Senior Application Analyst- Consultant Senior Application Analyst- Consultant Senior Application Analyst- Consultant - Mindlance, Inc San Francisco, CA Authorized to work in the US for any employer Work Experience Senior Application Analyst- Consultant Mindlance, Inc - San Francisco, CA March 2018 to Present Client: Charles Schwab At TransUnion, we have a welcoming and energetic environment that encourages collaboration and innovation we're consistently exploring new technologies and tools to be agile. This environment gives our people the opportunity to hone current skills and build new capabilities, while discovering their genius. Come be a part of our team - you'll work with great people, pioneering products and cutting-edge technology ? Performed static code analysis for client using tools such as Veracode and Checkmarx ? Subject Matter Expert in Software development life cycle ? Analysis of code of different applications across the client platform ? Review source code in .Net, PHP, Java, J2EE, Internet-Web ? Help reduce the attack surface on client application and limit the number of vulnerabilities by finding software bugs early in the development life cycle well before the application goes to production ? Provide security code reviews using Veracode and Checkmarx and evaluate results for security vulnerabilities for banking applications ? Review vendors application code to remediate flaws inside the code ? Collaborate with other information security teams in the evaluation, development, implementation, communication, operation, monitoring and maintenance of security policies and procedure to promote a secure and innovative environment ? Identifying emerging vulnerabilities, risks and threats during design iterations and provide appropriate countermeasures. Penetration Tester SME - Web Apps Security Tata Consultancy Services October 2016 to February 2018 Clients: McGraw Hill, JCPenney At Capital One, we're building a leading information-based technology company. Still founder-led by Chairman and Chief Executive Officer Richard Fairbank, Capital One is on a mission to help our customers succeed by bringing ingenuity, simplicity, and humanity to banking. We measure our efforts by the success our customers enjoy and the advocacy they exhibit. We are succeeding because they are succeeding.   Guided by our shared values, we thrive in an environment where collaboration and openness are valued. We believe that innovation is powered by perspective and that teamwork and respect for each other lead to superior results. We elevate each other and obsess about doing the right thing. Our associates serve with humility and a deep respect for their responsibility in helping our customers achieve their goals and realize their dreams. Together, we are on a quest to change banking for good.   Manager, Penetration Testing ? Performed Dynamic and Static application security testing across multiple platforms ? Conducting internal penetration testing for various clients across the state ? Supervised a team of six employees offshore in Usa by supporting multiple applications ? Experience in information security technologies such as Splunk Enterprise Security, IDS/IPS, and McAfee Vulnerability management. ? Expertise in identifying OWASP Mobile and Web applications top 10 and SANS 25 vulnerabilities ? Providing customers with best practice guidelines and practical suggestions to protect against or mitigate threats; provided remediation recommendations as needed ? Performing Web application vulnerability assessments/ Network based security assessments ? Expertise in analyzing threats and categorizing them based on critical of the security vulnerability ? Involved in scoping, identification, analysis and evaluation of application security risk. ? Performed vulnerability assessment & penetration-testing using automated tools on web applications and Mobile applications. ? Evaluated vulnerabilities identified due to configuration issues, patch management and third-party applications ? Led a team of 3 consultants to perform Vulnerability Assessment on the Web Based application. ? Involved in detection & classification of vulnerability based on OWASP Top Ten methodology. ? Work on common vulnerabilities such as directory traversal, parameter manipulation, information disclosure, web server vulnerabilities, buffer overflows, format string bugs, race conditions, weak authentication & authorization schemes, session management, cookie manipulation and forceful browsing. ? Installed, configured & customized Fortify Secure Code Analyzer to assist in Secure Development Process (Tools Usage - W3af, Paros, Metasploit, Social Engineer Toolkit,Kali Linux, Burp Suite & ZAP) Cyber Security Analyst - Consultant Valiant Solutions - Washington, DC August 2014 to October 2016 Responsibilities: We are seeking an IT Cyber Security Analyst to join our diverse cyber security team reporting to the CISO. Members of this team are responsible for protecting SLAC networks from cyber threats by actively monitoring for security anomalies, performing vulnerability assessments, and balancing security with business rules/needs. You'll need past experience and understanding of the cyber security environment, common network and host-based attacks, attack methods, and network defense architecture; in addition, have previous experience working in a security operations environment. ? Performed Unauthenticated / Authenticated web application scans using HP Webinspect. Worked closely with developer to mitigate vulnerability findings Gray Box &White box testing and manual penetration testing. Configuration Management on Assessment Management Platform (AMP). Execute HP Fortify Webinspect scans and verify reported vulnerabilities with Burp Proxy ? Performed vulnerability scanning using QualysGuard to identify potential security vulnerabilities, prepares reports on security risks and help determine the most appropriate corrective measures ? Conducted testing of Internet facing applications, as well as applications containing Personal Identifiable Information. Lead monthly conference call to discuss vulnerability reports with developer. Demonstrated experience in Web Application Security, Penetration testing. Found common web site security issues (XSS, CSRF, Session fixation, SQL injection, information leakage, application logic, etc.) across various platforms. Executed daily vulnerability assessments, threat assessment, and mitigation and reporting activities in order to safeguard information assets and ensure protection has been put in place on the systems. ? Conducted open security testing standards and projects, including OWASP secure coding practices and Top Ten testing framework, FISMA, NIST, OWASC. Serves as an IT security subject matter expert and establishes and implements formalized plans to address operational IT security issues ? Perform vulnerability scans using Nessus Security Center. Assigned roles and permissions to user and department staff. Conducts Pre-assessment and Post assessment activities for assigned systems. ? Maintain Google spreadsheet for all GSA Applications and Systems. Knowledge of common application vulnerabilities, current threat vectors and mitigations. Identify security risks, threats and vulnerabilities of networks, systems, applications and related components. ? Conducted vulnerability assessment on the application & underlining infrastructure. ? Performed Web Application Testing using IBM Rational AppScan, intrusive and non-intrusive techniques. (Tools Usage - IBM Rational AppScan, Paros, Qualys Guard, Burp Suite) Penetration Tester SME - Principal Consultant GBTI Solutions - McLean, VA June 2013 to August

