Edoardo Ottavianelli

edoardottt.com

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

Experience

- **Hacktive Security** Full Remote
  `Offensive Security Analyst` *Mar. 2024 - Present*
  - Conducted penetration tests for many famous firms, identified high-severity vulnerabilities in web applications, network infrastructures, and APIs.
  - Delivered detailed, high-quality reports outlining vulnerabilities, potential impacts, and actionable remediation steps, enhancing clients' security posture.
  - Executed on-site internal network penetration tests thorough security assessments compliant with industry standards.
  - Performed advanced Research initiatives and contributed to the development of security tools and techniques.

- **Sapienza University** Full Remote
  `Security Researcher` *June 2023 - Feb. 2024*
  Received a research grant at DIET Department to continue the studies on security in programmable networks.
  - Designed, implemented and tested an innovative framework for anomalies and attacks detection in network environments through log analysis using Python and Bash.
  - Discovered vulnerabilities (CVEs) and new attack methodologies through testing, static and dynamic analysis in network applications written in Java.

- **Consortium for the Research in Automation and Telecommunication (CRAT)** Full Remote
  `Network Security Researcher` *Sep. 2023 - Feb. 2024*
  PANTSAT, a project commissioned by the European Space Agency (ESA):
  - Studied and defined system scenarios, technical requirements and specifications for a new communication protocol for satellite networks.
  - Reviewed designs and implementations of various state-of-the-art network protocols for compatibility and security standards

- **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 at the CISA 2021 Competition and third place overall on Researcher Leaderboard Valid Submissions Since Launch.

- **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, Go, Bash, Java, C, JavaScript, SQL, HTML and other C-family languages.
- **Technologies**: Linux (Local, VM and on Cloud), Windows, Git, GitHub Actions, ClickUp, BurpSuite, SAST and DAST, Metasploit, Nessus, Nuclei and other vulnerability scanners, Docker, Relational Databases, VSCode, Wireshark, Postman.

Education

- **Sapienza University** Rome, Italy
  `Master's Degree in Cybersecurity; 109/110` *Oct. 2020 – May 2023*
  Dissertation: ”Proposal and Investigation of a framework for Cross App Poisoning attacks detection in Software Defined Networks.”
- **Sapienza University** Rome, Italy
  `Bachelor's Degree in Computer Science; 103/110` *Sept. 2016 – Oct. 2020*
  Dissertation: ”Design and development of the End User Development system in SeismoCloud”.
- **Fabio Besta Scientific High School** Orte, Italy
  `Scientific High School Diploma; 71/100` *Sept. 2011 – July 2016*

Awards - Certifications - Licenses

- **CASA by APISec** Aug. 2024
  `Certified API Security Analyst (CASA 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)`

Open Source Projects

Open-sourcing since 2018, reached 13k+ stars on GitHub: github.com/edoardottt

- **scilla**: Information Gathering tool - DNS / Subdomains / Ports / Directories enumeration
- **cariddi**: Take a list of domains, crawl urls and scan for endpoints, secrets, api keys, file extensions, tokens and more
- **csprecon**: Discover new target domains using Content Security Policy.
- **lit-bb-hack-tools**: Little Bug Bounty and Hacking Tools.

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

Languages

- **Italian**: Native speaker.
- **English**: Professional Working Proficiency.