# PRATIK SANJAY KHAIRNAR

**Web Penetration Tester (VAPT) | CEH v13**

Pune, Maharashtra, India | +91 87999 81052 | pratik.khairnar.sec@gmail.com

linkedin.com/in/pratik-khairnar-sec | github.com/pratik-khairnar-sec | pratikkhairnarsec.web.app

## PROFESSIONAL SUMMARY

CEH v13-certified final-year B.Tech (Cyber Security & Forensics, CGPA 7.42/10) focused on manual web application and REST/GraphQL API VAPT, backed by custom offensive tooling: Burp Montoya API extensions (Java 17/21) and statistical blind-SQLi and headless-browser XSS engines (Python). Handled evidence on 15+ live cybercrime and multi-lakh financial fraud cases with the Nashik Police Cyber Cell under ISO/IEC 27037. Reports follow OWASP Top 10, WSTG v4.2, ASVS v4.0 and CVSS v3.1, with deterministic PoCs.

## PROFESSIONAL EXPERIENCE

**Penetration Testing Intern (VAPT)** | Cyber Warfare Intelligence Lab (OPC) Pvt. Ltd. *Nov 2026 - Present*

- **Web & API Security Testing:** Perform manual testing of authorised web applications, APIs and networks for OWASP Top 10 flaws: injection, broken authentication, access control (IDOR/BOLA), XSS, SSRF and security misconfiguration.
- **Recon & Scanning:** Map attack surface and entry points using Nmap, Nessus/OpenVAS, OWASP ZAP and Burp Suite.
- **Verification & Reporting:** Manually validate scanner findings, remove false positives and prove impact with reproducible PoCs (Burp Suite, SQLMap, custom scripts); rate with CVSS v3.1, map to OWASP Top 10 and report with evidence and remediation.
- **Retesting & Collaboration:** Support senior testers, retest fixes to confirm closure and follow scope and rules of engagement.

**Cyber Crime & Digital Forensics Intern** | Cyber Police Station, Nashik Police Commissionerate *Jan 2026 - May 2026*

- **Live Investigations:** Assisted officers on 15+ live cybercrime, intrusion, identity theft and multi-lakh financial fraud cases; acquired, hashed and preserved evidence under ISO/IEC 27037 chain of custody.
- **PCAP & C2 Reconstruction:** Analysed Wireshark captures to rebuild malicious TCP/HTTP sessions, uncover beaconing and isolate C2 infrastructure and payload delivery paths.
- **CDR/IPDR Forensics:** Correlated CDR/IPDR records (across NAT timestamps) with bank transaction logs to trace fraudulent payment gateways; aided charge sheet preparation.
- **APK Reverse Engineering:** Triaged malicious Android APKs with Jadx/Apktool; extracted hardcoded C2 endpoints, SMS-interception permissions and IOCs for CERT-In.

## PROJECTS - OFFENSIVE SECURITY TOOLING

- **AUTHENTIX Enterprise v3.0.0 (Java 17/21, Montoya API):** Burp extension with asynchronous traffic analysis and a 3-way differential IDOR engine (Attacker, Victim, Admin) with soft-200 disambiguation; 34 deterministic invariants (OTP replay, session fixation, JWT alg:none/key confusion) chained into 16 account-takeover paths; live detection of 30+ credential patterns.
- **TaintQL v2.0.0 (Python 3, Playwright):** GraphQL auditor parsing query ASTs for introspection exposure, depth limits and batching bypasses; intercepts client mutations at runtime; Burp proxy routing, JSON output, 27/27 pytest tests passing.
- **BlindStrike v7.0.0 (Python 3):** Blind SQLi framework that baselines latency and filters network jitter using IQR bounds (Q3+1.5*IQR); multi-threaded time/boolean extraction on MySQL, PostgreSQL, MSSQL, Oracle and SQLite.
- **Reflectra v7.0.0 (Python 3, Headless Chrome):** 2,600+ context-prioritised DOM XSS payloads (HTML, attribute, JavaScript) confirmed via headless dialog-event hooks (alert/prompt/confirm) to eliminate false positives.

## TECHNICAL SKILLS

**AppSec & VAPT:** BOLA/IDOR, BFLA, business logic flaws, OAuth 2.0/JWT attacks, race conditions, blind SQLi, XSS, SSRF, CORS

**API & Protocols:** REST auditing, GraphQL (introspection, depth tampering, AST), WebSockets, gRPC triage, HTTP smuggling

**Engineering:** Java 17/21 (Montoya API, Swing), Python 3, Bash, Playwright/CDP, Docker

**OS:** Kali Linux, Android, Tails, Windows

**Standards:** OWASP Top 10 2021, WSTG v4.2, ASVS v4.0, NIST SP 800-115, CVSS v3.1, Threat Modeling, SSDLC

**Tools:** Burp Suite Pro, Postman, Nmap, SQLMap, OWASP ZAP, Metasploit, Nessus/OpenVAS, Wireshark, Jadx, Apktool, Git

**Forensics:** Chain of Custody (ISO/IEC 27037), CDR/IPDR Analysis, PCAP Analysis, APK Analysis, IOC Extraction, CERT-In Reporting

## EDUCATION

**B.Tech, CSE (Cyber Security & Forensics)** | Sandip University, Nashik, Maharashtra | CGPA: 7.42/10 *2023 - 2027*

**Relevant Coursework:** Application Security & VAPT, Digital Forensics, Network Defense, Cryptography, Reverse Engineering, SSDLC, Computer Networks, Operating Systems, Database Management Systems, Web Technologies

## CERTIFICATIONS

**Certified Ethical Hacker (CEH v13)** | EC-Council | Exam ID: ECC8042517936

**Cisco Certified Network Associate (CCNA)**