**INFORMATION SECURITY ANALYST**

**Anki Reddy**

**Ph: 402-431-2236**

**Email:** appsec44556@gmail.com

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

| **Summary :** |
| --- |

* Over **13** years of experience as an IT professional within Information Security.
* Involved in Software development Life cycle (SDLC) to ensure security controls are in place.
* Experience in Threat Modeling during Requirement gathering and Design phases.
* Experience on vulnerability assessment and penetration testing using various tools like Burp Suite, DirBuster, Nmap, Nessus, Kali Linux, Metasploit, Acunetix
* Experience with Security Risk Management with TCP-based networking.
* Experience with **TCP/IP, Firewalls, LAN/WAN**.
* Performed static code Assessment using Veracode and identified the false positives.
* Monitor, Analyze and respond to security incidents in the infrastructure. Investigate and resolve any security issues found in the infrastructure according to the security standards and procedures.
* Experience in Linux system administration.
* Performing rapid7 and Nessus Scans against Infrastructure like Web Servers, appservers and dB servers to identify the existing environmental vulnerabilities.
* Perform Vulnerability assessment on all the workstations in the organization to identify if they are patched and updated.
* Static Code Analysis during the development phase.
* Integrated Vera code with **SDLC** process to ensure every build is analyzed using static code analysis
* A Certified Ethical Hacker.
* A Pen tester with experience of penetration testing on various applications in different domains.
* Penetration testing based on **OWASP Top 10**.
* A good team player, Inquisitive, good in basic concepts and an excellent team player.
* Performed the gap analysis to identify scenarios like privilege escalation.
* Performed software Licensing audit.
* Interpreted least privilege for applications and segregation of duties.

| **Specialties:** |
| --- |

* Penetration testing, Vulnerability management & assessment
* Application security, Network security
* DAST, SAST and IAST

| **Certifications:** |
| --- |

* Ethical Hacking and Countermeasures (CEH) from EC-Council.

| **Core Qualifications:** |
| --- |

**Penetration Testing** : Backtrack, Kali Linux, Metasploit, Burp Suite, OWASP-Zap

**Application Security** : IBM AppScan, HP-Web inspect, Hp-fortify, checkmarx, Veracode, Acunetix, BlackDuck

**API testing**  : Postman, SoapUI

**Network Security** : Nessus, GFI Lan guard, Nexpose, Metasploit

**Standards** : OWASP, SANS, OSSTMM, SWAT Checklist, S-SDLC, Business Logics Vulnerabilities.

**Program Language** : Java, Java Script, Python, .Net

| **Organization and Role :** |
| --- |

**Client: Optum/UHG, Minneapolis, MN June 2023 to till date**

**Position: Senior Penetration tester**

**RESPONSIBILITIES:**

* We perform PCI every quarter in that we do network services and Web services.
* Good knowledge on web technologies like HTML, CSS, JavaScript to ensure the protection from XSS by reviewing the code.
* Worked on the DOM XSS by analyzing the JavaScript.
* For the network we use Nmap and Metasploit scripts. For the Web we use Metasploit scripts and work manually also.
* Alternatively we do nexus scan and infrastructure scan for both network and Web services.
* Experience in api testing tools like (e.g postman, SoapUI)
* In Depth knowledge on OWASP top 10 api vulnerabilities and mitigations.
* Conducting manual API and mobile pen test using burp suite.
* Proficient in understanding application-level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, weak cryptography, authentication flaws etc.
* Proficient in understanding application-level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, cryptographic attacks, authentication flaws etc
* Analyze data packets, review signatures, analyze and interpret PCAP using Wireshark
* Monitor the Security of Critical System (e.g., e-mail servers, database servers, Web Servers, Application Servers, etc.
* Conducted Vulnerability Assessment of networks using Qualys and Nessus.
* Perform vulnerability analysis utilizing Ethical Hacking tools, techniques and procedures.
* Initiate Incident Response procedures to mitigate and, or eliminate, known threats to the client's business operations.
* 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.

