ISEP INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO

**Mestrado em Engenharia Informática**
**Desenvolvimento de Software Seguro (DESOFS)**
2024/2025

# Project

## 1 Introduction

In this assignment, students are required to develop a project in a team. This project aims to develop students' skills in developing applications following the Secure Software Development Life Cycle (SSDLC) process.

The main goal is to get a computational system secure. Such computational system must have a well-defined purpose (school management system, social network, sales management and so on) with necessary functionalities to fulfill it.

The assignment is to be made in groups of four/five students of the same PL class (exceptions must be approved). The topic/theme or purpose is free (however, it must be discussed with PL instructors) and must be communicated until week 5 by email to `pbs@isep.ipp.pt`. This communication must include the name of the system, a brief description, the number and name of all member as well as the class id (according ). The accepted proposals will be added to a list in the Section 7.

## 2 Requirements (some)

The project consist on a development of a back-end application (running in a web server). The back-end application is a web application programming interface (API) (REST API or something similar) plus a relational database (memory database is not allowed).

Mandatory features:

- Considering the Domain-Driven Design (DDD) concepts, the Domain model has to encompass at least three aggregates (one of them could be for users).
- Authorization (with at least three different roles).
- Execution of the operating system functionalities in back-end server, such as creating directories, reading/writing files and so on.

## 3 Contents and Delivery

The project is split into two phases: Phase 1 and Phase 2. During the Phase 1, which takes three weeks, it is required to perform (and document) operations related to SSDLC Analysis and Design steps.

- Phase 1
  - Analysis/Requirements
    - Functional and non-functional requirements

    - Secure development requirements
    - Abuse cases
    - ...
  - Design
    - Threat modeling
    - Secure design
    - Secure architecture
    - Security test planning
    - ...

Phase 2 is split into two sprints, each taking three weeks, and it is required to perform (and document) operations related to SSDLC Implementation, Testing and Deployment steps.

- Phase 2: Sprint 1
  - Development and Testing;
    - DevSecOps: pipeline
    - Code reviews
    - SAST, DAST and IAST
    - SCA
    - Security testing
    - ...
- Phase 2: Sprint 2
  - Development, Testing and Deployment;
    - DevSecOps: pipeline
    - Code reviews
    - SAST/DAST and IAST
    - SCA
    - Security testing
    - Security configuration and installation
    - Security assessment
    - ...

The project code and documentation have to be available at one **git-based web repository** for instructors. Teams must give **administrator** permission to their PL instructor. To do so, they must use one of the following email addresses (check with your PL class instructor):

- crr@isep.ipp.pt
- ffs@isep.ipp.pt
- nap@isep.ipp.pt
- pbs@isep.ipp.pt

The development of the project must be supported by a repository, in which the teams must automate the SSDLC operations to aid their work.

- The repository name has to have the following structure: `desofs2025_<class-id>_<team-number>` (for example: `desofs2025_thu_crr_1`). Check the `<class-id>` field in Section 7.
- In the repository, at root level, there must have a folder called `Deliverables`.
  - This folder is to be used for storing *deliverables* and the ASVS checklist of each project phase or sprint.
    - A *deliverable* is a summary (with repository references for documentation, code snippets, files, and others) of the work carried out in a phase or sprint.
    - The OWASP Application Security Verification Standard (ASVS) is a list of security related elements that can be used as the main guideline for developing secure software and also to specify the security level.
  - These *deliverables* and ASVS checklist will be used for phase or sprint assessments.

# 4 Planning

The next table shows the week semester mapping,in which it is considered the first week day is on **Monday** and the last week day is on **Sunday**.

| **Week** | **Dates** | **Week** | **Dates** |
|---|---|---|---|
| 1 | 24/02 – 02/03/2025 | 9 | 28/04 – 04/05/2025 |
| 2 | 03/03 – 09/03/2025 | | **Queima** |
| 3 | 10/03 – 16/03/2025 | 10 | 12/05 – 18/05/2025 |
| 4 | 17/03 – 23/03/2025 | 11 | 19/05 – 25/05/2025 |
| 5 | 24/03 – 30/03/2025 | 12 | 26/05 – 01/06/2025 |
| 6 | 31/03 – 06/04/2025 | 13 | 02/06 – 08/06/2025 |
| 7 | 07/04 – 13/04/2025 | 14 | 09/06 – 15/06/2025 |
| 8 | 14/04 – 20/04/2025 | 15 | 16/06 – 22/06/2025 |
| | **Easter** | 16 | 23/06 – 29/06/2025 |

