Name: Mounika

Email: daniel@trovetechs.com

Phone: 8033683556

 **Summary**

* **8 years** of professional IT Experience as **Security Engineer** in various domains like **Penetration testing, Web Application security testing, Vulnerability Assessment, code review and generating reports using tools.**
* Excellent knowledge in **OWASP Top 10, SIEM and THREAT CLASSIFICATION** methodologies.
* Experienced in vulnerability assessment of internet facing assets and internal assets using tools like **Burp Suite, IBM Appscan, Nessus, Live HTTP headers Metasploit, Wire shark, SQL map, OWASP ZAP Proxy, Acunetix, Nmap, and HP Fortify.**
* Updated risk assessments business to reflect regulatory and business changes, as well as the impact of audit, **compliance testing**, and regulatory exam results on risk assessments.
* Experience in **SQL Injection protection**, **XSS** protection, script injection and major hacking protection techniques.
* Good Knowledge on Network Protocols such as **TCP/IP, SNMP, SMTP, NTP, DNS, LDAP,** etc.,
* **Installing and configuring servers**, in accordance with standards and operational requirements including hardening of Operating Systems.
* Proficient in **configuring operating system** (**Kali Linux, Windows, Backtrack**) utilities and programming.
* Managed the cycle of project continuity, reviewed the technical work of the team, and ensured the quality of service deliverables.
* Worked on windows server administration activities.
* Excellent programming skills on **JavaScript, Python, XML and AJAX**.
* Experience in documenting the testing process using MS-Office tools including MS-Word, MS-Excel, and MS-Project.
* Experience in Identity Access Management (IAM) and SAML Federation features and components.
* Install and configure federated single sign-on (F-SSO), Web services security management, and federated provisioning services.
* **Risk assessment** on the application by identifying the issues and prioritizing the issues based on risk level.
* Worked in implementing best application security practices for **microservices** and **Restful API**. Ran application security scans on Microservices and Restful API using tools such as Acunetix.
* Monitor **SIEM** feeds to identify possible enterprise threats. Investigate threats to determine nature of incident
* Performed **Authenticated Penetration Testing** and OWASP web application testing for **authorization.** Implemented processes to have **access control** for various web applications.
* Providing remediation to the developers based on the issues identified.
* Experienced in implementing Firewalls and updating IDS/IPS signatures.
* Experience with Internet/Intranet Networking Protocols and Services.
* Managed inventory of network hardware and Monitoring by syslog, SNMP, NTP.
* Worked on different LAN &amp; WAN technologies and expertise in implementing L2 technologies including VLAN’s, VTP, STP, RSTP, and Trunking and Port Security.
* Excellent team player, enthusiastic initiator, and ability to learn the fundamental concepts effectively and efficiently.
* Worked on AWS Cloud security, such as data protection, Infrastructure Protection, Identity and Access Management and Threat Detection and Continuous Monitoring.
* Knowledge on Microsoft Azure Firewall and Physical, Infrastructure and operational Security, design and architecture. Worked tools such as Terraform.
* Implemented security control concepts and worked with teams to implement security concepts within design and architecture.
* Excellent communication, analytical, troubleshooting, customer service and problem-solving skills; excels in mission-critical environments requiring advanced decision-making

**Technical Skills**

Vulnerability Assessment Tools : Burp Suite, Dirbuster, OWASP ZAP Proxy, NMap, Nessus, IBM Appscan, Metasploit, Accunetix, HP Web Inspect, Fortify, SQL Map, Wire

 Shark, Acunetix, Net Sparker,Open VAS.

Languages : C,C++,C#,Java script,Python

Web Technologies : HTML , XML, AJAX, CSS.

Database : SQL Server, MySQL, Postgres

Operating System : Windows, Linux,, Kali Linux

**EDUCATION**:

* Bachelor’s in information technology from Sri Vidyanikethan, Tirupati.

