IKP-9170V Web security
credit: 1
for BSc and MSc students

lecturer: Mag. Dipl.-Ing. Dr. Michael Sonntag
JKU Linz
https://www.ins.jku.at/staff/michael-sonntag

12-16. April 2021

Schedule (via Teams)
12. April (Monday) 16:00-17:30,
13. April (Tuesday) 16:00-17:30,
14. April (Wednesday) 16:00-17:30,
15. April (Thursday) 16:00-17:30,
16. April (Friday) 16:00-17:30,

Summary:

Aim of the course is to give an introduction to current security issues regarding websites, and how they can be solved through technological means. Students will be introduced to these topics through lectures and examples using a small live webserver.

Content (1 Semester-hour lecture):

Day 1: Introductory lecture on website security
Day 2: Lecture on web-browser security measures
Day 3: Lecture on website security (part 1)
Day 4: Lecture on website security (part 2)
Day 5: Lecture on website security (part 3)

Literature

Students can access the slides online. No books or articles are necessary for the lecture.

Examination

There will be an (online) exam after the end of the course, which will be graded by the lecturer.

Basic knowledge required by participants:

1. General computer science and software development background

Detailed content of the course

Lecture 1: Website security basics

- What is „Website security" and how common are problems/attacks?
- How are attacks performed?
- Who is responsible for website security?

Lecture 2: Browser security features

- The Same Origin Policy (SOP)
- Cookies: How to secure them
- Content Security Policy (CSP): what is it, how to use it, limitations
- Subresource integrity
- DNS Rebinding – what is it, countermeasures
- HTTP Strict Transport Security (HSTS)

Lecture 3: Website security (1)

- Typical vulnerabilities: SQL injection, Cross-site-request-forgery
- What do to against them: Prevention, mitigation, detection

Lecture 4: Website security (2)

- Typical vulnerabilities: Cross-site-scripting, Sensitive data exposure
- What do to against them: Prevention, mitigation, detection

Lecture 5: Website security (3)

- Typical vulnerabilities: Authentication & session management, Insecure direct object reference, Bombs/resource exhaustion
- What do to against them: Prevention, mitigation, detection