Lascaux A

A.1.1

Attaquant interne : administrateur,

Guide et commercial

Toutes les personnes qui se connectent à l’application doit être indiqués comme acteurs malveillants, toutes les parties prenantes

Le guide parce qu’il se connecte à la plateforme, l’utilisateur interne car il se connecte à la plateforme

A.1.2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Confidentialité | Disponibilité | Intégrité | Preuve |
| Très important | confidentiel | 24H/7 (banque) | Légale (payement bancaire, on a besoin que les informations soit correctes tel que la date, l’heure, etc) | Légal (inscrit dans les logs applicatifs) |
| Important | Interne | 48H (on peut se passer de pronote pendant 48H) | Opération( opérationnelle pour réaliser les opérations courantes) | Opération (personnes qui se connecte avec leur compte) |
| Pas de besoin | Public | >48H (payement salaire, on en a besoin qu’à la fin du mois) | Tests (données tests qui sont fausses) | Aucune trace (La personne qui visite le site Lascaux) |

Il faut quantifier dans le domaine professionnelle

1.

Très important confidentialité : légale, preuve

Important :

25.

Preuve commercial : pas de besoin, les preuves de déplacements sont pas importants ou oui important car on doit pouvoir prouver qu’il n’y a pas d’erreur pour les épreuves des gens, on peut les conserver 2 mois.

Question A.1.3

Opéération bancaire, avec une carte on conserve les informations jusqu’à 13 mois, la personne peut contester l’opértion bancaire avec une carte pendant 13 mois, il faut donc conserver les traces pendant 13 mois.

Durée de conservation : 13 mois

Données = nom, transaction(achat, payement), date

Ces informations sont la BDD (base de données)

Les logs : l’utilisateur s’est logé, on a une trace dans les logs,

En général les logs c’est un an, on peut mettre au minimum pour la durée de conservation 13 mois.

Back up

Archivage intermédiaire, mettre un processus d’archivage de la BDD,

Conditions pour un archivage : hors site(loin du site), chiffré, authentification (avocat ou juriste dans l’entreprise qui pourra accéder aux archives),

Impacts : financier, légale,

A.2.1

1. Le système ne répond pas : impact très élevé et gravité important, impact de l’image et revenus (perte financière et perte d’image), si le système ne répond pas

3. impact : en terme d’image, d’organisation des visites, perte de confiance, impact modéré

A.2.2

Attaque d’injection, masquer l’url,

Exploiter une faille dans le système,

A.2.3

Elévation des privilèges, au lieu d’accéder seulement aux données il accède au système

Admin system a oublié de fermer la session, ou il a marqué le mdp sur un post it

Mesure à prévoir : Autoriser un seul guide par visite, faire un mél au guide pour la visite, même si la bd est affecté si le guide n’a pas reçu d’email ça ne va rien affecter

A.2.4

Il n’y a qu’à partir : partie A à faire pour jeudi

14/03/2024

Lascaux B

Mot de passe : hacher

Numéro de compte bancaire : chiffrer

Encryption=IS

sensible: divulgation peut causer des problèmes: numéro de compte bancaire, mot de passe, caractéristiques physiques, état de santé, malvoyant, malentendant

Diminuer au minimum les données conservées

sensible: divulgation peut causer des problèmes: numéro de compte bancaire, mot de passe, caractéristiques physiques, état de santé, malvoyant, malentendant

SELECT \*

FROM Acheteur AS A

INNER JOIN Reservation AS R

INNER JOIN Billet AS B ON B.idReservation = R.id

INNER JOIN CategorieAge AS C ON B.idCategorieAge = C.id

INNER JOIN Langue AS L ON R.idLangue = L.id

WHERE A.id = :par\_idAcheteur

AND C.libelle = 'senior' AND

YEAR(dateReservation) = :par\_annee

AND MONTH(dateReservation) = :par\_mois

On enleve \*, on enleve la jointure, il faut prendre numéro réservation associé à l’acheteur

B.2.1

Compte utilisateur, un compte doit être individuel, principe du moindre privilège ou besoin d’en connaître.

CREATE USER lesoil@172.16.2.1 identified by ‘Lemot2PasseComplique128,,’

GRANT SELECT ON lascauxprod.\* TO [lesoil@172.16.2.1](mailto:lesoil@172.16.2.1);

FLUSH PRIVILEGES;

Une vue: offrir à un utilisateur une table virtuelle

CREATE VIEW AS vuedetest AS (

B.2.4

Filtrer les insultes, les commentaires, etc

Texte non rattaché à un billet : la personne ne s’est pas connecté, injection