**Ravi Sujith**

**Email:ravsujitej@gmail.com**

**Tel: 773-999-5627**

**SUMMARY:**

* 10+ years of Information Security, design and development experience in information security architecture, cryptography, security assurance, threat modeling, IT risk assessments, SSO, and risk remediation activities.
* Expertise in Application Security and identifying and fixing **OWASP** Top 10 and **SANS 25** security vulnerabilities.
* Implementation of **Docker** **Container** **Security** on Linux platforms. Development of **DevcSecOps** tools for automation.
* Strong foundation and In-depth technical knowledge of security engineering, computer and network security, authentication and security protocols.
* Hands-on with Penetration Testing, **DAST, SAST** and manual ethical hacking.
* Experience in conducting IT Security Risk Assessments in accordance to **NIST and FFIEC** framework.
* Worked with global security teams performing application and IT infrastructure security assessments.
* Performed security design and architecture reviews for web and mobile applications.
* Hands-on experience in developing threat models, security controls, threat analysis, creation of risk control matrices and risk mitigation strategies.
* Worked on Imperva and **AWS Cloud Security** in implementing Web Application Firewalls **(WAF).**
* Experienced in OWASP Top 10 and SANS Top 25 software guidelines, Federal Financial Institutions Examination Council's **(FFIEC)** regulations, including Payment Card Industry (PCI-DSS), HIPAA and Sarbanes-Oxley Section404 **(SOX),** SysTrust and SSAE 16.
* Experience in implementing Security Incident and Event Management System (SIEM) using HP ArcSight, Splunk.
* Ability to handle multiple tasks and work independently as well as in a team.
* An efficient team player in challenging and creative environment with excellent capacity to adapt new technologies and skills.
* Possess strong technical aptitude with strong analytical, work ethic, problem solving and communication skills.
* Proficiency with scripting languages such as Python, Perl, Java Script and Power Shell.

**TECHNICALSKILLS:**

***Information Security Tools:***

Paros, Nmap, BMC BladeLogic, Nessus, Rapid7 Nexpose, Tripwire, CyberArc, BeyondTrust, Symantec DLP, DBProtect, e-DMZ Password Auto Repository (PAR), Varonis, AppDetect, AppRador, JHijack, Metasploit Pro, ZED attack proxy, SQLMAP, Wireshark, Web Scarab, Amazon Web Services (AWS) Cloud security.

***DAST and SAST Tools:***

Fortify SCA, IBM AppScan Enterprise (ASE), Standard & Source editions, HP Web Inspect, QualysGuard, Burp Suite Pro, and SQL MAP.

***Operating Systems:***

Oracle Solaris UNIX, RedHat LINUX 4/5, Windows Server2003/2008.

***Java & J2EE Technology:***

Spring Framework, EJBs, Struts2, Servlets, Java Server Pages (JSPs), JMS, Java Mail API, JNDI, LDAP, JDBC, JTS, RMI, AWT, Swing, Socket Programming, IONA Orbix CORBA.

***DevSecOps:***

Jenkins, Maven, Docker Container, GitHub, TFS, BOTO3, AWS CLI, AWS ClooudWatch, AWS Config.

***SIEM:***

HP ArcSight ESM, Logger, Smart Connectors, Express, Splunk.

***Networking***:

Symantec Vontu DLP, Checkpoint, Palo Alto, Check Point, Cisco, IDS/IPS, Anti-virus, BMC BladeLogic, Remedy.

***Application Servers:***

Weblogic Server, Iplanet, Netscape Application Server and Microsoft IIS.

***Languages:***

Java, Python, C/C++, C#.NET, Perl, UML.

***Scripting Languages:***

AngularJS, XML, XSLT, XPath, XQuery, HTML/JavaScript/JQuery, AJAX.

***Middleware:***

TIBCO EMS, IBM WebSphere MQ, JMS.

***Databases:***

Oracle, MS SQL Server, Sybase.

***Web Services:***

Restful/SOAP, SOA, UDDI, WSDL.

***Web Servers:***

Apache Tomcat, Netscape Enterprise Server3.5, JBoss and JRun.

**EDUCATION:**

Bachelor of Engineering, India

**SECURITY CERTIFICATIONS / TRAINING:**

* Certified Information Systems Security Professional (CISSP) In Process
* Certified Security Analyst **(CSA)**
* Certified Ethical Hacker **(CEH)**

