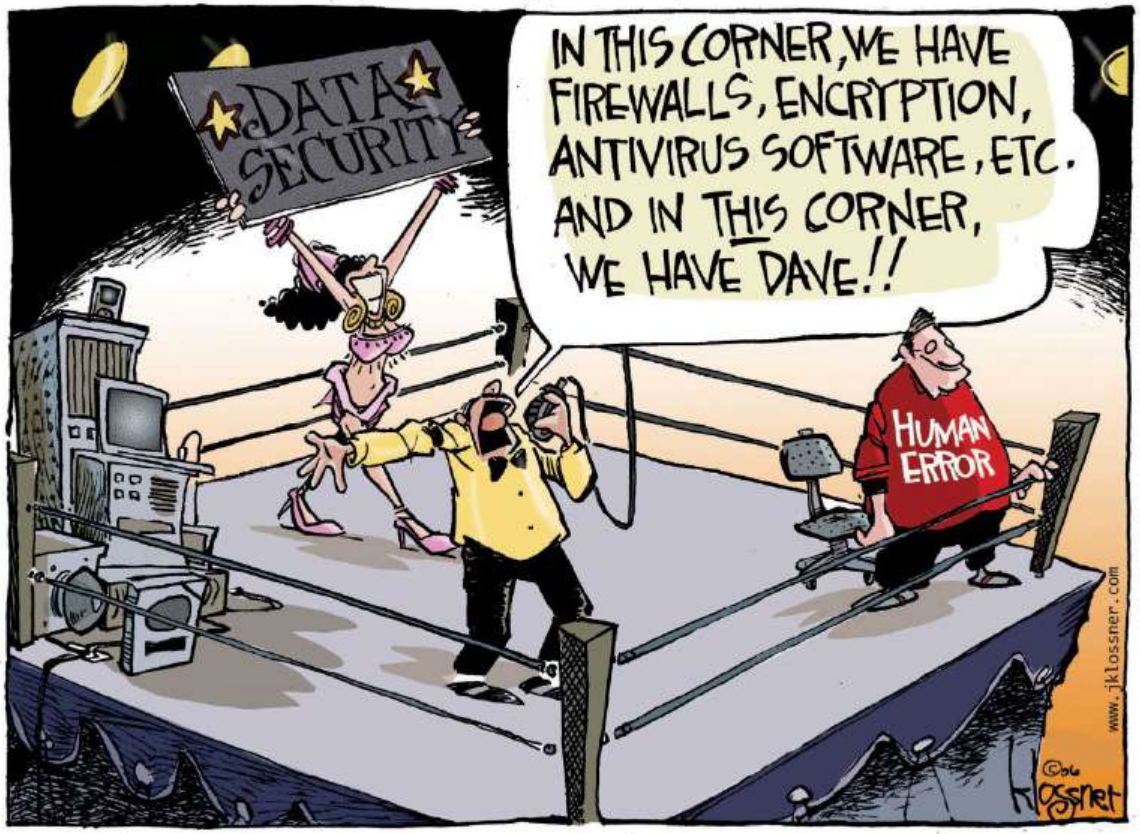
NTNU

Norwegian University of Science and Technology

TDT4237 Software Security and Data Privacy - Spring 2025



About Per Håkon Meland

- Lecturer: Per Håkon Meland
  - MSc and PhD from IDI, NTNU
  - Visiting scholar at UC Berkeley
  - Senior Research Scientist at SINTEF (>20 years)
  - Adjunct Associate Professor at IDI, NTNU
  - per.hakon.meland@ntnu.no

About Jingyue

- Coordinator and lecturer: Jingyue Li (Bill)
  - Master (Computer science) in China
  - Architect: IBM China Ltd.
    - Bank solutions
  - PhD and Post-Doc (Software engineering) at IDI
  - Principal researcher: DNV Research & Innovation
  - Jingyue.li@ntnu.no

Teaching Assistants

- Nicoline Mork
- Andreas Lilleby Hjulstad
- Nirushaan Selvaratnam
- Fredrik Fonn Hansen
- Lea Jahren-Andersen
- Eivind Nesje
- Ferdinand Tislevoll Eide
- Ahmed Yousif Mohamed Idries




Knowledge coverage

- Mainly according to ACM/IEEE Cybersecurity Curricula 2017
  https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

- Software security

- Data security and privacy

Software security

Software Security is the practice of building software to be secure and to continue to function properly under malicious attack.
(Gary McGraw)

