Shariq Malik

Technical Lead – Wipro Arabia

Cybersecurity enthusiast with 9+ years of experience and a strong background in Penetration Testing, Application Security, Red Teaming, and Network Security. Seeking a dynamic organization where I can leverage my skills, face new challenges, and pursue growth opportunities.

+92 345 4730838
+966 545 727238
malikshariq07@gmail.com
github@shariqmalik
/in/malikshariq/
MagnitoMac

Professional Experience

Wipro Arabia

(Oct 2024 – Present)

Jubail, Eastern, Saudi Arabia

The following responsibilities involve delivering application security services to a Fortune Global 500 enterprise, with a focus on penetration testing, vulnerability management, and secure code analysis for critical business applications.

— Technical Lead / Senior Security Consultant

(On-site for a Leading Global Chemical Manufacturing Company)

- Performed advanced web, API, and mobile application penetration tests, identifying and mitigating high-severity vulnerabilities impacting critical enterprise systems.
- Conducted detailed secure code reviews across multiple technology stacks (Java, .NET, and JavaScript frameworks), ensuring compliance with OWASP Top 10 and other security standards.
- Identified and exploited complex vulnerabilities, including privilege escalation, authentication bypass, and business logic exploitation.
- Created and utilized custom scripts, payloads, and automated tools to enhance the effectiveness of security assessments.
- Conducted security assessments of third-party applications and integrations, identifying risks in external vendor components.
- Provided detailed remediation guidance to development teams, ensuring timely and effective patching of vulnerabilities.
- Delivered technical and executive-level reports, highlighting findings, proof-of-concept exploits, and actionable recommendations.
- Worked directly with client security teams to define testing scopes, methodologies, and prioritize security risks.

Ebryx LLC

(Dec 2021 – Oct 2024)

Lahore, Pakistan

The following roles and responsibilities involve working as a managed security service provider member, researching and evaluating hacker techniques, system exploits, and vulnerabilities to support red team assessment activities.

— Lead Security Engineer

- Manage and lead a team of 30+ security engineers at Ebryx.
- Conduct comprehensive penetration testing on internal and external network infrastructures, web applications, mobile applications, and cloud environments for several Fortune 500 companies.
- Perform on-site penetration testing activities for multiple clients, identifying and mitigating 95% of critical vulnerabilities.
- Execute Red-teaming engagements, including social engineering tests as required.
- Collaborate closely with other application security engineers to review and test web, conventional, and mobile applications.

- Develop technical solutions and new tools to automate repetitive tasks, improving efficiency and saving 100+ man-hours per month.
- Write detailed reports, including assessment-based findings, outcomes, and recommendations for further system security enhancements.
- Lead client communications via calls and emails, covering penetration testing scoping, execution planning, testing methodologies, reporting, and other related inquiries.

— Security Engineer

- Conducted web and mobile application penetration testing for more than 200 customers.
- Evaluated network and infrastructure vulnerabilities and conducted penetration testing.
- Reviewed source code for corporate and consumer web applications.
- Identified methods and entry points for potential exploitation of vulnerabilities.
- Introduced new testing rules to uncover vulnerabilities, increasing detection rates by 20%.

Digital Forensics Research & Services Center (DFRSC)

(Dec 2016 – Dec 2021)

Lahore, Pakistan

Roles & Responsibilities:

— Team Lead Cyber Security

- Prepared and implemented security plans.
- Managed a team of 25 members.
- Delegated tasks related to security plans.
- Developed indigenous security tools.
- Delivered security training for 80+ students and professionals, improving their understanding of security best practices.

— Security Engineer

- Conducted web application penetration testing.
- Assessed network/infrastructure vulnerabilities and performed pen-testing.
- Automated various in-house tasks, including daily summaries and reports.
- Created social media OSINT and offensive security tools.

