IT Security

Application Security & SDLC

by Bjoern Kimminich

Curriculum 2nd Semester

- 1. Open Web Application Security Project (OWASP)
- 2. **XSS**
- 3. Injection
- 4. Authentication Flaws
- 5. Authorization Flaws
- 6. Sensitive Data
- 7. Insecure Dependencies & Configuration
- 8. XXE & Deserialization
- 9. Secure Development Lifecycle

Schedule

- Tuesdays, 09:15 11:45
- 9 lectures (03.08. 28.09.20)
- 😁 100% via ZOOM (invite distributed via email/calendar).

Test Exam

- **CW40** (90min)
- ??:?? ??:?? / Audimax
- **1** Covers topics from both semesters
- Adjourning the exam is discouraged

System Requirements

To perform the exercises on your private computer you need

- either Node.js (14.x, 12.x or 10.x)
- or Docker
- i On the university computers Node.js should already be available. You can verify this by running node v on the command line. It should display a 10.x (or higher) version.
- Nou can always fall back to your personal laptop for the exercises as it should be free from virtualization, proxying or installation hurdles!

Recommended Resources

- OWASP: OWASP Top 10 2017
- OWASP: OWASP Cheat Sheet Series

Literature Recommendations (optional)

- Kimminich: Pwning OWASP Juice Shop, 2020
- Stuttard, Pinto: The Web Application Hacker's Handbook 2, 2011
- Zalewski: The Tangled Web: A Guide to Securing Modern Web Applications, 2011
- Zalewski, Heiderich: Tangled Web Der Security-Leitfaden für Webentwickler, 2012
 (=)

Awesome Web Security

Curated list of Web Security materials and resources.

https://github.com/qazbnm456/awesome-web-security

