Pranav Garneria

9015000844 | pranavgarneria@gmail.com | linkedin.com/in/pranavgarneria/

Summary

- Red Team and Offensive Security Specialist with expertise in adversary emulation and end-to-end VAPT. Experienced in conducting full-scope red-team operations including reconnaissance, physical security testing, web/mobile/API/IP exploitation, wireless and network attacks, and post-exploitation tactics such as privilege escalation, lateral movement, persistence, and data exfiltration. Skilled in mapping attack chains to MITRE ATTACK, building realistic threat scenarios, and delivering PoCs and actionable remediation guidance to strengthen organizational defenses.

Education

Lovely Professional University — Jalandhar, Punjab
MCA Hons in Cyber Security — *August 2025 – Present*

GNA University — Phagwara, Punjab
Bachelor of Computer Application — *July 2022 – July 2025*

Noorpur Public School — Nurpur, Himachal Pradesh
Senior Secondary Education (Science Stream) — *2021 – 2022*

Experience

Cyber Security Analyst — August 2024 – Present
Cynox Security LLP — *Jamshedpur, Jharkhand*

- Lead offensive security and full-lifecycle VAPT engagements across web applications, API's, mobile and desktop apps, servers, firewalls and IP/network infrastructure.
- Identified and exploited high-impact issues including SQLi, XSS, Command Injection, Race Conditions, IDOR, Broken Authentication, and Business Logic flaws, delivering PoCs and detailed exploit chains.
- Developed comprehensive reports with technical findings, risk ratings, and remediation strategies; collaborated with internal teams and external researchers to validate and resolve vulnerabilities.
- Mentored and onboarded junior analysts and interns, delivering hands-on training in VAPT methodologies and red-team operations, guiding PoC/report writing, hands-on lab exercises, and professional communication for effective vulnerability disclosure and remediation.

Security Researcher — May 2023 – Present
HackerOne, BugCrowd, HackenProof — *Remote*

- Discovered and reported vulnerabilities including SQLi, XSS, RCE, IDOR, and Business Logic flaws across web, mobile, API, and infrastructure targets.
- Led red-team operations and VAPT, reporting 250+ findings across Web, API, mobile and infrastructure domains.
- Recognized for responsible disclosures with Hall of Fame mentions and awarded bounties, including a 200,800,1000,20,2500,3500,892 dollars payout for valid findings.

Cyber Security Trainee — June 2024 – August 2024
Cyberyaan Training and Consultancy — *New Dehli*

- Completed Certified Ethical Hacker (CEH) training.
- Simulated advanced attacks using MITRE ATT&CK mapping.
- Generated red team assessment reports with risk mitigation strategies.
- Practiced privilege escalation, persistence, and post-exploitation techniques.

Projects

KEYLOGGER | *Python, pynput library, File I/O handelling* — November 2023 – December 2023

- Designed and implemented a keylogger to demonstrate how keystroke-capturing malware operates and to analyze potential security risks.
- Captured and logged keystrokes in real time to study data leakage vectors and user activity monitoring.
- Implemented secure data storage and stealth techniques to simulate real-world attack scenarios.

SPYxPG Tookit | *Python, BashScript, Tools API* June 2024 – October 2024

- Built a Bash SELECT MODULE CLI wrapper that lets users quickly launch recon tasks (Whois, Nmap, DNS Lookup, Subdomain.
- Automated chaining of follow-up scans (masscan/nmap, httpx, dirsearch) via the Bash wrapper and exported consolidated.

TECHNICAL SKILLS

Core Skills: Web App Security, VAPT, Penetration Testing, Android/IOS Application Testing, Network Security, Wireless Testing, OSINT, API Testing, Firewall and Server Audits,Compliance, Footprinting and Enumeration, Active Directory,
Tools: Burp Suite, Postman, Nessus, Metasploit, Wireshark, SQLmap, Hydra, Curl, Nmap, Hashcat, Maltego, Bettercap, Shodan, Gobuster, Ffuf, Github, Ghauri, Google Dorking, Android Studio
Frameworks & Standards : OWASP Top 10, CVE, MITRE ATT&CK, ISO27001, NIST, CWE
Platforms : Kali Linux, Ubuntu, CSI Linux, Web3, Windows, Linux Environments

CERTIFICATIONS

Certified Ethical Hacker - Practical (CEH v12) | *EC-Council*

Ethical Hacking Essentials | *EC-Council*

Foundation of Cyber Security | *Palo Alto*

Dark Web Essentials | *EC-Council*

Hackers Prey CTF | *HackersPrey*

Information Security | *Infosys Springboard*

ACHIEVEMENTS

Hall of Fame recognitions: NASA, DHS (U.S.), BIA, Assa Abloy, CoinW, CoinmetroWeb3, Flow, OFZA Web3, and others.

CTF Champion — winner of 2 capture-the-flag competitions at GNA University (Cyberyaan and Tech Pragya).

Delivered 5+ hands-on workshops on Ethical Hacking, Offensive Security, VAPT, Networking, and Bug Bounty hunting for student and professional audiences.

Ranked Top 20 out of 1,000+ participants in Hackers Prey “Brute Force 4.0” CTF.

Discovered and responsibly disclosed numerous critical vulnerabilities including XSS, SQLi, HTML injection, insecure file upload, business logic flaws, race conditions, and 2FA bypasses — producing reproducible PoCs and remediation guidance.

Awarded 200,800,1000,20,2500,3500,892dollors bounties (including collaborative findings) through Bug Bounty platforms and Responsible Disclosure programs.