**Assignment 1**

**Vulnerabilities in software products**

Versão TL:DR

# Introdução

- Desenvolver uma loja online de merch. do DETI (Canecas, Copos, Canetas, T-shirts, Hoodies, Meias, Cuecas, Avó, Gato etc…).

- Loja **functional** com vulnerabilidades escondidas que não são aparentes para o user comum, mas podem ser exploradas para comprometer o sistema

- É necessário apresentar duas versões:

1ª versão com vulnerabilidades.

2ª versão corrigida com explicação detalhada das vulnerabilidades, como explorá-las e o seu impacto no sistema.

# Descrição

# - Funcinalidade sem erros/inconsistências (ie, pagina é de merch do DETI não vai “saltar” para o site do Ramona e funciona de igual modo para qualquer user comum registado).

- Deve incluir vulnerabilidades associadas com:

- CWE-79 (Cross-Site Scipting)

- CWE-89 (SQL Injection).

**Estas e outras vulnerabilidades devem ser consideradas de acordo com as seguintes regras:**

* Identificação do CWE.
* Implementação deve seguir a lógica e objetivo do website.
* Deve ser possível demonstrar a vulnerabilidade.
* Número total de vulnerabilidades DEVE EXCEDER o número de estudantes por 2 (ie, 4\*2 = 6, no minimo).
* 10% de Bónus se a vulnerabilidade é subtil, pode ser atribuída a um bug (não intencional) e pode ser “skipped” por “light analysis”.

A implementação pode ser simples e algumas funções podem estar ausentes (ex.: back-end pode estar omitido).

Após ler o RELATÓRIO, deve ser possível entender tudo, ie, objectivo da loja, vulnerabilidades e suas nuances, impactos e como evitar as mesmas.

# Execução, entrega e notas:

* **Execução:** Grupos de 4 com repositório privado (github/detiuav) usando Github Classroom (mandatório)
* **Entrega:** repo. git com **PELO MENOS 3 PASTAS** e **1 Ficheiro**:
  + **Pasta “app”:** Contem a aplicação insegura e explicação de como corer a mesma.
  + ***Pasta “app\_sec”:*** Mesma coisa mas é a aplicação Segura
  + ***Pasta “analysis”:*** contem scripts/descrições textuais, logs e screen captures para demonstrar a exploração de cada vulnerabilidade e a correcção implementada.
  + ***Ficheiro README.md:*** Contem: Descrição do projecto, autores e identificação de vulnerabilidades implementadas

**- NOTA:** Implementação e exploração de vulnerabilidades e análise de impacto, bem como qualidade do código e documentação produzida.

* Uso de ferramentas automaticas para scanner a aplicação não são proibidas MAS a nota tem em conta maioritariamente o trabalho do grupo e analise e não as deteções de problemas (pois são deliberadas).
* Código, aplicações ou elementos funcionais externos usados sem dar acknowledgement são PROIBIDOS (plágio, sujeito as coisas que conhecemos).
* Podemos usar temas e bibliotecas Python, PHP ou JavaScript desde que as vulnerabilidades sejam criadas pelos alunos.

# 

# IMPORTANTE:

Funcionalidade e segurança > quantidade de items ou aspecto estético.

**Lista de fundamentos base a seguir para criar a loja:**

## User Management:

* + User registration and login
  + User profiles
  + Password management (reset, change)
  + User roles and permissions (admin, customer)

## Product Catalog:

* + Product listings with details (name, description, price, images)
  + Product categories and filters
  + Product search functionality

## Shopping Cart:

* + Cart management (add, remove, update items)
  + Cart total calculation
  + Save cart for later or wish list

## Checkout Process:

* + Shipping and billing information collection
  + Payment processing (credit card, PayPal, etc.)
  + Order confirmation and receipt generation

## Inventory Management:

* + Tracking product availability (in-stock, out-of-stock)
  + Managing product quantities

## Order History:

* + View and track past orders
  + Reorder from order history

## Reviews and Ratings:

* + Allow customers to rate and review products
  + Display average ratings and reviews

# Referencias

* + [OWASP Top 10](https://owasp.org/www-project-top-ten/)
  + [CWE@MITRE](https://cwe.mitre.org/)
  + [SQLMap](https://sqlmap.org/)
  + [Nikto](https://github.com/sullo/nikto)
  + [OWASP ZAP](https://owasp.org/www-project-zap/)