## 初试ctf



https://blog.csdn.net/c1042503039

按照提示,用get方式提交参数,直接在url后面加上/?a=1(?应该是统一格式吧),我在这犯了一个错误,符号不小心用了中文形式的。

□ 答题	× 🛛 🗅 POST&GET	×	POST&GET	×	+				
$\leftarrow \   \rightarrow \   G$	③ 不安全   111.198.29.45:31966/?a=1								
请用GI	ET方式提交一个名为	a,值	<b>当为1的变</b> 量						
请再以POST方式随便提交一个名为b,值为2的变量									

# 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 xctf{f0f453f4cf9833d4338d1853b2fa3322}

C 查看器 Encryption →	□ 控制台 □ 调试器 {}样式编辑器 Encoding ▼ SQL ▼ XSS ▼ Oth	⑥ 性能 ❶ 内存 三 网络     er ▼ Chrome BackBar	8存储 🕆	无障碍环境 🔵 HackBar 🔒
Lo <u>a</u> d URL	http://111.198.29.45:31966/?a=1			
) E <u>x</u> ecute	✓ Post data ☐ Referrer ☐ User A	agent 🗌 Cookies		
	b=2			https://blog.csdn.net/c1042503039
flag就出现了 3、robots协议				
□ 答题	×	) robots	×	
$\leftarrow \rightarrow c$	③ 不安全   111.198.29	<b>9.45</b> :31977		

可以根据经验,直接在url后面加上/robots.txt

① 不安全 | 111.198.29.45:31977/robots.txt  $\leftarrow$  $\rightarrow$ C

User-agent: \* Disallow: Disallow: flag\_ls\_h3re.php

https://blog.csdn.net/c1042503039

之前到这就不会了,在朋友的提示下。访问f1ag\_1s\_h3re.php文件,即把robots.txt换成f1ag\_1s\_h3re.php。

← → C ③ 不安全 | 111.198.29.45:31977/f1ag\_1s\_h3re.php

### xctf{9e8499d961a52914a15b54516651320b}

https://blog.csdn.net/c1042503039

这里要介绍一个神器,dirsearch,扫目录脚本,通过dirsearch也可以发现robots.txt 4、备份文件

℃ ③ 不安全 | 111.198.29.45:31981

### 你知道index.php的备份文 件名吗?

https://blog.csdn.net/c1042503039

不知道没关系,用dirsearch可以扫描出来

应用程序	▼ 位置、	▶ 终端 ▼	<b>星</b> 期二00	:03	1	×	u(1))	() <b>-</b>
		自动	挂起					
		<b>外</b> 由于 1	长时间未活动,计算机将很	e快挂起h-master		•	•	8
文件	(F) 编辑(E)	查看(V) 搜到	索(S) 终端(T) 帮助(H)					
[23:	59:42] 403	- 297B	- /.htaccess.orig					^
[23:	59:42] 403	- 299B	<pre>- /.htaccess.sample</pre>					
[23:	59:42] 403	- 297B	- /.htaccess.save					
[23:	59:42] 403	- 297B	- /.htaccess.orig					
[23:	59:42] 403	- 295B	- /.htaccess_sc					
[23:	59:42] 403	- 295B	- /.htaccessBAK					
[23:]	59:42] 403	- 298B	<pre>- /.htaccess_extra</pre>					
[23:	59:42] 403	- 295B	- /.htaccessOLD					
[23:	59:42] 403 59:42] 403	- 293B	- /.ntaccess~					
[23:	59:421 403	- 291B	- /.htaroup					
[23:	59:42] 403	- 296B	- /.htpasswd-old					
[23:	59:42] 403	- 297B	<pre>- /.htpasswd_test</pre>					
[23:	59:42] 403	- 293B	- /.htpasswds					
[23:]	59:42] 403	- 291B	- /.htusers					
1001	00:01] 200 00:01] 200	- 438B - 494B	- /index.php - /index_nhn_bak					
[00:	00:01] 200	- 438B	<pre>- /index.php/login/</pre>					



