Proposition de corrigé

CAS Yak

Dossier A – Habilitations de l'application Holy

Mission A1 – Amélioration des bonnes pratiques

Question A1.1 & A1.2

Corriger les erreurs de nommage présentes dans cette méthode.
Proposer une documentation pour cette méthode.

```
/**
 * Recherche le mot de passe passé en paramètre dans la collection des anciens mots de passe
 * @param mdpRecherche mot de passe à rechercher
 * @return vrai si le paramètre existe dans les anciens mots de passe
 */
public boolean existeAncienMdp(String mdpRecherche)
{
    /* Renommer le nom de la méthode avec un verbe, exemple : existeAncienMdp
     * Renommer le paramètre m, exemple : mdpRecherche */
    …
}
```

Question A1.1. 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

Bonne Maîtrise		La méthode et le paramètre ont été correctement renommés.
Maîtrise partielle		Seule la méthode ou le paramètre a correctement été renommé.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question A1.2. 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

Bonne maîtrise		La documentation possède un descriptif, la signification du paramètre et de la valeur de retour.
Maîtrise partielle		La documentation est incomplète.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Mission A2 – Authentification : Validation des mots de passe

Question A2.1

Identifier la complexité des mots de passe attendue lors de l'authentification des utilisateurs.

Complexité du mot de passe :

- 12 caractères minimum,
- au moins une majuscule,
- au moins 3 minuscules,
- au moins 4 chiffres,
- au moins un caractère spécial.

Compétence évaluée :
Sécuriser les équipements et les usages des utilisateurs

- Gérer les accès et les privilèges appropriés

Bonne maîtrise		Tous les éléments de la complexité ont été identifiés.
Maîtrise partielle		Il manque un ou deux critères de complexité.
Non maîtrisé		Seul un ou deux critères de complexité ont été identifiés.
Non évaluable		Non répondu.

Question A2.2

Écrire le code de la méthode modifierMdp de la classe Utilisateur.

```
public boolean modifierMdp(String valMdp) {
        boolean ajout = false;
        if(verifierMdp(valMdp) && ancienMdp(valMdp)==false)
        {
                lesAnciensMdp.add(new MotDePasse(this.motDePasse, LocalDate.now()));
                this.motDePasse = valMdp;
                ajout = true;
        }
        return ajout;
}
```

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		Les deux tests de vérifications sont corrects, le mot de passe actuel est enregistré en tant qu'ancien mot de passe, le mot de passe actuel est modifié et la méthode retourne un booléen.
Bonne maîtrise		Il manque l'enregistrement du mot de passe actuel dans la collection des anciens mots de passe ou il est mal rédigé.
Maîtrise partielle		Les tests de vérifications sont incomplets ou manquants. Ou la méthode ne retourne pas de booléen.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Mission A3 – Validation de l'authentification

Question A3.1

Ajouter une méthode de test verifModifierMdp() pour compléter vos tests unitaires.

```
@Test
void verifModifierMdp() {
        assertFalse("mot de passe déjà utilisé auparavant il ne devrait pas être modifié",
unUtilisateur.modifierMdp("Lae99_Mat00!"));
        assertFalse("mdp ne correspond pas à la complexité",
unUtilisateur.modifierMdp("Mdp2023"));
        assertTrue("mot de passe non utilisé auparavant il devrait être modifié",
unUtilisateur.modifierMdp("Duv$54Foa67p"));
}
```

D'autres tests sur la complexité sont possibles, mais on en attend au moins un.

Compétence évaluée : Sécuriser les équipements et les usages des utilisateurs • Vérifier l'efficacité de la protection		
Excellente maîtrise		Réalisation de tests validant la complexité et l'utilisation d'un ancien mot de passe et d'un test validant la modification.
Bonne maîtrise		Il manque un ou deux tests de validation et/ou il manque l'entête.
Maîtrise partielle		Seul un test de validation est proposé.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question A3.2

Décrire un scénario de risque exploitant l'absence de restriction d'accès aux éléments du menu de l'application.

Un utilisateur malveillant (ou une personne extérieure à l'entreprise) effectue un traitement non autorisé par son habilitation.

Tout scénario cohérent sera accepté.

