ASAD NOOR

Penetration Tester | Web Application Security | Bug Bounty Researcher
Lahore, Pakistan +92-343-4666264 asadnoor951@gmail.com linkedin.com/in/asadnoor951

PROFESSIONAL SUMMARY

Cybersecurity professional with 3+ years of experience and a dual offensive/defensive background, now focused on web application penetration testing and bug bounty research. Proficient in full-cycle web app pentesting — recon through exploitation and reporting — applying OWASP Top 10 methodology, Burp Suite, and manual exploitation techniques across XSS, SQL injection, IDOR, authentication flaws, and business logic vulnerabilities. Holds real-world detection engineering experience (40+ MITRE ATT&CK-mapped rules, 500+ endpoint environment) that directly informs attacker thinking and improves exploit identification depth. Actively researching on HackerOne and Bugcrowd. Pursuing eJPT and BTL1 certifications.

CORE COMPETENCIES — OFFENSIVE SECURITY

Web App Pentesting	Full OWASP Top 10 coverage — XSS (reflected/stored/DOM), SQLi, IDOR, SSRF, XXE, broken auth, privilege escalation, business logic flaws
Recon & Enumeration	Subdomain enumeration (amass, subfinder, dnsx), JS file analysis, parameter discovery (ffuf, arjun), Google dorking, Shodan, Wayback Machine
Exploitation Tools	Burp Suite Pro (scanner, intruder, repeater, collaborator), SQLMap, Nikto, ffuf, Nmap, Nuclei, curl, Python scripting
Authentication Attacks	Broken auth chains, JWT manipulation, session fixation, OAuth flaws, MFA bypass, password reset logic abuse
Injection Attacks	Manual SQLi (Union, Boolean, Time-based), XSS payload crafting, SSTI, command injection, HTTP header injection
API Security	REST/GraphQL API testing — mass assignment, broken object-level auth (BOLA/IDOR), excessive data exposure, rate limit bypass
Bug Bounty Platforms	HackerOne, Bugcrowd — scoping, rules of engagement, report writing, CVSS severity mapping, PoC reproduction
Reporting	Pentest report writing: executive summaries, technical findings, PoC steps, CVSS scores, remediation recommendations
Supporting Skills	Network packet analysis (Wireshark), firewall rules, Linux privilege escalation basics, CVE research, threat modeling

WORK EXPERIENCE

Cybersecurity Engineer & SOC Analyst | PostEx (Fintech) — Lahore *Jan 2025 – Present*

Dual-role: detection engineering / SOC operations for 500+ endpoint fintech environment.

- Engineered 40+ custom detection rules mapped to MITRE ATT&CK (T1059, T1486, T1078, T1053), developing attacker-pattern intuition applied directly to offensive security research.
- Conduct proactive threat hunting across endpoint telemetry and log data, surfacing lateral movement, persistence, and C2 patterns — skills directly transferable to purple team and red team scenarios.

- Perform vulnerability assessments using OpenVAS and Nmap; lead CVE analysis, CVSS prioritization, and OS hardening per CIS Benchmark controls.
- Operate Elastic Defend EDR — monitor process injection, file activity, network behavior — providing hands-on understanding of EDR detection logic exploited during offensive engagements.
- Reduced SIEM false positives by 40% through correlation tuning, threshold calibration, and log filtering — demonstrating structured analytical methodology core to pentest triage.
- Designed n8n automation pipelines achieving sub-2-minute MTTN for P1/P2 alerts via Telegram and email.

Assistant Network Administrator | PostEx (Fintech) — Lahore *May 2023 – Dec 2024*

- Managed firewall ACL rules, VLAN segmentation, and network topology for 500+ node environment — network knowledge directly supporting network-layer pentest reconnaissance.
- Configured MikroTik routers with OSPF/BGP routing and L2VPN tunnels; supported threat containment by isolating compromised segments during SOC-flagged incidents.
- Maintained change logs, device configurations, and network documentation supporting audit and compliance requirements.

Technical Support Engineer | StormFiber — Pakistan *Feb 2023 – May 2023*

- Diagnosed L1/L2/L3 network faults for enterprise customers; coordinated with NOC during outages following SLA escalation procedures.

