

Hasnain Abbasi

+923172626120 | hasnainjr890@gmail.com

<https://www.linkedin.com/in/hasnainabbasi-a9b198211>

SUMMARY OF QUALIFICATIONS

Cybersecurity professional with a strong interest in ethical hacking, penetration testing, vulnerability analysis, and network security. Hard-working, energetic, personable, and technical-minded individual. I possess exceptional customer service and communication skills, with a solid ability to multitask and resolve issues quickly. Currently in a cybersecurity role where I continue to develop and learn new skills while contributing to the organization's overall success.

AREAS OF EXPERTISE

Vulnerability Assessment and Penetration Testing (VAPT) External / Internal Network Penetration Testing
Web Application Penetration Testing Security Tools (e.g., Burp Suite, OWASP ZAP)
Android/iOS Application Penetration Testing Threat Modelling
API Penetration Testing Secure Coding Review (SAST / DAST)
Active Directory / Azure AD Penetration testing
OSINT / Attack Simulation
SCADA Penetration Testing
Cloud Penetration Testing
Compromise Assessments
Root Cause Analysis
XDRs EDRs Solutions
Cloudflare Rules & Waf Implementation

EDUCATION & CERTIFICATIONS

Bahria University	Bachelor of Computer Science
TCM Security	Practical Network Penetration Tester (PNPT)

INE Security (FKA eLearn Security)	eLearn Security Junior Penetration Tester (EJPT)
The SecOps Group	Certified Network Security Practitioner (CNSP)
The SecOps Group	Certified AppSec Practitioner (CAP)
The SecOps Group	Ethical Hacking Essential (EHE)
APIsec University	Certified API Penetration Tester
Skill Front	ISO 27001

PROFESSIONAL EXPERIENCE

Inbox Business Technologies Limited (Pakistan - Onsite) VAPT Specialist (03-March-2025 – Present)

- Conduct comprehensive penetration testing across web, mobile (Android/iOS), desktop applications, APIs, and networks to identify and exploit security vulnerabilities.
 - Perform cloud security assessments and Active Directory (AD) assessments, ensuring robust identity and access management configurations.
 - Lead technical gap assessments and audits to evaluate existing security postures and recommend actionable improvements.
 - Review and analyse network device configurations (firewalls, routers, switches) for misconfigurations, weaknesses, and compliance with security best practices.
 - Execute vulnerability assessments using industry-standard tools to detect and prioritize threats across systems and infrastructure.
 - Collaborate with teams to deliver clear, detailed technical reports and assist in remediation planning and implementation.
-

ACE Money Transfer (Pakistan - Onsite) Team Lead Cybersecurity Department (12-08-2024 – 1 -March-2025)

- Spearheaded comprehensive penetration testing and red teaming across web, Android, iOS, network, and Active Directory environments, detecting and mitigating critical vulnerabilities.
- Conducted in-depth GRC (Governance, Risk, and Compliance) assessments, ensuring adherence to industry regulations and strengthening security posture.
- Collaborated closely with blue team members on rules testing, developing proactive defense mechanisms to enhance incident detection and response.
- Designed and managed firewall rules and configurations, reinforcing perimeter security to guard against evolving threats.
- Implemented and monitored advanced XDR (Extended Detection and Response) and EDR (Endpoint Detection and Response) solutions to streamline threat identification and remediation.
- Fostered a culture of security collaboration within cross-functional teams, aligning security strategies with broader organizational goals and objectives.
- Led regular threat simulations and security drills to prepare teams for real-world cyber threats and improve incident response times.

Apprise Cyber PVT LTD (Pakistan - Onsite) Team Lead Offensive Security Department (01-05-2022 – 2024)

- Performed penetration tests on Web, API, and Mobile Android/iOS Applications, discovering crucial vulnerabilities to boost cyber resilience.
- Led the charge in threat modeling, strengthening proactive security measures for a robust defense.
- Conducted sophisticated External/Internal Network Penetration tests to fortify our defenses against evolving threats.
- Promoted a security-conscious culture by collaborating with teams to implement and uphold security best practices.
- Offered valuable insights to protect digital assets, reinforcing the overall safety of our tech infrastructure.
- Delivered detailed vulnerability reports with practical guidance for developers and stakeholders to take swift, effective action.

- Collaborated with cross-functional teams to develop incident response strategies, further enhancing our ability to address security incidents swiftly and effectively.
- Perform advanced penetration tests, exploit vulnerabilities, and identify security weaknesses.

RS Softwire (SMC-Pvt) Ltd (Pakistan - Hybrid) Senior Penetration Tester (2021 - 2022)

- Performed penetration tests on Web, API, and Mobile Android/iOS Applications, discovering crucial vulnerabilities to boost cyber resilience.
- Led the charge in threat modeling, strengthening proactive security measures for a robust defense.
- Conducted sophisticated External/Internal Network Penetration tests to fortify our defenses against evolving threats.
- Develop and refine penetration testing methodologies, tools, and techniques.
- Choose and customize penetration testing tools to suit specific assessments.
- Assess network infrastructure for weaknesses, misconfigurations, and vulnerabilities.
- Evaluate the effectiveness of firewalls, intrusion detection systems, and access controls.
- Conduct in-depth assessments of web applications, identifying flaws like SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).

Code Avenue (Pakistan - Remote) Penetration Tester (01-05-2020 - 01-01-2021)

- Conducted targeted penetration tests on web and mobile applications, identifying and reporting high-impact vulnerabilities to safeguard client data.
- Developed detailed assessment reports with actionable remediation steps, enabling developers to address security issues effectively.
- Performed security validation on mobile app APIs, ensuring secure data handling and authentication practices.
- Collaborated with development teams remotely to review findings, contributing to secure coding practices and improved application security.

