**SUMANTH KUMAR TEJA**

**Email:** [sumanthkumar.t7777@gmail.com](mailto:sumanthkumar.t7777@gmail.com)**s**

**Phone Number: 903 347 3542**

**Greenfield, IN**

**PROFESSIONAL SUMMARY**

* Over 5 Years of professional IT Experience in Penetration Testing particularly focused on performing technical activities such as Code review, Vulnerability Analysis, Penetration testing, Secure Application Testing based on OWASP.
* Identifying and exploiting network level vulnerabilities on open ports like SSH vulnerabilities, SSL certificate related vulnerabilities, RDP, FTP, SMTP, and SNMP Vulnerabilities etc.,
* .Experience using a wide variety of security tools to include Kali-Linux, Wireshark, Nessus, Qualys Guard.
* Hands on Experience on vulnerability assessment and penetration testing using various tools like Burp Suite, Fiddler, ZAP Proxy, SQL map, HP Web Inspect and IBM AppScan,HP fortify, to determine the security of web application developed in different platforms like .NET, Java, AJAX, PHP and many others.
* Security assessment of online applications to identify the vulnerabilities in different categories like Input and data Validation, Authentication, Authorization, Auditing & logging.
* Experienced in Static Analysis Security Testing (SAST) using CHECKMARX and Dynamic Analysis Security Testing (DAST) using Burp Suite and Acunetix.
* Experience in different web application security testing tools like Accunetix, Metasploit, Burp Suite, Sqlmap, OWASP ZAP Proxy, Nmap and HP Fortify.
* Experience with TCP/IP, Firewalls, and LAN/WAN, UDP, IPSEC and routing protocols.
* Experience with scheduling firewall policy provisioning and user interaction to identify connectivity related issues.
* Experience in intelligence analysts in identification of threats, vulnerabilities, countermeasures, and conducted vulnerability compliance assessments, procedures, and corrections to Top Secret and unclassified networks.
* Assists in capacity planning, disaster Recovery planning and testing.
* Detailed reports based on Stride and Dread threat modelling.
* Involved in implementing and validating the security principles of minimum attack surface area, least privilege, secure defaults, avoiding security by obscurity, keep security simple, Fixing security issues correctly.

**TECHNICAL SKILLS**

* **Tools:** Burp Suite, IBM AppScan, Kali Linux, SQLmap, HP Fortify, Nexpose, HP Web Inspect, Metasploit, OpenVAS, OWASP ZAP proxy, SoapUI, QualysGuard, QRadar SIEM.
* **Tools:** N-map, Nessus
* **Platforms:** Windows XP, 10, UNIX/LINUX.
* **PenTest Tools:** Metasploit, NMAP, Wireshark
* **Operating Systems:** Windows, NT, Windows 98/XP/2000/2003/2007, MS-DOS, Linux

**EDUCATION**

* M.S. in Electrical Engineering University of Texas at Arlington, TX, USA
* B.E. in Electronics and Communication Engineering

**PROFESSIONAL EXPERIENCE:**

**Client:Elanco**

**Location: Greenfield, IN Date of Employment: Jan 2020-Till Now.**

**Penetration Tester**

**Job Description**

* Analyze and escalate events and incidents to SOC Analyst Level for response and resolution.
* Worked on OWASP top 10, SANS 25 and Common Vulnerabilities and Exposures (CVE) identifying, reporting and help developers in remediating the issues.
* Conducting Web Application Vulnerability Assessment, Threat Modeling and secure code reviews on the applications.
* Efficiently performed web application, vulnerability assessment using Burp Suite, HP Web Inspect, Nexpose and IBM AppScan.
* Perform manual security testing for OWASP Top 10 vulnerabilities like SQL Injection attacks, cross site scripting (XSS), CSRF, and Session Management etc.
* Security assessment of online web applications to identify the vulnerabilities in distinct categories like Input and data Validation, Authentication, Authorization and risk assessment.
* Experience in using Kali Linux performing web application assessment to identify, validate and exploit vulnerabilities using tools like Metasploit, DirBuster, OpenVAS, Nikto, SoapUI and Nmap.
* Experience working with SQLmap, an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.
* Identifying the risk level (critical, High, Medium, Low) and prioritizing vulnerabilities found in web applications based on OWASP Top 10, SANS 25 and GSEC.
* Performed static code reviews with the help of automation tools.
* Training the development team on the most common vulnerabilities and common code review issues and explaining the remediation's, prioritizing the issues found.
* STRIDE assessment of the applications during the design phase, identifying the threats possible and providing security requirements.
* Provide software security support related to Fortify, HP Web inspect and remediation guidance to development teams.
* Identifying vulnerabilities and threats based on client's security policy and regulatory requirements such as PCI, PII, HIPAA, and SOX.
* Performed penetration testing and vulnerability management over the enterprise systems to audit the standards to comply with NIST and ISO 2700x standards.
* Vulnerability Management by scanning, mapping and identifying possible security holes using Qualys Guard and Nessus scanner.
* Reviewing the reports and code removing the False Positives and identify the False Negatives.

