KHRISH DOSHI

Vadodara, India • +91 7990741233 • khrish007.123@gmail.com
github.com/Dev-Khrish • linkedin.com/in/khrish-doshi-6a1b6a320/

Profile Summary

Curiosity-driven offensive security practitioner specializing in web application pentesting and VAPT. Strong attacker-first mindset with deep reconnaissance habits, manual validation of vulnerabilities, and experience uncovering real-world flaws across production systems. Persistent learner with a hybrid recon + exploitation workflow and a growing track record of impactful findings.

Technical Skills

Pentesting & Recon: Burp Suite, Nmap, Masscan, Subfinder, Nuclei, Katana, JSSCanners, Eyewitness, FFUF, Arjun, SQLmap (basic)
Offensive Techniques: Reconnaissance, endpoint mapping, logic flaw discovery, JS analysis, parameter tampering, IDOR testing, authentication bypass, basic reverse engineering
Vulnerability Areas: XSS (reflected/DOM), IDOR, CORS misconfigurations, open redirects, SQLi (basic), rate-limit bypass, API issues
Languages (Reading/Debugging): Python, JavaScript, Java, C, Bash, PHP, SQL, JSON
Tools & Systems: Linux, Git, Docker (GUI), dnSpy, traffic analysis
Interests: Web app security, bug bounty, VAPT, IoT security

Security Experience & Findings

Payment Logic Manipulation – Food Delivery Platform

- Identified parameter tampering enabling unauthorized price manipulation while still returning valid payment gateway responses.
- Discovered flawed server-side validation; responsibly disclosed issue.

Reverse Engineering POS Software & Cloud Database Exposure

- Reverse-engineered a VB-based POS system using dnSpy and uncovered hardcoded SQL credentials inside a cloud-sync executable.
- Used credentials to access the central SQL database exposing sensitive customer and billing data.
- Reported to vendor; credentials were rotated and software patched.

University System Vulnerability Research

- Found exposed WebSocket endpoints leaking student information.
- Identified parameter pollution enabling extraction of event registration data.
- Discovered insecure API allowing manipulation of student payment-status fields.

General Application Testing

- Reported vulnerabilities across 5–8 applications through platforms like HackerOne and Bugcrowd.
- Repeatedly found XSS, open redirects, CORS misconfigurations, IDORs, and logic flaws using a hybrid manual–automation workflow.

Education

B.Tech in Computer Science Engineering 2023–2027
Parul University — 6th Semester, CGPA: 7
Certifications: DSA (Apna College), Web Development (Apna College)

Strengths

Attacker-first mindset; deep-dive recon approach; rapid learning through experimentation; hybrid testing methodology; strong intuition for abnormal system behavior; persistence in analysis.