Data Privacy

Compliance with data protection laws and regulations. Focus on how to collect, process, share, archive and delete the data

≠

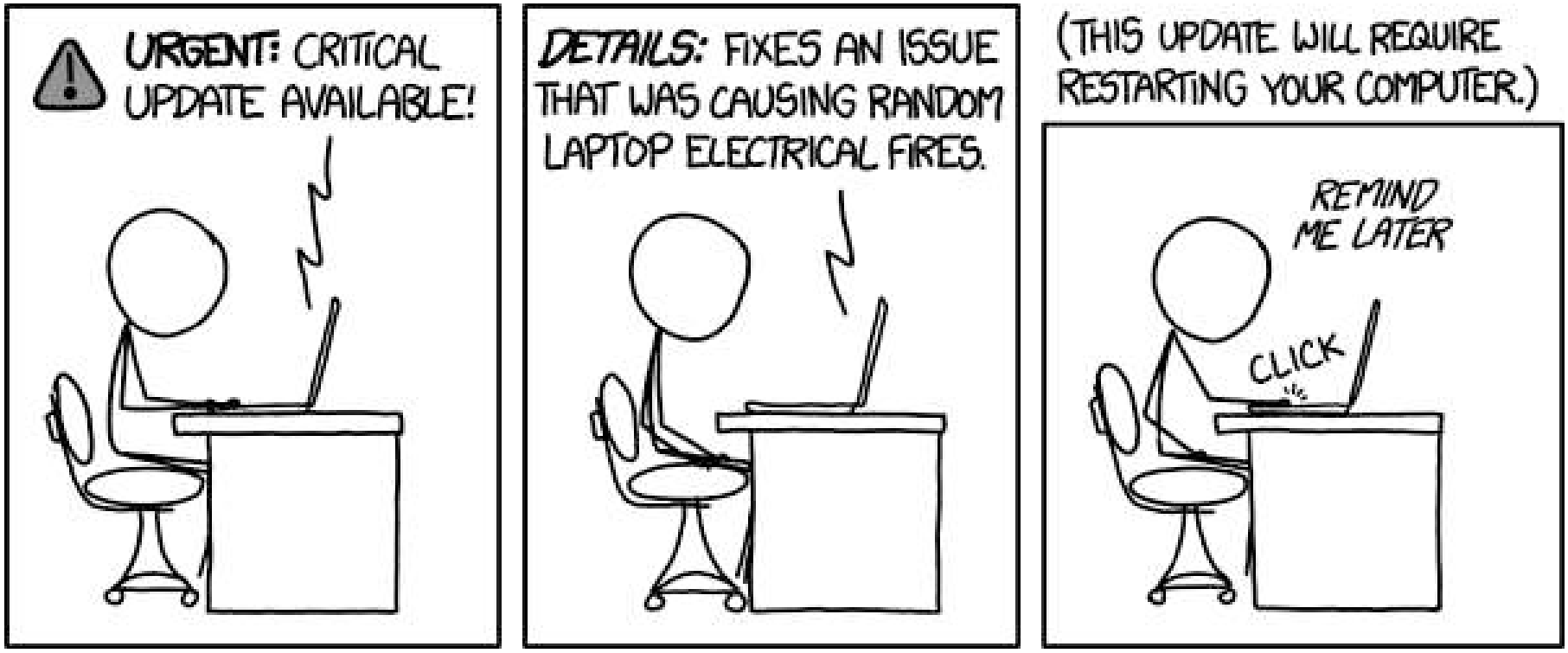
Data Security

Measures that an organization is taking in order to prevent any third party from unauthorized access.

https://dataprivacymanager.net/5-things-you-need-to-know-about-data-privacy/

Goal of teaching

Avoid «Penetrate & Patch»

