BTS SIO – ÉPREUVE E6 SLAM

PRÉFIGURATION DE SUJET ZÉRO CAS Lascaux IV

Éléments de correction avec préfiguration de barème

Ce document préfigure ce que seront les éléments de corrigé utilisés par les correcteurs pour l'épreuve E6 évaluant le bloc 3 option SLAM. Il s'agit d'un exemple qui n'est pas destiné à être utilisé en l'état, le cas Lascaux IV n'étant lui-même pas un sujet destiné à évaluer des candidats en quatre heures. Le découpage en points est partiellement présent à titre d'illustration. Il conviendra évidemment de l'adapter au contexte dans lequel les questions de ce sujet seront utilisées.

Dossier A – Participation à l'atelier d'analyse des risques sur l'application *Web*

Mission A1 – Évaluation des risques à partir des récits utilisateurs

Question A1.1
Indiquer si le tableau contenant les acteurs à l'origine de malveillance est complet. Justifier votre réponse.

Le tableau est incomplet car le guide et le responsable commercial ne sont pas mentionnés. Or, ces partenaires internes à l'entreprise peuvent divulguer des informations confidentielles sur les visiteurs.

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement
- Prendre en compte la sécurité dans un projet de développement d'une solution applicative

Excellente maîtrise	**3**	Les deux acteurs sont identifiés et la réponse est justifiée.
Bonne maîtrise	**2**	Un seul acteur est identifié et la réponse est justifiée.
Maîtrise partielle	**1**	Un ou deux acteurs existants sans justification.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Question A1.2
Proposer une évaluation des récits utilisateurs 1 et 25 pour chacun des 4 critères (disponibilité, intégrité, confidentialité et preuve).

	Intitulé de la *user story*	Disponibilité	Intégrité	Confidentialité	Preuve
1	En tant qu'acheteur, je veux acheter en ligne les billets pour plusieurs personnes afin de pouvoir participer à une visite.	**	**	**	*
25	En tant que responsable commercial, je veux consulter les statistiques de temps passé par zone de visite et les activités réalisées par les visiteurs afin de proposer un meilleur service aux visiteurs.	*	**	-	-

Compétence évaluée :
Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques
- Caractériser les risques liés à l'utilisation malveillante d'un service informatique.

Excellente maîtrise	**2**	Les deux récits sont évalués de façon cohérente.
Maîtrise partielle	**1**	Évaluation ou cohérence partielle.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Question A1.3
Présenter ces conditions à Christine Berton.

Pour que les traces soient opposables en cas de contentieux, sans ambiguïté possible, leur contenu et leur interprétation doivent être documentés, au sein de la convention de preuve du service d'achat en ligne, dans la politique de traçabilité : pour chaque trace, il convient de décrire dans quel cas elle est produite, les éléments qui y figurent et le sens qu'ils ont**.**

Compétence évaluée :
Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques
- Organiser la collecte et la conservation des preuves numériques

Excellente maîtrise	**4**	Réponse correcte sur le fond et sur la forme (« communication écrite adaptée à l'interlocuteur »).
Bonne maîtrise	**3**	Réponse correcte, forme insuffisante.
Maîtrise partielle	**2**	Réponse partielle.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Mission A2 – Gestion des évènements redoutés

Question A.2.1
Proposer, pour les événements 1 et 3 fournis dans le tableau, les impacts pour l'entreprise et une estimation de leur gravité.

Numéro de l'événement	Événement	Impact pour l'entreprise	Gravité
1	Le système ne répond pas.	Perte d'acheteur (de clients) Mauvaise image de marque	*
3	Un attaquant accède à la base de données et modifie l'affectation des guides aux visites.	Désorganisation des visites, perte de réputation	**

** : modérée* *** : très élevée*

Compétence évaluée :
Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

- Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité

Excellente maîtrise	**4**	Le candidat indique les impacts des deux événements et propose une estimation de leur gravité.
Bonne maîtrise	**2**	Le candidat indique les impacts d'un seul événement et propose une estimation de sa gravité.
Maîtrise partielle	**1**	Le candidat indique soit les impacts soit l'estimation de leur gravité mais pas les deux.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Question A.2.2
Proposer des mesures à prévoir lors du développement pour contrer l'évènement redouté numéro 4.

Numéro de l'événement	scénario de risque (*abuser story*)	Mesures à prévoir
4	En tant qu'acheteur, je peux imprimer les billets d'un autre acheteur.	4.1 Chiffrement du numéro de réservation.
		4.2 Vérifier que le numéro de réservation appartient bien à l'acheteur connecté.

