**Sr. SECURITY ANALYST**

**TEJASWINI**

**Contact No:** (443) 467-9066

**Email:** tgalla028@gmail.com

**SUMMARY**

* Professional with **6** years of progressive experience in Information Technology with extensive experience in Information Security, Application Security, Penetration Testing, Security Architecture Review, PCI DSS Compliance, Project management and Team building.
* Expertise in performing Application Security risk assessments throughout the SDLC cycle.
* Excellent knowledge in CWE, OWASP Top 10 2017, and WASC THREAT CLASSIFICATION 2.0 methodologies.
* Leading the Application security team which includes Application Security design, review, testing and remediation
* Good understanding of the different **PCI DSS** domains.
* Proven experience in manual/automated security testing, secure code review of web and mobile applications.
* Expertise in identifying flaws like SQL Injection, Insecure Direct Object Reference, Security Misconfiguration, Sensitive Data Exposure, Cross Site Scripting (XSS), CSRF, Phishing Through Frames, Link Injection, Broken Authentication, Sensitive Data Exposure, Security Misconfiguration, Insufficient Logging and Monitoring and Unvalidated Redirects.
* Security assessment based on **OSSTMM** methodology and **OWSAP** framework.
* Experience in different web application security testing tools like **Acunetix**, **Metasploit**, **Burp Suite**, Sqlmap, **OWASP ZAP Proxy, HP Fortify** and **Veracode**.
* Capabilities include project & client relationship management, metrics and reporting.
* Expertise in managing large security programs comprising different security domains and global teams.
* Experience in establishing process for periodic reviews of privilege user groups at AD, database and application level.
* Implementation and review of **security controls** across **SDLC**.
* Expertise in Security Information and Event Management (**SIEM**), Intrusion detection & Prevention, TCP/IP, Forensics and malware Analysis tools.
* Strong understanding of Agile and Scrum methodologies.
* Good understanding of the different security and distribution groups in **AD**, privileges roles on databases, different **GPO** policies pertaining to User Account Control.
* Security analysis of **Firewall** rules and **Web proxy policies**
* Infrastructure (OS, Database, Web servers) audits.
* Good experience in Web technologies like HTTP, HTML, CSS, Forms, Database Connectivity.
* Experience using automated vulnerability assessment tools (**Qualys, Nmap, Retina, Nessus, Nexpose)**.
* Playing progressive roles from Functional Tester, Developer and Security Analyst to Lead Security Consultant.
* Reported critical vulnerabilities like SQL Injection, Remote Code Execution, Cross Site Scripting as a part of the Security research program through the medium of bug bounties

**EDUCATION**

* **Masters** at Kent State University, Ohio

**TECHNICAL SKILLS**

**Languages:** Java, ASP.NET, SQL, Shell Scripting, HTML, JavaScript

**Tools:** IBM App Scan Enterprise, AppScan for Source Analysis, Veracode, Qualys,

HP Web Inspect, Nessus, Nmap, **Burp Suite**, Postman and Fiddler.

**Skills:** Pen Testing, SAST, DAST

**Methodologies:** OWASP, CVE, BSSM

**Other Tools:**  Visual Studio, Soap UI, Eclipse

**Compliances:**  HIPAA, PCI, PHI, PCI DSS

**Databases:** MongoDB, IBM DB2, MS-SQL, MySQL

**Operating System:** RHEL, Linux, Windows

**Domains:** Healthcare, Retail, Airlines

**EMPLOYMENT**

**United Airlines, IL**

**Role: Security Engineer III**  **May 2018– Present**

* As a security advisory analyst primary function is to Support the information security consultancy function by analyzing the Projects for security risks. And impacts, documenting and communicating. Requirements and recommendations and monitoring compliance through the development lifecycle.
* Working on creating the application profile, policy settings and manual scans as the primary scope of Veracode Implementation for SAST scans.
* Providing best security practices and guidance for **OAM** integrations.
* Planning, Scheduling, tracking and reporting on manual/automated security testing on the internet and intranet applications.
* Extensive experience on Dynamic scans as part of **GDPR** to ensure that all united systems house data are up to the level of security required.
* Defined the security program and integrated application security throughout all phases of Software Development Life Cycle (SDLC) from Requirements Gathering to Testing.
* Review and Validate the User Access Compliance on a quarterly basis
* Review the requirements for privileged access on an everyday basis and provide recommendations.
* Review and validate the privileged users and groups at Active Directory, Databases and application on a periodic basis.
* As part of security advisory team working closely with **IAM** team on access management and authentication process for on boarding applications.
* Reviewing the applications for **OAM** requests on providing access and approvals.
* Establishing and improving the processes for privileged user access request.
* Highlight the user access and privileged user access risks to the organization and providing the remediation plan.
* Initiative to stream line the access control mechanism of various applications.
* Provided the development team with detailed reports based on the findings obtained from the manual and automated testing methodologies, also provide the necessary remediation for individual findings.
* Attended meetings with development team to discuss the previously submitted reports on the findings to ensure that the fixes are made to those applications.
* Performed a threat analysis on the new requirements and features.

**Tools and Methodologies:** OWASP, Burp Suite, Qualys WAS.

**Agero, MA**

**Role: Penetration testing/Security Tester Aug 2016 – April 2018**

**Team**: Application Development– This team is Responsible for developing and testing all the web and desktop applications for the users who use services of Agero.

* Performing manual application security testing on the everyday changes carried out in the application.
* Used various Firefox add-ons like Flag fox, Wappalyzer, Live HTTP Header, Tamper data to perform the pen test.
* Scan Networks, Servers, and other resources to validate compliance and security issues using numerous tools.
* Port scans servers using NMAP and closes all unnecessary ports to reduce the attack surface.
* Performing Server Hardening Audits which includes OS, Database, and Web Servers
* Developed Hardening scripts for Linux OS, Apache Web server and Oracle database.
* Conduct penetration testing using automated tools such as AppScan, Paros Proxy, WebInspect, Traffic Viewer, TCP Dump etc.
* Experience in using Kali Linux to do web application assessment with tools like Dirbuster, Nikto, and Nmap
* Leading the online application team in reporting the issues and taking them to closure
* Performing static code reviews with the help of automation tools
* Performing a threat analysis on the new requirements and features
* Review of firewall rules and policies in web proxy.
* Highlight the user access and privileged user access risks to the organization and providing the remediation plan.

**Tools:** OWASP, OSSTMM, PCI DSS, IBM App Scan, HP Web Inspect, Nessus, Nmap, **Burp Suite**, Web Scarab, Wire Shark, DirBuster

**Vsoft Corporation**

**Role: Application Security Analyst Aug 2015– Dec 2015**

* Performed Web Application Security / Penetration Testing in accordance with OWASP standards using manual techniques and also automated tools.
* Vulnerability assessment using Nessus and other monitoring tools like ESM for asset management
* Black box pen testing on internet and intranet facing applications.
* In the team, main focus of work was to audit the application prior moving to production
* Verify if the application has implemented the basic security mechanisms like Job rotation, Privilege escalations, Lease Privilege and Defense in depth.
* Conduct source code review of application using Fortify.
* Good experience in Web technologies like HTTP, HTML, CSS, Forms, Database Connectivity.
* Guiding the developers in fixing the issues by simulating the attack
* Performing a threat analysis on the new requirements and features