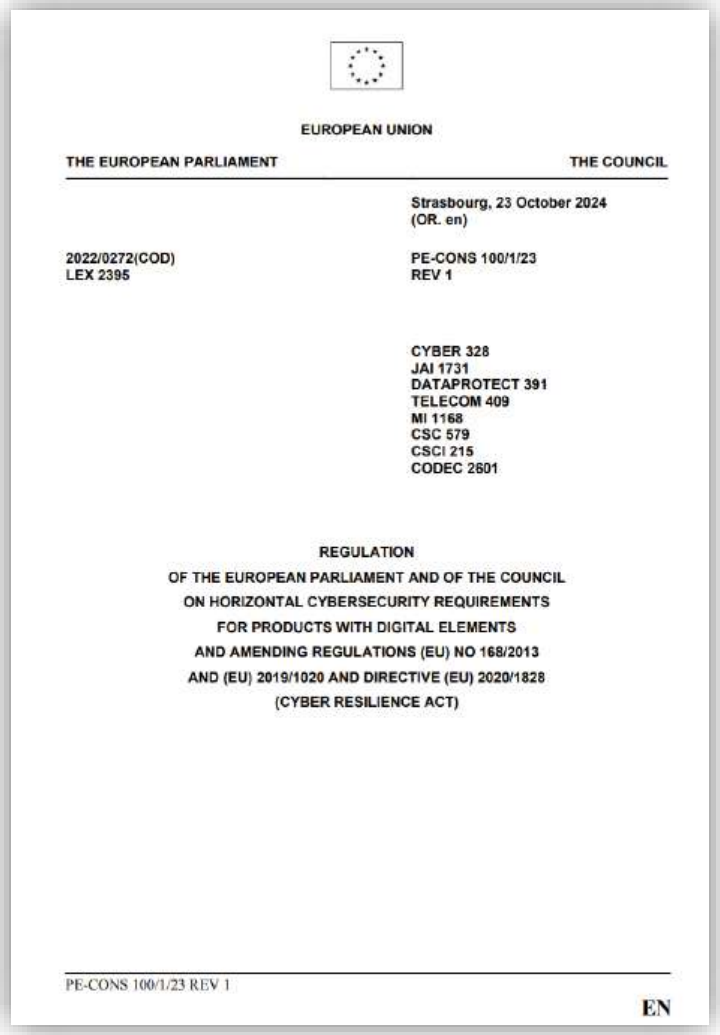


https://xkcd.com/1328

- 54% of organizations push vulnerable code in order to meet a critical deadline, with plans to remediate in a later release.
- 29% of developers lack the knowledge to mitigate issues identified

The European Cyber Resilience Act (CRA)

- Starting January 2025
- Key obligations
  - Risk assessment
  - Documentation (SDLC, SBOM, …)
  - Conformity
  - Vulnerability reporting
- Exceptions: Web-pages, OSS, …



EUROPEAN UNION

THE EUROPEAN PARLIAMENT | THE COUNCIL

Strasbourg, 23 October 2024
(OR. en)

2022/0272(COD)
LEX 2395

PE-CONS 100/1/23
REV 1

CYBER 328
JAI 1731
DATAPROTECT 391
TELECOM 409
MI 1168
CSC 579
CSCI 215
CODEC 2601

REGULATION
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
ON HORIZONTAL CYBERSECURITY REQUIREMENTS
FOR PRODUCTS WITH DIGITAL ELEMENTS
AND AMENDING REGULATIONS (EU) NO 168/2013
AND (EU) 2019/1020 AND DIRECTIVE (EU) 2020/1828
(CYBER RESILIENCE ACT)

PE-CONS 100/1/23 REV 1

EN

https://data.consilium.europa.eu/doc/document/PE-100-2023-REV-1/en/pdf

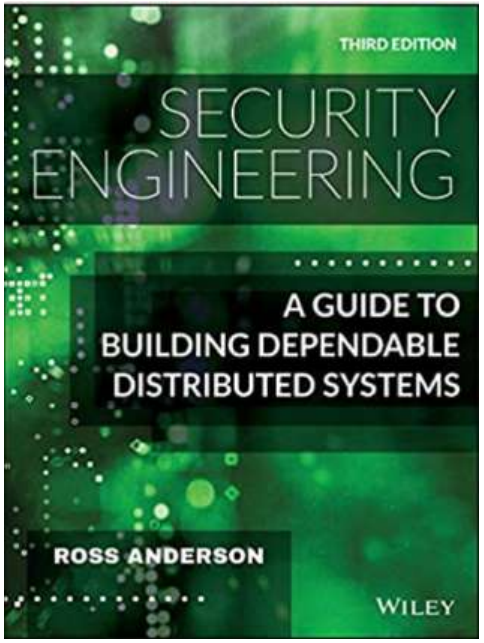
Detailed teaching goals

- Identify typical security vulnerabilities of web applications listed in OWASP top 10, such as SQL injection, XSS, and XSRF, by reviewing the source code and penetration testing. Students should also be able to fix the identified vulnerabilities;
- Explain typical cryptography concepts and algorithms related to web application, including, e.g., block cipher, stream cipher, digital signature, and SSL/TLS handshaking procedure;
- Apply threat modeling methods to analyze web application, learn to think like an attacker and build barriers;

