NTNU | Norwegian University of Science and Technology

WEB SECURITY LAB ASSIGNMENT

TTM4135

Tjerand Silde

02.03.2026

Quick Overview

- A lab project with **3 parts** and **one final report**
- Group work: **3–4 students** per group (self-enroll on Blackboard)
- TA support: in-person + online via Ed Forum (+ Zoom/Teams if needed)
- Counts for **20%** of the total course grade, **50%** of portfolio
- Lab handout, VM instructions, and report template available
- **Milestones must be demonstrated live** to a TA during assistance hours

Part I: Encrypted Email (PGP/GPG)

Goals:

- Generate a PGP keypair using GPG
- Upload your public key to `keys.openpgp.org`
- Retrieve keys of group members and the lab key
- Milestone 1: send a signed + encrypted file to TAs

Important details:

- Must send from your **NTNU student email**
- Public key must be uploaded, and not revoked, **before** submission
- TA verifies both your email and how you produced the message

Why this matters:

- Practical use of asymmetric cryptography
- Understanding the OpenPGP trust model (web of trust)
- Foundation for comparing PGP and X.509 (Parts I vs II)

Part II: Web Server + Certificate

Goals:

- Create and configure a VM using NTNU SkyHiGh
- Install and configure Apache
- Obtain and install a certificate from Let's Encrypt
- Milestone 2: Configure HTTPS and achieve an **A+** rating on SSL Labs

Important details:

- Follow Certbot instructions (Apache integration)
- Certbot may generate multiple config files – order matters
- **Do NOT enable the RSA ciphersuite** until Milestone 2 is completed

Why this matters:

- Real-world HTTPS configuration experience
- Understanding certificate authorities, chains, and the trust hierarchy
- Demonstrates practical TLS configuration concepts from lectures

Part III: Examining TLS Traffic

Goals:

- Capture TLS 1.2 traffic using Wireshark
- Inspect handshake fields: nonces, encrypted pre-master secret, etc.
- Extract and use the (pre-)master secret to decrypt TLS traffic
- Milestone 3: Use `TLS_RSA_WITH_AES_128_CBC_SHA`

Important details:

- Change operating system version for the VM
- Browser must disable TLS 1.3 and allow the RSA ciphersuite
- Wireshark can decrypt using key log files or extracted secrets
- Save all packet captures – **server access ends after report deadline**

Why this matters:

- See TLS internals “on the wire”
- Understand key derivation and security implications

What Do We Expect From You?

I + II: Follow instructions carefully; complete all milestones

III: More open-ended analysis and exploration

In practice:

- Keep documentation (screenshots, commands, configs) as you work
- All group members must contribute; notify TAs if someone is inactive
- Save logs, Wireshark captures, and config files before VM access ends
- Points awarded for both task completion and high-quality reporting

Assistance Hours Schedule

TA support available:

- In-person during scheduled lab hours:
  - Weeks 11, 12, 13
  - 09:00 – 17:00
  - Room Electro A175
- Online via Ed Forum; Zoom/Teams if needed
- **All milestones must be demonstrated live** to a TA

Important Dates / Suggested Schedule

- Week 1: Part I (PGP/GPG)
- Week 2: Part II (Apache + HTTPS)
- Week 3: Part III (TLS traffic analysis)

- **Milestones deadline: March 27th, 17:00**
- **Report deadline: April 24th 2026, End of Day**

Note: Server access is removed after the report deadline.

If You Need Help

Where to ask questions:

- Ed discussion forum (primary channel – monitored by TAs)
- TA office hours (in-person or online); reach out or stop by
- Allowed: online searching, discussing concepts with other groups

Not allowed:

- Sharing solutions or copying text, configs, or captures between groups
- Using another group's report or server configuration

Breakdown of Grade

- **50%** – Milestones (10% of total course grade)
- **50%** – Final report (10% of total course grade)

Milestones are graded on a pass/fail basis and must be **demonstrated live**.

The Lab Report

- Use the official LaTeX template (mandatory)
- Maximum length: **8 pages** (excluding title, references, appendices)
- Reproduce each question in full before your answer
- Use reputable academic or technical references

Evaluation:

- 10%: Format, grammar, clarity, citation style
- 90%: Technical accuracy, reasoning, completeness

Common Pitfalls (Avoid These!)

- Enabling the RSA ciphersuite **before** finishing SSL Labs (cannot get A+)
- Forgetting to disable directory listing (`Options -Indexes`)
- Not saving Wireshark captures or configs before VM access is removed
- Sending Milestone 1 email from the wrong address or wrong key
- Forgetting to switch the VM OS to different Ubuntu version for Part III
- Using unreliable online sources in the report

Milestones Summary

Milestone 1:

- Signed + encrypted group identity file emailed to lab
- Must come from your NTNU email
- Shown to a TA during assistance hours

Milestone 2:

- Achieve SSL Labs **A+**
- Show configuration and result to a TA
- Enable RSA ciphersuite only **after** this

Milestone 3:

- Demonstrate TLS 1.2 with `TLS_RSA_WITH_AES_128_CBC_SHA`
- Show Wireshark captures and analysis to a TA

Questions?