Bhakta Sharma

Aspiring Penetration Tester · Cybersecurity Researcher

Alipurduar, West Bengal, India bhaktabsharma@gmail.com bhaktabsharma.github.io/Portfolio
linkedin.com/in/bhaktabsharma github.com/bhaktabsharma tryhackme.com/p/bhaktabsharma

PROFESSIONAL SUMMARY

Computer Science and Engineering student and aspiring cybersecurity researcher focused on web application security, penetration testing, bug bounty reconnaissance and digital forensics. Builds security tools and practice labs, documents TryHackMe challenges as writeups, and is working toward the EC-Council CEH v12 and CHFI certifications. Open to cybersecurity opportunities, security research and meaningful collaborations.

EDUCATION

Bachelor of Technology (B.Tech), Computer Science and Engineering

Alipurduar Government Engineering and Management College (AGEMC)

Pursuing · currently in the 3rd semester (November 2026)

Diploma in Civil Engineering

2021 – 2024

Cybersecurity self-study

TryHackMe, EC-Council study material, NVH Digital Forensic program

2023 – Present

CYBERSECURITY SKILLS AND TOOLS

Web application security — Injection, XSS, access control and authentication flaws studied in local labs. Burp Suite, OWASP ZAP, SQLMap, Nikto, Gobuster, ffuf, Wappalyzer.

Reconnaissance and enumeration — Subdomain, live host, port, URL, JavaScript endpoint and parameter discovery. Nmap, Recon-ng, Maltego, subfinder, httpx, katana, ffuf, nuclei.

Penetration testing (lab environments) — Windows exploitation, Active Directory attacks and Linux privilege escalation on TryHackMe. Metasploit, Hydra, John the Ripper, Hashcat, BloodHound, Mimikatz, Netcat, Searchsploit, LinPEAS and WinPEAS, Kali Linux.

Digital forensics — Evidence handling, memory, disk and network analysis. Autopsy, Volatility 3, FTK Imager, Wireshark, Sysmon, Osquery.

Malware analysis (static triage) — Ghidra, YARA, pefile, VirusTotal.

Network monitoring and defence (SOC) — Wireshark, Snort, Zeek, NetworkMiner, Splunk, Wazuh, Elastic Stack (ELK), Aircrack-ng.

Programming and automation — Python, Bash, JavaScript, TypeScript.

Tools listed are those used or studied in labs, TryHackMe rooms and personal projects. No proficiency ratings are claimed.

PERSONAL PROJECTS

Bug Bounty Recon Engine github.com/bhaktabsharma/BugBounty-Recon-Engine

Automates the first mile of a bug bounty engagement — turns a domain into a structured attack-surface map in one self-contained, checkpointed Bash script that can be safely killed and resumed.

Stack: Bash, subfinder, httpx, nmap, katana, ffuf, nuclei

Automated Recon & Enumeration Toolkit v2.0 github.com/bhaktabsharma/ReconForge

Modular recon framework for authorised testing and lab practice.

Stack: Python 3.8+, DNS Enum, Port Scanner, Subdomain BF, HTML Report

SQL Injection Practice Lab github.com/bhaktabsharma/SQL-INJECTION-LAB

A full-stack SQL injection playground for repeatable local practice.

Stack: React, TypeScript, Vite, Node.js / Express, SQLite

Faultline — Local Web Hacking Lab github.com/bhaktabsharma/Faultline-Web-Security-Labs

36 hands-on web application vulnerability labs across three difficulty tiers.

Stack: Node.js, Express, JavaScript, Local-only

ReconQL — Dorking & Recon Search Engine github.com/bhaktabsharma/ReconQL-Passive-Recon-Console

A Google-dorking recon search engine for bug bounty hunting, covering subdomain enumeration, API discovery, parameter discovery, exposed files, and login panels.

Stack: JavaScript, Google Dorking, GitHub Pages

Crawlspace — Attack Surface Discovery github.com/bhaktabsharma/Crawlspace-Attack-Surface

An attack-surface discovery taxonomy and query generator, built as a recon checklist so nothing gets missed while scoping a target.

Stack: HTML5, JavaScript, Static Site

CaseFile — Personal Security Wiki github.com/bhaktabsharma/CaseFile

A personal security knowledgebase covering techniques, tools, and lessons learned across labs and CTF challenges — structured for fast recall mid-lab.

Stack: JavaScript, Knowledgebase, Static Site

XSS Bugs Lab github.com/bhaktabsharma/XSS-Bugs-Lab

Deliberately vulnerable React, Vue, and Next.js environments for XSS practice, so each framework's own quirks get proper attention.

Stack: React, Vue, Next.js, SQLite

PRACTICAL ACHIEVEMENTS

- TryHackMe: Top 1% globally, 200+ rooms completed and a 250+ day streak (profile snapshot, last verified 11 Nov 2026).
- TryHackMe learning paths completed: Jr Penetration Tester and SOC Level 1 (2024). In progress: Red Teaming and Cyber Defence.
- Published 6 detailed CTF writeups (Blue, Internal Windows, Memory Forensics, Pickle Rick, PCAP Analysis, AD Penetration) and 12 TryHackMe room notes on the portfolio site.
- Published 8 open-source security tools and practice labs on GitHub.

CERTIFICATIONS

NVH Digital Forensic (3-month program), Grade A+

NewVersionHacker · Issued 8 June 2026 · valid till 9 June 2028 · Certificate no. CN-NVHDF26B07002AB

Ethical Hacking 101: Beginners Guide to Ethical Hacking

Simplilearn SkillUP · Issued 12 June 2026 · Certificate code 10338271

TryHackMe learning paths: Jr Penetration Tester, SOC Level 1

TryHackMe · 2024

Certified Ethical Hacker (CEH v12)

EC-Council · In progress, not yet earned

Computer Hacking Forensic Investigator (CHFI)

EC-Council · In progress, not yet earned

LANGUAGES

English, Bengali, Hindi