Project Completion Report

Project Title: Creating Secured Website with Clear Authentication

Completed by: Muhammed Fadil Bin Noushad PV

Project Overview:

This project involved building a secure login page that effectively protects user credentials and manages sessions. The focus was on implementing best practices in authentication and session management, ensuring the security of sensitive data, and preventing common web vulnerabilities.

Detailed Steps:

1. Set Up the Project Environment:
   - Installed Apache, PHP, and SQLite on Kali Linux.
   - Configured the Apache server to serve the login page.

2. Create the Login Page (HTML):
   - Designed a simple and secure login page using HTML.
   - Ensured that the page included fields for username and password.

3. Develop the PHP Script for Authentication (`login.php`):
   - Implemented logic to handle form submissions securely.
   - Used prepared statements to prevent SQL injection attacks.
   - Ensured proper session handling and redirection upon successful login.

4. Create and Secure the SQLite Database:

- Created an SQLite database (`users.db`) to store user credentials.
- Added a `users` table with fields for `id`, `username`, and `password`.
- Inserted a test user with a hashed password using PHP?s `password_hash()` function.

5. Hashing Passwords:
- Created a PHP script (`hash_password.php`) to generate and display the hash of a password.
- Used the script to hash the password "qwerty123" and stored it in the database.

6. Database Configuration and Verification:
- Configured SQLite to ensure the database could be accessed securely from the PHP script.
- Verified that the user data was stored correctly by running SQL commands.

7. Configure PHP for SQLite:
- Ensured that the SQLite3 extension was enabled in the PHP configuration.
- Modified the `php.ini` file to include `extension=sqlite3`.

8. Testing the Login Functionality:
- Tested the login page by entering the test credentials.
- Verified that correct credentials led to a successful login and incorrect ones did not.

9. Finalization and Security Checks:
- Conducted final checks to ensure all security measures were in place.
- Reviewed the PHP, HTML, and database configurations for potential vulnerabilities.

Outcome:

The project resulted in a robust and secure login page that demonstrates best practices in web

security. It exemplifies your ability to implement essential cybersecurity measures in web applications, providing strong protection against unauthorized access and data breaches.