

# MUHAMMAD SHAMSHAIR

+973 33797561 / + 92 342 2564131

muhammad\_shamshair@hotmail.com

<https://pk.linkedin.com/in/muhammad-shamshair-b1106b190>

<https://github.com/M-Shamshair>

## PROFESSIONAL SUMMARY

More than 10 years of working experience in Cyber Security Field. Worked on Linux based embedded system with AI (Artificial Intelligence) including hardware and software control. Very passionate to work in Vulnerability Assessment & Penetration Testing (VAPT) including security of Network, Infra, App (Web/Mobile), Cloud System and OT/ICS.

As a freelance professional, I've had the privilege of managing and successfully delivering international projects, leveraging remote collaboration to enhance my skillset. This hands-on experience has allowed me to tackle intricate challenges with innovative solutions that aren't readily available on the public internet. I also stay connected with latest technology news/blog to keep my knowledge updated.

I am currently seeking opportunity in Cyber Security field that can enable me to further elevate my skills to more professional level. My commitment to staying at the cutting edge of the industry and my proven track record of problem-solving make me a valuable asset in the team.

## EXPERIENCE

### Project Manager Penetration Testing

#### Gulf International Bank (GiB)

From January 2024 to Till date | Manama, Bahrain

Working in GiB as a Project Manager Penetration Testing and independently looked after the following activities:

- PT related business and regulatory projects.
- Mock drills.
- Vulnerability management.
- Risk remediation tracking and management.

### Cybersecurity Technical Specialist

#### TAQA (Industrialization & Energy Services Company)

From September 2021 to September 2023 | Islamabad, Pakistan

Worked in TAQA group as a Cybersecurity Technical Specialist and independently looked after the following activities:

- Managing application security and VA/PT related activities.
- Reviewing SOC and Threat Hunting reports periodically.
- Handling NCA & Saudi-Aramco releases.
- Vendor compliance assessment as per TAQA standards.
- Worked on NCA-ECC and SAC-021 Framework.
- **Top Projects:**
  - Implementation of NCA controls and security solutions (MDM, EDR etc.)
  - Blackbox PT and Threat Hunting.
  - Compromise assessment with Loki & YARA rules.

## SKILLS

### Cyber Security Technical:

- Vulnerability Assessment.
- Vulnerability Management and Mitigation.
- Application Security.
- **Penetration Testing work in:**
  - Network, Infra, Desktop / Web Application, API, Backend Servers, Database.
  - Mobile App testing (Android/iOS).
  - Static and Dynamic testing.
  - Cloud System (IaaS, PaaS, SaaS, DaaS).
  - Microsoft Azure, AWS and Alibaba Cloud.
  - Internet and Intranet based network security testing.
  - SolarWinds, CISCO, Juniper, Routers, Network Flow Manager and Firewall Security.
  - OT, ICS, PLC and SCADA Networks.
  - IoT Devices – (Data logger, IP CAMs, Portals, Online Report Tools, Remote Control etc.)
- Security Architecture Design.
- SIEM Solution.
- Threat Hunting.
- Thread Modeling using DREAD and STRIDE.
- Incident Management.
- Digital Forensic Investigation and Research (DFIR).
- Offensive and Defensive skills.
- Microsoft ATP (Advance Threat Protection).
- Microsoft Security Center.
- R&D in Cyber Security.

### Programming Languages:

- **Python** – (Highly Professional Level).
- PHP, HTML, Java scripting, Bash, Kotlin, Java, Ruby, RUST – (Basic).
- C++, Assembly (at Advance Level with OOP – Hardware Programming).
- PLC Ladder Logic – (Basic).

## Application Security Analyst

### Telenor Microfinance Bank Limited

From September 2019 to September 2021 | Islamabad, Pakistan

Worked in TMFB as a Manager Application Security in Information Security Department (Risk Division) and independently looked after the following activities:

- Security of financial app **EasyPaisa**.
- VAPT of Network Devices, Infrastructure, Applications (Branchless and Core Banking).
- Worked as DevSecOps, to ensure the security of architecture design and mitigate code flaws.
- Awareness and Training for the implementation of Secure-SDLC process.
- Worked in CTI (Cyber Threat Intelligence) Unit with State Bank of Pakistan (SBP) team, to mitigate the risk of security threats from outside the organization.
- VAPT of in house Private Cloud including IaaS, PaaS, SaaS and DaaS. Provided by “**Ant Financial Services**”.
- Support SOC (Security Operation Control) team to improve SIEM maturity.
- Delivering a range of CR assessment types including Desktop/Web/Mobile Application, APIs, Databases, 3<sup>rd</sup> party Integrations and Servers.
- Worked closely with other teams such as Infra, Network, IT Dev., Operations, Solution Architect, PD & PMO for the mitigation of organizational risk.
- **Top Projects:**
  - VAPT of T24 Temenos (*Found 3 Zero Days, which were reported to **Temenos global***).
  - VAPT of **Alibaba cloud system** (*Implemented by Ant Financial group, China*).
  - Annually PT and Compromise assessment
  - Network Assessment Exercise.
  - Recommended permanent solution for prevent app cloning incident for reduce the Fraud/Risk.
  - Application Audits.

