USAMA ARSHAD

OFFENSIVE SECURITY LEAD · RED TEAM · FINTECH & CLOUD

Riyadh, Saudi Arabia · +966 56 913 7225 · gusama21@gmail.com
LinkedIn · GitHub · Website · Bugcrowd · Synack SRT · Medium

PROFILE

OSCP-certified Offensive Security Lead with 9+ years building and running red team, AppSec, and cloud security programs across web, mobile, API, GCP, AWS, and Kubernetes. Currently leading the offensive security function at Tabby, MENA's largest BNPL fintech, where I built autonomous VAPT pipelines, embedded AppSec into GitLab CI/CD, and hardened GKE workloads at scale. Delivered 80+ engagements for Fortune 500 and SAMA-regulated entities, published CVE-2024-3681, and represent Pakistan as a three-time national CTF champion and BlackHat MEA finalist. Recognized by Walmart, Achmea, The Sun, and the United Nations.

AREAS OF EXPERTISE

Red Team & Adversary Simulation MITRE ATT&CK, Purple Team, Physical Intrusion, OSINT, C2 Frameworks (Cobalt Strike, Sliver, Mythic), Initial Access, Lateral Movement, Persistence, Defense Evasion

Offensive Testing Web (OWASP Top 10), Mobile (OWASP MASVS, iOS / Android), API (REST, GraphQL, gRPC), Network and Infrastructure, Active Directory, WiFi, Thick Client, Source Code Review

Cloud & Container Security GCP, AWS, GKE / Kubernetes, Container Escape, IAM Privilege Escalation, Cloud Metadata Abuse, Workload Identity, Terraform IaC scanning, CIS Benchmarks

AppSec & DevSecOps GitLab CI/CD security gates, SAST, DAST, SCA, Secret Scanning, Threat Modeling (STRIDE), Secure SDLC, Code Review (Python, Go, Node, Java)

Tooling Burp Suite Pro, Frida, Ghidra, IDA, Nmap, Nuclei, Nessus, Acunetix, SonarQube, Metasploit, BloodHound, Sliver, FFUF, Sqlmap, Wireshark, custom Python and Go tooling

Compliance & Frameworks SAMA Cybersecurity Framework, PCI DSS, ISO 27001, OWASP ASVS, NIST CSF

PROFESSIONAL EXPERIENCE

Offensive Security Lead June 2025 - Present
Tabby *Riyadh, Saudi Arabia*

- Lead the offensive security function at MENA's largest BNPL fintech (14M+ users), owning red team, AppSec, and cloud security across web, mobile, API, GCP, and GKE.
- Architected and shipped autonomous VAPT dashboards integrating Jira and tracker automation, cutting assessment cycle time by 60% and eliminating manual reporting overhead.
- Run continuous red team and adversary simulations to surface real-world attack chains and pre-production exploit paths before release.
- Embedded SAST, DAST, secret scanning, and container scanning into GitLab CI/CD pipelines, gating insecure releases at merge time.
- Hardened GKE workloads via Workload Identity, network policies, admission controllers, and runtime detection across the GCP estate.
- Bridge offensive testing with secure-by-design engineering by partnering with product and platform teams from threat-modeling through release.

ISM Consultant & Team Lead August 2024 - May 2025
SecurEyes *Riyadh, Saudi Arabia*

- Led large-scale SAMA fintech security assessments covering major Saudi financial institutions, including end-to-end VAPT, source code review, and red team engagements.

- Executed full-scope red team operations spanning external and internal infrastructure, web, mobile, API, Active Directory, WiFi, physical security, cloud, and DLP / EDR evasion.
- Conducted in-depth source code reviews surfacing critical authentication, authorization, and business-logic flaws.
- Mentored a team of consultants, reviewed deliverables, and presented findings to executive stakeholders and regulators.

Senior Security Engineer December 2021 - July 2024
Ebryx *Lahore, Pakistan*

- Delivered 80+ offensive security engagements for Fortune 500 clients across penetration testing, source code review, and red teaming.
- Led a sub-team of consultants, owning project scoping, technical execution, peer review, and final report quality.
- Authored detailed reports translating complex exploitation chains into business-impact narratives for executive audiences.

Red Team Member, Synack Red Team March 2021 - Present
Synack *Remote*

- Active SRT member performing continuous vulnerability discovery and exploitation on private bug bounty targets.
- Identified high-impact vulnerabilities including IDOR, BOLA, authentication bypass, and business-logic flaws on enterprise targets.

Penetration Tester March 2018 - May 2021
Security Wall *Lahore, Pakistan*

- Reported validated vulnerabilities across 50+ client engagements covering web, mobile, and network targets.
- Built reusable internal tooling and methodologies that improved team throughput on recurring assessments.

SELECTED ACHIEVEMENTS

- CVE-2024-3681 — Original 0-day vulnerability research and responsible disclosure.
- BlackHat MEA CTF Finalist (2023, 2024) — Top 32 / 29 globally out of 250+ teams, representing Pakistan.
- Cyber Hackathon Hat-Trick (2021, 2022, 2023) — Three consecutive podium finishes in Pakistan's national CTF, awarded by the President, Prime Minister, and IT Minister.
- Hall of Fame acknowledgements from United Nations, Walmart, Achmea, and The Sun for responsibly disclosed vulnerabilities.
- Recurring speaker at universities and security conferences on offensive security and AI-driven attack automation.

SELECTED PROJECTS

SecurityWire github.com/usama0x01/SecurityWire

- Security platform combining a mobile vulnerability scanner with a web bug bounty marketplace. Companies onboard targets, researchers submit findings, validated reports trigger payouts.

AI-Driven Offensive Automation

- Internal tooling and dashboards automating end-to-end VAPT, Jira integration, and triage orchestration for offensive security teams.

CERTIFICATIONS & EDUCATION

OSCP Offensive Security Certified

HTB Offshore Hack The Box Pro Lab — Active Directory and Banking infrastructure

PEH Practical Ethical Hacker — TCM Security

CNSS Certified Network Security Specialist — ICSI

BSc. Computer Science 2018 - 2021

COMSATS University, Lahore, Pakistan · Languages: English (Professional), Urdu (Native)