KARAN CHAUDHARY

CYBER SECURITY TESTER / ANALYST / ENGINEER

+91 9771077075
LinkedIn | Twitter
Portfolio Website
0xKaranChaudhary@gmail.com

Self-taught ethical hacker with 3.5 years of experience in Web, API, and Network pentesting. Secured over 100 companies and 20+ government organizations. I've conducted over 70+ VAPT assessments, identifying over 450 vulnerabilities.

TECHNICAL SKILLS

- **Expertise:** Black box testing, web, API, network, DAST/SAST, VAPT/WAPT, vulnerability disclosure & management, Owasp top 10, Social engineering, OSINT, Kali Linux etc.
- **Tools**:
  - **Penetration Testing & Exploitation:** Burp Suite Pro, Metasploit, Nmap, SQLMap, Hydra & Postman
  - **Reconnaissance & OSINT:** Shodan, Censys, Amass, Project Discovery tools
  - **Vulnerability Scanning & Management:** Tenable Nessus Pro, Rapid7 Insight
  - **Threat Intelligence & Monitoring:** Maltego, Virustotal, URLScan
  - **Red Team & Adversary Simulation:** Empire framework
  - **Blue Team & Defensive Security:** Wireshark
  - **Others:** AWS, Docker, Git
- **Frameworks & compliance**: GDPR, NIST
- **Language**: Python, Bash scripting
- **Development**: automation tools, Burp Suite extensions, browser plugins

WORK EXPERIENCE

Security Tester @ **9ine Consulting** — **June 2022 - Present**

- Web, API, and Network pentesting for internal and external clients.
- Production release security testing of own application (9ine Platform).
- Collaboration with dev teams to ensure successful production deployment.
- End-to-end collaboration with 70+ clients and engineers to define security needs and performed Vulnerability Assessment and Penetration Testing (VAPT).
- Monitor and assess data breach sources to identify potential leaks involving client data, ensuring proactive security measures and incident response.
- Automation scripts, frameworks, and Burp Suite plugin development.
- Generated various red team templates.
- Assist in the creation and delivery of secure development training.
- Evaluated 50+ vulnerability reports to determine validity, risk, and severity for private bug bounty programs.

Associate Security Consultant @ **REOFT Technologies** — **Nov 2021 - June 2022**

- Vulnerability assessments and penetration testing (VAPT).
- Assist clients in incident response activities.
- Red Teaming projects and engagements.
- Research and development of security tools and sophisticated attacks.
- Security framework development

Bug Hunter — **2019 - Present**

- Finding security vulnerabilities in public/private and government programs
- Secured companies like Microsoft, Apple, Disney, Mozilla, OnlyFans, Gorgias, TradingView, Shopify, Twitter, Semrush, PlayStation, 1Password, NCIIPC (Government of India), and many more

ACHIEVEMENTS

- CVE-2021-31982 & $10,000 from Microsoft for finding SSRF vulnerability in Edge browser (Chromium engine)
- 2 times "Employee of the month" winner in 9ine consulting
- Featured in 'Eight Super Bug Hunters of India' (2021)
- Honored by Chandigarh police for developing cyber patrolling software (2019)
- Featured in multiple newspapers for discovering vulnerabilities in a live hacking event organized by Chandigarh Police (2019). [IndiaTimes, NationNews]

PROJECTS

- **LeakAlert:** A browser extension that actively detects exposed secrets/tokens/api/credentials while browsing [Github].
- **Project Alpha**: Framework for comprehensive web security testing, capable of detecting 35+ vulnerability types, from reconnaissance to critical bugs [Github].
- **Discern**: SSRF hunting tool written in bash [Github].
- **Match Monitor**: Burp Suite plugin that actively scans request and response data for sensitive information like passwords, tokens, and APIs, using regex and hardcoded searches to identify over 2,700 types of secrets.
- **Bomb Everything**: Burp Suite plugin that injects various payloads—open redirect, XSS, SSRF, SQLi, SSTI, LFI, and RFI — into every entry point, including headers and parameter values, in parallel with each request sent.
- **E-Commerce website:** End-to-end development and management of a WooCommerce-based e-commerce platform, from developing custom pages and product designs (using Adobe tools), database & security management and handling over 500+ users. [MangalMood.com]
- **Hardware**: Multiple hardware and network hacking projects using Raspberry Pi 3, Wifi Pineapple and NodeMCU
- Practical experience through virtual job simulations that replicate real-world tasks from leading companies on *TheForage.com.*
  - **MasterCard**: Design and interpret email phishing attacks simulation
  - **JPMorgan Chase & Co**: Financial Payment Fraud Analysis
  - **JPMorgan Chase & Co**: Built an Email Classifier

CERTIFICATES

- eJPT v2 - eLearnSecurity Junior Penetration Tester
- AWS Cloud Practitioner

ONGOING PROGRESS AND UPCOMING DEVELOPMENTS

- OSCP - Offensive Security Certified Professional (on-going)
- Mobile security

PERSONAL ATTRIBUTES

- Training & presentation skills
- Experience working with developers
- Experience in conducting penetration testing using various methodologies (black box, gray box, white box)
- Experience in managing teams & tasks in the absence of managers
- Experience in addressing client’s inquiries or issues promptly and professionally and articulate ideas & information with clear and concise communication

LANGUAGES

- English - full professional proficiency
- Hindi - native or bilingual proficiency