Compétence évaluée : Assurer la cybersécurité d'une solution applicative et de son développement • Prévenir les attaques		
Excellente maîtrise	**3**	Le candidat propose des mesures adaptées.
Bonne maîtrise	**2**	Le candidat propose une seule mesure adaptée.
Maîtrise partielle	**1**	Le candidat propose des mesures partiellement adaptées.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Question A.2.3
Proposer un scénario de risque (abuser story) et des mesures à prévoir pour l'événement redouté numéro 3.

Numéro de l'événement	scénario de risque (*abuser story*)	Mesures à prévoir
3	En tant qu'attaquant externe, je peux modifier l'affectation des guides aux visites dans la base de données.	3.1 Un guide doit être disponible à la date d'une visite.
		3.2 Un guide doit parler la langue de la visite à laquelle il est associée.

Compétence évaluée : Assurer la cybersécurité d'une solution applicative et de son développement • Prendre en compte la sécurité dans un projet de développement d'une solution applicative		
Excellente maîtrise	**4**	Le candidat propose un scenario de risque pertinent et des mesures adaptées.
Bonne maîtrise	**3**	Le candidat propose un scenario de risque pertinent et une mesure adaptée.
Maîtrise partielle	**1**	Le candidat propose un scenario pertinent sans mesures ou des mesures seules .
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Question A.2.4
Proposer deux évènements redoutés en lien avec les besoins de sécurité du récit utilisateur (*user story*) 15.

Les événements doivent concerner principalement l'intégrité des données (cf tableau besoins de sécurité)

- Un attaquant accède à la base de données et injecte des commentaires non reliés à un billet ;
- Un attaquant accède à la base de données et ajoute des commentaires diffamatoires.

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement
- Prendre en compte la sécurité dans un projet de développement d'une solution applicative

Excellente maîtrise	**3**	Le candidat propose deux événements redoutés cohérents, un sur l'intégrité et un autre concernant la disponibilité ou la preuve ou l'intégrité.
Bonne maîtrise	**2**	Le candidat propose deux événements redoutés cohérents concernant la disponibilité et/ou la preuve ou bien un seul sur l'intégrité.
Maîtrise partielle	**1**	Le candidat propose des évènements redoutés en lien avec la confidentialité.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Mission A3 – Prise en compte du règlement général sur la protection des données (RGPD) dans les récits utilisateurs

Question A3.1
Lister pour chacun des récits utilisateurs (*user stories*) numérotés 22 et 25, les actions à mettre en œuvre pour respecter le RGPD.

Pour le récit utilisateur numéro 22 :

- Procéder au hachage du mot de passe ;
- Obtenir le consentement préalable du visiteur (*opt-in*) lors de la création de compte ;
- Mettre à disposition les conditions de stockage et d'utilisation des données ;
- Donner la possibilité de supprimer son compte et les données personnelles (photos/vidéos).

Pour le récit utilisateur numéro 25 :

- Gérer les habilitations pour que seul le directeur commercial puisse accéder à la fonctionnalité décrite dans le récit utilisateur.
  Dans le cadre du RGPD, la CNIL fait un rappel précis sur le sujet de la « bonne gestion des habilitations » qui s'inscrit dans le RGPD. Une entreprise doit vérifier :
  - que les données qu'elle traite sont nécessaires à ses activités ;
  - qu'aucune donnée dite « sensible » n'est traitée ou, si c'est le cas, qu'elle a bien le droit de les utiliser ;
  - que seules les personnes habilitées ont accès aux données dont elles ont besoin ;
  - qu'elle ne conserve pas des données au-delà de ce qui est nécessaire.
- Établir une fiche de registre relative au traitement des statistiques.

Compétence évaluée : Protéger les données à caractère personnel • Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel		
Excellente maîtrise	**3**	Le candidat propose, pour chacun des deux récits, les actions pertinentes et opérationnelles.
Bonne maîtrise	**2**	Le candidat propose, pour chacun des deux récits, des actions pertinentes et opérationnelles (pas toutes les actions attendues).
Maîtrise partielle	**1**	Des connaissances non contextualisées.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Question A3.2
Expliquer quel risque de sécurité vient contrer cet ajout.

Cet ajout permet de contrer (limiter) le risque d'usurpation d'identité (prise de contrôle du poste, vol d'id de session).

Compétence évaluée : Protéger les données à caractère personnel • Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel		
Excellente maîtrise	**3**	La personne candidate identifie le risque et l'explique.
Maîtrise partielle	**2**	La personne candidate identifie le risque sans explication complémentaire
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Dossier B – Sécurisation des données

Mission B1 – Vérification de la confidentialité des données

Question B.1.1
a) Identifier les données personnelles présentes sur la représentation conceptuelle de la base de données.
b) Identifier, parmi ces données personnelles, celles qui sont sensibles.

