

# Suyash Shrestha

## Cybersecurity Graduate

Anamnagar, Kathmandu • 9814261900 • xuyash55@gmail.com

 @ <https://github.com/blackrabbit1x0>  @ <https://www.linkedin.com/in/suyash-shrestha-b72a1019a/>

Cybersecurity graduate specializing in Vulnerability Assessment and Penetration Testing (VAPT). Experienced in conducting structured security assessments in lab environments using industry tools and frameworks such as OWASP Top 10 and MITRE ATT&CK. Active CTF competitor with strong analytical and technical investigation skills. Passionate about identifying security weaknesses and delivering practical remediation strategies.

## EXPERIENCE

---

### Cybersecurity Lab Analyst (Academic / Personal Lab)

*Softwarica College Lab Environment*

Mar, 2024 - Present

- Conducted full vulnerability assessment workflow (Recon → Enumeration → Exploitation → Reporting) in controlled lab environments.
- Identified and validated SQL Injection, XSS, authentication bypass vulnerabilities.
- Documented findings using structured VAPT reporting format (Executive Summary, Risk Rating, Remediation).

### CTF Competitor – Hack@Sec CTF Team

*Hack@Sec*

Jan, 2024 - Present

- Participated in international Capture the Flag (CTF) competitions focused on network analysis, cryptography, and log-based challenges.
- Performed technical investigation of security scenarios under time constraints.
- Collaborated with team members to analyze vulnerabilities and propose solutions.

## EDUCATION

---

### Secondary Education Examination

Birgunj

*Kanchanjunga Senior Secondary School*

Apr, 2004 - Jan, 2019

### Higher Secondary

Kathmandu

*Liverpool International Secondary School*

Jul, 2019 - Mar, 2021

### BSc (Hons) Ethical Hacking and Cybersecurity

Kathmandu

*Softwarica College of IT and E-Commerce*

Mar, 2023 - Present

Focused on cybersecurity principles, ethical hacking, and digital forensics with practical lab-based learning. Developed strong skills in penetration testing, network defense, and secure system design.

## PROJECTS

---

### Red-Team Adversary Simulation (G0130)

Simulated end-to-end penetration testing scenarios following MITRE ATT&CK framework in a controlled lab environment. Conducted reconnaissance, privilege escalation testing, and documented findings with remediation recommendations.  
<https://github.com/blackrabbit1x0/Red-Team-Adversary-Simulation-G0130->

### Hardwarica-C2

Developed a controlled post-exploitation simulation tool to understand persistence techniques and system vulnerabilities. Focused on analyzing security weaknesses and defensive considerations.  
<https://github.com/blackrabbit1x0/Hardwarica-C2>

### LexVault-PKI

Built a secure authentication and encryption system using RSA and AES-GCM to understand cryptographic controls, key management, and secure communication protocols.

<https://github.com/blackrabbit1x0/LexVault-PKI>

## PhishSense

Designed an AI-based phishing detection application to identify malicious email patterns and suspicious indicators, demonstrating understanding of email security and threat prevention mechanisms.

<https://github.com/blackrabbit1x0/Phishsense>

## Event-Triggered Exam Forensics Framework

An ethical, invigilator-controlled digital forensics framework designed to support post-event investigation of suspected academic misconduct in computer-based examinations—without continuous surveillance or invasive monitoring.

<https://github.com/blackrabbit1x0/event-triggered-exam-forensics>

## ACHIEVEMENTS

---

### Hack@Sec CTF Team – National & Global Ranking

Member of Hack@Sec, Nepal's top-ranked cybersecurity CTF team.

Ranked 1st nationally and Top 50 globally on CTFtime.org (2025) through participation in international Capture the Flag competitions.

### 1st Place – Softwarica Hackfest 2025

Secured 1st place in a competitive cybersecurity challenge covering network analysis, cryptography, and log-based investigations. Demonstrated strong analytical thinking, problem-solving ability, and practical understanding of security concepts under time-constrained conditions.

### 3rd Place – Softwarica Hackfest v2.0 2025

Earned 3rd place in a competitive cybersecurity event featuring network security, log analysis, and system-based challenges. Showcased strong analytical skills and the ability to identify and interpret technical indicators effectively.

## TRAINING/CERTIFICATIONS

---

### SOC / Blue Team Training

2025

*TryHackMe*

Completed hands-on SOC and blue team labs focusing on log analysis, alert investigation, and incident response fundamentals using simulated environments.

### Security Monitoring & Log Analysis

2025

Practical exposure to Windows Event Logs, Linux system logs, and basic security event investigation in controlled lab environments.

### MITRE ATT&CK & Threat Simulation

2026

*Online Self-Paced Training*

Studied attacker techniques and defensive mapping using the MITRE ATT&CK framework to understand detection strategies and response planning.

### Security Training & Labs

2026

*Online Self-Paced Training*

Hands-on experience configuring and analyzing logs using Wazuh and Splunk in simulated lab environments.

## SKILLS

---

Linux Administration, Vulnerability assessment, MITRE ATT&CK Mapping & Threat Intelligence Integration, Wazuh (SIEM & host-based monitoring – lab setup), Web application security testing (OWASP Top 10), Basic exploitation techniques (lab environment), Networking & Protocol Analysis

## LANGUAGE

---

Nepali, English, Hindi, Japanese

