Vaibhav Jain

+91 8527671247 | vaibhavjain@protonmail.com
linkedin.com/in/jain-vaibhav | github.com/vaibhavjain2609 | jainvaibhav.me

Education

National Forensic Sciences University — Jaipur, India
M.Sc. Digital Forensics and Information Security — *Expected June 2027*
- **Coursework:** Web Application Security, Malware Analysis and Forensics, and Network Security Forensics

California State University — Sacramento, CA
Bachelor of Science in Computer Science — *Graduation: May 2024*

Experience

DevOps and Network Security Intern — Jun 2026 – Jul 2026
Ekvayu Tech Private Limited — *Noida, India*
- Built a 7-stage GitLab CI/CD pipeline where 5 security scanners gate the deploy rather than follow it: Gitleaks (secrets), Bandit and Semgrep (SAST), Checkov (Dockerfile and Compose IaC), and Trivy (filesystem and image).
- Enforced identical gates across all 3 environments, and fronted the pipeline with Ruff, mypy, and hadolint so lint or type failures halt the run pre-build; extended it post-deploy with OWASP ZAP DAST and smoke tests.
- Instrumented 100+ Docker Compose containers across 3 sites with Prometheus and Grafana, and hardened firewalls with VLAN segmentation to limit lateral movement.
- Uncovered 3 critical defects in a core analysis subsystem, where a reused container-naming sequence left metrics and logs unattributable to the workload that produced them.

IT Contractor — Dec 2025 – Jan 2026
Praveen Aggarwal Chartered Accountants — *New Delhi, India*
- Architected an 80-user Active Directory environment from scratch and deployed a hybrid Active Directory + Entra ID integrated SSL VPN on a Sophos XGS firewall with MFA and conditional access policies.
- Minimized data loss risk in disaster scenarios by implementing automated backup policies to Azure Blob Storage, meeting 24-hour RTO and 4-hour RPO targets.
- Reduced email infrastructure costs by 60% by migrating 20 mailboxes from Google Workspace to Microsoft 365.

Cybersecurity Analyst Intern — Jun 2025 – Aug 2025
Ekvayu Tech Private Limited — *Noida, India*
- Discovered and reduced attack surface for an internally developed security tool by remediating 15+ critical vulnerabilities via VAPT using Burp Suite and OWASP ZAP.
- Secured code repository infrastructure by migrating a GitLab server while implementing configuration hardening, access controls, and least-privilege policies.
- Resolved 10 vulnerabilities across production servers and internal apps via Nessus-based threat assessments.

Technical Projects

MedConnect | *Next.js, FastAPI, PostgreSQL, TypeScript, Docker, Keycloak, Redis* — Feb 2026 – Apr 2026
- Designed a multi-tenant clinic architecture with tenant-scoped data access, and enforced ABDM-compliant cross-clinic data sharing through a patient consent system with link codes, approval workflows, and revocation support.
- Resolved 12+ production issues including N+1 queries, race conditions, and security misconfigurations to improve API reliability and security.

btrfsparser | *Python, Filesystem Forensics, Reverse Engineering* — Feb 2026
- Recovered deleted files and metadata from raw BTRFS disk images by parsing the superblock, walking the chunk tree to map logical to physical addresses, and traversing B-trees for inodes and directory entries.
- Reassembled files across 3 extent types (inline, compressed, and regular) while validating CRC32C checksums to guarantee forensic integrity.

KK Society | *Next.js, Spring Boot, PostgreSQL, TypeScript, Docker, Auth0* — May 2025 – Dec 2025
- Audited and enforced Role-Based Access Control and rate limiting across 90+ API endpoints to mitigate broken access control and improve resilience against DoS attacks.
- Integrated the RazorPay payment gateway and a state-tracked service request workflow, streamlining collections and request visibility for 970 society members.

Incident Response and Malware Analysis | *Volatility 3, Wireshark, Kali Linux, Python* — Nov 2025
- Identified indicators of compromise (IOCs) including hardcoded C2 URLs and malicious hashes through static malware analysis using strings, exiftool, and Detect It Easy.
- Conducted memory forensics using Volatility 3 to identify malicious processes and extract network artifacts.

Skills

Languages: Python, Java, C/C++, SQL, Bash, PowerShell, TypeScript
DevSecOps: GitLab CI, GitHub Actions, Docker, Semgrep, Bandit, Trivy, Checkov, Gitleaks, SAST/DAST, Prometheus, Grafana, Azure
Security Tools: Burp Suite, OWASP ZAP, Nessus, Nmap, Wireshark, Volatility 3, Autopsy, OWASP Top 10, OWASP ASVS
Infrastructure & Identity: Active Directory, Entra ID (Azure AD), Keycloak, Auth0, RBAC, Sophos XGS, OPNsense, VLAN Segmentation, Linux
Frameworks & Tools: Next.js, React, FastAPI, Spring Boot, PostgreSQL, Redis, Git