

# ALI NAWAZ MALIK

 +92 325 3969391  ali.malik9545@gmail.com  linkedin.com/in/ali-malik-76212a253

## PROFILE

Cyber Security undergraduate specializing in vulnerability assessment, SIEM/XDR solutions, OSINT investigations, and network defense. Proficient with leading security tools, penetration testing techniques, and incident response workflows. Experienced in building and testing secure applications, configuring security infrastructure, and conducting digital forensics. Adept at translating technical findings into actionable recommendations, with a strong focus on improving organizational security posture. Seeking opportunities to apply hands-on expertise in SOC operations, threat detection, and security engineering.

## EDUCATION

### Air University Islamabad

B.S. in Cyber Security

2022 – Present

Islamabad, Pakistan

## EXPERIENCE

### Codistan

Cybersecurity Intern

July 2025 – Aug 2025

OnSite / Islamabad

- Performed web vulnerability scans (**Nikto**, **WPScan**, **ZAP**); documented missing headers, mixed content, outdated components.
- Built vulnerable Flask app to demonstrate **SQLi** and **XSS** for developer security training.
- Conducted OSINT on suspicious IPs/domains (**Shodan**, **Nmap**, **AbuseIPDB**), WHOIS/DNS, subdomain enum, spoofed-domain checks; compiled reports.
- Installed/evaluated **Wazuh**, **Security Onion** (Suricata, Zeek) for SOC2-aligned SIEM/XDR.
- Set up **pfSense** lab; simulated **SYN flood** attacks, wrote firewall rules, verified in Wireshark/pfSense logs.
- Ran **Nessus/Nmap** scans; analyzed findings; created remediation plan (protocol hardening, credentialled scans).
- Reverse-engineered Android/iOS apps (**MobSF**, **JAD**); found hardcoded secrets, risky logging, sensitive permissions.
- Investigated **OneDrive/AggregatorHost** deletion; paused sync, restored data, hardened endpoints, collected artefacts.

### Yellow World Tech (UAE)

Cyber Security Intern

Jul 2024 – Aug 2024

Remote

- Assisted with log review, vulnerability checks, and documentation; gained exposure to SOC workflows.

## PROJECTS

### PhishDetect – ML-based URL Classifier

Python, Flask, scikit-learn

- Analyzes URL features to classify **Phishing vs Legitimate**; provides confidence score and reasons in a clean UI.

### ILA-SOC – Intelligent Log Analysis & Incident Response (FYP)

Python

- Lightweight, ML-powered log analysis platform with threat intel and dashboards for affordable SOC/SIEM use.

## SKILLS

- Security Tools:** Nikto, Nessus, ZAP, WPScan, Burp, Nmap, SQLMap
- SOC/Monitoring:** Wazuh, Security Onion, Wireshark, pfSense, Linux tooling
- OSINT/DFIR:** Shodan, AbuseIPDB, WHOIS/DNS, subdomain enum, Windows Event Viewer
- Programming:** Python (Flask), Bash, SQLite, HTML/CSS/JS, Git

## CERTIFICATIONS

### Google Cybersecurity Professional Certificate (V2)

Credential ID: A936C54ZGW7R

### HTML, CSS, and JavaScript for Web Developers – JHU

Credential ID: 62V6R24N317U

### Cryptography – ISC2

Credential ID: OVOIEWQBMFJO

### Introduction to Networking – NVIDIA

Credential ID: 9DEUZFA1WPW9