Les données personnelles permettent d'identifier directement ou indirectement une personne.

Les données sensibles forment une catégorie particulière des données personnelles dont le traitement est particulièrement risqué. Il s'agit par exemple des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données concernant la santé ou la vie sexuelle.

a) Pour l'entité Acheteur : nom, prenom, mel, telephone, numeroCarteBancaire, motDePasse
Pour l'entité Billet : nom, prenom, dateNaissance, civilite, sexe, mel, estMalentendant, estMalvoyant, qrCode

b) Pour l'entité Billet : estMalentendant, estMalvoyant

Compétence évaluée :
Protéger les données à caractère personnel
- Recenser les traitements sur les données à caractère personnel au sein de l'organisation

Excellente maîtrise		Le candidat identifie de façon complète les données personnelles et les données sensibles.
Maîtrise partielle		Le candidat ne distingue pas les données personnelles des données sensibles, c.-à-d. que seule la réponse à la question a) est valide
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question B.1.2
Lister les données devant être chiffrées et celles devant être hachées, pour assurer la confidentialité des données de la table Acheteur.

Données à chiffrer : numeroCarteBancaire, nom, prenom, telephone + mel
Données à hacher : motDePasse

Compétence évaluée :
Protéger les données à caractère personnel
- Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel

Excellente maîtrise		Les deux listes sont correctes.
Bonne maîtrise		Le candidat propose une réponse correcte partielle : mot de passe à hacher et liste des données à chiffrer incomplète.
Maîtrise partielle		Le candidat liste seulement les données à chiffrer.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question B.1.3
Réaliser les modifications demandées dans le courriel de Denise Bradord.

```
1. Select B.nom, B.prenom, mel
2. from Acheteur as A
3. join Reservation as R on R.idAcheteur = A.id
4. join Billet as B on B.idReservation = R.id
5. join CategorieAge as C on B.idCategorieAge = C.id
6. join Langue as L on R.idLangue = L.id
7. where A.id = :par_idAcheteur
8. and C.libelle = 'senior'
9. and year(dateReservation) = :par_annee
10. and month(dateReservation) = :par_mois
```

ligne 1 : remplacer select * par **select B.nom, B.prenom, mel**
Le select * fournit toutes les données des tables utilisées par la requête, or seuls le nom, le prénom et l'adresse mail des visiteurs sont nécessaires

ligne 3 : ajouter **on R.idAcheteur = A.id** pour éviter que toutes les réservations soient prises en compte

ligne 6 : supprimer la jointure avec Langue, cette table étant inutile car aucune de ses données n'est à prendre en compte pour la requête

Remarque : si la base de données était gérée par un SGBD différent de *MySQL* (SQLServer par exemple), la requête ci-dessus retournerait une erreur de syntaxe mais *MySQL*, plus tolérant à l'égard des comportements non conformes, accepte cette requête au niveau syntaxique.

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement
- Participer à la vérification des éléments contribuant à la qualité d'un développement informatique

Excellente maîtrise		Les trois modifications correctes sont proposées.
Bonne maîtrise		Deux modifications correctes.
Maîtrise partielle		Une modification correcte.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Mission B2 – Sécurisation de l'accès à une base de données

Question B.2.1
Justifier la création du compte utilisateur et de ses caractéristiques.

Trois raisons pour justifier ce compte et ses caractéristiques :

- La création d'un compte propre à l'utilisateur, au nom de l'utilisateur, permet d'identifier la personne connectée à la base de données et d'associer une action à un responsable ;
- L'accès à partir d'une machine limite l'accès depuis l'extérieur : l'accès ne pourra se faire qu'à partir d'un poste interne à l'entreprise ;
- La consultation des données des tables autorisées renforce la sécurité car Mme Lesoil dispose uniquement d'un accès en lecture aux tables nécessaires au besoin.

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement
- Prévenir les attaques

Excellente maîtrise		La justification est pertinente car elle expose trois raisons.
Bonne maîtrise		Le candidat expose deux raisons.
Maîtrise partielle		Le candidat propose une seule raison pertinente.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question B.2.2
Rédiger les requêtes permettant de créer le compte utilisateur et les contraintes de sécurité demandées.

```
-- création du compte utilisateur qui sera utilisé
CREATE USER 'lesoil'@'172.16.2.1' IDENTIFIED BY 'L#pbGd\M589@';
-- affectation des droits de lecture sur les tables utilisées par la requête :
GRANT SELECT on lascauxprod.CategorieAge to 'lesoil'@'172.16.2.1'  ;
GRANT SELECT on lascauxprod.Visite to 'lesoil'@'172.16.2.1' ;
GRANT SELECT on lascauxprod.Billet to 'lesoil'@'172.16.2.1'  ;
GRANT SELECT on lascauxprod.Commentaire to 'lesoil'@'172.16.2.1'  ;
```

On évaluera le mot de passe choisi et la connexion de l'utilisateur à partir de la machine autorisée.

