IT Security Engineer / Analyst IT Security Engineer / Analyst IT Security Engineer / Analyst - Fannie Mae Bethesda, MD IT Security Engineer with around 9 years of experience. Responsible for the overall security posture of the organization including Security Architecture & Design, Cloud Security, Security Investigation, Third Party Vendor Assessments, Network Security, Penetration Testing and Secure Coding. In-depth knowledge of .Mobile Application Security, Application Security Controls and Validation, IT Risk Assessments, Continuous Integration (CI) and Continuous Delivery (CD) and Automation of Vulnerability Scanning (DevSecOps), Incident Response (IR), Regulatory Compliance (NIST, PCI-DSS, CIS, FFIEC, HIPAA, SOX) and Secure Software Development Life Cycle (secureSDLC). Authorized to work in the US for any employer Work Experience IT Security Engineer / Analyst Fannie Mae - Bethesda, MD February 2015 to Present Responsibilities: Conducted Vulnerability Assessment (DAST and SAST) of Web and Mobile (iOS and Android Applications, including third party applications. The tools IBM AppScan, ZAProxy, BurpSuite Pro, Checkmarx, HP Fortify have been utilized for scanning the applications. Conducted IT security risk assessments including, threat analysis and threat modeling (STRIDE). Performed code analysis with CHECKMARX. Conducted application penetration testing of 85+ business applications. Triaged security vulnerabilities to eliminate false positives and worked with the developers for remediation. Acquainted with various approaches to Grey & Black box security testing. Hands-on with database security / Vulnerability scanner using ImpervaScuba. Implemented Secure Software Development Life Cycle processes; developed secure coding practices for web, mobile applications, including database and middleware systems. Developed Security API and deployed to development teams which helps them write lower risk applications in a secure manner. Participated in the implementation of Public Key Infrastructure (PKI) for securing data at rest and data in transit. Involved in the implementation of encryption and decryption of confidential data and supported the certificate key life cycle. Developed security policies and standards and made sure the business applications are in compliance with the standards. Conducted architectural reviews of OAuth2.0, SAML and Single Sign-on (SSO) for corporate applications. Implemented IAM for various applications deployed in the AWS Cloud. Developed IAM policies, roles controlled access to the users. Created AWS S3 Bucket policies. Identifying the critical, High, Medium, Low vulnerabilities in the applications based on OWASP Top 10 and SANS 25 and prioritizing them based on the criticality. Proficient in understanding application level vulnerabilities like XSS, SQL Injection, ClickJacking, CSRF, authentication bypass, cryptographic attacks, authentication flaws etc. Conducted security assessment of PKI Enabled Applications Skilled using Burp Suite Pro, HP Web Inspect, IBM AppScan Standard, Source and Enterprise, NMAP, Qualysguard, Nessus, SQLMap, RSAArcher, FireEye Retina for web application penetration tests and infrastructure testing. Performing onsite & remote security consulting including penetration testing, application testing, web application security assessment, onsite internet security assessment, social engineering, wireless assessment, and IDS/IPS hardware deployment. Capturing and analyzing network traffic at all layers of the OSI model. Monitor the Security of Critical System (e.g. e-mail servers, database servers, Web Servers, Application Servers, etc.). Performed pen testing of both internal and external networks. The pen testing scope included O/S SQL, Oracle Database. Performed the configuration of security solutions like RSA two factor authentication, Single Sign on (SSO), Symantec DLP and log analysis using Splunk SIEM. Change Management to highly sensitive Computer Security Controls to ensure appropriate system administrative actions, investigate and report on noted irregularities. Conduct network vulnerability assessments using tools to evaluate attack vectors, Identify System Vulnerabilities and develop remediation plans including, security policies, standards and procedures. The experience has enabled me to find and address security issues effectively, implement new technologies and efficiently resolve security problems. With having strong Network Communications, Systems & Application Security (software) background looking forward for implementing, creating, managing and maintaining information security frameworks for large scale challenging environments. Security Engineer Vodafone, HYD, IND May 2012 to February 2015 Responsibilities: Conducted Vulnerability Assessment for various applications. Managed security assessments to ensure compliance to firm's security standards (i.e., OWASP Top 10, SANS25). Specifically, security testing has been performed to identify XML External Entity (XXE), Cross-Site Scripting and SQL Injection related attacks within the code.

Conducted security assessment of Cryptography applications including the apps that use Hardware Security Model (HSM). Performed the penetration testing of mobile (Android and iOS) applications, specifically, APK reverse engineering, traffic analysis and manipulation, dynamic runtime analysis was performed. Participated in Web Application Security Testing including the areas covering Mobile, Network, security, WIFI. Skilled using Burp Suite, Checkmarx, HP Fortify, NMAPfor web application penetration tests. Security assessment of online applications to identify the vulnerabilities in different categories like Input and data Validation, Authentication, Authorization, Auditing & logging. Vulnerability Assessment of various web applications used in the organization using Burp Suite, and Web Scarab, HP Web Inspect. Experience with Identity and Access Management (IAM) and development of user roles and policies for user access management. Analyzed correlation rules developed for SIEM(Splunk) system. Follow up and ensure the closure of the raised vulnerabilities by revalidating and ensuring 100% Closure. Update with the new hackings and latest vulnerabilities to ensure no such loopholes are present in the existing System. Security Engineer Equifax - Alpharetta, GA November 2009 to May 2012 Roles and Responsibilities: * Performed the tasks of designing Advanced Security & Management Solutions for the organization. * Experience with Identity and Access Management (IAM) and development of user roles and policies for user access management. * Performed dynamic and static analysis of web application using IBM AppScan * Well versed with various vulnerabilities and attacks at application - OWASP top 10, SQL Injection, XSS, CSS, LDAP injection, XPath injection etc. * Conducts regularly review of Global Security Incidents as well as reports and update the same to the internal teams. * Deployed and configured Symantec Data Loss Prevention (DLP) for both data in transit and data at rest. * Execute and craft different payloads to attack he system to execute XSS and different attacks * Identified database security vulnerabilities using SQLMAP pen testing tool. * Performed IT Risk Assessment Services and provides Solutions to mitigate Risks identified and reported. * Conducted security assessments for various applications supporting Corporate & Investment Banking, Loan, Treasury, Equities and FI businesses. The web application infrastructure such as IBM WebSphere, Apache Tomcat, and IIS web/application servers were reviewed for compliance to firm's security baselines. * Developed correlation rules for Security Incident and Event Management (SIEM) system. Reviewed the solution implemented for "log forwarding" from various network devices to ArcSight central logging for alerting and security monitoring. * Ensured that the operation, design, and management of information systems are in according to the standards of the organization. * Established and maintained a framework to ensure that information security policies, technologies and processes are aligned with the business regulations of the organization. * Identifies as well as applies innovative practice in security to enhance the global operations of the organizations. * Performed risk assessments and defines strategies to address the identified risks. * Ensured that risk identification, mitigation controls and analysis are integrated into application life cycle and change management processes. * Performed PCI-DSS (3.2, 3.1) pre-assessment audit for the entire network as well as the related applications in preparation for the annual external PCI compliance audit. Education Bachelor's

Name: Ronald Parker

Email: smithsandra@example.net

Phone: (402)462-9926