Assignment 1
Vulnerabilities in software products

Version 1.0

Version log:

- 1.0: Initial version

1 Introduction

In this assignment, students are tasked with developing an online shop specializing in DETI memorabilia at the University of Aveiro, encompassing products like mugs, cups, t-shirts, and hoodies.

The primary goal is to create a functional shop with concealed vulnerabilities that are not apparent to casual users but can be exploited to compromise the system. Students are required to present both a flawed and a corrected version of the shop, detailing how these vulnerabilities are explored and their impact.

Grading will be based on vulnerability exploration and impact analysis, as well as code implementation and quality of the produced documentation.

2 Detailed description

This assignment will focus on the existence of vulnerabilities in software projects, their exploration, and avoidance.

Students will develop a small online shop application that sells memorabilia for DETI (Department of Electronics, Telecommunications, and Informatics) at the University of Aveiro. The online shop will feature a variety of items, including mugs, cups, t-shirts, hoodies, and similar memorabilia.

The application should provide its function without errors, without inconsistent behavior, and without pages/sections/fragments that do not fit the purpose of the online shop.

However, this online shop should also suffer from a specific set of weaknesses, which are not obvious to the casual user but may be used to compromise the application or the system.

Students should provide both a flawed and correct version of the online shop application, together with a report demonstrating how those vulnerabilities are explored and their impact. The project must include vulnerabilities associated with CWE-79 (Cross-Site Scripting) and CWE-89 (SQL Injection). An additional set of weaknesses must be considered, according to the following rules:

- The CWE must be identified.
- The implementation must follow the logic and purpose of the online shop.
- Students should be able to demonstrate the vulnerability.
- The total number of vulnerabilities should exceed the number of students by 2.
- A bonus of 10% can be provided if the vulnerability is subtle, can be attributed to a bug (not intentional), and can be skipped by some light analysis.

It is expected that a user can fully understand the purpose of the online shop and use it to purchase memorabilia related to DETI at the University of Aveiro. The implementation can be simple, and some functions may be missing (e.g., the back-end can be omitted). After reading the report, a reader should be able to understand the online shop, the vulnerabilities, their exploration and impact, and how they can be avoided.

3 Project execution, delivery and grading

The project 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`: contains the insecure application, including instructions to run it.
- `app_sec`: contains the secure application, including instructions to run it.
- `analysis`: contains scripts/textual descriptions/logs/screen captures demonstrating the exploration of each vulnerability and the fix implemented;
- `README.md`: contains the project description, authors, identifies vulnerabilities implemented;

Projects will be graded according to the implementation and exploration of the flawed code, the implementation of the secure code, and the documentation produced.

The use of automated tools to scan the application is not forbidden. However, grading will mostly consider your work and your analysis, not on the findings (as they are deliberate).

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. Themes and python/php/javascript libraries can be used, as long as the vulnerabilities are created by the students. If any content lacking proper acknowledgment is found in other sources, the current rules regarding plagiarism will be followed.

4 About the online shop

The shop should be the one-stop destination for DETI memorabilia at the University of Aveiro! It should offer a wide range of items, from mugs and cups to t-shirts, hoodies, stamps, stickers, magnets, pins, whatever allows allowing you to proudly showcase your affiliation with the Department of Electronics, Telecommunications and Informatics.

Our primary focus is functionality and security, so while the shop can accommodate multiple items, we prioritize simplicity in the user interface, avoiding unnecessary complexity and aesthetics. We understand that a pretty UI is not your main goal here.

To kickstart your project, we present examples of various areas within the shop, providing a foundation for your creative exploration:

1. **User Management:**
   - User registration and login
   - User profiles
   - Password management (reset, change)
   - User roles and permissions (admin, customer)
2. **Product Catalog:**
   - Product listings with details (name, description, price, images)
   - Product categories and filters
   - Product search functionality
3. **Shopping Cart:**
   - Cart management (add, remove, update items)
   - Cart total calculation
   - Save cart for later or wish list
4. **Checkout Process:**
   - Shipping and billing information collection
   - Payment processing (credit card, PayPal, etc.)
   - Order confirmation and receipt generation
5. **Inventory Management:**
   - Tracking product availability (in-stock, out-of-stock)
   - Managing product quantities
6. **Order History:**
   - View and track past orders
   - Reorder from order history
7. **Reviews and Ratings:**

  - Allow customers to rate and review products
  - Display average ratings and reviews

5 References

- OWASP Top 10
- CWE@MITRE
- SQLMap
- Nikto
- OWASP ZAP