C|EH
CERTIFIED ETHICAL HACKER

Chetan Raghunath Chaudhari

chetanchaudhari1183@gmail.com **+91 9767193362**
Mumbai, Maharashtra

Results-driven Security Analyst with 2.5+ years of experience in **Web, API, and Payment Gateway Security Testing**, specializing in **Vulnerability Assessment and Penetration Testing (VAPT)**. Proven experience conducting **end-to-end security testing, including payment gateway testing, for India's No. 1 bank** across multiple platforms such as **Web, UPI, Android, and iOS**. Proficient in **manual and automated security assessments**, identifying and mitigating security risks in applications, APIs, and networks. Skilled in industry-standard tools such as **Burp Suite, Nessus, and OWASP ZAP**. Strong knowledge of **OWASP Top 10, API Security, Mobile Security, and Web Application Security**. Passionate about safeguarding digital assets and staying ahead with advanced attack techniques and evolving threat landscapes.

Professional Summary

- Over **2.5+ years months** of experience in **Vulnerability Assessment and Penetration Testing (VAPT)**, security testing, and penetration testing.
- Proven experience in conducting **Payment Gateway Security Testing** for India's leading banking platforms, including channels like **Web, UPI, Android, and iOS**.
- Proficient in exploiting **OWASP Top 10** vulnerabilities and conducting in-depth **vulnerability assessments**.
- Skilled in **security testing, penetration testing, network security testing,** and **vulnerability remediation**.
- Well-versed in the **Web OWASP Top 10** and **API OWASP Top 10**.

Skills and Technical Expertise

Technical Skills

- **Vulnerability Assessment Mitigation:** Expert in identifying, analyzing, and mitigating security risks in **web applications, APIs**, and **enterprise networks**. Specialized in **OWASP Top 10, API Security**.
- **Penetration Testing (VAPT):** Skilled in conducting **manual and automated penetration testing** using tools such as **Burp Suite, OWASP ZAP, Metasploit, SQLMap, Nmap, Nessus, Wireshark**, and **Postman**.

Tools and Technologies

- **Security Testing Tools:** Burp Suite Pro, OWASP ZAP, Metasploit, Nmap, Nessus, Wireshark, SQLMap.
- **Operating Systems:** Linux (Kali Linux, ParrotOS, Ubuntu), Windows.
- **Programming Languages:** Python, Java, HTML, JavaScript.

Work Experience

Technical Consultant at CyRAACS, Mumbai *April 2025 – Present*

Web Application VAPT
Roles and Responsibilities:

- **Information Gathering:** Collected and analyzed application details through a comprehensive client questionnaire.
- Utilized **Kali Linux tools** such as **Nikto, Nmap, SSLScan, and Dirb** to identify application misconfigurations and gather network information for further penetration testing.
- **Vulnerability Assessment (VA):** Conducted active scans using **Burp Suite Pro and OWASP ZAP**, verified scan reports, eliminated false positives, and manually confirmed firm vulnerabilities.

- **Penetration Testing (PT):** Performed in-depth testing on identified weak areas, covering **OWASP Top 10 vulnerabilities** and other critical security flaws, including **Broken Authentication, Broken Access Control, Injection, Cross-Site Scripting (XSS)**, and more.
- **Reporting:** Compiled and submitted a detailed **VAPT report** to the client, outlining all confirmed findings and providing remediation recommendations.

API VAPT
Roles and Responsibilities:

- **Information Gathering:** Collected and analyzed API documentation, including **Swagger, Postman collections, and OpenAPI specifications**, to understand API structure and functionalities.
- Used **tools like Postman, Burp Suite, and JWT.io** to enumerate API endpoints, analyze authentication mechanisms, and identify potential misconfigurations.
- **Vulnerability Assessment (VA):** Conducted active scanning and manual testing to detect security flaws, focusing on issues like **Broken Object Level Authorization (BOLA), Broken User Authentication, Excessive Data Exposure, and Mass Assignment**.
- **Penetration Testing (PT):** Performed in-depth API security testing, identifying **OWASP API Security Top 10** vulnerabilities such as **Injection (SQLi), Broken Access Control, Server-Side Request Forgery (SSRF), and Insecure Direct Object References (IDOR)**.
- **Reporting:** Compiled and delivered a detailed API security assessment report, documenting vulnerabilities, their impact, and remediation strategies.

Payment Gateway Security Testing
Roles and Responsibilities:

- Performed comprehensive security testing for India's leading banking platforms, covering **Web, UPI, Android, and iOS** channels.
- Conducted **functional, integration, and regression testing** to ensure seamless payment flows across multiple merchant types and transaction scenarios.
- Executed **3DS2 authentication, PCI-DSS compliance, and encryption validation** for secure transaction processing.
- Validated **transaction life cycle events** including authorization, capture, refund, cancellation, and chargeback flows.
- Tested **UPI mandates, collect requests, intent-based payments,** and QR code scanning for end-to-end reliability.
- Performed **positive, negative, and edge-case scenarios** to assess system behavior under high load and network disruptions.
- **Reporting:** Compiled and submitted a detailed **VAPT report** to the client, outlining all confirmed findings and providing remediation recommendations.

Education

- **Bachelor of Computer Science**, Savitribai Phule Pune University **2023**
  CGPA: 8.85
- **Master of Computer Application**, Savitribai Phule Pune University **2025**
  CGPA: 7.89