

IT Security

Application Security & SDLC

by Bjoern Kimminich

Bjoern Kimminich

- [Nordakademie](#) Graduate (199a)
- IT Architect / AppSec Officer at [Kuehne + Nagel](#)
- Lecturer at [Nordakademie](#) since 2009
- Volunteer in the [Open Web Application Security Project](#)
- Board Member of the [German OWASP Chapter](#)
- Project Lead of the [OWASP Juice Shop](#)

Contact Information

- bjoern.kimminich@nordakademie.de ([062A 85A8 CBFB DCDA](#))
- <https://keybase.io/bkimminich>
- <https://twitter.com/bkimminich>
- <skype:bkimminich?chat>

Course Material

- All slides and references are in  language
- The lecture can be held in  or  language
- All course material is available *only on GitHub* at <https://github.com/bkimminich/it-security-lecture>
- Slides can be [downloaded as PDF](#) from GitHub
- All slides are published as [Open Educational Resources](#) under an unrestrictive [CC BY 4.0](#) license

You can help save a  by not  all slides for the entire course in advance as content might change during the course!

Curriculum 2nd Semester

- Open Web Application Security Project (OWASP)
- Common Attacks (Injection, XSS, CSRF, XXE, Deserialization)
- Authentication & Authorization Flaws
- Software Dependency Management
- Sensitive Data
- Secure Development Lifecycle
- Web Application Firewalls
- Security Automation & AppSec Pipeline

Organizational

- Tuesdays 9:15 - 11:45
- 9 lectures (31.07. - 29.09.18)
- **90min test exam** in last semester week
 - Covers topics from **1st and 2nd semester**

Rules

- Physical presence at lectures is mandatory and will be logged
- Exercises are mandatory (unless explicitly marked as *optional*)
- Active participation is encouraged. Otherwise at least be quiet

System Requirements

For most of the hands-on exercises you need *either*

- [Node.js](#) (8.x or 9.x)

or

- [Docker](#)

or

- [Vagrant](#)

Recommended Literature

- Kimminich: [Pwning OWASP Juice Shop](#), 2018
- OWASP: [OWASP Top 10 - 2017](#), 2017
- OWASP: [OWASP Cheat Sheet Series](#), 2018
- Stuttard, Pinto: The Web Application Hacker's Handbook 2, 2011