

D . Praveen Kumar

Mobile No: 8919616827



Email id: devaragudipraveen8@gmail.com

PROFESSIONAL SUMMARY

Security Engineer with hands on experience on vulnerability Assessment and Penetration Testing, Web Security, Network Security, Mobile Security, End Point Management and Security Standards – OWASP Top 10, SANS 25, GDPR etc.

PROFESSIONAL EXPERIENCE

4.2years (May 2019 to till date) of experience in

Novitas Technologies private limited as a Security Engineer.

CEH- Certified Ethical Hacker

Trained and Certified in Certified Security Tester Certification

TECHNICAL SKILLS

- | | |
|-------------------------------------|---|
| ➤ Vulnerability Scanners (DAST) | : Nessus, ZAP, App Scan, Qualys, Veracode, Burp Suite |
| ➤ Vulnerability Scanners (SAST) | : Veracode, Checkmarx , App Scan – source, SonarQube |
| ➤ Network Scanning and monitoring | : Nmap, Wireshark, Netcat |
| ➤ Penetration Testing Tools | : Metasploit, msfvenom, Open Source Intelligence methodology |
| ➤ Mobile Security | : Emulators – Genemotion, Dex2Jar, UnZip, APK Tool, Java De-compiler, |
| ➤ Security Standards and Compliance | : OWASP Top10, SANS 25, PCI-DSS, GDPR , HIPPA |
| ➤ Web Technologies | : HTML, Java, JavaScript, XML Web Services |
| ➤ Operating Systems and Cloud | : Windows family, Kali Linux |
| ➤ Database and Servers | : Sql Servers 2008/2012/2016, Apache, Tomcat, IIS, Postgresql |
| ➤ Defect/Test Tracking Tool | : JIRA |

WORK HISTORY

Security Engineer, 5/2019 to Till Date

Novitas Technologies private limited – Bangalore, India

- ❖ **Manual Threat Modelling:** Threat modelling of web applications using STRIDE, DREAD, CVSS and Attack Tree techniques.
- ❖ **Secure Architecture:** Secure architecture and coding of web applications using threat modelling in conjunction with SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing) Tools.

- ❖ **SAST (Static Application Security Testing):** Performed source code reviews to the applications using enterprise automated tools and Manual process. Performing False Positive analysis.
- ❖ **DAST (Dynamic Application Security Testing):** Performed Vulnerability Assessment for web applications, API and Network. Validating the target for all the vulnerabilities like XSS, SQL Injection etc.
- ❖ **Mobile Security:** Good Knowledge and working experience in reverse engineering on binaries and applications and reverse engineering tools. Experience in Emulators, Simulators and mobile security Tools like Dex2Jar, MobSF, Genemotion, APK Tool etc.
- ❖ Analysis of Cryptographic standards - Encryption, Hashing, Digital certificate for all the applications and suggesting the best standards based of the purpose of the application.
- ❖ Configuring web applications for dynamic scanning using any of the authentication methods like Basic authentication, Forms authentication etc.
- ❖ Knowledge of Integration of CI/CD tools like Jenkins, Team City with Dynamic and Static application scanners.
- ❖ Analysis of Project requirement documents and functional specification document.
- ❖ Defining scope of security testing for the application based on the requirement analysis.
- ❖ Define security testing tasks or user stories to include in the projects test activities backlog.
- ❖ Identification of Resources, Timelines, Risks and Dependencies for Security Testing.

Significant Projects:

Project:	US based Insurance Application - VAPT
Description:	Web application VAPT -Vulnerability Assessment and Penetration Testing for Insurance based client portal
Position:	Security Analyst
Contribution:	<ul style="list-style-type: none"> • Vulnerability Assessment and Penetration Testing for Web application and API. • Secure designing and Architecture. • Created use cases based on the Secure design. • Preparation of Test Strategy based on the Security use cases. • Taking part in user story understanding. • Performing threat modeling session using STRIDE. methodology with the development team and identifying threats before development work on story begins. • Add the identified threats as user stories in backlog alongwith main functional story. • Creating test cases for user stories identified as threats with OWASP top 10 standards, testing using Burp Suite, and SOAP UI.

	<ul style="list-style-type: none"> Execute the threat user stories test cases once the security requirement is developed. <p>Training other test engineer/QA member on threat modeling process and creating test case using OWASP top 10 standards.</p>
Team Size:	8

Project:	Banker Portal
Description:	Web Application and API Penetration Testing for the banking portal.
Position:	Security Test Engineer
Contribution:	<ul style="list-style-type: none"> Vulnerability Scanning using Web vulnerability scanner Veracode, Qualys and Burp suite Pro. Manual Verification of automated scan reports. Analysis of vulnerabilities and executions to meet the compliance. Security Test Strategy preparation and approvals. Security Test execution and reporting as per the CVSS Standards. Worked with cross functional teams to resolve dependencies and risks. Defect Logging and Defect Tracking in QC and JIRA. Creating test cases as per OWASP top 10 standards and taking part in execution. Performed API Pen Testing using POSTMAN and Burp suite.
Team Size:	6

EDUCATION

B. Tech (Electronics and Communications), 03/2012.]

MOULA ALI College of Engineering, JNTU, Anantapur.

DECLARATION

I, **D . Praveen**, do hereby confirm that the information given above is true to the best of my knowledge.

Date:

Name:
D Praveen

Place:

WORK HISTORY