Compétence évaluée : Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face aux cyberattaques • Caractériser les risques liés à l'utilisation malveillante d'un service informatique		
Bonne maîtrise		Le scénario est cohérent.
Maîtrise partielle		Le scénario n'est pas précis.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question A3.3

a. Écrire le code de la méthode getNiveauHabilitation de la classe Utilisateur.

```
public int getNiveauHabilitation() {
        return this.sonHabilitation.getNiveau();
}
```

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		
Bonne maîtrise		Le code est fourni sans erreur.
Non maîtrisé		Le code possède une erreur.
Non évaluable		Non répondu.

Question A3.3

b. Compléter le code du constructeur de la classe AppliHoly.

```
public AppliHoly(Utilisateur unUtil) throws HeadlessException {
        …
        // seuls les menus ayant un niveau d'habilitation inférieur ou égal à celui de l'utilisateur connecté doivent être accessibles
        for(ElementMenu unEl : lesMenus)
        {
                if(unEl.getNiveauHabilitation() <= unUtil.getNiveauHabilitation())
                {
                        unEl.rendreAccessible();
                }
        }
}
```

On acceptera toute itérative (for, foreach, while, …) même issu d'autres langages que Java.

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		La collection d'éléments menu est correctement parcourue. La modification de l'accessibilité de l'élément menu est bien faite.
Bonne maîtrise		La condition du si ou l'accessibilité de l'élément menu possède une erreur.
Maîtrise partielle		Le code possède de nombreuses erreurs.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Dossier B – Intégrer « Happy Box » au système d'information initial

Mission B1 – Sécuriser les données personnelles

Question B1.1

Réaliser le tableau demandé par Mme Lenvy durant l'entretien.

	Données personnelles	Données sensibles
Désir d'Ailleurs	idcli, nom, prénom, dateNaiss, adresse, codePostal, ville, tél, mél, numPièceIdentité, pseudo	Booléen EstAMobilitéRéduite Relation vers Vaccin (table association Dernière injection) la date de la dernière injection
EchapBox	id, nom, prénom, dateNaiss, adresse, codePostal, ville, tél, mél, numPièceIdentité, pseudo	Il n'y en a pas

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		Toutes les données personnelles et sensibles des deux bases de données ont été énoncées. Le candidat a précisé qu'il n'existe pas de données sensibles dans la base EchapBox.
Bonne maîtrise		Toutes les données personnelles des deux bases de données ont été énoncées. Seule une donnée sensible a été énoncée.
Maîtrise partielle		Toutes les données personnelles et sensibles des deux bases de données n'ont pas été énoncées.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question B1.2

Écrire la requête permettant de modifier la table Client de la base de données de EchapBox.

ALTER TABLE EchapBox.Client ADD accordPubli boolean DEFAULT FALSE ;

On acceptera toute autre solution cohérente à la place de *boolean*.

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

Bonne maîtrise		La requête ne contient pas d'erreur
Maîtrise partielle		La requête contient une erreur
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question B1.3

Rédiger le corps du courriel destiné aux utilisateurs.

La forme d'un courriel n'est pas demandée ; il ne faut pas évaluer celle-ci.

Le courriel doit mentionner :

- l'adresse du formulaire ;
- la nature de la sollicitation – la demande de consentement,
- la description exacte du traitement envisagé et de ses finalités,
- la possibilité de ne pas répondre sans donner son accord pour autant,
- les droits des personnes (notamment droit de suppression des données à tout moment)

Compétence évaluée :

Protéger les données à caractère personnel

- Sensibiliser les utilisateurs à la protection des données à caractère personnel

Excellente maîtrise		Le message contient l'ensemble des éléments attendus.
Bonne maîtrise		Le message contient au moins 3 éléments attendus.
Maîtrise partielle		Le message contient 1 à 2 éléments attendus.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question B1.4

Proposer une solution détaillée permettant de conserver une trace du processus ainsi que l'intégrité de cette trace.

La solution doit proposer de conserver le formulaire de recueil du consentement (code de la page web) et une empreinte cryptographique (hash) de ce·s fichier·s éventuellement conservés dans une archive.

Non attendu : la datation précise de la mise à disposition du formulaire.

Compétence évaluée :

Préserver l'identité numérique de l'organisation

- Déployer les moyens appropriés de preuve électronique

Excellente maîtrise		La solution proposée reprend les 2 éléments du corrigé.
Bonne maîtrise		La solution proposée ne reprend qu'un seul élément du corrigé.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question B1.5

Donner la structure de la nouvelle table ClientAnonyme en utilisant le formalisme du document B2.

