Spring Web Security Fundamental

Owner: Kwaku Duah
Reviewer: Thomas Darko
Contributors:
Date Generated: Tue Aug 20 2024

Executive Summary

High level system description

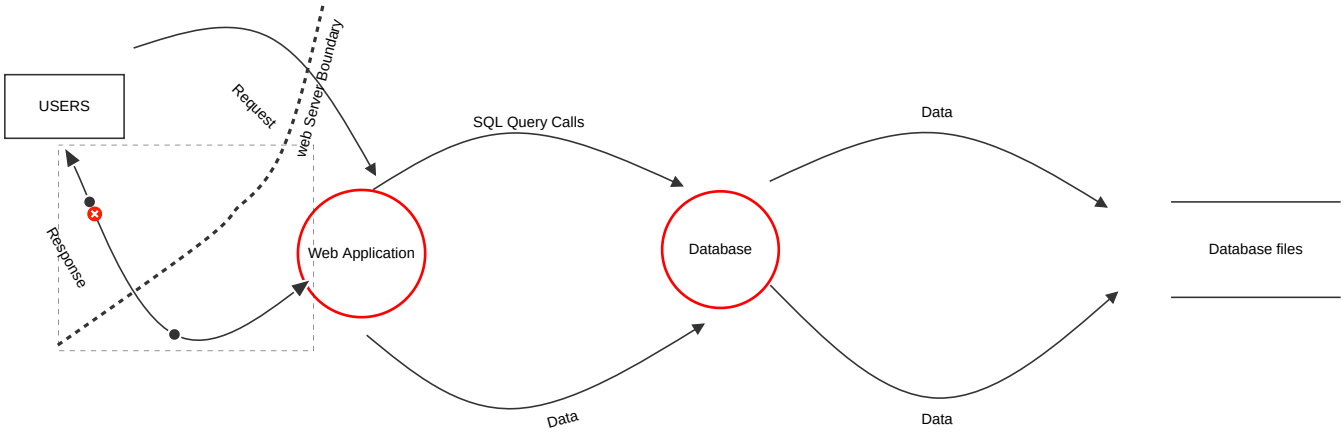
1. Authentication Service: Validates user credentials, issues and manages authentication tokens (JWT)
2. Authorisation Service: Checks user permissions and roles, enforces access control for resources.
3. User Management Service: Handles user registration, profile management, and stores user data.
4. Database: Stores user credentials (hashed), profiles, and roles.

Summary

Total Threats	6
Total Mitigated	2
Not Mitigated	4
Open / High Priority	0
Open / Medium Priority	3
Open / Low Priority	1
Open / Unknown Priority	0

Data Flow Diagram

This the whole flow of the web application



Data Flow Diagram

Web Application (Process)

Access to the website

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Tampering	Tampering	High	Mitigated		Malicious actors modify data or code through weak input validation	Use strong input validation, secure storage practices, and integrity checks to protect data and code
7	Denial Of Service	Denial of service	High	Mitigated		Attackers overwhelm the application, making it unavailable.	Implement rate limiting, traffic filtering, and resource scaling to mitigate DoS attacks
8	Elevation of privilege	Elevation of privilege	Low	Open		Attackers gain unauthorised higher-level access.	Regularly update and patch software, enforce least privilege principles, and conduct security audits to prevent privilege escalation.

Database (Process)

Database with files stored and password hashed

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Spoofing	Spoofing	Medium	Open		Attackers can impersonate legitimate users by stealing credentials or exploiting session vulnerabilities, gaining unauthorised access to web applications.	Implement multi-factor authentication and secure session management to prevent unauthorised access.
3	Repudiation	Repudiation	Medium	Open		Users deny actions due to insufficient logging	Ensure comprehensive logging and use digital signatures to provide non-repudiable proof of actions
4	Information Disclosure	Information disclosure	Medium	Open		Sensitive data is exposed due to misconfigurations	Apply least privilege access controls, strong encryption, and proper data handling to protect sensitive information.

Sequence Diagram

Sequence Of Events

Sequence Diagram