Tushar Kumar Saini

Vadodara, Gujarat | +91-96605 70234 | tusharsaini6378@gmail.com
LinkedIn Profile | GitHub: Ghost19-ui

Professional Summary

Third-year B.Tech Computer Science student specializing in Cybersecurity through the **Quick Heal Industry Embedded Program**. Adopts a "breaker" mindset to understand system vulnerabilities and strengthen defenses. Passionate about the intersection of **Artificial Intelligence, Hardware Security, and VAPT**. Currently developing AI-driven defense engines and offensive hardware toolkits. Seeking a 6-month internship in VAPT, SOC Analysis, or Network Security.

Education

Parul University — Vadodara, Gujarat
Bachelor of Technology in Computer Science (Cybersecurity Specialization) — *Aug 2023 – Present*

- Expected Graduation: June 2027
- **Relevant Coursework:** Network Security, Digital Forensics, Ethical Hacking, Offensive Security Lifecycle.

Technical Skills

Vulnerability Assessment: OWASP Top 10, Reconnaissance, Attack Surface Mapping, Phishing Simulations
Security Tools: Nmap, Burp Suite, Metasploit Framework, Wireshark, Hashcat
Hardware Security: BadUSB (Digispark/Linux/Android), HID Payloads, Offline Cracking Rigs
Defense Concepts: Network Defense, Intrusion Prevention Systems (IPS), Zero-day Anomaly Detection

Key Projects

WADE – Web AI Defense Engine (Formerly SentinAI) | *AI Defense*

- Designed a browser-centric **AI-based Intrusion Prevention System (IPS)** that scores pages and URLs in real-time.
- Moves beyond static signature matching to detect zero-day phishing attempts and malicious sites.

AAPE – Adaptive AI-Powered Penetration Toolkit | *Offensive Hardware*

- Engineered a dual-mode **BadUSB device** (HID + live-boot Kali) for realistic USB attack demonstrations.
- Integrated with the **Dual USB Ecosystem** (AAPE-RED + SHIELD-AI) to simulate Red/Blue team scenarios.

Intelligent Web Honeypot | *Defensive Lab*

- Developed a defensive lab environment to trap SQL Injection and Brute-force attackers.
- Automated the logging of IP addresses, geolocation, and behavioral patterns to auto-block malicious traffic.

Offline Password Cracking Rig | *Hardware Lab*

- Conceptualized and built a budget-friendly **GPU rig** for experimenting with **Hashcat**.
- Focused on wordlist research, custom rule creation, and high-speed hash cracking experiments.

Cybersecurity Tool Development | *Scripting & Analysis*

- **Port Scanner:** Built a reconnaissance tool to scan hosts for open ports and enumerate services.
- **Brute-Force Simulator:** Developed a tool to study online password attacks and rate-limiting policies.
- **Hashed Password Cracker:** Created a tool to demonstrate the risks of weak passwords using wordlists.

Certifications & Training

Quick Heal Industry Embedded Program — Parul University
Cybersecurity Specialization — *2023 – Present*

- Intensive training focused on the offensive security lifecycle, digital forensics, and applied defense strategies.