**APDS7311 ICE 1 TASK**

Karabo Dlamini ST10139672

1. Application security involves protecting applications from threats by addressing vulnerabilities through secure coding practices, access control, encryption, and other defenses.
2. Any data that enters your system and any data that enters your system from an untrusted source. To truly secure your app you must treat any kind of data as untrusted

3.1. Blacklist Input Validation: Relies on blocking specific inputs, which is unreliable as attackers can bypass the blacklist.

3.2. Lack of Parameterized SQL: Leads to SQL injection, as unsanitized inputs can manipulate database queries.

3.3. Use of Weak/Incorrect Ciphers: Results in insecure encryption, making sensitive data vulnerable to being decrypted by attackers.

4.

* User enters credentials.
* Browser sends a login request to the server.
* Server validates the credentials.
* If valid, server generates an access token.
* Server returns the token to the client.
* Client stores the token (e.g., cookies, local storage).
* On future requests, client sends token for authorization.
* Server verifies token validity.
* User gains access to authorized resources if the token is valid.