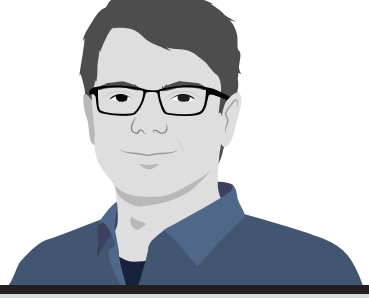
Secure Web Development

IT-Security Training



Training Contents

(3 DAYS)

Web applications are temptingly easy to create. Nowadays a few lines of code are sufficient to make a web application available to the Internet. However, this preceived simplicity often misleads developers to neglect important security aspects.This creates globally accessible entry points which attackers can often abuse with the simplest methods and minimal effort.

In the training *Secure Web Development*, using real-life examples, the participant is taught how an attacker finds and exploits security vulnerabilities in web applications.

The training will address the following questions:

- How do attackers proceed when looking for vulnerabilities in a web application? Which tools and procedures are used?
- How well is my web application protected against attacks? Where is it vulnerable?
- How can I harden my web application against attacks in just a few steps?
- Which measures are necessary to prevent future attacks against my web application?

Requirements

The course is designed for people who want to familiarize themselves with web hacking. This course is helpful for web developers (front-end and back-end), heads of a web development department and information security officers. It is helpful if you are familiar with web technologies, such as HTML.

Lecturer

Marcus Niemietz

For over a decade Marcus Niemietz has been working as penetration tester and web security trainer. As a co-founder of Hackmanit he has been responsible for web security since 2014. In addition, he is actively researching at the Ruhr University Bochum to prevent both UI redressing and cross-site scripting attacks. He is a regular speaker at numerous international IT security conferences, including the USENIX Security, Black Hat and Microsoft's renown hacker conference BlueHat. Marcus Niemietz is the publishing author of a book in the field of web security.

Contact

marcus.niemietz@hackmanit.de
www.hackmanit.de

HACKMANIT

Universitätsstraße 150 (ID 2/469)
44801 Bochum
Germany

DAY 1

- Short Introduction
  - HTTP, HTML, CSS, XML, DOM
- Social Engineering
- Information Disclosure
- Logical Flaws
- Same-Origin Policy
- Cross-Site Request Forgery
- Cross-Site Scripting
  - Non-persistent XSS
  - Persistent XSS
  - DOM-based XSS
  - Self-XSS
  - Mutation-based XSS
  - Scriptless Attacks

DAY 2

- Session Hijacking and Session Fixation
- UI-Redressing and Clickjacking
- DOM Clobbering
- File Inclusions and Path Traversal
- Remote Command and Code Execution
- SQL- and NoSQL-Injections

DAY 3

- Secure-Coding
  - OWASP TOP-10
  - Character Sets
  - DOCTYPE-Switch
  - Content Security Policy
  - Feature und Referrer Policy
  - Burp Suite
- Security Requirements