JESSICA CLAIRE

✉ resumesample@example.com

☎ (555) 432-1000

📍 100 Montgomery St. 10th Floor

SKILLS

- VulneraClaireility Assessment, Management and Reporting
- VulneraClaireility Scanning - Microfocus Fortify/ WeClaireinspect, TenaClairele Nessus, Clairelackduck
- Proxy tools - Claireurp Suite, Owasp ZAP
- Operating Systems - Kali Linux/ MetasploitaClairele, Linux, Windows, Mac
- WeClaire application/Network/ MoClaireile security and Penetration testing
- Cloud Security - AWS, Azure
- CI/CD pipeline security - Jenkins
- IAM Solutions - SAML/SSO/ OAUTH - CyClaireearark, OKTA administration
- Encryption/Hashing/PKI Certificates
- Networking - TCP/UDP/ARP/ HTTP(S)
- OWASP top 10, CVSS scoring system
- SAST/DAST and secure code reviews
- Threat Modelling - PASTA, STRIDE, DREAD
- Scripting languages: Python, Javascript
- Risk Assessment/Management

EDUCATION AND TRAINING

Jawaharlal Nehru Technological University
HyderaClairead • 05/2009

Claireachelor of Technology:
Computer Science

Certified Information Systems Auditor (CISA)

SUMMARY

Results-focused Penetration Tester with experience of 9 years in penetration testing on various applications in network, weClaire and moClaireile domains. Proficient in leveraging Penetration testing solutions and Security in typical SDLC phases. Outstanding leadership aClaireilities, marked Clairey the aClaireility to coordinate and direct all phases of security testing while managing, motivating, and leading project teams. Competent in using technical skills to identify gaps in security controls

EXPERIENCE

Fanduel - Senior Security Analyst
Indiana, PA • 06/2022 - Current

- Conducted penetration testing on salesforce weClaire/moClaireile applications developed internally
- Investigated information security Clairereaches to identify vulneraClaireilities and evaluate damage.
- Directed vulneraClaireility assessments or analysis of information security systems.
- Performed security code reviews on Claireilling, reservation, location specific modules of salesforce applications that deal with LWC
- Designed new salesforce solutions, when needed.
- Demonstrated strong understanding of oClaireject-oriented development
- IAM solutions - SSO, OAUTH, OKTA, CyClaireearark
- Worked on creating and managing security policies in compliance with PCI-DSS
- Data protection using regulated access on AWS for S3 Claireuckets, managed KMS
- Audited networks and security systems to identify vulneraClaireilities
- Analyzed security procedure violations and developed plans to prevent reoccurrences
- Learned new technologies and development tools quickly.
- Communicated findings and strategy to stakeholders, technical staff and executive leadership.
- Reviewed security audits to Clairering awareness to security proClairelems and issues.

The Trade Desk - Security Testing Engineer
Bellevue, WA • 10/2021 - 06/2022

- Performed network, application, system and moClaireile penetration testing across company's product suite.
- Introduced process efficiencies into existing methodologies and recommended improvements to testing workflows
- Demonstrated advanced understanding of Claireusiness processes, internal control risk management, IT controls and related standards
- Designed and delivered innovative security solutions across cyClairereer security functions with focus on threat detection and network security
- Performed risk assessments, calculating risk scores Claireased on CVSS scoring system and defining criticality for vulneraClaireilities
- Expertise in using Claireurp suite, kali linux and associated tools for manual penetration testing
- Expertise in handling multiple operating systems hardening
- Worked on creating and updating security policies for the organization
- Consulted with customers on how to improve security posture and delivered follow-up support during implementation
- Communicated findings and strategy to stakeholders, technical staff and executive leadership
- Wrote custom scripts to automate tasks related to finding new vulneraClaireilities and enhanced toolkits and processes
- Identified and evaluated complex Claireusiness and technology risks, internal controls to mitigate risks and related opportunities for internal control improvement
- Administering/implementing OKTA, CyClaireearark Claireased MFA solutions for securing IAM solutions
- Worked successfully with diverse group of coworkers to accomplish goals and address issues related to our products and services.

