Assignment 2
Application Security Verification Standard (ASVS)

Version 1.0

Version log:

- 1.1: Added reference to OpenID Connect (OIDC)
- 1.0: Initial version

1 Introduction

The Application Security Verification Standard (ASVS) is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, tool vendors, and consumers to define, build, test and verify secure applications. In this sense, it establishes a framework of requirements and controls that guide the design, development and testing of contemporary Web/mobile applications.

In this assignment, students should evolve their DETI memorabilia online shop to comply with level 1 Application Security Verification Standard requirements. Students should first conduct a full Web application compliance audit, and then implement security improvements resulting from the audit.

The original purpose of the shop shall be maintained. The goal is to have a functional and secure shop with the ability to sell DETI memorabilia (mugs, cups, t-shirts, hoodies, and similar memorabilia). Students are required to present both the original and the improved version of the shop, detailing the outcomes of the security audit and the improvements implemented.

Grading will be based on multiple criteria, including the initial ASVS evaluation, identification of high relevance issues, justification of its impacts and the quality of the solutions. The code implementation and quality of the produced documentation will also be key elements of the evaluation.

2 Detailed description

Students have developed a small online shop application that sells memorabilia for DETI (Department of Electronics, Telecommunications, and Informatics) at the University of Aveiro. As originally stated, this store is expected to run without errors, without inconsistent behavior, and without pages/sections/fragments that do not fit the purpose of the online shop.

This assignment will begin with the audit of the developed Web application (**secure version**) according to the requirements for level 1 of the Application Security Verification Standard (ASVS). Level 1 is the minimum level of verification required for all Web applications. Controls at this level are fully testable by automated methods along with (some) manual dynamic methods. 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 (e.g., a 4 student group should analize 8 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);

Students should provide both the original and improved version of the online shop application, together with a report describing the impact of the identified issues and how they have been addressed.

3 Alternative authentication techniques

Regarding authentication based on OAuth 2.0 with OIDC, several alternative identity providers can be used:

- Google Identity
- Okta's Auth0
- Autenticação.gov

As for TOTP authentication, since this is a standard protocol (defined in RFC 6238), there are many client applications available for mobile devices, such as Google Authenticator, available on Android and iPhone.

About FIDO/FIDO2 authentication, you need to have a FIDO/FIDO2 token (we can provide 2 or 3) and you should use the WebAuthn API.

4 Project execution, delivery and grading

As for the first project, this work is expected to be implemented by **a group of 4 students**, and **MUST** reside in a private repository in the github/detiuaveiro organization, using the Github Classroom functionality (this is mandatory).

Delivery should consist of a git repository with at least three folders and a file:

- `app_org`: contains the original application, including instructions to run it.
- `app_sec`: contains the improved secure application, including instructions to run it.
- `analysis`: contains audit checklist/textual descriptions/logs/screen captures describing the identified issues for ASVS Level 1 and the implemented fixes;
- `README.md`: contains the project description, authors, and identifies the audited issues and the implemented improvements;

Projects will be graded according to the relevance of the security issues identified, implementation of the secure code, and the documentation produced.

This project is expected to be authored by the students enrolled in the course. The use of existing code snippets, applications, or any other external functional element without proper acknowledgement is strictly forbidden. If any content lacking proper acknowledgment is found in other sources, the current rules regarding plagiarism will be followed.

5 References

- OWASP ASVS checklist for audits

- OWASP Application Security Verification Standard
- Have I Been Pwned API