Haseeb Khalid

Newark, NJ | (862)235-6270 | haseebkhalid1507@gmail.com
linkedin.com/in/haseebkhalid1507 | github.com/haseebkhalid1507 | portfolio
Cloud Security Engineer | Zero Trust & EASM | OWASP Member

Education

New Jersey Institute of Technology — Newark, NJ
Master of Science in Cybersecurity and Privacy — *Jan 2025 – Dec 2026*

Manipal Institute of Technology — Udupi, India
B.Tech in Computer and Communication Engineering | Minor: Computational Intelligence — *Aug 2019 – Jul 2023*

Experience

Graduate Teaching Assistant – Cryptography & Security — Aug 2025 – Dec 2025
New Jersey Institute of Technology — *Newark, NJ*

- Lead TA for CS408/CS608 (Cryptography, Internet Security); graded assignments and exams on PKI, TLS/SSL, and applied cryptography for 100+ students.

Security Engineer — Jul 2023 – Oct 2024
Clouddefense.ai – *Cloud Security Platform (CNAPP)* — *Remote*

- Architected EASM product (Python/Go) automating discovery of 10,000+ cloud assets across AWS/Azure/GCP; reduced mean-time-to-detection by 65%.
- Engineered Zero Trust IAM policy engine analyzing CloudTrail logs to auto-generate least-privilege policies; reduced over-permissioned access by 78% for 50+ customers.
- Built production microservices (Spring Boot/FastAPI) with OWASP Top 10 mitigations; achieved 99.9% uptime handling 1M+ daily requests.
- Automated cloud misconfiguration remediation via custom Python scripts integrated with CNAPP platform.

Cloud Security Research Intern — Feb 2023 – Jun 2023
Clouddefense.ai – *Cloud Security Platform (CNAPP)* — *Remote*

- Analyzed 50+ malware samples and SIEM logs; developed detection rules reducing false positives by 45%.
- Automated CIS Benchmark compliance via 80+ Terraform modules; resolved 500+ misconfigurations across AWS/Azure/GCP.

Lead Security Researcher (Application Security) — Jan 2022 – Nov 2022
BugBase – *Vulnerability Disclosure & Bug Bounty Platform* — *Bangalore, India*

- Led penetration testing for 20+ enterprise clients; identified 150+ vulnerabilities (SQLi, IDOR, auth bypass) with 98% client satisfaction.
- Triaged 300+ vulnerability reports across web/mobile apps; assigned CVSS scores and coordinated remediation timelines.
- Drafted the initial ISMS documentation and achieved ISO 27001 certification by collaborating with Sprinto.

Software Engineering Intern — Aug 2021 – Oct 2021
Trailytics – *AI-Powered Analytics Platform* — *Remote*

- Developed secure REST API (Flask/MySQL) with input validation and SQLi prevention for 1,000+ daily users.
- Automated 15+ operational workflows with Python; reduced processing time by 60%.

Technical Skills

Security Domains: Cloud Security (AWS/Azure/GCP), Application Security (SAST/DAST), Penetration Testing, Vulnerability Assessment, EASM, Zero Trust Architecture, DevSecOps, Cryptography
Security Tools: Burp Suite Pro, OWASP ZAP, Nessus, Metasploit, Nmap, Wireshark, Nuclei, sqlmap, Prowler, ScoutSuite, Trivy, Snyk, SonarQube, Semgrep
Cloud & DevOps: AWS (EC2, S3, IAM, CloudTrail, GuardDuty, Security Hub), Azure (Sentinel, Defender), Docker, Kubernetes, Terraform, GitHub Actions, CI/CD
Programming: Python, Java, JavaScript/Node.js, Go, Bash, SQL, Spring Boot, FastAPI, Flask, REST APIs, JWT/OAuth 2.0

Projects

Glyph – MCP Security Scanner & Runtime Proxy | *Python, ONNX, JSON-RPC, SQLite, PyPI* 2026

- Built dual-mode MCP security platform: static config scanning (7 rules) + real-time traffic interception proxy (7 runtime rules) with response quarantine, config pinning, and ANSI sanitization; 10K LOC, 197 tests.
- Validated against real-world CVEs (Invariant Labs GitHub MCP exploit, Anthropic Git MCP RCE, marmelab PoC); achieved 83% detection on 23-vector adversarial research corpus with zero false positives.

VelociRAG – RAG Engine for AI Agents | *Python, ONNX Runtime, FAISS, SQLite, MCP* 2026

- Created open-source 4-layer retrieval engine (vector + BM25 + knowledge graph + metadata) with RRF fusion and cross-encoder reranking; no PyTorch, no GPU, no API keys. 1.5K+ PyPI downloads, 525 tests, 12K LOC.
- Engineered ONNX-powered search with sub-200ms latency, incremental graph indexing, and MCP server; published to PyPI, AUR, and the official MCP Registry with automated CI/CD across all three targets.

NiteSpeed – Security Platform for Startups | *FastAPI, Next.js, Docker, Redis, PostgreSQL* 2025

- Built API-first security platform combining web vulnerability scanning (TLS, headers, XSS) with AWS cloud posture checks and CIS compliance mapping.
- Engineered modular recon pipeline with Docker SDK orchestration, Redis job queues, and JWT authentication; achieved scan-to-findings in under 2 minutes.

Security Homelab – Self-Hosted Infrastructure | *Docker, Prometheus, Grafana, Loki, WireGuard, Nginx* Ongoing

- Built headless Linux server running 20+ Docker containers with Nginx reverse proxy, Pi-hole DNS, WireGuard VPN, and full observability stack (Prometheus, Grafana, Loki).
- Engineered AI agent orchestration platform with 12 specialized agents, 4-layer semantic search, persistent memory system, and automated CI/CD pipelines.

Certifications & Recognition

CompTIA Security+ (SY0-701) | *Active – Verification: 4f104745-9230-4395-98a5* Nov 2024

Google Cybersecurity Professional Certificate | *Coursera* Jul 2021

2nd Place – Ineuron National Hackathon | *Top 2 of 400 teams* Jun 2022

3rd Place – LokiCTF (International) | *Top 3 of 4,000+ participants* Jul 2021

Professional Engagement & Leadership

Member – OWASP Foundation | *Open Worldwide Application Security Project* Nov 2025 – Present

Head of Web Exploitation & Team Captain Oct 2019 – Sep 2022

Cryptonite – Cybersecurity Research Team, Manipal Institute of Technology

- Led 25-member team in 50+ CTF competitions globally, achieving top 10 placements in 2 international events.
- Organized niteCTF 2021: designed 20+ security challenges, managed AWS infrastructure, attracted 800+ teams from 50+ countries.
- Conducted 12+ workshops on OWASP Top 10, API security, and authentication bypass techniques for 200+ students.