Présentation du contexte

La grotte de Lascaux, située à Montignac en Dordogne, est une grotte ornée du paléolithique, découverte en 1940. Elle fait partie du patrimoine mondial de l'Unesco depuis 1979.

Très vite, les scientifiques ont constaté que les visites humaines détérioraient les peintures, ce qui a conduit à fermer la grotte au public en 1963.

Le département de la Dordogne, l'Europe, l'État et la région Aquitaine Limousin Poitou-Charentes ont été à l'origine d'un grand projet d'envergure: le centre international de l'art pariétal Montignac-Lascaux (Ciap) qui a ouvert ses portes le 15 décembre 2016 sur le site de Lascaux.

Le Ciap, appelé également Lascaux IV, offre au public une réplique de la grotte de Lascaux en permettant aux visiteurs d'utiliser les technologies d'aujourd'hui pour personnaliser leur visite avant, pendant et après.

Le conseil départemental de la Dordogne a été nommé maître d'ouvrage de Lascaux IV.

Cette réplique de la grotte comporte une partie musée où le visiteur est en interaction permanente avec ce qu'il côtoie, grâce à l'utilisation d'une tablette appelée compagnon de visite (CDV). Mille six cents CDV en dix langues sont mis à la disposition des visiteurs.

Le CDV est connecté à un maillage de dispositifs Wi-Fi et *Bluetooth* du bâtiment composé de cinquante bornes Wi-Fi et de deux cents balises *Bluetooth* qui permettent au CDV de se localiser, de communiquer et aussi de se synchroniser avec les serveurs multimédias du Ciap. Des centaines de tablettes sont prêtées chaque jour pour permettre à chaque visiteur d'avoir une expérience numérique unique et personnalisée.

L'organisation cliente

Le Ciap dispose de plusieurs systèmes d'information (SI) internes,à savoir SI bâtimentaire, SI administratif (ressources humaines, comptabilité, etc.), SI visiteur et SI scénographie (écrans, vidéo projections, lumières, etc.). L'articulation de ces SI internes avec la billetterie en ligne, le site internet, l'application mégadonnées (*big data*) permet au Ciap la gestion de ce qu'il appelle l'expérience utilisateur.

Il peut y avoir cinq mille visiteurs par jour. Grâce à l'application tablette pour les CDV, le site internet, la plateforme d'échanges (MyLascaux),la solution mégadonnées (*big data*), il s'agit d'assurer un service très complet de gestion de la relation client avant, pendant et après la visite. Sur la partie après visite, plus d'un million de visiteurs peuvent se connecter.

Le SI administratif est exploité par trois personnes. Outre la gestion avec un progiciel de gestion intégré, il gère les employés (128 en haute saison en 2019 par exemple) avec un annuaire d'entreprise, ce dernier permettant de gérer les différents niveaux d'habilitations dans l'organisation.

La direction des systèmes d'information (DSI) du conseil départemental a lancé des appels d'offre dont un pour les outils numériques et multimédia et un pour les applications informatiques. Elle a expertisé les réponses, a donné aux prestataires retenus la stratégie numérique et un cadre de standards à respecter. Elle a fait et continue à faire le lien avec les utilisateurs.

Dix lots concernaient spécifiquement l'appel d'offrepour les outils numériques et multimédia (dont plusieurs liés aux CDV) et cinq portaient sur l'informatique. Quatre entreprises de services numériques (ESN) ont obtenu des lots de ces deux appels d'offre.

L'entreprise prestataire de services

L'ESN Aquilasc, éditeur de logiciels de gestion sur mesure de type client lourd, *Web* ou mobile et spécialisée dans le secteur du tourisme, a été retenue pour deux lots. Soucieuse de s'inscrire dans une vision durable et responsable de son activité, cette entreprise est labellisée entreprise numérique responsable(ENR) chaque année, et ce depuis 2012.

Le premier appel d'offre concerne l'application *Web* de la gestion des réservations de billets et de l'organisation des visites. Le deuxième appel d'offre porte sur l'application mobile permettant une visite interactive du musée avec le compagnon de visite (CDV).

Aquilasc est composée de 30 personnes et dispose d'un budget d'investissement de 1,2 million d'euros et d'un budget de fonctionnement de 1,7 million d'euros. Elle dispose de 4 serveurs pour ses activités ; un poste de travail et un mobile multifonction (*smartphone*)sont mis à disposition de chaque employé(e).