PROJECTS — OFFENSIVE SECURITY

Bug Bounty & Web Application Security Research — *HackerOne · Bugcrowd · Active*

- Apply systematic OWASP Top 10 methodology across public bug bounty programs targeting web applications and APIs.
- Identify and report vulnerabilities including reflected/stored XSS, SQL injection (manual + SQLMap), IDOR, broken authentication, and business logic flaws using Burp Suite, manual testing, and fuzzing.
- Execute multi-phase recon: subdomain enumeration, JS file analysis for leaked endpoints/keys, parameter discovery with ffuf, and Wayback Machine crawling for legacy attack surface.
- Write structured disclosure reports with CVSS scoring, reproduction steps, impact analysis, and remediation recommendations per platform standards.

Web Application Penetration Testing Lab — *Self-Hosted · DVWA · HackTheBox · TryHackMe*

- Built a local lab environment (DVWA, Metasploitable, custom Docker targets) for practicing full exploitation chains.
- Completed TryHackMe Jr. Penetration Tester and DevSecOps learning paths, covering SQLi, XSS, file upload bypasses, SSRF, and API exploitation.
- Practiced HackTheBox web challenges — enumeration, LFI/RFI, JWT cracking, deserialization, and SSTI payloads.

MITRE ATT&CK Detection Rule Library — *Production SIEM · ELK + Wazuh*

- Developed 40+ detection rules across 15+ ATT&CK techniques (T1059, T1486, T1078, T1053, T1136, T1021) for ransomware, lateral movement, and persistence detection.
- Offensive value: reverse-engineering rule logic exposes detection gaps and informs evasion thinking for red team/pentest engagements.

Vulnerability Assessment & Hardening Program — *Production Infrastructure*

- Executed recurring OpenVAS and Nmap scanning cycles across 500+ node infrastructure; prioritized by CVSS and business impact.

- Applied CIS Benchmark hardening (Linux and Windows Server), eliminating high-severity misconfigurations — practical attacker-perspective knowledge of exposed attack surface.

TECHNICAL SKILLS

Pentest Tools	Burp Suite, SQLMap, Nikto, ffuf, Nuclei, Nmap, Amass, Subfinder, Arjun, curl
Recon / OSINT	Shodan, Google Dorking, Wayback Machine, JS file analysis, dnsx, httpx
Scripting	Bash, Python (basic automation, payload scripting), PowerShell
SIEM / Detection	ELK Stack (Elasticsearch, Logstash, Kibana), Wazuh, Splunk
EDR / Endpoint	Elastic Defend, FIM (Wazuh), OpenVAS
Network	MikroTik RouterOS, Wireshark, Nmap, OSPF/BGP, VLANs, TCP/IP, L2VPN
Infrastructure	Linux (Ubuntu/CentOS), Windows Server, Active Directory, Proxmox VE, VMware
Frameworks	OWASP Top 10, MITRE ATT&CK, CIS Benchmarks, NIST CSF, CVSS v3.1
Platforms	HackerOne, Bugcrowd, HackTheBox, TryHackMe, DVWA

CERTIFICATIONS

- **CCNA** — Cisco / Corvit System *(2022)*
- **Certified Ethical Hacker (CEH)** — EC-Council *(2022)*
- **CyberOps Associate** — Cisco *(2024)*
- **Ethical Hacker** — Cisco *(2024)*
- **SOC Analyst** — Palo Alto Networks
- **Fundamentals of Network Security** — Palo Alto Networks
- **Fundamentals of Cloud Security** — Palo Alto Networks
- **Jr. Penetration Tester Learning Path** — TryHackMe
- **DevSecOps Learning Path** — TryHackMe
- **Web Fundamentals Learning Path** — TryHackMe
- **eJPT — Junior Penetration Tester** — eLearnSecurity *(In Progress)*
- **BTL1 — Blue Team Level 1** — Security Blue Team *(Planned)*

EDUCATION

BS – Computer Science · NCBA&E, Lahore *2018 – 2022*