Design and Implement an Intentionally Vulnerable Application

Goal

The goal of this assignment is for students to develop a small-scale application of their choice (namely web or desktop) that intentionally contains at least 3 realistic and exploitable security vulnerabilities. The purpose is to understand how vulnerabilities are introduced during development and to later study their exploitation and mitigation.

Instructions

1. Design and implement a simple application that serves a specific function (e.g., user registration, messaging, file upload, etc.).
2. Introduce one or more common security flaws such as:
    - Command Injection
    - Race condition
    - Insecure File Handling
    - Input validation errors
    - SQL Injection
    - Cross-Site Scripting (XSS)
    - Insecure Authentication or Session Management
    - Etc.

Delivery

- Application with documented code. It should run in any operating system and without special restrictions, e.g. .jar file or a web page with a tomcat server. Guidelines to execute the application are mandatory **and if the application cannot be executed, it will not be graded**.
- A report (max. 10 pages excluding the cover) which describes:
    - how the vulnerabilities have been introduced
    - how vulnerabilities can be exploited
    - how vulnerabilities can be mitigated (but not implemented, just described)

The mark will be linked to the complexity of chosen vulnerabilities and their exploitation.