Regaan R

Chennai, India — regaan48@gmail.com

linkedin.com/in/regaan — github.com/regaan — regaan.rothackers.com

Professional Summary

Aspiring Offensive Security Engineer with demonstrated expertise in application security, API/WebSocket testing, and AI/LLM red teaming through independent research. Skilled in identifying OWASP Top 10 vulnerabilities (XSS, SSRF, IDOR, SQLi, RCE) and developing security tools. Creator of WSHawk and Basilisk. Published researcher with CVE disclosures and high-performance e fuzzers. Eager to contribute to entry-level offensive security roles.

Technical Skills

Languages: Go, C, C++, Python, TypeScript, Java, Rust
Security Testing: OWASP Top 10, API Security Testing, Web Application Penetration Testing, WebSocket Security, Network Penetration Testing, Protocol Fuzzing, WAF Bypass, LLM Red Teaming
Vulnerability Classes: XSS, SSRF, IDOR, SQL Injection, Command Injection, Authentication Bypass, CSRF, RCE, XXE, Path Traversal
Tools: Burp Suite, Nmap, Wireshark, Metasploit, ffuf, Nuclei, Nikto, sqlmap, Postman, Playwright, Docker
Systems & Infrastructure: Linux Internals, Windows Internals, Syscalls, TCP/IP, LLVM, Docker, Redis, PostgreSQL, Node.js, Next.js, GitHub Actions, CI/CD
AI/ML Security: Genetic Algorithms, Prompt Evolution, Adversarial ML, LLM Quantization

Education

Diploma in Computer Science 2019 – 2022
Mohamed Sathak Polytechnic College, Chennai, India Graduated with 83% overall

Key Projects

WSHawk – WebSocket Security Scanner github.com/regaan/wshawk
WebSocket security testing framework featuring payload mutation and browser-based validation. Supports multiple vulnerability classes including XSS, SSRF, and SQL Injection with 22 integrated testing tools. Reached 8,800+ PyPI installations.

Basilisk – AI Red Teaming Framework github.com/regaan/basilisk
Genetic algorithm-driven framework for adversarial prompt generation and LLM security evaluation. Implements 29 attack modules aligned with OWASP LLM Top 10. Reached 2,900+ PyPI installations. Associated research paper published (DOI: 10.5281/zenodo.18909538).

ProtoCrash – Protocol Fuzzer github.com/regaan/ProtoCrash
Coverage-guided mutation fuzzer for network protocol implementations written in Go. Achieves approximately 350,000 executions per second with support for distributed execution.

PoCSmith – Exploit Assistant github.com/regaan/PoCSmith
LLM-powered tool trained on exploit and CVE datasets to automate proof-of-concept generation.

Research & Responsible Disclosure

CVE-2026-33340 — Server-Side Request Forgery (SSRF) in lollms-webui. CVSS Score: 9.1.
GHSA-w6c4-c4gj-m272 — Remote Code Execution via insecure `eval` in lollms-webui. CVSS Score: 10.0 (CVE pending).
Authored comprehensive vulnerability reports including reproduction steps, CVSS scoring, CWE mapping, proof-of-concept details, and remediation guidance for open-source AI platforms.

Publications

Basilisk: AI Red-Teaming Framework for LLM Security Evaluation
Regaan R., March 2026. DOI: 10.5281/zenodo.18909538. Introduces a genetic algorithm approach for adversarial prompt generation across 29 attack modules, demonstrating improved effectiveness over static testing methods.

Certifications & Achievements

- **Certified Ethical Hacker (CEH)** — EC-Council, 2025–2026
- **OffSec Echo** — Completed intensive 9-week program covering digital forensics, cloud security, and malware analysis
- **Guest Lecturer – Mobile App Development** — Dwaraka Doss Goverdhan Doss Vaishnav College (Feb–Mar 2026). Delivered a 30-day workshop on mobile development and OS fundamentals to 50+ undergraduate students; received average instructor rating of 4.8/5
- **Workshop Instructor** — Cyber attack engineering workshop at eHackify, 2025
- **Guest Speaker** — Offensive R&D workshop at Mohamed Sathak Polytechnic College, 2026
- **Published Researcher** — Basilisk paper indexed on Zenodo, Figshare, OSF, and OpenAIRE