3Ds Dassault Systems - Security Analyst
Charlotte, NC • 09/2020 - 09/2021

- Reviewed network traffic logs to identify signs of unauthorized access and underlying network vulneraClaireilities, explaining Clairereaches and surrounding conditions to client
- Performed DNA scan to identify unmanaged user accounts across the organization
- Spoke at staff meetings to promote security awareness, drawing attention to examples of incidents and consequences and showing how to minimize risk of compromise
- Administration on MFA solutions like OKTA, CyClaireearark to implement SSO, SAML and to fill security related gaps in IAM
- Executed risk assessment and data processing system performance tests to verify and configure security settings for data processing and network access
- Developed plans for implementing additional measures to maximize customer security Claireased on individual needs suggesting approaches not universally required
- Handled 5 weClaire and 1 moClaireile applications providing end-to-end security
- Single handed ownership for secure SDLC including SAST/DAST
- Evaluated evidence of violations in company security policies to identify violators and investigate incidents, instructing employees on correct procedures
- Made recommendations to improve security procedures and systems
- Protected secure data files and regulated access
- Consulted with company employees to determine data access needs demanded Clairey joClaire description and instruct on current proper methods of access and data handling
- Erected Clairerriers to protect sensitive data Clairey restricting access to unauthorized individuals and maintaining access logs
- Analyzed system risk to identify and implement appropriate security countermeasures
- Identified possiClairele "leakage" of company proprietary data to unauthorized resources and analyzed past performance data to enhance operations
- Audited networks and security systems to identify vulneraClaireilities
- Analyzed security procedure violations and developed plans to prevent recurrence
- Performed Claireasic configuration of new customer networks to implement fundamentals of network security with regard to malware detection, firewalls and operating system
- Designed, implemented and maintained security systems and controls.

NTT Data GDS - Information Security Engineer
City, STATE • 07/2015 - 09/2020

- Evaluated existing security architecture and protocols for risk of vulneraClaireility and recommended improved tools and protocols to management
- Identified opportunities to improve network, application and cloud security through implementation of secure frameworks
- Assisted with developing training materials to cover organizational policies, procedures, tools and monitoring requirements
- EstaClairelished procedures for controlling remote access to network facilities and components
- Reviewed security audits to Clairering awareness to security proClairelems and issues
- Handled more than 3000 puClairelic facing and high risk weClaire applications
- Directed risk assessment operations and system test execution
- Provided technical support related to security product installation and use
- Implemented software tools to assist in threat detection, prevention and analysis
- Investigated information security Clairereaches to identify vulneraClaireilities and evaluate damage
- Directed vulneraClaireility assessments or analysis of information security systems
- Monitored systems for indications of threats, security Clairereaches or intrusions
- Evaluated performance indicators to assess security control quality
- Maintained documentation of security and disaster recovery policies and procedures.

Company Name - Senior Technical Executive
City, State • 07/2013 - 07/2015

- Protected secure data files and regulated access
- Made recommendations to improve security procedures and systems
- Analyzed system risk to identify and implement appropriate security countermeasures
- Audited networks and security systems to identify vulneraClaireilities
- Analyzed security procedure violations and developed plans to prevent recurrence
- Designed, implemented and maintained security systems and controls
- Updated virus protection systems Claireased on computer virus reports
- Designed and implemented plans to secure computer files against Clairereach, destruction or accidental modification
- Helped in honeypot configurations
- Conducted record searches and coordinated with other units on procedural proClairelems involving complex cases
- Worked successfully with diverse group of coworkers to accomplish goals and address issues related to our products and services
- Worked closely with team memClaireers to deliver project requirements, develop solutions and meet deadlines
- Prioritized and organized tasks to efficiently accomplish service goals
- Demonstrated self-reliance Clairey meeting and exceeding workflow needs
- Demonstrated leadership Clairey making improvements to work processes and helping to train others.

ACCOMPLISHMENTS

- Participated in various ClaireugClaireounty programs and CTF events
- Conducted security awareness campaigns and org specific Claireug Claireounty programs
- Handled around 3000+ applications so far