Depuis quatre ans, Aquilasc utilise la méthode agile *Scrum*pour la gestion de ses projets. Cette méthode permet d'impliquer l'organisationcliente durant la durée totale du projet et de lui livrer de manière régulière de nouvelles versions de l'application, avec leur lot de corrections et de nouvelles fonctionnalités, apportant ainsi de plus en plus de valeur métier à l'application.

Un contrat de prestation de services a été établi entre le conseil départemental de la Dordogne et Aquilasc. Il définit la nature des interventions de l'ESN, leurs durées et délais et établit les métriques selon lesquelles la prestation sera jugée finie et délivrée.

Vous faites partie de l'équipe *Scrum,* votre mission consiste à participer au développement des applications *Web* et mobile.

En mode agile, vous avez la charge d'analyser les spécifications techniques pour concevoir, développer et maintenir les logiciels. Les bases de données utilisées par les applications sur lesquelles vous allez intervenir sont gérées par le système de gestion de base de données (SGBD) *MySQL*.Vous testez et intégrez en continu les solutions développées.

Au sein de l'équipe technique, vous devrez :

- participer à l'atelier analyse de risques ;
- sécuriser des données ;
- gérer l'identification des utilisateurs ;
- préparer l'environnement de développement et piloter les sous-traitants.

Vous vous appuierez sur les dossiers documentaires mis à votre disposition.

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

Votre équipe est en charge du développement des nouvelles fonctionnalités de l'application *Web* permettant notamment la réservation et l'achat en ligne de billets de visite par des acheteurs (particulier, agence de voyages, comité d'entreprise, etc.). Une autre fonctionnalité attendue rapidement est la possibilité pour les visiteurs de créer un compte sur l'application *Web* MyLascaux après leur visite avec leur numéro de billet pour retrouver les données collectées par le compagnon de visite(CDV) lors de leur visite.

Votre équipe est en charge du développement de ces nouvelles fonctionnalités.

Mission A1 – Évaluation des risques à partir des récits utilisateurs

Votre administrateur *Scrum*(*ScrumMaster*), dont le rôle est de veiller à ce que l'équipe respecte les règles de la méthode *Scrum*, vous demande de participer à un atelier d'analyse de risque au sein de l'équipe de développement afin d'évaluer les risques sur les récits utilisateurs (*user stories*) qui ont été planifiées pour la première itération de développement (*sprint* 1).

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

Le tableau « Besoins de sécurité pour les récits utilisateurs (*user stories*) » propose pour chaque récit de l'itération (*sprint*) une évaluation du besoin de disponibilité, d'intégrité et de confidentialité des données manipulées et la nécessité d'éléments de traçabilité faisant office de preuve. L'évaluation des récits utilisateurs(*user stories*)n'a pas été finalisée.

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

Sachant que vous avez suivi une formation en BTS SIO, Christine Berton, la responsable de produit (*Product Owner*),vous demande quelles sont les conditions pour que les éléments de traçabilité puissent servir de preuve en cas de contentieux avec un acheteur.

Question A1.3
Présenter ces conditions à Christine Berton.

Mission A2 – Gestion des événements redoutés

Le tableau « Impacts des événements redoutés » permet de définir l'impact et la gravité en terme de sécurité des événements liés à des actes de malveillance pour l'entreprise.

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.

Pour l'instant, le tableau « Scénarios de risque et mesures à prévoir » du dossier documentaire contient les mesures à appliquer pour contrer l'événement redouté numéro 2.

Christine Berton a identifié un événement redouté numéro 4concernant le récit utilisateur (*user story*)numéro 2 qui porte sur l'impression des billets au format PDF (*Portable Document Format*).

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

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

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

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

Question A.3.1
Lister pour chacun des récits utilisateurs (*user stories*)numérotés 22 et 25, les actions à mettre en œuvre pour respecter le RGPD.

Christine Berton vous demande d'ajouter un nouveau récit utilisateur (*user story*): "En tant que visiteur, je veux être déconnecté du site lorsque je ferme mon navigateur ou à l'issue d'une période d'inactivité fixée".

Question A.3.2
Expliquer quel risque de sécurité vient contrer cet ajout.

Dossier B – Sécurisation des données

La réservation des billets est possible sur internet : un acheteur (particulier, agence de voyages, comité d'entreprise, etc.) peut réserveren indiquant à quel moment il souhaite venir et les personnes qui participeront à cette visite.

