****L MOUNICA

Application Security Engineer

Phone: 510-766-1364

Email: mounica.appsec@gmail.com

**SUMMARY:**

* Around 6 years of experience in IT industry as web application security professional. Specialized in **information technology assurance, web application security, application security controls and validation, regulatory compliance and Secure Software Development Life Cycle** (Secure SDLC).
* Experience in Developing and Implementing of Information Security Policies and Guidelines as per **OWASP (Open Web Application Security Projects), SANS Secure Coding guidelines**
* Hands on Experience on vulnerability assessment and penetration testing using various tools like **Burp Suite, Fiddler, ZAP Proxy, SQL map, HP Web Inspect and IBM AppScan, checkmarx, HP fortify.**
* Experienced and proficient in Security Framework of OWASP, BSIMM, Secure SDLC along with expertise in OWASP Top 10, SANS 25, CWE and CVSS.
* Capable of identifying flaws like **Injection, XSS, SQL injection, Insecure direct object reference, Security Misconfiguration, Sensitive data exposure, Functional level access control, CSRF,** Invalidated redirect.
* Conducted testing over the applications to comply with **PCI DSS Standards.**
* Analyze & implements security specific solutions for improving the security level in terms of operational security and risk management.
* Recommending security strategy and objectives that result in the planning and use of tools and processes to monitor the security profile of logical client's Information technology infrastructure.
* Gaining proficiency in **Mobile Security Testing, Cloud Security and DevOps Security Testing.**
* Involved in Secure Software Development Life Cycle (secure SDLC) process.
* Possesses substantial understanding and experience on the SSDLC, which has been effectively translated across a number of consulting engagements.
* Hands - on with **DAST, SAST and manual ethical hacking.**
* Create detailed assessment reports with remediation, recommendations, and present findings to clients and re-testing the security issues.
* Vulnerability Assessment includes analysis of bugs in various applications spread across N-tier on various domains by using both manual and Automation tools.
* Excellent oral and written communications, interpersonal, negotiation, judgment, decision-making, analysis and problem-solving skills.
* Working knowledge of **AWS Cloud** Security in implementing Web Application Firewalls (WAF).
* Familiarity with Agile/Scrum methodologies.
* Managed the company web site including content development, payment gateways, and other web based services.
* Experience in ticketing system like **Remedy, HP Quality Center, JIRA.**
* 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.

**SKILL SET:**

**Core Expertise:**Web Application, Security Vulnerability Assessments, Threat Management, Penetration Testing, SDLC, Support/Troubleshooting

**Web Applications:**Acunetix Web Vulnerability Scanner, IBM AppScan, Zap, HP Web Inspect, Paros, Fiddler2, Brup Suite, FortyDB

**Servers & Databases:**MSSQL, Oracle

**Web Services Testing:**Soap UI tool and SOA Test tools for web services security

**Tracking Tools:**Bugzilla, QC Trac, Team Forge

**Network Auditing:**Nessus, GFILAN Guard, NMAP

**Web Technologies:**HTML, Web Services, XML

**Languages:**C, Java, Python Scripting, HTML, Pearl, Ruby

**Domain knowledge:**

* Technology Platforms
* Testing Framework
* Testing Approach
* Security Testing Tools
* JAVA/J2EE, ASP.Net
* PHP, SQL, SAP
* Knowledge in Android and iOS Platforms
* OWASP Top 10, NIST, BSI,
* OSSTMM
* DAST (Dynamic Application Security Testing of Web, Thick client, Web Services.)
* Dynamic Scanning Tools( Webinspect, Appscan, Appspider)
* SAST (Static Application Security Testing/Code Review)
* Automated and Manual Testing Methods, Penetration Testing, Risk Assessment.
* Threat Profile based Security Assessments
* IBM AppScan, HP WebInspect, Burp Suite Pro, Acunetix, Qualys Guard, Nessus, Checkmarx and Veracode Testing Suite

**Open Source:**OWASP ZAP, Fiddler, WebScarab, nMap, Backtrack, Firefox Plugins, SQLMap, Xenotix, SSL Scan, SSL Digger SOAP UI, Rest Client, POSTER, EchoMirage, Wire Shark

