Security Engineer Security Engineer Security Engineer - CISCO San Jose, CA ? Over 8+ years of experience in IT professional within Information Security. ? Involved in Software development Life cycle (SDLC) to ensure security controls are in place. ? Experience in Threat Modeling during Requirement gathering and Design phases. ? Experience on vulnerability assessment and penetration testing using various tools like Burpsuite, DirBuster, NMap, Nessus, Kali Linux, Metasploit, Accunetix ? Experience with Security Risk Management with TCP-based networking. ? Experience with TCP/IP, Firewalls, LAN/WAN. ? Performed static code Assessment using Veracode and identify the false postivies. ? Monitor, Analyze 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. ? Experience in Linux system administration. ? Performing rapid7 and Nessus Scans against Infrastructure like Webservers, appservers and dB servers to identify the existing environmental vulnerabilities. ? Perform Vulnerability assessment on all the workstations in the organization to identify if they are patched and updated. ? Static Code Analysis during development phase. ? Integrated Vera code with SDLC process to ensure every build is analyzed using static code analysis ? A Certified Ethical Hacker. ? A Pen tester with experience of penetration testing on various applications in different domains. ? Penetration testing based on OWASP Top 10. ? A good team player, Inquisitive, good in basic concepts and an excellent team player. ? Performed the gap analysis to identify scenarios like privilege escalation. ? Performed software Licensing audit. ? Interpreted least privilege for applications and segregation of duties. ? SOX Compliance Audit experience on controls like User access management, Change Management, Incident Management. Authorized to work in the US for any employer Work Experience Security Engineer CISCO - Sanjose, CA, US April 2017 to Present RESPONSIBILITIES: ? Black box pen testing on internet and intranet facing applications ? 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 ? Providing details of the issues identified and the remediation plan to the stake holders ? Gray Box testing of the applications. ? Identified hidden files using dirbuster. ? Worked on DOM based XSS manually. ?

Worked on Directory Traversal attacks manually ? Implemented Agile Methodology to follow the work flow process. ? Worked on Middle ware technologies to ensure the application safety (TOMCAT) ? Verified the existing controls for least privilege, separation of duties and job rotation. ? Identification of different vulnerabilities of applications by using proxies likeBurpsuite to validate the server side validations ? Collaborating on cross-team and cross product technical issues with a variety of resources including development to document software defects and customer suggestions. ? Worked on billion laugh attacks manually by intercepting burp suit. ? Functional level access control is performed to avoid the privilege of misusing the sensitive data. ? Had worked on Accunetix tool for quick assessment of vulnerabilities. ? Participate in documentation and product review process for new product introductions. ? Contributing to the knowledge base by authoring and editing articles to share current information with team members. ? Worked on fimap to check the possibility of vulnerabilities. ? Worked on DOS and Fire wall intrusion to ensure the security of leakage of code. ? Performed API testing using Soap UI ? Attended meetings on Webex with team of Vice presidents and making valuable contributions. ? Execute and craft different payloads to attack he system to execute XSS and different attacks ? Identified issues on sessions management, Input validations, output encoding, Logging, Exceptions, Cookie attributes, Encryption, Privilege escalations. ? Provided and validated the controls on logging like Authentication logging, profile modification logging, logging details, log retention duration, log location, synchronizing time source, HTTP logging. Environment: Burp suite, Nexpose, HTTP headers, Acunetix, fimap, dirbuster, Soap UI. IT Security Consultant Coca-Cola - Atlanta, GA July 2015 to March 2017 RESPONSIBILITIES ? Ensured all the controls are covered in the checklist Performed Vulnerability Assessment of various web applications used in the organization using Paros Proxy, Burp Suite, and Web Scarab, IBM Appscan. ? Implemented OWASP TOP TEN 2010 Vulnerabilities Assessment. Online application testing and CR regression testing, assessment and reporting. ? Detected and prioritize vulnerability exposures and coordinating with the team for complete closure. ? Static and dynamic scanning of various application using Checkmarx and IBM Appscan, Identify false positives and report in SSC. ? Used tools like NMAP, Nessus, google dorks,

Flagfox, DirBuster, and LiveHTTP Header to gather more information of the application and perform security assessment. ? Conducted host based security by using kali Linux to identify different ports and services running and identifying vulnerabilities by using NMAP script engine. ? Exploited the systems with vulnerabilities using Metasploit framework. ? Analyzed the application for vulnerabilities in categories like Input and data validation, Authentication, Authorization, Configuration Management. ? Performed security assessment by creating test scenarios and test cases against the categories like Sensitive data, Session management, Cryptography, Exception management, Auditing and logging. ? Created documentation for the vulnerabilities identified and reporting it to the application development team. Ensuring timely delivery of issues reported and remediation. ? Followed DREAD approach to provide the risk rating to the vulnerabilities identified. Preparing report with executive summary, technical details and the remediation's ? Performed Web Service Testing using SOAP UI to analyze the vulnerabilities. ? Conducted Web Application User ID access reconciliation and audit of the privileged Database and application user IDS on quarterly basis. ? Understanding new security technologies for potential utilization in the application security testing. ? Audited the project for SOX Compliance by collecting & reviewing the evidences. Making sure all the NCs are closed before the next quarter Audit. ? Performed User Access Management and Identity Management for the various client applications through automatic disablement of dormant users and audit on monthly basis ? Implemented Gap Analysis of present Risk assessment methodology and conducting risk assessment and mitigation steps for the client. ? Identified latest threats and vulnerabilities and conducting the impact analysis to improve the risk level by continuous risk assessment. ? Prepared RMR [Risk Management Report] on account level. Risk assessment done for the account of 8 different projects. Provision of remediation's to minimize risk and follow up to ensure proper implementation as per the control objective. ? Implemented of Software Security Assurance framework in the whole project by conducting Sessions like Secure Programing practices to all the developers. Involving in the complete Agile as a security consultant. Trained modules like Secure design requirements, threat modelling, secure coding practices, penetration testing. ? Using snap tool for create ticket and Hp Qc for defect logging and tracking