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement
- Prévenir les attaques

Excellente maîtrise	**6**	Le candidat propose une réponse complète correcte : 5 requêtes + l'utilisation de @'172.16.2.1' et d'un mot de passe robuste dans le create user
Bonne maîtrise	**4**	L'instruction create est correcte et au moins un grant est correct.
Maîtrise partielle	**2**	L'instruction create ou les instructions grant sont correctes.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Question B.2.3
Rédiger une courte note expliquant l'intérêt d'une vue en termes de sécurité.

Seules les données fournies par la vue sont visualisables.
Avec une vue, l'utilisateur Lesoil n'aurait accès qu'aux données fournies par celle-ci. Il lui serait, de ce fait, impossible de faire une autre requête et donc d'accéder à d'autres données.

Compétence évaluée :
Sécuriser les équipements et les usages des utilisateurs
- Gérer les accès et les privilèges appropriés

Excellente maîtrise	**3**	Réponse correcte sur le fond et sur la forme.
Bonne maîtrise	**2**	Réponse correcte sur le fond.
Maîtrise partielle	**1**	Le candidat propose une réponse partielle.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Question B.2.4
Expliquer en quoi la modération des commentaires est un enjeu important pour Lascaux IV.

La modération des commentaires est nécessaire pour garantir :
- l'absence de publication de données à caractère personnel (nom d'un guide...) ;
- l'absence de messages inappropriés (publicité...) ;
- la source des commentaires (visiteur réel).

L'absence de modération pourrait avoir des conséquences juridiques (DCP...) et économiques (impact sur l'image de marque, baisse de fréquentation...) pour l'organisation.
Extrait du guide d'accompagnement : « L'enseignement de CEJMA permettra de compléter les conséquences techniques des risques liés à l'utilisation malveillante d'un service informatique en abordant les conséquences économiques (pertes financières, détérioration de l'image de l'organisation, etc.) et juridiques (atteintes au patrimoine informationnel et notamment aux données à caractère personnel, violation des droits de propriété intellectuelle, atteinte à l'identité de l'organisation etc.) qui peuvent en découler. »

Notons qu'une partie des enjeux relève également du bloc 1 (e-reputation).

La modération permet de contrôler et superviser les publications des internautes pour préserver l'image de l'entreprise sans empêcher la liberté des échanges.

Compétence évaluée :
Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques
- Caractériser les risques liés à l'utilisation malveillante d'un service informatique

Excellente maîtrise	**3**	Plusieurs risques économiques et juridiques abordés.
Maîtrise partielle	**1**	un seul enjeu abordé.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Question B.2.5
Proposer à Roger Zanches une requête pour répondre à son besoin.

```
SELECT COUNT(*)
FROM commentaire
WHERE idBillet  IS NULL
```

Remarque : on exigera la présence du comptage, étant donné que l'on demande uniquement de rechercher l'existence de commentaires non reliés à un billet. Un select ramenant des lignes de la table Commentaire n'est pas approprié ici, au regard du besoin.

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement
- Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures

Excellente maîtrise	**3**	Requête correcte avec la clause « count(*) ».
Maîtrise partielle	**1**	Le candidat propose une ébauche correcte sans la clause « count(*) ».
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Mission B3 – Adaptation de la représentation conceptuelle de la base de données

Question B.3.1
Identifier et justifier les données devant être supprimées pour une mise en conformité vis à vis de la fiche de registre établie par le DPO.

Suppression de la date de naissance. Cette date est saisie mais elle n'a pas besoin d'être enregistrée : elle permet simplement de déterminer la tranche d'âge du visiteur en vue de définir le tarif du billet (déjà réalisé grâce à l'association entre Billet et CategorieAge).

Suppression des coordonnées bancaires car elles ne servent que pour le paiement.

