II.3524 - Software security module

General information

Module title : Software security
Module identification : II.3524
Personr in charge : Saad EL JAOUHARI
ECTS : 5 credits
Average amount of work per student: from 100h to 150h with 42h in presential
Team work : Yes
Key words : Software security vulnerabilities, OWASP, vulnerability testing, security by design, change management, mobile application security, privacy by design

Presentation

Designing and developing a software, a website or a mobile application without taking into account the security aspect is like designing a car without a bumper, a windshield or a door locking system. This module aims to raise awareness and teach good security practices when developing software in general and Web and mobile applications in particular. It is based on the recommendations of the ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) and on the findings of the OWASP on the 10 most widespread software security flaws (https://owasp.org/www-project-top-ten/). In this module, students will be able to participate in coding workshops focused on security that will allow them to anticipate security flaws during the design and implementation stages of software, to detect security flaws, to secure existing code or to overcome an intrusion problem.

Educational objectives

Linked to the ISEP competency framework

Special skills

- Design a software or hardware technological object with safe and standardized operation
    - Master the management of the realization or development process
    - Ensure the quality and safety of a system
- Act in project mode
    - Know how to act as a project manager
        - Make optimized and adapted technical choices

Transversal skills

- Act as a dynamic player in a group
    - Work in a team, in a network, and in a culturally diverse environment
    - Lead a team, motivate it and make it evolve
    - Be a force of proposal
- Act as a responsible professional concerned with strategic issues
    - Demonstrate critical thinking and autonomy
    - Ensure the development of one's own skills

At the end of the module, learners will have learned to:

- Understand security requirements throughout the software life cycle
- Detect vulnerabilities in running applications
- Manage changes: update/upgrade existing software and/or replace one system with another

Prerequisites

- Have a solid knowledge of software development methods (from the most classical V methods to the most modern ones like Agile)
- Be comfortable with software development: programming

Content/program

Concepts

The following concepts, will be addressed:

- Confidentiality, Authenticity, Integrity, Availability, Traceability, Non-repudiation
- Security in the Software Development Life Cycle (SDLC)
- Security by design
- Source code related vulnerabilities, external code, etc.
- Identification and application of security controls in development environments
- Evaluation of the effectiveness of software security
- Evaluation of the impact of a new software acquisition
- Definition and application of guidelines and standards in writing secure code, both for web and mobile applications.
- ANSSI rules for secure software development
- ANSSI rules for the acquisition of software for the security of an IS.
- Privacy by Design and personal data processing
- Malicious code and attacks on applications: viruses, Trojan horses, worms, logic bombs, backdoors, etc.

Tools used by the teacher/instructor

The teacher/instructor will use the following tools/methods:

- OWASP ZAP
- Mobile Security Testing

Tools used by the learner

At the end of the module, learners will have learned to use the following tools:

- Tools for detecting vulnerabilities in code: OpenVAS, Nessus, etc.
- Vulnerability testing: Nessus, OpenVAS, Qualys, Core Impact, or Nexpose
- Web application security vulnerability detection with OWASP Zed Attack Proxy (ZAP)
- Development environments

Teaching methods

Learning methods

Presentation of the fundamentals in class with exercises and case studies. Implementation in the form of practical work initially, then in the form of a mini project. The practical work and the project will be done in groups of two.

Evaluation methods

- Individual : Final exam (30%)
- Collective : Practical work (TP) reports (35%) and a mini project (35%)

Working language

Module entirely delivered in English, students' productions in French or English as they wish

Bibliography- Webography – Other sources

- https://www.ssi.gouv.fr/guide/regles-de-programmation-pour-le-developpement-securise-de-logiciels-en-langage-c/

- https://www.ssi.gouv.fr/agence/publication/securite-et-langage-java/
- https://www.ssi.gouv.fr/particulier/logiciels-preconises-par-lanssi-2/
- Mike Chapple, James Michael, Darill Gibson. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 8th Edition. Chapter 21. Malicious Code and Application Attacks. Copyright © 2018 by John Wiley & Sons, Inc., Indianapolis, Indiana. ISBN: 978-1-119-47593-4
- Mike Chapple, James Michael, Darill Gibson. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 8th Edition. Chapter 20. Software Development Security. Copyright © 2018 by John Wiley & Sons, Inc., Indianapolis, Indiana. ISBN: 978-1-119-47593-4