Environment: Windows, ASP, Kali Linux, Nessus, Nmap, Metasploit, IBM Apppscan, Checkmarx, SNAP, HP QC, Burpsuite, AWS Security Analyst T-Mobile - Seattle, WA October 2013 to June 2015 RESPONSIBILITIES: ? Incident response, Detection, and Investigations ? Perform pen tests on different application a week. ? Preparation of security testing checklist to the company ? Ensured all the controls are covered in the checklist. ? Physical Pen Testing which includes social engineering, site reconnaissance, lock picking, security bypass, phishing attacks, etc. ? Independently conduct a security assessment, penetration test, and report creation to identify security risks, threats and vulnerabilities of networks, systems, applications, and related components. ? Identified attacks like SQL, XSS, CSRF, RFI/LFI, logical issues. ? Provided security implementation for authorization, by controls like principle of lease p44rivilege, Relinquishing privilege when not in use, Non Guessable tokens, forced browsing. ? Performed semi-automated and manual Web Application and Network Penetration Testing utilizing multiple tools to include, but not be limited by: Burp Suite, Net Sparker, Tenable Nessus, SQLMap, App Detective, Custom Scripts, metasploit, nmap, netcat, and other tools within the Kali Linux toolset. ? Controls on session management like Server side session states, session termination, Session ID randomness, expiration, Unique tokens, concurrent logged in session, session fixation prevention. ? Information gathering of the application using websites like Shodan, Reverse DNS, Hackertarget.com, Google dorks. ? Worked on static code analysis by using the automated tool HPfortify. ? Worked on protecting sensitive data exposure. ? Using various Firefox add-ons like Flag fox, Live HTTP Header, Tamper data to perform the pen test ? Generated automated report by using HPwebinspect. ? Performed manual testing based on the automated generated report. ? Performed monitoring using security assessment tools. ? Monitored security events, correlating information, and identifying incidents, issues, threats, and vulnerabilities found by agency data sources, but are not limited to, vulnerability scanners, baseline configuration management systems, hardware asset management systems, software asset management systems, network contextual analyzer systems, intrusion detection systems (IDS) ? Worked on the XSS, Path traversal attacks manually ? Performed Security Event Analysis as a point of escalation in regard to web based

attacks. ? Worked on the url based vulnerabilities such as redirect and forward, Session management cookie data retrieving. ? Identified the CSRF (Cross Site Request Forgery) by inserting tokens. ? Worked on unauthenticated data access manually. ? Worked on the sensitive data exposure by analyzing the cryptographic algorithms. ? Performed Crawling of application to know the behavior of it. ? Access a web-based collaborative environment to rapidly resolve security issues in software code using HPwebinspect. ? Diagnosed and troubleshot UNIX and Windows processing problems and applied solutions to increase client security. ? Performed Unit testing for proper functioning of UI. ? 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. Environment: UNIX, ASP, Kali Linux, Jira, Nessus, Nmap, Metasploit, Hpfortify, Hpwebinspect, HPQC IT Security Analyst Cycops India Pvt ltd June 2010 to September 2012 RESPONSIBILITIES: ? Perform threat modeling 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. ? Analyzed 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. ? Worked on the DOM XSS by analyzing the JavaScript. ? Good knowledge on web technologies like HTML, CSS, JavaScript to ensure the protection from XSS by reviewing the code. ? Worked on Ng-directives in angular.js for vulnerability assessments. ? Ensured to draft the script manually based on vulnerability. ? Revalidate the issues to ensure the closure of the vulnerabilities. ? Verify if the application has implemented the basic security mechanisms like Job rotation, Privilege escalations, Lease Privilege and Defense in depth. ? Using various add on in Mozilla to assess the application like Wappalyzer, Flagfox, Live HTTP Header, Tamper data. Environment:Wappalyzer,

Flagfox, Nexpose, Live HTTP header, IBM app scan Education Bachelor's Skills SECURITY (7 years), TESTING (5 years), INCIDENT RESPONSE (1 year), NETWORK SECURITY (Less than 1 year), OPERATIONS (Less than 1 year) Additional Information Specialties: ? Incident response, Detection, and Investigations ? Threat analysis and incident Security Operations ? Penetration testing, Vulnerability management & assessment ? Cyber threat intelligence ? Application security, Network security

Name: Michelle Russell

Email: debbie18@example.com

Phone: 284.926.1976x509