Noor Elahi Ali Shibly

Cybersecurity Analyst

+880 1739-339099
shibly6@gmail.com
linkedin.com/in/shibly6
github.com/Shibly6
noorelahialishibly.com

Motivated B.Sc. in Software Engineering graduate with a major in Cybersecurity, seeking an entry-level role where I can apply my skills in enterprise vulnerability assessment and security analysis.

EDUCATION

B.Sc. in Software Engineering
Major: Cybersecurity

Daffodil International University
Relevant Coursework: Network Security, Cryptography, Secure Software Engineering

CGPA: 3.74/4.00

PROFESSIONAL TRAINING

Network Security Assessment

Grameenphone Ltd.
Supervisor: Mohammad Shahadat Hossain (Principal Security Architect)

- Conducted TCP/SSL vulnerability assessment across 1,280+ IPs in enterprise infrastructure
- Discovered 4 hosts with deprecated TLS (v1.0/1.1) and SWEET32 vulnerability
- Performed multi-phase reconnaissance using Masscan, Nmap, SSLScan — identified 152 live hosts
- Developed automated Bash scripts for batch scanning and vulnerability identification

RESEARCH EXPERIENCE

Cloud Security Research
IaC Misconfiguration Detection

Daffodil International University
Supervisor: Dr. Imran Mahmud (Dept. Head, Sr. IEEE Member)

- Developed unsupervised ML framework to detect Terraform security misconfigurations
- Achieved 94% ROC-AUC with Autoencoder, 94.9% PR-AUC with Isolation Forest
- Engineered 22 security features from AWS S3 bucket configurations
- Created explainable visualization pipeline for CI/CD integration

Technologies: Python, scikit-learn, Terraform, AWS S3, Pandas | *Paper pending IEEE publication*

CYBERSECURITY PROJECTS

LiteRecon_AI — AI-Powered Reconnaissance Platform

github.com/Shibly6/LiteRecon_AI

- Built full-stack platform integrating 11 security tools (Nmap, SSLyze, Feroxbuster, etc.)
- Implemented multi-provider AI analysis with local LLMs (Ollama) and cloud APIs
- Developed automated PDF report generation with executive summaries

Tech: Python, FastAPI, React, Ollama, Nmap, Kali Linux

CVE-2025-29927 Vulnerability Lab

github.com/Shibly6/vulnerability-labs

- Built vulnerable lab for critical Next.js middleware bypass (CVSS 9.1)
- Created step-by-step Burp Suite exploitation tutorial
- Documented root cause analysis and mitigation strategies

Tech: Next.js, Burp Suite, HTTP Protocol, Web Security

TECHNICAL SKILLS

Security Tools	Nmap, Wireshark, Burp Suite, SSLScan, Bash
Web Security	OWASP Top 10, SQL Injection (SQLi), Cross-Site Scripting (XSS), Authentication Flaws
Network Security	TCP/IP, Vulnerability Assessment, Firewall Fundamentals
Programming	Python (Security Scripting), Bash, Java
Platforms	Kali Linux, Ubuntu, Windows
Methodologies	Vulnerability Assessment Process, MITRE ATT&CK Framework
Cloud	AWS S3, Terraform (Basics)

ADDITIONAL INFORMATION

Languages	Bengali (Native), English (Fluent)
Operating Systems	Kali Linux, Ubuntu, Parrot OS, Windows
Strengths	Analytical Thinking, Problem Solving, Team Collaboration, Adaptability