

Aman Singh

Email: Aman.Singh.Pentest@gmail.com

Linkedin HackerOne Bugcrowd GitHub Medium X

Objective

A highly motivated and [skilled pentester and bug bounty hunter with hands-on experience in web application security, vulnerability testing, and ethical hacking](#). Seeking a position to leverage my skills and knowledge in a Product Security Analyst role to contribute to securing digital platforms and enhancing security protocols.

Skills

- Manual and automated testing tools: [Burp Suite, Nikto, Nmap, Gobuster](#)
- [Vulnerability identification: XSS, SQLi, IDOR, RCE and Security Misconfigurations](#)
- Bug bounty submissions on platforms like HackerOne
- [Network security & vulnerability scanning](#)
- Scripting: [Python, Bash, JavaScript](#)
- Languages: [HTML, C++, CSS, Python and Javascript](#)
- Deep knowledge of [OWASP Top 10 & mitigation strategies](#)
- Understanding of DevSecOps practices

Experience

- **Bug Bounty Hunter** — Freelance (July 2020 – Present)
 - Performed [web, mobile, and network penetration tests](#)
 - Discovered & reported bugs on [HackerOne and BugCrowd programs](#)
 - Generated security reports & mitigation recommendations
 - Used tools like [Burp Suite, Nmap, SQL, TOR, Wireshark, Splunk and Wazuh](#)
 - Delivered presentations on findings to clients

Technical Proficiency

- Networking & TCP/IP (3+ years): [Identifying network-based attack vectors](#).
- Web App Pentesting (4 years): [OWASP Top 10 focus, real bugs on HackerOne and Bugcrowd](#).
- Burp Suite (3+ years): [Manual testing, Repeater, Intruder and Scanner](#)
- Nmap (3+ years): [Network enumeration, service detection, Port Scanning](#).
- Splunk (1 year): [Log analysis and Security Monitoring](#).
- Wazuh (1 year): [Host-based intrusion detection and Log Correlation](#).
- Tor (2 years): [Anonymous browsing and traffic obfuscation for research and testing](#).
- Wireshark (2 years): [Packet analysis for traffic inspection and troubleshooting](#).
- SQL (2 years): Manual query crafting for SQL injection testing and data retrieval.
- Python (3 years): Automation scripts, simple exploits, parsing tools for bug bounty hunting.
- JavaScript (2 years): XSS payloads, client-side logic during pentests.
- Bash/Shell (2 years): Automated enumeration, scanning, system tasks in Kali Linux.

Projects

- **Vault Repository[GitHub]**– Created Cybersecurity Vault containing Real-World use of Tools and Techniques for Testing.

Education

Class 12 ([Science, Math, Computer Science](#)) – CBSE, India (2024)

Languages

- [English – Proficient](#)
- Hindi – Native

Interests

- Ethical hacking
- Cybersecurity research
- Bug bounty hunting
- Networking and technology