KOTESWARARAO K

Security Analyst

+91-7670868221 | koteswarcstech@gmail.com

Experience Highlights:-

- Over 5 years of experience in security assessments **Vulnerability Assessment and Penetration Testing.**
- Hands on experience in both **Mobile** & **Web Based Application Security Testing (SAST/DAST).**
- 2years of experience in **Source Code Review** (SAST) analysis.
- Hands on experience with both **Automation and Manual Testing Tools.**
- Performed Application Penetration Testing for various clients.
- Assisting in review of business solution architectures from security point of view which helps avoiding security related issues/threats at the early stage of project.
- Experience in running scans on Source code files **using Checkmarx and verifying vulnerabilities to eliminate false positives.**
- Skilled using Various Tools for web application penetration tests such as **Burp Suite, OWASP ZAP, Checkmarx, Wireshark, WinHex, Nmap, Nessus, Acunetix**.
- Ability to perform Threat modeling, secure code review, Penetration Testing (Web), Vulnerability Assessment.
- Proficient in understanding application level vulnerabilities like **XSS, SQL Injection**, **authentication bypass, weak cryptography, Session Management**, etc.
- Performed Web Application Security / Penetration Testing in accordance with OWASP standards and SANS guidelines, using manual techniques and Automation tools.
- Skilled in executing **OWASP top 10 test cases.**
- Conducted **application architecture review** for few projects.
- Publishing monthly dashboards, taking follow up for closure of vulnerabilities.
- Executing test cases, reviewing results, and working with development team to remediate the open issues.
- Reporting the identified issues in the industry standard framework.

Education Summary: -

- B Tech – Electronics & Communication Engineering from Loyala Institute of Technology college, JNTUK University, GUNTUR in 2015.

Professional Experience: -

Working as **Security Analyst** in **Tech-Mahindra(C2H)** Services , From Aug-2018 to tilldate

Trainings and Certifications: -

- **CEH Certified**
- Cyber Securities Workshop

Skills Summary: -

Testing	:	Security Testing
Industry Standards	:	OWASP-Top 10
Vulnerability Assessment Tools	:	Burp Suite, OWASP ZAP, WebInspect, Nmap, Wireshark, WinHex, Acunetix, SSL Scan.
Source Code Review Tools	:	Checkmarx
API Testing Tools	:	Postman
Operating Systems	:	Windows, Linux
Programming Languages	:	HTML, CSS, JavaScript, Python

Key projects: -

Client: AT&T
Role: Test Engineer

Roles & Responsibilities:-

- Conducted web application penetration testing on business applications
- Perform infrastructure security assessments by analyzing the networks, enumeration of services on hosts and identify vulnerabilities.
- Exploitation of identified vulnerabilities in network hosts by using existing exploits or manual methodologies.
- Manual web application penetration testing using Burp Suite.
- Using web application vulnerability scanners like **Webinspect and checkmarx to perform automated testing.**
- Proficient in identifying application-level vulnerabilities like **XSS, SQL Injection, CSRF, IDOR, Authentication & Authorization bypass and Cryptographic flaws etc**.
- False positives removal by analyzing the results from automated scanners.
- Reporting the vulnerabilities with evidences, business impact and remediation steps.
- Responsible for timely delivery of status updates and final reports to clients.
- Work closely with developers and network/system administrators while fixing the findings.
- Vulnerability management by keeping track of reported issues and ensure fixing.

Client: Hartford Insurance
Role: Test Associate

Roles & Responsibilities:-

- Using web application vulnerability scanners to perform automated assessments.
- Manual penetration testing of the applications to identify vulnerabilities based on OWASP standard.
- Performed mandatory security checks based on Input Validation, Authentication, Authorization, Configuration Management, Sensitive Data Exposure and Session Management.
- Performed security testing on **APIs using Postman**.
- Performed **Threat Modelling of the applications in coordination with development teams**.
- Used Nessus and Nmap to perform network wide security assessments.
- Provided details of the issues identified and the remediation plan to the stakeholders.
- Manual report generation/submission for daily maintaining tasks.
- Using standards like **CVSS (Common Vulnerability Scoring System) to provide the severity (Critical, High, Medium, Low)** rating to the vulnerabilities identified.

DECLARATION: -

I consider myself with all above mentioned aspects. I am also confident of my ability to work in a team. I hereby declare that the information furnished above is true to the best of my knowledge.

KOTESWARARAO K