Security Consulting Consultant Security Consulting Consultant Security Consulting Consultant - Accenture Reston, VA 5 years of experience as Security Engineer in various domains such as Web Application security testing, Vulnerability Assessment, penetration testing, threat modeling and generating reports Certified in Cyber Security. Hands-on experience in developing threat models, security controls, threat analysis, creation of risk control matrices and risk mitigation strategies. Hands-on experience on OWASP -Top 10 for Web and Mobile applications. Expertise knowledge in Penetration Testing, DAST, SAST and manual ethical hacking. Experienced in System Support and Linux Platforms focusing on Information Security. Working Knowledge of Secure Software Development Life Cycle[SSDLC]. Experienced in analyzing the Security requirements for application development. Experience in conducting IT Security Risk Assessments in accordance to NIST and FFIEC framework. Experience in vulnerability assessment and penetration testing using various tools like Burp Suite, Dir-Buster, OWASP ZAP proxy, HP WebInspect, NMAP, Nessus, Nikto, web scanner, w3af, HP Fortify, IBM App Scan enterprise, Kali Linux. Work with global security teams performing application and IT infrastructure security assessments. In-depth knowledge of penetration testing for web and mobile (iOS and Android) applications. Have a good understanding of Web Application based attacks to include Denial-of-service attacks, MITM attacks, Local file inclusion(LFI), Remote file inclusion(RFI) and Buffer overflow. Performed security design and architecture reviews for web and mobile applications. Knowledge of AWS Cloud Security in implementing Web Application Firewalls (WAF). Hands on Experience working with LAN and WAN topologies, TCP/IP protocol, routers, switches, and firewalls in Internet, Intranet and Extranet environments. Worked on Firewall Administration, Rule Analysis, and Rule Modification. Worked with Cloud compliant and web application security using Qualys Guard. Excellent scripting and debugging skills on JavaScript, Python Scripting, Php and Ruby. Good Understanding of Object Oriented Programming. Expertise in generating DDL, DML and DRL queries in SQL to retrieve data from target database and in designing schemas, creating databases and executing queries using SQL. Experienced in commonly used protocols like TCP/IP, DHCP, SSL, SSH, DNS, OSPF, DNS, FTP, IMAP4, SMTP,

SNMP Good knowledge in System Administration Effective in executing multiple tasks and assignments and Strong team player. Sponsorship required to work in the US Work Experience Security Consulting Consultant Accenture March 2018 to Present Responsibilities Security Architecture Analysis Conducting Application vulnerability assessments with manual testing and automated scanner Manual Web application testing using Burp Suite, Firefox addons, kali Linux tools and Automated Testing using dynamic web scanning tools such as WebInspect Reporting Vulnerability findings to Application owners and helping them in remediation of vulnerabilities. Conducting Project security reviews, security requirements and design Reviews to implement security at Concept & analysis phases in SDLC. Create client specific penetration test reports based on both automated and manual testing results. Drive client meetings explaining technical and business impacts of vulnerabilities. Security Testing of deployed application in Test environments for OWASP top 10 Vulnerabilities. Experience in information security with specific application penetration testing with IOT Applications. Identify security issues such as Cross Site Scripting (XSS Stored & Reflected), SQL Injection, Cookie Manipulation, HTML injection, CSRF, Session Fixation, OpenSSL Insecure Development, Insecure Direct object Reference. Engage in false positive review of dynamic scan results. Conducting Application Vulnerability Assessments, analysis, monitoring and reporting, and audits. Identified issues that could be a future vulnerability and Reported. Retesting the application for the found vulnerabilities & Post production support. Working on the remediation of web security issues for client's core applications. Performed Risk assessment to ensure corporate compliance. Familiarity with DevSecOps Environment. IT Security Engineer/Pen Tester College Board - Reston, VA August 2017 to March 2018 Responsibilities Security Code Review and Penetration Testing for all Internal & External Applications of the CollegeBoard applications. Follow up with Development teams to get recent functionality changes, their security analysis scheduling and coordinating with my team to sync with the project changes. Evaluating the business requirements, Application Functionality with the Project teams to do assessment. Security support for Enterprise Architecture(EA) team to support Secure SDLC implementation Analyze the application for Security Assessment by both manual &

