SAGAR JONDHALE

Penetration Testing Consultant | VAPT (Web, Mobile, API) | CVE-2025-53545 Published
10+ Hall of Fame and Rewards | CRTA Certified | 60+ Applications & APIs Assessed

+91 9324597930 | sagarjondhle@gmail.com | LinkedIn.com/sagarjondhale | SagarSec.in | Medium Blog

PROFESSIONAL SUMMARY

Penetration tester with 3+ years assessing web, mobile, and API attack surfaces across 60+ production applications in banking and enterprise environments. Published CVE author and recognized by 10+ global Hall of Fame programs including NASA, Nokia, Philips, and BASF for responsibly disclosed vulnerabilities. Skilled in manual exploitation, OWASP Top 10 methodology, and end-to-end VAPT delivery, with hands-on contribution to a CERT-In empanelment assessment. Seeking a penetration testing role with an international security team.

KEY PROOF POINTS

- **CVE-2025-53545** - independently discovered and published under own name in the global CVE database
- **10+ Hall of Fame recognitions** - including NASA, Nokia, Philips, and BASF for responsible disclosure
- **CRTA (Certified Red Team Analyst)** and **APIsec Certified Practitioner** - offensive security credentials
- **60+ web applications and 70+ APIs** manually assessed for production banking and enterprise clients
- **Secured UK Ministry of Defence and 30+ Indian government websites** through bug bounty and VDP programs

TECHNICAL SKILLS

- **Offensive Testing:** Web Application Penetration Testing, Mobile (Android/iOS) Security Testing, API Penetration Testing, Network VAPT, Manual Exploitation, OWASP Top 10
- **Tools:** Burp Suite, Kali Linux toolset, Frida, Jadx, Nmap, manual testing methodology
- **Specialized Areas:** Payment Gateway / PCI-DSS Security Assessments, Bug Bounty Hunting, Vulnerability Research, Responsible Disclosure, Web application Testing, Mobile Application testing
- **Program & Reporting:** End-to-End Vulnerability Assessment and Penetration Testing (VAPT) Project Management, Technical Reporting, Patch Verification & Re-testing

EXPERIENCE

Penetration Testing Consultant (VAPT Engineer)
June 2025 – Present

Banking Client – Mumbai, Maharashtra

- Performs hands-on penetration testing SAST/DAST and vulnerability re-validation across web, mobile, and API attack surfaces for core banking infrastructure.
- Independently re-exploits previously identified vulnerabilities to verify that remediations fully close the attack path, rather than relying on automated re-scans.
- Performs manual exploitation to separate true positives from false positives flagged by the Infosec team, reducing noise for engineering stakeholders.
- Advises vendors on remediation across code-level, server-level, and load balancer configurations to eliminate root-cause vulnerabilities.
- Owns end-to-end tracking of risk exceptions and risk acceptances, maintaining KPIs across the assessment lifecycle.

Associate Consultant (Penetration Tester)
Feb 2024 – June 2025

Anzen Technologies – Navi Mumbai, Maharashtra

- Conducted payment gateway security assessments on mobile applications, identifying flaws in financial transaction flows and verifying PCI-DSS-aligned controls.
- Performed manual penetration testing on 60+ web applications using OWASP Top 10 methodology, exploiting and reporting SQL injection, XSS, and insecure authentication vulnerabilities.
- Conducted API security assessments across 70+ APIs, targeting authentication, authorization, input validation, and encryption to uncover real-world exploitation paths.

- Acted as technical liaison between application owners and the offensive security team, verifying that remediations withstood re-exploitation before sign-off; escalated unresolved high-risk findings to stakeholders.

Cyber Security Intern *July 2023 – Jan 2024*
Anzen Technologies – Mumbai, Maharashtra

- Identified and exploited common web application vulnerabilities including SQL injection, XSS, and insecure direct object references using manual testing techniques.
- Built hands-on proficiency with Burp Suite and the Kali Linux toolset for web testing, and Frida and Jadx for Android application security testing.
- Tested API authentication mechanisms (including OAuth) and authorization logic for sensitive data handling flaws.
- Delivered detailed vulnerability reports outlining exploitation steps, business impact, and remediation guidance for developers and stakeholders.
- Contributed to a CERT-In empanelment assessment, performing manual web application security testing on a demo application and co-authoring the team's consolidated findings report.

Bug Bounty Hunter *2023 – Present*
HackerOne / Bugcrowd / VDP Programs – Remote

- Achieved 10+ Hall of Fame recognitions, including NASA, Nokia, Philips, and BASF, for responsibly disclosed vulnerabilities.
- Discovered and reported **CVE-2025-53545**, published under own name in the global CVE database.
- Identified and reported critical vulnerabilities to the UK Ministry of Defence and 30+ Indian government websites.
- Earned bounties, swag, and recognition from organizations including Jio and Mollie, plus appreciation letters from LG and TruCSR.

CERTIFICATIONS

- Certified Red Team Analyst (CRTA)
- APIsec Certified Practitioner

EDUCATION

- Bachelor of Science in Information Technology - Mumbai University
- Higher Secondary Certificate - Maharashtra Board

LEADERSHIP & COMMUNITY

- Led cross-functional security assessment projects at Anzen Technologies with teams of 8+, covering web, mobile, and API security while consistently meeting deadlines.
- Active contributor to cybersecurity communities through meetups, conferences, and workshops; publishes technical write-ups on bug bounty findings and secure development practices.