Edoardo Ottavianelli

edoardottt.com

edoardott@gmail.com
github.com/edoardottt
linkedin.com/in/edoardoottavianelli

Experience

- **Hacktive Security** — Full Remote
  `Senior Security Consultant` — *March 2024 - Present*
  - Conducted and led penetration tests, code reviews and red team activities for many companies, identified high-severity vulnerabilities in web applications, network infrastructures, APIs and desktop clients.
  - Delivered high-quality detailed reports outlining vulnerabilities, potential impact, and actionable remediation steps, enhancing clients' security posture.
  - Performed advanced research initiatives and contributed to the development of security tools.

- **Sapienza University** — Full Remote
  `Security Researcher` — *June 2023 - Feb. 2024*

  Received a research grant from the DIET Department to study security in programmable networks, designed and implemented a log-analysis framework for anomaly detection, identified vulnerabilities and innovative attack techniques in Java-based network applications.

- **Consortium for the Research in Automation and Telecommunication (CRAT)** — Full Remote
  `Network Security Researcher` — *Sep. 2023 - Feb. 2024*

  For the European Space Agency (ESA) PANTSAT project, I analyzed system scenarios, defined technical requirements for a satellite communication protocol, and evaluated network protocols for compatibility and security.

- **Bugcrowd** — Full Remote
  `Independent Security Researcher` — *Nov. 2021 - Nov. 2023*

  Identified and reported 300+ security vulnerabilities in high-profile companies and U.S. Government offices, with a specialization in web and network applications. Recognized for outstanding work by reaching second place in the CISA 2021 Competition and third place overall in the Valid Submissions Since Launch Researcher Leaderboard.

- **SeismoCloud** — Rome, Italy
  `Software Developer` — *Mar. 2020 - Oct. 2020*

  Designed, implemented and secured an user-friendly End User Development system (Docker, NodeJS) able to configure and control networks of IoT devices and online services. Contributed to the REST API system (Golang).

Technical Skills

Application and Network Security, Software Development and Security Code Reviews. Extensive knowledge of networks and networking protocols (TCP/IP, Routing, HTTP, DNS, IPS, IDS, WAF, Firewall, Proxy).

- **Languages**: Python, Golang, Bash, Java, JavaScript, SQL, and other C-family languages.
- **Technologies**: Linux, Windows, Active Directory, Git, GitHub Actions, BurpSuite, SAST and DAST, Metasploit, Nessus, Nuclei and other vulnerability scanners, Docker, Relational Databases, VSCode, Wireshark, Semgrep, Postman, ClickUp.

Awards - Certifications - Licenses

- **OSCP by OffSec** — Jun. 2026
  `Offensive Security Certified Professional (OSCP Certificate link)`

- **CRTP by AlteredSecurity** Feb. 2026
  Certified Red Team Professional (CRTP Certificate link)
- **SecAI+ by CompTIA** Oct. 2025
  Certified CompTIA SecurityAI+ (SecAI+ Certificate link)
- **Security+ by CompTIA** Feb. 2024
  Certified CompTIA Security+ (Sec+ Certificate link)
- **ICCA by INE** July 2023
  Certified Cloud Associate (ICCA Certificate link)
- **eWPT by eLearnSecurity (INE)** June 2023
  Certified Web Application Penetration Tester (eWPT Certificate link)
- **eJPT by eLearnSecurity (INE)** Sept. 2022
  Certified Junior Penetration Tester (eJPT Certificate link)

Education

- **Sapienza University** Rome, Italy
  Master's Degree in Cybersecurity; 109/110 *Oct. 2020 – May 2023*
- **Sapienza University** Rome, Italy
  Bachelor's Degree in Computer Science; 103/110 *Sept. 2016 – Oct. 2020*
- **Fabio Besta Scientific High School** Orte, Italy
  Scientific High School Diploma; 71/100 *Sept. 2011 – July 2016*

Open Source Projects

Open-sourcing since 2018, reached 20k+ stars on GitHub: github.com/edoardottt

Security Advisories

Discovered, reported and responsibly disclosed many undetected vulnerabilities in popular products (mainly with code reviews, but also manual testing, static and dynamic analysis): edoardottt.com/cve