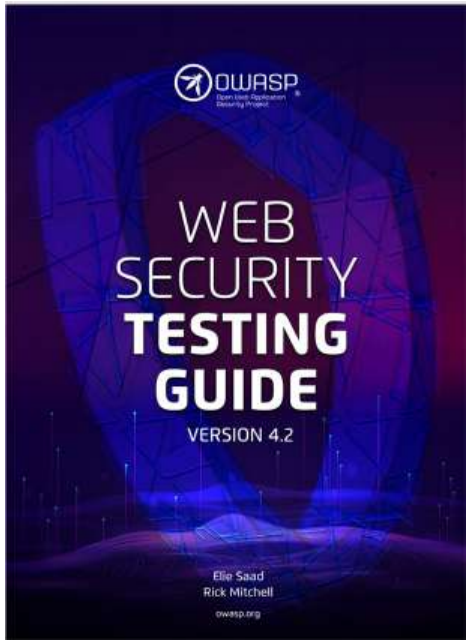
Detailed teaching goals (cont')

- Describe and compare software engineering practices and standards related to software security;
- Apply risk-based testing for development, figuring out why test? what to test? how to do it?;
- Explain key authentication and authorization concepts and methods, such as different authentication methods, multilevel security control, and role-based access control;
- Explain and apply principles of GDPR and data privacy, protecting personal spaces and avoiding hefty fines for your future tech company.

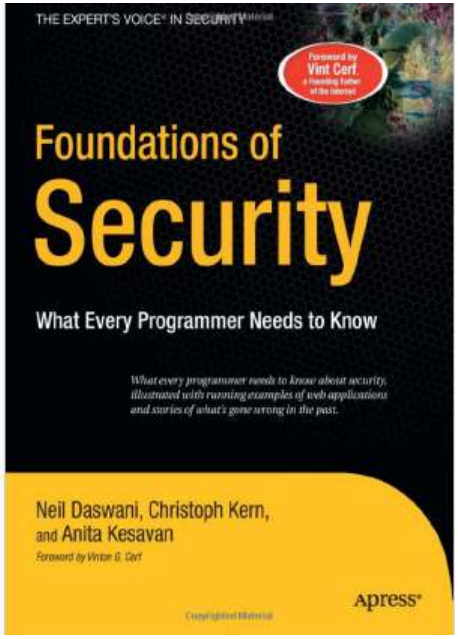
Curriculum



3rd Edition
http://www.cl.cam.ac.uk/~rja14/book.html
(Free!)



https://owasp.org/www-project-web-security-testing-guide/
(Version 4.2)
(The whole book)



Uploaded to Blackboard
Also available at NTNU lib online
(Selected chapters)

…and some other papers and web pages.
The list and the related papers and books are uploaded to blackboard.

NTNU

Home | Tournaments | Training | Courses | Assessments | Resources | Metrics | Administration | Help

Welcome to Secure Code Warrior!

Hone Your Skills

Practise finding, identifying and fixing real-world software security vulnerabilities.

Defend Your Code

Defeat the attackers targeting your client's systems and code to gain points. Rise through the levels to tackle more difficult security vulnerabilities in critical systems.

Demonstrate Your Expertise

Compete against other developers and see how you rate compared with other developers in your industry or region.

Continue

NTNU

SELECT THE LANGUAGE(S) YOU WANT TO TAKE YOUR COURSES WITH

- Ansible Basic
- Bash Basic
- C Basic
- C Embedded
- C# (.NET) Basic
- C# (.NET) Core
- C# (.NET) MVC
- C# (.NET) Web API
- C# (.NET) Web Forms
- C++ Basic
- C++ Embedded
- COBOL Basic
- CloudFormation Basic
- Docker Basic
- Java Android SDK
- Java Basic
- Java Enterprise Edition (JSF)
- Java Enterprise Edition (JSP)
- Java Enterprise Edition API
- Java Servlets
- Java Spring
- Java Spring API
- Java Struts
- JavaScript Angular.io (2+)
- JavaScript Basic
- JavaScript Node.js (Express)
- JavaScript Node.js API
- JavaScript React
- JavaScript React Native
- JavaScript Vue.js
- Kotlin Android SDK
- Kotlin Spring API
- Objective-C iOS SDK
- PHP Basic
- PHP Symfony
- PL/SQL Basic
- Perl Dancer2
- PowerShell Basic
- Pseudocode Basic
- Pseudocode Mobile
- Python API
- Python Basic
- Python Django
- Python Flask
- Ruby Rails
- Rust Basic
- Salesforce Apex
- Scala Play
- Swift iOS SDK
- Terraform Basic
- TypeScript Basic