Le jour de la visite, un guide prend en charge tout le groupe et réalise la visite. À la fin de la visite, chaque personne en possession d'un billet peut déposer des commentaires sur le déroulé de la visite.

Le module réservation des billets en ligne est en cours de développement. L'équipe que vous avez rejointe est en phase de test des récits utilisateurs (*user stories*) pris en charge au cours de la première itération (*sprint* 1).

Mission B1 – Vérification de la confidentialité des données

Denise Bradord intervient à la fin de chaque itération (*sprint*) pour validerla qualité du produit avant la livraison. Les tests qu'elle vient de réaliser ont mis en évidence des problèmes de confidentialité au niveau :

- de la table qui contient les caractéristiques des acheteurs ayant réalisé une réservation ;
- de l'implémentation du récit utilisateur (*user story*) n° 5 : celui-ci permet aux acheteurs de consulter leurs réservations réalisées pour des seniors durant un mois précis.

Elle vous a adressé un courriel pour vous informer des problèmes rencontrés sur le récit utilisateur (*user story*) n° 5.

Denise Bradord vous confie la résolution deces problèmes.

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

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.

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

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

Suite à votre intervention, les fonctionnalités développées lors de la première itération (s*print*) viennent d'être intégrées en production.

La fonctionnalité permettant au service commercial de visualiser les commentaires laissés suite aux visites doit être développée lors la deuxième itération (*sprint 2*). En attendant, une de vos collègues Pierrette Lesoil doit transmettre à ce service le résultat d'une requête exécutée directement sur la base de données de production. Cette requête permet d'obtenir le libellé de la catégorie d'âge du visiteur, la date de la visite ainsi que les commentaires laissés par le visiteur.

Pour des raisons de sécurité, un compte utilisateur *lesoil* destiné à Pierrette Lesoil doit être créé pour accéder à la base de production *lascauxprod*. Pierrette Lesoil ne pourra accéder à la base de production qu'à partir du poste ayant l'adresse IP 172.16.2.1 et ne pourra consulter que les tables utilisées par la requête.

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

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

Lors d'une réunion quotidienne (*Daily Meeting*),Denise Bradord vous fait remarquer qu'il serait plus judicieux d'utiliser une vue pour réaliser cette requête.

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

Chaque visiteur peut, suite à sa visite, déposer plusieurs commentaires à partir de l'application *Web*. Le service commercial a un rôle de modérateur de ces commentaires : il peut choisir de les publier ou non. Par ailleurs, il peut éventuellement répondre aux clients.

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

Les commerciaux viennent de constater que le nombre de commentaires à traiter a très fortement augmenté, de manière inexplicable.

Roger Zanches, responsable du service commercial, ne voudrait pas que certains commentaires proviennent d'une personne malveillante.

Il vous demande de vérifier s'il existe des commentaires qui ne seraient pas reliés à un billet.

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

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

IMPORTANT : la candidate ou le candidat peut retenir le formalisme de son choix (schéma entité-association, diagramme de classes)pour représenter les évolutions conceptuelles demandées

La deuxième itération (*sprint 2*) nécessite de faire évoluer la représentation conceptuelle de la base de données.

Christine Berton, la responsable de produit (*Product Owner*), a constaté que les commentaires sur le niveau de langue des guides étaient parfois inappropriés, voire insultants, pour certains guides. Étant donné que l'article 12 du RGPD indique que toute personne physique peut exercer son droit d'accès aux données qui la concernent, elle vous demande d'adapter la base de données pour prendre en compte l'article 6 de la loi «Informatique et Libertés» qui prévoit que les informations collectées doivent être adéquates, pertinentes et non excessives au regard de la finalité poursuivie.

Par ailleurs, le délégué à la protection des données (DPO) vous demande :

- d'appliquer certaines règles de sécurité pour la gestion des mots de passe des acheteurs ;
- de proposer une mise en conformité de la structure de la base de données d'après la fiche de registre relative au traitement de réservation des billets qu'il a complétée.

En respectant les consignes de Christine Berton et du DPO, détaillées dans le dossier documentaire, vous devez faire évoluer 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.

Question B.3.2
Proposerles 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.

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

IMPORTANT : la candidate ou le candidat peut choisir de présenter les éléments de code à l'aide du langage de programmation de son choix ou de pseudo-code algorithmique.

