Blekinge Institute of Technology
Department of Computer Science

Revision: 1
Reg.no: BTH-4.1.14-0245-2020

COURSE SYLLABUS

Säkerhet i webbsystem

Web System Security

7.5 credits (7,5 högskolepoäng)

Course code: DV2596
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

Subject area: Computer Technology
Language of instruction: English
Applies from: 2020-08-31
Approved: 2020-03-01

1. Decision

This course is established by Dean 2020-02-11. The course syllabus is approved by Head of Department of Computer Science 2020-03-01 and applies from 2020-08-31.

2. Entry requirements

Admission to the course requires at least 120 credits, of which at least 90 credits are in 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 as well as be able to develop solutions for protection and conduct tests.

Experience of operation or development of WEB applications and knowledge in HTTP, SQL, and PHP is desirable.

3.2 Content

• Basics and methods of protection in web, encryption and email protocols.
• Web system architectures
• Web attacks and vulnerabilities
• Authentication / Authorization
• Client attacks and protection in modern browsers
• Server attacks, such as remote command execution.
 - Attack techniques and avoidance of protection, such as code reuse attacks different version of vulnerabilities and attacks such as in-band, blind, out-of-band and second-order.
• Enumeration attacks and disclosure and leakage of information
• Remote command execution
• Disclosure and leakage of information
• Logical attacks
• Development of protected sites
• Open Web Application Security Project (OWASP) is used for implementation / testing
• Security review of a WEB site

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:
• be able to explain web protocols based on known vulnerabilities and weaknesses
• be able to describe the Common Vulnerability Scoring System (CVSS)
• be able to explain web protocols based on known vulnerabilities and weaknesses

- be able to explain the security aspects when using languages and framework, eg. PHP, JavaScript, and SQL
- be able to explain authentication mechanisms and counter techniques to bypass authentication
- understand Cross-site scripting (XSS) attacks and SQL injections
- be able to explain impacts of one or more combined vulnerabilities that limit or extend the damage given

4.2 Competence and skills

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

- be able to install and configure the web server for high security independently
- be able to use and search open vulnerability databases (Comon Vulnerability databases CV -DB) to prevent and find security problems
- be able to use best practice of known design patterns for secure web applications
- be able to utilize OWASP where applicable
- be able to conduct internal and external penetration testing of web applications and related infrastructure

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
- be able to identify vulnerabilities, weaknesses and implement appropriate improvement.

5. Learning activities

The teaching is organised around online lectures, pre-recorded videos, together with written material, literature, and research literature. Throughout the course, communication, feedback, and discussions with teachers and fellow participants will take place through email and the course's online learning platform.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
2010	Laboratory session 1	3 credits	GU
2020	Laboratory session 2	3 credits	GU
2030	Written assignments	1.5 credits	GU

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

The course-PM for each course revision should include 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

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