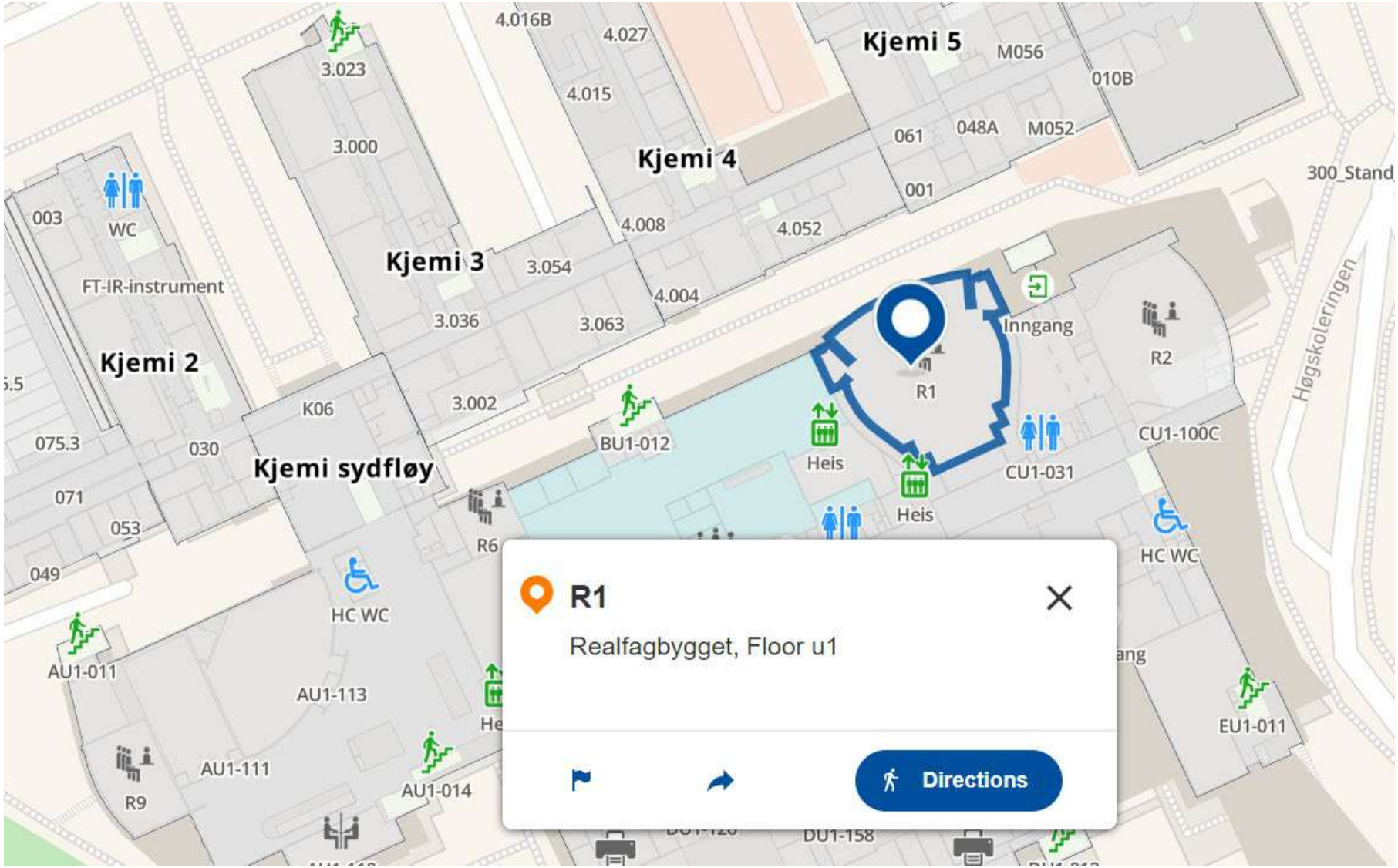
Lecture plan (tentative)

