Muhammad Umar Ahamed Saleem

(510) 766-8962 | muhammadumarahamedsaleem@gmail.com | linkedin.com/in/umarahamedsaleem | San Jose, CA

Education

San Jose State University (SJSU) **Aug 2026 – Present**

B.S. in Engineering Technology, Computer Network System Management *San Jose, CA*

Relevant Coursework: Computer Networks (CCNA curriculum), Enterprise Networking, Network Administration, Network Security, Ethical Hacking

Certifications & Technical Skills

Certifications & Rankings: CompTIA Security+, Network+, A+, SOC Analyst (Intermediate) | #1 Enterprise Leaderboard (Immersive Labs)
Security Tools: Burp Suite Pro, CrowdStrike Falcon, Wazuh EDR, Splunk SIEM, OX Security, AWS Route 53, Ghidra, Tenable Nessus
Languages & Protocols: Python, JavaScript, Git, Bash, SAML 2.0 / SSO, TCP/IP, DNS, REST APIs
Methodologies: Vulnerability Assessment & Penetration Testing (VAPT), Application Security Mapping, Threat Modeling, MITRE ATT&CK Framework, Subdomain Takeover Prevention, OWASP Top 10

Experience

Stanford Health Care (Technology & Digital Solutions) **May 2026 – Jul 2026**

Cybersecurity Intern *Palo Alto, CA*

- Audited backend Django source code in a core clinical platform, discovering a critical flaw where omitted SAML cryptographic signature checks enabled account takeover via forged assertions.
- Co-authored vulnerability report, developed PoC exploits, and validated production patches using `python-saml`'s `process_response()` engine in staging alongside the AppSec Lead.
- Architected a multithreaded Python scanner deployed across **1,600+ enterprise cloud domains** (50 parallel threads in under 3 mins) with a 5-stage pipeline (DNS, TLS, HTTP, 3-Layer Fingerprinting) evaluating Route 53 records.
- Integrated fingerprinting engine analyzing **7,500+ hosting signatures** (AWS S3, Azure, Heroku, GitHub Pages) and engineered automated reporting (HTML, CSV, JSON) for monthly delta scans.
- Utilized Burp Suite to audit clinical workflows, map REST APIs, and evaluate access control models handling sensitive patient data.

Seagate Technology **May 2025 – Aug 2025**

Information Security Intern *Fremont, CA*

- Monitored network assets across enterprise subsidiaries using CrowdStrike Falcon, **reducing external threat exposure by 15%**.
- Executed systematic vulnerability assessments across external services, domains, and IP infrastructure, identifying and escalating **20+ critical misconfigurations**.
- Analyzed codebases and system configurations to detect architectural security weaknesses, building actionable remediation workflows that **accelerated issue resolution by 30%**.
- Documented remediation lifecycle tracking to ensure **100% of flagged vulnerabilities were resolved** within strict SLA parameters.

Projects & Cyber Ranges

Hackfinity Global CTF Competition (#108 / 2,000+ Teams) | *Burp Suite Pro, AWS CLI, Wireshark, Kali* **March 2025**

- Cleared 41 tasks (**1,305 pts**) after joining 48 hours late to place **Rank #108 / 2,000+ global teams** in a live incident response environment.
- Bypassed AI guardrails (`Evil-GPT v2`) via prompt manipulation to leak root flags, and exploited web **IDOR** vulnerabilities using Burp Suite.
- Conducted AWS CLI enumeration on Secrets Manager and exposed S3 buckets to extract sensitive credentials.
- Isolated a non-standard C2 channel in Wireshark PCAP data, detecting persistent IMAP exploits and memory-resident scheduled tasks.

PortSwigger Web Security Academy & CTF Labs | *Burp Suite, Python, Linux, Git* **Mar 2026 – Aug 2026**

- Achieved **#1 Enterprise Leaderboard ranking** on Immersive Labs across **68+ hours** of labs, earning Intermediate SOC Analyst certification.
- Practiced hands-on web vulnerability labs on PortSwigger Web Security Academy, focusing on **OWASP Top 10** risks, logic flaws, and access controls.
- Engineered a public GitHub repository detailing root-cause writeups, **PoCs**, and secure code fixes for **PicoCTF** challenges.