STRIDE Threat Modeling Report

Application Name: Secure Web Application

Objective: Identify and mitigate security threats using the STRIDE methodology.

Category	*Description*	*Example in Your App*	*Mitigation Strategy*
Spoofing	An attack targeting the impersonation of a person or a device.	An attacker logs into the system using a stolen password or fake identity.	Implement secure Password Hashing with bcrypt.
Tampering	Changing or modifying data without authorization.	An attacker intercepts an HTTP request and modifies the role from "User" to "Admin".	Use HTTPS (TLS), Input Validation, and Signed JWT Tokens to ensure data integrity.
Repudiation	Performing an action and denying it due to a lack of system records.	A user changes sensitive data and denies it because there are no logs proving their identity.	Enable Detailed Logging.
Information Disclosure	Disclosure of sensitive information to unauthorized individuals.	A vulnerability in the API exposes sensitive user fields like email or ID to unauthorized viewers.	Implement Encryption in transit, and use generic error messages.
Denial of Service	Attacks aiming to stop or slow down the system service.	An attacker sends 100,000 requests per second to the website to crash the server.	Implement Rate Limiting.
Elevation of Privilege	An attacker with limited privileges gaining higher unauthorized access.	A regular user exploits a vulnerability like SQL Injection to become an Admin.	Apply the Principle of Least Privilege and strict Role-Based Access Control (RBAC).