ClientAnonyme(numSeq, civilité, annéeNaissance, departement)
numSeq clé primaire

On acceptera tout identifiant qui ne permet pas de retrouver le client correspondant.
On pourra accepter :

- **une tranche d'âge à la place de l'année de naissance**
- **le code postal à la place du département**

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		La relation contient tous les éléments attendus.
Bonne maîtrise		Il manque un élément dans la relation, mais tous les autres sont bien définis.
Maîtrise partielle		La relation n'est pas correctement identifiée. Ou il reste des données trop précises.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Mission B2 – Détecter les agissements frauduleux

Question B2.1

Justifier le niveau de gravité affecté aux risques R1 et R2, en décrivant l'impact que ces risques pourraient avoir sur l'entreprise.

Les risques 1 et 2 ont un impact financier extrêmement grave pour l'entreprise, ce qui justifie le niveau 4 (maximal) affecté.
Complément : L'entreprise (ESN) qui ne met pas en place une protection correspondant à l'état de l'art, peut être attaquée par son client, ici, YAK. Yak pourrait perdre de l'argent par sa faute.

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

Bonne maîtrise		L'impact financier et le niveau de gravité sont justifiés.
Maîtrise partielle		Seul l'impact financier est énoncé sans relation avec le niveau de gravité.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question B2.2

Écrire la requête permettant de visualiser la liste des clients (id, nom et prénom) ayant un contrat avec un acompte versé supérieur ou égal au montant à payer.

```
SELECT idCli, nom, prenom
FROM Client
        JOIN Devis_Voyage ON Devis_Voyage.idCli = Client.idCli
        JOIN Contrat_Voyage ON Contrat_Voyage.idDevis = Devis_Voyage.idDevis
WHERE acompte >= montantapayer
```

On acceptera une requête qui dénombre le nombre de contrat par client répondant à la condition.

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

Excellente maîtrise		La requête ne contient pas d'erreur.
Bonne maîtrise		Tous les champs attendus ne sont pas affichés et/ou les jointures contiennent une erreur de syntaxe.
Maîtrise partielle		La condition n'est pas évaluée correctement et/ou il manque une jointure.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question B2.3

Terminer la rédaction du déclencheur (*trigger*) en ajoutant la vérification de cette règle métier.

```
SET @montant_minimum = 75*@nb_jours*NEW.nbParticipant;
IF NEW.montantapayer < @montant_minimum THEN
    SIGNAL SQLSTATE '10002' ;
    SET MESSAGE_TEXT = 'Le montant du contrat est inférieur au montant minimum autorisé pour ce voyage' ;
END IF;
```

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

Excellente maîtrise		Le montant minimum est bien calculé, la condition est correctement évaluée et l'erreur est gérée.
Bonne maîtrise		Le code est incomplet.
Maîtrise partielle		Le calcul du montant minimum n'est pas correct et la condition n'est pas correcte.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Dossier C – Amélioration de la sécurité des applications Web

Mission C1 – Vérifier la conformité de la protection de l'authentification

Question C1.1

Décrire le fonctionnement de la protection mise en place contre une attaque de type CSRF.

Lorsque l'utilisateur arrive sur le formulaire de modification de son mot de passe, on enregistre dans un champ caché du formulaire HTML le jeton contenu dans une variable de session.

Avant de réaliser un traitement on vérifie que les deux jetons existent et qu'ils sont identiques.

Cela permet de garantir la relation entre le navigateur et le serveur *Web*, l'utilisateur est bien à l'origine du traitement et non un pirate.

Compétence évaluée :

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

- Prévenir les attaques

Bonne maîtrise		La protection est décrite complètement.
Maîtrise partielle		La protection est décrite partiellement (par exemple : il manque l'enregistrement du jeton dans un champ caché du formulaire, …)
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Mission C2 – Analyse des fichiers de journalisation

Question C2.1

a. Identifier tous les événements présents dans l'extrait du fichier de journalisation de l'application *Désir d'Ailleurs* du 10/05/2023.

- En analysant le fichier de logs de l'application, on constate que l'utilisateur AllanG a effectué une tentative de connexion qui a échoué, puis s'est connecté correctement. (**Non attendu : Il semblerait qu'il ait saisi une mauvaise information**)
- De même une tentative est effectuée sans saisie des champs login et mot_de_passe.
- En revanche les autres logs sont plus suspects. Un nombre important de tentatives de connexion a lieu en une seconde.

