Parth Narula

Security Researcher, Penetration Tester and Application Security

parth.narula@scriptjacker.in | +91 74970 54662 | India | parthnarula.scriptjacker.in | linkedin.com/in/parth-narula-86283821a | github.com/scriptjacker

Professional Summary

Security researcher and penetration tester working across web applications, APIs, Android, cloud and AI systems. Credited by 386 organizations in 38 countries, among them Apple, WHO, UNESCO, CERT-EU, Nokia, Boeing, NVIDIA, Red Hat and the BBC, with 331 Hall of Fame listings and first researcher status at 45 programs. Strongest on broken access control, business logic, authentication and API flaws, with a published CVE and a CVSS 9.0 vendor advisory to my name, and I write every finding up so a team can reproduce it, fix it and retest it. Looking for a security analyst, penetration tester or application security engineer role.

Core Competencies

Offensive security: Vulnerability Assessment and Penetration Testing (VAPT), Web Application Penetration Testing (WAPT), dynamic application security testing (DAST), API security testing (REST and GraphQL), Android and mobile penetration testing, network penetration testing, red teaming, reconnaissance, OSINT and Google dorking, subdomain enumeration

Vulnerability classes: broken access control, IDOR and BOLA, business logic flaws, authentication and session handling, OAuth 2.0 and OpenID Connect flaws (redirect URI validation, missing PKCE), SSRF, SQL injection, XSS, CSRF, server side template injection, race conditions, mass assignment, CORS misconfiguration, credential and PII exposure, subdomain takeover

Standards and process: OWASP Top 10, OWASP API Security Top 10, OWASP LLM Top 10, CVSS severity rating, secure SDLC and CI/CD security, SAST and SCA alongside DAST, coordinated and responsible disclosure, vulnerability management from triage to retest, proof of concept development, report writing, remediation guidance

AI and cloud security: LLM, agentic and RAG application testing, Model Context Protocol (MCP) server security, prompt injection, AI red teaming, cloud security and IAM across AWS, Azure and GCP: dangling CNAME and subdomain takeover, Azure AD tenant disclosure, exposed managed database services, Firebase authentication enumeration

Technical Skills

Tools: Burp Suite, OWASP ZAP, Nmap, Metasploit, Postman, Wireshark, Kali Linux, Android Studio, Cisco Packet Tracer, Git, Apache, Nginx, Linux CLI

Platforms and networking: Linux, Windows, Active Directory tooling, containers and container security, TCP/IP, DNS, routing and firewalls, REST and GraphQL APIs, web servers

Programming and scripting: Python, Bash, PHP, JavaScript, SQL, Ruby, C, C++, HTML, CSS

Professional: leadership, teamwork, communication, problem solving, time management, decision making, research

Professional Experience

Security Researcher, Independent, through vulnerability disclosure and bug bounty programs — Nov 2023 to Present

- Reported vulnerabilities to 386 organizations across 38 countries, earning 331 Hall of Fame listings and first researcher status at 45 programs, including City of Berlin, Commerzbank, BankAxept, Port of Tallinn and the University of St Andrews.
- Focus on broken access control, business logic, authentication and API flaws: an IDOR exposing 85,000+ email addresses, mass assignment leading to account takeover, and a self XSS chained into stored XSS.
- Reconnaissance at scale: an exposed Apache Guacamole instance found through dorking led to shell access on a Nokia subdomain (Nokia Hall of Fame, June 2026).
- Cloud and AI surfaces: a dangling AWS CNAME and an Azure AD tenant disclosure at a German media group, an exposed managed database at a national dairy brand, Firebase authentication enumeration at a Finnish retailer, and information disclosure and blind SSRF reached through Model Context Protocol servers.
- Found two vulnerabilities in Netwrix PingCastle, an Active Directory assessment tool: an update package installed with no integrity verification and a path traversal reachable through prefix matching. Fixed in 4.0.0.31 and published by Netwrix as advisory ADV-2026-018 at CVSS 9.0, which credits me by name. CVE identifiers are requested and pending.
- Published CVE-2025-56697 for a stored XSS, and coordinated SQL injection and information disclosure fixes through CERT-In on Indian government and public sector assets.
- Every report carries reproduction steps, business impact and remediation advice, then a retest once the fix lands. 136 of these acknowledgements are public pages linked from my portfolio.