 **Monitoring** **Tools Used:**Burp Suite, DirBuster, OWASP ZAP Proxy, Qualys gurd, Nmap, Nessus, Kali Linux, PCI DSS compliance, Metasploit, Accunetix, IBM app scan, HP Web Inspect, Hp Fortify

**Advanced Security Scanning and Penetration Testing Tools:**Metasploit Pro, SOAPUI, IBM App scanner, Nexpose Vulnerability Scanner, Wireshark, Network Packet Analyzer, Kali Linux, OpenVAS Vulnerability Scanner, Nessus Scanner, TCPDump, NETCAT, Netsparker, Burp-suite Web Application Scanner, OWASP ZAP, NMAP Port Scanner, SQLMap, DirBuster, Splunk, Tripwire, W3AF Web application security scanner.

**PROFESSIONAL CERTIFICATIONS:**

**EC Council – Certified Ethical Hacker**

**Cisco Certified Network Associate - CCNA**

**EDUCATION:**

* **Master’s in cyber security**, University of North Carolina at Charlotte, Charlotte, NC.

**EXPERIENCE:**

**QUALCOMM, San Diego, CA**

**Application Security Engineer**  **September 2019—Present**

**Responsibilities:**

* Identified issues on sessions management, Input validations, output encoding, Logging, Exceptions, Cookie attributes, Encryption, Privilege escalations.
* Skilled using Burp Suite, Acunetix Automatic Scanner, NMAP, Dirbuster, IBM AppScan, Nessus, SQLMap for web application penetration tests and infrastructure testing.
* Responsible in web application vulnerabilities (OWASP TOP 10, SANS, NIST) to review application source code to find its security vulnerabilities (CSRF, XSS, SQL Injection, Privilege Escalation, etc.) and recommend remediation.
* Implemented SQL Plan Management on mission critical application to lock down execution plans for high usage SQL statements.
* Reference CVEs and Tenable Nessus to mitigate vulnerabilities.
* Created risk assessments based on CIS Benchmarks and CVSS scoring methodology and provided remediation guidance to court and national program offices
* Experience in detecting - SQL injection, XML injection, techniques to obtain command prompts on the servers, PDF exploits, HTTP response splitting attacks, CSRF, web services vulnerabilities.
* Routing and switching fundamentals, the TCP/IP and OSI models, IP addressing.
* Working on all internal & external applications of Unisys containing Web, WebServices & Flash applications.
* Manage Healthcare PCI (Payment Card Industry) Compliance Program and ensure card holder data security standards meet PCI DSS (Payment Card Industry Data Security Standards) requirements. Serve as the initial point of approval for acceptability of PCI evidence.
* Troubleshoot and fix network connectivity issues using TCP/IP and OSI Model.
* Conduct continuous monitoring and analysis of security threat information and event logs via IBM Q-Radar Forensics and Vulnerability manager content development and use cases.
* Monthly Automated Scans of the online applications in production using Web inspect and followed by report presentation.
* Provide assistance to IT staff and provide all security specifications for all vendor products and evaluate all requests for security architecture.
* Assess all risk and evaluate all impact for technology changes in processes and maintain knowledge of all security systems and deploy all required infrastructure.
* Manage all repeated threats to all systems and perform vulnerability tests.
* Manage Firewalls, IDS/IPS, build out security infrastructure including Vulnerability scanning and SIEM.
* Having good experience in Secure SDLC and Source Code Analysis (Manual & Tools) on WEB based Applications.
* Knowledge of SIEM (Security Information and Event Management) solution Splunk, able to perform searches, create reports, alerts and dashboards.
* Experience on HP fortify tool, Ticketing system -JIRA, Remedy
* Build enterprise risk dashboards and generate reports as needed for the organization
* **Environment:**JAVA, Asp.net, MySQL, Apache Kali Linux, Burp Suite, Dirbuster, Microsoft Visual Studio, HP Fortify, AppScan, Nmap, Wireshark, PCI-DSS.