**Client: Best Buy, Minneapolis, MN Nov 2021 to May 2023**

**Position: Application Security Engineer**

**RESPONSIBILITIES:**

* We perform PCI every quarter in that we do network services and Web services.
* Perform security code reviews and provide remediation guidance in Java web applications and Microservices.
* Good knowledge on web technologies like HTML, CSS, JavaScript to ensure the protection from XSS by reviewing the code.
* Worked on the DOM XSS by analyzing the JavaScript.
* For the network we use Nmap and Metasploit scripts. For the Web we use Metasploit scripts and work manually also.
* Alternatively we do nexus scan and infrastructure scan for both network and Web services.
* Experience in api testing tools like (e.g postman, SoapUI)
* In Depth knowledge on OWASP top 10 api vulnerabilities and mitigations.
* Conducting manual API and mobile pen test using burp suite.
* Communicate with development staff for test planning and create weekly reports, develop test cases ensure code functionality and identify defects to implement strategy to enhance testing.
* Performed Static Application Security Testing Assessments for the Web Applications, Microservices and Mobile Applications using Checkmarx.
* Performed Application Security program (DAST and SAST) at the enterprise level to identify, report and remediate security vulnerabilities from applications deployed in DEV, PRE-PROD and PROD environments.
* Integration of IBM AppScan tool with Jenkins in agile development process for dynamic analysis security testing.
* Worked extensively with software development teams to review the source code, triage the security vulnerabilities generated by Checkmarx and eliminated false positives.
* Improving the Application Security Posture of the company's online business by performing periodic assessments on mission critical applications.
* Log defects in Jira and assign to the application team for the fixes and Work with application teams to help them remediate the security vulnerabilities.
* Perform risk analysis to identify points of vulnerability and recommend disaster recovery strategies and business continuity planning.
* Identifying and evaluating new marketing opportunities to increase the website traffic and online production.
* Proficient in understanding application-level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, cryptographic attacks, authentication flaws etc
* Analyze data packets, review signatures, analyze and interpret PCAP using Wireshark
* Monitor the Security of Critical System (e.g., e-mail servers, database servers, Web Servers, Application Servers, etc.
* Perform vulnerability analysis utilizing Ethical Hacking tools, techniques and procedures.
* Initiate Incident Response procedures to mitigate and, or eliminate, known threats to the client's business operations.
* 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.

**Client: TD Ameritrade/Charles Schwab, Omaha, NE June 2018 to Oct 2021**

**Position: Sr Application Security Engineer**

**RESPONSIBILITIES**

* Conduct application security assessments / penetration tests and implement tools for dynamic/automated code reviews
* Perform security code reviews and provide remediation guidance in Java web applications and Microservices.
* Perform software security design and/or code reviews.
* Assess the security risks associated with software applications.
* Work with application development groups to understand different types of vulnerabilities, attack vectors and remediation approaches for web, mobile applications and APIs.
* Educate employees on security related development best practices.
* Help application teams build applications which are secure by providing security requirements and security patterns, reusable code, etc
* Ensure application design and implementation best-practice with role-based and appropriate access standards, as well as integration with Identity and Access Management environments.
* Ensure compliance with society, regulatory, and industry standards for application security.
* Continuously evaluate the organization’s existing application security practices, define and measure security-related activities, and demonstrate concrete improvements to the application assurance program within the organization.
* Provide secure application development training to developers and provide guidance on the development of web-based training for ongoing awareness.
* Conduct code reviews and penetration testing
* Develop and maintain unit and integration tests designed to ensure security controls are tested on every Bidwell review results that come out of fortify and checkmarx tools, those tools scan the code of those apps.review the report and schedule meeting with developer discuss the issues we found in the application and open the jira tickets
* Experience partnering with development teams to balance innovation and security concerns analyzing large amounts of disparate data to produce easily understandable content Security reviews of web and mobile applications.
* Run scan and deal with output of scan, it points to source code of java or whatever language, understand reading that code, understand what it’s doing, how java handles encryption and authentication, and then we talk to developers and deal.
* Review result that comes from BlackDuck tool and create Jira tickets
* Create Jenkins jobs
* Determining the risk rating based on the Common Vulnerability Scoring System (CVSS).
* Manually testing the web application against the OWASP Top 10 vulnerabilities using BURP SUITE.
* Creating detailed reports for the developers and application owners to mitigate the issues found in the source code analysis and penetration tests.
* Tracking the fixes and closing tickets.

