SAHIL ANIL NIKAM

VAPT Analyst | Web Application Penetration Testing | Vulnerability Assessment | OWASP

Nashik, Maharashtra, India ● +91 8329935878 ● sahilnikam133@gmail.com
Portfolio: hackwithsahil.vercel.app ● linkedin.com/in/sahil-nikam ● github.com/sahilnikam2410
Immediate joiner — open to relocation: Pune / Mumbai / Bengaluru / Hyderabad / Gurugram

CEH + WAPT Certified | **OWASP Top 10** Hands-On | **3-Month** Security Internship | **Cyber 50** Founder

PROFESSIONAL SUMMARY

B.Tech Computer Science graduate (2026, CGPA 8.53) with hands-on offensive and defensive security experience across web application penetration testing, vulnerability assessment and red-team attack simulation mapped to MITRE ATT&CK. Formally certified in **CEH** and **WAPT** through the SevenMentors SOC Analyst Program, alongside Networking, Linux and Python modules. Practical exposure to WAPT methodology on DVWA and lab targets, SQL injection, reconnaissance with Nmap, traffic analysis with Wireshark and security configuration assessment. Dual-sided perspective from SOC internship experience, translating attacker TTPs into detection and remediation guidance.

CORE TECHNICAL SKILLS

Offensive Security / VAPT ▸ Web Application Penetration Testing (WAPT), Vulnerability Assessment, OWASP Top 10, SQL Injection, Session Hijacking Analysis, Reconnaissance & Enumeration, Red-Team Attack Simulation, Exploit Testing in Authorised Labs

Tools ▸ Nmap, Wireshark, Burp Suite, DVWA, Kali Linux Toolset, VirtualBox, Wazuh, Splunk, Sysmon

Defensive Crossover ▸ MITRE ATT&CK Mapping, Detection Engineering, Security Configuration Assessment, System Hardening, IDS & Honeypot Deployment, Incident Response

Networking ▸ TCP/IP, DNS, HTTP/HTTPS, CCNA Fundamentals, Network Scanning, Protocol & Traffic Analysis

Reporting & Scripting ▸ Structured Vulnerability Reporting, Remediation Guidance, Python (automation and tooling), Bash, C, C++, Java

CERTIFICATIONS

> **SOC Analyst Program — SevenMentors Pvt. Ltd.** — certified in all five modules, including **CEH (Certified Ethical Hacker)** and **WAPT (Web Application Penetration Testing)**, plus **Networking**, **Linux** and **Python for SOC**.

- TATA Cybersecurity Analyst Job Simulation — Forage (2024)
- Cybersecurity — Tech Mahindra Foundation / Skill India (2024)
- IT Security Foundations: Network Security — LinkedIn Learning (2025)
- Ethical Hacking: SQL Injection — LinkedIn Learning (2024)

PROFESSIONAL EXPERIENCE

SOC Analyst Intern (Offensive & Defensive)
Mar 2026 – Jun 2026

ESCOSS LLP

- Ran security configuration assessments across Windows and Linux endpoints, identifying misconfigurations and hardening gaps and documenting remediation guidance.
- Investigated attack activity including brute-force attempts, tracing attacker technique through to impact and authoring structured technical reports.
- Deployed and administered Wazuh SIEM and implemented Splunk, gaining direct visibility into how exploitation attempts surface in defender telemetry.
- **Internship certified by the COO and Director.**

Founder & Security Lead
2024 – Present

Vrikaan — AI Threat Detection Platform (vrikaan.com)

- Lead security engineering for a consumer platform: phishing and scam detection, real-time monitoring and dark-web exposure scanning.
- Analysed live phishing and social-engineering campaigns and converted attacker techniques into automated detection and classification logic.

Cyber Security Intern
Aug 2023 – Sep 2023

Academor Online E-Learning Services Pvt. Ltd.

- Performed network scanning and reconnaissance with Nmap; analysed phishing, DoS/DDoS and session-hijacking techniques from a defensive perspective; completed cryptography and ethical-hacking labs on Kali Linux.

KEY PROJECTS

The Silent Operator — Red-Team Simulation & Detection Lab
Final-Year Project ● 2025–2026

- Executed controlled red-team attacks against a multi-host lab (Windows 10, Kali Linux, VirtualBox), mapped each technique to MITRE ATT&CK, then validated whether defences detected them — exposing and closing gaps.

Protocol Cinema — Covert-Channel C2 Research
Security Research ● 2025

- Studied a steganographic command-and-control technique tunnelling data through public APIs in an authorised lab, then translated the attacker TTPs into detection logic for covert exfiltration, mapped to MITRE ATT&CK.

Protocol Honeypot — Intrusion Detection System
Security Project ● 2025

- Built a honeypot and network IDS to attract, capture and analyse real reconnaissance and unauthorised access attempts, profiling attacker behaviour into actionable alerts.

EDUCATION

B.Tech, Computer Science & Engineering
2022 – 2026 ● CGPA 8.53 / 10

Sandip University

Programming: Python, C, C++, Java, Bash ● **Languages:** English (Professional), Hindi (Native), Marathi (Native)