Shreyas Chavhan | Offensive Security & AI/LLM Security Researcher

chavhanshreyas@gmail.com | LinkedIn | Remote (India) — Open to Global Roles

PROFESSIONAL SUMMARY

Offensive security researcher. Authored CVE-2026-5189 (**CVSS 9.8 Critical**) — a source-level Remote Code Execution chain in **Sonatype Nexus Repository Manager**, a widely-used artifact repository across global Java and CI/CD pipelines. Specializes in **AI/LLM agent security** — prompt injection, guardrail bypass, and privilege escalation in production LLM systems.

PROFESSIONAL EXPERIENCE

AppSecure Security | Security Engineer | Remote
Oct* 2025 - *Present

- **Solo-owned 20+ offensive security engagements** across ~17 enterprise clients (**web, android, red team, and purple team exercises)** — delivering **13 Critical and 27 High severity findings** (115+ total), including multiple **CVSS 10.0** attack chains.
- **Led end-to-end AI/LLM security assessments** for production LLM agent platforms and conversational AI products. Discovered techniques including: (i) **multi-turn prompt-injection** chains. (ii) **multi-step guardrail bypasses**. (iii) invisible prompt injections. (iv) full-read SSRF via LLM web-scrape tooling, and more.
- **Found criticals on hardened, well-tested targets** — cross-tenant admin account takeover on a **Fortune 500 CIAM** platform; 5 blind SQL injection vulnerabilities (time-based + boolean, all WAF-bypassing) across multiple backend microservices of an Indian **NBFC fintech**; account takeover chains via stored XSS on a **major SE Asian consumer marketplace**; mass PII enumeration on a publicly-traded insurance aggregator.
- **Engineered AppSecure's internal "Write with AI" report generator** — designed the prompt architecture, iterated on system prompts to balance cost and accuracy constraints, and partnered with the dev team on frontend integration. **Reduced per-report writing time from ~90 minutes to 5–10 minutes (≈9× speedup)**, adopted company-wide and standardizing report structure across the entire pentest team.

Offensive Security Researcher | Independent Security Research | Remote
Full-time: Aug* 2023 – *Sep* 2025 | *Part-time (alongside AppSecure): Mar* 2026 – *Present

- CVE-2026-5189 (**CVSS 9.8 Critical**) — pre-authenticated **RCE** chain in **Sonatype Nexus Repository Manager**, used across global Java and CI/CD pipelines.
- **8 high-severity findings (4 Critical, 4 High)** across multiple private programs in the **past 90 days**, including 4 RCEs and a full-read SSRF — with an **average impact score of 33.33** on HackerOne.
- **Submitted 108+ vulnerability reports during full-time independent research (Aug 2023 – Sep 2025)** across 40+ enterprise applications, working with Fortune 500 programs including **Microsoft, Stripe, and Quora**, with **41% of validated findings rated High or Critical** severity.
- Averted a platform-wide security incident by identifying **a critical vulnerability on Quora,** impacting all **400+ million monthly active users.**
- **Achieved a critical patch from Microsoft** by discovering and weaponizing a Remote Code Execution vulnerability on a key asset, despite initial program scope limitations.
- **Featured on security podcasts** including **Critical Thinking Bug Bounty Podcast** (Justin Gardner & Joel Margolis) and **Bug Bounty Reports Explained** (gregxsunday). Shared my security Journey via Blog , X and GitHub.

TECHNICAL SKILLS

- **Offensive Security & Pentesting:** Web Application Pentesting · Android Application Pentesting · API Security Testing · Source Code Review · Red Team · Purple Team · OWASP Top 10 · OWASP ASVS
- **AI / LLM Security:** Prompt Injection · Guardrail Bypass · LLM Security · AI Security · Agent Security · System Prompt Extraction · AI Red Teaming · OWASP Top 10 for LLM Applications
- **Vulnerability Classes**: RCE · SSRF · SSTI · IDOR · SQL Injection (Blind / Time-Based / Boolean-Based) · Stored, Reflected & DOM XSS · CSRF · XXE · Unsafe Deserialization · Hard-coded Credentials · JWT Vulnerabilities · OAuth 2.0 Flaws · Cross-Tenant Access Control · Web Cache Deception · Web Cache Poisoning · GraphQL Vulnerabilities · CORS Misconfigurations · Path Traversal · Information Disclosure · WAF Bypass Techniques
- **Tools:** Burp Suite Professional · OWASP ZAP · SQLMap · SSTIMap · ffuf · katana · httpx · nmap · Frida · MobSF · JADX · adb · Custom Python/Bash tooling

EDUCATION

International Institute of Information Technology, Pune **Aug 2019 - June 2023**
Bachelor of Engineering in Computer Engineering; CGPA: 8.82/10