ABDULELAH ALASMARI

abdulelahalasmari@hotmail.com | abdulelah.sa | **LinkedIn**: Abdulelah A. | **GitHub**: PayloadSurgeon | **Medium**: @abdulelahalasmari

PROFESSIONAL SUMMARY

Cybersecurity Engineer with hands-on experience securing applications, systems, networks, and cloud environments. Brings a strong foundation in offensive and defensive security, vulnerability management, security monitoring, and automation. Adept at identifying security gaps, assessing risk, and delivering practical improvements that strengthen organizational security posture

EDUCATION

Master of Science in Cybersecurity - Summa Cum Laude | New York University, Brooklyn, NY **January 2026**
GPA: **4.00/4.00** | Awards: Distinguished Academic Achievement Award

Bachelor of Science in Cybersecurity - Summa Cum Laude | Florida International University, Miami, FL. **April 2024**
GPA: **3.98/4.00** | Awards: **#1 Outstanding Graduate in Cybersecurity** | Enterprise IT & Cybersecurity Project Grand Prize Winner

PROJECTS/RESEARCH

- Conceived and led end-to-end development of **Privacy-Preserving Diabetes Risk Prediction** using fully homomorphic encryption; earned a Best Paper Honorable Mention at ABH 2026.
- Architected **CloudGuard**, a Spark-based threat hunting pipeline that analyzed **2M+ AWS CloudTrail** events using machine learning and MITRE ATT&CK enrichment, enabling near-real-time detection of high-confidence threats.
- Designed and developed **PhishLearn**, a phishing simulation and awareness platform that enabled controlled internal phishing campaigns, strengthening employee readiness and reducing exposure to real-world social engineering attacks.
- Directed agile delivery of **SecureHaven**, a petabyte-scale data lakehouse initiative that remediated **871+ vulnerabilities**, strengthened security compliance, and informed risk-based mitigation decisions across stakeholders.

WORK EXPERIENCE

Teaching Assistant, Penetration Testing and Vulnerability Analysis | New York University **Jan 2025 – Jan 2026**

- Evaluated **250+** red-team assessments per semester across web, network, Active Directory, and Linux labs, validating enumeration with **Nmap/Gobuster**, exploitation with **Burp Suite, Metasploit, and SQLmap**, and post-exploitation paths.
- Reviewed student red-team assessments to identify **OWASP Top 10** flaws, exposed services, weak AD controls, and privilege-escalation paths; developed remediation guidance and **MITRE ATT&CK** detection opportunities.
- Guided **150+** students through **Burp Suite, OWASP ZAP, Nmap, Metasploit, Linux enumeration, OSINT, privilege escalation, and reverse-engineering** methodology, improving technical reporting quality.

Offensive Security Researcher | OSIRIS Lab, New York University **Sept. 2024 – Jan 2026**

- Conducted web, network, and host-security research using **Burp Suite, OWASP ZAP, Nmap, Metasploit, Gobuster, SQLmap, and Python** to enumerate, validate, and document exploitable weaknesses.
- Performed exploit-development and reverse-engineering research with **C/C++, GDB, AFL-Fuzzer, Binary Ninja, and Linux**, identifying memory-corruption flaws and improving software resilience.
- Translated validated attack paths into secure-design recommendations, **MITRE ATT&CK**-mapped detections, and defensive guidance for application, network, and endpoint security teams.

OT Cybersecurity Intern | Manresa Wilds - Norwalk, Connecticut **May 2025 – Aug 2025**

- Built a web-based OT cybersecurity monitoring platform integrating **70+** Ubiquiti (UniFi) cameras and sensors, centralizing device telemetry, security events, and asset visibility to support real-time monitoring of connected environments.
- Secured the supporting network with **Nmap, Wireshark, Nessus, and Wazuh**, identifying and prioritizing exposures, anomalies, and vulnerabilities.

DevSecOps Intern | Stetson University - DeLand, Florida **Sept. 2021 – Jun 2022**

- Reviewed **50+** web applications using manual secure-code review, **Burp Suite, OWASP ZAP, SQLmap, and Nessus**, identifying **SQL injection, XSS, and OWASP Top 10** weaknesses for remediation.
- Developed **30+** dynamic websites using **PHP, SQL, HTML/CSS/JavaScript**, secure input validation, authentication controls, and safer database handling to improve security and reliability.

SKILLS

Certifications: eJPT, CompTIA Security+, CompTIA CySA+, CompTIA CSAP, MITRE eCTF 2025 (Attack Phase)
Offensive Security & AppSec: Burp Suite, Nmap, Metasploit, BloodHound, Impacket, SQLmap, OWASP ZAP, Snyk, AFL-Fuzzer
Detection Engineering & Purple Team: Splunk, Microsoft Sentinel, Wazuh, Zeek, Sigma, Atomic Red Team, Wireshark, MITRE ATT&CK
Cloud Security & Automation: AWS CloudTrail, Docker, Terraform, Kubernetes, Python, PowerShell, Bash, C/C++, Java