Whooping (Korea – Remote) VDP Engineer And Penetration Tester (01-01-2020 - 01-05-2020)

- Develop and maintain the organization's Vulnerability Disclosure Program.
- Create clear and accessible channels for external parties to report security vulnerabilities.
- Acknowledge and validate vulnerability reports received from external researchers.
- Collaborate with security researchers and provide necessary guidance or clarifications.
- Identify and exploit vulnerabilities to assess the security posture of an organization.
- Develop and execute detailed penetration testing methodologies.
- Collaborate with teams to remediate identified vulnerabilities and weaknesses.
- Stay up-to-date with the latest security threats and emerging attack techniques.

Independent Penetration Tester (Freelance) (2020 – 2023)

- Conducted independent penetration testing engagements for various clients.
- Collaborated closely with clients to understand their specific requirements and objectives.
- Utilized industry-standard vulnerability scanning and exploitation tools and techniques, such as Burp Suite, OWASP ZAP, Nmap, and Metasploit.
- Conducted Web Application, API and Mobile applications penetration testing, including identifying common vulnerabilities like SQL injection and cross-site scripting (XSS).
- Evaluated authentication and authorization mechanisms (JWT, OAuth, session management) for security weaknesses.
- Explored and exploited privilege escalation vulnerabilities to assess overall system security.
- Successfully identified and reported critical vulnerabilities for various clients, including broken access controls, business logic flaws, and information disclosure bugs.
- Employed API fuzzing techniques to uncover potential security weaknesses and injection flaws.
- Provided detailed vulnerability reports with actionable guidance for developers.

Bug Bounty Hunter (2020 – Present)

- Strong understanding of OWASP Top Ten project for identifying critical security risks.
- Analyzing complex application architectures to uncover potential attack vectors.
- Skilled in using tools like Burp Suite, OWASP ZAP, and Nmap for vulnerability scanning and penetration testing.

- Knowledgeable in authentication and authorization mechanisms (JWT, OAuth, session management).
- Experience in identifying and exploiting privilege escalation vulnerabilities to assess overall system security.
- Proficient in API fuzzing techniques to uncover potential security weaknesses and injection flaws.
- Writing detailed vulnerability reports with actionable guidance for developers.
- Report many critical , High and medium severity vulnerabilities on HACKERONE AND BUGCROWD

CYBERSECURITY PROJECTS

Principles of Cybersecurity

- Implemented risk management and risk assessment to manage, prioritize, and reduce risks for organizations.
- Researched and examined numerous advanced persistent threat (APT) groups and their anatomy
- Studied and performed different forms of social engineering to learn mitigation techniques.
- Performed cybercrime investigations to identify and eliminate threats.
- Conducted surveys on targets to identify assets, collect human intelligence, and assess vulnerabilities.

Network Technologies and Network Security

- Used command-line tools (ping, ipconfig, ifconfig, netstat, tracert, arp) to troubleshoot and analyze system connectivity issues and identify a network's security posture.
- Learned about, implemented, and configured protocols (SRTP, FTP, SFTP, FTPS, SSH, TLS, IPsec, SMTP, POP3, IMAP4, HTTP(S), Kerberos, LDAP, NTP, DHCP, RDP) to support different use cases.
- Studied, Installed, and configured switches, routers, and firewalls to create a secure and efficient network.
- Understood and utilized different security zones (DMZ, intranet, extranet) and network separation (airgaps,VLANs, proxy servers) to construct secure networks.
- Installed and configured IDSs/IPSs (Snort) to monitor networks to detect and analyze potential attacks.

Cyber Operations

- Performed XSS attacks to redirect targets and grab cookies, SQLi attacks to exfiltrate usernames and password hashes.
 - Carried out buffer overflows to create new user accounts and change login sessions.
 - Used TELNET and Metasploit to obtain remote access on Metasploitable VMs.
 - Implemented rapid triage to identify and categorize issues into four priority levels: low, medium, high, and critical.
 - Employed the concept of order of volatility to preserve forensic data.
-

PROJECTS PERFORMED / DOING

Mr. Hasnain Abbasi has done more than 150 + national and international projects including (Application, Network, Compromise Assessments) penetration tests. Some of the projects are mention below

- KARACHI SHIPYARD AND ENGINEERING WORK (KSEW) Penetration Testing (Internal, Infrastructure)
- National Telecommunication Center (NTC)
- AlAmthal Finance (Saudi Arabia)
- NATIONAL INSURANCE COMPANY (NICL) Penetration Testing (Internal Portals)
- Lucky Core Industries (LCI) Penetration Testing (Internal Infrastructure, External)
- RSM PAKISTAN Penetration Testing (External, Internal And infrastructure)
- HABIBMETRO Penetration Testing (External Web Application)
- Haball Penetration Testing (Infrastructure)
- The Talent Games Penetration Testing (Internal Web Application)
- UNIKREW Penetration Testing (Internal Portals)
- Avanza Solutions Penetration Testing (Source Code Review)
- Hackathon Cybersecurity Workshop Delivered national level hackathon hands on practical workshop in multiple cities of Pakistan including Islamabad, Karachi, Rawalpindi, Peshawar, Multan and Lahore.
- BYKEA Penetration Testing (WEB, ANDROID, IOS)
- ABHI Penetration Testing (ANDROID, IOS)

- QisstPay Penetration Testing (ANDROID, IOS)
- Caary Penetration Testing (ANDROID, IOS)
- Sastaticket Penetration Testing (ANDROID, IOS)
- SNGPL (SCADA pentest)

HALL OF FAME

Company Name	Hall of Fame URL
STOPFAP	https://www.stopfap.org/thanks