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

封神台

https://hack.zkaq.cn/battle

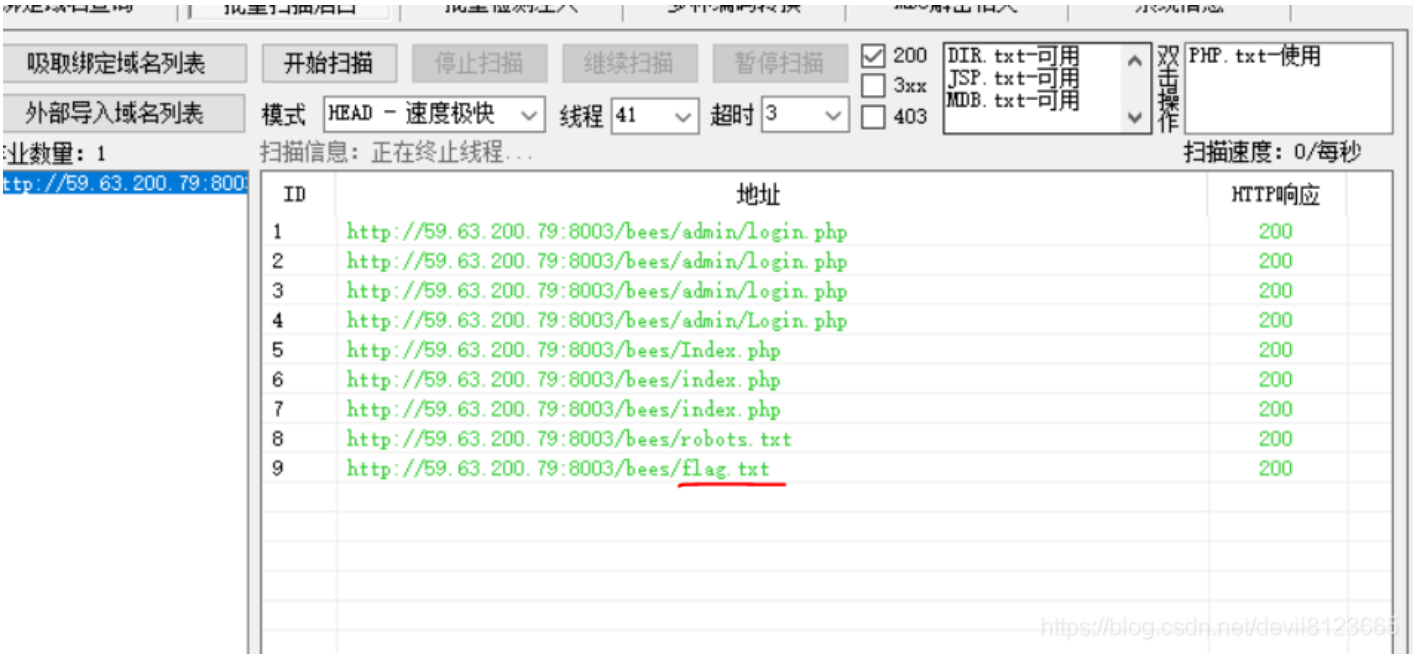
靶场

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



