RAHIL SAHU

APPLICATION SECURITY ENGINEER | PRODUCT SECURITY | SECURITY ARCHITECTURE | VAPT

Indore, Madhya Pradesh, India • +91 8770456536 • rahilsahu2000@gmail.com
LinkedIn • GitHub • Portfolio

PROFILE

Application Security Engineer and penetration tester with 4+ years securing web applications, mobile applications (Android/iOS), REST APIs and network infrastructure through Vulnerability Assessment and Penetration Testing (VAPT). Identified, validated and reported 700+ security vulnerabilities — including Remote Code Execution (RCE), privilege escalation, broken access control and business logic flaws — mapped to the OWASP Top 10 and OWASP API Security Top 10.

Sole security owner for a RegTech SaaS organization, accountable for the full application security and product security program: offensive security testing, Secure Software Development Lifecycle (Secure SDLC) integration of SAST, DAST and SCA, vulnerability management, security architecture review, security operations and compliance. Operates Wazuh SIEM, Cloudflare WAF, SentinelOne EDR/CSPM and DefectDojo; secures cloud workloads across Microsoft Azure and AWS; and drives CVSS-based, risk-prioritized remediation aligned to ISO/IEC 27001, GDPR and third-party risk management.

CORE COMPETENCIES

APPSEC	Web Application Penetration Testing, Application Security Assessment, API Security Testing (REST), Mobile Application Security Testing (Android/iOS), Secure Code Review, Security Architecture Review, Secure Software Development Lifecycle (Secure SDLC), shift-left security, DevSecOps toolchain integration, OWASP Top 10, OWASP API Security Top 10
ARCHITECTURE	Security architecture and design review, attack-surface analysis, and data-flow analysis, authentication architecture (JWT, MFA/TOTP), authorization and RBAC design, API authorization, secure file-upload design, session management, encryption and sensitive-data protection, security-by-design
OFFENSIVE	Vulnerability Assessment and Penetration Testing (VAPT), black-box / grey-box / authenticated testing, network and infrastructure penetration testing, vulnerability scanning, exploitation and post-exploitation, privilege escalation (Windows and Linux), reconnaissance and OSINT, phishing simulation and social engineering
VULN CLASSES	SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Insecure Direct Object Reference (IDOR), Server-Side Request Forgery (SSRF), XML External Entity (XXE), Remote Code Execution (RCE), broken access control, broken authentication and session management, security misconfiguration, sensitive data exposure, business logic flaws
AST TOOLING	Static Application Security Testing (SAST) — SonarQube, SonarCloud | Software Composition Analysis (SCA) — Snyk, CodeAnt.ai | Dynamic Application Security Testing (DAST) — Burp Suite Professional, Acunetix, Nuclei
VULN MGMT	DefectDojo vulnerability management, CVSS scoring and risk-based prioritization, remediation tracking and SLA management, false-positive triage, retesting and closure validation, technical and executive vulnerability reporting
SECOPS	Security Information and Event Management (SIEM) — Wazuh on Docker | Endpoint Detection and Response (EDR) and Cloud Security Posture Management (CSPM) — SentinelOne | Web Application Firewall (WAF) — Cloudflare | VirusTotal threat intelligence, log monitoring, threat detection, alert triage, security incident response
CLOUD & INFRA	Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), cloud security assessment, secure server deployment and hardening, secure configuration review, Privileged Access Management (PAM) — JumpServer, OpenRport, Docker, Kali Linux, Windows Server, MySQL database security
GRC	ISO/IEC 27001, GDPR, HIPAA, Third-Party Risk Management (TPRM) and vendor security assessment, client security questionnaires, risk assessment and treatment, security policy and standards, security awareness and secure coding training
TOOLING	Burp Suite, Nmap, Nessus, Acunetix, Wireshark, Metasploit Framework, SQLMap, Nuclei, HTTPx, MobSF, Frida, Objection, Subfinder, Amass, CloudBrute, WinPEAS, AccessChk, GoPhish, Evilginx, Git, Python (security automation), Java

SECURITY ARCHITECTURE & DESIGN REVIEW

Design-phase security ownership — architecture review and control definition before code is written.

– Review product security architecture and proposed designs, identifying gaps across authentication, authorization, data flows, APIs and application components, and recommending controls before implementation.

