CHINTAN GURJAR

(CEH, CCFA, CCFH, CTIA, OSCP, CBE, SANS MGT516)

Mobile: +44 XXXXXXXXX
Email: chintangurjar@outlook.com
LinkedIn | **GitHub** | **www.chintangurjar.com**

13 years of total experience in penetration testing, red team operations, threat intelligence and vulnerability management. Proven track record of building and leading high-performing security testing teams. Expertise in developing comprehensive penetration testing methodologies, conducting red team exercises, and implementing adversary emulation programs aligned with MITRE ATT&CK framework.

CORE COMPETENCIES

- Offensive Security Leadership
- Red Team Operations Management
- Penetration Testing Expertise
- Adversary Emulation
- Security Testing Automation
- Team Development
- End-to-End Project Management
- Vulnerability Scanning
- Web, Mobile and API Pentest

CERTIFICATIONS

- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)
- Certified CrowdStrike Falcon Administrator (CCFA)
- Certified CrowdStrike Falcon Hunter (CCFH)
- Certified Threat Intelligence Analyst (CTIA)
- Certified Blockchain Expert (CBE)

TECHNICAL SKILLS

Penetration Testing Tools	BurpSuite, OWASP ZAP, Metasploit, Cobalt Strike, Nmap, Wireshark, Bloodhound, SQLmap, Nessus, John-the-ripper, Hashcat, Postman
Mobile Testing Tools	MobSF, Frida, Drozer, Android Debug Bridge (ADB)
Automation & Scripting	Python & Bash Scripting, REST API Integration
OSINT & Reconnaissance	Maltego, Shodan, SpiderFoot, VirusTotal, WHOIS and DNS Analysis, Amass, Project Discovery Tools, Frogy2.0, Google Dorks
Frameworks & Standards	MITRE ATT&CK, OWASP Top 10, NIST, OSSTM, PTES
Operating Systems	Kali Linux, Red Hat, Windows

PROFESSIONAL EXPERIENCE

Threat & Vulnerability Manager
Marks & Spencer (M&S) *October 2023 – June 2025*

- Established and led the penetration testing and other security assessment activities for M&S under the hood of central vulnerability management division.
- Developed strategic roadmap for offensive security capabilities, aligning with business priorities and threat landscape for using internal team and external pentest/red-team partners and vendors.
- Created standardized penetration testing frameworks and reporting templates and actionable remediation guidance.
- Collaborated adversary emulation program based on MITRE ATT&CK framework, simulating real-world threat actors to test detection and response capabilities under the hood of central global M&S threat intelligence team led by me.
- Developed and implemented security testing automation tools, increasing testing coverage while reducing manual effort.
- Established purple team exercises to improve collaboration between offensive and defensive security teams.
- Managed HackerOne Bug-Bounty program end-to-end.

Global Senior Vulnerability Management Analyst
TikTok *November 2022 - October 2023*

- Led penetration testing initiatives for critical TikTok application backend services.
- Conducted security architecture reviews and threat modeling sessions to identify design-level security flaws.
- Managed HackerOne Bug-Bounty program end-to-end.
- Created knowledge base of common vulnerabilities and remediation strategies based on bug bounty findings.
- Designed and implemented standardized methodologies for web, mobile, and API security testing.
- Created security testing playbooks for different application types and technology stacks.

Security Engineering Manager (Vulnerability & Attack Surface Management)
Tesco *December 2020 - November 2022*

- Collaborated and co-managed the offensive security activities across 7 countries and 5 subsidiaries, establishing standardized testing methodologies.

- Supported comprehensive penetration testing program aligned with business objectives and regulatory requirements.
- Designed and implemented risk-based vulnerability management program with intelligence-driven prioritization.
- Integrated penetration testing results into vulnerability management workflows to validate and prioritize remediation efforts.
- Managed HackerOne bug bounty program, coordinating vulnerability triage and remediation.
- Collaborated with SOC, SIEM, Threat Intelligence, and Red-Team to improve security posture.

Manager, Cybersecurity
KPMG New Zealand *July 2017 - December 2020*

- Led 110+ penetration tests and 10 red team engagements for government and critical infrastructure clients.
- Managed diverse team of offensive security specialists, providing technical guidance and professional development.
- Developed custom penetration testing methodologies tailored to client environments and regulatory requirements.
- Conducted physical security assessments as part of comprehensive red team exercises.
- Conducted threat modeling and architecture reviews for managed CI/CD platforms, offering feasibility studies and design decision support.
- Created adversary emulation scenarios based on threat intelligence and MITRE ATT&CK framework.
- Implemented security controls and guardrails for cloud-native application development.
- Provided strategic security guidance to executive leadership teams across multiple industries.
- Developed remediation roadmaps based on penetration testing findings, prioritizing actions based on risk.
- Created and delivered executive briefings on offensive security results and recommendations.
- Leveraged KPMG's threat hunting services to provide tactical and operational security intelligence.

Security Consultant/Engineer/Analyst
NotSoSecure, ZebPay, Lucideus, LetsNurture *December 2011 - June 2017*

Before 2017, I:

- led web and network penetration testing engagements for multiple clients, identifying critical vulnerabilities and providing remediation guidance,
- conducted red team exercises simulating sophisticated threat actors to test client security controls,
- performed security assessments of mobile applications, identifying authentication, authorization, and data protection issues,
- developed security testing automation tools to increase efficiency and coverage,
- collaborated with development teams to implement secure coding practices and security controls.

COMMUNITY ENGAGEMENT & CONTRIBUTIONS

- **Black Hat USA 2025 Arsenal:** Presented a talk on the automated external attack surface management toolkit I developed.
- **Penal Discussion:** **Qualys EMEA 2024**
- **Open-Source Contribution:** Developed **Frogy 2.0**, an automated external reconnaissance and Attack Surface Management toolkit.
- **Security Operations Center (SOC) Strategist:** **Liminal** - Custody Solutions (Remote)
- **Board of Advisors:** **Cyber Peace Foundation**
- **Conference Contributions:** Co-trained "Mobile Application Hacking and Security" at HackCon 2014
- **CVE Research:** Discovered CVE-2016-7786 (Sophos UTM) and CVE-2020-35387 (EDT Web Application)

PUBLICATIONS & TECHNICAL CONTRIBUTIONS

- **Course Author:** "**Applied Attack Surface Analysis & Reduction**" at EC-Council
- **Technical Reviewer:** "Resilient Cybersecurity: Reconstruct your defense strategy in an evolving cyber world" written by Coca Cola CISO. **Amazon Link**

EDUCATION

MSc. Computer Security & Forensics
University of Bedfordshire (UK) *2013 - 2014*