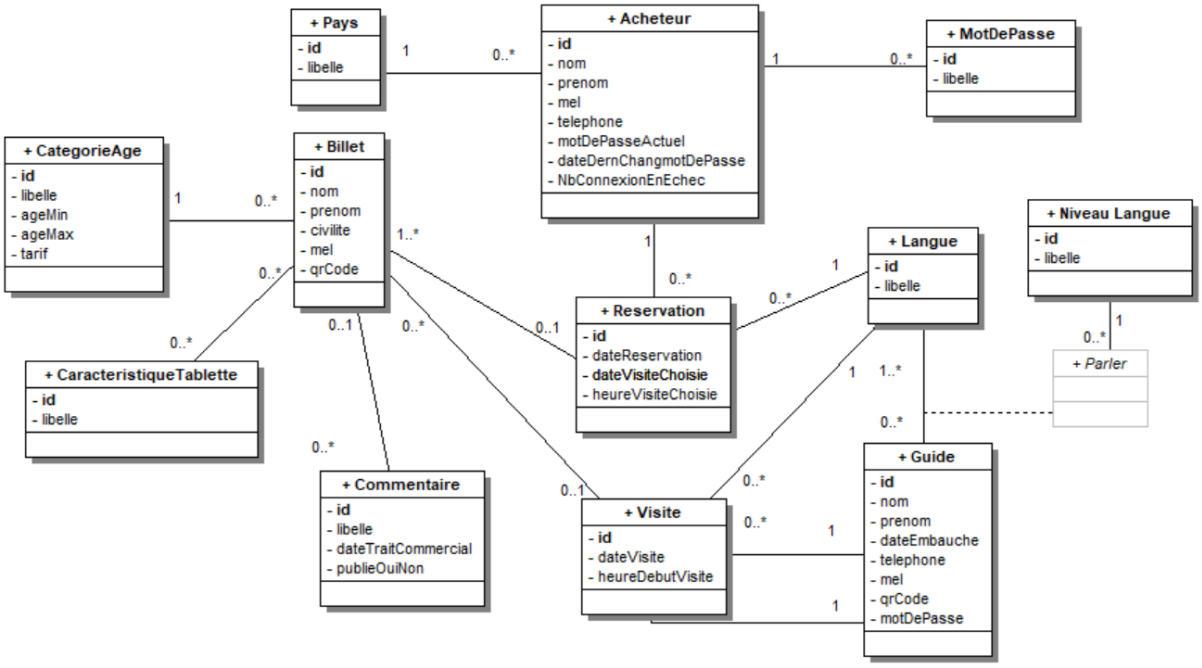
Suppression du sexe car il peut être déduit de la civilité.

Compétence évaluée :
Protéger les données à caractère personnel
- Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel

Excellente maîtrise	**3**	Le candidat identifie de façon complète les trois suppressions à effectuer pour appliquer la réglementation et les justifient correctement.
Bonne maîtrise	**2**	Le candidat propose de supprimer la date de naissance et une autre donnée.
Maîtrise partielle	**1**	Le candidat propose seulement de supprimer la date de naissance en le justifiant.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

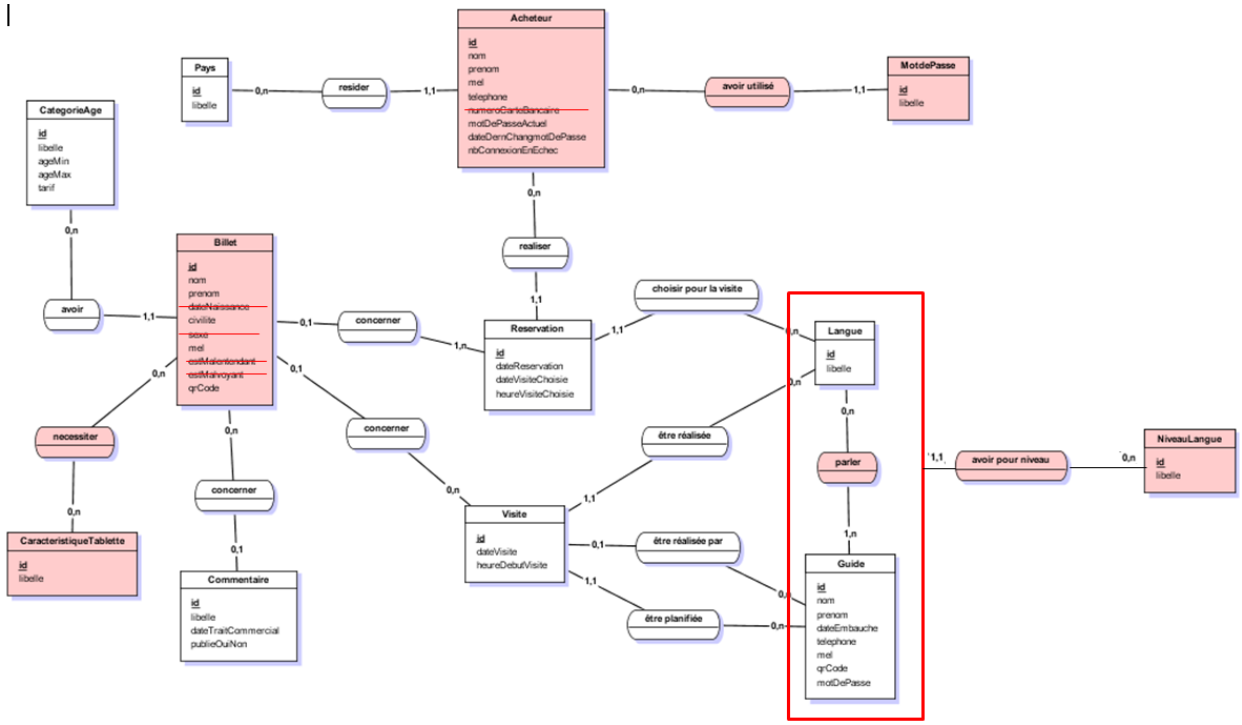
Question B.3.2
Proposer les modifications à réaliser pour répondre aux nouvelles exigences. Seuls les éléments du schéma existant qui sont concernés par l'évolution seront repris dans le schéma proposé.

