dartalis

Security Awareness for Web Developers

the Art of Information Security

A critical security challenge.

While some of the common security issues can currently be addressed with widely used security tools and technologies, other security breaches are much harder to avoid with standard means: the ones introduced by your in-house developed source code.

Any code written by a software programmer contains a potential security vulnerability and malicious hackers know that only too well. Indeed, statistics show that enterprise web applications are now the main target of attacks.

So why are web applications so insecure?

An easy answer would be that the majority of the developers don't focus on security when they create an application.

However, a further analysis might point out that the former statement is an easy blame. In fact, developers are not helped by today's context

- Secure development needs the developer to be security aware. However, development courses usually introduce to the development language and framework but too often omit to go over the security risks.
- Stressed to deliver more rapidly, even a security-aware developer will focus on functionality and tangible productivity gains rather than changes that might improve security.
- Development Frameworks don't enforce security when the developers use it
- Technologies change fast and developers need to be able to use newer versions of complex development frameworks in the appropriate way. This requires the developer to actually know that there is a change and to inform himself on how to use it correctly.
- Frameworks themselves introduce vulnerabilities and were not designed with security in mind
- Frameworks are complex and require the developer to understand more than just the development language. He needs to know what happens when and where the code executes

To summarize, two families of vulnerabilities exist: the ones introduced by the used technologies/frameworks and the ones introduced by the developer himself. The goal of this course is to create awareness among the risks that the developer might introduce by himself.

dartalis proposes a course based on the well-known Open Web Application Security Project (OWASP) which is a worldwide free and open community focused on improving the security of application software. Additionally, concrete attacks will be analyzed during workshops to show what really happens and how it can be prevented. For more in-depth security knowledge on a specific development language, dartalis also offers a Secure Development Course.

dartalis S.A. 17 rue Edmond Reuter L-5326 Contern Tel: +352267 469 1 Fax: +352 267 469 32 training@dartalis.lu

dartalis

Security Awareness for Web Developers

the Art of Information Security

What the course includes

The covered topics are:

- Introduction and Information Security
  Introduces information security, its main concepts and why it is important
- OWASP in a nutshell
  Provides insight about OWASP and its main subprojects
- What are Web Applications
  Introduces web applications, technologies and frameworks that are used
- Secure Design Principles
  Outlines security principles that should be observed by any developer
- Authentication
  Exposes the different authentication methods and the risks that they introduce
- Cryptography
  Explains the different cryptography families that exist, how they can be used and for what purpose
- Phishing, scamming, pharming, worms and malware
  Introduces developers to these attack vectors
- SQL injections
  Provides an in-depth analysis of this well-known type of attack
- XSS, XSSI, and XSRF injections
  Analyses the concepts behind these recent attacks
- Client State validation
  Describes the common pitfalls of session handling
- Buffer overflows
  Analyses the concepts behind such attacks
- Error Handling
  Describes the best practices in error handling
- Framework considerations
  Elaborate J2EE and/or .NET security considerations and tips

The dartalis consultants who will teach the course have a thorough understanding of the different attacks and security principles described during the class. They can obviously elaborate and go in-depth if a topic is of particular interest to the participants.

Logistics

The following practical details apply to this course:

- Course will be held at the dartalis premises. Max. 5 participants per class.
- This 2 day course is held from 09h00 to 17h00. Lunch included.
- The course material is in English, spoken language can be adapted to the group: EN, FR, DE, LU.

dartalis believes that Information Security should be managed as a recurrent and structured process which continuously enhances your security. The **Security Awareness for Web Developers** course is a full part of this process and provides to specific stakeholders the the security knowledge required to sustain a successful security initiative. Please contact us for additional information on the **dartalis Information Security Lifecycle**.

dartalis S.A. 17 rue Edmond Reuter L-5326 Contern Tel: +352267 469 1 Fax: +352 267 469 32 training@dartalis.lu