Mohammad Arif

Product Security Engineer | MS Cybersecurity Candidate
mohammadarif1@toromail.csudh.edu | Long Beach, CA | mohdarif.com
https://www.linkedin.com/in/mohd--arif/ | https://github.com/Zero0x00

Summary

Product Security Engineer with 5+ years of experience securing Web, API, and cloud-native applications through application security testing, threat modelling, and security automation. Experienced in integrating security controls into CI/CD pipelines, performing secure architecture reviews, and identifying vulnerabilities in authentication, authorization, and API workflows. Strong background in AWS security, offensive security testing, and secure software development practices.

Skills

Application Security
Web Security, API Security, Mobile Security, Threat Modeling, Secure SDLC, Vulnerability Management, OWASP Top 10

Cloud & DevSecOps
AWS Security, IAM, S3, VPC, CI/CD Security, SAST, DAST

Tools
Burp Suite, Nmap, Nessus, Checkmarx, Sonatype, Prisma Cloud, Lacework

Programming
Python, Bash, OAuth, JWT, Applied Cryptography

Emerging Areas
AI/ML Security, Adversarial Machine Learning

Experience

Poshmark Chennai
Product Security Engineer Sept 2023 - July 2025

- Implemented security review workflows across 50+ repositories to improve secure code coverage and reduce risk exposure
- Integrated SAST, API and Mobile DAST tooling into CI/CD pipelines to automate application security testing
- Conducted Design review and threat modelling for all the new functionalities shipping for production
- Identified and remediated 20+ high and critical vulnerabilities across third-party integrations and production services
- Performed Web, API, and Mobile application security assessments, reducing remediation timelines by 80%
- Hardened AWS environments by identifying IAM, S3, and network security misconfigurations
- Partnered with engineering teams to remediate vulnerabilities and improve secure coding practices
- Developed internal automation workflows integrating Checkmarx, Sonatype, and Jira for vulnerability management
- Built hands-on security labs and CTF exercises for internal engineering security training

Paytm Bangalore
Sr. Security Engineer April 2023 - Sept 2023

- Integrated application security controls into SDLC workflows and engineering release pipelines
- Conducted threat modelling and secure architecture reviews for customer-facing applications
- Performed secure code reviews and assisted developers in remediating OWASP Top 10 vulnerabilities
- Managed bug bounty program, triaged and validated 100+ valid security findings.
- Developed the Security Champion program for accelerating security culture within the organisation

Paytm Bangalore
Security Engineer June 2021 - April 2023

- Performed Web, API, Mobile, and infrastructure security testing across customer-facing applications
- Reduced critical vulnerabilities by 45% through manual testing and automated security validation workflows
- Secured CI/CD deployment pipelines in collaboration with DevOps and engineering teams
- Developed remediation playbooks and vulnerability triage workflows to accelerate security fixes
- Conducted source code reviews and security assessments for application services and APIs

Myntra Bangalore
Security Intern May 2020 - May 2021

- Conducted Web and API security testing across 30+ applications under senior mentorship

- Identified high-impact vulnerabilities and assisted engineering teams with remediation validation
- Built Jira dashboards and workflows for vulnerability tracking and SLA reporting

Projects

AWS Cross-Account Attack Path Visualization 2025 - Present
- Built a graph-based detection tool to identify cross-account attack paths across AWS Organizations.
- Modeled IAM trust relationships, role assumptions, and privilege escalation paths using Neo4j.
- Visualized risky access paths to help prioritize remediation of excessive permissions.

GitHub Actions Security Review Tool 2024 - Present
- Developed a tool to analyze GitHub Actions workflows for insecure CI/CD configurations.
- Checked workflows for risky permissions, unsafe triggers, exposed secrets, and insecure third-party actions.
- Identified misconfigurations that could enable supply chain attacks or unauthorized code execution.

CI/CD Security Build-Gating Automation 2024 - Present
- Built automation to query Checkmarx scan status and enforce security gates in CI/CD pipelines.
- Blocked merges and failed builds when high or critical vulnerabilities were detected.
- Integrated security validation into developer workflows to prevent vulnerable code from reaching production.

AI/ML Security Lab: Black-Box Fraud Detection Testing 2024 - Present
- Built an interactive machine learning security lab simulating a deployed fraud detection model.
- Tested how controlled inputs can be used to probe model behavior, infer decision boundaries, and reverse-engineer black-box predictions.
- Demonstrated model abuse risks including input manipulation, decision boundary discovery, and adversarial probing.
- Documented defensive recommendations for rate limiting, monitoring, feature hardening, and abuse-case testing.

Community & Leadership

OWASP Community Contributor

Security Conference Volunteer (BSides, Seasides)

Conducted security workshops and Capture-The-Flag (CTF) sessions

Core team member of Seasides Conference

Education

California State University, Dominguez Hills Master of Science
Cybersecurity Carson, CA • Expected Dec 2026

Awards

Best Team Player 2024
Poshmark

Superstar Award 2023
Paytm Security Team

Superstar Award 2022
Paytm Security Team

Rising Star Award 2021
Paytm Security Team

Security Researcher Hall of Fame 2019
Mastercard, Bosch, Western Union

Talks & Conferences

Speaker at Blackhat 2025
Tool Demonstration at Blackhat

Speaker at DEFCON 2025
Tool Demonstration at DEFCON (AppSec & Cloud Villages)

Speaker at cloud village at Seasides Conference 2025
"SSRF: Anatomy of a Cloud Attack (Demo with Burp Suite + AWS Metadata) & basics of Terraform"

Speaker at c0c0n Security Conference 2024
PCI 4.0, JavaScript Security for product security teams

Trainer at Seasides Conference 2023
Fundamentals of Attacking and Defending AWS Cloud