SAMI ALI

samiali38183@gmail.com | (571) 290-8908 | samiali38183.github.io | linkedin.com/in/sami-ali-1a4b89345 | github.com/samiali38183

PROFESSIONAL SUMMARY

Cybersecurity student (B.S. Information Technology, GPA 4.0) with hands-on experience as a Vulnerability Assessment Team intern at DHS (CBP). CompTIA Security+ and AWS Certified Cloud Practitioner; working toward OSCP. Builds Python tools for attack emulation, detection-gap measurement and injection-flow analysis, plus a localhost-only web vulnerability lab.

CORE COMPETENCIES

Python • MITRE ATT&CK • Atomic Red Team • Stratus Red Team (replayed logs) • taint analysis / SAST • OWASP Top 10 • Sigma • vulnerability management (Nessus/Tenable) • CISA KEV / EPSS / CVSS • AWS fundamentals • Docker • GitHub Actions • Git • pytest • Wireshark • Linux • Power BI

CERTIFICATIONS

Certifications: CompTIA Security+ | AWS Certified Cloud Practitioner
In progress: OSCP | AWS Certified Security – Specialty
Work authorization: U.S. Citizen

PROFESSIONAL EXPERIENCE

Vulnerability Assessment Team Analyst Intern | Dept. of Homeland Security (CBP) | Ashburn, VA | May 2026 – Aug 2026

- Matched Nessus/Tenable scan results against the CISA Known Exploited Vulnerabilities (KEV) catalog to identify high-risk systems and aged findings.
- Designed a risk-based prioritization method weighing KEV status, asset criticality, exposure, EPSS and CVSS, and benchmarked remediation against CISA BOD 26-04 timelines.
- Built a multi-page Power BI dashboard and an executive briefing on actively exploited vulnerabilities and mitigations for technical and leadership audiences.
- Wrote compliance reports and remediation recommendations aligned with the NIST Cybersecurity Framework and FedRAMP.

PROJECTS

vulnlab — Localhost web-vulnerability lab (Python, Flask)

- Three small intentionally vulnerable services (SSRF through a redirect, SQL injection in ORDER BY, IDOR), each with a test that shows the impact on loopback only, the fix, and a regression test that fails against the vulnerable version.
- Ran its own analyzer on every version (it flags the SSRF and SQL injection, false-positives on both fixes, and cannot see the IDOR) and wrote a Sigma detection per bug class, replayed on recorded logs.

tripline — ATT&CK emulation and detection-gap measurement (Python)

- Runs Atomic Red Team emulations on Linux and Windows CI runners (and replays public AWS CloudTrail logs) across 14 ATT&CK techniques, including setuid privilege escalation (T1548.001), LSASS credential dumping (T1003.001), cron persistence (T1053.003) and ingress tool transfer (T1105).
- Measured what defenders miss: the stock SigmaHQ setuid/setgid rule flagged neither recorded attack event and 0 of 108 generated variants (octal modes, clustered flags, full paths); a replacement rule catches 106. Across 251 variants of three Linux attacks the expected rules catch 200.

sinkline — Finds exploitable injection flows in Python web apps

- Static analyzer that traces attacker-controlled request data to sinks across files and flags the classes pentesters exploit: SQL and command injection, SSRF, insecure deserialization, XSS, path traversal and XXE. Each finding carries the source-to-sink path; 43 rules mapped to OWASP and CWE.
- Independent OWASP BenchmarkPython check (own scoring script): +0.52 true-positive minus false-positive rate on the 10 taint categories vs. Bandit +0.07 and Semgrep +0.04. Found and fixed a shell-injection flaw in its own GitHub Action.

kevgate — Hardened API with attack-surface tests in CI

- FastAPI vulnerability-intake service with hashed scoped API keys, rate limiting and a STRIDE threat model; CI runs an OWASP ZAP baseline scan (67 rules pass, 0 failures) and kind-cluster tests confirming a privileged pod is rejected and pod egress is denied.

EDUCATION

Bachelor of Science, Information Technology | Minor: Cybersecurity
George Mason University | Expected May 2028 | GPA: 4.0

Associate of Science, Information Technology
Northern Virginia Community College | May 2026 | GPA: 3.7