Raghav Sharma

Cyber Security Enthusiast | CRTA · CNSP · Microsoft SOC Analyst Associate

wrk.raghav@gmail.com | +91 8077808259 | Ghaziabad, Uttar Pradesh

linkedin.com/in/heyraghav | github.com/hey-raghav | heyraghav.in

PROFESSIONAL SUMMARY

B.Tech CSE student (ABESIT) with CRTA, CNSP, and Microsoft SOC Analyst Associate certifications, hands-on experience in VAPT, AI/ML security tooling, and web application penetration testing. Active bug bounty contributor with published CVEs and hands-on offensive security research. Built two security tools (WAPT_AI, ReconMind).

WORK EXPERIENCE

Cybersecurity Intern — ENCODERSPRO PRIVATE LIMITED (Remote) *Jun 2025 – Jul 2025*

- Performed VAPT against staging environments, identifying OWASP Top 10 vulnerabilities with CVSS-based risk ratings; delivered prioritised remediation reports.
- Ran black-box network penetration tests (Nmap, Metasploit) to enumerate services and validate firewall rules; conducted OSINT across 10+ targets.

PROJECTS

WAPT_AI – AI-Powered Web Application Penetration Testing Framework *Mar 2026 – Present*

github.com/hey-raghav/WAPT_AI

- Built Sentinel, a live traffic-interception dashboard (Burp Suite + mitmproxy) for manual/automated pentesting, analyzing every request/response via Claude to surface HIGH/CRITICAL findings.
- Researched LLM-driven vulnerability detection across 23+ vuln classes (SQLi, XSS, SSTI, JWT) using Claude/Gemini/Ollama for payload generation; multi-threaded across 50+ endpoints/session.

ReconMind – Autonomous Recon Engine *May 2026 – Present*

github.com/hey-raghav/ReconMind

- 5-phase pipeline: subdomain enum → live host probing → crawling → Nuclei sweeps → screenshots; ~70% reduction in manual recon time.
- Integrated Claude API to automate threat prioritisation and generate security finding reports.

CVE / SECURITY DISCLOSURES

CVE-2026-75916, CVE-2026-75917 & CVE-2026-82653 — SiYuan Desktop *Aug 2026*

- Identified and disclosed two stored-XSS-to-RCE vulnerabilities (CVSS 8.4) in SiYuan via unescaped block metadata rendered in the block-reference hint popup and file-tree tooltip, chained with Electron's nodeIntegration for OS command execution.
- Also found a stored HTML/script injection (CVSS 8.9): unescaped bazaar package names rendered via confirmDialog() into innerHTML, executing attacker JavaScript when a user uninstalls a malicious package.
- Coordinated disclosure via GitHub Security Advisories (GHSA-5prr-vgxq-69g9, GHSA-jjq3-3942-x99r, GHSA-hvwp-43j9-4xgf).

CVE-2026-75916 · CVE-2026-75917 · CVE-2026-82653

TECHNICAL SKILLS

Networking: TCP/IP, HTTP/HTTPS, DNS, SSH, FTP, JWT
Security Monitoring: Log Analysis, Splunk, Risk & Compliance Assessment, Incident Response
Security Tools: Burp Suite, Nmap, Metasploit, Nuclei, Wireshark, Searchsploit
AI/ML Security: LLM Integration, AI-driven Threat Detection, Prompt-based Payload Generation
Offensive: VAPT, Network Pentesting, OSINT, CVE Research, Risk Rating
Frameworks & Methodologies: OWASP Top 10, MITRE ATT&CK
Programming: Python, Bash, PowerShell, JavaScript, HTML, CSS
OS / Cloud: Kali Linux, Ubuntu, Windows 11, AWS
Platforms & VCS: TryHackMe, HackTheBox, PortSwigger Web Security Academy, Git, GitHub

CERTIFICATIONS

Microsoft Certified: Security Operations Analyst Associate *August 2026 | Active*

Certified Red Team Analyst (CRTA) — CyberWarFare Labs *February 2026 | Active*

Certified Network Security Practitioner (CNSP) — The SecOps Group *January 2026 | Active*

EDUCATION

B.Tech. – Computer Science and Engineering *Oct 2023 – May 2027*

ABESIT, Ghaziabad, Uttar Pradesh | In Progress