**Environment**: Hp Fortify, Checkmarx, JIRA, Burp Suite, Jenkins, Black Duck, White Hat

**Client: Coca-Cola, Atlanta GA Sep 2016 to May 2018**

**Position: Application Security Analyst**

**RESPONSIBILITIES**

* Ensured all the controls are covered in the checklist Performed Vulnerability Assessment of various web applications used in the organization using Paros Proxy, Burp Suite, and Web Scarab, IBM AppScan.
* Implemented **OWASP TOP TEN 2010 Vulnerabilities Assessment**. Online application testing and CR regression testing, assessment and reporting.
* Detected and prioritize vulnerability exposures and coordinating with the team for complete closure.
* Static and dynamic scanning of various applications using Fortify and IBM Appscan, Identify false positives and report.
* Used tools like NMAP, Nessus, google dorks, Flagfox, DirBuster, and LiveHTTP Header to gather more information about the application and perform security assessment.
* Conducted host based security by using kali Linux to identify different ports and services running and identifying vulnerabilities by using NMAP script engine.
* Exploited the systems with vulnerabilities using Metasploit framework.
* Analyzed the application for vulnerabilities in categories like Input and data validation, Authentication, Authorization, Configuration Management.
* Performed security assessment by creating test scenarios and test cases against the categories like Sensitive data, Session management, Cryptography, Exception management, Auditing and logging.
* Created documentation for the vulnerabilities identified and reported it to the application development team. Ensuring timely delivery of issues reported and remediation.
* Followed DREAD approach to provide the risk rating to the vulnerabilities identified. Preparing report with executive summary, technical details and the remediation
* Performed Web Service Testing using SOAP UI to analyze the vulnerabilities.
* Conducted Web Application User ID access reconciliation and audit of the privileged Database and application user IDS on quarterly basis.
* Understanding new security technologies for potential utilization in the application security testing.
* Audited the project for SOX Compliance by collecting & reviewing the evidence. Making sure all the NCs are closed before the next quarter Audit.
* Performed User Access Management and Identity Management for the various client applications through automatic disablement of dormant users and audit on monthly basis
* Implemented Gap Analysis of present Risk assessment methodology and conducting risk assessment and mitigation steps for the client.
* Identified latest threats and vulnerabilities and conducted the impact analysis to improve the risk level by continuous risk assessment.
* Prepared RMR [Risk Management Report] on account level. Risk assessment done for the account of 8 different projects. Provision of remediation to minimize risk and follow up to ensure proper implementation as per the control objective.
* Implemented the Software Security Assurance framework in the whole project by conducting Sessions like Secure Programming practices to all the developers. Involving in the complete Agile as a security consultant. Trained modules like Secure design requirements, threat modeling, secure coding practices, penetration testing.
* Using snap tool for create ticket and Hp Qc for defect logging and tracking