The following table shows the milestones. The **Start** refers to **Monday** at **0:01** and **End** to **Sunday** at **23:59** of the respective week (there are two exceptions). **Launch** and **Assessment** refer to whole week.

| **Week nr** | **Milestone** |
|---|---|
| 1 | |
| 2 | Launch: Project |
| 3 | |
| 4 | |
| 5 | |
| 6 | End: Teamwork composition |
| 7 | Start: Project: Phase 1 |
| 8 | End: Project: Phase 1 (27/04) |
| Easter | |
| 9 | Start: Project: Phase 2: Sprint 1<br>Assessment: Project: Phase 1 |
| Queima | |

| | |
|---|---|
| 10 | Assessment: Project: Phase 1 |
| 11 | End: Project: Phase 2: Sprint 1 (25/05) |
| 12 | Start: Project: Phase 2: Sprint 2<br>Assessment: Project: Phase 2: Sprint 1 |
| 13 | Assessment: Project: Phase 2: Sprint 1 |
| 14 | End: Project: Phase 2: Sprint 2 (11/06) |
| 15 | Assessment: Project: Phase 2 |
| 16 | Assessment: Project: Phase 2 |

**Pay attention:** * These assessments will take place in the PL classes and all team members have to be (mandatory) present.

## 5 Assessment

The DESOFS course has defined two assessment **Moments** plus **Exam**:

- Moment 1 (M1): Project: phase 1;
- Moment 2 (M2): Project: phase 2;
- Exam (E).

These Moments (M1 and M2) and E are:

- **"Mandatory" for all students, regardless of their status**.
- M1, M2, and E are graded in the interval [0.00,20.00];

**The DESOFS final grade (CF) is determined as follows**:

- CF = M1 * 0.20 + M2 * 0.40 + E * 0.40.
  - All CF components are graded in the interval [0.00,20.00]
  - M2 = 0.15 * Sprint1 + 0.15 * Sprint2 + 0.10 Project.
    - Sprint1 = Project: Phase 2: Sprint 1
    - Sprint2 = Project: Phase 2: Sprint 2
    - Project = Overall Project

**To grant access to the E**:

- (M1 * 0.20 + M2 * 0.40) / 0.60 >= 8.00 (8.00/20.00).

**To get success, you have to:**

- Grant access to the E
- E >= 8.00 (8.00/20.00).
- CF >= 9.50

**M1 and M2 are carried out in teams of 4/5 students, however the evaluation can be individual.**

# 6 Detailed Rubrics

The project will be assessed using the following rubric. The table describes the criteria for the maximum score (100%). We will assign scores of 100%, 75%, 50%, 25% and 0 according to the fulfillment of these criteria.

## 6.1 Phase 1: Threat Modeling

| **Criteria** | **Weight** | **Excellent:100%** |
|---|---|---|
| Organization and Language | 5% | Good organization of document and repository. Easy to follow, with all components linked to a main document. No major language (Grammar, Usage, Mechanics, Spelling) errors. |
| Analysis | 10% | System overview, architecture, and complete, well documented, domain model; all major components described; |
| Dataflow | 15% | Relevant data flows are documented in sufficient detail; System components, data flows, trust boundaries, and external entities are documented and use correct notation. Level 0 and 1 DFDs presented and levels 2+ presented when complexity justifies |
| Threat Identification and Analysis | 20% | Identifies most relevant threats, properly applying STRIDE per element of the DFD. Details attack vectors and threat agents with abuse cases. |
| Risk Assessment | 10% | Employ a well-defined risk assessment methodology to prioritise risks; justifies decisions |
| Mitigations | 10% | Proposes specific, clear and feasible mitigations to threats identified, focusing on high priority ones |
| Requirements | 20% | Security requirements justified (best practice, from threats identified, regulatory, ...) . Addressing: authentication & access control, data security, communication, input validationand data handling, third-party components, logging and monitoring. |
| Security Testing | 10% | Defines security testing methodology; Defines or refers to abuse cases; Threat modelling review process; Completeness of ASVS assessment, focusing on architecture; Tracebility between documented security requirements and tests |