2014 Responsibilities: ? Functioned as presales consultant role for the Security & Vulnerability Offering. ? Focused on presales, development of practice collateral, education & support of the marketing team. Worked on Avaya and Citrix Solutions. Client - Library of Congress / Peace Corps (Washington, DC) ? Conducted Web Application Security Testing (Black Box Testing) using automated tools and detailed manual testing looking for typical web application specific security holes like Cross-Site Scripting, SQL Injection, URL redirection as well as attempts to avert business logic of the application. ? Focused on OWASP Top 10 vulnerability assessment and test framework development. ? Customized report generated by Webinspect aligned to client requirements. ? Coordinated with developers in understanding & fixing of vulnerabilities as part of the QA process. ? Scanned financial database for Peace Corps for vulnerabilities based on the RESTful architectures. Conducted white / gray box penetration testing on the financial systems. ? Involved in Infrastructure Security Assessment based on OSSTMM methodology, Vulnerability Assessment and Penetration testing of infrastructure. ? Identified vulnerability mitigation techniques and OS hardening routines across platforms. ? (Tools Usage - IBM AppScan, Paros, sqlmap, Kali Linux, Cobalt Strike, Hping, Burp Suite) Technical Lead / Web Application Security Tester Infosys Ltd - Bridgewater, NJ December 2012 to June 2013 Bridgewater, NJ Dec 2012 to Jun 2013 Client - Pfizer - Pharmaceutical Company (Collegeville, PA) Technical Lead / Web Application Security Tester Every day at Perspecta, we enable hundreds of thousands of people to take on our nation's most important work. We're a company founded on a diverse set of capabilities and skills, bound together by a single promise: we never stop solving our nation's most complex challenges. Our team of engineers, analysts, developers, investigators, integrators and architects work tirelessly to create innovative solutions. We continually push ourselves - to respond, to adapt, to go further. To look ahead to the changing landscape and develop new and innovative ways to serve our customers. ? Assisted in managing Nessus Tenable Security Center across multiple platforms ? Involved in design & management of projects related to new security requirements & enhancements to the Internet infrastructure. ? Planned & developed secured information systems & network infrastructure to strategically support Internet infrastructure. ? Conducted penetration testing &