**WORK EXPERIENCE:**

**CVS Health, Woonscoket, RI**

**Sr. Security Engineer Feb 2017 – Present**

* Multifactor Authentication **(MFA)** for **AWS** root accounts (Implementation), designed password rotation policies. Management of Access Keys, Secret Assess Keys for new users.
* Developed **WACLS** for **AWS** Web Application Firewalls **(WAF)** and configured the rules and conditions to detect security vulnerabilities in Cloud.
* Developed security requirements for applications and infrastructure deployed in the Cloud.
* Developed security requirements for both infrastructure and applications (web and mobile) and worked with Infrastructure engineering, application development, DBAs, SysAdmin teams and made sure the requirements are incorporated into the systems during the design and architecture phase of the delivery life cycle.
* Rolled out **IBM AppScan** products such as **AppScan Enterprise (ASE),** Standard, Source, Developer plug-ins to various development teams across the business lines.
* Performed 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, ClickJacking, Session Management/Hijacking, and SQL Injection related attacks within the code.
* With team, Implemented data token in different environments to ensure compliance (AWS- Cloud).
* Developed **DevSecOps** tools for automating various security scanning processes. The tools such as Jenkins, Python, **Docker**, PowerShell, **BOTO3, and AWS CLI** have been used for automation. Developed AWS Security Groups to control traffic.
* Secured **Docker Container** workloads by implementing **namespaces,** control groups and access controls for workloads.
* Installed, configured and administered IBM AppScan Enterprise, including scan agent configuration, scan scheduling, troubleshooting of failed scans, user administration.
* Implemented authentication solutions for various types of applications using **OAuth2.0, SAML** and OpenID.
* Good understanding of web application attacks including **SQL, XSS, ClickJacking, CSRF**, and other common security issues beyond the OWASP Top 10.
* Designed security architecture for web and mobile apps. Reviewed Solution overview Documents **(SODs)** to identify security anomalies in the system architecture and design, and provided recommendations to address data security and privacy concerns.
* Developed threat modeling framework **(STRIDE, DREAD)** for critical applications to identify potential threats during the design phase of applications.
* Worked extensively with software development teams to review the source code, triage the security vulnerabilities generated by IBM AppScan, **Burp Suite, Imperva WAF HP Web Inspect**, **HP Fortify** and eliminated false positives.
* Participated in the development of IT security risk assessments for enterprise applications. The NIST, HIPAA frameworks have been utilized for IT risk assessments. This included leading the data discovery meetings, identification of existing controls and validates them against the expected controls. The control gaps or non-compliance to security policies were presented to the stake holders for remediation.
* Working knowledge of Splunk in developing search queries including, knowledge objects such as Event Types, Tags, Database Queries etc.
* Configured **Safenet / Gemalto ProtectDB** to enable column level encryption for securing confidential customer data.
* Implemented file system security by applying hashing techniques for protecting data stored in files on the file servers.
* Ensured that Cloud security best practices have been followed. Configured **AWS Simple Storage Service (S3)** to secure organization’s critical file systems. Implemented **Access Control Lists (ACLs)** and Bucket Policies for controlling access to data.
* Developed AWS Service Roles to protect Identity Provider access. Implemented multiple layers of security, including security groups, network access control lists, to control access to Amazon EC2 instances in subnets.
* Performed the **API** security testing of web services including **SOAP, REST, and JSON/XML.**
* Performed penetration testing for mobile applications.
* Implemented authentication for applications using web application vulnerability scanning tools (IBM AppScan, IBM AppScan Source, **HP Fortify, HP Web Inspect, Burp Suite Pro, ZAP, Kali Linux, etc.).**
* Implemented **SSO for Azure AD** & Mobile applications.
* Good configuration Knowledge with SSO, Fortify, **Checkmarx**, AppScan for Web and Mobile Applications and remediation of issues.
* Strong knowledge of web application security, web-related protocols **(HTTP, HTTP/2, SSL, WebSockets,** etc.).
* Administered cryptography, public and private key management and implemented dual keys to address segregation of duties issue between DBAs and security Admins.
* Generated executive audit summary reports showing the security assessments results, recommendations and risk mitigation plans and presented them to the respective business sponsors and senior management.
* Worked with **DevOps** teams to automate security scanning into the build process.
* Participated in the implementation of Imperva Database Activity **Monitoring (DAM) and AWS Cloud security** for applications being deployed in the Cloud. Developed **WACLS** and configured to rules and conditions to detect security vulnerabilities in the Cloud Front.
* Developed security best practices for the applications and infrastructure deployed in AWS.
* Analyzed security incidents originated from various network/application monitoring devices (e.g., **Symantec DLP**) and coordinated with engineering teams for tracking and problem escalation, root cause analysis, including remediation.
* Performed the penetration testing of mobile (Android and iOS) applications, specifically, APK reverse **engineering**, traffic analysis and manipulation, dynamic runtime analysis.

