Anusha Gorrepati

Senior Security Analyst
anusha208514@gmail.com
(719) 695-9493

PROFESSIONAL SUMMARY:

- Overall 6 years of progressive experience in Information Technology with extensive experience in Information Security, Application Security, Software Security, Enterprise Vulnerability Management, penetration testing and generating reports using tools.
- Strong experience of web application vulnerability assessments, penetration testing. Ability to conduct penetration testing for well-known technologies and known security flaw concepts SQL injection, XML injection, XSS, CSRF, IDOR, Path Traversal, authentication flaws, authentication bypass, cryptographic attacks etc.
- Experience in vulnerability assessment and penetration testing using various tools like Burp Suite, IBM AppScan, OWASP ZAPproxy, SQLmap, DirBuster, NMap, Nessus, Hp Fortify, Kali Linux, OpenVAS, Qualys and Metasploit.
- Good Knowledge on OWASP Top 10, CWE methodologies.
- Good knowledge in Web technologies like HTTP, HTTPS, HTML, CSS, Web application firewalls, checking logs, Forms, Database Connectivity.
- Vulnerability Assessment includes analysis of bug's domains by using both manual and Automation tools.
- Knowledge in Windows/Linux operating system configuration, utilities and programming.
- Having good Knowledge on Secure SDLC and Source Code Analysis (Manual & Tools) on WEB based Applications.
- Good knowledge on IBM Appscan to enhance the web application security and experience in risk assessments.
- Ability to exploit recognized vulnerabilities and reporting the identified issues in the industry standard framework.
- Good exposure on network penetration tests, ethical hacking and implemented vulnerability assessments.
- Evaluated operational effects of security system attacks.
- Proven experience in manual/automated security testing, secure code review of web and mobile applications.
- Good knowledge of network and security technologies such as Firewalls, TCP/IP, LAN/WAN, IDS/IPS, Routing and Switching.
- Good knowledge and Hands on SQL and programming skills in Java, Selenium Automation.
- Good team player and ability to learn the concepts effectively and efficiently.
- Ability to work in large and small teams as well as independently.

EDUCATION:

- Bachelors of Technology in Electrical and Electronics Engineering, JNT University, India.

TECHNICAL SKILLS:

Tools	IBM AppScan, BurpSuite, DirBuster, SQLmap, Kali Linux, OpenVAS, HPWeb Inspect, HP Fortify, OWASP ZAP
Network Tools	N-map, Tenable Nessus,Qualys

Language	C, C++, Java, .Net
Web Technologies	HTML, CSS, JavaScript
Platforms	Windows, Linux
Web Server	Apache, IIS 6.0/7.0
Database	MS SQL, Oracle, MySQL, Sql Server
Packages	MS-Office (Word, Excel, Pivot Tables), MS Visio

EMPLOYMENT

Client: Century Link, Denver, CO **2016 to Present**

Role: Security Analyst

Responsibilities:

- Performed Vulnerability Assessment of various web applications used in the organization using IBM AppScan, Burp Suite, HP Web Inspect, SQLmap, N-map.
- Implemented OWASP TOP TEN Vulnerabilities Assessment. Online application testing and CR regression testing, assessment and reporting.
- Capable of identifying flaws like SQL Injection, XSS, Insecure direct object reference, Security Misconfiguration, Sensitive data exposure, Functional level access control, CSRF, Invalidated redirects.
- Familiar with BurpSuite tool to identify the vulnerabilities manually.
- Executed Network Penetration vulnerability assessment on internal network to check out for the various vulnerabilities in the existing network and ensured to communicate the correct mitigation for the existing vulnerabilities to the client.
- Performed Dynamic Application Security Testing (DAST) using tools such as IBM AppScan, Burp Suit.
- Prepared comprehensive security report detailing identifications, risk description and recommendations for the Vulnerabilities.
- Coordinate with team members to provide guidance related to requirements.
- Provided comprehensive report on vulnerabilities and action plan to mitigate the identified vulnerabilities.
- Utilizing various logs, rules, and indicators of compromise to correlate events for the purposes of exploit prevention and incident response.
- Researching, identifying and implementing best security practices for all systems and service deployments.

Environment:

IBM App Scan, Burp Suite, SQL Map, Kali Linux, Metasploit, OWASP Top 10, and SANS Top 25, Nessus Security Center, Qualys Guard, HP WebInspect, IDS reports, CVSS Scores, Plan against Phishing Attacks, PKI enabled Applications, Network and Security.

Client: Kaiser Permanente, Denver, CO **2015 to 2016**

Role: Web Penetration Tester

Responsibilities:

- Performed Manual Penetration Testing and automation on web applications.
- Performed the manual code review to remove the False Positives.
- Performed Patch management related tasks and Vulnerability Assessment on various applications.
- Experience in different web application security testing tools like Burp Suite, SQLmap, and DirBuster.
- 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.
- Experienced in Dynamic Application Security Testing (DAST) & Static Application Security Testing (SAST).
- Performed Dynamic Application Security Testing (DAST) using tools such as HP WebInspect, HP Fortify.
- Security assessment based on OWASP framework and reporting the identified issues in the industry standard framework.
- Experience with tool such as Nessus vulnerability scanner. Generate reports and executing the daily tasks.
- Performed authenticated and unauthenticated vulnerability infrastructure scanning.
- Develop Vulnerability Assessment Report (VAR) to document findings and recommend remediation measures.
- Handled Baseline Configurations, vulnerability exceptions and Compliance exceptions.
- Security test planning and security test execution on Web platform projects.
- Scan Networks, Servers, and other resources to validate compliance and security issues using numerous tools.
- Assist developers in remediating issues with Security Assessments with respect to OSWASP standards.

Environment:
SQL Injection, XSS, Application Security, Dynamic Analysis, Manual Testing, vulnerability assessment

Client: CBay Systems Pvt Ltd **2010 to 2013**
Role: Security Engineer
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 HP WebInspect, IBM AppScan.
- 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.
- Scan Networks, Servers, and other resources to validate compliance and security issues using numerous tools.

- Assist developers in remediating issues with Security Assessments with respect to OSWASP standards.

Environment:

SQL Injection, XSS, Application Security review, Security Assessments, Manual Testing, OWASP Top 10