Emanuele Picariello

Github: github.com/emanuelepicas
LinkedIn: linkedin.com/in/emanuele-picariello-520231199
YouTube: youtube.com/@emanuelepicariello
Email: info@emanuelepicariello.com
Mobile: +39-3276699391
Location: Amsterdam, Netherlands

Summary

Emanuele Picariello is a senior-level cybersecurity professional with over **4 years of experience** delivering advanced penetration testing, red teaming, and comprehensive security assessments across mobile, cloud, and network environments. With a **research-driven** and proactive approach, he has led full-scope security reviews, performed rigorous **threat modeling**, and guided secure architecture design to harden applications against evolving threats. Leveraging **AI automation** and production-quality coding, he integrates security into every stage of the development lifecycle, ensuring products are secure by design. His extensive expertise in **vulnerability analysis**, **secure code review**, and **incident investigation** makes him an ideal candidate for roles requiring both offensive and defensive security strategies in mission-critical environments.
He is continually expanding his knowledge, most recently through hands-on projects and courses on the **Hugging Face** platform, to stay ahead in the rapidly evolving field of application security.

Outlier - Advanced Coders - AI Training (Contract) *December 2024 - Present*
At Outlier, he trains AI **large language models (LLMs)** to write better code, employing **reinforcement learning with human feedback (RLHF)** for cutting-edge generative AI models. Operating remotely for clients in the San Francisco Bay Area, he enhances model performance while ensuring robust **data protection** and operational efficiency.

Synack Red Team - Red Team Member (Freelance) *December 2024 - Present*
He engages in advanced **red teaming** and **penetration testing**, performing remote vulnerability assessments and product security reviews to strengthen clients' overall **cybersecurity** posture.

Secura B.V. - Security Specialist - Amsterdam, The Netherlands *April 2023 - December 2024*
At Secura B.V., he led scope calls to define both external and internal attack surfaces, enabling focused and comprehensive security assessments. He evaluated vulnerabilities across cloud infrastructures (**AWS, Azure, and GCP**) and delivered high-quality, actionable reports outlining innovative **safeguards** and **controls**. His work included secure code reviews, threat modeling, and the integration of security measures into product architecture to ensure secure-by-default design. He actively contributed to incident investigations using advanced security tools such as **NIDS**, **SIEM**, **EDR**, log aggregation solutions, and Linux command-line utilities. Additionally, he streamlined workflows through red team automation with **Python** and **Go**, and integrated **SAST/DAST** tools into CI/CD pipelines using **Jenkins**.

YouTube - Content Creator *February 2022 - Present*
As a content creator, he produces engaging educational content on **IT Security** and **AI**. His videos—hosted on the **PortSwigger** website under community solutions—demonstrate practical security exploits such as **JWT authentication bypass via flawed signature verification** (https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-flawed-signature-verification) and **client-side prototype pollution** (https://portswigger.net/web-security/prototype-pollution/client-side/browser-apis/lab-prototype-pollution-client-side-prototype-pollution-via-browser-apis). He also shares strategies for passing certifications (e.g., **OSCP**, **OSEP**, **BSCP**, **CRTO**) in dedicated tutorials.

Accenture Security - Security Delivery Analyst - Rome, Italy *July 2022 - March 2023*
At Accenture Security, he conducted **penetration tests** and managed vulnerability assessments across cloud-based applications. Implementing robust vulnerability management solutions such as **Qualys**, he identified and mitigated risks effectively. He developed custom **Python** scripts to automate **SAST** and **DAST** processes using tools like **Snyk** and **Veracode**, reducing testing time by **30%**, and integrated security tools into CI/CD pipelines with **Jenkins** and **Docker**. He performed extensive network testing and infrastructure security assessments on **AWS** and **Azure**, collaborating with engineering teams to embed security throughout the software development lifecycle. Additionally, he played an active role in security incident investigations by leveraging tools such as **NIDS**, **SIEM**, **EDR**, and log aggregation solutions.