Éléments de corrigé du diagramme de classes intégrant le corrigé des questions B3.1 et B3.2 :



Remarque : les attributs nommés 'id' sont des identifiants.

Éléments de corrigé du schéma entité-association intégrant le corrigé des questions B3.1 et B3.2 :



Remarque : la fausse ternaire peut être représentée avec une agrégation, comme proposé dans le corrigé fourni, mais il est également possible d'utiliser une association d'association, une pseudo-entité ou une DF.

Compétence évaluée : Assurer la cybersécurité d'une solution applicative et de son développement • Prendre en compte la sécurité dans un projet de développement d'une solution applicative		
Excellente maîtrise	**6**	Modélisation cohérente sur les trois pôles ; "Guide-Langue-Niveau", "Acheteur-MotDePasse" et "Billet-CaractéristiqueTablette"
Bonne maîtrise	**4**	Modélisation cohérente sur deux pôles.
Maîtrise partielle	**2**	Un seul pôle est cohérent.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Dossier C – Gestion de la connexion des utilisateurs sur le compagnon de visite (CDV)

Mission C1 – Identification des visiteurs

Question C.1.1
Identifier les faiblesses du script *getVisiteur.php* du point de vue de la cyber sécurité, en expliquant leurs conséquences possibles sur le système.

Il y a plusieurs faiblesses ici :

A. Le script *getVisiteur.php* ne devrait pas appeler la fonction *getVisiteurByQrCode* sans avoir préalablement filtré l'argument à passer.

Code (non exigé) permettant de corriger ces faiblesses :

```
header("content-type: application/json; charset=utf-8");
// vérifie que le champ qrcode est passé en post et renseigné
if (filter_has_var(INPUT_POST, 'qrcode') == true) {
        // filtre l'argument à passer
        $qrcodeFiltre = filter_input(INPUT_POST, 'qrcode', FILTER_SANITIZE_STRING) ;
        echo getVisiteurByQrCode($qrcodeFiltre);
} else {
        $erreur['erreur'] =  "absence de code QR";
        echo json_encode($erreur);
}
```

La technique de filtrage permet de se prémunir contre ces attaques qui pourraient avoir des conséquences graves de corruption et d'effacement de données.

B. La fonction *getVisiteurByQrCode* ne respecte pas bien son contrat :

- Le code de la fonction n'est pas suffisamment sûr et permettrait une attaque de style "injection SQL". La technique de requête préparée permet de se prémunir contre ces attaques qui pourraient avoir des conséquences graves de corruption et d'effacement de données.
- la fonction *getVisiteurByQrCode* ne teste pas le cas où le visiteur n'est pas trouvé dans la base de données

```
$ligne = $req->fetch(PDO::FETCH_ASSOC);
if ($ligne == false) {
        $erreur['erreur'] =  “Pas de visiteur avec ce code QR”;
        return  json_encode($erreur);
} else {
        return json_encode($ligne);
}
```

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement
- Mettre en œuvre et vérifier la conformité d'une solution applicative et de son développement à un référentiel, une norme ou un standard de sécurité

