REMPART INTERNATIONAL

TRAININGS

Cybersecurity for web development

The security of digital communication mediums

Target audience

All people performing function related to the development of information system and network monitoring (reasearch and development manager, project leader, developer…)

Goal

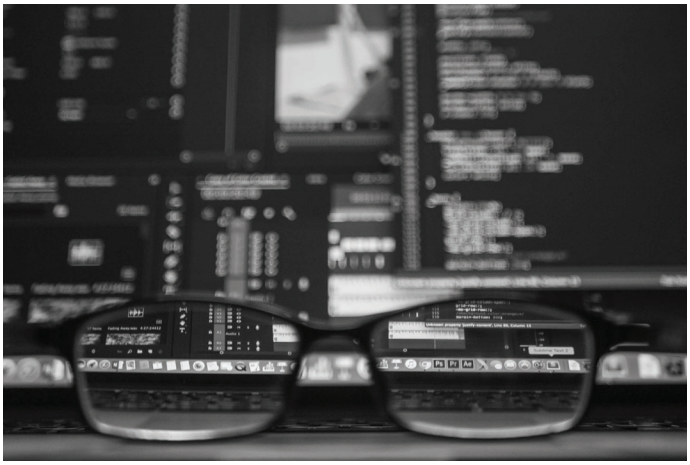
The purpose of this training is to improve the cybersecurity (and the quality as a side effect) of your web applications. After the presentation of the most common errors in the field of the web, this training will give you the good practices and the tools to minimize the vulnerabilities in software development.

Location

Within your company

Duration

10 hours



Training programme

Day 1

- A bug example that becomes a vulnerability : SQL injection
- The list and protection against classic bugs Top 10 OWASP (XXS, CSRF)
- Cybersecurity principles : minimization of attack surface, in-depth defense

Day 2

- Workflow and versioning code (git), ticketing
- Code documentation, doxygen example, encoding standards
- Tests : unitary, non-regression, integration, performances
- Continuous integration (buildbot)
- Project management and cybersecured development
- Conclusion : top 10 secure development practices

In addition to this training, we recommend to you to carry out an audit in order to optimize your protections.

Contact us for more information

Rempart-International
26, rue de Louvigny–L 1946 Luxembourg
T : +352 288 557 - contact@rempart-international.com
RCS Luxembourg B196245- Autorisation ME N°10058858/0 - 10058858/1 - 10058858/2 - Autorisation MJ N° 22-2-800-458