Education

BS Computer Science

2016 - 2020

Lahore Garrison University

Core Competencies

- **Web Application Pentest:** Proficient in assessing web applications for security vulnerabilities, including SQL injection, XSS, XXE, CSRF, SSRF, SSTI, and OWASP Top Ten vulnerabilities. Experience with tools such as Burp Suite, OWASP ZAP, Nessus, Acunetix, Nikto, SQLMap, and Custom Scripts.
- **Mobile Application Pentest:** Skilled in evaluating the security of mobile applications (iOS and Android) on various platforms, identifying weaknesses, and proposing effective remediation strategies. Proficiency with tools like Jadx, Objection, MobSF, and Frida.
- **LLM / AI Application Pentest:** Experienced in assessing security risks in LLM- and AI-powered applications, including prompt injection, data leakage, insecure RAG implementations, excessive permissions, and authorization bypass in AI workflows, aligned with OWASP Top 10 for LLM Applications.
- **API Pentest:** Strong knowledge of API security testing, including authentication and authorization flaws, insecure API endpoints, and data exposure issues. Familiarity with tools like Postman and OWASP API Security Project.

- **Network Pentest:** Experienced in conducting network penetration tests, identifying vulnerabilities in network infrastructure, and recommending mitigation measures. Proficiency with tools like Nmap, Wireshark, and Metasploit.
- **Red Teaming Operations:** Extensive experience in simulating advanced cyberattacks, including social engineering, lateral movement, and persistence techniques. Skilled in conducting full-scale red team exercises to evaluate an organization's security preparedness. Experience with tools such as Cobalt Strike, Empire, Metasploit, CrackMapExec, Impacket, BloodHound, PowerView, Powersploit, Mimikatz, chisel, and PowerUpSQL
- **Cloud Assessment:** Competent in assessing the security of cloud environments, including AWS Cloud Platform. Able to identify cloud-specific vulnerabilities and recommend mitigations.
- **SAST (Static Application Security Testing):** Proficient in using SAST tools to analyze source code for security vulnerabilities, including tools like FortifySCA.
- **Vulnerability Assessment:** Capable of performing comprehensive vulnerability assessments, scanning systems and applications for potential security weaknesses, and delivering detailed reports with remediation recommendations.
- **Programming Language:** Proficient in programming languages such as C#, C, PHP, and Python. Can identify and exploit vulnerabilities in code written in these languages.
- **Scripting & Automation:** Skilled in scripting and automation using Python, BASH, BATCH, and PowerShell. Can create custom scripts for security testing and automation of repetitive tasks.

Soft Skills

- Strong analytical and problem-solving skills
- Excellent communication and team collaboration
- Quick to learn new technologies
- Detail-oriented and organized
- Proactive and self-motivated
- High ethical standards and integrity

Certifications

- Offensive Security Certified Professional (OSCP)
- Offshore (HTB Pro Lab)
- Jr Penetration Tester (PTI)
- Certified AppSec Practitioner (CAP)
- Certified Network Security Practitioner (CNSP)
- Huawei Certified Network Professional (HCNP)
- Huawei Certified Network Associate (HCNA)

Relevant Projects & Community Contributions

- **Hoaxshell:** https://github.com/t3l3machus/hoaxshell
- **Seeker:** https://github.com/thewhiteh4t/seeker
- **CrackMapExec:** https://github.com/Porchetta-Industries/CrackMapExec

Achievements

CyberHackathon Pakistan 2022

- Secured 1st position in CyberHackathon Pakistan in regional finals

CyberHackathon Pakistan 2021

- Secured 2nd position in 2 categories of CyberHackathon Pakistan in the regional finals

HackTheBox

- Due to completing many CTF challenges, was rated as an Elite Hacker on HackTheBox

Excellence & performance awards

- Secured 2nd position in Huawei ICT Skill Competition Global Final 2018
- Secured 2nd position in Huawei ICT Skill Competition Middle-East Final 2017
- Top 10 National Finalists Huawei ICT Skills Competition 2016

Acknowledgments

- Acknowledged by ESET SMART Security™ for reporting a vulnerability