

Parv Bajaj

Gurugram, IND
(+91) 8814086059
Parvbajaj2000@gmail.com
LinkedIn:// parvbajaj

Sr. Application Security Engineer with 4+ years of experience in the field of Cyber Security. Proven track record in leading information security teams and conducting comprehensive assessments across Web, Mobile Applications, APIs, Thick Clients, and Network. Skilled in Red Teaming, Source Code Reviews, Cloud Architecture Reviews and Secure Configuration Reviews.

PROFESSIONAL EXPERIENCE

FinThrive Gurugram
Application Security Engineer April 2024–Present

- Conducted penetration testing and security assessments across 35+ products, including web, mobile, APIs, thick clients, and SaaS platforms.
- Integrated SAST and DAST (Checkmarx) tools into CI/CD pipelines, improving vulnerability detection and remediation.
- Conducted secure design reviews and code audits, enforcing OWASP Top 10, SANS 25, and secure SDLC compliance.
- Performed security reviews for cloud-based applications (AWS, Azure, GCP), validating encryption in transit, OAuth/SAML authentication, and RBAC policies.
- Developed automated security testing workflows using Python, Bash, Jenkins, and PowerShell, reducing manual pentesting efforts.
- Led threat modeling and risk assessment sessions, applying STRIDE framework and MITRE ATT&CK techniques.
- Partnered with developers to build security capability - launched a bug bounty program pilot, crafted security release process, and delivered developer trainings on secure coding best practices.

Grant Thornton Bharat LLP Gurugram
Sr. Security Consultant September 2021–April 2024

- Conducted penetration testing on web applications, APIs, mobile apps, and thick clients using BurpSuite, Postman, MobSF, Frida, and echoMirage.
- Conducted network security assessments (firewall rules, segmentation, Active Directory) and vulnerability testing using Nmap, Wireshark, and Metasploit; delivered actionable remediation guidance to client teams.
- Applied STRIDE threat modeling to identify security flaws in application architecture and cloud deployments.
- Analyzed security incidents and logs using SIEM to detect, investigate, and mitigate threats.
- Ensured compliance with GDPR, PCI DSS, and ISO 27001 security standards while improving security posture across development teams.

EDUCATION

The NorthCap University Gurugram
B.Tech in Computer Science (Specialization in Cyber Security)

PROJECTS

SubShot

- Built SubShot, a subdomain enumeration tool with HTTP/HTTPS probing and screenshotting capabilities; won 2nd place at Technovation.

NCU CTF

- Organized a CTF sponsored by **Offensive Security**, designing challenges across Web, Reverse Engineering, OSINT, and other domains.

ACHIEVEMENTS & PUBLICATIONS

- **Hall of Fame** - Recognized by hippovideo.io and NCIIPC (x4) for responsible vulnerability disclosure.
- **CVE-2025-56146** - Reported a Missing SSL Certificate Validation vulnerability in the Indian Bank IndSMART Android app, impacting login/OTP/payment flows.
- **Research Paper** - Authored 'Cloud Security – The Future of Data Storage' in Springer book series.
- **Technical Blogging** - Author of in-depth technical blogs covering application security, AI Security, AI PenTesting, and practical exploit development, including detailed Hack The Box (HTB) and TryHackMe (THM) walkthroughs; published on Medium.
- **GitHub** — Maintaining active repositories showcasing tools and automation scripts (e.g., SubShot).
- **Conference Speaker** - Presented a talk on "Automating Information Security with Python" sharing insights on developing scripts for security tasks

CERTIFICATIONS

- Certified Red Team Professional (CRTP)
- Web Application Penetration Tester Extreme (eWPTX v2)
- Certified Ethical Hacker (CEH v11)
- Certificate of Cloud Security Knowledge (CCSK)
- Junior Penetration Tester (eJPT)
- Certificate of Competence in Zero Trust (CCZT)
- INE Certified Cloud Associate (ICCA)
- CCNA: Introduction to Networks
- AWS Academy Cloud Graduate
- APIsec Certified Practitioner

SKILLS

- **Penetration Testing & Security Assessments:** Web, Mobile, API, SaaS, Thick Client, Network Security, SAST, DAST, AI Security
- **Cloud & CI/CD Security:** Azure, AWS, GCP, Docker, Kubernetes, Wiz, ORCA Security, Security in DevOps Pipelines
- **Secure SDLC & Threat Modeling:** OWASP Top 10, STRIDE, Secure Design Reviews, OAuth, SAML, RBAC
- **Security Incident Handling & SIEM:** Splunk, CrowdStrike, Threat Analysis, Log Forensics
- **Regulatory Compliance & Security Standards:** GDPR, PCI-DSS, ISO 27001, CIS Benchmarks
- **Programming & Scripting:** Python, Bash, PowerShell, JavaScript, SQL