NTNU

Norwegian University of Science and Technology

TDT4237 Software Security and Data Privacy – Summary

5.5.2025

Per Håkon Meland & Jingyue Li

POLITICS

Trump is a Critical Vulnerability

The Trump administration nearly killed CVE, the system that names and tracks software vulnerabilities worldwide. When trust-based digital infrastructure becomes a political bargaining chip, our entire security framework is at risk.

Data and Politics
17 Apr 2025 — 3 min read

https://www.dataandpolitics.net/trump-is-a-critical-vulnerability/

NTNU

Course summary - 1

Description	Students should be able to	To read
Security concepts and principles	• Understand basic security goals • Understand typical attacks • Apply high-level security guidelines	• Slides: Security principles
OWASP Top 10	• Understand various web application related attacks, vulnerabilities and countermeasures. • Be able to find out vulnerabilities in Python code snippets and know how to fix them • Explain various password related concepts and authentication methods	• Slides: OWASP part 1, OWASP part 2 • OWASP web testing guide • Foundations of security book (Chapters 8, 9, 10) • Security engineering book (Chapter 3.4 and 3.5)

Course summary - 2

Description	Students should be able to	To read
Cryptography introduction	• Explain various cryptography methods presented in the slides • Explain public & private key concepts, digital signature, certificates, and SSL handshake • Apply the cryptography methods correctly	• Slides: Crypto intro • Security engineering book (Chapter 5)
Authorization and Multi-Level Security Authentication and Single sign-on Control hijacking attacks	• Explain discretionary, mandatory, role-based, and attribute-based access control policy and their pros and cons • Explain Biba and Bell-Lapdula models • Explain SSO, SAML 2.0, OAuth 2.0, OpenID • Explain buffer overflow attack and mitigation	• Slides: Authorization and stuff • Security engineering book: Chapter 6 (Access control) and Chapter 9 (Multi-level security) • Foundations of security book (Chapter 6: Buffer overflow)

NTNU

Course summary - 3

Description	Students should be able to	To read
Threat modeling and STRIDE	• Explain what threat modeling is about • Explain the difference between attacker-centric and software-centric threat models • Apply various threat modeling methods, e.g., misuse case, attack tree, bow-tie and data flow diagrams • Explain and apply STRIDE	• Slides: Threat modeling and STRIDE • The threat modeling manifesto: https://www.threatmodelingmanifesto.org/ (values and principles) • Security engineering book: Chapter 2: Who is the opponent, Chapter 27.3: Lessons from safety-critical systems

NTNU

Course summary - 4

Description	Students should be able to	To read
Risk management during development	• Explain the various steps typical of risk management (e.g., RMF) • Explain approaches on how to quantify risks • Apply RMF to analyze the security of a system • Explain the difference between good and bad security requirements • Define security requirements • Define a vulnerability score (CVSS)	• Slides: Risk Management during development • Security engineering book: • Chapter 8.6: The economics of security and dependability • Chapter 27.2: Risk management • Chapter 27.4: Prioritising protection goals • CVSS (Lecture slides and https://www.first.org/cvss/calculator/4.0)

NTNU

Course summary - 5

Description	Students should be able to	To read
Static analysis and tools for security	• Explain different static analysis approaches	• Slides: Static analysis tools for security (recorded)
Penetration Testing for Web application	• Explain practices and challenges of penetration testing in industry	• Slides: Introduction to real-world pentesting (recorded)

NTNU

Course summary - 6

Description	Students should be able to	To read
Secure coding with LLMs	• Explain what AI assistants can do • Explain advantages and disadvantages of AI assistants related to secure coding • Explain risks of AI code generation	• Slides

NTNU

Course summary - 7

Description	Students should be able to	To read
Privacy by Design	• Explain data privacy and GDPR basics • Explain how to process personal data • Explain how to comply with data privacy principles • Explain data privacy activities and roles during product development • Understand a Data Protection Impact Assessment (DPIA)	• Slides (lecture and workshop) • Security engineering: Chapter 26: Surveillance or privacy • (https://gdpr-info.eu/)