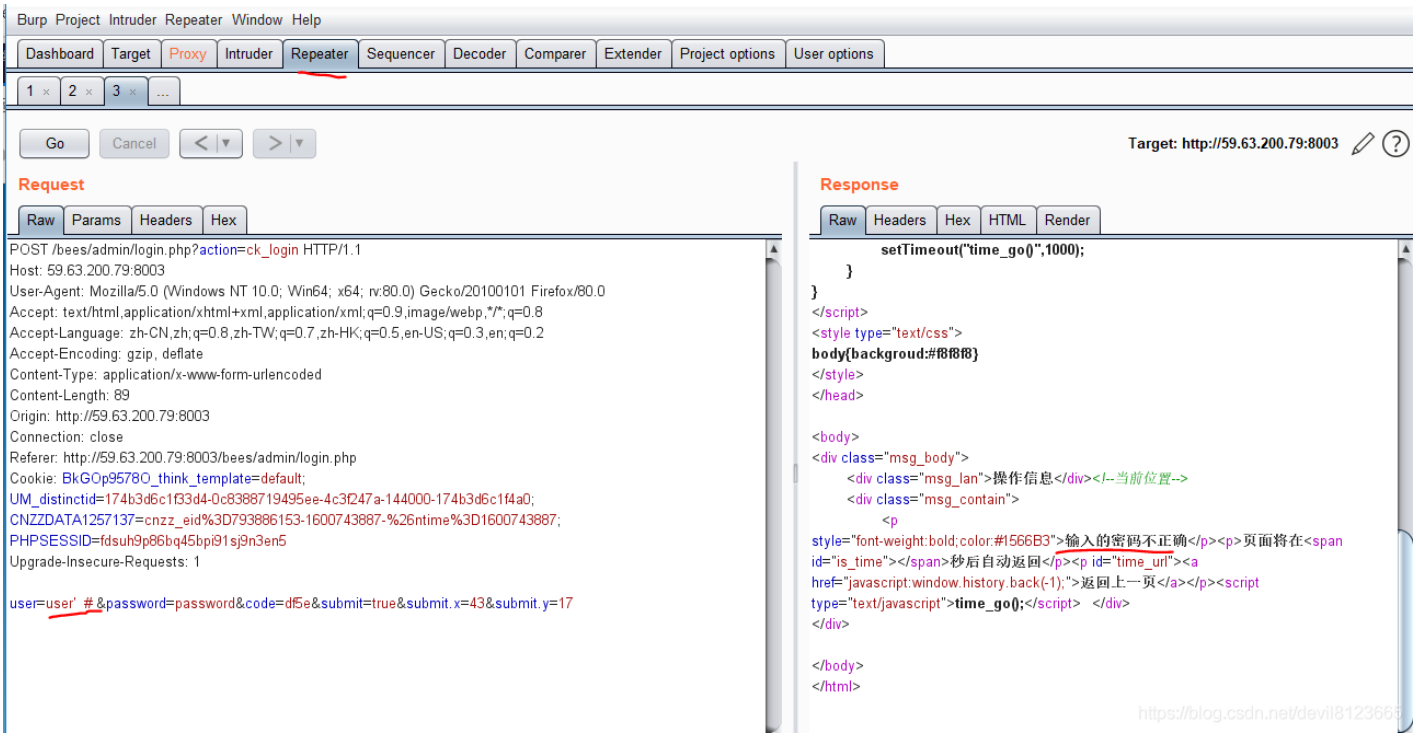
访问链接即可获得flag值。

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，看是否可以进行注入



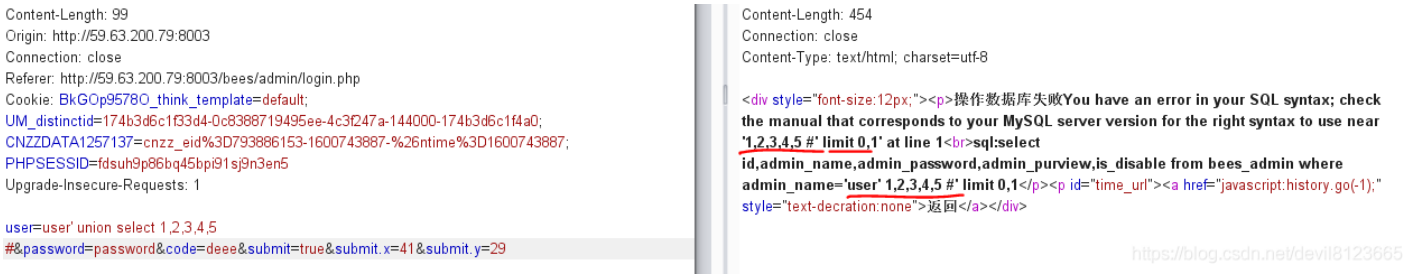
抓到包后send to repeater ， 将密码“user” 加上单引号跟“#”注释符号，发送，发现存在注入点