### 6.2 Phase 2: Sprint 1

| **Criteria** | **Weight** | **Excellent:100%** |
|---|---|---|
| Organization and Language | 5% | Good organization of document and repository. Easy to follow, with all components linked to a main document. No major language (Grammar, Usage, Mechanics, Spelling) errors. |
| Development | 30% | Developed enough functionality to showcase automation. Documented set of development best practices adopted. Evidence of security audits, code reviews, static code analysis, software composition analysis, and other relevant practices. |
| Build and Test | 30% | Inventory of components, execution of test plans, dynamic analysis, configuration validation, artifact scanning, and other relevant practices. |
| Pipeline automation | 20% | Most practices are automated. |
| ASVS | 15% | Completeness of ASVS assessment; Tracebility between documented security requirements and tests |

### 6.3 Phase 2: Sprint 2

| **Criteria** | **Weight** | **Excellent:100%** |
|---|---|---|
| Organization and Language | 5% | Good organization of document and repository. Easy to follow, with all components linked to a main document. No major language (Grammar, Usage, Mechanics, Spelling) errors. |
| Development | 35% | Developed functionality according to complexity requirements (number of aggregates, authorization, backend functionality). Well organized code, according to best practices: domain encapsulation, consistent security controls, and more. Logging mechanisms introduced. |
| Build and Test | 35% | Scripted builds and tests. Mostly fully automated. Complete set of tests from static analysis, component analysis, dynamic analysis and more. |
| Production | 5% | Appreciatted, but not the emphasis of this project. Evidence of management of production infrastructure, logging and traceability, incident management, patch management, configuration management, OR other relevant practices. |
| Operate | 5% | Appreciatted, but not the emphasis of this project. Evidence of system and user monitoring, backup and restore, penetration testing, vulnerability managment OR other relevant practices. |

| | | |
|---|---|---|
| ASVS | 15% | Completeness of ASVS assessment; Tracebility between documented security requirements and tests |

### 6.4 Project

| Criteria | Weight | Excellent:100% |
|---|---|---|
| Overall quality | 100% | Overall high quality in delivered code, report and other artifacts. Very complete package. Practices from Phase I are very complete, or significantly improved. |

## 7 Themes/Topics and Teams

### 7.1 Class – Week day: Monday, Prof: FFS, Room: B309, ID: mon_ffs

| Team Number | Repo name | Team elements | Topic |
|---|---|---|---|
| 1 | desofs2025_mon_ffs_1 | - Diogo Magalhães, 1201100<br>- Daniel Graça, 1201822<br>- Rodrigo Tigre, 1201689 | Crypto Vault |
| 2 | desofs2025_mon_ffs_2 | - Hugo Coelho, 1162086<br>- Ilídio Magalhães, 1191577<br>- Paulo Abreu, 1240481<br>- Pedro Oliveira, 1240482 | AMAP |
| 3 | desofs2025_mon_ffs_3 | - Marco Verbruggen, 1170623<br>- André Santos, 1240438<br>- João Pires, 1210624<br>- Luís Silva, 1201198 | Medical Consultation Manager |

### 7.2 Class – Week day: Tuesday, Prof: CRR, Room: B408, ID: tue_crr

| Team Number | Repo name | Team elements | Topic |
|---|---|---|---|
| 1 | `desofs2025_tue_crr_1` | • Bernardo Azevedo, 1211111<br>• Leandro Fernandes, 1211118<br>• Gustavo Caiano, 1210983<br>• Hélder Serralva, 1181180 | MedSecure – Gestão Segura de Consultas |
| 2 | `desofs2025_tue_crr_2` | • Leila Felizarda, 1240470<br>• Pedro Ferreira 1201172<br>• Sandro Dias, 1201244<br>• Tomás Ribeiro,1191113 | |
| 3 | `desofs2025_tue_crr_3` | • Filipe Magalhães, 1211606<br>• Hugo Bumba, 1241935<br>• Pedro Ferreira, 1210825 | PetClinic |

