Krish Modh

rmodh4@gmail.com | linkedin.com/in/krish-modh | github.com/KrishModh | krish-modh-portfolio.vercel.app | Vadodara, India

Summary

Application Security-focused Computer Science undergraduate with hands-on experience in full-stack web development, API security, and vulnerability research. Skilled in identifying authentication flaws, insecure API design, and OWASP Top 10 vulnerabilities through a build-break-fix methodology. Seeking to apply developer intuition and security analysis skills to protect large-scale applications at Google.

Technical Skills

Application Security: OWASP Top 10, Burp Suite, Authentication & Authorization Flaws, API Security Testing, Threat Modeling, Secure Code Review, Defensive Coding
Programming Languages: Python, JavaScript, C, C++, Java
Web & Backend: Node.js, React, Flask, Django, FastAPI, REST APIs, HTML/CSS
Databases: MySQL, SQLite, MongoDB, Oracle SQL
Tools & Platforms: Burp Suite, Postman, Git, GitHub, VS Code, Linux (Kali, Ubuntu), CLI
Certifications: Cybersecurity Fundamentals, Oracle Cloud Infrastructure 2025 AI Foundations Associate, JavaScript, Introduction to Python

Projects

Hostel Management System | *Python, Flask, MySQL, Role-Based Access Control*

- Built a full-stack multi-role web application with secure session management and role-based access control (RBAC) to restrict unauthorized data access across admin, staff, and student roles.
- Implemented secure authentication flows including hashed password storage and session expiry, mitigating common auth vulnerabilities (OWASP A07:2021 – Identification and Authentication Failures).
- Performed self-audit of the application for IDOR, privilege escalation, and SQL injection vulnerabilities; patched all identified issues with parameterized queries and strict access enforcement.

Password Manager | *Python, Cryptography, SQLite*

- Designed a local credential management system with AES encryption for stored secrets and a master-password architecture to prevent plaintext credential exposure.
- Applied secure storage principles including key derivation (PBKDF2) and salted hashing, directly addressing OWASP A02:2021 – Cryptographic Failures.

API-Driven To-Do Application | *Flask, REST API, SQLite*

- Developed a RESTful backend with token-based authentication; analyzed API endpoints for Broken Object Level Authorization (BOLA/IDOR) and broken function-level authorization flaws.
- Applied input validation and error-handling best practices to prevent information leakage and injection attacks through API responses.

Weather Application | *JavaScript, React, REST API Integration*

- Integrated third-party REST APIs with secure API key management and client-side input sanitization to prevent XSS and injection through user-controlled inputs.

Security Research & Learning

OWASP Top 10 – Self-Directed Vulnerability Research

- Actively studying and mapping OWASP Top 10 (2021) vulnerabilities — including Injection, Broken Access Control, Cryptographic Failures, and Security Misconfiguration — through hands-on lab environments.
- Practicing web application penetration testing techniques using Burp Suite (Proxy, Repeater, Intruder) to intercept, manipulate, and analyze HTTP traffic.
- Analyzing real-world CVEs and public bug bounty reports to understand exploit chains in authentication, session management, and API security.

Education

Parul University Vadodara, India

Bachelor of Technology in Computer Science *June 2024 – April 2028*

- Relevant Coursework: Data Structures, Operating Systems, Database Management, Computer Networks, Object-Oriented Programming.
- Self-directed specialization in Application Security, Web Security, and Secure Software Development.

Certifications

Oracle Cloud Infrastructure 2025 Certified AI Foundations Associate | Cybersecurity Fundamentals | JavaScript | Introduction to Programming Using Python | HTML and CSS