**Introduction:**The assignment focuses on **enhancing the security** of a DETI memorabilia online shop to comply with **Level 1 Application Security Verification Standard (ASVS) requirements**. This involves conducting a **full web application compliance audit** and **implementing security improvements** while maintaining the shop's original purpose of selling DETI memorabilia.

**Grading Criteria:**Students are evaluated based on multiple criteria, including the initial ASVS evaluation, identification of high-relevance issues, justification of impacts, quality of solutions, code implementation, and documentation.

**Detailed Description:**

* The online shop, originally developed by students, must run without errors and inconsistent behavior. **The assignment begins with a security audit according to ASVS Level 1 requirements**.
* Students use the **OWASP ASVS checklist to analyze security** and address key issues. They must **implement improvements** and **add two selected software features** from a provided list, ensuring the original and improved versions are presented along with a detailed report.
* Students are required to employ the OWASP ASVS checklist for audits to conduct the security analysis and identify the **2 x Number of Students key issues**.
  + Moreover, students should act upon the selected key issues by improving the application accordingly while ensuring the implementation of two software features, along with the corresponding requirements, to be freely selected from the following list:
  + Password strength evaluation: requiring a minimum of strength for passwords according to V2.1, with breach verification using an external service;
  + Multi-factor Authentication (MFA) requiring the user to provide two or more verification factors to gain access to the Web application. Alternative authentication methods include the following:

– OAuth 2.0 + OIDC Login: enable login via OAuth 2.0 and OpenID Connect (OIDC) to authorize access to the Web application (relevant ASVS requirements: V2.1, V2.2);

– TOTP authentication login: enable login via one-time passwords generated with TOTP to authorize access to the Web application (relevant ASVS requirements: ASVS V2.8);

– FIDO/FIDO2 authentication login: enable login via challenge-response authentication implemented by FIDO/FIDO2 tokens to authorize access to the Web application (ASVS V2.9, V2.3).

* + Encrypted database storage: requiring that critical data is cyphered on the Web application (V6.1, V6.2, V8.3);

**Alternative Authentication Techniques:**Various authentication methods, **including OAuth 2.0, TOTP, and FIDO/FIDO2**, are available. Students can use identity providers like **Google Identity, Okta’s Auth0, or Autenticação.gov for OAuth 2.0. TOTP** authentication employs standard protocols with mobile applications like **Google Authenticator, and FIDO/FIDO2** authentication requires **tokens** and the **WebAuthn API.**

**Project Execution, Delivery, and Grading:**

* The project, designed for a group of four students, should be in a private GitHub repository within the detiuaveiro organization.
* Delivery includes **three folders (original app, improved secure app, analysis)** and a **README.md** with project details, authors, audited issues, and implemented improvements.
* Grading considers the **relevance of identified security issues**, **implementation of secure code**, and **documentation quality**.

**References:**

* **OWASP ASVS checklist for audits**
* **OWASP Application Security Verification Standard**
* **Have I Been Pwned API**