MUHAMMAD SAIM ALI

Associate DevSecOps Engineer • AWS • Cloud Security • DevOps

Lahore, Pakistan • +92 300-1788055 • me.msaim04@gmail.com • LinkedIn • GitHub

PROFESSIONAL SUMMARY

Associate DevSecOps Engineer with hands-on experience in AWS cloud infrastructure, CI/CD automation, containerization, and Kubernetes orchestration. Skilled in designing scalable cloud environments using Terraform, implementing GitOps workflows, and performing web application penetration testing. Proficient in Docker, Kubernetes, GitHub Actions, ArgoCD, Helm, SonarQube, Trivy, Burp Suite, and core AWS services. Passionate about building secure, automated, and production-ready systems.

CORE SKILLS

Cloud & Infra	AWS (EC2, VPC, RDS, S3, IAM, ALB, Route53), Terraform, Linux Administration, TCP/IP, DNS, HTTPS, SSL/TLS, NAT
Containers & K8s	Docker, Kubernetes, Helm, Nginx
CI/CD & DevOps	Git, GitHub Actions, ArgoCD, Infrastructure as Code (IaC)
Monitoring	Prometheus, Grafana, Loki, Node Exporter, cAdvisor
Security	OWASP Top 10, Burp Suite, Nmap, SQLMap, Nuclei, Metasploit, Wireshark, SonarQube, Trivy, Penetration Testing, Vulnerability Assessment
Programming	Python, Bash, SQL

PROFESSIONAL EXPERIENCE

DevSecOps Engineer | **WaxonIT Solutions, Lahore** *Sept 2025 – Present*

- Designed and provisioned AWS infrastructure using Terraform, including VPC, EC2, IAM, RDS, S3, and Application Load Balancer.
- Developed CI/CD pipelines using GitHub Actions for automated build, testing, security scanning, and deployment workflows.
- Containerized applications using Docker and deployed workloads on Kubernetes clusters; managed Deployments, Services, ConfigMaps, Secrets, and Ingress configurations.
- Implemented GitOps-based deployments using ArgoCD and managed application packaging with Helm charts.
- Integrated SonarQube and Trivy into CI/CD pipelines to automate code quality checks and vulnerability scanning.
- Configured Nginx reverse proxy with SSL/TLS certificates, HTTPS redirection, and production-grade web server security.
- Built centralized monitoring and logging with Prometheus, Grafana, Loki, Node Exporter, and cAdvisor.
- Performed web application penetration testing using Burp Suite, Nmap, SQLMap, Nuclei, and custom methodologies; identified and reported critical vulnerabilities including IDOR, Authentication Bypass, OTP Bypass, and Access Control Issues.
- Applied Linux hardening, firewall policies, and IAM least-privilege principles to reduce attack surface.

KEY PROJECTS

Enterprise DevSecOps Platform (AWS + Terraform + CI/CD)

- Designed modular AWS infrastructure using reusable Terraform IaC practices.
- Built GitHub Actions CI/CD pipelines with integrated SonarQube and Trivy security scanning.
- Configured IAM policies, SSL/TLS encryption, and ArgoCD GitOps automated deployments.

Kubernetes Multi-Tier Application Deployment

- Deployed multi-tier applications on Kubernetes using Deployments, Services, ConfigMaps, Secrets, and Ingress.
- Managed releases with Helm charts; implemented autoscaling and production-grade monitoring.

Monitoring & Observability Platform

- Built a centralized monitoring and logging stack using Prometheus, Grafana, Loki, Node Exporter, and cAdvisor.
- Designed dashboards and alerting rules for proactive incident detection across cloud infrastructure.

Web Application Penetration Testing & Security Assessment

- Identified vulnerabilities including IDOR, Authentication Bypass, OTP Bypass, and Security Misconfigurations using Burp Suite, Nmap, SQLMap, Nuclei, Wireshark, and Metasploit.
- Delivered detailed security reports with prioritized remediation recommendations.

Automated Web Security Scanner (Final Year Project – In Progress)

- Developing an automated OWASP Top 10 vulnerability scanner integrated directly into CI/CD pipelines with automated reporting and remediation guidance.

EDUCATION

BS Software Engineering — **CGPA: 3.68 / 4.00**
University of Lahore — *2023 – 2026*

CERTIFICATIONS

- AWS Certified Solutions Architect – Associate
- Docker Certified Associate (DCA)
- IBM Certified Penetration Tester
- AWS Cloud Practitioner (In Progress)

ACHIEVEMENTS

- Identified and responsibly disclosed critical vulnerabilities in live production applications.
- Participated in the NADRA Bug Bounty Program.
- Secured 3rd Place in University Coding Competition.
- Built end-to-end DevSecOps pipelines integrating CI/CD, security scanning, monitoring, and cloud infrastructure automation.
- Identified critical data leaking vulnerability in University of Lahore's admission portal.