Course summary – 8

Description	Students should be able to	To read

Microservice security
 	
Software supply chain security
	• Explain microservice architecture
	• Explain microservice security challenges
	• Explain microservice security countermeasures
	• Explain security patterns for microservices
	
	• Explain software supply threats
	• Explain countermeasures
	• Explain Transparency technologies (e.g. SBOM)
		• Slides: Microservice security
		• Slides: Software supply chain security
		• Recommended papers:
		  • SoK: Security of Microservice Applications: A Practitioners' Perspective on Challenges and Best Practices https://dl.acm.org/doi/pdf/10.1145/3538969.3538986
		  • SoK: Analysis of Software Supply Chain Security by Establishing Secure Design Properties https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1177&context=ecepubs

NTNU

Course summary - 9

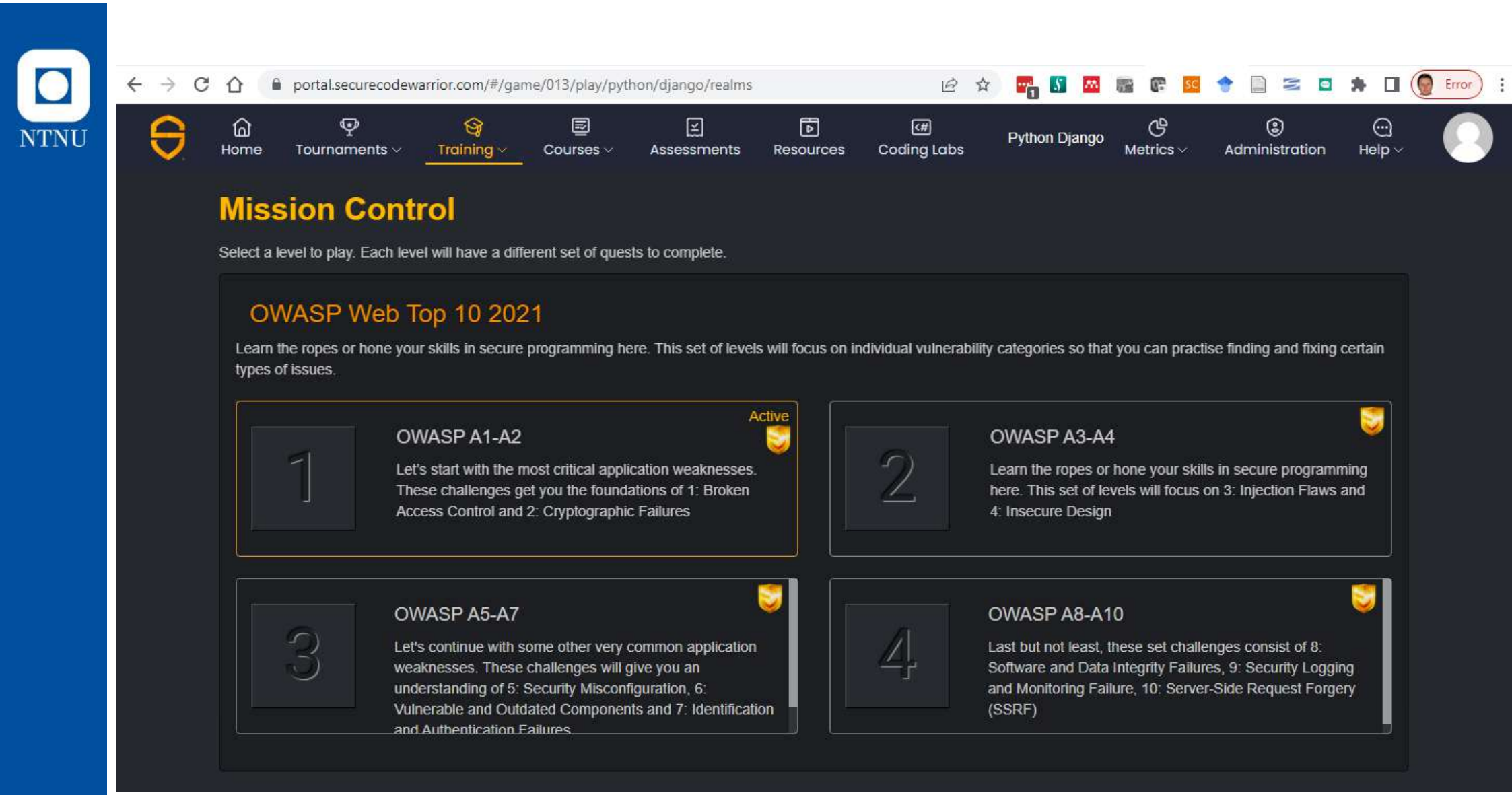
Description	Students should be able to	To read
AI for security Social engineering	• Explain how AI and cybersecurity relate (AI for cybersecurity, malicious AI, cybersecurity for AI). • Understand the ATLAS case study • Explain common techniques used for social engineering.	• Slides from Nektaria and Erlend Andreas • Recommended reading: Security Engineering, Chapter 3 Psychology and Usability, Chapter 25.3 AI/ML

