A02:2021 - Cryptographic Failures

Description

Les échecs cryptographiques font référence à des problèmes liés à l'utilisation incorrecte ou inadéquate de la cryptographie. Ces problèmes peuvent inclure des algorithmes de chiffrement faibles, une gestion incorrecte des clés, des protocoles de chiffrement mal implémentés, et des données sensibles transmises ou stockées sans protection adéquate.

Raisons de vulnérabilité

- Utilisation d'algorithmes de chiffrement obsolètes ou cassés.
- Clés cryptographiques mal gérées ou exposées.
- Protocole de chiffrement mal configuré ou implémenté.
- Absence de chiffrement pour des données sensibles en transit ou au repos.
- Utilisation de bibliothèques cryptographiques non sécurisées ou mal implémentées.

Impact

Les impacts peuvent inclure la divulgation de données sensibles, des attaques de type Man-in-the-Middle, la compromission de sessions utilisateur, et d'autres formes d'exploitation des données.

Prévention et Atténuation

1. **Utilisation de normes cryptographiques robustes** : Utiliser des algorithmes de chiffrement et des protocoles reconnus et recommandés par des organisations de sécurité, tels que AES pour le chiffrement, RSA pour les échanges de clés, et TLS pour les communications sécurisées.
2. **Gestion sécurisée des clés** : Mettre en œuvre une gestion rigoureuse des clés, y compris la rotation régulière des clés, le stockage sécurisé des clés, et l'utilisation de HSM (Hardware Security Modules) si nécessaire.
3. **Chiffrement des données sensibles** : Chiffrer toutes les données sensibles en transit (par exemple, via HTTPS/TLS) et au repos (par exemple, via AES).
4. **Tests de sécurité** : Intégrer des tests de sécurité automatisés pour vérifier les configurations de chiffrement et détecter les faiblesses.
5. **Formation et bonnes pratiques** : Former les développeurs sur les bonnes pratiques en matière de cryptographie et les sensibiliser aux risques associés à une mauvaise implémentation.

Outils et Ressources

- **OWASP Cryptographic Storage Cheat Sheet** : Guide pour une gestion sécurisée du stockage cryptographique.
- **SSL Labs** : Un outil pour tester les configurations TLS des serveurs web.
- **OpenSSL** : Une bibliothèque populaire pour implémenter les protocoles SSL et TLS.

Exemple

Une application web utilise le protocole HTTPS, mais avec une configuration TLS obsolète qui permet l'utilisation de suites de chiffrement faibles comme RC4. Un attaquant pourrait exploiter cette faiblesse pour déchiffrer les communications entre l'utilisateur et le serveur, exposant ainsi des données sensibles telles que des informations de connexion ou des numéros de carte de crédit.