Blekinge Institute of Technology
Department of Computer Science

Revision: 1
Reg.no: BTH-4.1.14-0312-2022

COURSE SYLLABUS

Säkerhet i webbsystem

Web System Security

7.5 credits (7,5 högskolepoäng)

Course code: DV2621
Main field of study: Computer Science, Software Engineering
Disciplinary domain: Technology
Education level: Second cycle
Specialization: A1N - Second cycle, has only first cycle course/s as entry requirements

Language of instruction: English
Applies from: 2022-08-29
Approved: 2022-03-01

1. Decision

This course is established by Dean 2021-12-03. The course syllabus is approved by Head of Department of Computer Science 2022-03-01 and applies from 2022-08-29.

2. Entry requirements

Admission to the course requires 90 credits, of which at least 40 credits withinn a technical area with one completed course with a minimum of 6 credits in programming in C or C++, PHP or Python and one completed course with a minimum of 4 credits in Network Security, Data Communication, Network Technologies and one completed course with a minimum of 4 credits in Web Technologies or Databases
or at least 120 credits, of which at least 90 credits within a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).

3. Objective and content

3.1 Objective

Web application security encompasses that the student should learn to understand and discover weaknesses and vulnerabilities in web applications both on the server side and on the client side. The objective for this course is for students to understand how weaknesses and vulnerabilities can be used, how they can be discovered and which solutions that can be used to protect web applications and minimalize the risk of such attacks.

3.2 Content

- Web system architectures and technologies.
- Reconnaissance attacks to the web applications
- Web Servers Vulnerabilities
- Injections attacks and Mitigation
- General session security.
- General authentication vulnerabilities
- General authorization and access control errors
- Server-side Request Forgery
- Business logic vulnerabilities
- OWASP Project (Open Web Application Security Project)
- Web Application Compliance: ISO 27000 series, PCI-DSS, HIPPA, SOC2, SOX, NIST
- Web-site security testing process.

4. Learning outcomes

The following learning outcomes are examined in the course:

4.1 Knowledge and understanding

On completion of the course, the student will be able to:

- explain vulnerabilities and weaknesses in web protocols and applications
- explain the security aspects of different technologies, frameworks and platforms
- explain authentication mechanisms and counter techniques to bypass authentication

- explain web application authorization and session management requirements and weak point
- understand Cross-site scripting (XSS) and Cross-site Request Forgery (CSRF) attacks
- understand Server-side Request Forgery (SSRF) attacks
- understand reasons and consequences of different injection vulnerabilities

4.2 Competence and skills

On completion of the course, the student will be able to:
- use best practice of known design patterns for secure web applications
- conduct internal and external security testing of web applications and related infrastructure
- utilize OWASP Project methodology

4.3 Judgement and approach

On completion of the course, the student will be able to:
- analyze and evaluate security information in a WEB client / server system
- identify vulnerabilities, weaknesses and implement appropriate improvement

5. Learning activities

The teaching is organized around lectures, recorded videos, together with presentations and literature. Throughout the course, communication, feedback, and discussions with teachers and fellow participants will take place through email, the course's online learning platform and physical or online-meetings.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
2210	Laboratory Session	4.5 credits	GU
2220	Practical Component	1.5 credits	GU
2230	On-campus Examination	1.5 credits	GU

The course will be graded G Pass, UX Fail, supplementation required, U Fail.

The information before a course occasion states the assessment criteria and make explicit in which modes of examination that the learning outcomes are assessed.

An examiner can, after consulting the Disability Advisor at BTH, decide on a customized examination form for a student with a long-term disability to be provided with an examination equivalent to one given to a student who is not disabled.

7. Course evaluation

The course evaluation should be carried out in line with BTH:s course evaluation template and process.

8. Restrictions regarding degree

The course can form part of a degree but not together with another course the content of which completely or partly corresponds with the contents of this course.

9. Course literature and other materials of instruction

- The Web Application Hacker's Handbook. Second Edition. Finding and Exploiting Security Flaws. Dafydd Stuttard, Marcus Pinto, ISBN: 978-1-118-02647-2.

- Web Penetration Testing with Kali Linux. Joseph Muniz. Aamir Lakhani, ISBN: 978-1782163169.

- Mastering Modern Web Penetration Testing. Prakhar Prasad, ISBN: 978-1785284588.

Materials such as research articles and other course materials, as well as recommendations for additional reading, are provided via the courses' online platform and via the BTH library services.

10. Additional information

This course replaces the course DV2577