Bugku ctf writeup--web进阶-Bugku-cms1

原创

<darkeye> 于 2018-03-30 13:53:00 发布 5127 收藏
分类专栏： CTF 文章标签： writeups

本文链接：https://blog.csdn.net/qq_33417843/article/details/79756576

Web进阶---Bugku-cms1

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...	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...	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?q=admin-login	200

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 */
/* 创建数据库 `songcms` */
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,
  `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

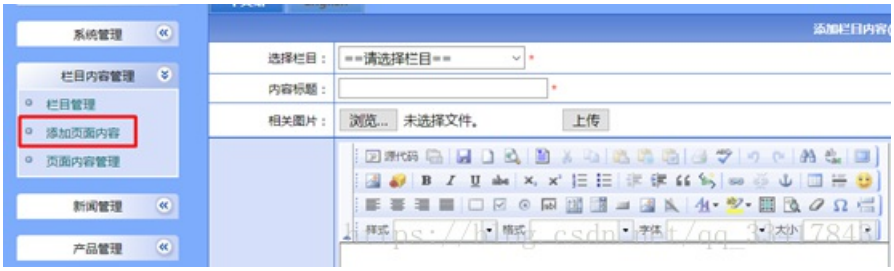
admin和admin888，密码是md5加密，在线解密可得。

Step2：后台登录

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

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

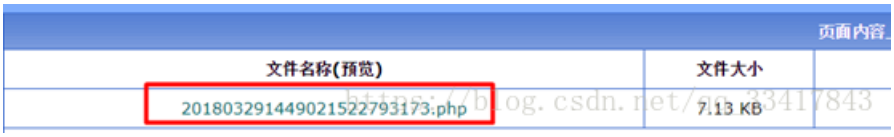


Step3：上传图片马

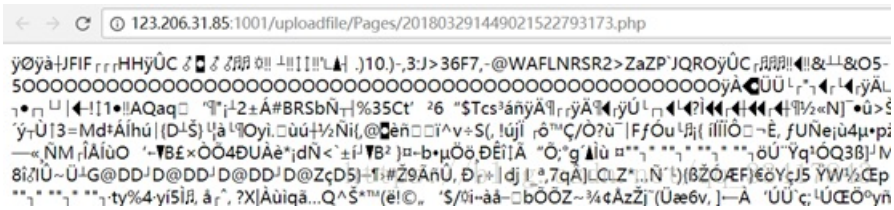
利用php一句话和图片生成图片马，比如1.jpg，修改后缀为1.jpg;.php

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

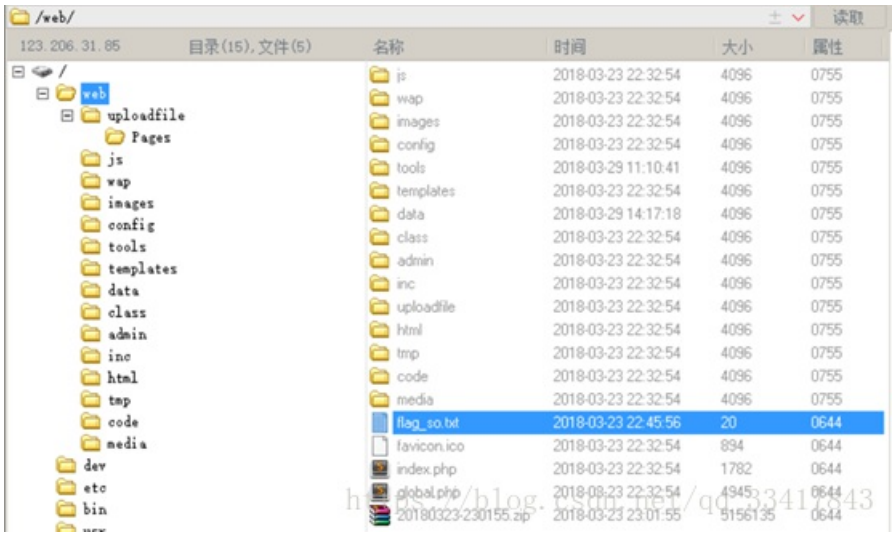
在服务器文件管理模块里的页面内容上传图片找到刚才上传的图片：



访问一下，然后用菜刀连接



Step4：上菜刀



在web目录下发现flag