

OUEDRAOGO

DERA

WENDTOIN ISSAKA

SAOUDATOU

Enseignant: **M. OUEDRAOGO W. A. Marc Christian**

Module: **PROJETS TUTORÉS**

ENONCE

Projet 3 : Plateforme de location de biens

Développez une plateforme permettant aux utilisateurs de mettre en location des biens (voitures, logements, équipements, etc.), de gérer les réservations, les paiements et les avis des utilisateurs.

1. DISPONIBILITÉ : MOYEN

L'impact d'une indisponibilité due à la cryptographie est généralement moindre que celui d'une violation de la confidentialité.

2. INTÉGRITÉ : TRÈS FORT

La cryptographie est essentielle pour garantir l'intégrité des données en les protégeant contre les modifications non autorisées.

3. CONFIDENTIALITÉ : TRÈS FORT

La cryptographie est le principal moyen de garantir la confidentialité des données en les rendant illisibles pour les utilisateurs non autorisés

4. PREUVE : MOYEN

La cryptographie peut fournir des preuves d'intégrité et de non-répudiation.

II

PARE-FEU

Ecrire un algorithme dont le nom est « merci » et qui permet d'afficher à l'écran la phrase suivante :

1. DISPONIBILITÉ : TRÈS FORT

Le pare-feu doit être disponible pour filtrer le trafic réseau et garantir que les services essentiels restent accessibles

2. INTÉGRITÉ : FORT

Pour prévenir les attaques et garantir que seuls les flux autorisés passent

3. CONFIDENTIALITÉ : FORT

Les pare-feu peuvent filtrer le trafic réseau et masquer certaines informations sensibles, mais ils ne garantissent pas la confidentialité des données.

4. PREUVE : MOYEN

Le pare-feu doit fournir des journaux d'audit pour prouver son efficacité dans la détection et le blocage des tentatives d'accès non autorisées



CONTRÔLE D'ACCÈS LOGIQUES

1. DISPONIBILITÉ : **MOYEN**

Les contrôles d'accès doivent être disponibles pour garantir que seules les personnes autorisées peuvent accéder aux ressources

2. INTÉGRITÉ : **TRÈS FORT**

Les contrôles d'accès logiques sont essentiels pour garantir l'intégrité des données en limitant l'accès aux utilisateurs autorisés.

3. CONFIDENTIALITÉ : **ÉLEVÉ**

Les contrôles d'accès logiques permettent de protéger la confidentialité des données en limitant l'accès aux utilisateurs ayant un besoin légitime d'y accéder.

4. PREUVE : **FORT**

Les contrôles d'accès doivent fournir des traces d'audit pour prouver l'accès restreint aux personnes habilitées

IV**SÉCURITÉ PHYSIQUE DES
ÉQUIPEMENTS ET LOCAUX****1. DISPONIBILITÉ : TRÈS FORT**

Les équipements doivent être disponibles et opérationnels pour assurer la continuité des opérations

2. INTÉGRITÉ : TRÈS FORT

La sécurité physique est essentielle pour garantir l'intégrité des équipements et des données contre les dommages physiques.

3. CONFIDENTIALITÉ : FORT

La sécurité physique peut contribuer à la confidentialité en limitant l'accès physique aux équipements et aux données.

4. PREUVE : FAIBLE

Ecrire un algorithme dont le nom est « merci » et qui permet d'afficher à l'écran la phrase suivante :

I

CRIPTOGRAPHIE