The lectures will be on Mondays from 10.15 to 12.00 at GL-RFB R1

Week	Date	Theme	Lecture
3	13.01	Course Introduction Security concepts and principles	Per Håkon Meland Jingyue Li
4	20.01	Web App. OWASP Top 10: part 1	Per Håkon Meland
5	27.01	Web App. OWASP Top 10: part 2	Per Håkon Meland
6	03.02	Cryptography introduction	Per Håkon Meland
7	10.02	Authorization and Multi-Level Security Authentication and Single sign-on Control hijacking attacks	Per Håkon Meland
8	17.02	Threat modeling and STRIDE	Per Håkon Meland
9	24.02	Risk Management during development	Per Håkon Meland
10	03.03	Winter vacation	

Lecture plan (tentative) (cont')

Week	Date	Theme	Lecture
11	10.03	Static Analysis and Tools for Security	Guest Lecture (Tosin Daniel Oyetoyan from HVL) (Digital, Teams link will be provided later)
		Pen Testing for Web Applications	Guest Lecture (Harrison Sand from Mnemonic) (Digital, Teams link will be provided later)
12	17.03	Secure coding with LLMs	Guest Lecture (Maxim Salnikov from Microsoft)
13	24.03	Privacy by Design	Guest Lecture (Knut Soelberg from Aboveit)
14	31.03	Microservice security	Jingyue Li
		Software supply chain security	
15	07.04	AI for Security	Guest Lecture (Nektaria Kaloudi from SINTEF)
		Social Engineering	Guest Lecture (Erlend Andreas Gjære from Secure Practice)
16	Easter		
17	Easter		
18	28.04	Secure Development Activities and lifecycles	Daniela Soares Cruzes (NTNU/Visma)
19	05.05	Course summary, Final Evaluation of the Course and Feedback to Professors, and more information on Exam.	Jingyue Li & Per Håkon Meland

