

**Hayli Patel**

* A security analyst with 7+ years of experience.
* Expertise in performing Application Security risk assessments throughout the SDLC cycle Performed Application security which includes Application Security design, review, testing and remediation.
* Monitor Intrusion Detection Systems (IDS) console for active alerts and determine priority of response.
* Experienced and proficient in Security Framework of OWASP, BSIMM, Secure SDLC along with expertise in OWASP Top 10, SANS 25, CWE and CVSS.
* Deployed and worked on plethora of Commercial tools like HP Web Inspect, IBM AppScan, Acunetix, Qualysguard and variety of Open Source tools. Have knowledge on other security framework in the likes of BSIMM, OSSTMM.
* 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.
* Executed roles of Application Security Pen Tester, Security Analyst, and Security project coordinator in programs involving applications from diversified technology platforms across business portfolio.
* Conceptualized and developed incident investigation and fraud prevention system

 for Centralized Log Server and Log Analysis.

* Performed Vulnerability assessments and preventions on the development side by leveraging the tools like Nmap, Nessus, IBM app scan.
* Implemented and maintained firewall for preventive measures and being compliant with laws and regulations.
* Managed the company web site including content development, payment gateways, and other web based services.

**Skill Set**

|  |  |  |  |
| --- | --- | --- | --- |
| **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)    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 |

**SUMMARY of Experience and Roles Executed**

**Application Security Testing (Vulnerability Assessment and Penetration Testing):** Discussion with stakeholders, Information Gathering, Threat Profiling and Prioritization of the applications for testing, Design and formulate test plans, Set tool policy, Conduct Automated Scans, False positive removal and analysis, Define and finalize manual test scripts, conduct manual assessment, prepare report, status update to management and stakeholders, support for Issue remediation to development team.

**Security Project Coordination:**Define Scope, identify project risks and formulate mitigation plans, formulate security assessment plans, discussion with stakeholders, Onsite-Offshore delivery, status reporting and dashboard presentation, support for end to end vulnerability management, risk management in the likes of ISO 27001-ISMS

**Vulnerability Management**: Vulnerability identification, Issue Analysis and prioritization as per severity and criticality, Issue fix and verification of fixes through retest, Monitoring and Reporting of Issue trends and Dashboards to Management and relevant stakeholders.

**MonitoringTools 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

**WORK EXPERIENCE**

**Client Name: T-Mobile, Seattle, WA (Feb 2016 - TILL DATE)**

**Role:** Application Security Test Analyst

**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.
* 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.
* **Environment:** JAVA, Asp.net, MySQL, Apache Kali Linux, Burp Suite, Dirbuster, Microsoft Visual Studio, HP Fortify, AppScan, Nmap, Wireshark, PCI-DSS.

**Client Name: World Bank Washington, DC (Jan 2015- Jan 2016)**

**Role:** Application Security Test Analyst

**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.

**Client Name: State of DC, Washington, DC (Nov 2012- Dec 2014)**

**Role:** Security Tester

**Responsibilities:**

* Worked with the development team to understand the application landscape and formulated test plans
* Define test policy for automated scanners and manual test scripts for applications across platforms.
* Conduct application security vulnerability assessment and penetration testing using IBM Appscan.
* Conducted secure code reviews using automated tools and manual techniques.
* Prepared Monthly and Quarterly Issue trend analysis report and suggested measures for improvement.
* Conducted Threat Profiling and Threat Modeling of applications across complexities and technology platform.
* Responsible for delivery execution through Onsite-Offshore delivery model to ensure projects SLA’s
* Prepared PoC’s for security issues identified in assessments and conducted sessions for development team on secure coding & remediation solutions for critical and high severity issues.
* Used Stepping thread group for creating test scenario and execution.
* Configured master and slave machines by matching Java and JMeter and setting up environment variables for running tests through JMeter.
* Responsible for creating the Production load test scripts using HP LoadRunner and Neoload for Holiday Readiness Programme.
* Mostly worked on eCommerce web , backend webservices and mobile applications.
* Design scenarios in HP tools and Neoload to evaluate the performance of the application. Execute different kinds of performance tests like load test, stress, volume and endurance tests.
* Worked with Engineer Team in setting the LG's and virtual setup of third party system to test applications.
* Used HP Service Virtualization Environment to test Web Services API Driven Applications.
* Installed AppyDynamics agents in AppServers and Created dashboards in AppDynamics to monitor the server metrics.
* Used AppDynamics to perform transactional analysis on slow performing transactions
* Used AppDynamics to perform Cross-Application Tracing
* Used IP Spoofing whenever necessary to create a realistic load.
* Used Riverbed Tools (TTW,AIX) to monitor the metrics like CPU, Memory ,Exceptions/sec in analyzing the application's performance.
* Issues Identified are logged as defects and worked with Engineering team and development teams in improving the performance of the application.
* Identified Memory leak issue for an application with help of Engineering team and worked closely with Development team in resolving the issue.
* Worked with Engineering Team to provide Performance Test Results to development Team with detailed information about the application's Performance
* Never missed the deadline when required to do Load Testing.

**Environment:** HPLoadrunner, HP Service Virtualization, Neoload, .Net, AppDynamics, SQL, Jmeter, Riverbed Tools(TTW,ARX, AIX), Apache Tomcat, Oracle, Microsoft SQL Server, TOAD.

**Client name: Mindtree, Hyd , India (Jan 2011- Oct 2012)**

**Role:** Penetration tester

**Responsibilities:**

* Instructed application team in secure programming during all phases of application lifecycle (SDLC) based on OWASP standards.
* Performed general controls oversight and review on out-sourced or in-house IT projects to verify compliance with internal/external standards.
* Ensuring confidentiality, Integrity and availability of the system is maintained.
* Verified the existing controls for least privilege, separation of duties and job rotation.
* Ensure the issues identified are reported as per the reporting standards.
* Ensuring confidentiality, Integrity and availability of the system is maintained.
* Black box pen testing on internet and intranet facing applications.
* OWASP Top 10 Issues identifications like SQLi, CSRF, XSS and unvalidated redirects etc.
* Working with Developers, QA Engineers, Project Managers and Business Owners to educate and implement industry best practices for remediating software security vulnerabilities.
* Creating and managing an Application Security Metrics Dashboard
* Provide security vulnerabilities (XSS, CSRF, SQLi, DDOS, etc.) remediation support to Java, .net, PHP and Ruby developers
* Review and Analysis of 3 rd Party Web Application Penetration Test Findings prior to implementation
* Provide OWASP Top Ten training to QA Engineers and Software Developers.
* Create custom Injection and Scripting attacks/exploits for Application Security Testing.

**Environment:** JMeter, Java, AppDynamics, JIRA, Jenkins, Confluence, Apache Tomcat, Oracle, Microsoft SQL Server, Fiddler, HP Web Inspect, Burp Suite Pro and HP Fortify SCA