Excellente maîtrise	**8**	Le candidat analyse les faiblesses et les justifie en exposant les conséquences.
Bonne maîtrise	**6**	Le candidat analyse partiellement les faiblesses et leurs conséquences.
Maîtrise partielle	**3**	Le candidat analyse partiellement les faiblesses sans détailler les conséquences.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Question C.1.2
Modifier le script *getVisiteur.php* en utilisant une requête préparée.

```
$qrCode = filter_input(INPUT_POST, 'qrcode', FILTER_SANITIZE_STRING) ;

$sql = "SELECT billet.id as id, civilite, nom, prenom, mel,
        categorieAge.id as idCategorieAge, libelle AS libCategorieA
        FROM billet
        JOIN CategorieAge ON idCategorieAge = CategorieAge.id
        WHERE qrCode = :qrCode";
$req = $conn->prepare($sql);
$req->bindValue(':qrCode', $qrCode, PDO::PARAM_STR);
$req->execute();
```

La première instruction n'est pas exigée, mais les bonnes pratiques conseillent d'utiliser la fonction filter_input pour supprimer les balises et les caractères spéciaux des données transmises dans $_POST.

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement
- Mettre en œuvre et vérifier la conformité d'une solution applicative et de son développement à un référentiel, une norme ou un standard de sécurité

Excellente maîtrise	**3**	Le candidat propose une solution avec une requête préparée correcte.
Maîtrise partielle	**1**	La requête est préparée mais elle est fausse.
Non maîtrisé	**0**	Réponse non adaptée.
Non évaluable	**0**	Non répondu.

Question C.1.3
Décrire les mesures à mettre en place pour éviter qu'un visiteur peu scrupuleux puisse scanner un billet trouvé par terre ou dans une poubelle et ainsi effectuer une visite avec un billet déjà utilisé.

Plusieurs solutions sont envisageables :
- Vérifier que le billet n'a pas encore été flashé en appelant la méthode isBilletUtilise() de la classe Visiteur. Cet appel se fera dans la méthode *identifierVisiteur* de la classe MainActivity ;
- Contrôler que la date et l'heure de la visite ne sont pas antérieures au moment où le billet est scanné ;
- Modifier la requête SQL située dans la fonction *getVisiteur.php* pour vérifier que le billet n'est pas affecté à une visite

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement
- Prévenir les attaques

Excellente maîtrise		Le candidat propose au moins deux mesures pertinentes et opérationnelles. Le candidat décrit les solutions retenues (au-delà de la simple énumération).
Bonne maîtrise		Le candidat propose au moins deux mesures pertinentes et opérationnelles sans les décrire ou bien une seule mesure décrite.
Maîtrise partielle		Le candidat propose une seule mesure sans la décrire.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Mission C2 – Authentification des guides

Question C.2.1
Rédiger la méthode *doitChangerMdP*() de la classe Guide.

```
public boolean doitChangerMdP(){
        // on récupère la date du jour
        LocalDate dateLimite = LocalDate.now();
        // on calcule la date un trimestre avant
        dateLimite = dateLimite.minusMonths(3);
        return this.actuelMotDePasse.getDateCreation().isBefore(dateLimite);
}
```

Compétence évaluée :
Sécuriser les équipements et les usages des utilisateurs
- Gérer les accès et les privilèges appropriés

Excellente maîtrise		Code complet et fonctionnel (avec respect de la signature de la méthode).
Bonne maîtrise		Code cohérent mais erreur sur la gestion des dates ou oubli de l'instruction « return ».
Maîtrise partielle		Code incomplet.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question C.2.2
Modifier la méthode *setMotDePasse*() de la classe Guide afin de prendre en compte la nouvelle contrainte de sécurité demandée lors de cette nouvelle itération (*sprint*).

```
public boolean setMotDePasse(String unMotDePasse){
  boolean modifRealisee = true;
  LocalDate aujourdhui =  LocalDate.now();

  //1-Vérifier que le mot de passe n'est pas le même que l'actuel
  if (unMotDePasse.equals(this.actuelMotDePasse.getMotDePasse()) {
       modifARealiser = false;
    } else {
    //2-vérifier que le mot de passe n'a pas été utilisé durant les 12 derniers mois
    LocalDate douzeMoisAvant = aujourdhui.minusMonths(12);

    for(MotDePasse mdp : this.lesAnciensMotsDePasse){
      if(mdp.getDateCreation().isAfter(douzeMoisAvant) &&
      mdp.getMotDePasse().equals(unMotDePasse)){
          modifARealiser = false;
          break;
    }
  }
  //3-Si ok on archive le mot de passe actuel et on met à jour le nouveau mot de passe
  if(modifARealiser){
    //On archive le mot de passe actuel
    this.lesAnciensMotsDePasse.add(this.actuelMotDePasse);
    //Mise à jour du nouveau mot de passe
    this.actuelMotDePasse = new MotDePasse(aujourdhui, unMotDePasse);
  }

  return modifARealiser;
}
```

On peut également utiliser un for pour parcourir l'historique comme ceci :

```
int tailleHisto = this.lesAnciensMotsDePasse.size() ;
for (int i = 0; i < tailleHisto && modifARealiser) {
     MotDePasse mdp = this.lesAnciensMotDePasse.get(i);
     [...]
}
```

Remarque : La solution présentée ici utilise le parcours de collection proposé dans le sujet, mais d'autres solutions sont possibles comme l'utilisation d'une boucle "tant que non trouvé", ou de filtrage (stream, filter et lambda expression) par exemple.

