Shantanu Ghumade

shantanu.ghumade@gmail.com | +91-8626052714 | Cyberjaya, Malaysia
LinkedIn: https://www.linkedin.com/in/dark-warlord14/
GitHub: https://github.com/dark-warlord14
Personal Blog: https://securityjunky.com
HackTheBox: https://app.hackthebox.com/users/147927
CTF Profile: https://ctf.hackthebox.com/user/profile/3774

Summary

Senior Application Security Engineer with 6+ years of hands-on experience across AppSec, Cloud Security, and DevSecOps. Proven track record of embedding security into SDLC via secure code reviews, CI/CD automation, and cloud hardening at scale. Builder mindset with strong experience developing custom security tooling and AI-driven automation to improve detection, triage, and operational efficiency.

Certifications

- OffSec Web Expert (OSWE) *(Jan 2026)*
- OffSec Certified Professional (OSCP) *(Jul 2021)*

Work Experience

Deriv, Malaysia

Senior Security Engineer *(Jan 2023- Present)*

- Led end-to-end security assessments across web, mobile, API, network, and cloud products, including secure code and architecture reviews.
- Improved cloud security posture by implementing CIS-aligned hardening across 20+ AWS accounts and 20+ GCP projects.
- Conducted secure code reviews for Perl, Node.js, Python, Go, React.js, and Flutter, enabling early vulnerability detection.
- Owned and scaled DevSecOps adoption, including pre-commit hooks and org-wide secret prevention controls.
- Built and maintained CI/CD security pipelines integrating SAST, SCA, IaC scanning, and secret detection.
- Managed Deriv's HackerOne bug bounty program end-to-end, optimizing triage workflows and researcher engagement.
- Leveraged EDR solution(CrowdStrike) and SIEM(datadog) for advanced threat detection, incident response, and proactive threat hunting.
- Owned incident response and investigations, including correlating logs from various platforms, conducting root-cause analyses, and implementing preventative safeguards to minimize recurrence.
- **AI & Security Automation**

    - **Threat Feed Automation**: Built an AI-driven threat intelligence feed tailored to internal tech stack for proactive risk identification.
    - **Security Assistant:** Developed an internal RAG-based security assistant to answer employee security queries using Information Security policies, internal processes as knowledge bases.
    - **HackerOne Triage Bot:** Designed an automated HackerOne prescreening agent, reducing manual triage effort and improving initial response time.
    - **Vendor Prescreening:** Automated third-party vendor risk prescreening using LLM-based research and risk flagging.
    - **Compliance Gap Analysis Framework**: Created an AI-powered compliance gap analysis framework to compare internal policies against regulatory requirements.
- **Detection & Incident Response**
    - Performed threat detection and hunting using CrowdStrike (EDR) and Datadog (SIEM).
    - Led incident response investigations, root-cause analysis, and preventive control implementation.
    - Malware Reversing of a sophisticated campaign where a fake AI recruiter on LinkedIn lures developers into a private GitHub repository for a "coding assessment."
        - https://medium.com/deriv-tech/how-a-fake-ai-recruiter-delivers-five-staged-malware-disguised-as-a-dream-job-64cc68fec263

SecureLayer7, Pune, India (Feb 2020 - Jan 2023)

Lead Security Consultant (Feb 2022- Jan 2023)

- Led end-to-end security testing engagements for a diverse portfolio of global clients across the finance, technology, and payment solutions industries.
- Selected for critical on-site international engagements to conduct comprehensive infrastructure penetration tests for high-value clients, including a major national bank in Mongolia and a key payment solutions provider in India.
- Communicated complex vulnerability details and strategic remediation plans to executive-level stakeholders, ensuring swift resolution of critical security risks.
- Earned two promotions within three years due to consistently delivering high-quality security assessments and exceptional client outcomes.
- Conducted Webinar on Mobile Application Security
    - https://blog.securelayer7.net/webinar-mobile-app-pen-testing-understanding-android-apps-and-how-to-secure-them/

Security Consultant (Feb 2021- Feb 2022)

- Performed in-depth source code analysis and mobile application penetration tests (Android/iOS) for enterprise clients, identifying critical flaws before they could be exploited.
- Conducted sessions on topics such as "Fuzzing HTTP Requests" and "HTTP request smuggling."

Associate Security Consultant (Feb 2020- Feb 2021)

- Conducted over 50+ web application, API, and network vulnerability assessments for a wide range of clients.
- Systematic, Structured Reporting and Documentation of the vulnerabilities found during VAPT engagement through manual and automated testing.

Technical Skills

- **Application Security & Penetration Testing**
  - Performed comprehensive security assessments across web, mobile (Android/iOS), API, network, and cloud environments.
  - Proficient with various tools for penetration testing, including Burp Suite, Postman, MobSF, Frida, and Nmap.
  - Experienced in secure code review, architecture reviews, and system configuration reviews.
- **Cloud Security:**
  - Hands-on experience securing cloud infrastructures on AWS, GCP, and Alibaba Cloud through robust configuration reviews and hardening, utilizing both manual and automated tools.
  - Experienced with reducing public resource exposure by implementing SCP policies, enforcing standard best practices, and regularly flagging public resources across multiple cloud services.
- **DevSecOps & Automation & AI**
  - Integrated security into CI/CD pipelines via automated SAST, DAST, IAC security checks and secret scanning.
  - Developed custom tooling to automate various security checks, such as Nuclei scanning and subdomain takeover detection.
  - Developed AI-driven bots and workflows using frameworks like Langchain to enhance security operations, including threat intelligence and triage automation by automating manual tasks.
- **Enterprise Security Platform Experience**
  - Hands-on experience with tools for vulnerability management, EDR, SIEM, security awareness training, and WAF services (e.g. Qualys, CrowdStrike, Jamf, Kandji, JumpCloud, Datadog, CloudFlare, Github, HackerOne, Upguard, etc)

Open Source Contributions

- JSScaner - Tool for scanning JavaScript files to identify exposed endpoints and secrets, enhancing reconnaissance capabilities.
- ffufplus - Enhanced the FFUF tool with additional features and automation for advanced web fuzzing
- CVENotifier - A CVE feed notifier for targeted technology or the products

Bug Bounty Experience

- **Synack:** Synack Red Teamer - Level 2 *(Aug 2021 – Present)*
- **HackerOne:** https://hackerone.com/dark_warlord14 (*Aug 2019 – Present)*
- **BugCrowd**: https://bugcrowd.com/dark_warlord14 *(Oct 2019 – Present)*