Security Analyst Security Analyst Security Analyst - T Mobile Fremont, CA ? Over 9+ 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 SDLF 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. Work Experience Security Analyst T Mobile - Seattle, WA April 2015 to Present 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 SQLi, 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, Nessus, Nmap, Metasploit, Hpfortify, Hpwebinspect Security Engineer CISCO - Sanjose, CA, US February 2013 to March 2015 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, HTTP headers, Acunetix, fimap, dirbuster, Soap UI. Penetration Tester TCS October 2010 to January 2013 RESPONSIBILITIES: ? Perform application and infrastructure penetration tests along with physical security reviews. ? Define requirements for information security solutions and perform reviews of application designs and source code. ? Design, develop and implement penetration tools and tests and also use existing ones to handle penetration testing activities. ? Document and discuss security findings with information technology teams. ? Work on improvements for security services and provide feedback and verification about existing security issues. ? Perform attack simulations on company systems and web applications to determine and exploit security flaws ? Monthly Reviews carried out over the Vulnerability Assessments and Penetration testing. ? Raising issues against any High severity vulnerabilities in the Scan reports. ? Ensured compliance with legal and regulatory requirements. ? Exhibited client facing skills and capability to articulate technical concepts to a variety of technical and non-technical audiences. ? Assisted in review of business solution architectures from security point of view which helped avoiding security related issues/threats at the early stage of project. ? Strong Network Communications, Systems & Application Security (software) background looking forward for implementing, creating, managing and maintaining information security frameworks for large scale challenging environments. ? 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. Environment: Nmap, Nessus, Burpsuite, Sqlmap, Dirbuster. IT Security Analyst Cycops India Pvt ltd June 2008 to September 2010 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, Live HTTP header, IBM app scan Skills Incident response (2 years), Network Security (Less than 1 year), Operations (Less than 1 year), Security (9 years), testing (6 years) 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: Robin Lee

Email: qcole@example.org

Phone: 473-332-6813