Chetan Raghunath Chaudhari

chetanchaudhari1183@gmail.com +91 9767193362
Pune, Maharashtra

Results-driven **Security Analyst with 2+ years** of experience in **Web & API Security Testing**, specializing in **Vulnerability Assessment and Penetration Testing (VAPT)**. Proficient in **manual & automated security testing, identifying and mitigating security risks in web applications, APIs, and networks**. Skilled in security tools such as **Burp Suite, Nessus, and OWASP ZAP**. Strong understanding of **OWASP Top 10, API Security, and Web Application Security**. Passionate about securing applications and continuously learning advanced attack techniques.

Professional Summary

- Over **2 years and 2 months** of experience in **Vulnerability Assessment and Penetration Testing (VAPT)**, security testing, and penetration testing.
- 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, 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

Security Analyst at MarkGenic Software PVT LTD, Pune *January 2023 - Present*

Projects

Web and Security Assessment
Client: Sekure CRM
Project Overview: Sekure CRM is a comprehensive **payment gateway and management platform** designed for merchants across various industries, including **retail, restaurants, grocery, and wholesale**. It offers several key features to streamline business operations and enhance customer support:

- **CRM Portal:** A centralized system for managing users, employees, and merchants efficiently.
- **Sek Partner Portal:** A dedicated platform enabling resellers to manage Sekure product sales.
- **Commission Portal:** Provides real-time earnings insights for commission agents.
- **QA Portal:** Handles customer queries effectively, prioritizing them based on severity and urgency.

Sekure CRM enhances **payment processing, business management, and customer engagement** by offering an integrated and secure platform tailored to merchant needs.

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.

Network VA
Roles and Responsibilities:

- Conducted network vulnerability assessments using **Nessus and Nmap** to identify security risks and weaknesses.
- Analyzed and prioritized vulnerabilities based on **risk severity and business impact**.
- Validated findings to eliminate false positives and provided actionable insights.
- Prepared detailed reports with prioritized recommendations for remediation.

Education

- **Degree:** Bachelor Of Computer Science
- **Institution Name:** Savitribai Phule Pune University
- **Graduation Year:** 2023
- **CGPA:** 8.85