Bugku ctf writeup--web进阶-Bugku-cms1



Bugku-cms1 100

地址:http://123.206.31.85:1001 后台可以getshell哟

flag在根目录



Step1:扫目录(工具自备)

ID	地址	HTTP响应
1	http://123.206.31.85:1001/?.asp	200
2	http://123.206.31.85:1001/index.php?chemin=%2f%2f%2f%2f%2f%2f	200
3	http://123.206.31.85:1001/index.php?option=com_user&view=reset&layout=con	200
4	http://123.206.31.85:1001/index.php	200
5	http://123.206.31.85:1001/global.php	200
6	http://123.206.31.85:1001/global.php	200
7	http://123.206.31.85:1001/index.php?chemin=.%2f%2f%2f%2f%2f%2f	200
8	http://123.206.31.85:1001/index.php	200
9	http://123.206.31.85:1001/index.php?option=com_user&view=reset&layout=con	200
10	http://123.206.31.85:1001/data/	200
11	http://123.206.31.85:1001/index php? # admin-loginOg. CSdn. net/qq_3	34200843

分析扫描结果可以看到一个/data目录

看看里面有什么东西,访问之后,发现一个sql文件,下载下来查看

/* This file is created by MySQLReback 2018-03-23 22:48:28 */
DROP DATABASE IF EXISTS `songcms`;/* MySQLReback Separation */ CREATE DATABASE `songcms`
/* 创建表结构 `song_admin` */
DROP TABLE IF EXISTS `song_admin`; /* MySQLReback Separation */ CREATE TABLE `song_admin`
`ID` int(8) unsigned NOT NULL AUTO_INCREMENT
`UserName` tinytext NOT NULL, https://blog.csdn.net/qq 33417843
`PassWord` tinytext NOT NULL,

文件中包含了用户名和密码,查找一下admin,发现有两个账户 admin和admin888,密码是md5加密,在线解密可得。 没有扫到后台管理,自己测试,在url后添加/admin,竟然就是后台

利用第一步中的账户密码去尝试一下,发现admin888才是管理员

^ (0	123.20	06.31.85:1001/admin/
管理首页 退出	航	▲ 关闭菜单 SongCMS企业建站系统
系统管理	«	当前版本:Version v3.13 免费版 (发布日期:2009-10-09)
栏目内容管理	«	服务器时间:2018年3月29日 15:47:04 服务器操作系统 · Linux (内核版本 · 2632-64262el6x8664)
新闻管理	()	1865ml2417g805 - Entox (Fiselic+ Entox (Fise
产品管理	*	站点物理路径:/web PHP版本:5.3.27o1
视频媒体	()	支持ZEND编译运行:× //blog.csdn.net/qq_33417843

根据题目提示,后台可以getshell,那么找上传点,在栏目内容管理里有添加页面内容

系统管理 《		添加栏目内容
	选择栏目:	==请选择栏目== ~ ~ *
栏目内容管理 🗧	内容标题:	•
 ビ目管理 	相关图片:	浏览
◎ 添加页面内容		
 页面内容管理 		□ #### E Z 및 ## ×, x' 庄田 漆 課 56 % ## ④ ↓ □ ∺ 59
新闻管理 《		
产品管理 《		計響ps://hil嘟囔_csdnli糟t/qq_30类7848

Step3: 上传图片马

利用php一句话和图片生成图片马,比如1.jpg,修改后缀为1.jpg;.php

然后在系统全局设定里,文件上传类型添加php,接着上传成功

NICOMPER X	ROMESEDECCE VO .	
◎ 系统全局设定	文件上传大小限制1:	2000 кв
 网站基本设置 	文件上传类型::	jpg,jpeg,qif,png,mp3,doc,php
% 系统操作日志	文件上传大小限制;;	10240 кв
• 系统高级参数设定	L WAS LODING !!	far Hos mo3 flying off ineg php
◎ 増加管理员	U.S. C. Bacar	10000000000000000000000000000000000000

在服务器文件管理模块里的页面内容上传图片找到刚才上传的图片:

			页面内容
文件名称(預览)		文件大小	
201803291449021522793173.php	log.csdn.r	et/ д_{13 к834} 1	7843

访问一下,然后用菜刀连接

÷	⇒ C	0 123.206.3	1.85:1001/upload	file/Pages/2018	0329144902152	22793173.php		
ÿ0 50 7.9 8î	Öÿà†JFIF DOOOOO 1	rrrHHÿÛC	3 ở ở∄ ởịi ⊥ịi ∏ịi XOOOOOOOO "Ĩ" ¡42±Á#BRSb ਪ੍ਰੋà ਪੈOyì. □ùú łł ÒÕ4ĐUÀè*idÑ D ^J D@DD ^J D@Z å ſ^, ?X Àùìqã	L↓ .)10.)-,3:J>))00000000)Ň⊣%35Cť ²6 ½Ňi{,@Qèñ⊡ï <`±í ^J ¥B² }¤-b• ;cD5)⊣1i#Ž9Ãñ Q^Š*™(ě!©"	36F7,-@WAF 00000000 5 "\$Tcs³áñÿÄ ^v÷S(, !újĩ _r ô μÖö ĐÊîĨÃ "(Û, Đ _[]-]dj [<u>]</u> * '\$/vī-àå-□bÕ	LNRSR2>ZaZ DOOOOOOO ¶r rÿĶ(rÿÚ ^L r [™] (7)?ù [−] Ff(Õ;°g´ l Ìù ¤** ₁ * .7qÄ]LQLZ*∏Ñ ÕZ~¾¢ÅzŽj [~]	P`JQROÿÛC DOOOOÿÀ d'4?Ì4(44 Du ¹ ß{ íĬĬÎÔ U ¹ BŽÓÆF} Üæ6v,]A	ſ∄₿₿!! 4!!&^{⊥⊥}&O5 ÜÜ ^L r ⁺ 1 4 r ^L 4 ,ÿÄ 4 r 4 ¦¶½«N] [¯] •û> [¬] È, fUÑejù4µ• <u>1</u> öÚ [™] G ¹ ÓQ3BJ ^J ĕõY¢J5 ÌŶ₩½Œ 'ÚÜ [°] ¢; ¹ ڌհy

Step4: 上菜刀

读取
属性
0755
0755
0755
0755
0755
0755
0755
0755
0755
0755
0755
0755
0755
0755
0755
0644
0644
0644
0644

在web目录下发现flag

	2123.206.31.85	123.206.31.85	+
载入	/web/flag_so.txt		
flag		1	17049
	https://blog.c	csdn.net/qq_334	1784