

# ZAIN ABDULLAH

Islamabad, Pakistan — House #7, Street 9, Sector A, DHA Phase 2, Islamabad  
zainabdullah394@gmail.com — +92 349 5821883 — linkedin.com/in/zainabdullah

## Profile

Dedicated and versatile **Cyber Security and Digital Forensics student** with hands-on experience in scripting, networking, and penetration testing. Proficient in identifying and mitigating security risks with a strong foundation in Linux, network protocols, and digital forensics. Currently working as a **Full Stack Developer (MERN Stack)** at **Stellix Soft LLC** since July 2025, developing and deploying secure, scalable web applications while integrating backend APIs and security best practices. Passionate about both **cybersecurity** and **software development** with growing interests in **machine learning applications in security**.

## Technical Skills

**Programming and Scripting:** Python, JavaScript (ES6+), Bash, C++, TypeScript

**Web Development:** React.js, Node.js, Express.js, MongoDB, RESTful APIs, JWT, Git, Docker

**Cybersecurity Tools:** Metasploit, Burp Suite, Wireshark, Nmap, Aircrack-ng, Ettercap

**Machine Learning:** NumPy, Pandas, Scikit-learn, TensorFlow (basic), Data Preprocessing, Model Evaluation

**Networking:** OSI Model, TCP/IP, DNS, DHCP, NAT, VLANs, Subnetting

**Authentication and Protocols:** 802.1X, EAP, RADIUS, WPA/WPA2

**Operating Systems:** Kali Linux, Ubuntu, Windows

**Automation:** Log parsing, packet filtering, vulnerability scanning, reporting

**Other Tools:** GitHub, Postman, VS Code, Docker, Microsoft Office Suite

## Education

**Bachelor of Science in Cyber Security**

**National University of Computing and Emerging Sciences (FAST-NUCES)**, Islamabad

*Expected Graduation: 2026*

## Employment History

**Full Stack Developer (MERN Stack)**

Stellix Soft LLC, Islamabad

*July 2025 – Present*

- Developing scalable web applications using React.js, Node.js, and MongoDB with secure authentication and data handling.
- Implemented REST APIs and integrated third-party services for analytics and payment systems.
- Collaborating with UI/UX designers to create responsive interfaces.
- Ensuring code quality and application security by integrating best practices in encryption, validation, and session management.

**Junior Penetration Tester Intern**

Common Criteria Office, Islamabad

*July 2024 – September 2024*

- Conducted penetration testing using Kali Linux, Burp Suite, and automation scripts.
- Wrote Python and Bash scripts to accelerate vulnerability scans and report generation.
- Authored detailed security reports with remediation guidelines.

**Lab Assistant**

FAST-NUCES, Islamabad

*August 2023 – July 2024*

- Guided students in network security labs and penetration testing.
- Configured routers, firewalls, and simulated wireless attacks.
- Assisted in automating penetration testing tasks with custom scripts.

**Teaching Assistant**

FAST-NUCES, Islamabad

*August 2021 – June 2023*

- Supported instructors in Discrete Structures, Information Security, and Artificial Intelligence.
- Assisted students with lab tasks, grading, and debugging assignments.

## Selected Projects

**1. SecureChat App (MERN Stack)** Built an end-to-end encrypted chat application with JWT-based authentication, socket.io for real-time communication, and AES encryption for message privacy.

**2. TaskFlow - Project Management Platform** Developed a full-featured task management tool with React frontend, Node.js/Express backend, and MongoDB database; implemented role-based access control and analytics dashboards.

**3. Cryptography Project** Implemented AES and RSA algorithms in Python with CLI-based key generation, encryption, and decryption modules.

**4. Penetration Testing Simulation** Created a mock enterprise network, performed exploits using Metasploit, and automated scans with Bash scripts.

**5. Wireless Security Assessment** Analyzed 802.1X traffic using Aircrack-ng and Wireshark to evaluate enterprise Wi-Fi security posture.

### **6. Small Machine Learning Projects**

- *Phishing URL Classifier*: Built a logistic regression model to classify URLs as safe or malicious.
- *Network Intrusion Detection*: Used scikit-learn to train a random forest on the KDD Cup dataset for anomaly detection.
- *Log Pattern Analyzer*: Implemented an anomaly detection script using Python for detecting irregular log patterns.

## Networking & Scripting Focus

- Designed and tested subnetted networks with VLANs and IP assignments.
- Automated port scanning, log monitoring, and backup routines via Bash scripts.
- Captured and analyzed traffic using Wireshark to understand authentication flows.
- Troubleshooted network performance using ICMP, traceroute, and DNS tools.