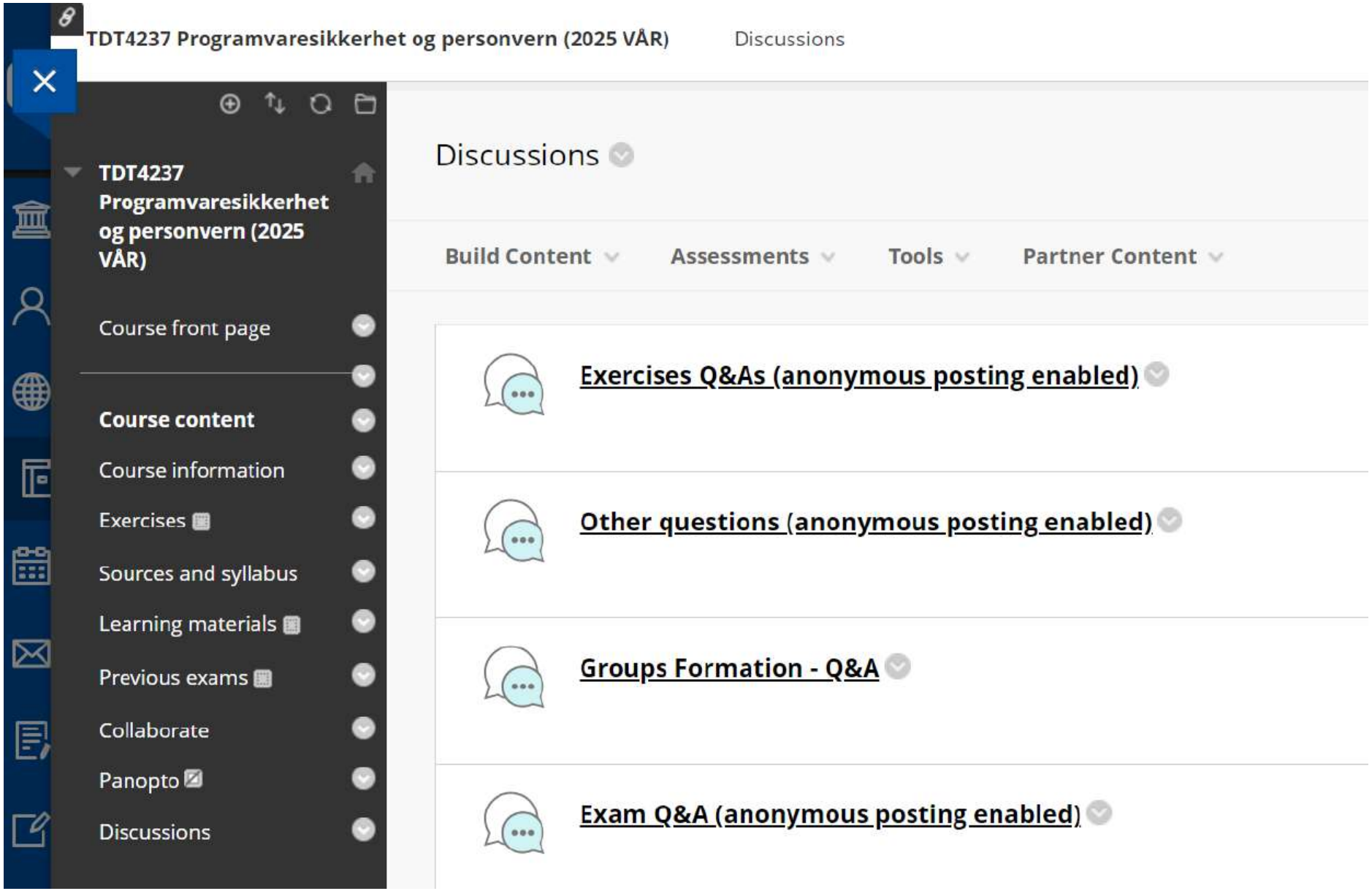

Kjemi 5
Kjemi 4
Kjemi 3
Kjemi 2
Kjemi sydfløy
4.016B
4.027
4.015
3.023
3.000
M056
010B
061
048A
M052
001
300_Stand
003
WC
FT-IR-instrument
4.008
4.052
3.054
4.004
3.036
3.063
3.002
K06
075.3
030
071
053
049
BU1-012
Heis
Heis
R1
Inngang
R2
CU1-031
CU1-100C
Høgskoleringen
R6
HC WC
HC WC
AU1-011
AU1-113
AU1-111
AU1-014
R9
EU1-011
DU1-158
R1
Realfagbygget, Floor u1
Directions

Evaluation and grading

- Exercises and written exam (5th of June)
- Four exercises count for 100 points, in which you **must have at least 70 points in total, more than 60% of the points for exercises 1 to 3,** to be eligible to take the exam.
- The distribution of the exercise grade is:
  - Exercise 1: 30 points (group exercise)
  - Exercise 2: 30 points (group exercise)
  - Exercise 3: 20 points (group exercise)
  - Exercise 4: 20 points (individual exercise) (If you score more than 80% on the Secure Code Warrior test set, you will earn all 20 points. Otherwise, you will receive 0 points. However, Secure Code Warrior allows you to retake the same test set multiple times.)

Exercises

- The exercise introduction lectures are on Thursdays, 10:15 - 12:00, GL-RFB R1.
- Weeks without exercise introduction lectures will have teaching assistants using the same room to answer questions
- We have a discussion forum in Blackboard so that TAs can help answer your questions there
- TA support email: tdt4237@idi.ntnu.no


TDT4237 Programvaresikkerhet og personvern (2025 VÅR)
Discussions
TDT4237 Programvaresikkerhet og personvern (2025 VÅR)
Course front page
Course content
Course information
Exercises
Sources and syllabus
Learning materials
Previous exams
Collaborate
Panopto
Discussions
Discussions
Build Content
Assessments
Tools
Partner Content
Exercises Q&As (anonymous posting enabled)
Other questions (anonymous posting enabled)
Groups Formation - Q&A
Exam Q&A (anonymous posting enabled)

Deadline for exercises

- All exercises have a deadline for delivery.
- This deadline may only be exceeded after agreement with the
  - Course responsible (Jingyue.li@ntnu.no)
  - TA (email: tdt4237@idi.ntnu.no)
- If no such agreement exists, we will deduct points on the grade for any obligatory exercise for each week it is delayed.

Exercise schedule (Tentative)

#	Weeks	Exercises schedule		
		Introduction lecture	Start	Deliverable and deadline
Exercise 1	4-9	23.01 10:15-12:00	23.01	The “vulnerability” report 26.02 at 23:59 (Wednesday), Week 9
Exercise 2	10-14	27.02 10:15-12:00	27.02	Vulnerability fixes 02.04 at 23:59 (Wednesday), Week 14
Exercise 3	14-18	03.04 10:15-12:00	03.04	Threat modeling and risk management framework 30.04 at 23:59 (Tuesday), Week 18
Exercise 4	4-18	23.01 10:15-12:00	23.01	Finish the assessment in Secure Code Warrior 30.04 at 23:59 (Tuesday), Week 18

