

Darlin Diaz Muñoz

darli2819@gmail.com | 610-329-6667

[Linkedin.com/in/darlin-diaz-munoz](https://www.linkedin.com/in/darlin-diaz-munoz) | github.com/darlin883

SUMMARY OF QUALIFICATIONS

Software Engineering student and CompTIA Security+ certified with hands-on lab experience in vulnerability scanning and web application testing. Familiar with SOC fundamentals including alert triage and log review through security labs. Strong foundation in secure coding principles and OWASP Top 10 awareness. Seeking a SOC Analyst I / Junior Cybersecurity Analyst role.

TECHNICAL SKILLS

Systems & OS: Windows, Linux (Ubuntu, Kali).

Languages: Python, Java, JavaScript, HTML/CSS, SQL, SQLite, PHP

Security Tools: Burp Suite, Wireshark, Nmap, Hydra, Gobuster, Dirb, Metasploit, Git

Security Concepts: OWASP Top 10, SQL Injection, SSRF, Vulnerability Scanning, Log Review, Alert Triage, TCP/IP

Virtualization & Homelab: Proxmox VE, VirtualBox

EDUCATION & CERTIFICATIONS

A.S. Software Engineering, Thaddeus Stevens College of Technology — Expected 2026

Certifications:

- CompTIA Security+
- CompTIA CySA+ (In progress)

PROFESSIONAL EXPERIENCE

Mary's Daycare Center, LLC | Remote

Software Engineering Intern

2026 – Present

- Configured a Linux web server to deploy an internal web application, supporting uptime, testing, and troubleshooting.
- Contributed as a software engineering intern on a web-based system, supporting backend logic, application setup, testing, and troubleshooting under guidance.

Thaddeus Stevens College of Technology | Lancaster, PA

Software Engineering Tutor

2025 – Present

- Tutored peers in core programming concepts across Python, Java, and web development.
- Mentored students to strengthen problem-solving, debugging, and cyber awareness skills.

TECHNICAL PROJECTS

Home Lab (Proxmox + AdGuard Home) | Virtualization, DNS Security

- Built a home lab using **Proxmox VE** to run isolated VMs for security learning and testing.
- Deployed **AdGuard Home** for network-wide DNS filtering and validated behavior through DNS query logs and client testing.

Burp ClusterBomb Tools | Python 3.8+, Burp Suite, SQLi, SSRF, Automation

- Built **Python automation scripts integrated with Burp Suite** to enumerate **SQL injection (boolean, error, time-based)** and test **SSRF** using **ClusterBomb payload strategies**, reducing manual testing effort.
- Implemented **proxy support, structured logging, and error handling**, and documented modular workflows in a GitHub repository to enable repeatable, authorized web security assessments.

For More Projects | darlin883.github.io/Portfolio/