# Karol Nieckarz

Beilngries, Germany | +49 152 59616839 | karolnieckarz1111@gmail.com | karollol.vercel.app

## Profile

Security researcher with six years of hands-on experience in reverse engineering and software security. Started in 2020 with game software reverse engineering and paid cheat development, then shifted increasingly into vulnerability research during 2025, with recent work focused on Windows internals, Linux kernels, containers, and sandboxes. Found and documented CVE-2026-50416, a Windows 11 kernel information disclosure. Currently studying Computer Science and looking to move into full-time vulnerability research.

## Security Research

**CVE-2026-50416 - Windows 11 kernel information disclosure** 2026

- Discovered a kernel pointer disclosure in the user-mode mapping of the Windows 11 desktop heap.
- Confirmed that the pointer was readable from Low Integrity, AppContainer, and LPAC processes, allowing recovery of kernel desktop-heap and object addresses and weakening KASLR.
- Produced a reproducible proof of concept and technical write-up. Microsoft advisory | Write-up and proof of concept

**Java runner security assessment - THI assignment platform** 2026

- Assessed a Docker-based Java runner that intentionally executed untrusted student code and identified isolation failures exposing shell access, server source, system files, and other students' submissions.
- After the runner was hardened, reached the Node.js inspector from the Java execution context, exposing application source, environment variables, route modification, and command execution as the runner account.
- Ported CVE-2026-31431 from Python to Java FFM and demonstrated privilege escalation to container root. Tested about 20 Linux kernel CVEs and additional kernel attack surfaces against the hardened runner.

**Sensitive information disclosure - Technische Hochschule Ingolstadt (THI)** 2026

- Identified an information disclosure exposing student application material and internal HR documents.
- Reported the issue and retained the university's written acknowledgement. University acknowledgement

**Independent vulnerability disclosure programs** mid 2025-present

- Reported vulnerabilities directly to vendors, including cases still awaiting triage or fixes.

**Game cheat development and loader cracking** 2020-mid 2025

- Worked on several paid game cheat projects, including independently developing and maintaining one of my own.
- Cracked licensing and anti-tamper in third-party cheat loaders and kept cheats working after game updates.

## Education

**B.Sc. Computer Science - Technische Hochschule Ingolstadt** 2025-present

Currently enrolled. Looking to transition into full-time vulnerability research.

**Fachhochschulreife (Fachabitur) - Maximilian-Kolbe-Schule, State Vocational Upper Secondary School (Fachoberschule), Neumarkt** 2022-2024

International Business track, focused on international business administration and economics.

## Languages

| | | | |
|---|---|---|---|
| German | Native proficiency | Polish | Native proficiency |
| English | Fluent | French | B1 |

## Additional Information

German and Polish citizenship. Unrestricted work authorization across the European Union. Available for remote, hybrid, on-site, and relocation-based positions.