Fredrik Dietrichson

Penetration Tester & Security Researcher

Tønsberg, Norway · contact@fredrikd.com · +47 979 78 589 · linkedin.com/in/fredrik-j-dietrichson · github.com/FredrikEV

SUMMARY

Penetration tester and security researcher with prior experience as a Red Team operator. I perform web application, API, network, Active Directory, OT/ICS and IoT security assessments for clients across finance, energy, public sector, and transport. Alongside client work I do independent vulnerability research, with several published CVEs and security advisories in open-source software.

SECURITY RESEARCH & VULNERABILITY DISCLOSURE

SSRF via HTTP Redirect Bypass — Papra

CVE-2026-48051 · GHSA-5g86-85rp-f9hx · May 2026

Found and reported a Server-Side Request Forgery vulnerability in the webhook delivery system. SSRF protection validated registered webhook URLs but ignored redirect destinations, allowing an authenticated user to make the server reach internal addresses. Credited as reporter. Advisory →

Authorization Bypass: Payment Method Restriction — Sylius

CVE-2026-53638 · GHSA-6955-hrm5-c4qp · June 2026

Found and reported an authorization bypass in the shop account API of a PHP e-commerce platform. Authenticated customers could assign payment methods restricted by channel configuration, bypassing a check correctly enforced on the equivalent checkout endpoint. Credited as reporter. Advisory →

WeKan Security Hall of Fame

Responsible disclosure recognition

Listed in the WeKan Hall of Fame for responsibly reporting a Broken Function Level Authorization vulnerability (CVSS 8.1) affecting 48 REST endpoints in the open-source kanban platform. Recognition →

Additional advisories in draft / pending publication.

CORE SKILLS

OFFENSIVE – Penetration testing · Red teaming · Assumed-breach & internal network testing · Purple-team exercises · Phishing & email security testing · Physical security & lockpicking

APP & API – Web application & API security testing · Authentication & authorization testing · Vulnerability research & analysis · Source-code review

INFRA & DOMAINS – Active Directory & Windows · Cloud (Azure / Entra ID) · OT/ICS · IoT & hardware (firmware extraction, reverse engineering, vulnerability hunting)

OTHER – OSINT · Security awareness training & talks

EXPERIENCE

Penetration Tester & Security Expert — Semaphore Consulting Partners

August 2024 – Present · Oslo, Norway

Ethical hacking and security assessments for clients across finance, energy, public sector and transport as Penetration Tester, Test Lead and Project Lead.

- Web & API penetration testing across varied stacks (React, C#, Kotlin/Spring Boot, Blazor), including e-commerce and SaaS platforms.
- Internal network and Active Directory / Entra ID assessments, including assumed-breach scenarios.
- OT/ICS assessments of industrial and factory networks.
- Security talks and training — secure coding, how penetration testing works, and lockpicking workshops.

Red Team Operator — PwC Norway

August 2023 – August 2024 · Oslo, Norway (Associate → Senior Associate)

Part of the PwC Red Team (Cyber Threat Operations) as an ethical hacker.

- Penetration tests, red team engagements, and technical security consultancy for national and international clients.
- External and internal network testing, Active Directory, and OT/ICS assessments.

- Development of internal tooling.
- Purple-team detection exercises across the energy and public sectors.

Intern — Cyber Security and Privacy — PwC Norway

January 2023 – August 2023 · Oslo, Norway

Introduction to red team operations, IAM / PAM solutions and GRC.

EARLIER ROLES

Student Assistant — University of South-Eastern Norway · 2021–2022 — teaching assistant, introductory PHP programming.

Sales & Marketing Specialist — New Japan Trading AS · 2016–2020 — webshop manager; digital and physical marketing.

Manager — D&D Consult AS · 2014–2020 — family-owned consultancy; polymer-technology market research.

Trainee — Innovation Norway · 2013–2014 — Royal Norwegian Embassy, Tokyo.

Project Assistant — Re-Turn AS · 2007–2015 — nanotechnology, lab work, market research, production.

Food Server — Egon Restaurant Ullevål · 2012–2013 — part-time alongside studies.

Machine Operator — Jackon AS · 2011 — Styrofoam production, night shift.

COMMUNITY & SPEAKING

BSides Oslo — Lockpicking Village

Co-organizer & Instructor · 2024 & 2025

Co-organized and ran the Lockpicking Village, teaching physical-security and lockpicking fundamentals to attendees.

CERTIFICATIONS

- **Practical IoT Pentest Associate** — TCM Security. Hands-on IoT/hardware security: ROM flashers, logic analyzers, UART/SPI protocols, firmware extraction and reverse engineering, vulnerability identification and reporting.
- **Microsoft Certified: Azure Fundamentals (AZ-900)** — Microsoft. Foundational knowledge of cloud concepts, Azure management, services and tools.

RELEVANT COURSES

- **OffSec WEB-300 — Advanced Web Attacks and Exploitation** (2024). Prototype pollution, SSRF, .NET deserialization, RCE, blind SQL injection, source-code review, persistent XSS, session hijacking.
- **TCM Security** — Linux Privilege Escalation (2023), Windows Privilege Escalation (2023), Open Source Intelligence / OSINT (2023), Practical Ethical Hacking — The Complete Course.
- **The Complete JavaScript Course** (2022, Udemy); **React Front To Back** (2022, Udemy).

EDUCATION

- **BSc, Computer and Information Sciences** — University of South-Eastern Norway (2020–2023).
- **BA, Japanese Language and Literature** — University of Oslo (2007–2010).
- **Web development course** — NTNU (2018).
- **International marketing courses** — BI Norwegian Business School (2010–2012).

LANGUAGES

Norwegian (native) · English (professional working) · Japanese (limited working proficiency)

INTERESTS

Physical security and lockpicking · hardware tinkering and soldering projects · 3D printing · hands-on testing of new offensive tooling (e.g. Flipper Zero) · reading hardware-hacking literature · keeping current with AI/LLM security research

References available on request.