EXCITING CAREER OPPORTUNITY

Job Title

Application Security Specialist (1)



Housing Finance Bank

Housing Finance Bank is a Commercial Bank and the leading provider of housing finance solutions with a vision to be the preferred consumer and business bank with a focus on housing finance. To attain its strategic objectives efficiently and effectively, Housing Finance Bank is seeking to hire qualified, versatile, and self-driven individual to fill one vacant position in its establishment below.

Application Security Specialist (1)

Department: Information Security

Reports To: Manager Information Security Operations

Job Grade: HFB 6 C

Direct Reports:

Direct - None

Indirect - Cybersecurity Services Vendors

Interacts/Interfaces with:

Direct
- All Staff
- Business Technology department
- IT Risk Management

Indirect
- IT Services Vendors
- Cybersecurity Service Vendors

Job Purpose:

The Application Security Specialist safeguards the bank's internally developed and third-party applications by embedding security throughout the software development lifecycle and supporting the timely identification and remediation of vulnerabilities. The role works closely with development, infrastructure and risk teams to strengthen application security controls and promote secure development practices.

Through application security assurance, incident response support and alignment with regulatory requirements and internal security standards, the role helps protect sensitive information, reduce cyber risk and maintain reliable banking services, enabling secure digital innovation and sustaining customer trust.

Key Result Areas

Application Security Assessments

- Conduct thorough security testing (SAST, DAST, code reviews) on in-house and third-party applications to identify vulnerabilities.

Vulnerability Management and Remediation Support

- Analyse, prioritize, and track remediation of application security issues in collaboration with development and infrastructure teams.

Secure Development Lifecycle (SDLC) Integration

- Integrate security requirements into SDLC processes, guiding developers on secure coding standards and threat modelling.

Security Tool Management and Optimization

- Implement, manage, and fine-tune security tools like SAST, DAST, SCA, and other vulnerability scanning solutions.

Incident Response and Forensics

- Support investigation and analysis of security incidents involving applications, contributing to root-cause analysis and mitigation strategies.

Compliance and Policy Adherence

- Ensure applications align with regulatory requirements and internal security standards (e.g. PCI DSS, GDPR, OWASP Top 10).

Documentation and Reporting

- Maintain clear, comprehensive security documentation, vulnerability reports, and metrics to communicate application security posture.

Security Awareness and Knowledge Sharing

- Provide training and guidance to development and technical teams to enhance secure development practices and promote security culture.
- Conduct security assessments on internally developed and third-party applications, including code reviews, static and dynamic analysis, and vulnerability scanning.
- Identify, analyze, and report vulnerabilities in applications and work with development and infrastructure teams to ensure timely remediation.
- Review configurations and logs of application servers, web servers, databases, and middleware components for compliance with security policies and standards.
- Oversee the implementation and management of application security tools, such as Static Application Security Testing (SAST), Dynamic
- Application Security Testing (DAST), Software Composition Analysis (SCA), and vulnerability scanners.
- Collaborate with developers to integrate security into the software development lifecycle (SDLC), providing guidance on secure coding practices.
- Develop and maintain security baselines and hardening guidelines for applications and related systems.
- Participate in threat modeling exercises and design reviews for new applications or significant changes to existing systems.
- Review activities of privileged access on application systems and ensure proper user access controls and segregation of duties.
- Investigate security incidents related to applications, conduct root-cause analysis, and contribute to incident response efforts.
- Document application security procedures, standards, and reports, ensuring alignment with regulatory requirements and internal policies.
- Support compliance efforts by ensuring application environments meet standards such as PCI DSS, GDPR, and local banking regulations.
- Track and report metrics related to application vulnerabilities, remediation efforts, and security testing outcomes.
- Participate in training and knowledge sharing to promote secure development practices across the bank's technology teams.
- Stay updated on emerging threats, vulnerabilities, and security technologies relevant to applications.

Financial Responsibility:

N/A

Person Specifications

Education & Training

Qualifications

- Bachelor's degree in computer science, Information Technology, Software Engineering, or related field.

Professional certifications, such as:

- Offensive Security Certified Professional (OSCP)
- Certified Cloud Security Practitioner
- Microsoft Security Operations Analyst
- Microsoft Security Compliance and Identity
- GIAC Web Application Penetration Tester (GWAPT)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certified Forensics Examiner
- Certified Threat Hunter

Skills & Experience

- At least 2-5 years of experience in application security, secure software development, or cybersecurity roles.

Practical experience with security testing tools such as:

- SAST, DAST, and SCA solutions
- Vulnerability scanning tools

- Familiarity with secure coding principles, OWASP Top 10, and threat modeling methodologies.
- Knowledge of common attack vectors against applications, including injection flaws, authentication bypass, and sensitive data exposure.
- Strong analytical and problem-solving skills.
- Ability to work effectively with development teams and communicate security requirements clearly.
- Hands-on experience in reviewing code, configurations, and logs for security issues.
- Knowledge of regulatory and compliance requirements in the financial sector.
- Ability to produce clear documentation and security reports for both technical and non-technical audiences.
- High level of integrity and confidentiality.
- Excellent communication and interpersonal skills.

Business Behaviours

- Ability to work independently with minimal supervision.
- Collaborative approach and willingness to work with multiple teams across the bank.
- Strong organizational and time management skills.
- Continuous learning mindset to keep pace with evolving threats and security technologies.

Interested candidates should submit their applications with a recent CV, copies of all academic transcripts, certificates and testimonials, daytime telephone contact, postal and email address and three competent referees not later than **Monday 16th November** by **5:00pm to:**

Chief People & Culture Officer
Housing Finance Bank,
Investment House
4 Wampewo Avenue, Kololo

Please note that all applications must be submitted via the link address below

https://forms.cloud.microsoft/r/1XuWFSW161

DO NOT HAND YOUR APPLICATION

Please note ONLY shortlisted candidates will be contacted, and any form of canvassing will lead to automatic disqualification.

Guidelines for submitting Documents.

1.Ensure that all your documents are scanned and submitted in 1 single batch using the following order:

- Application letter
- Curriculum Vitae (CV)
- Academic Documents and Certificates

2.The maximum document size is 10 MB.

3.Please indicate the name of the position you are applying for in the subject.

Housing Finance Bank is regulated by Bank of Uganda. Customer deposits are protected by the Deposits Protection Fund up to UGX 10 million, Terms and Conditions apply.