

STEFANY DOS SANTOS

Security Researcher | Web3 & Application Security

Florida, United States | sftwrlabs@gmail.com | sftwrlabs.com

github.com/sftwrstef | hackenproof.com/hackers/0xsftwr

PROFILE

Independent security researcher focused on authorization boundaries, protocol logic, bridge accounting, escrow flows and invariant violations. 25+ paid findings across security programs, with 15 paid reports listed on my public HackenProof profile. Background in programming, network security and software projects; emphasis on reproducible evidence, realistic impact and clear technical reporting.

SECURITY RESEARCH

Independent Security Researcher | SFTWR Labs / 0xSFTWR | August 2025 - Present

- Investigate identity-binding, cross-context authorization and access-control failures, including whether users can access resources outside their intended permissions.
- Review smart-contract and protocol state transitions, develop local proofs of concept and control cases, and document prerequisites, reproduction steps, impact, recovery and scope limitations.
- Use Foundry/Solidity, Python, Git and Linux tooling for source review, testing and security diagnostics. Use AI-assisted tools alongside source inspection and reproducible tests.
- Public HackenProof record includes Critical and High findings. Disclosed Critical report OVLRSDD-227 concerns an Overlayer bridge credit-path underflow that reverts the hub receive path. Private findings and confidential proof-of-concept details remain undisclosed.

SELECTED ENGINEERING PROJECTS

- **EQxLogic:** Developed an automated crypto-trading project using Python/Node.js and exchange APIs, with risk controls, real-time alerts and logging. Project development began in 2023.
- **SOL Space:** Developed AI collaboration and knowledge-workflow components using Next.js, Supabase and LangChain, including retrieval-augmented generation and multi-user workflows.
- **Luggy:** Built lost-and-found recovery workflows using Supabase, Flask and React, with authentication, QR-based claim verification and webhook/API integrations.

TECHNICAL SKILLS

Security: Vulnerability research, authorization analysis, threat modeling, smart-contract review, proof-of-concept reproduction, negative/control tests, impact analysis and technical reports.

Tools: Python, Solidity, Foundry, JavaScript/Node.js, Git, Linux, Docker, Next.js, React and Supabase.

Data & cloud: SQL (5 years); AWS (working knowledge).

EDUCATION & CERTIFICATIONS

Palm Beach State College - Bachelor of Applied Science, Network Security & Forensics

Associate of Science, Programming

CompTIA Security+ | CompTIA Network+

PUBLIC WORK SAMPLES

github.com/sftwrstef/web3-security-research-methodology

github.com/sftwrstef/cosmwasm-ante-gas-boundary

Public methodology and diagnostic research harness; not additional claims of accepted vulnerabilities.