automation. Perform validation and verification. Recommend process improvements. Define the timelines to the given application & Conduct the security assessments and Report out the vulnerability findings with remediation process to the development team. Troubleshooting The Firewalls, VPN Devices and Routers. Retesting the application for the found vulnerabilities & Post production support. Conducted studies of new security technologies to provide more efficient and cost effective 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. Investigate logs and payloads for server crashes/core dumps, DDoSattacks, SQL/XSS etc. Adding rules to firewalls and routers. Perform Server scans for both internal and external IP addresses using Rapid 7 Nexpose. Utilized Kali Linux and Metasploit for exploiting the systems. Assist developers in remediating issues with Security Assessments with respect to OWASP standards. Follow up and ensure the closure of the raised vulnerabilities by revalidating and ensuring 100% Closure. Information Security Analyst Unisys - Blue Bell, PA June 2016 to July 2017 Responsibilities Conducting Application vulnerability assessments with manual testing and automated scanners. Reporting Vulnerability findings to Application owners and helping them in remediation of vulnerabilities Security Testing of deployed application in Test environments for OWASP top 10 Vulnerabilities. Responsible for Performing of penetration testing on web applications which involves Manual & Automated (Tool-driven). Performed Static and Dynamic Analysis and Security Testing (SAST and DAST) for various applications as per firm's security standards (i.e., OWASP) Manual Web application testing using Burp suite, Firefox addons, and Automated Testing using HP Web Inspect, Checkmark, HP fortify and kali Linux tools. Identify security issues such as Cross Site Scripting, SQL Injection, Cookie Manipulation. To address and integrate Security in SDLC by following techniques like Threat Modeling, Risk Management, Logging, Penetration Testing, etc. Conducting Application Vulnerability Assessments, analysis, monitoring and reporting, and audits. Identified issues that could be a future vulnerability and Reported. Performed annual clean up activity for firewall rules. Working on the remediation of web security issues for client's core

applications. Performed Risk assessment to ensure corporate compliance. Information Security Engineer Hood College November 2014 to May 2016 Responsibilities Responsible for performing security assessments, informing the client about inherent security risks, and providing meaningful hardening and mitigation strategies. Conduct network and web-based application penetration tests, physical security assessments, logical security audit, and hands-on technical security evaluations. Identification of Injection, Business logic, Authentication, Session Management, etc. related flaws in applications and encasing attack scenarios and associated risk to business. Responsible for documenting manual testing (MT) process document for assessing the security risk of that application Analyze the Vulnerability assessment reports. Identifying the critical, High, Medium, Low vulnerabilities in the applications based on OWASP Top 10 and SANS 25 and prioritizing them based on the criticality. Experienced in Telecommunication &Networking and Developed Network Topologies Stimulators using with GNS3 tool Involved in Testing Network simulator and validating the responses. Configuring VLANs/routing/NATing with the firewalls as per the network design. Worked on network management including configuration and troubleshooting corporate networks. High familiarity with Windows and UNIX environments at command line. Written UNIX shell scripts and Commands for deploying and configuring. Studied and analyzed client requirements to provide solutions for network design, configuration, administration, and security Experience in Cisco switches and routers, Physical cabling, IP addressing, Wide Area network configurations (Frame-relay and ATM) Making configuration changes to storage/servers/Cisco ASA, routers, SonicWALL, switches, Wireless access points as required Experience with maintenance and troubleshooting of connectivity problems using Ping and Trace route Managed IP address space using subnets and variable length subnet masks (VLSM) Involved in troubleshooting problems on day to day basis and provided solutions to fix the problems Worked on TCP/IP protocol and commonly used ports. Assist with VPN protocols & it's security, Ensuring the data packets encrypted with Wireshark implementation. Provided in depth technical expertise for remediation of identified issues. Associate Security Engineer CFST - Hyderabad, Telangana September 2013 to August 2014 Responsibilities Involved in Application

vulnerability assessments with manual testing and automated scanner. Web Application Pentest based on OWASP standards and testing guide and reporting to the client Involved in Identified Vulnerabilities (XSS and Authentication) through external penetration testing in a web application. Reporting Vulnerability findings to Application owners and helping them in remediation of vulnerabilities. Conducted Project security reviews, security requirements and design Reviews to implement security at Concept & analysis phases in SDLC Involved in vulnerability scanning and penetration test to analyze the information and determine the risk to the organization. Review security logs of various devices to perform analytics and forensics methodologies. Manual Web application testing using Burpsuite, Firefox addons and Verify the false positives of the vulnerabilities reported by automated scanner. Prepared comprehensive security report detailing identifications and recommendations for the Vulnerabilities performs exploit, vulnerability and penetration assessments that identify current and future internal and external security vulnerabilities

Review security logs of various devices to perform analytics and forensics methodologies. Log management and event management of various Platforms, devices using SIEM. Assist SIEM report generation on Daily, Monthly Basis Education Master's Skills SECURITY (4 years), TESTING (4 years), LINUX (2 years), SQL (2 years), WIRESHARK (1 year) Additional Information TECHNICAL SKILLS: Web Application Security Scanner HPWebInspect, Kali Linux tools Security Tools Burp Suite, w3af, Nikto, Vega, OWASP ZAP Mobile Application Security-Testing Android Mobile emulators. Network Vulnerability Scanner Nmap, Nessus, Qualysguard, Wireshark Networking Tool GNS3, VPCS/QEMU, Firewall Routing Computer Forensics tools Forensic Tool Kit(FTK), Digital Forensic Framework(DFF) Programming Languages JAVA, Microsoft.net Tools &Applications Maven, Intellij IDEA, SQL, Python, Putty, WinScp Operating System LINUX, Windows XP/VISTA/7 &10 Databases My-SQL Web Technologies Java Script, HTML, CSS, PHP.

Name: Christopher Harmon

Email: jason00@example.org

Phone: 001-627-782-5092x29018