Accenture Technology - Application Development Analyst - Rome, Italy *September 2021 - July 2022*
At Accenture Technology, he developed an automated electrical infrastructure system to manage new electrical connections. As part of an international Agile project with a team of **50 people** from Europe and South America, he integrated various systems using RedHat tools such as **JBPM** for synchronous and asynchronous operations. He conducted functional analysis and tested critical processes using **Docker**, contributing to the development of scalable and efficient systems with **Java** and **Spring Boot**.

Sourcesense - Software Developer - Rome, Italy *October 2019 - August 2021*
At Sourcesense, he provided international customer support for **JIRA plugins**, developing and enhancing plugins following **Atlassian Developer** guidelines. Managing three plugins published on the **Atlassian Marketplace**, he spearheaded sales activities that increased annual revenue by **60%**. He utilized **Java**, **JavaScript**, and **TypeScript** to enhance functionality and user experience.

Education

Bachelor Degree in Computer Science and Engineering *December 2021*
Università degli Studi Roma Tre, Roma, Italy

Technical Skills

- **Programming Languages:** Python, Go, PHP, Java, C#, JavaScript, TypeScript, Bash, PowerShell, Ruby, Perl
- **Cloud Platforms:** AWS, Azure, Google Cloud Platform (GCP)
- **Security Tools:** Veracode, SonarQube, Snyk, OWASP ZAP, Burp Suite, Qualys, Rapid7, Synack, **SIEM**, **NIDS**, **EDR**
- **CI/CD Technologies:** Jenkins, AWS CodeBuild, Puppet, Docker
- **Infrastructure as Code:** Terraform, Ansible
- **Operating Systems:** Linux, Windows, iOS, Android, MacOS
- **Frameworks:** .NET, React, AngularJS, Kubernetes
- **Data Security:** Experienced in **data protection**, **encryption**, **data classification**, and **log analysis**

Certifications

- **Red Hat Certified System Administrator**
  (https://www.credly.com/badges/29afb1d6-fcf2-4be8-b860-c797d94a51db/public_url)
- **Burp Suite Certified Practitioner**
  (https://portswigger.net/web-security/e/c/07c1e0a7a6089ea5)
- **eWPT - eLearning Web Application Penetration Testing**
  (https://verified.elearnsecurity.com/certificates/a0d3ea6a-4083-47ce-a001-8813d8c1c260)
- **eWPTx - eLearning Web Application Penetration Testing eXtreme**
  (https://verified.elearnsecurity.com/certificates/02f39488-253d-44e6-9036-df723515f12a)
- **OSCP - Offensive Security Certified Professional**
  (https://www.credential.net/a8693bbe-37d3-4133-aeb9-b8893599cbe6)
- **OSEP - Offensive Security Expert Professional**
  (https://www.credential.net/37a18a39-e2ab-44d6-a27b-86ef5b48bd9e)
- **Certified Red Team Operator**
  (https://eu.badgr.com/public/assertions/UZ6-r3tfSYetcl2bcM2tKg)

Private AI Projects

Currently, he is building and refining **GEN AI workflows** and fine-tuning models using a modern, scalable framework for AI development. He focuses on creating robust APIs and employs advanced techniques to streamline deployment and orchestration. Emanuele is actively expanding his knowledge through hands-on projects and courses on the **Hugging Face** platform, further strengthening his capabilities as a GEN AI Developer.

CTF & Training

Actively engaged in **CTF Time weekly practice & pwnable.kr**, he continuously refines his skills in **information gathering**, **exploit development**, and **reverse engineering** on Linux and Windows. Regularly practicing **buffer overflow exploitation** and comprehensive **network penetration testing** (including **enumeration**, **privilege escalation**, and **web attacks**), he leads interactive training sessions for executives with tailored materials. He currently participates in the **0din GENAI Bug Bounty program** and expands his expertise with the **OWASP Top 10 for Large Language Models**, while also exploring AWS proxy tools and mobile app projects.