NTNU

Course summary - 10

Description	Students should be able to	To read

Secure Development Activities and lifecycles	• Understand the 10 steps	• Slides from Daniela
		• Security engineering book: Chapter 27: Secure systems development
		• Recommended reading:
		  • Microsoft Security Development Lifecycle (SDL) : https://www.microsoft.com/en-us/securityengineering/sdl
		  • Microsoft security activities: https://www.microsoft.com/en-us/securityengineering/sdl/practices


portal.securecodewarrior.com/#/game/013/play/python/django/realms
Error
Home
Tournaments
Training
Courses
Assessments
Resources
Coding Labs
Python Django
Metrics
Administration
Help
Mission Control
Select a level to play. Each level will have a different set of quests to complete.
OWASP Web Top 10 2021
Learn the ropes or hone your skills in secure programming here. This set of levels will focus on individual vulnerability categories so that you can practise finding and fixing certain types of issues.
Active
1
OWASP A1-A2
Let's start with the most critical application weaknesses. These challenges get you the foundations of 1: Broken Access Control and 2: Cryptographic Failures
2
OWASP A3-A4
Learn the ropes or hone your skills in secure programming here. This set of levels will focus on 3: Injection Flaws and 4: Insecure Design
3
OWASP A5-A7
Let's continue with some other very common application weaknesses. These challenges will give you an understanding of 5: Security Misconfiguration, 6: Vulnerable and Outdated Components and 7: Identification and Authentication Failures
4
OWASP A8-A10
Last but not least, these set challenges consist of 8: Software and Data Integrity Failures, 9: Security Logging and Monitoring Failure, 10: Server-Side Request Forgery (SSRF)

Evaluation and grading

- Exercises and written exam

- 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)

NTNU

Structure of the exam

- A big case study (about 1/3)
  - ~1,5 hour
- Open-ended questions (about 1/3)
  - ~2 hours
- Close-ended questions (about 1/3)
  - ~30 minutes

Example open-ended question

- Explain the difference between Discretionary access control (DAC) and Mandatory access control (MAC). Give an example of each.

With DAC, the owner of a resource decides how it can be shared. The owner can choose to give read, write, or other access to other users. In contrast, MAC is a centralized access control model where access class is assigned to each subject and object.

DAC example: Linux file system, Google Docs, Sharepoint, Web applications
MAC example: Mac OS, Military systems, Trusted Computing Base

Another open-ended example

- Explain what a clickjacking attack is and how to defend against the clickjacking attack.