### 7.3 Class – Week day: Wednesday, Prof: FFS, Room: B409, ID: wed_ffs

| Team Number | Repo name | Team elements | Topic |
|---|---|---|---|
| 1 | desofs2025_wed_ffs_1 | - Margarida Pereira, 1211105<br>- Pedro Moreira, 1211138<br>- Ricardo Alves, 1201562<br>- Manuel Sá, 1240472<br>- Javier Moras, 1240255 | Frame404 |
| 2 | desofs2025_wed_ffs_2 | - Márcia Guedes, 1201771<br>- Natália Freitas, 1240597<br>- João Dinis, 1211546<br>- Nuno Alves, 1140422<br>- Marta Ruano, 1200943 | |
| 3 | desofs2025_wed_ffs_3 | - Diana Marques, 1240445<br>- Diogo Costa, 1211514<br>- Pedro Costa, 1211439<br>- Pedro Vilarinho, 1211149<br>- Tiago Tavares, 1240494 | AMAP |
| 4 | desofs2025_wed_ffs_4 | - Martim Oliveira, 1181754<br>- António Guerra, 1190409<br>- David Ferreira, 1240444<br>- Tiago Silva, 1191938<br>- Rafael Gomes, 1211426 | Subscrição de Planos de Música. |

| | | | |
|---|---|---|---|
| 5 | desofs2025_wed_ffs_5 | Bruno Lopes, 1240441<br>Diogo Oliveira, 1240447<br>Gonçalo Azevedo, 1211560<br>Ivo Moutinho, 1240464<br>Tiago Teixeira, 1240493 | RecipeFlow |

### 7.4 Class – Week day: Wednesday, Prof: NAP, Room: B403, ID: wed_nap

| Team Number | Repo name | Team elements | Topic |
|---|---|---|---|
| 1 | desofs2025_wed_nap_1 | • | |

### 7.5 Class – Week day: Wednesday, Prof: PBS, Room: B311, ID: wed_pbs

| Team Number | Repo name | Team elements | Topic |
|---|---|---|---|
| 1 | `desofs2025_wed_pbs_1` | • João Veiga, 1201082<br>• Rui Barbosa, 1211106<br>• Luís Araújo, 1240159<br>• Paulo Mendes, 1211017 | Plataforma de e-commerce. |
| 2 | `desofs2025_wed_pbs_2` | • Daniel Oliveira, 1210693<br>• Diogo Silva, 1240446<br>• Fábio Monteiro, 1231423<br>• Maria Inês Gomes, 1240473<br>• Rúben Rodrigues, 1240490 | Sistema Seguro de Gestão de Seguros de Saúde |
| 3 | `desofs2025_wed_pbs_3` | • António Fernandes, 1190402<br>• Carla Barbosa, 1200928<br>• Carlos Rodrigues, 1230172<br>• Jorge Almeida, 1222598<br>• Nuno Figueiredo , 1230202 | Library Online Rental System |

### 7.6 Class – Week day: Thursday, Prof: CRR, Room: B209, ID: thu_crr

| Team Number | Repo name | Team elements | Topic |
|---|---|---|---|
| 1 | desofs2025_thu_crr_1 | • Miguel Moreira, 1211240<br>• Alice Resende, 1211518<br>• Sofia Marinho, 1211297<br>• João Parracho, 1201094<br>• Rui Marinho, 1191448 | Loja de videojogos e-commerce. |
| 2 | desofs2025_thu_crr_2 | • Francisco Xastre, 1211650<br>• José Castro, 1960548<br>• Diogo Sousa, 1222132<br>• Ricardo Aragão Correia, 1240599 | Loja de E-commerce de artigos desportivos |
| 3 | desofs2025_thu_crr_3 | • Isaac Santos, 118242<br>• João Batista, 1211396<br>• Wimy Carvalho, 1161297<br>• João Mata, 1151352 | sistema para gerir uma biblioteca |