|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Amit A** **Fort Lauderdale, FL** [**Pardeep@vlinkinfo.com**](mailto:Pardeep@vlinkinfo.com)**(203)552-2554**  |  | | --- | | **Area OfExpertise**  * Static ApplicationSecurity Testing (SAST) * Dynamic Application Security Testing (DAST) * Secure code review * Penetration testing * Mobile Security * API and Cloud Security * DevSecOps * Risk Assessment * Patch Management * Security Testing & Evaluation * Vulnerability Management * Conducting Security Trainings | | **Tools**  HP Fortify, AppScan, CheckMarx VeracodeOWASP Zap Proxy,BurpSuite, Zen map, Mac Nikto, Qualys, Rapid 7, Wireshark,Tenable Nessus, Mobile SF, Soups, ReadyAPI and Firefox Add-ons such as SQL Inject Me, XSS Me, Web Developer add-on, REST Client. | | **Certification**  * Certified Ethical Hacker (C|EH) * Certified Information Systems Auditor (CISA) * AppScan Certified * Microsoft Azure Administrator AZ 104 | | **Clients& Industries**   * 10+ Public Sector States and Local clients * Insurance companies * Major Telecom clients * Retail * Communication * Product * Media & entertainments * Apple Inc * Blue shield California * Major Banking | | **Education**  * Master of Science (MS) in Software Systems from BITS Palani India. * Bachelor of Engineering in Information Technology from India | | **Location** Fort Lauderdale Florida, USA | | |  | | --- | | **Summary** I am an accomplished **Security Specialist** at Fannie Mae, boasting over **14 years of expertise inboth IT and Application cybersecurity domains**. My professional focus revolves around various facets of cyber security, including application, system, mobile, API, cloud, and risk management. Throughout my career, I have partnered with esteemed government agencies and Fortune 500 companies, providing them with top-notch security solutions.  I hold a bachelor's degree in computer science from a prestigious university in northern India, as well as a master's degree in computer science from BITS Palani, India. Among the cutting-edge areas in Cyber Security, I have extensive hands-on experience in Vulnerability Assessment, Secure Code Analysis, Mobile Security Testing, and DevSecOps. These domains have enabled me to stay at the forefront of cybersecurity best practices and contribute significantly to the safeguarding of critical systems and data for my clients. | | **Security Specialist –Fannie Mae Inc. - Nov 2023 – Until Now**   * Working with Fannie Mae in Risk assessment project * Assess and synthesize multiple audit results and corresponding remedial measures undertaken. * Provide recommendations for further actions aimed at enhancing compliance maturity.   **Specialist Senior - Deloitte & Touché LLP - July 2015 to July 2023**  **Application Security:**   * Led the implementation and administration of security measures for applications and systems. * Developed and maintained security standards and guidelines for secure software development. * Experience with Threat Modeling and Secure Design reviews * Conducted application security assessments using DAST, SAST, SCA, IaC, IAST, RASP and Container scanning tools. * Triaged scan results and reviewed application source code to confirm findings and eliminate false positives. * Proficient in utilizing a wide range of programming languages, including Java, C/C++, Python, JavaScript, PHP, Ruby on rail, NodeJS, .NET, and more. Experience in leveraging SAST tools to perform comprehensive security assessments across diverse codebases, ensuring robust application security across various technologies. * Collaborated with development teams to integrate application security into the CI/CD process. * Stayed up-to-date on industry trends and threats, implementing appropriate measures for asset protection. * Responded to security incidents and led investigations to determine root cause and implement remediation measures. * Experience with securing enterprise web applications and OWASP Top 10, CVSS, CWE, WASC, and SANS-25 * Provided training and guidance to development teams on secure coding practices and threat mitigation. * Mentored and provided directions to junior members of the team. * Perform threat modeling, conduct security architecture reviews, and provide training to architects and developers to enhance adoption of secure coding practice within the product development lifecycle. * Experience with CI/CD pipeline tools such as GitLab, Jenkins, or Azure DevOps * Knowledge of federal compliance standards, including NIST 800-53, FIPS, or FedRAMP   **Application Security Tools used:**   * SAST: Fortify, Appscan, Checkmarx, SonarQube, Veracode, Coverity * DAST: Burp Suite, OWASP ZAP, Acunetix, Web Inspect, Wireshark, Firefox plugins, Kali Linux * SCA: Black Duck, WhiteSource, Snyk * IaC Security: Terraform Security Scanning, AWS CloudFormation Guardrails, Checkov * Container Security: Docker Security Scan, Clair, Anchore * CI/CD pipeline tools : GitLab, Jenkins, or Azure DevOps   **Vulnerability Assessment and Penetration Testing (VAPT):**   * Proficient in performing Vulnerability Assessment and Penetration Testing (VAPT) to assess the security of applications, systems, and networks. * Comprehensive knowledge of security testing methodologies, tools, and frameworks to identify and exploit vulnerabilities effectively. * Ability to simulate real-world attack scenarios and use ethical hacking techniques to uncover weaknesses and improve cybersecurity defenses. * Strong understanding of common security vulnerabilities, attack vectors, and exploitation techniques.   **VAPT Tools used:**   * Vulnerability Assessment Tools: Nessus, OpenVAS, Nexpose, QualysGuard, etc. * Penetration Testing Tools: Metasploit, Burp Suite, OWASP ZAP, Nmap, Wireshark, etc. * Web Application Scanning: Acunetix, WebInspect, Netsparker, etc. * Network Scanning Tools: Nmap, Wireshark, etc. * Exploitation Frameworks: Metasploit, BeEF, etc.   **API Security Testing:**   * In-depth understanding of API security principles and best practices, including authentication, authorization, encryption, and input validation. * Proficient in identifying and mitigating common API security vulnerabilities, such as SQL injection, XML external entity (XXE) attacks, and cross-site request forgery (CSRF). * Experience in implementing secure API design patterns, such as OAuth, JWT, and API keys. * Strong knowledge of API security standards, including OAuth 2.0, OpenID Connect, and TLS. * Ability to conduct API security assessments and threat modeling to identify potential risks and weaknesses.   **API Security Tools used:**   * OWASP API Security Top 10 tools, Postman, SoapUI, etc. * Apigee, Kong, Amazon API Gateway, etc.   **Mobile Security Testing Tools:**   * Comprehensive knowledge of mobile security principles and best practices for both Android and iOS platforms. * Proficient in identifying and mitigating common mobile security vulnerabilities, including insecure data storage, weak authentication, and insecure communication. * Experience in conducting mobile security assessments, penetration testing, and code reviews to identify security flaws in mobile applications. * Strong understanding of mobile application security standards, guidelines, and industry frameworks. * Ability to analyze mobile application binaries to detect and address potential security risks. * Familiarity with secure mobile development practices and the ability to guide developers in writing secure code. * Knowledge of mobile device management (MDM) and mobile application management (MAM) solutions to enforce security policies on mobile devices.   **Mobile Security Testing Tools:**   * Mobile security testing tools: AppScan Mobile Analyzer, MobSF, AndroBugs, iNalyzer, Frida, etc. * Mobile application scanning tools: MaaS360, AirWatch, MobileIron, etc.   **DevSecOps Security Testing:**   * Proficient in integrating security testing into the DevSecOps pipeline to identify and address security vulnerabilities throughout the software development life cycle. * Extensive knowledge of DevSecOps principles and best practices, emphasizing the seamless integration of security into the CI/CD process. * Experience in automating security testing, including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Software Composition Analysis (SCA), and Container Security Scanning. * Ability to conduct security code reviews and work closely with development teams to remediate identified vulnerabilities. * Strong understanding of security testing methodologies, frameworks, and industry standards. * Familiarity with security testing tools and techniques for web applications, APIs, mobile applications, and cloud environments. * Knowledge of infrastructure as code (IaC) security testing to ensure the security of infrastructure configurations. * Moderate exposure to SIEM tools like QRadar and Splunk   **DevSecOps Security Testing Tools used:**   * Fortify, Checkmarx, SonarQube, Veracode (for SAST); Burp Suite, OWASP ZAP, Acunetix (for DAST); Black Duck, WhiteSource, Snyk (for SCA); Docker Security Scan, Clair, Anchore (for container security scanning); etc. * OWASP Amass for reconnaissance, Nmap for network scanning, etc.   **Risk Assessment Skills:**   * Assist the Program Managers and the (ISSM) in the development and maintenance of System Security Plans (SSP) and associated artifacts such as the Plan of Action & Milestones (POA&M), Risk Assessment Report, and Continuous Monitoring Strategy. * Strong understanding of risk management methodologies and frameworks, including ISO 31000, NIST SP 800-30, HIPAA and FAIR (Factor Analysis of Information Risk). * Ability to assess risks based on their likelihood, impact, and potential consequences to prioritize mitigation efforts effectively. * Experience in developing risk assessment reports, highlighting key findings and recommendations for risk treatment. * Familiarity with industry-specific risk assessments, such as IT risk assessments, cybersecurity risk assessments, and business impact assessments. * Conducted thorough analysis and assessment of the organization's network to identify vulnerabilities and design effective micro-segmentation policies using Illumio. * Collaborated with cross-functional teams to integrate Illumio's capabilities into incident detection and response processes, improving incident response times and reducing potential damage from cyber threats. * Configured and managed Illumio policies to ensure compliance with industry standards and internal security requirements, enhancing overall regulatory adherence. * Conducted regular training sessions for cybersecurity teams to educate them on effectively utilizing Illumio for mitigating cybersecurity risks and responding to incidents. * Strong analytical and critical thinking skills to assess complex risks and develop appropriate risk mitigation strategies. * Effective communication and presentation skills to convey risk assessment results to stakeholders and management.   **Risk Assessment Tools used:**   * RiskLens, RiskyProject, OpenFAIR,Illumio etc. * GRC (Governance, Risk, and Compliance) software RSA Archer, ServiceNow GRC, etc.   **Client Details:**  **State of Indiana –July 2015 to Jan 2020**   * Played a key role in supporting Program Managers and the Information Systems Security Manager (ISSM) in crafting and maintaining comprehensive System Security Plans (SSP). These plans were designed to meet client-specific needs and ensure robust cybersecurity measures. * Utilized a strong understanding of renowned risk management methodologies and frameworks such as ISO 31000, NIST SP 800-30, HIPAA, and FAIR to bolster clients' security postures. * Effectively assessed risks based on their likelihood, potential impact, and consequences, aligning efforts to prioritize risk mitigation strategies that best served our clients' interests. * Developed insightful risk assessment reports, encapsulating crucial findings and offering actionable recommendations for risk treatment, ensuring our clients were well-informed and prepared for potential security challenges. * Demonstrated expertise in industry-specific risk assessments, such as IT risk assessments, cybersecurity risk assessments, and business impact assessments, tailoring our approach to address the unique risks our clients face in their respective domains. * Leveraged strong analytical and critical thinking skills to thoroughly evaluate complex risks, enabling the creation of appropriate, client-centric risk mitigation strategies. * Effectively communicated risk assessment results to stakeholders and management, employing clear and concise language to ensure our clients had a comprehensive understanding of their security landscape and potential vulnerabilities.   **State of Florida Feb 2020- Jan 2022**   * Drove security enhancement efforts by performing thorough Risk Assessments and GAP Analyses utilizing the Archer tool, ensuring our clients' systems and networks were tailored to their unique security needs and risk tolerance. * Applied HP Fortify for Secure Code Analysis, meticulously examining the codebase to fortify applications against vulnerabilities, thereby bolstering our clients' software security and reducing potential risks. * Leveraged IBM AppScan and manual testing for Vulnerability Assessment, tailoring the approach to align with our clients' specific environments, providing a comprehensive understanding of potential vulnerabilities and risks. * Conducted Penetration Testing using a suite of manual tools like OWASP ZapProxy, BurpSuite, Zenmap, Mac Nikto, Firefox Add-ons, and Nessus, ensuring a personalized approach to identifying vulnerabilities in our clients' applications and networks. * Enabled our clients to achieve heightened security by performing thorough Vulnerability Assessment and Penetration Testing (VAPT) on applications, systems, and networks, providing them with a tailored security assurance strategy.   **New York Life Insurance Feb 2022 – July 2023**   * Skillfully integrated security testing into the DevSecOps pipeline, ensuring early detection and swift resolution of security vulnerabilities for our clients. This proactive approach enhanced the security of their software throughout the development life cycle. * Applied extensive knowledge of DevSecOps principles and best practices, emphasizing the seamless integration of security into the Continuous Integration/Continuous Deployment (CI/CD) process. This approach was tailored to prioritize our clients' security requirements. * Automated security testing processes, encompassing Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Software Composition Analysis (SCA), and Container Security Scanning. This automation ensured swift identification and resolution of security issues, promoting a secure software environment for our clients. * Conducted meticulous security code reviews and collaborated closely with development teams to remediate identified vulnerabilities promptly. By aligning with our clients' objectives, we ensured the delivery of secure and robust software solutions.   **Security Consultant – Agreeya Solutions – Verizon Wireless**  **Nov 2014-July 2015 – 9 months**   * Secure Code Analysis is performed using HP Fortify. * Vulnerability Assessment performed using IBM AppScan and   manual testing.   * Penetration Testing is performed manually using tools like   OWASP ZapProxy, BurpSuite, Zenmap, Mac Nikto, Firefox  Add-ons, and Nessus.  **Security Consultant – Infosys Ltd: June 2012- Nov 2014 – 2 years**   * Secure Code Analysis is performed using HP Fortify and IBM Appscan for various clients. * Penetration Testing is performed manually using tools like   OWASP Zap Proxy, Burp Suite, Zen map, Mac Nikto,  Firefox Add-ons, and Nessus.   * Automated Penetration testing was performed using HP’s   Web Inspect tool.   * Vulnerability Assessment performed using IBM AppScan and   manual testing  **Team Lead – Tata Consultancy Services: September 2010 – June 2012 – 2 years**   * Functional regression testing, maintenance and development and the testing for client internal tool * Scheduling, understanding of the system, software development, and unit testing are the main responsibilities. * Technologies and Tools: Linux, Java Struts 1.2, JSP 2.0, JDBC, HTML, CSS, JavaScript, PostgreSQL 8.1, and Servlets.   **Software Developer – DiviNet Access Technology Ltd.**  **Pune: September 2007 – September 2010 – 3 Years**   * As a developer I was involved in analysis, design and development, Implementation, testing and Maintenance of Client /Server applications. * Experience with coding, debugging, and maintenance of production systems. * Technology and Tools: C/C++, Linux, Java Struts 1.2, JSP 2.0, JDBC, Servlets, JavaScript, PostgreSQL 8.1, HTML, CSS | |