
```

这一串先转十进制再转字符就是答案

但是我不懂为什么 我总算把攻防世界的web新手题做完了哈哈哈哈哈哈哈