PRANEETHA KANTU Mobile: 571-306-0499
Email: praneetha.kantu@gmail.com

Professional Summary

Client focused application security engineer seeking to improve the organization's security posture through effective risk & vulnerability assessments, vendor management & organizational leadership. Conceptualize and execute program vision from start to finish, managing complex milestones while adapting to changes and shifting priorities. Persuasive and articulate; communicates effectively with technology & business stakeholders to protect against reputational and/or financial harm.

Education & Certifications

- CISSP - ISC2
- CEH - Certified Ethical Hacker, EC Council
- Security+ - CompTIA
- Master's degree in computer science from Northwestern Polytechnic University (California)

Security Technology skills

- **Security Assessments**: Internal and 3rd party risk assessments (Blackbox/Greybox /Whitebox testing) on web applications, web services and mobile apps.
- **Methodology**: OWASP, OSSTMM, WASC-TC, SANS 25
- **Standards**: PCI-DSS, ISO 27000, HIPAA
- **Engagements:** Architecture reviews & Threat modelling (STRIDE Methodology), Dynamic testing, Code reviews, Cloud (AWS) infrastructure review.
- **Types**: DAST, SAST & IAST
- **Tools:** Burp, ZAP, Netsparker, Appscan, Nmap, Webinspect, Wireshark, Acunetix, Checkmarx, Fortify, IDAPro, Whitehat, SD elements, Sqlmap, Nessus, Metasploit, openssl, sslyze, Aws Cli
- **Languages & Scripting:** C, Java, .Net, HTML, XML, SQL, Python, JavaScript

Work Experience

System Soft Technologies
(FINRA, Reston) - Application Security Engineer August 2018 - Till Date

- Perform vulnerability assessments and penetration testing on Finra and CAT web applications that includes a wide scope coverage of activities such as Code analysis (Java, .net and Python), Cloud (AWS) configuration hardening guidelines, review network and firewall groups ,encryption standards implemented, triage the scan results using Black duck & OWASP Dependency checker.
- Build excellent relationships with application development teams and their managers.
- Manage and design the issue management around web application vulnerabilities, their tracking, reporting, metrics, resolution and validation.
- Introduce and manage both Vulnerability disclosure and Bug Bounty programs through vendor managed platform.
- Perform Threat modelling and identify testcases and promote, implement security test case automation with proxy and development team test automation suite (cypress, protractor and selenium)

- Develop, maintain and promote baseline security testing framework into part of development team’s regression testing.
- Evaluated IAST vendors and DAST tools and coordinate, schedule and support the weekly release management activities related to SAST and Antivirus tool releases.
- Document and manage application security assessment policy, procedures, tests and guidelines.
- Train developers (Java, .net and python) on relevant applications and aws cloud security controls using secure code warrior platform.

System Soft Technologies
(VISA, Ashburn) - Information Security Analyst April 2017 - August 2018

- Lead the application security efforts to enroll and assess of over 300+ Visa’s public facing web application into web application vulnerability management program.
- Bolstered in identifying all the in-scope applications attack surface of the organization.
- Play a key role (RISKIQ) in discovering the misused assets such as organization’s subdomain takeover, employee personal sites, sites with improper DNS entries, malware, expired SSL certs.
- Identify and track issues on the sites flagged as GDPR non-compliant until its resolved.
- Serve as application security expert, providing technical support to the development teams and external vendors.
- Initiate and lead the effort to have all Visa’s public facing API into web application vulnerability management program.
- Assist with identifying RiskIQ’s key performance indicators & manage Bug bounty program.
- Designed and implemented automation workflow prototype for security vulnerabilities using Python, Jira, White hat Sentinel & Archer thereby help manage the security findings efficiently.

System Soft Technologies
(FINRA, Maryland) - Application Security Engineer Oct 2013 - March 2017

- Performs Web application penetration testing on the organization application's as well as COTS applications.
- Aided and familiarized the external auditors helping them understand the organization’s approach towards vulnerability assessment and penetration testing, providing needed documents, reports and explain about the fix implemented for the issues identified.
- To triage the web vulnerability reports (Vendor Third party penetration testing reports), questionnaires based on ISO-27000, PCI compliance documents and the Data Centre documents of the vendor applications.
- Examine and identify excessive firewall (expired) rules communicating from lower environments to Production environment and review database patch.
- Inspect the findings from code scan to gain granularity for the actual finding’s vs false positives.
- Fine-tuned appscan policies based on the application platform in order to reduce the time consumption during the scan.
- To identify any PCI data being logged using SPLUNK query tool.
- Working on reconnaissance of external attacks via WAF to provide the detailed report to the respective team as needed.

System Soft Technologies
(AEP, Ohio) – Application Security Engineer Nov 2012- Oct 2013

- Perform Threat modeling, source code review and Penetration Testing (dynamic & manual) on web and mobile web applications as well various SOAP and REST based web services & prepare the Risk Assessment report based on the organization's defined metrics.
- Vulnerability Assessment on vendor-based Web Start (JNLP FILES) applications.
- Involved in build server configuration for IBM Appscan source scanner.
- Evaluated various vendor security training programs to educate IT Security and Development teams aligned on building security into the SDLC.

System Soft Technologies - Security Engineer Aug 2011 – Nov 2012

- Involved and enforced security measures in Design and Development of Employee Portal.
- Performed pen testing & code reviews for rest services, web application, Android and IOS apps.
- Involvement in development of various functionalities for Customer Information tracking system such as implementing data encryption to store and retrieve sensitive data (using C# libraries).

System Soft Technologies
AppLabs Technologies (India) - Software Engineer Oct 2009 - March 2011

- Security Audit and pen testing on 4 modules of an Israel based Application Service Provider providing real-time sales & customer services for organizations doing business on internet.
- Web Application Penetration Testing on leading UK based online school web application and gaming applications.
- Performed Non-intrusive tests on AppLabs Internal Network.

System Soft Technologies
AppLabs Technologies (India) - Associate Software Engineer March 2007 - Jan 2008

- VAPT on AppLabs intranet and other internal portals.
- Both Web Application Penetration Testing and Network Security Assessment on a non-banking finance company & is world's fastest growing micro finance as well multinational Bank in USA.

System Soft Technologies
AppLabs Technologies (India) - Internship May 2006 - Feb 2007

- Security Audit and Penetration Testing of American clinical research website that provides patient recruitment solutions for the bio-pharmaceutical industry.
- Web Application Penetration Testing and Network Security Assessment of an American Reinsurance Provider Website.

Note: - Client names are not mentioned due to Non-Disclosure Agreement with clients. The above details are only indicative & not comprehensive. Specific client details have not been mentioned to maintain high confidentiality.