RAHUL PARMAR

APPLICATION & PRODUCT SECURITY · VAPT / PENETRATION TESTING · VULNERABILITY MANAGEMENT · SECURITY RESEARCH

rahulparmar838@gmail.com • +91 76982 39585 • linkedin.com/in/rahul-parmar31 • Gandhinagar, Gujarat, India

PROFESSIONAL SUMMARY

Cybersecurity professional with **5+ years** across product security, application security, VAPT and security operations. Built an organisation's entire security function from the ground up — processes, tooling and a **5-person team** — closing **300+ vulnerabilities to an ~80% remediation rate**, and delivered VAPT across **100+ applications** for banking, financial services and oil & gas clients at PwC. Currently run **DevSecOps** and secure-release reviews for enterprise IBM Maximo Application Suite — SAST, DAST, SCA and container scanning (Mend, OWASP ZAP, Twistlock), analysing CVEs/PSIRTs and SBOM risk, and hands-on remediation of open-source and container findings. Independent researcher with **4 published CVEs**, Hall of Fame recognition from Apple, the United Nations, Dell, eBay and 15+ other organisations, and a **Top-15 NCIIPC (NTRO)** ranking for disclosures affecting Government of India systems.

CORE COMPETENCIES

Offensive Security	VAPT, Web / API / Mobile Penetration Testing, Red Teaming, Purple Teaming, Breach & Attack Simulation, Phishing Simulation, VPN & Network Security Testing, OWASP Top 10, OWASP API Top 10, JWT / OAuth / Rate-Limit Bypass
Application / Product Security	DevSecOps, SAST, DAST, SCA, API Security, Secure SDLC, Threat Modeling, CI/CD & Pipeline Security, Secrets Management, Code Signing, Container & Image Security, Secure Release Review (SRR)
Vulnerability Management	CVE Analysis, CVSS Scoring & Prioritisation, PSIRT / PVR Workflows, SBOM & Open-Source Risk, False-Positive Validation, Security Exceptions, Remediation Tracking & Executive Reporting
Detection & Response	Threat Hunting, Dark-Web Monitoring, Microsoft Sentinel (SIEM), Defender for Endpoint, Sophos XDR, Azure WAF, Firewall Hardening, Brand-Abuse Monitoring
Cloud & GRC	AWS, Azure, Cloud Security Audits, ISO 27001 (Lead Auditor), SOC 2, DPDP Act 2023, Security Compliance & Governance, Risk Assessment, Security Architecture Review
Program & Leadership	Security Program Build-Out (0→1), Team Leadership (5-person team), Hiring, Mentoring & Training, Process & Policy Definition, Stakeholder Management, Executive Reporting
Toolset	Burp Suite, OWASP ZAP, Mend, Twistlock / Prisma Cloud, Nuclei, Subfinder, httpx, Nmap, Nessus, Metasploit, Acunetix, Netsparker, HP Fortify, Hashcat, Autopsy, OSForensics, Sentinel, Defender, Sophos XDR, Azure WAF, Wireshark

PROFESSIONAL EXPERIENCE

Software Developer — Product Security / Secure Release Review (SRR) · IBM

Dec 2025 – Present

*Gandhinagar, Gujarat · Security-focused **DevSecOps** role covering IBM Maximo Application Suite (MAS) and associated SaaS / cloud services*

- Own security review and secure-release sign-off across MAS components, gating releases against enterprise security milestones.
- Run **DAST (OWASP ZAP), SAST & SCA (Mend) and container image scanning (Twistlock / Prisma Cloud)** across product releases as part of the DevSecOps pipeline.
- Triage findings and **remediate open-source / SCA and container vulnerabilities** hands-on — dependency upgrades, base-image fixes and configuration hardening — validating each fix through re-scan.
- Analyse CVEs, PSIRTs and PVRs — severity, ageing and release impact — and perform **SBOM and open-source dependency analysis** to surface licence, supply-chain and security risk.
- Review security evidence across CI/CD, secrets management, MFA, code signing, environment separation and threat models.
- Partner with product, development and cloud teams to close security gaps and produce executive-level vulnerability reporting supporting SRT activities.