– Designed and reviewed JWT-based authentication architecture covering token lifecycle, expiration, refresh-token handling, signature validation, claims design, key management and secure token storage.
– Performed security architecture review of multi-factor authentication (MFA) implementations, assessing enrollment, verification flows, OTP/TOTP handling, recovery mechanisms, session binding and bypass scenarios.
– Reviewed file upload architecture and specified controls for file-type validation, content inspection, size restrictions, secure storage, access control, filename handling and prevention of malicious file execution.
– Define security requirements and architectural controls for role-based access control (RBAC), least privilege, session management, API authorization, encryption and sensitive-data protection.
– Review trust boundaries and data flows to surface broken access control, IDOR/BOLA, privilege escalation, authentication bypass and insecure direct object access at design time rather than in production.
– Partner with development and product teams during the design phase to embed security-by-design principles, and maintain reusable security design patterns for authentication, authorization, API security and file handling.

PROFESSIONAL EXPERIENCE

Penetration Tester • TeamLease RegTech Pvt. Ltd. May 2024 – Present

Sole information security resource — full ownership of application security, security operations and compliance.

– Own the organization's end-to-end application security and product security program as its only security engineer, spanning offensive security testing, vulnerability management, Secure SDLC, security operations, cloud security and compliance.
– Perform VAPT on web applications, Android and iOS mobile applications and REST APIs against the OWASP Top 10 and OWASP API Security Top 10, using Burp Suite Professional for web and API security testing and MobSF, Frida and Objection for mobile application security testing.
– Identified, validated and reported 86 Critical and 194 High-severity vulnerabilities, including Remote Code Execution, privilege escalation and broken access control; prioritized findings by CVSS score and drove risk-based remediation that measurably reduced critical and high exposure.
– Embedded Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and Software Composition Analysis (SCA) into the software development lifecycle using SonarQube, SonarCloud, Snyk and CodeAnt.ai — shifting vulnerability detection left and reducing security defects reaching production.
– Administer DefectDojo as the central vulnerability management platform, consolidating manual penetration testing, automated scanning, SAST and SCA findings into a single tracked remediation workflow with owner assignment and closure validation.
– Deployed and configured Wazuh Security Information and Event Management (SIEM) on Docker with VirusTotal threat-intelligence integration for centralized log collection, threat detection, alert triage and incident response; operate Cloudflare Web Application Firewall (WAF) to protect production web applications and SentinelOne EDR with CSPM for endpoint and cloud posture management.
– Manage cloud infrastructure security and secure server deployments in Microsoft Azure; implemented hardened remote access through JumpServer Privileged Access Management (PAM) and OpenRport, reducing exposed administrative attack surface.
– Completed and managed 300+ Third-Party Risk Management (TPRM) assessments and client security questionnaires, unblocking enterprise deals and evidencing ISO/IEC 27001-aligned control maturity.
– Serve as primary technical liaison for external VAPT engagements, owning vulnerability validation, false-positive triage, developer remediation guidance and retest sign-off.
– Run phishing simulation and social engineering campaigns with GoPhish and Evilginx, deliver secure coding training to engineering teams, and evaluate WAF and Data Loss Prevention (DLP) solutions through vendor security assessments and proof-of-concept testing.

Cyber Security Analyst • Softude Infotech Pvt. Ltd. Sep 2022 – May 2024

– Conducted Vulnerability Assessment and Penetration Testing (VAPT) across web applications, mobile applications and APIs aligned to the OWASP Top 10, producing detailed technical vulnerability reports and executive summaries for technical and non-technical stakeholders.
– Managed day-to-day information security operations, including security monitoring, vulnerability remediation tracking and enforcement of security policies and secure configuration standards.
– Designed and automated secure data backup, encryption and cloud transfer workflows using Python and AWS services, strengthening data protection, confidentiality and recoverability.
– Acted as primary point of contact for external VAPT engagements, including retesting and remediation validation to confirm effective closure of reported findings.
– Participated in ISO/IEC 27001 audits and ensured application and process alignment with GDPR requirements; executed GoPhish phishing simulations and led secure coding training for development teams.

Java Developer Intern • Collexa Technologies Pvt. Ltd. Aug 2021 – Nov 2021

– Built Java applications on object-oriented design principles — including a modular Library Management System with structured exception handling — plus core data structures and algorithms; software development grounding that underpins current secure

code review and developer-facing remediation work.

PROJECTS

Vibe coded, GUI-first tools. Security tooling is used for authorised testing in my own lab and on in-scope engagements.

