KALYANI KARRA

Sr Security Analyst
Email: kkreddy961@gmail.com
(410) 756-0695

PERSONAL PROFILE

A highly accomplished Security Tester with extensive experience in complete Software Development Life Cycle including requirements gathering, design, development, testing and implementation.

PROFESSIONAL SUMMARY

- Around 6 years of IT experience in **Information Security**, **Application Security**, **Network Security** and **Mobile Security**.
- Expertise in performing Application Security Risk assessments throughout SDLC.
- Excellent knowledge in **OWASP Top 10** Vulnerabilities, CWE and WASC Threat Classification 2.0 methodologies.
- Good understanding of **PCI DSS** compliance, **PKI** and **Cryptographic Protocols**.
- Extensive experience on **vulnerability assessment** and **penetration testing** using various tools like Acunetix, Metasploit, BurpSuite, Sqlmap, OWASP ZAP Proxy, Nessus, Nmap, QualysGuard and HP Fortify.
- Expertise in identifying flaws like **SQL Injection**, Insecure Direct Object Reference, Security Misconfiguration, Sensitive Data Exposure, **Cross Site Scripting (XSS), CSRF,** Path Traversal and Unvalidated Redirects.
- Extensive experience in using **Kali Linux** to do web application assessment using tools like DirBuster, Nikto and Nmap.
- Extensive experience in performing **SAST (Static Application Security Testing/White-Box Testing**) and **DAST (Dynamic Application Security Testing/Black-Box Testing).**
- Expertise in managing large **security programs** comprising different **security domains** and global teams.
- Implemented and reviewed **security controls across SDLC**.
- Extensive experience in Vulnerability Assessment and Penetration Testing on **Web** and **Mobile based Applications** and **Infrastructure.**
- Extensively worked on Security Analysis of **Firewall rules** and **Web Proxy policies**.
- Extensive experience in establishing process for **periodic reviews** of **Privilege User Groups** at **AD, Database** and **Application Level.**
- Proficiency in SQL, PL/SQL, Java, **Shell Scripting**, **PERL Scripting**, C and HTML.
- Participated in **Bug Bounty programs** for different organizations to report critical vulnerabilities in their infrastructure.
- Able to work on own initiative or as part of a team, backed by excellent communication skills along with the capability to solve problems efficiently.
- Diversified domain experience in Energy, Utilities, Manufacturing, Banking, and Financial Services.

EDUCATION

- **Bachelor of Technology** in **Electronics and Communications** at Sahasra Engineering College (Aff. JNTU), India.

TECHNICAL SKILLS

Vulnerability Testing	Tenable Nessus, Nmap, QualysGuard
Application Security	Websense, IBM Rational AppScan, Burp Suite, Paros, HP WebInspect, HP Fortify, Sqlmap, Nikto, Metasploit, Kali Linux, DirBuster, Wireshark
Methodologies	OWASP Top 10, CWE
Compliances	PKI, PCI DSS

Databases	Oracle, SQL Server
Query Tools	SQL Developer, SQL Server Management Studio
Languages	SQL, PL/SQL, Java, HTML, XML, C, Shell Scripting and PERL Scripting
Source Control	Team Foundation Server, Visual Source Safe, CVS and SVN
Platforms	UNIX (Solaris), LINUX (RedHat), Windows Server

EMPLOYMENT

Exelon (Constellation), Baltimore, MD **Nov 2016 – Present**

Security Analyst

Exelon is the nation's leading competitive energy provider. The Exelon family of companies participates in every stage of the energy business, from generation to competitive energy sales to transmission to delivery. This project involves testing different web applications across the organization.

- Involved in Planning, Scheduling, Tracking, and Reporting on Manual/Automated Security testing on Internet and Intranet Applications.
- Extensive experience in Vulnerability Assessment of various web applications used in the organization using BurpSuite, WebScarab, HP Web Inspect and QualysGuard.
- Well versed in Understanding Application Level Vulnerabilities like SQL Injection, XSS, CSRF, Authentication Bypass, Authentication Flaws, and Cryptographic Attacks.
- Performed Security code review using static code analysis tools like HP Fortify and IBM AppScan and helped team to remediate security issues with sample code.
- Assisted in managing Tenable Nessus Security across multiple platforms, SMB exploitation using Nmap and Metasploit Framework and implemented security policies within the client's infrastructure.
- Worked on white-box testing and Black-box testing.
- Reviewed and Validated Privileged Users and Groups at Active Directory, Databases and application on a periodic basis.
- Captured Critical, High, Medium and Low Vulnerabilities in the applications based on OWASP Top 10 Vulnerabilities and prioritized them based on the criticality.
- Provided the development team with detailed reports based on the findings obtained from Manual and Automated testing methodologies and remediation for individual findings.

Environment: OWASP Top 10, Burp Suite, WebScarab, Kali Linux, QualysGuard, HPWeb Inspect, IBM AppScan, HP Fortify, Sqlmap, Nmap, Metasploit, Tenable Nessus, AppScan Enterprise.

T. Rowe Price, Owings Mills, MD **Jan 2016 – Oct 2016**

Information Security Engineer

T. Rowe Price Group, Inc. is an American publicly owned global asset management firm that offers funds, advisory services, account management, and retirement plans and services for individuals, institutions, and financial intermediaries. This project involves Security Testing for firm-wide web applications.

- Extensively Worked on Web Application Vulnerability Assessment and Threat Modeling, Gap Analysis, Secure Code Review on the applications.
- Performed Manual Code Review to find logic flaws, which are not identified by Automated Tools.
- Extensively used Paros Proxy, Burp Suite, WebScarab, Acunetix Automatic Scanner, and Nmap for Web Application Penetration Testing and Conducted Functional Testing of RSA 2-factor Authentication.
- Well versed in Understanding Application Level Vulnerabilities like SQL Injection, XSS and CSRF.
- Conducted Social Engineering Attacks using Backtrack and Kali Linux.
- Trained development team on the most common vulnerabilities and common code review issues and explained the remediation.

Environment: Acunetix, Burp Suite, Nmap, Application Firewall, YASCA, Paros Proxy, WebScarab, HP Web Inspect, Kali Linux.

NeerInfo Solutions **July 2012 – Oct 2015**

Role: Security Tester

NeerInfo Solutions is an HR services boutique, dedicated to catering to the end-to-end HR needs of companies. This project aims at Security Testing web-based applications.

- Performed Black box Penetration Testing on Internet and Intranet facing applications.
- Performed Threat Modeling of the applications to identify threats.
- Identified issues in web applications in various categories like Cryptography and Exception Management.
- Used various Add-Ons in Mozilla to assess the applications like Wappalyzer, Flagfox and Live HTTP Header.
- Worked on risk assessment on the application by identifying the issues and prioritizing the issues based on risk level.
- Provided remediation to the developers based on the issues identified in testing and re-validated them to ensure the closure of the vulnerabilities.

Environment: MS SQL, Burp Suite, Sqlmap, Nikto, OWASP ZAP Proxy, HP Fortify, Nmap, Metasploit.