Kaan Dedeoğlu

contact@kaandedeoglu.com

kaandedeoglu.com | linkedin.com/in/kaandedeoglu | github.com/dedeoglukaan | hackerone.com/dedephus

Profile

Computer Engineering graduate working full time on offensive application security, focused on authorization and access-control flaws in large open-source products. Seven findings have been independently triaged by the vendors' security teams — in large open-source products — including two Criticals (CVSS 9.6 and 9.3) that each take an ordinary authenticated user to full administrative control. Also builds the tooling behind the work: an autonomous research platform that carries a target from reconnaissance to a validated, reproducible report.

Education

BSc in Computer Engineering — Sep. 2020 – Jun. 2025
Eskişehir Technical University, Turkey — Language of Instruction: English

Relevant Experience

Independent Security Researcher — Jul. 2025 – Present
HackerOne – `@dedephus` — Remote

- **Seven findings independently triaged by vendor security teams** — two Critical (CVSS 9.6 and 9.3), four High (8.5, 8.1, 7.7, 7.6) and one Medium (5.3), all in large open-source products. The two Criticals each take an ordinary authenticated user to full administrative control; the Highs are authorization gaps around privileged operations, and the Medium is an authenticated full-read SSRF.
- **Where the leads came from:** a call-site census of an operation that is guarded elsewhere in the same codebase, and what a release line newly ships enabled — not a pattern any single grep would surface. Each authorization finding was armoured with a negative control: the same account refused on the neighbouring operation and allowed on this one.
- Program names and technical detail stay out of public documents until the vendor discloses the report. None of my findings are disclosed, so none of them are described here. The detailed version of this section is available on request.
- Submitted **65 reports across 12 bug bounty programs** since April 2026; every report ships with a reproducible PoC and a severity argued in CVSS terms.
- **How I work:** read the open-source codebase for authorization gaps and unguarded internal clients, then prove each candidate with a working end-to-end PoC on a local deployment. I do not report anything I cannot prove.
- Ramped up full time from July 2025 — web application security fundamentals, systematic study of disclosed HackerOne reports and public vulnerability research, and a repeatable testing methodology — before the first submission in April 2026.

IT Systems Intern — Oct. 2024 – Dec. 2024
Eskişehir Technical University – IT Department — Eskişehir, Turkey

- Deployed a production-like DSpace 8 backend on Ubuntu 22.04 for the university digital library, integrating Java 17, PostgreSQL, Apache Solr and Spring Boot services.
- Hardened the database layer: dedicated PostgreSQL role, connection security through `pg_hba.conf`, and the `pgcrypto` extension for UUID support.
- Configured HTTPS through an Apache reverse proxy with a Let's Encrypt certificate, plus cron automation for daily indexing, media filtering and checksum verification.

IT Systems Intern — Jul. 2024 – Aug. 2024
Creentech — Istanbul, Turkey

- Administered Debian-based Linux systems: user management, permissions, sudo policy, systemd services and cron-based automation, scripted in Bash.
- Assisted the network team with FortiGate firewall policies, VLAN setup, static routing and web filtering; worked alongside production monitoring in Grafana and Zabbix.

Selected Projects

the-grind – Autonomous Security Research Platform Apr. 2026 – Present
Python, TypeScript, Bash, Caido, Docker – private repository, walkthrough on request

- Designed the platform to run the full bug bounty workflow as one continuous agent loop rather than a scanner: reconnaissance, attack-surface mapping, exploitation, PoC generation, adversarial validation and report drafting. Roughly **1,560 commits** over four months.
- **Encoded 19 vulnerability classes as 27 executable methodology modules** (∼11,000 lines): broken access control and IDOR, SSRF, SQL and NoSQL injection, XSS, authentication bypass, OAuth/SAML, race conditions, RCE, SSTI, XXE, path traversal, cache poisoning, GraphQL, WebSocket, cloud and CI/CD misconfiguration, and LLM/AI application security.
- **Wrote `ct`, a context-frugal interface to the Caido proxy.** The stock client pushed full request and response bodies into the agent's context window and exhausted it within a few requests; `ct` replaces that with filtered traffic reads, regex search inside stored responses, batch variant testing that surfaces only deviating responses, one-shot authorization verdicts, and field-level A/B diffing.
- **Built `brutal-triager`, a three-pass adversarial validator** that must fail to refute a finding before it can be reported: hostile code review with a decisive empirical test, a fresh PoC reproduction pass that hunts fabricated evidence, and severity benchmarking against **14,617 disclosed HackerOne reports** plus live CVE research.
- **Enforced a deliberately selective promotion gate:** a lead becomes a reportable finding only with an unconditional end-to-end PoC, a concrete victim and concrete damage, and a final exploitation step an external researcher can actually execute — which is what keeps speculative work out of submissions.
- Integrated the supporting toolchain: every request routed through one auditable proxy, interactsh for blind and out-of-band confirmation, Playwright for browser-verified client-side findings, a custom SSRF scanner and JavaScript bundle secret mining. Each session appends its dead ends to a persistent learnings file that the next one reloads.

OSTEODEEP – AI Bone Health Assessment Jan. 2024 – Jun. 2025
Graduation Project on knee X-rays – IEEE published, TÜBİTAK 2209-A funded

- **Published in an IEEE conference:** IEEE Xplore | open-access PDF.
- Built the end-to-end ML pipeline over 1,947 knee X-rays: CLAHE contrast enhancement, augmentation constrained to preserve anatomical integrity, parallel deep-feature extraction from EfficientNetB2 and VGG-19, PCA reduction, and an SVM (RBF) + XGBoost stacking ensemble.
- Reached **90.10% accuracy** and **0.96 macro ROC AUC** on 3-class classification, with 91.20% recall on the clinically hardest osteopenia class, outperforming standalone CNN baselines.

Training & Certifications

Garanti BBVA Technology Security Academy Oct. 2023 – Feb. 2024
Enterprise Technology & Cybersecurity Program with Patika.dev

- Reached the final stage as **one of 20 participants out of 3,600 applicants**: 450 were admitted, and successive technical evaluations narrowed the field to 20.
- Covered Linux internals, network protocols and enterprise application security, with threat modeling and secure architecture review applied to real-world systems.

Certifications: Wiz Bug Bounty Masterclass (Apr. 2026) | Web App Security & Bug Bounty, Udemy (Jul. 2025) | Cisco NDG Linux Unhatched (Feb. 2025) | Cisco Introduction to Cybersecurity (Jan. 2025)

Technical Skills

Security: Web application security, OWASP Top 10, broken access control (IDOR / BOLA / BFLA), SSRF, injection (SQL, NoSQL, template), authentication and OAuth/SAML flaws, race conditions, source-code review, threat modeling, CVSS scoring
Security Tools: Caido, Burp Suite, ffuf, nuclei, subfinder, httpx, katana, TruffleHog, interactsh, Playwright
Systems: Linux administration, networking, Docker, Git, PostgreSQL, Elasticsearch/Kibana, reverse proxies, CI/CD
Programming: Python, Java (Spring Boot), TypeScript, Bash, SQL
Spoken Languages: Turkish (native), English (professional working proficiency)