**Professional Experience**

**Vonage, Holmdel, NJ**

**DevOps Security Engineer July 2019 – Present**

**Responsibilities:**

* Experience coordinating and performing vulnerability assessments using automated and manual tools (**Tenable, Trend Micro** etc.).
* Scanning the application servers using Tenable.sc and building scanners within the Tenable.
* Analyzing the Tenable scans results and Trend Micro scan results.
* Ability to review and **analyze vulnerability** data to identify security risks to the organization’s network, **infrastructure**, and **application** and determine any reported vulnerabilities that are false positives.
* Capability to prepare security vulnerability and **risk management** reports for management.
* Leadership and Teaming skills to coordinate **remediation of vulnerabilities** within established timeframes.
* Proficiency in C/C++ Programming and Bash, Python or other scripting languages.
* Familiarity with Information Security **frameworks/standards** (i.e. CIS, NIST, xRFC2196, etc.).
* Comprehension in the security areas of Key Management Systems, **Certificate Management**, Encryption, **Penetration Testing**, **Vulnerability Scanning**, Security and Monitoring tools, etc.
* Knowledge of Windows and Linux patch management and related information security functions **(authentication**, **encryption**, iptables, SSL, Ciphers, etc.)
* Working knowledge of industry best practices with regards to information security Ability to work with APIs and Plugins to integrate security tools into established **CI/CD pipelines.**
* Experience coordinating and performing vulnerability assessments using automated and manual tools (Tenable, NMAP, etc).
* Worked in security compliance audits for Residential and Enterprise line of business.

**Walgreens, Deerfield, Illinois**

**Application Security Engineer December 2018 -June 2019**

**Responsibilities:**

* Conducting **application** and **infrastructure** penetration tests, Security Consulting as well as physical security review and Social Engineering tests for our clients.
* Perform Penetration Testing in accordance with **OWASP standards and SANS 25** using manual techniques and Automated Tools.
* Application testing Using **Burp Suite Pro and Live HTTP Headers** for Web and Mobile applications to identify the vulnerabilities and to validate the Server-side validations.
* Using **NMap**, **OpenVAS**, **Security Center** and **NESSUS** for Network and Port Scanning for closure of unnecessary ports.
* Using **DirBuster** to brute-force directories and **Fierce** to scan and brute-force domains (DNS).
* Identified security issues on **DOM (Document Object Model)** based environments.
* Using **Metasploit** to exploit Proof of Concepts and **SQL** **Map** to dump the database data to the local folder.
* Responsible for security testing of web flows using **IBM AppScan** tool.
* Skilled using **Burp Suite, Acunetix Automatic Scanner, NMAP, Dirbuster, Qualysguard, Nessus, SQL Map** for web application penetration tests and infrastructure testing.
* 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.
* Conduct network Vulnerability Assessments using tools to evaluate attack vectors, Identify System Vulnerabilities and develop remediation plans and Security Procedures.
* Working knowledge in Simulators and Emulators, cross browser testing like Fire Fox, Google Chrome, Safari and Internet Explorer.
* Performing onsite & remote security consulting including penetration testing, application testing, web application security assessment, onsite internet security assessment, social engineering, wireless assessment, and IDS/IPS hardware deployment.
* Perform live packet data capture with **Wire shark** to examine security flaws.
* Utilize various Firefox add-ons like **Flag fox, Live HTTP Header**, Tamper data to perform the pen test.
* Revalidate the issues to ensure the closure of the vulnerabilities.

