

# Edoardo Ottavianelli

[edoardoottavianelli.it](mailto:edoardoottavianelli.it)

[edoardott@gmail.com](mailto:edoardott@gmail.com)

[github.com/edoardottt](https://github.com/edoardottt)

[linkedin.com/in/edoardoottavianelli](https://linkedin.com/in/edoardoottavianelli)

## EXPERIENCE

---

- **Bugcrowd** Full Remote  
*Security Researcher* Nov. 2021 - Present
  - **bugcrowd.com/edoardottt**: Successfully identified and reported 200+ security vulnerabilities in high-profile companies and U.S. Government offices, with a specialization in web applications.
  - **CISA Competition**: Recognized for outstanding work by reaching second place at the Cybersecurity and Infrastructure Security Agency (CISA) 2021 Competition.
- **SeismoCloud** Rome, Italy  
*Software Developer* Mar. 2020 - Oct. 2020
  - **SeismoCloud EUD system**: Designed, implemented and secured an user-friendly End User Development system (Docker, NodeJS) to enable non-technical users to configure and control networks of IoT devices and online services (e.g. automate actions such as sending Telegram/Email messages and posting tweets through IoT devices data).
  - **API development**: Resolved issues in the SeismoCloud REST API system (Golang) providing information on Sensors signalings, devices and users' data, as well as associated statistics.

## 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

## TECHNICAL SKILLS

---

Software Development, Application and Network Security. Advanced knowledge of networks and networking protocols.

- **Languages**: Python, Go, Bash, Java, C, Javascript, SQL, HTML. Sometimes other C-family languages.
- **Technologies**: Linux (Local, VM and VPS), Windows, Git, GitHub Actions, BurpSuite, SAST and DAST, Metasploit and other security scanners, Docker, MySQL, PostgreSQL, MongoDB, SQLite, VSCode, Wireshark, Postman.

## PERSONAL PROJECTS

---

Open-sourcing since 2018, reached 8k+ stars on GitHub: [github.com/edoardottt](https://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.

## AWARDS - CERTIFICATIONS - LICENSES

---

- **eJPT by eLearnSecurity**  
Certified Junior Penetration Tester ([eJPT Certificate link](#))
- **Class B European Driving License**

## SECURITY ADVISORIES

---

Discovered, reported and responsibly disclosed many undetected vulnerabilities in popular products:

- CVE-2023-30097 A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the private task field.
- CVE-2023-30096 A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the user information field.
- CVE-2023-30095 A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the channel description field.
- CVE-2023-30094 A stored cross-site scripting (XSS) vulnerability in TotalJS Flow v10 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the platform name field in the settings module.
- CVE-2023-30093 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-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 PUBLICATIONS

---

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