

KHANT SHAH

Cybersecurity Analyst | VAPT | Penetration Testing | Web & API Security
shahkhant13@gmail.com | +91 9898024637 | [linkedin.com/in/khant-shah](https://www.linkedin.com/in/khant-shah) | Vadodara, India

PROFESSIONAL SUMMARY

Detail-oriented Cybersecurity Analyst with hands-on experience in Vulnerability Assessment and Penetration Testing (VAPT) across web, API, mobile, and network environments. Delivered 7+ end-to-end penetration testing engagements independently, uncovering critical vulnerabilities including a 0-click account takeover (CVSS ~9.0) and authentication bypass flaws. Proficient in OWASP Top 10 standards, CVSS scoring, proof-of-concept (PoC) development, and responsible disclosure. Additional background in full-stack web development enables a developer-aware approach to vulnerability assessment and secure design.

TECHNICAL SKILLS

Penetration Testing: Web Application, API, Mobile, Network (Black Box & White Box)

Security Tools: Burp Suite, OWASP ZAP, Nikto, Metasploit, Nmap, Netcat, Wireshark

Frameworks & Standards: OWASP Top 10, CVSS Scoring, Responsible Disclosure, Risk Assessment

Reporting: VAPT Reports, Proof-of-Concept (PoC) Creation, Vulnerability Management, Remediation Roadmaps

Development: React JS, Express JS, Node.js, PHP, MySQL, MongoDB, WordPress, WooCommerce, Tailwind CSS

Other: Threat Analysis, Secure Coding Practices, Technical Documentation

WORK EXPERIENCE

Cybersecurity Analyst Intern | **Invesics Cyber Forensics** | *Feb 2025 – Present* Vadodara

- Independently completed 7+ end-to-end penetration testing projects across web and API applications, performing both black box and white box assessments.
- Discovered a 0-click account takeover vulnerability (CVSS score ~9.0); produced full PoC, coordinated responsible disclosure, and recommended session-binding and token validation fixes.
- Identified authentication bypass flaw in production login flows enabling unauthorized account access without credentials; delivered CVSS-scored VAPT report and remediation roadmap.
- Conducted comprehensive vulnerability assessments aligned with OWASP Top 10 standards, uncovering critical and high-impact vulnerabilities across client environments.
- Produced professional technical documentation including CVSS-scored reports, PoC write-ups, and mitigation strategies for each engagement.

WordPress Developer | **Swiss Tech** | *Jul 2024 – Jan 2025* Vadodara

- Designed and developed custom WordPress themes and plugins meeting unique client requirements across multiple industry verticals.
- Built, updated, and maintained responsive, SEO-friendly websites; integrated WooCommerce and custom payment gateways for e-commerce clients.
- Developed dynamic, data-driven web applications using Core PHP; applied secure coding practices to reduce injection and authentication vulnerabilities.

Web Development Intern | **DotTech** | *Jun 2023 – Dec 2023* Vadodara

- Gained hands-on experience in modern web development using React JS, Express JS, Tailwind CSS, HTML/CSS, JavaScript, MySQL, and MongoDB.
- Built and deployed dynamic, responsive full-stack applications; strengthened problem-solving and coding skills through real-world project implementation.

KEY PROJECTS & FINDINGS

- **Discovered session fixation flaw leading to full account takeover with no user interaction. Produced PoC, coordinated responsible disclosure, and recommended session-binding and token validation fixes.**0-Click Account Takeover (CVSS ~9.0):
- **Identified logic flaw in production login flow allowing account access without valid credentials. Delivered CVSS-scored report with remediation roadmap.**Authentication Bypass:
- **End-to-end penetration testing across web and API applications; strong track record of identifying critical vulnerabilities and producing actionable security reports.**7+ Independent VAPT Engagements:

EDUCATION

B.E. Computer Science & Engineering — Babaria Institute of Technology, Vadodara 2021 – 2024

Diploma in Computer Engineering — RMS Polytechnic, Vadodara 2018 – 2021

SSC (10th) — Urmi School, Vadodara 2016 – 2017

CERTIFICATIONS & LEARNING

Received Certifications:

NPTEL: Blockchain & its Application (IIT)

EC-Council: SQL Injection Attacks

Forage Mastercard: Cybersecurity Job Simulation

Forage TATA: Cybersecurity Job Simulation

Udemy: OWASP Top 10 For Mobile Application 2025 Edition

Actively pursuing: eLearnSecurity Junior Penetration Tester (eJPT)