

COSC 3364 – Principles of Cybersecurity

Lab 06

Database Access Control and SQLi

Ethan Conner

Provide screenshots where * is indicated.

Within MariaDB construct the following database named RECORDS:

STUDENTS

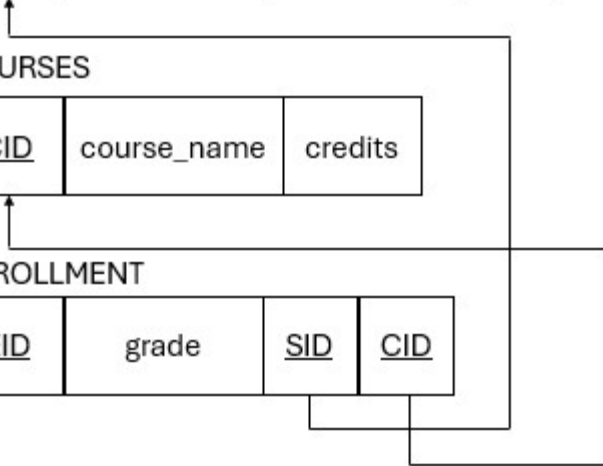
<u>SID</u>	first_name	last_name	DOB
------------	------------	-----------	-----

COURSES

<u>CID</u>	course_name	credits
------------	-------------	---------

ENROLLMENT

<u>EID</u>	grade	<u>SID</u>	<u>CID</u>
------------	-------	------------	------------



1. Create an admin user with all privileges and grant option.
2. Sign in as admin.
3. Create and use database RECORDS.
4. Generate the tables from the schema above and show tables.*
5. Insert three entries to each table and select all from each table.*
6. Create user Alice with all privileges and grant option.
7. Exit admin and sign in as Alice.
8. Create user Bob with SELECT privilege on RECORDS.ENROLLMENT.
9. Exit Alice, sign in as admin, and show all users.*
10. Revoke all privileges from Alice.

- a. What do you expect to happen to the SELECT privilege granted to Bob?
 - b. What did happen to the SELECT privilege granted to Bob?
11. Exit admin and sign in as Bob.
 12. Generate SQL statement utilizing a where clause of unknown SID to display all grades.*
 13. Attempt to include a drop table statement on ENROLLMENT along with previous SQL statement.*

Screenshots

4.

```
MariaDB [RECORDS]> SHOW TABLES
-> ;
+-----+
| Tables_in_RECORDS |
+-----+
| Courses            |
| Enrollment         |
| Students           |
+-----+
3 rows in set (0.000 sec)

MariaDB [RECORDS]> █
```

5.

```
MariaDB [RECORDS]> SELECT * FROM Students
-> ;
+-----+-----+-----+-----+
| SID | first_name | last_name | DOB       |
+-----+-----+-----+-----+
| 1   | Alice      | Smith     | 2002-01-14 |
| 2   | Bob        | Johnson   | 2000-04-19 |
| 3   | Joe        | Graftsma  | 2001-06-02 |
+-----+-----+-----+-----+
3 rows in set (0.000 sec)

MariaDB [RECORDS]>
```

```

MariaDB [RECORDS]> SELECT * FROM Courses
-> ;
+-----+-----+-----+
| CID | course_name | credits |
+-----+-----+-----+
| 1 | Mathematics | 3 |
| 2 | Biology | 4 |
| 3 | History | 2 |
+-----+-----+-----+
3 rows in set (0.000 sec)

MariaDB [RECORDS]>

```

```

MariaDB [RECORDS]> SELECT * FROM Enrollment
-> ;
+-----+-----+-----+-----+
| EID | grade | SID | CID |
+-----+-----+-----+-----+
| 1 | 90 | 1 | 1 |
| 2 | 85 | 2 | 2 |
| 3 | 78 | 3 | 3 |
+-----+-----+-----+-----+
3 rows in set (0.000 sec)

MariaDB [RECORDS]>

```

9.

```

MariaDB [(none)]> SELECT user FROM mysql.user
-> ;
+-----+
| User |
+-----+
| admin |
| alice |
| bob |
| mariadb.sys |
| mysql |
| root |
+-----+
6 rows in set (0.001 sec)

MariaDB [(none)]>

```

10.a. I expect him to lose all privileges as well.

11.a.

```
MariaDB [(none)]> SELECT * FROM RECORDS.Enrollment
-> ;
+-----+-----+-----+
| EID | grade | SID | CID |
+-----+-----+-----+
| 1 | 90 | 1 | 1 |
| 2 | 85 | 2 | 2 |
| 3 | 78 | 3 | 3 |
+-----+-----+-----+
3 rows in set (0.000 sec)

MariaDB [(none)]> show grants for 'bob'@'localhost';
+-----+
| Grants for bob@localhost |
+-----+
+-----+
| GRANT USAGE ON *.* TO `bob`@`localhost` IDENTIFIED BY PASSWORD '*2470C0C06DEE42FD1618BB99005ADCA2EC9D1' |
| GRANT SELECT ON `RECORDS`.`Enrollment` TO `bob`@`localhost` |
+-----+
2 rows in set (0.000 sec)

MariaDB [(none)]> █
```

Still had privileges

12.

```

MariaDB [RECORDS]> SELECT Grade FROM Enrollment WHERE SID = '' OR 1=1;
+-----+
| Grade |
+-----+
| 90 |
| 85 |
| 78 |
+-----+
3 rows in set (0.000 sec)

MariaDB [RECORDS]> █
```

13.

```
MariaDB [RECORDS]> SELECT Grade FROM RECORDS.Enrollment WHERE SID = '' OR 1=1; DROP TABLE Enrollment;
+-----+
| Grade |
+-----+
|    90 |
|    85 |
|    78 |
+-----+
3 rows in set (0.000 sec)

ERROR 1142 (42000): DROP command denied to user 'bob'@'localhost' for table `RECORDS`.`Enrollment`
MariaDB [RECORDS]> 
```