MANISH JANGRA

Security Analyst | VAPT & Penetration Testing

Web, network and API penetration testing, from recon and exploitation to reports that developers and stakeholders can act on. CEH and CRTA certified; critical finding accepted by Epic Games.

Gurugram, India +91 93505 45502 manishjangra1811@gmail.com linkedin.com/in/manish-jangraa
github.com/manishjan1811

PROFESSIONAL SUMMARY

Security analyst with hands-on **VAPT** experience across 10–15 client environments (websites, APIs and networks), certified **CEH** and **CRTA**. Reported a **critical OTP and 2FA bypass** that Epic Games accepted through Bugcrowd. I automate my own tooling (Reconbro.sh, Webtools.sh) and, as a web developer myself, test for the flaws developers actually introduce and write fixes they can apply the same day.

CORE SKILLS

Penetration Testing	Web application, network and API testing · OWASP Top 10 · Broken Access Control · Authentication, OTP / 2FA and JWT attacks
Vulnerability Classes	SQL injection, XSS, CSRF, SSRF, IDOR, REST API flaws, cloud and container misconfiguration (documented in my VAPT notes)
Recon & Scanning	Nmap, Subfinder, httpx, Nessus, Nikto, Wireshark, OWASP Dependency-Check, Reconbro.sh (custom)
Exploitation & Analysis	Burp Suite, Metasploit, OWASP ZAP, Postman, Kali Linux
Risk & Reporting	CVSS scoring, evidence-backed assessment reports, remediation guidance, patch review and retest, explaining risk to non-technical stakeholders
Methodology	Recon, scan, exploit, report, fix and retest; always scoped, authorised and documented end to end
Bug Bounty	Bugcrowd, HackerOne, responsible disclosure
Scripting & Platforms	Bash, Python, JavaScript, Webtools.sh (custom) · Linux, Windows, Unix, Git, Docker

WORK EXPERIENCE

Cyber Security Intern — *Scudo Cyber Solution Pvt. Ltd.* 03/2026 – 06/2026

- **End-to-end VAPT:** Carried out vulnerability assessment and penetration testing on 10–15 client environments, covering websites, APIs and network infrastructure, from reconnaissance and scanning through exploitation and reporting.
- **On-site client work:** Travelled to client offices (Noida and nearby) to run assessments and walk IT teams through findings in person.
- **Exploitation with impact:** Identified and exploited vulnerabilities using Burp Suite, Nessus and OWASP methodology, proving what an attacker could actually reach instead of handing over scanner output.
- **Reporting & remediation:** Wrote assessment reports covering findings, risk levels and remediation steps for engineers and non-technical stakeholders, then worked with client IT teams to prioritise and close the issues.
- **Confidentiality:** Client names and findings are withheld, in line with Scudo's confidentiality terms.

BUG BOUNTY & SECURITY RESEARCH

Epic Games — *Critical authentication bypass, Bugcrowd public program* 2025

- **Finding:** Found that account creation could be completed without passing OTP or 2FA verification, defeating the controls meant to stop unverified and abusive accounts.
- **Outcome:** Documented the issue with technical detail, impact analysis and remediation guidance; the report was **accepted as a critical finding**.

Security tooling — *open source on GitHub* github.com/manishjan1811

- **Reconbro.sh:** Bash tool that chains subdomain enumeration, live-host probing and screenshots into one repeatable run.
- **Webtools.sh:** installs a complete web pentesting toolkit (recon, fuzzing, scanners) with a single command.
- **VAPT Notes:** notes on 20 vulnerability classes across web, API, cloud, CI/CD and mobile, plus a security-header analyzer.

CERTIFICATIONS & HONORS

- **Certified Ethical Hacker (CEH)** — EC-Council (2025)
- **Certified Red Team Analyst (CRTA)** — CyberWarFare Labs (July 2025) ID CRTA-686e984c8758984542bf2324
- **Accepted critical bug bounty** — Epic Games, via Bugcrowd public program (2025)

EDUCATION

Diploma in Cyber Security — *Craw Cyber Security, Saket, Delhi* 2025

Bachelor of Computer Applications (BCA) — *Om Sterling Global University* Completed 2026