A clickjacking attack is when an attacker uses transparent layers to trick a user into clicking a button or link on the top-level page (which is transparent and malicious) when they intended to click on the button or link below the top-level page

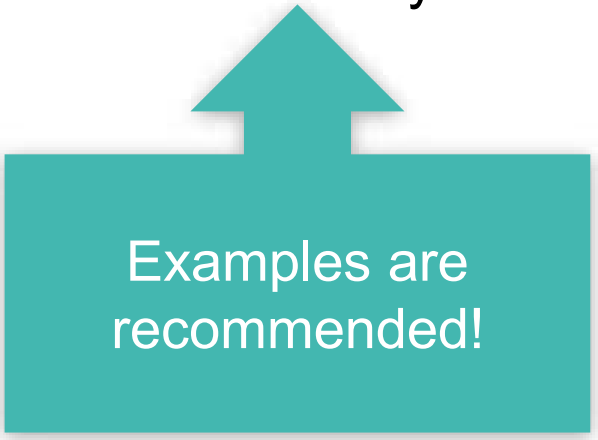
To prevent clickjacking, you can implement any of the following defenses:

- Preventing other web pages from framing the site you want to defend (e.g., Defending with X-Frame-Options Response Headers)
- Employing defensive code in the UI to ensure that the current frame is the most top-level window

Yet another open-ended…

- Explain the difference between privacy and confidentiality

Privacy means control of your own secrets, whereas *Confidentiality* is an obligation to protect someone else's secrets. **For instance**, your medical privacy is protected by your doctors' obligation of confidentiality.



And another…

```
http://www.exampleTDT4237.com/reset-
password?token=eyJhbGciOiJIUzI1NiIsInR5crheyKiwIwk.eyJzdWIiOiIxMjM0
NTY3ODkwIiwi
```

- 1) How can someone exploit this?
- 2) What can you do to protect such tokens? Name at least 2 ways.

Tokens in URLs can be easily exposed through browser history, server logs, network sniffing and other means. In this case, someone can obtain the token and use that to change the password of the user.

1. Use HTTPS: HTTPS encrypts the communication between the client and server, preventing attackers from intercepting and stealing the token.
2. Generate unique tokens: Generate a unique token for each user and each session, and ensure that each token can only be used once. This way, even if an attacker intercepts a token, they will not be able to reuse it in a subsequent request.
3. Limit token lifespan: Set an expiration time for each token, so that even if an attacker intercepts it, they will only be able to use it for a limited time period.

Example close-ended questions

Q&A

- Do we have to submit a drawing/sketch on the exam?
  - No
- Am I allowed to use a dictionary?
  - You are allowed to use a simple bilingual dictionary if the examination is held in a language other than your native tongue. **You do not have to apply for this.**
  - https://i.ntnu.no/wiki/-/wiki/English/Permitted+examination+aids
- Do we have to code during the exam?
  - Find vulnerabilities and fix
  - Note that copy-paste does not work well in Safeexambrowser (at least from what I remember).

Q&A

- Would it be possible to get a solution for the 2022 exam?
  - We only have a censor guide, which is not the same as a solutions. You should rather look for solutions in the curriculum (then you will learn more as well).
  - Inspera does not allow for censor guide export
- How long did old exams last for?
  - 4 hours
- Can Per Håkon be bribed?
  - No use, won't be doing any grading

Q&A

- Will you say the code questions in the exam will resemble the SCW or exercise 4 in difficulty level?
  - There are usually different levels of coding questions on the exam. None that are super hard since you have limited time and no help.
- Will I get a negative score for incorrect answers?
  - No, so better to guess than leave blank
- What happens if I fail the exam?
  - Welcome back after the summer

Tips

- Use the slides as the table of content to the reading material
- The exam will focus on applying the theories you have learned from lectures, reading the book chapters (++) and performing exercises
- The case studies and questions in previous years' exams can be used for practice
- Not all questions from previous years are relevant to this year, e.g., we did not cover mobile security this year
- There is a discussion channel in Blackboard for Q&A exam related questions