Une nouvelle itération (*sprint*) commence ; vous êtes maintenant en charge du développement de l'authentification des utilisateurs sur les compagnons de visite (CDV). Ces tablettes peuvent être utilisées par n'importe quel visiteur ou guide accompagnateur. Vous reprenez le travail effectué par votre prédécesseur lors de l'itération précédente et pouvez prendre connaissance de l'architecture logicielle utilisée en consultant le document C2.

Mission C1 – Identification des visiteurs

Dès le départ de la visite, le guide remet un CDV à chaque visiteur et l'invite à scanner le code QR (*QrCode)* placé sur son billet. Le visiteur sera ainsi identifié. L'objectif de cette identification est de proposer au visiteur des fonctionnalités différentes selon sa catégorie d'âge, par exemple un contexte ludique pour les enfants. L'application d'identification a été partiellement réalisée en *Java*.

Principe de fonctionnement:

La tablette établit, en Wi-Fi, des connexions avec un serveur par le biais de requêtes suivant le protocole de transfert hypertexte (*Hypertext Transfer Protocol - HTTP*). Ces dernières déclenchent l'exécution de scripts (en langage *PHP*) qui interrogent le serveur de base de données. Les résultats récupérés seront convertis au format de notation des objets en *JavaScript* (*JavaScript Object Notation - Json*) et renvoyés à la tablette.

Évolutions envisagées **:**

- vérification de la logique du code et des possibilités d'attaques par injection de code lors de l'utilisation des variables $_POST, $_GET, $_COOKIE ;
- évolution du script *getVisiteur.php* par l'utilisation d'une requête préparée.

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

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

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

Mission C2 – Authentification desguides

Les guides utilisent également un compagnon de visite (CDV) pour gérer leurs visites. Ils ont un code QR (*QrCode)* spécifique qui leur donne un accès à d'autres fonctionnalités sensibles interdites aux simples visiteurs. L'identification du guide est complétée par la saisie d'un mot de passe.

Principe actuel de fonctionnement du changement de mot de passe :

Lors de sa première connexion, un guide doit obligatoirement modifier le mot de passe qui lui a été attribué par défaut. Par la suite, il peut changer son mot de passe lorsqu'il le désire.

La date de création d'un mot de passe est conservée conjointement au mot de passe (classe MotDePasse). À chaque changement de mot de passe, l'application vérifie que le nouveau mot de passe n'est pas identique à l'ancien et, si ce n'est pas le cas, le changement est validé et l'ancien mot de passe est ajouté à la liste des anciens mots de passe du guide.

La fonctionnalité de changement du mot de passe doit être améliorée lors de cette nouvelle itération(*sprint*).

Évolutions envisagées :

Lors de la connexion sur le CDV, le guide sera invité à changer son mot de passe si celui-ci date de plus de trois mois. Une méthode *doitChangerMdp()*vérifiera la date de validité du mot de passe et retournera un booléen contenant « vrai » si le mot de passe doit être changé, « faux » sinon.

Par ailleurs, la méthode s*etMotDePasse()*, utilisée pour changer le mot de passe, doit être modifiée : le nouveau mot de passe ne doit pas être identique à l'ancien, ni même à l'un des mots de passe utilisés par le guide durant les douze derniers mois.

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

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*).

Le délégué à la protection des données (DPO) s'interroge sur la pertinence de la durée de recherche de l'historicité du mot passe à 12 mois.

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

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

L'itération zéro (*sprint 0*) prépare le développement en précisant, pour toute l'équipe, les points suivants : les objectifs du client, le périmètre de l'application, les contraintes, les intervenants dans le projet, les utilisateurs finaux, la modélisation du domaine métier, l'architecture technique, le mode de travail sur le projet, le budget, le planning global, la gestion des sous-traitants, etc.

C'est un moment privilégié pour l'équipe qui va apprendre à se connaître et à travailler ensemble. Cette itération n'apporte pas de valeur immédiate ; elle ne se termine pas forcément par une livraison.

Mission D1 – Rejet des mauvaises pratiques de développement

Des propositions pour le mode de travail sur le projet ont été émises par les différents participants lors de cette itération zéro (*sprint 0*). Elles sont dans le dossier documentaire.

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.

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

La gestion des compagnons de visite (CDV), sur lesquelles l'application de visite sera déployée, appartient au périmètre du projet.

Il a été décidé de sous-traiter la gérance du parc des CDV auprès d'une société spécialisée dans la gestion de parcs mobiles.

Le contrat passé avec cette société devra inclure des règles de sécurité liées aux accès et aux données.

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