Compétence évaluée :

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

- Analyser les connexions (logs)

Excellente maîtrise		Les trois événements ont été identifiés.
Bonne maîtrise		Il manque un événement.
Maîtrise partielle		Seul un événement a été identifié.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question C2.1

b. Émettre une hypothèse sur l'origine de l'événement qui attire votre attention dans une courte note à destination de votre responsable.

Il pourrait s'agir d'une attaque par force brute tentant d'identifier le mot de passe de l'utilisateur RichardP dont le login a probablement fuité.

Non attendu : Il faut, de manière urgente rester attentif à ces tentatives de connexion pour prendre des mesures si nécessaire, notamment désactiver ce compte compromis et fournir un compte alternatif à l'utilisateur authentique.

Compétence évaluée :

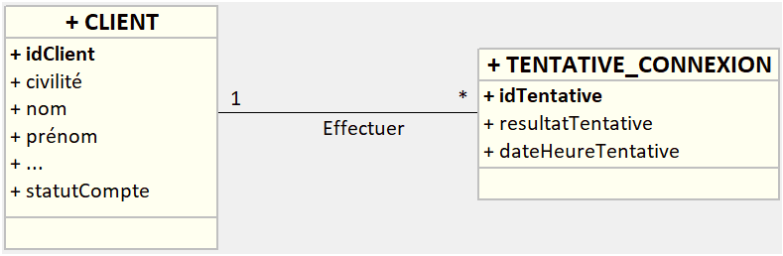
Assurer la cybersécurité d'une solution applicative et de son développement

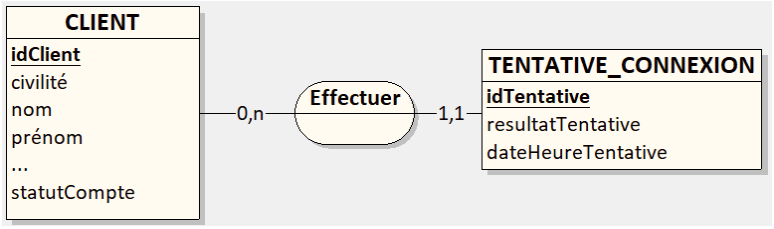
- Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures

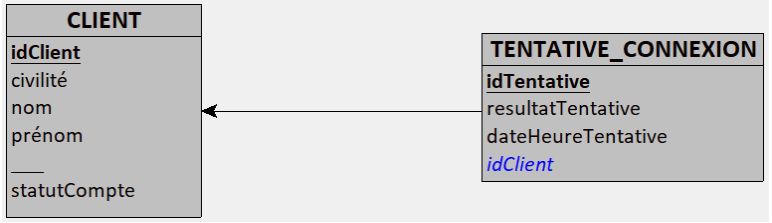
Bonne maîtrise		L'attaque par force brute est bien identifiée.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question C2.2

a. Proposer, dans le formalisme de votre choix, une évolution de la base de données permettant de répondre à cette demande.
b. Donner 2 enregistrements illustrant une tentative de connexion par un même utilisateur.







Une solution avec un identifiant relatif (idClient et horodatageTentative) sera acceptée en fonction de la cohérence avec la question C2.2b qui présentera un horodatage jusqu'à la milliseconde.

ÉVALUATION COMMUNE DES QUESTIONS A ET B.

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		La modélisation proposée répond à la demande et est en cohérence avec les exemples fournis.
Bonne maîtrise		La modélisation proposée ne répond que partiellement à la demande (incohérence ou pas d'exemple fourni).
Maîtrise partielle		Le candidat ne fournit que des exemples d'enregistrement répondant convenablement à la demande.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Question C2.3

Proposer et décrire, sans l'implémenter, une solution technique permettant de désactiver le compte.

Toute solution (applicative ou au niveau de la BdD) vérifiant qu'au bout d'un certain nombre de tentatives de connexions infructueuses successives, le compte soit désactivé.

Compétence évaluée : Sécuriser les équipements et les usages des utilisateurs • Identifier les menaces et mettre en œuvre les défenses appropriées		
Bonne maîtrise		La solution proposée est cohérente.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.