Senior Software Security Engineer · Zarca Interactive (Zisystech)

Nov 2022 – Nov 2025

Mumbai, Maharashtra · Founding security hire — built and led the organisation's security function and team

- **Built the security function from the ground up** — defined the VAPT, vulnerability-management, monitoring and incident-response processes, selected and deployed the tooling stack, and established reporting to leadership where no security program previously existed.
- **Built and led a 5-person security team**, hiring and training junior analysts on VAPT methodology, triage and incident response — building in-house capability rather than relying on external vendors.
- Identified **300+ vulnerabilities** across the application and infrastructure estate and drove remediation with engineering down to ~55 open — an **~80% closure rate**.
- Built and ran the **breach & attack simulation** and organisation-wide phishing simulation programmes, improving detection coverage and employee resilience.
- Led SAST and DAST assessments across the product portfolio and drove remediation through to verified fix.
- Performed proactive **threat hunting**, dark-web monitoring and brand-abuse detection to surface credential leaks, exposed assets and impersonation.
- Administered Microsoft Defender for Endpoint, Sophos XDR, Azure WAF and Microsoft Sentinel — rule tuning, detection engineering and security incident response.
- Conducted cloud security audits and firewall hardening reviews; managed **ISO 27001 and SOC 2** audit cycles end to end.

Risk Consultant · **PricewaterhouseCoopers (PwC)** — **Feb 2022 – Nov 2022**

Mumbai, Maharashtra

- Delivered **VAPT across 100+ client applications** — web, API and infrastructure — combining manual exploitation with automated tooling (Burp Suite, Acunetix, Netsparker, Nessus, Metasploit, Nmap, OWASP tooling, HP Fortify).
- Executed **3 full-scope breach & attack simulation / red-team engagements** for banking, financial services and oil & gas clients, emulating real-world adversary tradecraft end to end.
- Performed **VPN and remote-access security testing**, identifying configuration and authentication weaknesses across perimeter infrastructure.
- Classified findings against **CVSS** to prioritise client patch-management programmes; authored technical and executive reports translating exploit chains into business risk.

Security Analyst · **Bulwarkers Websecurity Pvt. Ltd.** — **Jul 2021 – Jan 2022**

Ahmedabad, Gujarat

- Performed vulnerability assessment and penetration testing across web and mobile applications for multiple client environments, applying OWASP / PTES methodology with manual exploitation alongside automated tooling.
- Documented reproducible proof-of-concepts and worked with developers to validate fixes through re-testing.

SECURITY RESEARCH & RESPONSIBLE DISCLOSURE

- **Published CVEs:** CVE-2023-3074 · CVE-2023-1975 · CVE-2023-1704 · CVE-2023-1703.
- **Hall of Fame** recognition through responsible-disclosure programs at *Apple, United Nations, Dell, Deutsche Telekom, eBay, FitBit, HubSpot, Springer Nature, Inflectra, Electro Rent, Worldline Global* and *APNIC*.
- **Letters of acknowledgement** from *Harvard University, Intuit, ESET, Avast, Huawei, Intel, HumanFirst* and *Worldline Global*.
- Ranked in the **Top 15 researchers** for reporting vulnerabilities in Government of India websites — NCIIPC India (a unit of NTRO), April 2021 newsletter.
- **Publications:** "Hashcat for Forensics" — National Journal of Anti Cyber Crime Research and Studies (ACCRS); Google Dorks published on Exploit-DB.

CERTIFICATIONS

ISO/IEC 27001 Lead Auditor — Jul 2024

Certified Ethical Hacker (CEH v11), EC-Council — May 2022

Certified Cybersecurity Educator Professional (CCEP)

Certified Network Security Specialist (CNSS), ICSI UK — May 2020

Autopsy Basics & Hands-On, Basis Technology — May 2020

OSForensics Triage, PassMark — May 2020 · **DPDP Act 2023** — 96%

EDUCATION

Post Graduate Diploma in Cyber Security & Cyber Forensics — Rashtriya Raksha University — **2020 – 2021**

M.Sc. Information Technology — Dr. C. V. Raman University — **2017 – 2019**

Bachelor of Business Administration — Kadi Sarva Vishwavidyalaya — **2013 – 2016**

EARLY CAREER & INTERNSHIPS

- **Summer Intern — Gurugram Police Cyber Cell** (Jun – Jul 2021): mobile, email, social-media, e-commerce, website-hacking and banking-fraud investigation.
- **Cyber Security R&D Intern — TechHack Technologies**, Noida (Dec 2020 – Feb 2021): VAPT execution, OWASP Top 10 research, rate-limit / JWT / OAuth bypass research.
- **PHP Trainee — Incisive Web Solution Pvt. Ltd.**, Gandhinagar (Jul – Dec 2017): PHP, CakePHP, MySQL — foundation for source-code-level security review.