Tobia Righi

Languages: Italian, English, Swedish and Spanish.

Whoami

I'm a security researcher and penetration tester with a deep passion for understanding and dissecting technology. I thrive on building innovative and secure solutions, as well as uncovering and exploiting security flaws. Those "aha!" moments, when I discover how something can be exploited and improved, are what drive me.

I enjoy collaborating with like-minded individuals, bouncing ideas around, and finding elegant solutions to complex problems. Leadership roles come naturally to me, and I relish the opportunity to guide teams toward effective outcomes.

Beyond the tech world, I'm into climbing, cooking, skateboarding, and chess. I am the happiest when I'm traveling and sharing good food with people who have interesting stories to tell are some of my favorite pastimes.

My goal? To learn something new every day, surround myself with great people, and have a blast while doing it.

Experience

Truesec - Penetration Tester

September 2024 - Present

- Providing the highest quality of pentests for major Nordic clients
- Working on web and api security, focusing on novel vulnerabilities and weaponized attack chains
- Specializing in Web and IoT security

Self employed - Bug Bounty Hunter

February 2024 - Present

- Focusing on novel attacks against authentication and access control solutions and applying them to various bug bounty programs.
- Hacking on YesWeHack, Intigriti and HackerOne
- Found vulnerabilities that resulted in 6+ CVEs, including one that affected all major mobile
- Submitted 5+ critical and 10+ high findings in the first 3 months of bug bounty hunting

Debricked - Application Security Specialist & Backend Engineer

June 2021 - February 2024

- Part of the core team developing a developer-centric SCA tool from startup phase to acquisition.
- Responsible for driving **feature development** such as:
  - Vulnerability matching & automated remediation
  - Open source package selection
  - Enterprise SSO and RBAC solutions
- Carrying out regular penetests against the Debricked product and infrastructure
- Leading internal application security initiatives, bug bounty program and Capture The Flag competitions.
- Responsible for the **product security** of Debricked within the OpenText organization.

Synack Red Team - Security Researcher

March 2023 - February 2024

- Hunting bugs on private programs in web applications and APIs

---

Security Research work

- Passkey authentication bypass vulnerability (CVE-2024-9956) in Chrome mobile and all other major browsers. Research blogpost at: https://mastersplinter.work/research/passkey/
- Uncovering vulnerabilities in the BankID authentication protocol: link
  - Found and reported over 20+ vulnerabilities across Swedish banks and other institutions
  - Presented such results at the Sec-T 2024 security conference in Stockholm
- Malicious Tensorflow models to gain RCE https://mastersplinter.work/research/tensorflow-rce/

CVEs

- CVE-2024-9956 Chrome Mobile
- CVE-2024-8273 Hypr Passwordless Platform (reserved)
- CVE-2024-XXXX Samsung Android OS (TBA)

Bug Bounty Experience

- HackerOne
- Intigriti
- YesWeHack
- BugCrowd

Certifications

eWPTX - Web application Penetration Tester eXtreme

- Cert-id: 86992097

Education

Bachelor in Network Security

Institution: Linneaus University Year of Graduation: 2025 (Part time)

- Thesis on Secure Dependency Management
- CTF team captain

Technical Skills

- **Programming languages I daily use:**

    - Python, PHP, Go and JavaScript

- **Programming languages I am learning:**

    - Rust and PowerShell
- 8+ years writing software, 4 of which professionally.
- Web & API pentesting techniques
- IoT security best practices and exploitation
- Vulnerability research processes
- SCA and vulnerability assessment tools
- Kubernetes & Docker
- CI/CD systems, Gitlab, Github and Azure
- DevSecOps experience with AWS and Google Cloud
- Bash and Linux administration skills
- Software Supply Chain Security expertise
- Experience with SCRUM and AGILE frameworks

Recent Achievements

- Published a new research blog about phishing Passkeys.
- Published a new research blog about vulnerabilities found in Swedish BankID configurations
- Published a challenge on HackTheBox demonstrating a novel way to attack OIDC implementations

---

Contacts

- Mail: splint@protonmail.com
- Security research: https://mastersplinter.work/research/
- GitHub: https://github.com/Splinter0
- Linkedin: https://www.linkedin.com/in/trighi
- X/Twitter: https://twitter.com/m4st3rspl1nt3r