## Information Security Manager

### Government of Pakistan

From February 2015 to June 2019 | Islamabad, Pakistan

For a long term project worked in a semi government organization as an Information Security Manager. Lead the Security team and independently looked after the following activities:

- Bug Hunting for Mobile, OS and Web Based Applications.
- Hardware, Software, Network and Web based penetration testing for Local/Remote Area.
- Supervised R&D Team.
- Virus/Malware/Backdoor Analysis and reverse engineering
- Suggestion/Decision & Implementation for Secure Networks.
- Python scripting for automation process.
- Supervise Red Team for in-house CTF Events.

## Governance Risk Compliance (GRC) Skills:

- Risk Assessment.
- Risk Management & Mitigation.
- Security standards development and implementation.
- Compliance assessment.
- SOP, Policies and Framework development.
- Application Audit.
- Site area audit (call center, branch office etc.)

## Managerial Skills:

- Tracker and Dashboard Development for Top Management.
- Proper Documentation and Reports.
- Awareness & Training Sessions.
- Cybersecurity Event Management.
- Team Building, Leadership and Work Management.
- Business Development and Strategy.
- Cybersecurity alignment with respect to organizational goals and objectives.

## Experience in Security Tools:

- BurpSuite, Fiddler, App-Proxy.
- Frida, Objection Framework.
- Nessus, Nexpose, Acunetix, IBM Web Inspect.
- Metasploit Framework, Wireshark, Nmap.
- IBM QRadar, Splunk (Basic understanding).
- Search Engine Doxing/Dorking etc.
- Passive and Active scanning.
- **Linux Distribution** Hands-on:
  - Kali Linux.
  - BackBox.
  - Parrot OS.
  - Arch Linux.
  - Ubuntu.
  - Red Hat.
  - CentOS.

## Other Skills & Activities:

- Ethical Hacking.
- Exploit Research and Development.
- Reverse Engineering and Bug Testing.
- Web Application Development, Design and Security.
- Offensive Security Experience for Open/Targeted System on Local & Remote Network.
- Cyber Security Expert (*at Professional Level*).

## Cyber Security Consultant

### Freelancer (Part Time)

From January-2011 to September-2019 | Islamabad, Pakistan

Since my student life in university, engaged for doing part time freelancing projects and independently looking after the following activities:

- VAPT related projects with Black-box, Gray-box and White-box testing.
- Different type of Electronics, IT, IoT and Information Security Projects.
- Web-Development & Secure Coding.
- Python Scripting for Scraping, Data Mining, Data Management, Image Processing, AI and Automation.
- Networks & System Security.
- Virus/Malware Analysis, Social Engineering and Tracing Type of Work Experience.
- Patching Server and Domain Vulnerabilities to prevent it from Hackers.

## EDUCATION

- **B.Sc. in Electronics**  
**COMSATS Institute of Information and Technology, Islamabad.**  
2008 to 2011
- **PLC & SCADA Industrial Automation**  
**Buraq Integrated Solution, Rawalpindi.**  
2011

## LANGUAGES

- **Urdu:** Expert
- **English:** Fluent
- **French:** Beginner

## PERSONAL INFORMATION

- **Nationality:** Pakistani
- **Religion:** Islam
- **Marital Status:** Married

## CERTIFICATIONS

1. **Certified Appsec Practitioner (CAP)**  
**The SecOps Group: Badge (N/A)**  
2023
2. **Certified Information Security Manager (CISM)**  
**ISACA: [Verify Badge](#)**  
2023
3. **Microsoft Azure Security & CISSP Modules (Learning)**  
**Skillsoft: [Digital Badges](#)**  
2022
4. **Certified Network Security Specialist (CNSS)**  
**ICSI, UK: [Verification Code \(17647968\)](#)**  
2020
5. **Certified Network Security Expert (Fortinet: NSE1 || NSE2)**  
**Verification Code NSE1: [jr1UfE3npX](#)**  
**Verification Code NSE2: [JaTDNzsHE](#)**  
2020
6. **Cisco Certified Introduction to Cybersecurity**  
**Cisco Networking Academy: [Verify Badge](#)**  
2020
7. **AWS Security Fundamentals**  
**Amazon Web Services (AWS): Badge (N/A)**  
2020
8. **Autopsy Basics and Hands On**  
**Basis Technology: Badge (N/A)**  
2020
9. **Certified Ethical Hacker (CEH v10)**  
**EC-Council Certification: [ECC0814752369](#)**  
2018