vulnerability assessment for in-house applications followed by preparation of detailed reports ? Designed, implemented, administered & troubleshot NIDS, HIDS and Antivirus infrastructure ? Performed architectural review, security policy, firewall rule base analysis, application testing and general benchmarking using manual and automated penetration testing Web Application Security Consultant Client - Financial September 2011 to December 2012 Responsibilities: Oasis Systems has an exciting opportunity for a Cyber Security Analyst in Rockville, MD. The Cyber Security Analyst acts as a lead consultant, interfacing between the customer and IT security consulting team throughout the federal information system Security Assessment & Authorization (SA&A) lifecycle process. The ideal candidate is very detail oriented with strong written and oral communication skills as well as a strong technical background. He/she will be responsible for planning, developing, finalizing, and reviewing key deliverables in each stage of the SA&A process. As a result, a strong understanding of standards and requirements outlined by FISMA, NIST, OMB and other federal guidelines is required. The Cyber Security Analyst will be actively engaged in identifying unique system characteristics, interviewing key organizational personnel (technical, administrative, and executive), and working with the consulting team to develop and manage security documentation throughout the system lifecycle in support of FISMA requirements. This includes, but is not limited to; security ? Helping customers manage cyber risk through a variety of services geared towards minimizing exposure and maximizing return on investment. Conducted network & application penetration testing, web application security reviews and source code security analysis for internal clients. ? Worked with developers and administrators to remediate identified vulnerabilities. Developed proof-of concept exploits and knowledge on risk rating methodology like CVSS scores. Assisted with clients to review policies and recommended adjustments. ? Knowledge about OWASP top 10 vulnerabilities with an understanding of Web based application vulnerabilities and SANS methodology. Performed on-site and remote penetration tests for diverse clients. IT Security Consultant Jacobs Engineering - Baton Rouge, LA December 2010 to September 2011 Responsibilities: ? Worked on network security including implementation for perimeter security ? Security hardening of network infrastructure and monitoring ? Developed secure network architecture for new and existing environments. ? Performed Engineering applications install on workstations and providing customers with best practices guidelines and practical suggestions to protect against threats. ? Scanned networks servers and other resources for customers to validate compliance and security issues ? Created details reports containing prioritized findings, demonstration of exploits, explanation of compromise impacts, and recommendations for mitigation ? Responsible for configuring and maintaining communications including firewalls, Internet connections, virtual private networks, point to point connections and remote access ? Specialized in network security assessments, perimeter defenses log analysis, information security monitoring and risk analysis. Technical Consultant & Security Stupp Corp - Baton Rouge, LA March 2009 to November 2010 Responsibilities: Performed daily backup of data and disk imaging systems using Acronis True Image Conducted penetration testing of web applications and networks and setup email accounts for new users through Active Directory Blackberry Enterprise Server Updates & Cell phone configuration and administration Worked closely with customers in resolving day to day problems in Unix / Networking environments. Configured and maintained wireless hardware devices including coordination of repair and maintenance through support vendor. Conducted penetration testing on in-house developed applications, production networks, and production systems and devices Assisted in resolution of exposed security weaknesses Installation Engineer Evault Inc - Emeryville, CA March 2007 to February 2009 Responsibilities: The Systems Engineer is responsible for ensuring the provision of a high performance, fault tolerant business systems infrastructure to corporate users and restaurants. He or she will be responsible for planning, implementing and supporting new enterprise technology as necessary. This role will also be expected to collaborate with Information Technology (IT) Team colleagues on the development, revision, and implementation of the IT Strategy. ? Installed remotely software Agent on client systems through GoToAssist - A remote support technology which included AIX, Linux, Exchange DR & MAPI, SharePoint, Oracle, WinXP, SQL, Solaris, HP-UX, iSeries AS/400 ? Installed new computer systems and connecting them into the Local Area Network. ? Managed Vault for all clients using Evault Director Software. ? Performed client backup and restores using Web Central

Control & Window Central Control ? Provided support to off-site clients via telephone and E-mail on policies, procedures and best practices ? Performed backup and restores using Storage virtualization ? Conducted daily maintenance of user's security accounts in Windows 2008 including desktop & workstations Programming Languages & Concepts PERL JavaScript Python Angular JS ? Applied Cryptography, Risk Analysis, Social Engineering, Web Apps, Cross-site Scripting, SQL injection, Thread Modeling, NASM, Network Protocol, Penetration Testing, Hack with Python, SLDC, Vulnerability, Data Leakage, File integrity, Virus / Trojan, Malware, Ollydbg, Database, PEBrowser, Buffer Overflow, Fuzzing Techniques, Immunity Debugger, Shellcode, WordPress Hacking, Metasploit Framework, Software Security Testing ? SOAP, XML, WSDL, NIDS, HIDS, FTP, IPsec, SSH, Gray Box, White Box, Black Box ? Red Team, Blue Team, DNS, Encoding, Encryption, Hashing Education Master in Science in Computer Crime in Computer Crime Madison University Bachelor in Science in Engineering in Engineering Odessa University Associate in Science in Information Systems in Information Systems DeVry University - Reedley, CA Skills DNS, SECURITY, NESSUS, NIST, NMAP, SOX, SIEM, SPLUNK, SSL, WIRESHARK, APACHE, LINUX, RADIUS, HTTP, TCP/IP, LDAP, TCP, TELNET, ANDROID, IOS Additional Information Skills: DNS (3 years), Linux (4 years), Nessus (1 year), Security (10+ years), testing (10+ years) Skills Technologies: IBM AppScan, Windows Server, W3af, Wireshark, Kali Linux, SIEM, Nessus, Web Scarab, HP Fortify, Nmap, Burp Suite Pro, Mobile Apps, Paros Proxy, Splunk, Cobalt Strike, Web Applications, HP WebInspect, Android Tamer, OWASP, Hping, NSLookUp, Telnet, L0pht Crack, Protocols/Standards/Systems: TCP/IP, UDP, Apache server, SSL/TLS, LDAP, HTTP(S), DNS, RADIUS, EAP (TLS, TTLS, MD5), and STRIDE / DREAD threat models. Cyber Kill Chain, NIST SP 800, SOX Rapid7Nexpose White Paper/ Patents/ Articles Published iOS: Application Penetration Testing - Course online at Pentestmag.com Mobile Security Framework - Research Project

Name: Jessica Pena

Email: iroth@example.net

Phone: +1-200-354-3759x020