Arbaaz Mohamadiqbal Jamadar

reachout@arbaazjamadar.com linkedin.com/in/arbaazz/ github.com/arbaaz29 arbaazjamadar.com

EDUCATION

University of Maryland, College Park *Maryland, USA*
Master of Engineering in Cybersecurity (GPA: 3.70) *Aug. 2023 – May. 2025*
Relevant coursework: Offensive Security, Cloud Security, Application Security

KIT's College of Engineering, Kolhapur *Maharashtra, India*
Bachelor of Technology in Computer Science (GPA: 3.30) *Aug. 2018 – May. 2022*
Relevant coursework: Computer Networks, Cloud Computing, Operating Systems

CERTIFICATIONS

- OSCP/OSCP+
- AWS Certified Security Specialty (SCS-C02)
- CompTIA Security+
- CompTIA CySA+ (ISC2 CISSP)
- AWS Certified Solutions Architect - Associate (SAA-C03)
- eJPT

ACHIEVEMENTS

- Amazon CTF (4th Worldwide)
- Wiz (18th Worldwide)
- HackTheBox (878th Worldwide)
- YesWeHack (780th Worldwide)
- TryHackMe (Top 10% Worldwide)
- CTFTime (100th Worldwide)

WORK EXPERIENCE

Cyber Security Analyst
Chicago EAC *Nov. 2025 – Present*

- Designed and enforced API security controls across internal and external endpoints, reducing exposed attack surface from 3 endpoints to 1 (67% reduction), neutralizing injection vulnerabilities through input validation, rate limiting, and authentication enforcement, remediating 2 confirmed weaknesses.
- Led 5 STRIDE-based threat modeling sessions across application and API layers, surfacing 12+ attack paths mapped to NIST CSF; prioritized remediation by exploitability × business impact, driving 4 architecture changes (auth hardening, segmentation, secret rotation) before code reached production.

Student Assistant
University of Maryland Dining Services *Jan. 2024 – May. 2025*

- Supervised 6–8 student workers during peak service, owning task delegation, escalation, and shift handoffs in a high-throughput environment serving 1,000+ patrons/day.
- Maintained a 100% on-time opening/closing record across 16 months while balancing a full-time Master's in Cybersecurity - funded graduate studies independently.

Cloud Engineer (Cloud Security Focus) - IT Department
KIT's College Of Engineering *Jun. 2022 – Aug. 2023*

- Tuned 40+ Splunk and ELK detection rules over 6 months, cutting false-positive volume by 30% (120 → 85 alerts/day) and reclaiming an estimated 8 analyst-hours/week for high-fidelity investigation.
- Automated incident response workflows using AWS Lambda and EventBridge-triggered playbooks, achieving an 83% reduction in weekly remediation time (6 hours → 1 hour) and cutting alert noise by 20%, enabling the team to focus on high-fidelity threat detection.

Security Analyst
CyberSapiens *Nov. 2021 – May. 2022*

- Executed 10+ structured web app pentests (Burp, ZAP, Nmap, Nessus, Metasploit) against authenticated and unauthenticated surfaces; identified and validated injection and broken-auth flaws with full PoC chains, and ruled out 30+ candidate findings through manual verification - keeping report signal-to-noise high.
- Delivered 10+ client-facing pentest reports with CVSS-scored findings, reproducible PoCs, and OWASP-aligned remediation; presented results to both engineering and executive stakeholders, with 100% of critical/high findings remediated within agreed SLAs.

PROJECT EXPERIENCE

Automated IAM Threat Management [Source Code] *Dec. 2025*

- Built open-source AWS IAM auditor (Python, boto3, Neo4j) auditing 2,000+ principals in <5s; YAML rule engine maps findings to MITRE ATT&CK, scores blast radius via PMapper-integrated escalation graph, and auto-generates IR playbooks and Sigma rules with deterministic IDs.

Multi-Layer Security Architecture Implementation [Source Code] *Apr. 2025*

- Performed comprehensive architecture review and penetration testing for high-traffic e-commerce platform (10K+ users), implementing defense-in-depth across network/application/data layers with PCI-DSS compliance and Terraform-based secure network segmentation.

Application Security Pipeline [Source Code] *Dec. 2024*

- Architected comprehensive DevSecOps pipeline integrating SAST/DAST/container scanning with policy-as-code enforcement (OPA/Conftest), collaborating with development teams to achieve 98% compliance while blocking 100% of critical vulnerabilities from production.

SKILLS

Languages: Python, Bash, Go, C, KQL, SQL, JavaScript, PHP, PowerShell.
Tools & Platforms: SAST/DAST (SonarQube, Semgrep), CrowdStrike Falcon, Terraform, Wireshark, Metasploit, Splunk SIEM, Ghidra, Nessus, AWS, Microsoft Azure, GCP, Docker, Kubernetes, ELK, AWS CSPM, GitHub, Active Directory, Postman, CloudWatch, GuardDuty, Red Canary, Wiz CNAPP, New Relic, DataDog, CrowdSec, Ghidra, Docker, SentinelOne, CircleCI, OPA/Conftest, Checkov, Terraform.
Security Frameworks: NIST CSF, CIS Benchmarks, MITRE ATT&CK, OWASP, Zero-Trust Architecture, SOC 2, HIPAA, PCI-DSS.
Technical Skills: Penetration Testing, DevOps, DevSecOps, IAM, SAST, DAST, SCA, API Security, Incident Response.