Tobia Righi

splint@protonmail.com

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.

Experience

Truesec - Penetration Tester

September 2024 - Present

- Specializing in Web and IoT testing, led multiple projects with major manufacturers to help them identify vulnerabilities in their devices and related software.
  - Using BLE man-in-the-middle techniques to take over smart devices.
  - Taking over user accounts with novel OAuth attacks.
  - Identified multiple Web vulnerabilities that could be chained to
- Took the lead role in multiple Red Team and assumed breach assessments, with special focus on evading EDRs and lateral movement using relaying techniques.
- Always approaching every assignment with the goal of showing maximum impact, by chaining multiple vulnerabilities together, focusing on gaining the highest level of access possible from no access at all.

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. With a special focus on: cross device authentication, 2FA OAuth2 and PassKeys
- Hacking on HackerOne, YesWeHack, Intigriti and BugCrowd
- Found vulnerabilities that resulted in 6+ CVEs, including one that affected all major mobile browsers.
- 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 security reviews of new features.
- Leading internal application security initiatives, bug bounty program and Capture The Flag competitions.
- Responsible for the product security of Debricked within the OpenText organization.

Certifications

eWPTX - Web application Penetration Tester eXtreme

- Cert-id: 86992097

CRTP - Certified Red Team Professional (Ongoing)

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

Education

Bachelor in Network Security

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

- Thesis on Secure Dependency Management
- CTF team captain

Technical Skills

- Python, Go, PHP, PowerShell and JavaScript
- 8+ years writing software
- 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
- Software Supply Chain Security expertise

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