

Edoardo Ottavianelli

edoardoottavianelli.it

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

ISTRUZIONE

- **Università La Sapienza** Roma, Italia
Laurea Magistrale in Cybersecurity Ott. 2020 – In corso
- **Università La Sapienza** Roma, Italia
Laurea Triennale in Informatica; 103/110 Set. 2016 – Ott. 2020
- **Liceo Scientifico Fabio Besta** Orte, Italia
Diploma Liceo Scientifico; 71/100 Set. 2011 – Lug. 2016

ESPERIENZA

- **Bugcrowd** Remoto
Security Researcher Nov. 2021 - In corso
 - **bugcrowd.com/edoardottt**: Trovate più di 150 vulnerabilità in società di alto livello e servizi del governo americano. Maggiormente interessato ad applicazioni Web. Uno dei vincitori del CISA Raffle.
- **SeismoCloud** Roma, Italia
Sviluppatore Software Mar. 2020 - Ott. 2020
 - **Sistema EUD SeismoCloud**: Ho sviluppato il sistema di End User Development di SeismoCloud usando Docker, Javascript e NodeRED. Anche gli utenti non tecnicamente avanzati possono creare azioni programmate usando i dati dei loro dispositivi, come inviare messaggi via Telegram/Email o postare tweet automatici quando si verificano degli eventi determinati dagli utenti.
 - **Sviluppo API**: Ho risolto alcuni problemi nel sistema API Rest di SeismoCloud. Queste API restituiscono informazioni riguardo le segnalazioni dei sensori, i dati generali dei dispositivi e degli utenti e varie statistiche.

COMPETENZE TECNICHE

- Penetration Testing di applicazioni Web e di Reti
- **Linguaggi**: Python, Go, Bash, HTML, SQL, Javascript.
- **Tecnologie**: Linux, Windows, VS Code, Git, BurpSuite, Docker, Postman.

Inoltre, elevata conoscenza delle reti e dei protocolli di rete.

PROGETTI PERSONALI

- **scilla**: Information Gathering tool - DNS / Subdomains / Directories / Ports enumeration
- **cariddi**: Take a list of domains, crawl urls and scan for endpoints, secrets, api keys, file extensions, tokens and more...
- **lit-bb-hack-tools**: Little Bug Bounty and Hacking Tools.
- **twitterbot2**: Like and retweet your tweets, or search tweets by topic. It stores and serves data with a Flask webapp.
- **Altre 40+ repository su GitHub**: github.com/edoardottt

PREMI - CERTIFICAZIONI - LICENZE

- **eJPT by eLearnSecurity**
Certified Junior Penetration Tester
<https://elearnsecurity.com/product/ejpt-certification/>
- **Patente di guida europea B**

SECURITY ADVISORIES

- 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.

LINGUE

- **Italiano:** Madrelingua.
- **Inglese:** Livello medio.

PUBBLICAZIONI SCIENTIFICHE

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