Mentor, Bug Bounty and Web Security, Unihackers — Jun 2025 to Present

- Mentor students and new hunters using real cases from my own reports, and author guides on API security testing, request manipulation and prompt injection.
- Invited speaker: web application penetration testing masterclass for around 150 students at Guru Jambheshwar University of Science and Technology, Hisar (Oct 2025).

Founder and Lead Penetration Tester, ScriptJacker LLP — 2023 to Present

- Manual security assessments of web applications, APIs, Android apps and networks for 150+ clients, with 2,500+ vulnerabilities reported and resolved.

Penetration Tester Intern, Forensic Academy — Aug 2023 to Sep 2023

- Built and tested an enterprise network in Cisco Packet Tracer, ran a web application penetration test against a live target and delivered the written report. Completed with Grade A+.

Certifications

CEH v13, Certified Ethical Hacker, EC-Council Nov 2025
eWPTX v3, Web Application Penetration Tester eXtreme, INE Security Dec 2025
eJPT v2, eLearnSecurity Junior Penetration Tester, INE Security Jan 2026
ACP, APIsec Certified Practitioner, APIsec University Mar 2026
Ethical Hacker, Cisco Networking Academy Nov 2025
EHE, Ethical Hacking Essentials, EC-Council Feb 2022

Key Achievements

- **Halls of Fame and acknowledgements** from Apple, WHO, UNESCO, CERT-EU, CERT-In, Nokia, Boeing, NVIDIA, Red Hat, Philips, Thales, TP-Link, Netwrix, TRATON, BBC, BASF, Michelin, MediaTek, Deutsche Börse, the United Nations and the Australian Government. 136 are public pages linked from my portfolio.
- **Letters and certificates of appreciation** from Drexel University (CISO), GeeksforGeeks, Maastricht University, Avans, Windesheim, CTW Inc, Nykaa and Neoshare.
- **Competitions:** AIR 21 of 10,000 at the HackWithIndia 2026 Web Hacking Competition. As team lead of ScriptJackers, 1st at the TechFusion 2026 CTF (Vaish College of Engineering, Rohtak, Oct 2026), Rootbreach (national, UTKANSH '26, NIT Jalandhar, Mar 2026), Cyber War 2026 (national, Quick Heal and CompTIA), RCS 2026 (national), Cyberthon 2026 and Encrypted CTF (Nov 2025); 2nd at Xploit404 (Apr 2026) and in Data Detectives on AI attacks and prompt injection at TechFusion 2026; 3rd at Trivarna 2.0 (international).

Projects

Agent driven reconnaissance and penetration testing, Python (in progress, private) Jun 2026 to Present
Layers of models orchestrate a test and choose an approach per target instead of following one fixed methodology, calling my own scripts and wordlists when needed.

ScriptJacker Recon Tool, Python, Ruby, Bash (github.com/scriptjacker/scriptjacker) May 2024
Full reconnaissance in one run: subdomain enumeration, directory busting, DNS recon, JavaScript analysis and vulnerability scanning, built to follow an end to end methodology rather than isolated commands.

Education

Bachelor of Computer Applications, Cybersecurity, Lovely Professional University, Phagwara, Punjab. Aug 2025 to Present
CGPA 9.75

Senior Secondary, Commerce, Vishvas Senior Secondary School, Hisar, Haryana. 86% Apr 2023 to Mar 2025

Matriculation, St. Mary's School, Hisar, Haryana. 84% Mar 2023