Exercise groups

- 1-3 students in each group (recommended 2-3 students per group)
- Use Blackboard to form a group
- If you cannot find a group or encounter problems signing up for a group, please send an email to:

  Ahmed Yousif Mohamed Idries (ahmed.y.m.idries@ntnu.no)

- Deadline: 1st of February

NTNU

- Exercises
- Sources and syllabus
- Learning materials
- Previous exams
- Collaborate
- Panopto
- Discussions

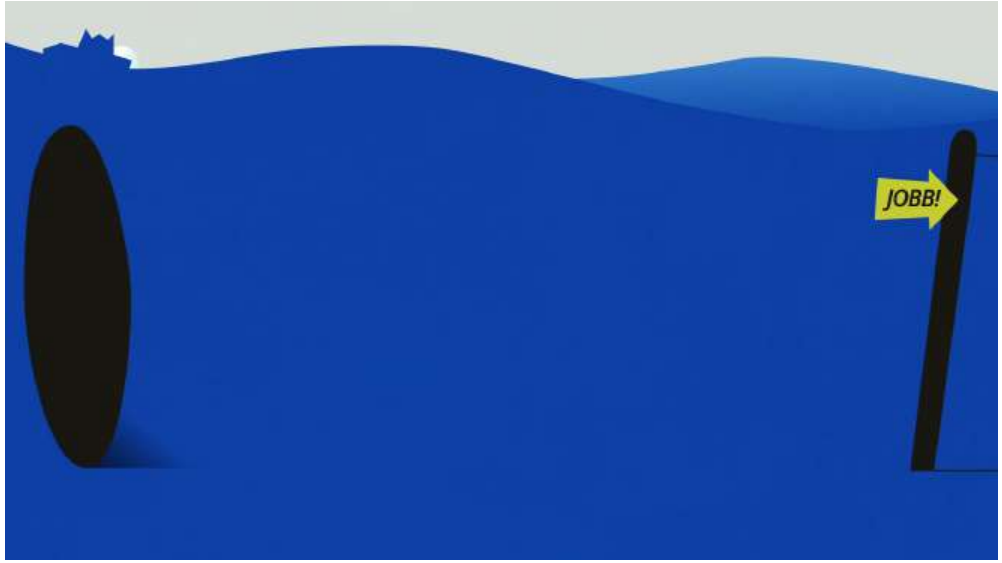
Course Management

Control Panel

- Content Collection
- Course Tools
- Evaluation
- Grade Center
- **Users and Groups**
- Groups
- Users

	NAME	GROUP SET	ENROLLED MEMBERS	SELF-ENROLL	AVAILABLE
	Group 1	Group	0	No	Yes
	Group 10	Group	0	No	Yes
	Group 11	Group	0	No	Yes
	Group 12	Group	0	No	Yes
	Group 13	Group	0	No	Yes
	Group 14	Group	0	No	Yes
	Group 15	Group	0	No	Yes
	Group 16	Group	0	No	Yes
	Group 17	Group	0	No	Yes
	Group 18	Group	0	No	Yes
	Group 19	Group	0	No	Yes
	Group 2	Group	0	No	Yes
	Group 20	Group	0	No	Yes

Evaluate and develop the course



Every time the course is held, we evaluate and make a plan for improvements

Evaluation and development ensure

- that the course is relevant
- that the learning activities are useful for reaching the learning goals
- that learning goals, learning activities and assessment activities

Feedback from the students is essential (and compulsory)

More information: i.ntnu.no/emne-evaluere

Reference group and survey

- A group of 2-3 students that have a special duty to provide feedback about the course during the semester
- We'll have 2-3 short lunch meetings where we can discuss content and form of lectures and assignments
- The group should be formed during the first 3 weeks, so please nominate yourself (or others)!
- Send an email to Jingyue.li@ntnu.no if you are interested by 1st of Feb.
- Digital surveys will be sent via Blackboard to all students. All students are highly encouraged to answer! It is important to the improvement of the course!

Warning

- Do not try any of the attacks discussed in this course on real production web sites!!!

- You can try penetration testing with
  - Your own application
  - Applications for teaching purpose, e.g.:
    - OWASP Juice shop https://owasp.org/www-project-juice-shop/
    - OWASP WebGoat https://github.com/WebGoat/WebGoat/
    - Damn Vulnerable Web Application (DVWA) https://dvwa.co.uk/)
  - SW call for help. Hackathons. Bug Bounties.
  - The exercise application of this course

About you

- We need to know a little more about you to adapt our teaching focus and exercises!