在url后面输入/index.php.bak,输入完后它会下载一个文件

index.php.bak

 $\overline{}$ 

打开即可



5, cookie

× 🗋 Cookie	×	+
全  <b>111.198.29.45</b> :31983		

### 你知道什么是cookie吗?

https://blog.csdn.net/c1042503039

老方法,先用dirsearch扫描一波(有经验的人应该都不用扫描了),在url后输入cookie.php

#### 111.198.29.45:31983/cookie.php

### See the http response

https://blog.csdn.net/c1042503039

之后根据提示,打开开发者工具看响应头,即可发现flag

Cookie	×	+										-	ð	×
(←) → C' ŵ	-	i 111.198.	<b>29.45</b> :31983/cookie.php			D.C.	··· ☆		III\ (	Ð	4	9	5 ABP	≡
🍯 新手上路 📄 常用网址 🌐	【新提	躍】首页 - 中…	💮 吾爱破解 - LCG - LSG	⊕ 翁恺_中国大学MOOC	💮 课件目录 - 云课堂	💮 杭州电	子科技大学教	💮 数字杭电	Digital	ize			□移动	版书签

#### See the http response

	○ 査看	器 🖸 控制	台 🛛 调试器	{}样式编辑器	@ 性能	』● 内存 🗦 网络	8 存储	☆ 无障碍环境	HackBar	Adblock Plu	IS		0 ··· ×
⑪	♡过滤し	JRL						II 所有 HT	ML CSS JS	XHR 字体 图像	媒体 WS 其他	3 目持续日志 日禁用缓存	不节流 ♥ HAR ♥
壮	态	方法	域名	文作 触发源	类型	传输	大小	0 臺秒 80	▶ 消息头	Cookie 参数	响应 耗时	堆栈跟踪	
200	GET	r 🥻	<b>X</b> 111.198.29.4 [	🖹 <mark>co</mark> document	html	572 字节	411 字节	46 夏秒	▼ 过滤消息头				^
200	GET	Г 🌶	🖌 libs.baidu.com 🛽	bo stylesheet	CSS	已缓存	97.22 KB		▼ 响应头 (319	字节)			

404	GET	🔏 111.198.29.4 🗅 fav img	html 已缓存	290 字节	Content-Encoding: gzip Content-Length: 253 Content-Type: text/html Date: Tue, 19 Feb 2019 05:26:32 GMT flag: xctf(3503f5658b82df74bb2f886ef4a7dce0)
Q	3个请求 已使	输 97.91 KB / 572 字节   完成: 236 毫秒	DOMContentLoaded: 15	2 毫秒 load: 257 毫秒	Keep-Alive: timeout=5, max=100

6、如图



f12, 查看器, 吧disabled=""删喽, 即可

一个不能按的按钮

flag

#### xctf{2333dc398d0064cef151c839077b3a40}

□ 🕞 查看器 🕞 控制台 🗆 调试器 {}样式编辑器	◎ 性能 📲 内存 📄 网络	各 6	🔒 存储 🛭 🕆 无障碍环境 🛛 🧶 HackBar 🛛 🕸 Adblock Pl	us	
+	へ 捜索 HTML	Ň	♥ 过滤样式 + 『	.cls	<b>下</b> 布馬
<html> event</html>		^	▶ 伪元素	^	▼弹性盒
<head></head>			此元素		选择一
<h3>一个不能按的按钮</h3> ▼ <form action="" method="post"></form>			│ 元素 <mark>白 {</mark> 内联   height: 50px;	t	▼网格
<pre><input class="btn btn-default" disabled="" name="auth" style="hei type=" submit"="" value="flag"/></pre>	ght:50px;width:200px;"		width: 200px;		此页面
			.btn-default.disabled, .btn-bootstrap.min.css:7	1	▼盒 <mark>模</mark> 型
<h3>xctf{2333dc398d0064cef151c839077b3a40}</h3> 		~	derault[disabled], fieldset[disabled].btn-default, .btn- default.disabled:hover, .btn-default[disabled]:hover, fieldert[disabled].bts.default.hover, .bts		
html > body > form > input.btn.btn-default			default.disabled:focus, btn-default:focusp		42503039