**Environment**: Windows, Kali Linux, Nessus, Nmap, Metasploit, IBM AppScan, Hp Fortify, SNAP, HP QC, Burp suite, AWS

**Client: CISCO, San Jose, CA Oct 2015 to March 2016**

**Position: Security Engineer**

**RESPONSIBILITIES:**

* Black box pen testing on internet and intranet facing applications
* OWASP Top 10 Issues identifications like SQLi, CSRF, XSS
* Preparation of risk registry for the various projects in the client
* Training the development team on the secure coding practices
* Providing details of the issues identified and the remediation plan to the stakeholders
* Gray Box testing of the applications.
* Identified hidden files using Dirbuster.
* Worked on DOM based XSS manually.
* Worked on Directory Traversal attacks manually
* Implemented Agile Methodology to follow the workflow process.
* Worked on Middleware technologies to ensure the application safety (TOMCAT).
* Verified the existing controls for least privilege, separation of duties and job rotation.
* Identification of different vulnerabilities of applications by using proxies like Burpsuite to validate the server side validations
* Collaborating on cross-team and cross product technical issues with a variety of resources including development to document software defects and customer suggestions.
* Worked on billion laugh attacks manually by intercepting Burpsuite.
* Functional level access control is performed to avoid the privilege of misusing the sensitive data.
* Had worked on an Acunetix tool for quick assessment of vulnerabilities.
* Participate in documentation and product review process for new product introductions.
* Contributing to the knowledge base by authoring and editing articles to share current information with team members.
* Worked on fimap to check the possibility of vulnerabilities.
* Worked on DOS and Firewall intrusion to ensure the security of leakage of code.
* Performed API testing using Soap UI
* Attended meetings on WebEx with a team of Vice presidents and made valuable contributions.
* Execute and craft different payloads to attack the system to execute XSS and different attacks
* Identified issues on sessions management, Input validations, output encoding, Logging, Exceptions, Cookie attributes, Encryption, Privilege escalations.
* Provided and validated the controls on logging like Authentication logging, profile modification logging, logging details, log retention duration, log location, synchronizing time source, HTTP logging.

**Environment**: Burp suite, Nexpose, HTTP headers, Acunetix, fimap, DirBuster.

**Client: ICICI Bank, India Oct 2012 to Sep 2015**

**Position: Penetration Tester**

**RESPONSIBILITIES:**

* Perform application and infrastructure penetration tests along with physical security reviews.
* Define requirements for information security solutions and perform reviews of application designs and source code.
* Design, develop and implement penetration tools and tests and also use existing ones to handle penetration testing activities.
* Document and discuss security findings with information technology teams.
* Work on improvements for security services and provide feedback and verification about existing security issues.
* Perform attack simulations on company systems and web applications to determine and exploit security flaws
* Monthly Reviews carried out over the Vulnerability Assessments and Penetration testing.
* Raising issues against any High severity vulnerabilities in the Scan reports.
* Ensured compliance with legal and regulatory requirements.
* Exhibited client facing skills and capability to articulate technical concepts to a variety of technical and non-technical audiences.
* Assisted in review of business solution architectures from security point of view which helped avoiding security related issues/threats at the early stage of project.
* Strong Network Communications, Systems & Application Security (software) background looking forward to implementing, creating, managing and maintaining information security frameworks for large scale challenging environments.
* Performing security analysis and identifying possible vulnerabilities in the key derivation function, create Vulnerability Assessment report detailing exposures that were identified, rate the severity of the system & suggestions to mitigate any exposures & testing known vulnerabilities.

**Environment**: Nmap, Nessus, Burpsuite, Sqlmap, Dirbuster, KaliLinux, Metasploit

**Client: Picom Technologies Pvt ltd, India Jun 2010– Sep 2012**

**Position: Security Analyst.**

**RESPONSIBILITIES:**

* Perform threat modeling of the applications to identify the threats.
* Identify issues in the web applications in various categories like Cryptography, Exception Management.
* Risk assessment on the application by identifying the issues and prioritizing the issues based on risk level.
* In the team, the main focus of work was to audit the application prior to moving to production.
* Explanation of the security requirements to the design team in initial stages of SDLC to minimize the efforts to rework on issues identified during penetration tests.
* Analyzed the XML and HTTP requests to find the vulnerabilities.
* Performed Vulnerability assessments and preventions on the development side by leveraging the tools like Nmap, Nessus, IBM app scan
* Providing remediation to the developers based on the issues identified.
* Worked on the DOM XSS by analyzing the JavaScript.
* Good knowledge on web technologies like HTML, CSS, JavaScript to ensure the protection from XSS by reviewing the code.
* Worked on Ng-directives in angular.js for vulnerability assessments.
* Ensured to draft the script manually based on vulnerability.
* Revalidate the issues to ensure the closure of the vulnerabilities.
* Verify if the application has implemented the basic security mechanisms like Job rotation, Privilege escalations, Lease Privilege and Defense in depth.
* Using various add-ons in Mozilla to assess the application like Wappalyzer, Flagfox, Live HTTP Header, Tamper data.

**Environment**: Wappalyzer, Flagfox, Nexpose, Live HTTP header, Burpsuite, Nmap

| **Academic Details:** |
| --- |

* Bachelor of Technology in Information Technology.
* Master’s in computer science.