Jacques Durandt

ST10242724

APDS7311 ICE Task 1

1. In your opinion what is application security?

Application security is ongoing process that makes applications more secure by identifying and fixing security vulnerabilities. It is concerned with ensuring that software behaves as expected when an application comes under attack, in an effort to safeguard data from being accessed by unauthorized users. Within application security, security threats like unauthorized data access and session hijacking are addressed while also ensuring confidentiality and availability of information within the application.

2. Discuss the threat of untrusted data

Untrusted data is seen as any type of data that is received by an application from an external or unknown source (such as user input or third-party APIs). This data can be seen as a threat because it can be manipulated by attackers in an effort to exploit vulnerabilities within the application. Protocols like proper validation and sanitization is essential to avoid these risks.

3. Explain how HTTP drives web traffic

Hypertext Transfer Protocol (also known as HTTP) is a protocol that drives web traffic by defining how requests and responses to those requests are transmitted between clients and servers. When a user interacts with a web page, their browser will send a HTTP request to the server, which asks for specific resources such as HTML pages, data or images. The server then processes the request and responds with an HTTP response that contains the requested data. HTTP is seen as stateless, meaning that each request is independent.

4. Distinguish between the most common anti-patterns:

- Blacklist Input Validation: This is seen as a flawed approach to input validation, in which the system rejects or sanitizes known harmful inputs. This is seen as an anti-pattern because it is easy to miss new or unforeseen attack vectors, which allows attackers to bypass the blacklist by finding unblocked malicious input.

- Lack of Parameterized SQL: This anti-pattern happens when SQL queries are built dynamically by concatenating user inputs into the query string, which in turn exposes the system to SQL injection attacks. Without parameterized queries, an attacker can manipulate inputs in order to execute arbitrary SQL code, in which case they can potentially gain access to sensitive database information.

- Use of Weak or Incorrect Ciphers: The use of outdated or weak encryption algorithms (also known as ciphers) is seen as a significant security risk because attackers can access sensitive data by breaking the. This anti-pattern usually happens when developers use insecure ciphers like MD5 or SHA1 instead of the more modern cryptographic standards like AES or SHA-256.

5. Discuss the nine steps of the Login workflow

1) User Input: The user enters their credentials (username and password) into the login form.

2) Submission: The user submits the form, and the client sends the login data to the server over a secure connection (HTTPS).

3) Input Validation: The server will validate the input in order to ensure that the credentials follow the expected format.

4) Hashing the Password: The server hashes the password by means of a secure algorithm to compare it with the stored hash in the database.

5) Database Query: The server will query the database in this step to find the user’s record based on the provided username or email.

6) Password Comparison: The server will compare the hashed version of the password that was provided with the stored hash. If they are indeed a match, the user is then authenticated.

7) Session Creation: A session will be created for the user upon successful authentication. This session may be represented by a token (like JWT), which is stored in local storage or in a cookie.

8) Authorization: The server will check if the authenticated user does indeed have permission to perform certain actions of access certain resources, their status and role permitting.

9) Redirect to Protected Resource: Once authenticated and authorized, the user will be redirected to the protected area within the application (like their profile).