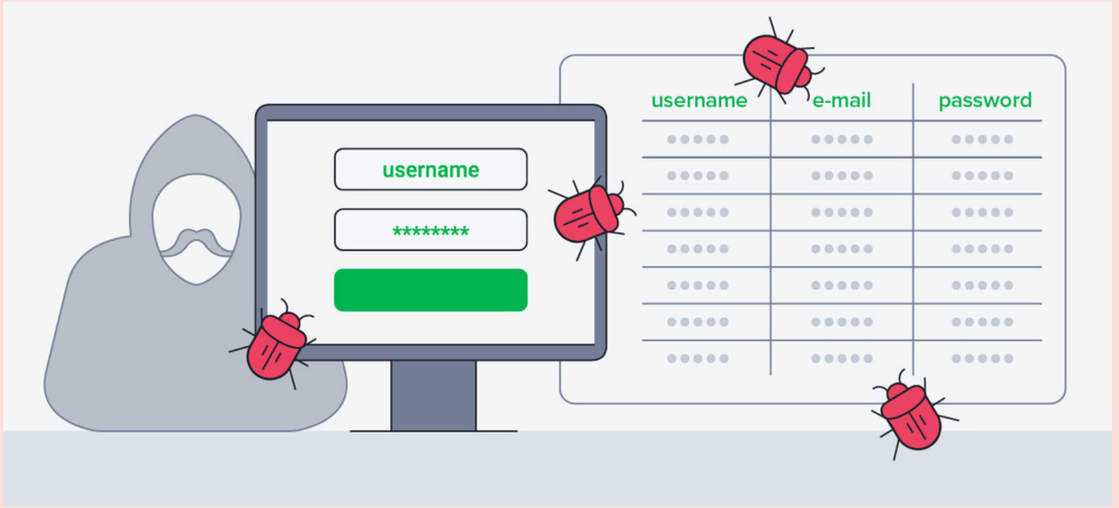
PRESENTATION

FICHE A02 Défaillances cryptographiques



INTRODUCTION

Definition

Données sensibles exposées et exemple scénario d’attaques

prévention

INTRODUCTION

la cryptographie désigne toutes failles et vulnérabilités dans un système de chiffrement , qui permettent aux pirates de contourner ou de déchiffrer des informations à caractères personnelles

DONNÉES SENSIBLES À VERIFIER

Mots de passe vulnérables
données liées au compte d’utilisateurs
Numéro carte bancaire (données personnelles liées)
sites web non sécurisés
Téléchargement de données à partir du web

SCENARIOS ET EXEMPLE D'ATTAQUES

Injection SQL et déchiffrement de données sensibles
exemple d'une application qui déchiffre automatiquement les numéros de carte bancaire
Absence de données sécurisées : Absence de chiffrement TLS (protocole de sécurité)
Hachage insuffisant des mots de passe : utilisation de hachage simple peut exposer son utilisateur à une attaque

MÉTHODE DE VÉRIFICATION

- Transmission sécurisée : vérifier si les données transmises passent par des protocoles sécurisés comme https et protocole TLS
- Algorithme et protocole cryptographiques : utilisation d'algorithme moderne et sécurisés et éviter les clefs de chiffrement faibles ou réutilisés
- Validation des certificats : Vérification des certificats des serveurs et leur chaines sont correctement validés
- Renforcer son mot de passe par le choix du nombre de caractère

CONCLUSION

- Il est important de mettre en place une pratique robuste de sécurité,en matière de cryptographie pour protéger les données sensibles
- Mettre en place des protocoles et des test de fishing pour former et mettre en garde des éventuelles attaques et adopter le bon comportement afin d’éviter des conséquences qui compromettent le cycle de vie de la donnée