**Blue Cross Blue Shield Association, Chicago, IL**

**Sr. Security Engineer June 2014 – Dec 2016**

* Performed pen testing of both internal and external networks as per **PCI-DSS** standards. The pen testing scope included O/S (Windows and Linux) and external facing web apps and database servers that store credit card information.
* Reviewed security vulnerability reports for applications and databases, analyzed and worked extensively with the development teams for the implementation of mitigating controls.
* Implemented **IBM AppScan** standard, source editions, HP Web Inspect and QualysGuard web application scanners. In addition, the security tools Metasploit and Burp Suite were utilized for manual penetration testing.
* Performed security assessments for the client-facing apps. The associated IT infrastructure such as database management systems, middleware systems, web services (SOA) were also included in the security assessments.
* Implemented Secure Software Development Life Cycle **(S-SDLC)** processes; developed secure coding practices for web, mobile applications, including database and middleware systems.
* Reviewed **Architecture Design Documents (ADD)** and Solution overview Documents (SODs) to identify security anomalies in the system architecture and design, and provided recommendations to address data security and privacy concerns.
* Implemented **HP ArcSight ESM** including, correlation rules, data-monitors, reports, event annotation stages, case customization, active lists, and pattern discovery.
* Conducted manual source code audits of the client-facing Wyndham brand web and mobile applications, including iOS and Android mobile apps. The key areas of confidential and sensitive data stored on the mobile devices were reviewed and made recommendations to secure customers’ PII and PCI data.
* Conducted pen testing for the Web Services **(SOA)** used by various travel agency partners to connect to Wyndham for booking and reservations.
* Reported security findings, recommendations and presented to the business users, executive committee and Compliance departments.
* Experience with Identity and Access Management **(IAM)** and development of user roles and policies for user access management.
* Performed Static and Dynamic Analysis and Security Testing **(SAST and DAST)** for various applications as per firm’s security standards (i.e., OWASP, SANS 25).
* Conducted workshops and user awareness training on security policies, procedures and baselines.
* Worked with software development teams, DB/Unix administrators and solution architects as a subject matter expert related to security compliance with PCI DSS and industry standards.
* Worked with Internet Engineering team in the design and configuration of Bluecoat Internet proxy. Implemented WebFilter database for URL content Filtering.
* Developed security policies and baselines for mobile and web applications. Performed compliance audits to ensure security policies and baselines have been adequately implemented.
* Participated in the implementation of Safenet / Gemalto product for encrypting customer credit card information using Public Key Infrastructure **(PKI).**
* Developed correlation rules for Security Incident and Event Management **(SIEM)** system. Reviewed the solution implemented for “log forwarding” from various network devices to HP ArcSight central logging for alerting and security monitoring.
* Performed PCI pre-assessment audit for the entire network as well as the related applications in preparation for the annual external PCI compliance audit.

**Morgan Stanley, New York, NY**

**Sr. Security Engineer Sept 2011 – May 2014**

* Performed the review of a newly implemented Security Incident and Event Management (SIEM) system. Reviewed technical specifications for SIEM, logging and proposed recommendations to improve the overall deployment of the solution.
* Developed security audit programs for IT infrastructure supporting Corporate and Investment Banking (CIB) department to facilitate end-to-end compliance with Global as well as Federal Financial Institutions Examination Council (FFIEC) guidelines and controls. Well versed with SysTrust and SSAE 16 Standards too.
* Managed Telecommunications audit mission covering Voice over IP (VoIP) infrastructure implemented in the firm.
* Performed penetration testing for external facing web applications. Security areas covering DMZ architecture, threat modeling, secure coding practices (i.e., OWASP standards) and vulnerability analysis were assessed.
* 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.
* Managed security assessments for various types of Operating Systems (O/S) used by the firm. The security audits of RedHat Linux, Oracle Solaris, Windows (including Active Directory) and IBM AIX were conducted. Several control enhancements, specifically, on the patch management process, were recommended.
* Executed database management system security audits across all business lines and entities in North America hub. Database servers such as, Oracle, SQL Server and Sybase were reviewed for compliance to global and local security baselines.
* Participated in the integrated security audits of Global Equities Derivatives & Commodities (GECD) and Fixed Income (FI) audit missions. Mainly responsible for the review of input/output processing, data completeness and accuracy of trade reconciliations and timely processing of batch jobs.

**IMS Tech Services**

**Java Programmer Aug 2008 – June 2011**

* Designed and developed a suite of applications used by the security operations department.
* Developed server side business components using Java Servlets, JSPs, and Enterprise Java Beans (EJBs).
* Automated code deployment to production environment by creating tasks using ANT deployment tool.
* Developed stored procedures, views and triggers using Oracle PL/SQL.
* Design and implementation of RESTful Web services.
* Developed application presentation layer, which is based on Spring MVC framework involving JSP, Servlets and HTML, CSS.
* Developed this web application to store all system information in a central location. This was developed using Spring MVC, jQuery, JSP, Servlets, Oracle 10g, HTML and CSS.
* Developed Servlets and Utilized Node.js to create a fast and efficient chat server.
* Implemented the Scrum Agile methodology for iterative development of the application.
* Involved in system design, enterprise application development using object-oriented analysis in Java/JEE6.
* Used Spring Framework for Dependency injection and integrated with the Hibernate framework for interacting with the Oracle database.
* Analyzed performance issues in the application, related system configuration and developed solutions for improvement.
* Involved in WebLogic and Tomcat application server installation and configuration in production, development and QA environments.