Theme: Hackathon Cyber Security: Quantum-Proof Systems

Background: In the wake of rapid digitalization, banks have shifted critical applications to public-facing environments to meet the "always-on" 24x7x365 demands of modern customers. However, the evolution of quantum computing has introduced a systemic vulnerability: the potential for existing cipher suites to be compromised, enabling "Harvest Now, Decrypt Later" (HNDL) attacks where adversaries intercept encrypted data today to decrypt it once cryptanalytically relevant quantum computers (CRQCs) emerge.

Problem Statement: To develop a software scanner to validate deployment of Quantum proof cipher and create cryptographic bill of material inventory for public facing applications (Web Server, API, System)

To develop a software scanner to generate following inventory only for public facing applications.

- Crypto inventory discovery (TLS Certificate, TLS-based VPN, APIs)
- Cryptographic controls like ciphers used, key exchange, used cipher suite and TLS version used, or any other which are required for public facing CBOM.

Outcome:

- To list the Crypto inventory discovery (TLS, TLS-based VPN, APIs) which are exposed to Internet.
- Recommend to use quantum-safe algorithms on the public facing applications along with actionable for non-PQC ready.
- If the asset is already quantum safe, the "Quantum-Safe" Label should be issued. Assets that successfully implement NIST-standardized Post-Quantum Algorithms are used, automatically awarded a digital "Post Quantum Cryptography (PQC) Ready" or "Fully Quantum Safe" certificate/label. This provides immediate assurance to users that the system is shielded against future cryptanalytic threats.

“Quantum-Ready Cybersecurity for Future-Safe Banking”