Information Security Analyst Information Security Analyst Information Security Analyst Edison, NJ Over 7+ years of experience as IT professional in Information security and penetration Testing in creation and deployment of solutions protecting applications, networks, systems and information assets for diverse companies and organizations. Involved in secure software Development Life cycle process and source code analysis on WEB based applications. Experience in Vulnerability assessment, Network Penetration Testing, Web application penetration Testing, Mobile application penetration testing. Experience in application security, vulnerability assessments and OWASP along with different security testing tools like Burp Suite, Dir Buster, OWASP ZAP Proxy, Nmap, Nessus, Kali Linux, Metasploit, HP Web inspect and IBM App scan. Experience as an Information Security Analyst, involved in OWASP Top 10 based Vulnerability Assessment of various internet facing point of sale web applications and Web services. Experience in working with Network infrastructure such as Firewalls (palo alto), IDS/IPS, Router, NAC, Switch, Unified threat management system. Involved in implementing and validating the security principles of minimum attack surface area, least privilege, secure defaults, defense in depth, avoiding security by obscurity, keep security simple, fixing security issues correctly. Experience in secure code review of various application using static code analyzer like HP FORTIFY and VERA CODE. Validate the false positive and report the issues. Involved in web application development with UI technologies like CSS, HTML, JavaScript. Broad Knowledge of hardware, software and networking technologies to provide a powerful combination of analysis, implementation, and support. Extensive knowledgeprotocols such as TCP/IP, UDP, IPSEC, HTTP, HTTPS, routing protocols and operating systems like Windows/Solaris/Linux, databases, application security and secure remote access. Having good knowledge in gathering requirements from stakeholders, devising and planning, strong technical understanding of vulnerabilities. Good experience in exploiting the recognized vulnerabilities. Good Knowledge on mobile application security testing using Mobisec. Good Knowledge in cloud security. Have excellent communication, analytical, troubleshooting, customer service and problem solving skills, excels in mission-critical environments requiring advanced decision-making. Authorized to work in the US for any employer Work Experience Information

Security Analyst United Airlines - Chicago, IL July 2016 to August 2017 Responsibilities: Perform security reviews of application designs, source code and deployments as required, covering all type of applications. Provide risk assessments to ensure corporate compliance. Provide oral briefings to leadership and technical staff, as necessary. Performed regular vulnerability scans on security systems and coordinate with development team to ensure achievement of all business objectives and recommend appropriate architectural solutions. Perform Port Scanning and Vulnerability assessment using Nmap and Nessusfor closure of unnecessary ports. Perform Penetration Testing in accordance with OWASP standards and SANS 25using manual techniques and automated tools. Perform web application penetration tests and infrastructure testing using Burp Suite pro and Acunetix Automatic Scanner. Monitor SIEM and IDS/IPS feeds to identify possible enterprise threats. Investigate threats to determine nature of incident using Qradar. Monitor the latest threat & vulnerabilities and alerts if any specific threats. Ensure the issues identified are reported as per the reporting standards. Validate the false positives and submission of detailed report Provide report and explain the issues to the development team. Provide remediation steps to the team and follow up. Retest the fixed issues and ensure the closure. Involved actively in the release management process to ensure all the changes of the application had gone to security assessment. Provided threat and vulnerability assessments, reports on daily basis to maintain the security posture of the systems and its application. Environment: Windows, Nmap, Nessus, checkmarx, Burpsuite pro, Acunetix, Qradar. Penetration Tester Wells Fargo - Charlotte, NC 2015 to June 2016 Responsibilities:. Perform manual and automated dynamic grey-box security testing and remediation testing on a wide range of web and native mobile-based applications hosted in multiple pre-prod environments using tools like IBM App Scan Standard, Burp suite and check marx. Provide analysis and remediation recommendations to application and infrastructure teams responsible for the maintenance of vulnerable applications. Worked on the IDS/IPS firewall reports, checking the firewall traffic and configurations policies Worked on the solar winds reports for checking the open ports devices Reviewed the threat activity map for monitor incoming and outgoing traffic Execute and provide analysis and remediation