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement

- Mettre en œuvre et vérifier la conformité d'une solution applicative et de son développement à un référentiel, une norme ou un standard de sécurité

Excellente maîtrise		La modification de la méthode prend en compte complètement la nouvelle contrainte.
Bonne maîtrise		Parcours de collection ou autre solution pertinente.
Maîtrise partielle		Code partiel (dates, conditionnelles…) sans parcours de la collection des anciens mots de passe.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question C.2.3 Argumenter en faveur ou non de cette durée.

Si l'on souhaite que le guide ne puisse pas utiliser un de ses anciens mot de passe, il n'y a aucune raison d'exclure les plus anciens, car ces derniers sont tout aussi vulnérables que les plus récents. Donc, la recherche devrait se faire sur tous les anciens mots de passe connus du guide.

Compétence évaluée : Sécuriser les équipements et les usages des utilisateurs • Gérer les accès et les privilèges appropriés		
Excellente maîtrise		Argumentation pertinente.
Maîtrise partielle		Argumentation non aboutie ou contenant des contradictions
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Dossier D – Préparation du développement et pilotage de la sous-traitance

Mission D1 – Rejet des mauvaises pratiques de développement

Question D.1.1
Relever les numéros des propositions qu'il faut rejeter à tout prix et justifier votre position pour chacune des propositions rejetées.

Les propositions 1, 2, 4 et 6 sont à rejeter.

Proposition 1 : le compte *root* dispose de tous les droits sur toutes les bases de données du serveur. Il est vivement déconseillé dans les scripts d'utiliser le compte *root* pour se connecter à la base de données. Un compte spécifique doit être créé pour l'application ayant uniquement les droits en *select, insert, update, delete* sur les tables de la base de données utilisées par l'application.

Proposition 2 : l'identifiant et le mot de passe de l'administrateur de l'application en production ne doit pas être divulgué aux développeurs.

Proposition 4 : les développeurs ne doivent jamais tester sur des bases de production, ils doivent disposer de bases de test contenant des données différentes des données de production.

Proposition 6 : l'activité des hackers est souvent concentrée les week-ends, il ne faut surtout pas arrêter les éléments de surveillance à ce moment-là.

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement
- Prendre en compte la sécurité dans un projet de développement d'une solution applicative

Excellente maîtrise	**4**	Les quatre propositions à rejeter sont identifiées, les rejets sont justifiés.
Bonne maîtrise	**3**	Trois propositions rejetées sont identifiées avec justification.
Maîtrise partielle	**2**	Deux propositions rejetées sont identifiées avec justification.
Non maîtrisé	**0-1**	Réponse non adaptée ou insuffisante (une seule proposition rejetée et justifiée).
Non évaluable	**0**	Non répondu.

Mission D2 – Rédaction d'un contrat de sous-traitance

Question D.2.1
Lister au moins trois préconisations qui devront apparaître dans la partie règle de sécurité du contrat des sous-traitants devant effectuer des interventions sur le site de Lascaux IV.

Générer des comptes avec des restrictions pour chaque intervenant externe.
Mettre en place un cahier de suivi des interventions.
Interdire la mise en place des logiciels de contrôle à distance.
Mettre en place une clause de confidentialité.
Ne fournir au prestataire que les données nécessaires à leur intervention et, pour les données de type client, prévoir un jeu de test ne reprenant pas les vraies identités.
Vérifier que les intervenants sont sensibilisés aux règles de sécurité informatique.
Ne donner accès qu'au lieu, machine et programme concernés par l'intervention.
Désigner un responsable chargé de vérifier le bon déroulement des interventions.

Toute autre proposition judicieuse peut être acceptée.

Compétence évaluée :
Sécuriser les équipements et les usages des utilisateurs
- Gérer les accès et les privilèges appropriés

Excellente maîtrise	**3**	Au moins trois préconisations sont listées.
Bonne maîtrise	**2**	Deux préconisations sont listées.
Maîtrise partielle	**1**	Une seule préconisation est listée.
Non maîtrisé	**0**	Réponse non adaptée
Non évaluable	**0**	Non répondu.