OWASP #2 – Cryptographic Failures

Gavin Lillard (IST-103)

Cryptographic Failures refer to risks that occur when incorrect implementations, configurations, or use of cryptographic mechanisms are present. This can inevitably lead to unauthorized access, data breaches and violation of user privacy. Modern society relies on cryptography to: “Ensure confidentiality, maintain integrity, provide authentication, and enable non-repudiation" (OWASP, 2023). If failure is present in any of these systems, potential attackers can use these to bypass the set security controls. Cryptographic risks include weak/broken algorithms, lack of encryption, improper key management, insecure protocols, missing/improper validation, and insufficient randomness. Weak algorithms would include MD5 or SHA-1 for hashing and DES or RC4 for encryption. Not encrypting important data at rest or in transit would lead to a lack of encryption. Using weak/default keys, using the same keys across different systems and not rotating your keys would imply improper key management (Monga, 2024).

OWASP (2023) suggests the best practices to prevent these failures would consist of using strong/modern cryptographic standards, implementing secure key management, encrypting sensitive data, enabling secure communications, using secure defaults, and regularly updating libraries. AES-256 would be great for encryption and SHA-256 would be great for hashing. Store your keys in a KMS and rotate your keys regularly, this would ensure a secure key management. It is crucial to make sure you encrypt your sensitive data. Use HTTPS and TLS 1.2 or higher for secure communications. Use libraries like Bouncy Castle or javax.crypto as well as keeping those libraries up to date to ensure secure defaults.

Works Cited

Monga, Ajay. “Cryptographic Failures: Understanding and Preventing Vulnerabilities.” *Medium*, 8 Dec. 2024, [medium.com/@ajay.monga73/cryptographic-failures-understanding-and-preventing-vulnerabilities-91c8b2c56854](mailto:medium.com/@ajay.monga73/cryptographic-failures-understanding-and-preventing-vulnerabilities-91c8b2c56854).