recommendations for automated static source code security testing Provide approval for applications to be released into a production environment based on the severity of open vulnerabilities in the application environment and the intended remediation date Manage a third-party security testing program, responsible for scheduled, regular security assessments of high-risk applications performed by an outside vendor Manage a secure coding development training program for application and mainframe development teams, designed to spread security awareness and reduce the overall level of risk from the development stages of SDLC Environment:Windows, Nessus, IBM AppScan Standard, Burpsuite, IBMAppScan source. IT Security Analyst Coca cola - Atlanta, GA January 2014 to March 2015 Responsibilities: Working as a Technical Security Consultant in the areas of application security highlighting the security controls needed at the design level. Understanding and implementation of security into SDLCvia application risk assessment, requirements gathering, design review, application vulnerability assessment. Port scanned servers using N map and closed all necessary ports to reduce the attack surface. OWASP Top 10 issues identifications like XSS, SQL Injection, CSRF etc. Validate input validations, session management, client protocol controls, cryptography, logging and information leakage. Ensure the issues identified are reported as per the reporting standards. Suggested the security requirements to the development team in various stages of SDLC to minimize the efforts to rework on issues identifies during penetration tests. Regularly performed research to identify potential vulnerabilities in and threats to existing technologies and provided timely, clear, technically accurate notification to management of the risk potential and options for remediation. SQL map to dump the database data to the local folder. Scan Networks, Servers and other resources to validate compliance and security issues using numerous tools using Nmap and Nessus. Support the Data Loss Prevention(DLP) and cyber security teams in editing core processes. Vulnerability assessment of various web applications used in the organization using various tools like BurpSuite pro and WebInspect. Drafted Javascript with respect to the vulnerabilities like XSS. CSRF etc. Identified issues on sessions management, Input validations, output encoding, Logging, Exceptions, Cookie attributes, encryption, Privilege escalations. Scan

Networks, Servers, and other resources to validate compliance and security issues using numerous tools using Nmap and Nessus. Support the Data Loss Prevention(DLP) and cyber security teams in editing core processes. Vulnerability Assessment of various web applications used in the organization using various tools like Burp Suite Pro and Web Inspect. Environment: Unix, Nessus, Sql map, Burpsuite pro, HP fortify, HP Webinspect, Metasploit. Security Analyst Bluethink IT consulting - Noida, Uttar Pradesh September 2012 to December 2013 Responsibilities: Performed vulnerability assessments, threat assessment, mitigation and reporting activities to safeguard information assets and ensure protection has been put in place on the systems. Found common website security issues like CSRF, XSS, applications logic, SQL injection, information leakage, session fixation etc across various platform. Information gathering of the application using websites like Shodan, Reverse DNS. Network scanning using tools like Nmap and Nessus. Metasploit to exploit the systems Performed live packet data capture with Wireshark to examine security flaws. Provided detailed reports on the findings of network and application penetration tests including mitigation and remediation activities. Ensures that the operation, design, and management of information systems are in according to the standards of the organization. Provide assistance to IT staff and provide all security specifications for all vendor products and evaluate all requests for security architecture. Provided fixes and filtering the false findings for the vulnerabilities reported in the scan reports. Create vulnerability assessment report detailing exposures that were identified, rate the severity of the system, and suggestions to mitigate any exposures and testing known vulnerabilities. Used Burp suite, Dir buster, N map tools on daily basis to complete the assessments. Environment:Windows, kali linux, Shodan, Nmap, Nessus, Wireshark, Burp suite, Dirbuster. Security Tester Signode India Limited July 2011 to August 2012 Responsibilities: Performed Web Application Security /Penetration Testing in accordance with OWASPstandards using manual techniques and automated tools. Provide assistance to IT staff and provide all security specifications for all vendor products and evaluate all requests for security architecture. Scan Networks, Servers, and other resources to validate compliance and security issues using numerous tools. Port scan servers using NMAP and close all unnecessary ports to

reduce the attack surface. Conduct penetration testing using automated tools such as App scan, Paros Proxy, Web Inspect, Traffic Viewer, TCP Dump etc. Used various Firefox add-ons like Flag fox, Live HTTP Header, Tamper data to perform the pen test. Utilize Nessus, Burp to scan, identify and remediate existing vulnerabilities. Training the development team on the most common vulnerabilities and common code review issues and explaining the remediation's. Environment:Windows, Live HTTP Header, Paros Proxy, Web Inspect Education Bachelor's Skills METASPLOIT (2 years), NESSUS (6 years), NMAP (4 years), SQL (2 years), VULNERABILITY ASSESSMENT (3 years), Information Security, Cyber Security, SEC, It Security Additional Information TECHNICAL SKILLS Vulnerability Assessment Tools: Burp Suite Pro, OWASP ZAP Proxy, Paros proxy, IBM Appscan, Metasploit, Acunetix, HP Web inspect, checkmarx, HP Fortify, Dirbuster, Wireshark, Qualsguard. Network Auditing Tools: NMap, Nessus Other Tools: Haviji, Sql Map, Sql ninja etc. Testing Tools: SOAP UI and SOA Test tools for web security services. Operating System: Kali Linux, GNU/Linux, Windows. Programming Languages: JAVA, C#, Python, PHP. RDBMS: MySQL, Oracle 10g/11g, PL/SQL. Scripting Languages: HTML5, CSS, XML, JavaScript.

Name: Daniel Garza

Email: tracywilson@example.com

Phone: 464-500-1377