Vivek Sharma

Email: college0912@gmail.com • **Address:** Bardoli, Gujarat, India
GitHub: github.com/VivekSharma0502 • **LinkedIn:** linkedin.com/in/viveksharma0502

Profile

IT diploma student focused on blue-team security and detection engineering. Built GapScan, an open-source scanner for leaked keys and backend misconfigurations, and a home SOC lab with Wazuh SIEM that closed 4 detection gaps and cut alert noise by ~77%. Security lead on an award-winning AI interview platform. Seeking a 6-month internship in SOC, security operations or cybersecurity.

Projects

GapScan — Open-Source Security Scanner Nov 2026
github.com/VivekSharma0502/gapscan · FastAPI, Celery, Redis, PostgreSQL, Next.js
- Built a self-hostable scanner for websites, GitHub repos and Firebase/Supabase backends, with plain-language findings and A+ to F grades.
- Scanned full git history for leaked keys through a GitHub App and gitleaks, storing only redacted fingerprints, never the secret.
- Ran read-only checks for open Supabase tables, public Firebase storage and admin keys in frontend code; linked a key leaked in a repo to the live site's backend as one critical finding.
- Added an SSRF guard on every outbound request, domain-ownership verification and rate limiting; raised my own site from D 48 to A+ 98.

Home SOC Lab — Detection Engineering with Wazuh SIEM Nov 2026
github.com/VivekSharma0502/home-soc-lab-wazuh
- Built a 3-VM SOC lab (Wazuh 4.14 SIEM on Ubuntu, Windows 11 endpoint with Sysmon, Kali attacker) on an isolated network.
- Simulated 7 attack techniques (port scan, SMB brute force, encoded PowerShell, backdoor admin, scheduled-task persistence) mapped to MITRE ATT&CK.
- Found and closed 4 detection gaps with 5 custom detection rules, including catching a persistence technique that bypassed Microsoft Defender.
- Root-caused an invisible port scan to two default settings (Windows audit policy, Wazuh agent event filter) and fixed both.
- Cut idle alert noise by ~77% (140 to 33 alerts/hour) with 6 validated tuning rules and eliminated all level-15 false positives.

Conlatus — AI Screening Interview Platform (Security Lead) 2026
1st Runner-up, AI Web Gen competition · FastAPI, Next.js
- Led security for a 3-person team: anti-cheat with tab-switch detection, gaze tracking (face-api.js) and copy-paste blocking.
- Locked interviews inside Safe Exam Browser with a custom config; direct browser access is rejected (HTTP 403).
- Tested and hardened the app against prompt injection, IDOR and broken access control.

ESP32 Smart Climate Monitor — IoT 2026
- Built an ESP32 temperature and humidity monitor with a DHT11 sensor and 16x2 LCD (4-bit mode); MQTT publishing in progress.

VaultX — Zero-Knowledge Password Manager 2026
- Encrypts credentials in the browser (PBKDF2 with 600,000 iterations + AES-GCM) before they reach the database, with per-user access rules, auto-lock and clipboard clearing.
- Also built LinkNest, a bookmark manager; both use Firebase and are deployed on Vercel.

Education

Diploma in Information Technology 2024 – Present
N. G. Patel Polytechnic (GTU)
- **CGPA:** 7.96

SSC (10th Standard) 2024
Vatsalya Vidhyalaya

Training, Certifications & Achievements

Cybersecurity Essentials — Cisco Networking Academy Jun – Jul 2026
- Network hardening with firewall/ACL rules in Packet Tracer, cryptography and hashing, Linux administration, malware basics.

CS50's Introduction to Cybersecurity — Harvard University In progress

1st Runner-up — AI Web Gen competition, Vivesmruti (RNGPIT Engineer's Day) 2026

Technical Skills

- **Security operations:** Wazuh SIEM, Sysmon, Windows Event Logs, detection rules & correlation, MITRE ATT&CK, alert triage & tuning, Microsoft Defender
- **Application security:** gitleaks secret scanning, SSRF prevention, Firebase/Supabase rules & RLS, security headers, SPF/DMARC/CAA
- **Offensive / network tools:** Kali Linux, Nmap, NetExec, Wireshark, Cisco Packet Tracer (firewall, ACLs)
- **Systems:** Linux (Ubuntu, systemd), Windows 11, PowerShell, Bash, VirtualBox
- **Programming:** Python, Java, C, JavaScript, SQL, HTML/CSS
- **Platforms:** Git/GitHub, FastAPI, Next.js, Firebase, Supabase (PostgreSQL), MySQL, Vercel, Celery, Redis, Docker, Cloudflare, GitHub Apps & webhooks

Languages

English (Proficient) • Hindi (Fluent) • Gujarati (Native)