**SCHNEIDER NATIONAL, Green Bay, WI**

**Application Security Analyst September 2018 – May 2019**

**Responsibilities:**

* Facilitated issues involving accounts on all hosting platforms, including troubleshooting basic server administration and accessibility issues in virtual dedicated and dedicated environments. Provided direct support for representatives and customers
* OWASP Top 10 Issues identifications like SQLi, CSRF, XSS.
* Experience in detecting - SQL injection, XML injection, techniques to obtain command prompts on the servers, PDF exploits, HTTP response splitting attacks, CSRF, web services vulnerabilities.
* Risk assessment using CIS benchmark and CVSS scoring methodology.
* Worked on Correlation and Parameterization in JMeter scripts. Used JavaScript for coding in developing scripts.
* Capable of identifying flaws like Injection, XSS, Insecure direct object reference, Security Misconfiguration, Sensitive data exposure, Functional level access control, CSRF, Unvalidated redirects.
* Primary role is risk management, vulnerability management, project risk advisory, regulatory compliance, and change management security support. Configured master and slave machines by matching Java and JMeter and setting up environment variables for running tests through JMeter.
* Explanation of the security requirements to the design team in initial stages of SDLC to minimize the efforts to rework on issues identified during Penetration tests.
* Responsible for creating the Production load test scripts using JMeter.
* Used AppDynamics to perform transactional analysis on slow performing transactions
* Using various add on in Mozilla to assess the application like Wappalyzer, Flagfox, Live HTTP Header, cookie manager, Tamper data.
* Responsible for identifying, escalating, and validating security incidents in accordance with customer-specific Incident Management procedures.
* Creating and building (Authoring) Corporate Information Security Program including all Policies, Procedures and Plans to include HITRUST and HIPPA regulations/standards.
* Developed and evaluated a variety of specific security solutions to solve threats that were specific to the varied situations at hand.

**Environment:**JMeter, Java, AppDynamics, JIRA, Jenkins, Confluence, Apache Tomcat, Oracle, Microsoft SQL Server, Fiddler, Remedy.

**ZENQ, Hyderabad, India**

**Security Tester January 2017– May 2018**

**Responsibilities:**

* OWASP Top 10 Issues identifications like SQLi, CSRF, XSS.
* Preparation of risk registry for the various projects in the client.
* Training the development team on the secure coding practices.
* Conducted research, mitigation, and coordination of actions designed to reduce information security risk across internet facing presence.
* Providing details of the issues identified and the remediation plan to the stake holders
* Verified the existing controls for least privilege, separation of duties and job rotation.
* Involved in a major merger activity of the company and provided insights in separation of different client data and securing PII
* Identification of different vulnerabilities of applications by using proxies like Burpsuite to validate the server-side validations
* Execute and craft different payloads to attack he system to execute XSS and different attacks.
* SQLMap to dump the database data to the local folder.
* Identified issues on sessions management, Input validations, output encoding, Logging, Exceptions, Cookie attributes, encryption, Privilege escalations.

**K CLINK TECHNOLOGY PVT, Hyderabad, India**

**Application Tester September 2014 - December 2016**

**Responsibilities:**

* Established vulnerability assessment practice, proactively ensuring safety of client-facing applications and minimizing client audit findings.
* Performing security analysis and identifying possible vulnerabilities in the key derivation function, create Vulnerability Assessment report detailing exposures that were identified, rate the severity of the system & suggestions to mitigate any exposures & testing known vulnerabilities.
* Having real time experience in Sql Injection protection, XSS protection, script injection and major hacking protection techniques
* To address and integrate Security in SDLC by following techniques like Threat Modeling, Risk Management, Logging, Penetration Testing, etc.
* Providing fixes & filtering false findings for the vulnerabilities reported in the scan reports.
* Adding new vulnerabilities to the Vulnerability Database for various platforms with proper exploits.
* Scan Networks, Servers, and other resources to validate compliance and security issues using numerous tools
* Assisting in preparation of plans to review software components through source code review or application security review
* Assist developers in remediating issues with Security Assessments with respect to OWASP standards.