

# Parth Padhiyar

## Senior Cybersecurity Consultant | Penetration Testing | Application Security

Ahmedabad, India | Open to global opportunities and international relocation

parthpadhiyar0x01@gmail.com | +91 73831 32738

linkedin.com/in/parthpadhiyar-060646125 | github.com/SubZ3r0-0x01

Portfolio: subz3r0x01.mywire.org

### PROFESSIONAL SUMMARY

---

Senior Cybersecurity Consultant at EY with 5+ years of experience in vulnerability assessment and penetration testing (VAPT) across web applications, APIs, mobile, cloud, networks, and source code. Combines hands-on testing and published vulnerability research with engagement delivery, technical quality reviews, and executive reporting. Builds and operates full-stack security platforms outside of client work (RBAC, multi-tenant, AI-driven scanning) and mentors analysts, translating validated findings into actionable remediation for enterprise and financial-sector clients.

#### Career impact across employer and independent engagements:

**750+ assessments | 3,000+ findings reported | 3 published CVEs | 25+ analysts trained and mentored | ~40% faster delivery with AI-assisted workflows**

### PROFESSIONAL EXPERIENCE

---

#### EY | Apr 2025 - Present

##### Senior Consultant | Sep 2026 - Present

Previously Consultant | Apr 2025 - Sep 2026

- Lead penetration testing engagements across enterprise web applications, REST and GraphQL APIs, and backend systems, validating authentication, authorization, and business-logic weaknesses.
- Test OAuth2/OIDC, session handling, and access controls to demonstrate authentication bypass, insecure direct object references (IDOR), and privilege escalation.
- Assess Android and iOS applications using Frida and MobSF, including certificate-pinning bypass, secure-storage analysis, and runtime instrumentation.
- Review Java and .NET source code for OWASP Top 10 issues; assess AWS IAM, S3, and network configurations for exposure and misconfiguration.
- Lead technical reviews of assessment reports and testing methodology, maintaining finding quality and communicating business impact and remediation priorities to client stakeholders.
- Support risk-based vulnerability management using Qualys, HCL AppScan, and VMDR, combining technical findings with executive-level reporting.

#### iAppSecure Solutions Pvt. Ltd.

##### Senior Security Analyst / Researcher / Consultant

Jun 2021 - Mar 2025

- Delivered security assessments using dynamic, static, and interactive application security testing (DAST, SAST, IAST) across web, API, mobile, and network systems.
- Led Java and .NET source-code reviews, wrote custom detection rules, and developed instrumentation-based testing methods to investigate application security weaknesses.
- Built and deployed [SharePointDirBuster](#) to identify anonymously accessible pages and access-control gaps in Microsoft SharePoint deployments.
- Supervised and mentored a team of 5-10 security analysts, coordinated client communication, and guided the resolution of critical findings.
- Served as a dedicated security consultant for a financial-sector client from Jan 2024 to Mar 2025, owning security assessment delivery and stakeholder coordination.

## EARLIER EXPERIENCE

---

### The South International School

#### IT Manager | Jun 2018 - Jun 2021

- Designed and deployed LAN/WAN infrastructure, VLAN segmentation, routing, switching, firewalls, and Active Directory for centralized authentication and policy management.
- Managed website hosting, SSL, patching, and backups; performed vulnerability assessments to protect systems and student information.

## TECHNICAL SKILLS

---

**Offensive security:** Penetration testing, red teaming, manual exploitation, business-logic testing, OWASP Top 10, attack-surface assessment, Active Directory, privilege escalation.

**Application and API security:** REST, GraphQL, OAuth2/OIDC, JWT, authentication, authorization, session management, secure code review (Java, .NET), DAST, SAST, IAST.

**Mobile and cloud:** Android, iOS, Frida, MobSF, runtime instrumentation, certificate-pinning bypass, AWS (IAM, S3, EC2, VPC), configuration and network security assessment.

**Security tools:** Burp Suite, Nessus, Qualys, HCL AppScan, VMDR, Checkmarx, Veracode, Nuclei, Subfinder, ffuf, SQLMap, TruffleHog, Gitleaks.

**Engineering and automation:** Python, PowerShell, TypeScript/Node.js, Linux, Git, Docker, CI/CD security (Jenkins, GitLab CI, GitHub Actions), AI-assisted triage and report generation, agentic AI VAPT automation, LLM API integration (OpenAI/Anthropic-style providers) and offline/local LLM deployment for data-sensitive environments, multi-tenant platform engineering (RBAC, SSO/SCIM).

**Delivery and leadership:** Engagement ownership, technical report reviews, risk-based remediation, executive communication, analyst training, and mentoring.

## SECURITY RESEARCH AND PUBLICATIONS

---

Identified three vulnerabilities in production frameworks and published technical analyses:

- **CVE-2024-48814** - SQL injection in Silverpeas CMS.
- **CVE-2024-55470** - Authentication bypass in Oqtane Framework.
- **CVE-2024-55471** - Insecure direct object reference (IDOR) in Oqtane Framework.

Technical write-ups: [parthpadhiyar0x01.medium.com](https://parthpadhiyar0x01.medium.com)

## SELECTED SECURITY TOOLS AND PROJECTS

---

- **Valkyrie (private, active development):** Self-hosted VAPT orchestration platform covering the assessment lifecycle end to end - intake, assignment, execution, findings, evidence, and client reporting - with RBAC and multi-tenant support.
- **Valxcan - AI-Based API Security Testing (private, not yet published):** AI-driven engine flagging known CVEs/CWEs on APIs instantly, plus a deeper AI assessment pass; model-agnostic (hosted LLM API or offline/local LLM), live-verified against real targets.
- **Valxcan - Automated Mobile Penetration Testing Pipeline (private, not yet published):** End-to-end automated mobile VAPT pipeline (Android and iOS), live-verified against real targets.
- **Valxcan - Agentic Web VAPT (private, not yet published):** Automated web application VAPT driven by AI agents, live-verified against real targets.
- **Burp Proxy Viewer (private, Python):** Exports Burp Suite proxy traffic to Postman collections, with a 13-scanner security dashboard (JWT analysis, header/CORS checks, CVE correlation, SSL/TLS scanning) and AI-assisted analysis.
- **PenTest Report Generator (JavaScript/Node.js):** Provides structured finding capture, evidence handling, AI-assisted drafting, and multi-format report export.
- **PyServeX (Python, published on PyPI):** Lightweight LAN file server with QR-code pairing and authentication for access from outside the LAN.
- **llama.cpp.Fuzz (Shell, AFL):** Scripted, interactive fuzzing setup for llama.cpp, applying memory-safety testing techniques to LLM inference infrastructure.

## EDUCATION AND PROFESSIONAL DEVELOPMENT

---

### M.Sc. Cyber Security | National Forensic Sciences University

Jul 2019 - Jun 2021

### Bachelor of Computer Applications (BCA) | Govt. BCA College, Gujarat University

Jul 2015 - Jul 2018

**Professional development:** OSCP preparation - in progress.