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 and comprehensive security assessments across diverse domains **mobile**, **cloud**, and **network**. He excels at uncovering sophisticated vulnerabilities and orchestrating strategic exploit campaigns, leveraging **AI automation** to streamline and enhance security operations. His holistic approach to threat detection and mitigation has empowered global enterprises to fortify their defenses, making him an ideal candidate for dynamic, high-impact security roles.
He is constantly improving and growing day after day to achieve international recognition as a leading security researcher.

Synack Red Team - Red Team Member (Freelance) *December 2024 - Present*
He engages in advanced **red teaming**, performing remote **penetration testing** and **vulnerability assessments** to strengthen clients' security postures across global projects.

Outlier - Advanced Coders - AI Training (Contract) *December 2024 - Present*
At Outlier, he trains AI **large language models (LLMs)** to write better code, performing **reinforcement learning with human feedback (RLHF)** for cutting-edge generative AI models. Operating remotely for clients in the San Francisco Bay Area, he contributes to enhancing model performance in code generation tasks, ensuring outputs are secure, efficient, and adhere to best coding practices.

Secura B.V. - Penetration Tester *April 2023 - October 2024*
During his time 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 to stakeholders. Leveraging red team automation with **Python** and **Go**, he streamlined assessment workflows and developed innovative tools, such as a **Fake Blog Generator** project (available on GitHub: https://github.com/emanuelepicas/Red-Teaming-Tools/tree/main/fakeBlogGeneratorWithGPTAPI), to enhance testing efficiency. He also conducted secure code reviews for appications built in **.NET**, **Java**, **React**, and **AngularJS**, and integrated **SAST/DAST** tools (SonarQube, OWASP ZAP, and Veracode) into CI/CD pipelines using **Jenkins**. By automating security tasks with **Python** and **Bash**, he improved operational efficiency by **30%**. Additionally, he reinforced Identity and Access Management (IAM) controls across cloud environments and executed mobile application security testing on both **iOS** and **Android** platforms using tools like **Frida**, **MobSF**, and **Burp Suite**.

YouTube - Content Creator *February 2022 - Present*
As a content creator on YouTube, he produces engaging educational content on **IT Security** and **AI**. His videos are hosted on the **PortSwigger** website under the community solutions, where he demonstrates practical security exploits. For instance, his **JWT authentication bypass via flawed signature verification** can be viewed at https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-flawed-signature-verification, and his **client-side prototype pollution via browser APIs** is available at https://portswigger.net/web-security/prototype-pollution/client-side/browser-apis/lab-prototype-pollution-client-side-prototype-pollution-via-browser-apis. He also showcases strategies to pass various certification exams (e.g., **OSCP**, **OSEP**, **BSCP**, **CRTO**) in dedicated videos, for example https://www.youtube.com/watch?v=c6zI40aLchE. Through tutorials, discussions, and demonstrations, he makes complex security concepts accessible to a broader audience.

Accenture Security - Security Delivery Analyst *July 2022 - March 2023*
At Accenture Security, he conducted **penetration tests** and managed **vulnerability assessments** across **cloud-based applications**. Implementing robust vulnerability management solutions like **Qualys**, he effectively identified and mitigated risks. He developed and deployed custom **Python** scripts to automate **SAST** and **DAST** processes using tools such as **Snyk** and **Veracode**, reducing testing time by **30%**. By integrating security tools into the CI/CD pipeline with **Jenkins** and **Docker**, he ensured continuous security coverage throughout the development lifecycle. He also performed **network testing** and **infrastructure security assessments** on **AWS** and **Azure** platforms, collaborating closely with engineering teams to enhance security practices within an **Agile** framework. Additionally, he deployed and configured vulnerability scanners, including **Rapid7** and **Synack**, in customer-segmented networks.

Accenture Technology - Application Development Analyst *September 2021 - July 2022*
At Accenture Technology, he developed an automated electrical infrastructure system that managed new electrical connections. Participating in an international **Agile** project with a team of **50 people** from Europe and South America, he integrated various systems using **RedHat** tools like **JBPM** for synchronous and asynchronous operations. He conducted functional analysis and tested critical processes using **Docker**. Collaborating with team members, he contributed to building scalable and efficient systems, utilizing **Java** and **Spring Boot** for application development.

Sourcesense - Software Developer *October 2019 - August 2021*
At Sourcesense, he provided international customer support for **JIRA plugins** developed by the company. He developed and improved plugins following **Atlassian Developer** documentation guidelines, managing three plugins that were published on the **Atlassian Marketplace**. Spearheading all sales activities, he increased annual revenue by **60%**. Utilizing **Java**, **JavaScript**, and **TypeScript**, he enhanced the functionality and user experience of the plugins, ensuring they met customer needs and industry standards.

Education

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

Technical Skills

- **Programming Languages:** Python, Go, 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
- **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

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 - eLearnSecurity Web Application Penetration Testing**
  (https://verified.elearnsecurity.com/certificates/a0d3ea6a-4083-47ce-a001-8813d8c1c260)
- **eWPTx - eLearnSecurity 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 Experienced Penetration Tester**
  (https://www.credential.net/37a18a39-e2ab-44d6-a27b-86ef5b48bd9e)
- **Certified Red Team Operator**
  (https://eu.badgr.com/public/assertions/UZ6-r3tfSYetcl2bcM2tKg)

CTF & Training

Regularly competing in **CTF Time** and **pwnable.kr**, he continuously hones his skills in **information gathering**, **exploit development**, and **reverse engineering** on Linux and Windows. He specializes in **buffer overflow exploitation** and comprehensive **network penetration testing** (**enumeration**, **privilege escalation**, **web attacks**). He also leads interactive live training sessions for executives, supported by tailored materials. Currently, he participates in the **0din GENAI Bug Bounty program**, increasing his expertise with the **OWASP Top 10 for Large Language Models**, and works on **AWS proxy tools** and mobile app projects.