Edoardo Ottavianelli

edoardoottavianelli.it

Email : edoardott@gmail.com
github.com/edoardott
linkedin.com/in/edoardoottavianelli

EXPERIENCE

- **Bugcrowd** — Full Remote
  Security Researcher — *Nov. 2021 - Present*
  - **bugcrowd.com/edoardott**: Discovered over 200 security vulnerabilities in high-profile companies and U.S. Government services, with a focus on web applications. Winner of the CISA Raffle.

- **SeismoCloud** — Rome, Italy
  Software Developer — *Mar. 2020 - Oct. 2020*
  - **SeismoCloud EUD system**: Created user-friendly End User Development system (Docker, NodeJS) to enable non-technical users to automate actions such as sending Telegram/Email messages, and posting tweets through IoT devices data.
  - **API development**: Resolved issues with the SeismoCloud Rest API (Golang) system providing information on Sensors signalings, devices and users' data, as well as associated statistics.

EDUCATION

- **Sapienza University** — Rome, Italy
  Master Degree in Cybersecurity — *Oct. 2020 – May 2023*

- **Sapienza University** — Rome, Italy
  Bachelor 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*

TECHNICAL SKILLS

- Software Development and Security, Web application and Network Penetration Testing

- **Languages**: Python, Go, Bash, Java, HTML, SQL, Javascript.

- **Technologies**: Linux, Windows, VS Code, Git, BurpSuite, Docker, Postman.

Moreover, advanced knowledge of networks and networking protocols.

PERSONAL PROJECTS

- **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.
- **Other 40+ repositories on GitHub**: github.com/edoardott

AWARDS - CERTIFICATIONS - LICENSES

- **eJPT by eLearnSecurity**
  Certified Junior Penetration Tester
  https://elearnsecurity.com/product/ejpt-certification/

- **Class B European Driving License**

Security Advisories

- CVE-2023-27070 A stored cross-site scripting (XSS) vulnerability in TotalJS OpenPlatform commit b80b09d allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the platform name field.

- CVE-2023-27069 A stored cross-site scripting (XSS) vulnerability in TotalJS OpenPlatform commit b80b09d allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the account name field.

- CVE-2023-24769 Changedetection.io before v0.40.1.1 was discovered to contain a stored XSS vulnerability in the main page. This vulnerability allows attackers to execute arbitrary Javascript code via a crafted payload injected into the URL parameter under the "Add a new change detection watch" function.

- CVE-2023-24279 A XSS vulnerability in Open Networking Foundation ONOS from version v1.9.0 to v2.7.0 allows attackers to execute arbitrary Javascript code via a crafted payload injected into the url parameter of the API documentation dashboard.

- CVE-2022-44019 In Total.js 4 before 0e5ace7, /api/common/ping can achieve remote command execution via shell metacharacters in the host parameter.

- CVE-2022-41392 A cross-site scripting (XSS) vulnerability in TotalJS commit 8c2c8909 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Website name text field under Main Settings.

Languages

- **Italian**: Native speaking.

- **English**: Middle-level speaking.

Scientific Papers

- **Simplify Node-RED for End User Development in SeismoCloud**
  Enrico Bassetti, Edoardo Ottavianelli, Emanuele Panizzi
  https://arxiv.org/pdf/2012.05637.pdf