Security Consultant Security Consultant Security Consultant - AbbVie Chicago, IL 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. Work Experience Security Consultant AbbVie - Chicago, IL November 2017 to Present Penetration

Testing) Responsibilities: Working in collaboration with both networking and security teams and participated in security assessment of web applications, systems and networks Performed both white box and black box testing for client facing applications Scheduled a Penetration Testing Plan throughout the organization and completed all the tasks in the given time frame Conduct penetration tests on systems and applications using automated and manual techniques with tools such as Metasploit, Burp Suite, Kali Linux, and other open source tools as needed and report the findings Work with tools like Burp Suite, DirBuster, Hp Fortify, Nmap, Acunetix, Webinspect, Nessus, IBM appscan and Checkmarx as part of the penetration testing, on daily basis to complete the assessments Worked with Snort for Intrusion Detection and Prevention (IDS/IPS) for the client network Conducted attack analysis on the IDS reports to detect the attacks and reported the analysis Conducted testing the applications to comply with PCI DSS Standards Performed vulnerability analysis over both wired and wireless networks Identifying the critical, High, Medium, Low vulnerabilities in the applications based on OWASP Top 10 and SANS Top 25 and prioritizing them based on the criticality Update with the new hackings and latest vulnerabilities to ensure no such loopholes are present in the existing system Worked on configuring. Monitoring and analyzing the firewall logs Proficient in understanding application level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, cryptographic attacks, authentication flaws etc Given presentations to client over their security issues and potential solutions for those problems Strong technical aptitude with exceptional talent in training and development IT SECURITY ANALYST Coastal International - Washington, DC January 2016 to October 2017 Responsibilities: Reviewing, maintaining, and ensuring all Assessments and Authorizations (A&A) documentation are included in the system security package. Ensure Implementation of appropriate security control for Information System based on NIST 800-53 rev4, FIPS 200, and System Categorization using NIST 800-60 and FIPS 199. Review and update remediation Plan of Action & Milestones (POA&Ms) in Cyber Security Assessment and Management (CSAM), gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist with the closure of the POA&M. Perform vulnerability and baseline scans, using tools such as Tenable Nessus, analysis scan

results, and document findings in POA&M. Collaborate with system administrators to remediate POA&Ms findings. Ensure vulnerabilities and risks are efficiently mitigated in accordance with the organization continuous monitoring Plan. Monitor controls post authorization to ensure continuous compliance with the security requirements. Identify new and maintain the disposal of information system inventory in accordance with established policies and procedures while ensuring accurate configuration management and property accountability. Modify and maintain procedures, operational process document, change control document, operational checklist, and detailed system specifications. Conducted security assessment interviews to determine the Security posture of the System and to develop a Security Assessment Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization to Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization. Information Security Analyst INDIGO IT, LLC - Reston, VA September 2013 to December 2015 ma Responsibilities: Ensure proper system categorization using NIST 800-60 and FIPS 199; implement appropriate security controls for information system based on NIST 800-53 rev 4 and FIPS 200. Perform kick Off Meetings Apply appropriate information security control for Federal Information system based on NIST 800-37 Rev 1. Facilitate Security Control Assessment (SCA) and monitor activities. Develop a Security Assessment Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization To Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization. Reviewing, maintaining, and ensuring all assessment and authorization (A&A) documentation is included in the system security package. Perform information security risk assessments and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues and also identified mitigation requirements. Work with system owners to develop, test, and train on contingency plans and incident response plans. Tests, assess, and document security control effectiveness. Collect evidence, interview personnel, and examine records to evaluate effectiveness of controls. Review and update remediation on plan of action and milestones (POA&Ms), in

organization's Xacter 360/CSAM. Work with system administrators to resolve POA&Ms, gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist in the closure of the POA&M. Activities for investigations. Security Tester CBay Systems Pvt Ltd - Bengaluru, Karnataka July 2011 to August 2013 Responsibilities: Performed Manual Penetration Testing and Vulnerability Assessment on various web applications. Performed the manual code review to remove the False Positives. Performed Vulnerability assessments and Patch management related tasks Experience in different web application security testing tools like Burp Suite, SQLmap, Nessus, and Qualys. Good understanding and experience for testing vulnerabilities based on OWASP Top 10. Capable of identifying flaws like SQL Injection, XSS, Insecure direct object reference, Security Misconfiguration, Sensitive data exposure, Functional level access control, CSRF, Invalidated redirects. Vulnerability Assessment includes analysis of bugs in various applications on various domains. Experienced in Dynamic Application Security Testing (DAST) & Static Application Security Testing (SAST) Performed Static Application Security Testing (SAST) using tools such as HP Fortify. Performed Dynamic Application Security Testing (DAST) using tools such as IBM AppScan, Kalilinux Security assessment based on OWASP framework and reporting the identified issues in the industry standard framework. Conducted Web Application Vulnerability Assessment, secure code review on the applications. Conduct re-assessment after mitigating the vulnerabilities found in the assessment phase. Assist developers in remediating issues with Security Assessments with respect to OSWASP standards. Education Bachelor's Skills NESSUS (5 years), EXCEL (Less than 1 year), MICROSOFT OFFICE (Less than 1 year), MS OFFICE (Less than 1 year), POWERPOINT (Less than 1 year) Certifications/Licenses Security Guard Additional Information TECHNOLOGIES AND EXPERTISE

Computer skills: Microsoft Office Suite, 70wpm, Adobe, PowerPoint, Excel Network tools: Nessus (SC-5), CSAM, IACS360

Name: Alexandra Burke

Email: rebecca10@example.net

Phone: 001-645-611-8392