3 使用order by 进行爆破删选字段数

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

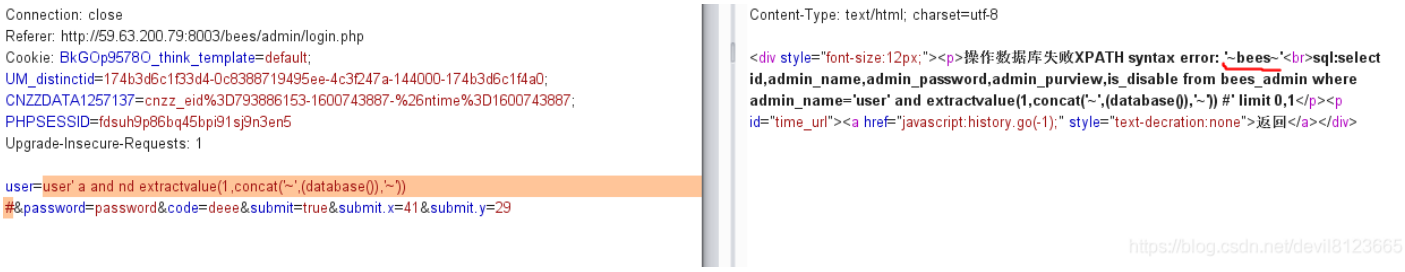


由上图划线处可以看到，系统进行了关键字的过滤，经过测试，发现“user' union seleselectct 1,2,3,4,5 #”下图可以绕过，但是没有回显字段。

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



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('~',(selselectect 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

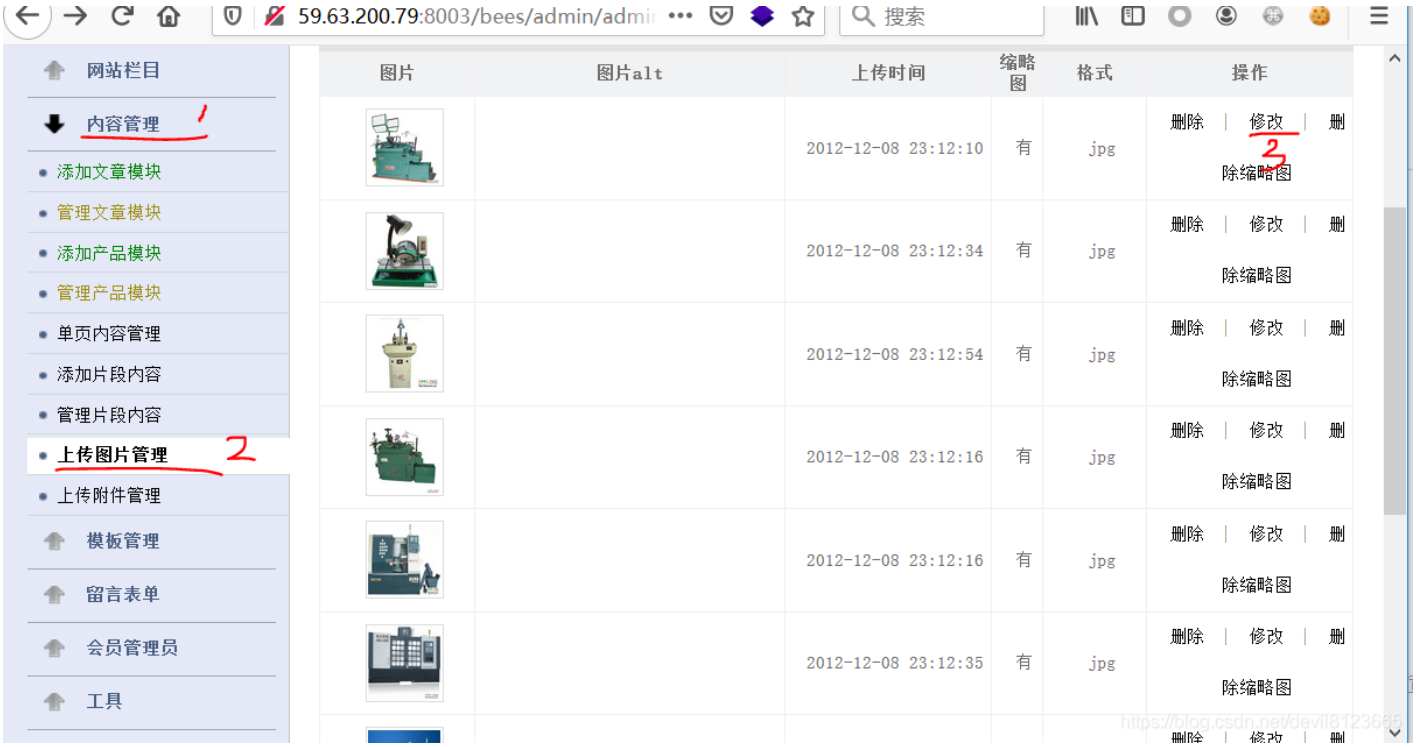
注入“user' a and nd extractvalue(1,concat('~',(selselectect admin_name fr from om bees_admin limit 1),'~')) #”获得用户名“admin”

注入“user' a and nd extractvalue(1,substr(concat('~',(selselectect 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。