DANISH SIDDIQUI

Senior Product Security Engineer | Offensive Security | AppSec, Cloud & AI/LLM Security | 22x CVE

Bengaluru, India • +91-8840544676 • danishismyname1@gmail.com

Portfolio • LinkedIn • GitHub • Bugcrowd • YesWeHack (djvirus)

PROFESSIONAL SUMMARY

Senior Product Security Engineer with 6+ years spanning offensive security, application security, and cloud security across high-growth SaaS and product environments. Currently the founding security engineer at Licious, owning end-to-end Product Security, DevSecOps, Bug Bounty, and ISO 27001:2022 readiness. Credited with 22 CVEs across open-source and commercial software, 160+ Hall of Fame acknowledgements (Google, Atlassian, Mastercard, SoundCloud, Paytm), and active research on YesWeHack, HackerOne, Bugcrowd, Intigriti, and Synack Red Team (invite-only). Focused on secure-by-design architecture, AI/LLM security (OWASP Top 10 for LLMs), and developer-first tooling — directly aligned with securing enterprise AI platforms at scale.

CORE COMPETENCIES

Application Security: Web / API / Mobile / Thick Client VAPT, OWASP Top 10 & OWASP API Top 10, STRIDE Threat Modeling, Secure Code Review (CodeQL, Semgrep)

Cloud Security: AWS (IAM, VPC, WAF, ALB, GuardDuty, CloudTrail, S3, Lambda), Azure, CSPM (Prowler, ScoutSuite, Pingsafe), CNAPP (ThreatMapper), Pacu

DevSecOps: CI/CD security integration, SAST (Semgrep custom rules), SCA & Container scanning (Trivy), IaC review, Secrets detection, Secure SDLC

Offensive Security: Red Team Engagements, Active Directory Pentesting, Chrome/Firefox Extension auditing, Attack Surface Management, Bug Bounty

AI / LLM Security: Prompt injection, RAG/retrieval-layer abuse, data leakage, OWASP Top 10 for LLMs, model integration security

Compliance & Program: ISO 27001:2022 SPOC, Bug Bounty program governance, severity taxonomy, triage SLAs, vulnerability management lifecycle

Languages & Tools: Python, Go, JavaScript, Kotlin, Bash, SQL, CodeQL | BurpSuite, Nmap, Metasploit, Nessus, Wireshark, Drozer

PROFESSIONAL EXPERIENCE

SDE-3, Product Security (Founding Security Engineer) | **Licious** *May 2025 – Present*

Bangalore, India (Hybrid) • D2C meat-tech unicorn serving millions of customers

- **Founded and scaled** the Product Security function as the first dedicated security engineer, owning AppSec, Cloud Security, DevSecOps, Bug Bounty, and Compliance across engineering teams.
- **Embedded** security into the SDLC by integrating SAST (Semgrep) and SCA / container scanning (Trivy) across CI/CD pipelines, reducing critical production-bound vulnerabilities by ~30% and cutting triage noise through custom rule tuning.
- **Designed and scaled** AWS cloud security posture using CSPM (Prowler, ScoutSuite) and CNAPP (ThreatMapper) to detect high-risk misconfigurations and exploitable attack paths across multi-account environments.
- **Led** AWS WAF & BotControl tuning to suppress false positives on critical /api/ endpoints, improving mobile client reliability without weakening bot-defense posture.
- **Drove** offensive security engagements across web, mobile, and AWS infrastructure — identifying critical attack paths and partnering with engineering on remediation.
- **Rebuilt and operates** the Bug Bounty program end-to-end — defined scope, severity taxonomy, triage SLAs, and payout governance to accelerate vulnerability remediation cycles.
- **Serves** as primary ISO 27001:2022 SPOC across HR, Finance, IT, and Engineering; established security policies, evidence collection, and audit readiness.

SDET-2, Product Security | **Halodoc** *Dec 2023 – May 2025*

Bangalore, India (Remote) • Southeast Asia's largest digital healthcare platform

- **Authored** multi-language custom Semgrep rules targeting framework-specific and business-logic vulnerabilities, improving detection coverage beyond out-of-the-box rulesets.
- **Integrated** DevSecOps practices into CI/CD pipelines (SAST, SCA, secret scanning) to catch security defects at pull-request time rather than production.
- **Owned** AWS cloud security and triaged incoming Bug Bounty submissions and CSPM (Pingsafe) findings, coordinating remediation with service owners.
- **Conducted** full-scope VAPT across web applications, mobile apps (Android/iOS), and AWS environments in a regulated healthcare context.

Senior Security Engineer | **Invia Pvt. Ltd.** *Sep 2022 – Nov 2023*

Noida, India • B2B cybersecurity services

- **Designed** and launched CyberShield360 — an Attack Surface Management product covering subdomain enumeration, port scanning, CVE correlation, and risk scoring — increasing client engagement by ~200%.
- **Led** internal VAPT on Invia's product suite and managed Azure cloud security hardening.
- **Authored** technical responses for RFPs covering VAPT and Red Team engagements; supported pre-sales scoping.

Security Analyst / Consultant | **FireCompass** *Jul 2021 – Sep 2022*

Bangalore, India (Remote) • Continuous Automated Red Teaming (CART) platform

- **Delivered** Continuous Automated Red Teaming, External Attack Surface Management (EASM), and Ransomware Attack Surface Testing (RAST) for top telecom, IT services, and financial services customers.
- **Executed** Deep/Dark Web assessments with prioritized real-time risk alerting and ransomware susceptibility testing.

Earlier Roles | **Vast Dreams • Codec Networks** *Jun 2019 – Jul 2021*

- **VA & PT** engagements on Web/API, Mobile, and Thick Client applications for Australian and Indian clients; internal and external penetration testing for a leading Dubai-based telecommunications company.

INDEPENDENT SECURITY RESEARCH & BUG BOUNTY

- **22 CVEs** assigned across open-source and commercial software, including CVE-2026-27859 (pre-auth DoS in Dovecot/Pigeonhole RFC 2231 parser), CVE-2026-23521, CVE-2024-57459, and CVE-2025-29074 through CVE-2025-29078.
- **160+ Hall of Fame** acknowledgements from Atlassian, Google, Mastercard, SoundCloud, Paytm, Achmea, and others.
- **Top 3 Bug Hunter** on Convertkit (Bugcrowd); active researcher on YesWeHack (djvirus), HackerOne, Bugcrowd, and Intigriti.
- **Member, Synack Red Team** — invite-only private vulnerability research network (<10% acceptance rate).
- **Research focus:** OIDC/OAuth auditing, browser extension security (Chrome/Firefox), algorithmic complexity (DoS) bugs in mail servers, open-source codebase auditing, and AI/LLM security.
- Featured publication: Exploring LLM Security Risks & OWASP Top 10 for LLMs — case studies and defensive patterns for enterprise AI platforms.
- Detailed case studies available on djvirus9.github.io — DevSecOps pipeline build-out, AWS attack path findings, ISO 27001 ownership, and CyberShield360 product build.

CERTIFICATIONS & COMMUNITY

- **Multi-Cloud Red Team Analyst** — CyberWarFare Labs (2024)
- **AWS Certified Security – Specialty**
- **Certified Red Team Professional (CRTP)** — Altered Security (2022)
- **Certified Ethical Hacker (CEH)** — EC-Council (2020) | Seasides Security Conference — Volunteer