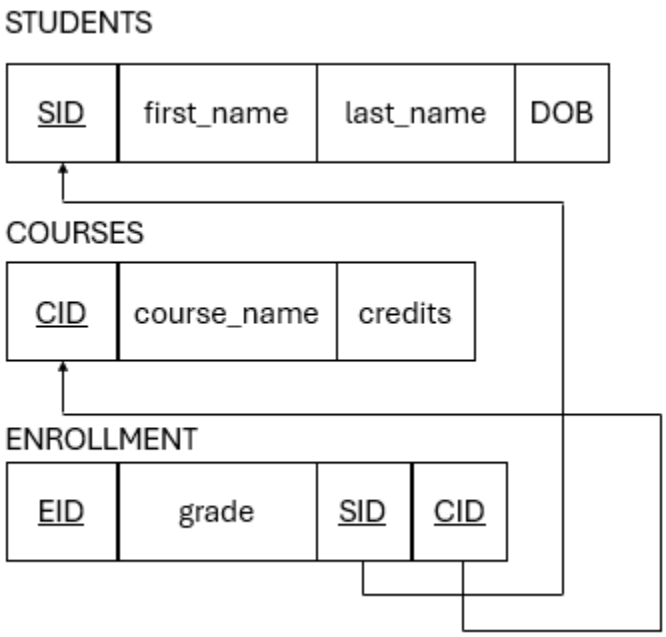
COSC 3364 – Principles of Cybersecurity
Lab 06
Database Access Control and SQLi

Provide screenshots where * is indicated.

Within MariaDB construct the following database named RECORDS:



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.*

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

MariaDB [RECORDS]>
```

5. Insert three entries to each table and select all from each table.*

```
MariaDB [RECORDS]> SELECT * FROM Students;
+-----+------------+-----------+------------+
| SID | first_name | last_name | DOB        |
+-----+------------+-----------+------------+
|   1 | Alice      | Smith     | 1998-01-15 |
|   2 | Bob        | Johnson   | 2000-03-20 |
|   3 | Charlie    | Brown     | 1999-05-10 |
+-----+------------+-----------+------------+
3 rows in set (0.000 sec)

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

MariaDB [RECORDS]> SELECT * FROM Enrollment;
+-----+------+------+-------+
| EID | SID  | CID  | grade |
+-----+------+------+-------+
|   1 |    1 |    1 |    97 |
|   2 |    1 |    2 |    88 |
|   3 |    1 |    3 |    74 |
|   4 |    2 |    1 |   100 |
|   5 |    2 |    2 |    67 |
|   6 |    2 |    3 |    70 |
|   7 |    3 |    1 |    45 |
|   8 |    3 |    2 |    87 |
|   9 |    3 |    3 |    99 |
+-----+------+------+-------+
9 rows in set (0.000 sec)

MariaDB [RECORDS]>
```

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.*

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

MariaDB [(none)]>
```

10. Revoke all privileges from Alice.

    a. What do you expect to happen to the SELECT privilege granted to Bob?

       Bob will retain the privilege even though Alice's privileges were revoked.

    b. What did happen to the SELECT privilege granted to Bob?

       Bob did retain the privilege (I also accidentally granted him all privileges instead of just SELECT privileges.)

11. Exit admin and sign in as Bob.

12. Generate SQL statement utilizing a where clause of unknown SID to display all grades.*

```
Database changed
MariaDB [RECORDS]> SELECT * FROM Enrollment WHERE SID = '' OR ""="";
+-----+------+------+-------+
| EID | SID  | CID  | grade |
+-----+------+------+-------+
|   1 |    1 |    1 |    97 |
|   2 |    1 |    2 |    88 |
|   3 |    1 |    3 |    74 |
|   4 |    2 |    1 |   100 |
|   5 |    2 |    2 |    67 |
|   6 |    2 |    3 |    70 |
|   7 |    3 |    1 |    45 |
|   8 |    3 |    2 |    87 |
|   9 |    3 |    3 |    99 |
+-----+------+------+-------+
9 rows in set (0.000 sec)

MariaDB [RECORDS]>
```

13. Attempt to include a drop table statement on ENROLLMENT along with previous SQL statement.*

```
MariaDB [RECORDS]> SELECT * FROM Enrollment  WHERE SID = '' OR ""=""; DROP TABLE Enrollment;
+-----+------+------+-------+
| EID | SID  | CID  | grade |
+-----+------+------+-------+
|   1 |    1 |    1 |    97 |
|   2 |    1 |    2 |    88 |
|   3 |    1 |    3 |    74 |
|   4 |    2 |    1 |   100 |
|   5 |    2 |    2 |    67 |
|   6 |    2 |    3 |    70 |
|   7 |    3 |    1 |    45 |
|   8 |    3 |    2 |    87 |
|   9 |    3 |    3 |    99 |
+-----+------+------+-------+
9 rows in set (0.001 sec)

Query OK, 0 rows affected (0.033 sec)

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

MariaDB [RECORDS]>
```

Mine did drop the table because I accidentally gave Bob all privileges.