Penetration tester/Vulnerability engineer Penetration tester/Vulnerability engineer Penetration tester/Vulnerability engineer - Dow Jones, NJ Atlanta, GA Sai Viswanath - 6+ yrs experience , Penetration Tester / Security Analyst , Visa ; OPT EAD , Available immediately Employer : Pradeep pradeep@trovetechs.com 803-335-4449 Work Experience Penetration tester/Vulnerability engineer Dow Jones, NJ July 2017 to Present Performed manual security testing on critical client applications. Uncovered high vulnerabilities at the infrastructure level for internet facing websites. Prioritizing the issues found, considering different factors like Impact and Likelihood. Strong Hands-on Experience in Web Application penetration testing, Network Infrastructure Penetration Testing. Brute force assessment to insure strong passwords and encryption. Performed Policy Compliance scanning and Vulnerability scanning using Qualys Policy Compliance Module Performed vulnerability scans using HP WebInspect, IBM App Scan, Qualys Guard, Retina, Nessus, Burp Suite, and Metasploit auxiliary modules. Conducted Dynamic and Static Application Security Testing (SAST & DAST) Acquainted with various approaches to Grey & Black box security testing. Update with the new hackings and latest vulnerabilities to ensure no such loopholes are present in the existing system. Security testing of APIs using SOAP UI. Experience in using Kali Linux to do web application assessment with tools like Dir-buster and NMAP. Perform threat modelling of the applications to identify the threats. OWASP Top 10 Issues identifications like SQL Injection, CSRF, XSS Execute and craft different payloads to attack the system for finding vulnerabilities with respect to input validation, authorization checks, etc. Training the development team on the secure coding practices Network scanning using tools like NMAP and Nessus. Training the development team on vulnerabilities, review issues, ease of exploitation, impact, security requirements and remedies for individual issues. Providing details of the issues identified and the remediation plan to the stake holders. Communicating and coordinating day-to-day project activities within the project team and assure that priorities are developed and known. 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 Proficient in understanding application level vulnerabilities like XSS, SQL

Injection, authentication bypass, weak cryptography, authentication flaws and exception management etc. Environment: Kali Linux, XML, Nmap, SOAPUI, HP WebInspect, IBM App Scan, Qualys Guard, Retina, Nessus, Burp Suite, Metasploit, Web Security Analyst State of Kentucky, KY March 2015 to June 2017 Black box pen testing on internet and intranet facing applications Follow information security policies, methods, standards, NIST standards, and practices to organize information systems, IT reference material, and interpret regulations. Monitor Intrusion Detection Systems (IDS) console for active alerts and determine priority of response. Review all incoming IDS alerts and document all identified problems. Monitor for Data Loss Prevention (DLP) using Symantec. Skilled using Burp Suite, Qualys, Automatic Scanner, NMAP for web application penetration tests. Good knowledge of network and security technologies such as Firewalls, TCP/IP, LAN/WAN, IDS/IPS, Routing and Switching. Monitor, Analyse and respond to security incidents in the infrastructure. Investigate and resolve any security issues found in the infrastructure according to the security standards and procedures. Actively search for potential security issues and security gaps that are beyond the ability of detection by any security scanner tool. Initiate and develop new mechanisms to addresses unidentified security holes & challenges. Participating in the development and maintenance of the security standards and procedures for the administration of user IDs, logins, and access to computer systems/networks according to security policies. Analyse risks and vulnerabilities of the network and propose solutions. Creating database of past threats, documenting all policies and filters deployed on the network Established security policies for systems, and designed and managed secure networks for clients. Risk assessment on the application by identifying the issues and prioritizing the issues based on risk level. Providing remediation to the developers based on the issues identified. Revalidate the issues to ensure the closure of the vulnerabilities. Environment: Burp Suite, Qualys, Automatic Scanner, NMAP, SQLmap, owasp top 10, HP fortify, Qualys guard, DS/IPS, CSS, CSRF, Nessus IT Security Analyst Way2Online - Hyderabad, Telangana November 2012 to December 2014 Perform threat modelling of the applications to identify the threats. Identify issues in the web applications in various categories like Cryptography, Exception Management. Risk assessment on the application by

identifying the issues and prioritizing the issues based on risk level. In the team, main focus of work was to audit the application prior moving to production. 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. Analysed the XML and HTTP requests to find the vulnerabilities. Performed Vulnerability assessments and preventions on the development side by leveraging the tools like NMAP, Nessus, IBM app scan Providing remediation to the developers based on the issues identified. Good knowledge on web technologies like HTML, CSS, JavaScript to ensure the protection from XSS by reviewing the code. Ensured to draft the script manually based on vulnerability. Revalidate the issues to ensure the closure of the vulnerabilities. Education Master's Skills CEH, Penetration Testing, owasp top 10 Additional Information Vulnerability Assessment Tools IDM Appscan, Burp Suite, Dirbuster, OWASP top 10, SAN 25, ZAP Proxy, Qualys, Kali Linux, Metasploit, Accunetix, HP Web inspect, Qradar, SIEM, SOAPUI Languages C++, JAVA, C#., .net Technologies HTML, CSS, XML, JavaScript. Operating System Windows, Unix/Linux, Mac OSX RDBMS Oracle, MySQL, MS SQL Networking N-map, Nessus, TCP/IP, UDP, IPV4, IPv6, LAN, WAN, Subnetting, firewall configuration

Name: Lori Stewart

Email: hansonanthony@example.com

Phone: 732-207-0341x4162