Antonio Vitale

vitaleleinfo@gmail.com github.com/vitalelele linkedin.com/in/antonio-vitale-sd/ antoniovitale.it

Professional Goals

Offensive Security Engineer and Penetration Tester with a focus on web and network security. Driven by the ”break-to-secure” mindset, I specialize in vulnerability research and exploitation to provide a realistic assessment of corporate risks. My core expertise lies in Python-based security automation, Linux hardening, and ethical hacking. I am eager to join a Red Team or Offensive Security unit to leverage my technical skills in uncovering critical flaws and strengthening infrastructure resilience.

Education

MSc in Cybersecurity (LM-66)
University of Milan Sep 2024 – Jul 2026 (expected)
Current GPA: 29.7/30.

BSc in Computer Science and Software Technologies (L-31)
University of Bari Aldo Moro Sep 2021 – Jul 2024
Graduated with full marks and honors (110/110 cum laude)
Best Bachelor's Thesis Awards in Cybersecurity 2024
Final GPA: 28.6/30

High School Diploma — IT and Telecommunications
ITSET Manlio Capitolo Sep 2016 – Jul 2021
Graduated with full marks and honors (100/100 cum laude)

Certifications

eJPT (Junior Penetration Tester)
INE Nov 2025
Credential: 23d46be9-f2f3-4e95-a9ad-54f90a8ed35b

Fundamentals of Digital Marketing
Google Oct 2025

Technical Skills

- **Offensive Security:** Pentesting (Web & Network), Metasploit, Nmap, Burp Suite, Wireshark, Kali Linux.
- **Security Automation:** Python (Expert), Bash scripting, custom exploit development, automated reporting.
- **Systems & Security:** Linux Hardening, ISO/IEC 27001/27002, OWASP (Web/API), ACL.
- **Software Development:** Python, Java, C/C++, Scikit-learn (Machine Learning for security).
- **Tools & Backend:** SQL, Docker, Git, Firebase, RESTful API design, Agile (Scrum).
- **Others:** Smart Contract Auditing fundamentals, Fuzzing tools, Solidity.

Projects

nmap2report — Pentest Reporting Automation *github.com/vitalelele/nmap2report*
Developed a high-performance Python tool to automate security reporting from Nmap XML output. It enriches scan results with CVE/CVSS data, severity ratings, and risk metrics, exporting professional PDF or Markdown reports for both triage and corporate delivery.
Technologies: Python, Jinja2, XML Parsing, Pandoc.

WordlistRefinery — Credential Auditing Engine *github.com/vitalelele/WordlistRefinery*
A high-performance command-line engine designed for processing massive password datasets. It enables entropy-based research, cleaning, and filtering of raw breach data to create attack-ready wordlists for digital forensics and offensive security workflows.
Technologies: Python, Data Processing, Performance Optimization.

QRX – QReXamination *github.com/vitalelele/QRX*
Bachelor's thesis project. A vulnerability scanner for secure generation and verification of QR codes. The tool follows OWASP standards for RESTful APIs, with a focus on mitigating phishing vectors via QR.
Technologies: Python, Flask, OWASP, REST.

Phishing Email Detection with SVM and NLP
University project for automatic phishing recognition using NLP and Machine Learning (SVM). Optimized through hyperparameter tuning and cross-validation.
Technologies: Python, Scikit-learn, NLP.

Misinformation-Fight-System *github.com/vitalelele/Misinformation-Fight-System*
Software platform for evaluating news credibility through automated source analysis and a trust score system based on OSINT and ML techniques.
Technologies: Python, Flask, HTML, Scrum.

More projects and full source code available at: github.com/vitalelele

International Experience and Participation

Erasmus+ "Let's Make School our Second Home!" Feb 2020 (Trikala, Greece)
Participation in Activity no. 5, focused on inclusion and teamwork in multicultural environments.

Civic Hack Matera Nov 2019
National civic hackathon for designing digital solutions with social impact.

Awards

- Best Bachelor's Thesis in Cybersecurity – University of Bari (2024)
- Best case study – Software Engineering course (BSc)

Languages

- **Italian:** Native speaker
- **English:** B2 (CEFR) — Excellent written and spoken proficiency

Let's Connect

I am actively seeking opportunities to contribute to an Offensive Security Team and tackle complex penetration testing challenges. Reach out via Email or LinkedIn.