**Client: AIG**

**Location: Fort Worth, TX**

**Penetration Tester Date of Employment: July 2018-Dec 2019.**

**Job Description:**

* Static Code analysis using HP Fortify to identify the vulnerabilities in the applications.
* Hands on experience performing security assessment with SAST and DAST using tools like HP Fortify, HP Web Inspect and IBM AppScan.
* Performed Vulnerability Assessments using - Kali Linux / Metasploit / BurpSuite / Paros / SQLmap and many open source tools.
* Responsible for Source code analysis of multiple teams using Checkmarx and updating the triaged report findings to developers.
* Initiated/run DAST, SAST scans (Fortify, Checkmarx)
* Identify and remediate application security vulnerabilities (OWASP top 10) using Dynamic analysis (DAST), static analysis (SAST) tools such as IBM Appscan, Checkmarx.
* Performed dynamic analysis (DAST) and static code reviews ( SAST)with Veracode, extracted reports and opened tickets to track the development efforts using JIRA, and meet with development teams as required and remediate
* Used Sqlmap and Nmap for VAPT, and prepared reports for audit according to OWASP with all issues and their mitigation.
* Proficient in detecting application level vulnerabilities like XSS, SQL Injection, CSRF, authentication flaws etc both through automation and manual testing.
* Identified issues on session management, Input validations, output encoding, Logging, Cookie attributes, Encryption, Privilege escalations.
* Create Vulnerability Assessment report detailing exposures that were identified, rate the severity of the system & suggestions to mitigate any exposures & testing known vulnerabilities.
* Performed Network scanning using tools Nessus and Nmap and generated reports.
* Responsible for maintaining, reporting and communication of SIEM between event-sources and endpoints.

**Client: UPS**

**Location: Mahwah,NJ**

**Security Analyst Date of Employment: October 2017- June 2018**

**Job Description**

* Performed penetration testing on CVS infrastructure and vulnerability assessment of application and database servers.
* Conducted security assessment of PKI Enabled Applications.
* Skilled using Burp Suite, Acunetix Automatic Scanner, NMAP for web application penetration tests.
* Good knowledge of network and security technologies such as Firewalls, TCP/IP, LAN/WAN, IDS/IPS, Routing and Switching.
* Involved in all the projects at all stages to help in the security related issues and solutions.
* Develop test cases to test web application according to OWASP and mapped every test case to NIST control.
* Vulnerability assessment using Nessus and other monitoring tools like ESM for asset management.
* Manage all repeated threats to all systems and perform vulnerability tests.
* Assisted in managing Nessus Tenable Security Center across multiple platforms SMB exploitation using NMAP and exploit from Metasploit Framework and implementing security policies within the client's infrastructure.
* Performed network & infrastructure vulnerability assessment using automated tools such as Qualys Guard and Nmap.
* Maintains network performance by performing network monitoring and analysis, performance tuning, troubleshooting network problems,Skilled using Burp Suite, Acunetix Automatic Scanner, NMAP, Dir-Buster, HP Fortify, Qualys-guard, IBM Appscan.
* Worked on Static Secure Code Reviews using Checkmarx and HP Fortify.
* Good knowledge in programming and scripting in .net, Java.
* 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.
* Security assessment of online applications to identify the vulnerabilities in different categories like Input and data Validation, Authentication, Authorization, Auditing & logging.
* Vulnerability Assessment of various web applications used in the organization using Paros Proxy, Burp Suite, and HP Web Inspect.
* Conducts regularly review of Global Security Incidents as well as reports and update the same to the internal teams.
* Manage the Security Incident and Event Management (SIEM) infrastructure
* Collaborate across the entire organization to bring Splunk access to product and technical teams to get the right solution delivered and drive future innovation gathered from customer input.
* Managed day-to-day activities of threat and vulnerability management, identify risk tolerances, recommend treatment plans and communicate information about residual risk.

**Spotric Systems, India Date of Employment: Jan 2016- July 2017**

**Cyber Security Analyst**

**Job Description**

* Conducted Vulnerability Assessment of Web Applications.
* Evaluated all repeated threats to all systems and performed vulnerability tests.
* Manage daily operational service monitoring activities over of the SOC security infrastructure.
* Daily monitoring of event collection, security intelligence and emerging threat information sources including SIEM, vendors, researchers, websites, newsfeeds and other sources.
* Create new content and manage existing notable events in Splunk Enterprise Security → Worked with Security Operations Centre (SOC) to fine-tune the False-Positives from the existing SIEM Rules.
* Working with Security Operations Center (SOC) to find the existing log gaps and provide a better data analysis to increase the overall security coverage.
* Manage Splunk Enterprise to collect, monitor, and analyze machine data.
* Performed/Assisted in installation, configuration, troubleshooting and maintenance of SIEM Agents, Log Managers/Collectors, and SIEM Central Managers/Aggregators.
* Deploying Splunk; creating Port mirroring/ installing Splunk/ Install Stream Application on Splunk/ Setting up Sys log in Cent OS/ installing Universal Forwarder.
* Used Splunk Enterprise Security for real time monitoring, to prioritize the acts and for rapid investigations.
* Deploy, configure and tune Flow data within SIEM; must also document how such data is to be used during event triage.
* Network Monitoring and security scanning utilizing Nessus Vulnerability scanning.
* Handling SIEM events and response in critical environments (Email Threat Analysis, Web Threat Analysis, Malware Analysis, etc.).
* Analyze multiple network and host-based security appliance logs (Firewalls, NIDS, HIDS, Sys Logs, etc.) to determine and apply proper remediation actions and escalation paths for each incident.
* Actively monitored and responded to activity impacting various enterprise endpoints facilitating network communication and data handling (McAfee End Point Security, DLP, Splunk)