Project Description

A secure web application that is immune to some of the **OWASP Top 10 2021** vulnerabilities.

- You will implement a **secure application** that satisfies a specific requirement from each picked vulnerability.
- Each requirement will be an implementation of **secure code** that protects the application from the vulnerability mentioned in the requirement.
- There is **no language restriction** to the application. You're allowed to create your own simple application that satisfies only the functions mentioned in the requirements.

Project Requirements

On each of the following requirements, you'll be given the name of the vulnerability and the requirement that should be implemented to protect the application from this vulnerability.

- **A01 Broken Access Control**

  There should be a login system in the application. Also, there should be an **admin page** that is restricted from the normal users. The inputs should be prevented from **path traversal attacks** as well (in case they're prone to the attack).

- **A02 Cryptographic Failures**

  Any sensitive data that is being sent to the server should be encrypted using **strong cryptographic encryptions**. Keys should be **hidden** from the source code (hard to apply cryptanalysis for the attacker).

- **A03 Injection**

  Any data retrieval parameters should be protected from both **SQL** and **XSS** injections.

- **A04 Insecure Design**

  Limit false login attempts for each session. If a user tries to enter a wrong password for more than 3 times or more in 1 minute, they should be restricted from submitting any more requests for 10 minutes.

- **A05 Security Misconfiguration**

  Add an insert image facility that accepts only **image extensions**. **Size limitation** should be applied as well.

- **A07 Identification and Authentication Failures**

  Perform a **two-factor authentication** for the login system available on the application. This is applied to ensure that the person who's trying to access the account is the one who's they're claiming to be. **Passwords should be hashed** in the DB.

Project Instructions

The project delivered through a presentation including the **project code**, and a **documentation report**. There will be an **individual oral discussion** and each student is required to discuss at least **1 requirement**.

- Students can split into teams of **6 members maximum** per team. No code collaboration is allowed.
- The **due date** of the project documentation is on the **25th of December**. The presentation and code showing is in **week 13**.
- The report should include a **description** of the project, with a fair background.
- The report should include **analysis and design** of the target application.
- The report should also include **detailed explanation** of the scenarios conducted to **run the program and their outputs**.
- The report should include the **code with detailed comments**.
- You must **cite all the references** i.e. any internet web site, book, journal, article etc. that you have used as a source of information for your report.
- Please turn in a **softcopy** of your work personally to the TA. You are encouraged to ask the TAs for any clarifications. **Late submission is not accepted**.