- **StudyFree GPT** — Free education ecosystem for Indian competitive-exam aspirants, built to optimize for learning outcomes rather than engagement metrics. Student and admin roles, built-in syllabus with per-topic progress tracking, AI-generated study roadmap that adapts to the student's learning patterns. No AI model is hosted — students supply their own API keys (Gemini for current affairs, OpenAI for tutor mode) and unlock only the features they want. All data encrypted at rest, credentials hashed, student API keys stored encrypted and scoped per user; architected to scale from MVP to an enterprise-grade platform without a rewrite.
- **Bulk URL Checker (GUI)** — Accepts URL lists from CSV, XLSX or TXT, requests them concurrently, and records status codes, response headers and timings into a detailed report, with optional automated proof-of-concept screenshots per URL.
- **Malicious File Generator (GUI)** — Embeds test payloads into arbitrary file types to exercise file-upload controls end to end: extension allow-lists, MIME and magic-byte validation, antivirus and sandbox scanning, and post-upload handling.
- **RLO Filename Spoof Generator (GUI)** — Generates filenames carrying the Unicode right-to-left override character (U+202E) to demonstrate extension-spoofing (MITRE ATT&CK T1036.002) against upload filters and mail clients, and for phishing-awareness demonstrations.
- **File Size Inflator (GUI)** — Pads any file type with dummy data to a target size to test upload size limits, client-side versus server-side enforcement, WAF request-body caps and storage-quota handling.
- **Ad Blocker Extension (Chromium)** — Request-filtering browser extension blocking roughly 80% of ad placements, built to understand rule matching and request interception inside the browser extension pipeline.
- **Meeting Attendance Recorder (Chromium)** — Captures the attendee roster of a live browser-based meeting — participants, total head count and per-person dwell time from join/leave timestamps — and exports it as an attendance register.

OPEN SOURCE — GITHUB

Public, MIT-licensed and tested — github.com/RahilSahu.

- **Aegis Security Platform** — The verification layer for scanner output: ingests Nuclei, ZAP, Burp and generic JSON/CSV findings, dedupes the same issue across tools, and verifies each finding with deterministic, non-destructive checks before AI triage; the AI can never set the verification status. Evidence-grade reports (Markdown, HTML, JSON) with a retest loop that diffs fixed, persistent and regressed findings. Python, FastAPI, CI-tested.
- **AdaptiveChat** — LLM chatbot that sets its own temperature per message, with prompt-injection and PII guardrails in both directions and LangGraph orchestration. Document chat (RAG) with cited sources and a bring-your-own-key web UI; live demo at adaptivechat.vercel.app.
- **Distributed Task Queue** — Production-shaped task broker in pure Python standard library: priority and FIFO leasing with owner-checked ack, fail and heartbeat, exponential-backoff retries into a dead-letter queue, delayed jobs and atomic JSON persistence.
- **Cloud Misconfiguration Scanner** — Unauthenticated public-exposure checks plus offline analysers for AWS, Azure, GCP and OCI policies, security groups and firewalls; concurrent fleet mode with JSON reporting.
- **Zero-Dependency Security Tools** — Ten single-purpose Python tools: HTTP security headers checker, TLS certificate inspector, DNS and email-auth checker, JWT analyzer, CORS misconfiguration checker, bulk URL checker, port scanner lite, RLO filename spoofer and upload test-payload generators — each with offline unit tests.
- **AppSec Field Notes** — Original engineering blog from real engagements: HTTP security headers audit, file-upload testing checklist, JWT audit walkthrough, SPF/DKIM/DMARC from the attacker's side, and RLO filename spoofing.
- **Community** — Reviewer for the OWASP Cheat Sheet Series: reviewed and approved a community pull request at the maintainer's request (November 2026).

CERTIFICATIONS

- Certified Ethical Hacker (CEH) — EC-Council | Aug 2024 – Aug 2027 | ID ECC1859370462
- Certified AppSec Practitioner (CAP) — The SecOps Group | Feb 2023 | ID 7040395
- Certified Cloud Security Practitioner – AWS (CCSP-AWS) — The SecOps Group | May 2023 | ID 7476871
- Modern Log Management Fundamentals and Practices — Purple Academy | Aug 2023

EDUCATION & LANGUAGES

B.Tech, Computer Science and Engineering • ADINA Institute of Science and Technology 2018 – 2022

Languages: English — professional proficiency • Hindi — native proficiency