



LUNDS UNIVERSITET
Lunds Tekniska Högskola

Course syllabus

Webbsäkerhet

Web Security

EITF06, 7,5 credits, G2 (First Cycle)

Valid for: 2023/24

Faculty: Faculty of Engineering, LTH

Decided by: PLED C/D

Date of Decision: 2023-04-18

General Information

Main field: Technology.

Compulsory for: C3

Elective for: BME5, D4-se, D4-ns, E5

Language of instruction: The course will be given in English on demand

Aim

The course aims at giving the student knowledge about the security problems and solutions that relate to web based technology. Some areas will be addressed in more detail.

Learning outcomes

Knowledge and understanding

For a passing grade the student must

- Describe how web applications can be realized and how they interact with a web server.
- Describe the different security problems that arise when using web based protocols, applications and servers.
- Describe why the problems arise and how they can be avoided.

Competences and skills

For a passing grade the student must

- Be able to analyze the security problem and be able to propose solutions.
- Show that you understand the technical solutions that are used to avoid a security flaw.
- Show that you understand the security limitations in web based services.
- Be able to write a report of a project result and to present it to an audience.

Judgement and approach

For a passing grade the student must

During the course you have to be prepared to present and discuss your project.

Contents

Cryptology: time-memory trade-off attacks.

Web applications security: Security in PHP and MySQL, validation of user data with regular expressions, SQL-injections, cross site scripting, cross site request forgery, directory traversal, file inclusion, session attacks, HTTP response splitting.

Server security: HTTP server, PHP and MySQL configuration.

Client Security: Javascript, cookie-security, same-origin policy, CORS.

Remote login: Basic and digest access authentication.

Email and Spam: Email security, spamming techniques, spam filters, email tracking, DKIM SPF, DMARC, hashcash.

DNS Security: DNS configuration, Amplification attacks, DNS cache poisoning, DNS rebinding, DNSSEC.

A selection of the following topics are also included:

- E-cash overview: Blind signatures, blockchain technologies and digital monies, Bitcoin, Ethereum, smart contracts.
- Secure communication: TLS attacks
- Database security: Inference, differential privacy
- Anonymity: Traffic analysis, Chaum's Mix, Tor

The course also includes project work, which is summarized in a technical report and presented in a seminar.

Examination details

Grading scale: TH - (U,3,4,5) - (Fail, Three, Four, Five)

Assessment: Approved project work and mandatory online exam is required to pass the course with grade 3. An additional written exam is required for grade 4 or 5.

The examiner, in consultation with Disability Support Services, may deviate from the regular form of examination in order to provide a permanently disabled student with a form of examination equivalent to that of a student without a disability.

Parts

Code: 0123. **Name:** Project.

Credits: 3,5. **Grading scale:** UG. **Assessment:** Passing grade requires an approved written report and an approved oral presentation.

Code: 0223. **Name:** Tentamen.

Credits: 4. **Grading scale:** TH. **Assessment:** Final course grade 3 can be acquired by passing both the project and an online exam. The online exam is compulsory. Course grades 4 and 5 can be acquired through an additional, but optional, written exam.

Admission

Assumed prior knowledge: EITA25 Computer Security, EDA016, EDAA50, EDAA55 Programming, First course, or EDAA45 Introduction to Programming, and EDAF90 Web Programming. The student should be able to set up a database and execute simple SQL-queries.

The number of participants is limited to: No

The course overlaps following course/s: EITF05

Reading list

- Lecture notes.

Contact and other information

Course coordinator: Christian Gehrman, christian.gehrman@eit.lth.se

Course homepage: <https://canvas.education.lu.se/courses/>

Further information: When the course is given in Swedish, some parts of the course may still be given in English. All course material is in English.