**Humana, Louisville, KY**

**Role: Information Security Analyst June 2017 - November 2018**

**Responsibilities:**

* Performed sophisticated penetration examinations for the purpose of ascertaining the technical weaknesses existing the web application systems.
* Perform compliance scanning to analyze configurations, facilitate implementation of configurations and hardening settings for web applications running or hosted on the networks, operating systems, applications, and other information system components.
* Well versed in understanding application level vulnerabilities like **SQL Injection, XSS, CSRF, authentication bypass, authentication flaws, cryptographic attacks** etc.
* Strong experience on assessing and mitigating **OWASP top 10** critical risks.
* Port scanned servers using **NMAP** and closed all unnecessary ports to reduce the attack surface.
* Identified, documented and communicated vulnerabilities to appropriate members of management team prioritizing remediation requirements and increasing focus on secure coding processes and configurations
* Experienced in **Black box, White box, responsive design, and exploratory testing, PKI Encryption algorithms**.
* Security assessment of online applications to identify the vulnerabilities in different categories like **Input and Data Validation, Authentication, Authorization, Auditing &amp; logging.**
* Performs tailored web-application penetration tests using advanced manual techniques
* Calculates vulnerability risk using **NIST CVSS** and existing mitigating control considerations.
* Security testing of APIs using SOAP UI.
* Performed on **Red team and Blue team** operations.
* Extensive knowledge of network and security technologies such as Firewalls, TCP/IP, LAN/WAN, IDS/IPS, Routing and Switching.
* In this role, I implemented and maintained security controls (**NIST SP 800-64/NIST SP 800-40 Rev.3**).
* Performed continuous monitoring on Information systems using **NIST SP 800-137**.
* Strong understanding on **DNS hijacking, DNS spoofing, content spoofing and wireless security** with hands-on Experience using **Kismet**.
* Conducted Web Application Vulnerability Assessment & **Threat Modeling, Gap Analysis, secure code reviews** on the applications
* Worked with technical management to create and implement best **DLP** policy by coordinating with McAfee by using McAfee Total Protection tool for DLP.
* Performed both defensive and adversarial perspective type of threat modelling of the applications for detection of various potential threats.
* Performed application security testing for **Restful API** infrastructure and **microservices** using **Acunetix**. Worked with technical management and implemented best security processes for both Microservices and Restful API.
* Worked with many teams to implement the design architecture of Azure and to explain, monitor and control security concepts.
* Worked with AWS Cloud Engineers in implementing AWS cloud security. Identified threats in the AWS cloud environment by using AWS Threat detection & continuous monitoring. In order to protect our data in AWS Cloud i have used AWS data protection services in which encryption key management and threat detection continuously monitors and protects your accounts and workloads. Filtered web requests based on IP addresses, HTTP headers, HTTP body, or URI strings, which allowed us to block common attack patterns, such as SQL injection or cross-site scripting to protect our Infrastructure. Used AWS tools such as Terraform.

**SHIP BY NIGHT IT SOLUTIONS, Hyderabad**

**Penetration Tester March 2015 - May 2016**

**Responsibilities:**

* Performed **vulnerability assessments, threat assessment, and mitigation and reporting activities** to safeguard information assets and ensure protection has been put in place on the systems.
* **Secured Code Review** of the applications using open source utilities identifying flaws in the coding practice and encouraging secured coding among the developer community.
* Drafted JavaScript with respect to the vulnerabilities like **XSS, CSRF** etc.
* Identified issues on sessions management, Input validations, output encoding, Logging, Exceptions, Cookie attributes, encryption, Privilege escalations
* Found common web site security issues (**CSRF, XSS, applications logic, SQL injection, information leakage, session fixatio**n etc.) across various platforms.
* Port scanning servers using **NMAP and Nessus**.
* Generated and presented reports on Security vulnerabilities to both internal and external customers using vulnerability tools.
* Preparation of risk registry for the various projects and coordination with the development team in Implementation of Security Needs**: Audits, planning, design, implementation, testing, and management**.
* Provided security implementation for authorization, by controls like principle of least privilege.
* Performing manual/automated application security testing on the major changes carried out in the application.
* Helped to research open-source intelligence feeds for current and emerging threat information
* Creation of secure virtualized lab for exploit creation, malware distribution analysis and security product testing
* Performed **Authenticated Penetration Testing** and **Authorization** web application testing **using tools such as ZAP.**
* Collaborated with fellow analysts to develop and streamline operational guidelines, to implement processes to have **access control** for various web applications and perform analytical support of security incident calls across the enterprise.

**World Bank, WA**

**Security Researcher March 2013 – February 2015**

**Responsibilities:**

* Participated in all technical aspects of LAN, WAN, VPN and security Internet Service projects including, short and long-term planning, implementation, project management and operations support as required.
* Training on pen tests on different applications a week.
* Preparation of security testing checklist to the company.
* Ensure all the controls are covered in the checklist.
* Good knowledge in Web technologies like HTTP, HTML, CSS, Forms, Database Connectivity.
* Updating the checklist on a weekly basis to ensure all the test cases are up to date as per the attacks happening in the market.
* Design and implement security policies on client network.
* Involved in a major merger activity of the company and provided insights in separation of different client data and securing PII.