BTS SIO – ÉPREUVE E6 SLAM - SUJET ZÉRO

CAS Lascaux IV

**Dossier documentaire**

[Documents associés au dossier A 18](#_Toc41659320)

[Document A1 : Besoins de sécurité pour les récits utilisateurs (*user stories*) de la première itération de l’application gestion des billets et des visites sur le site *Web* (extraits) 18](#_Toc41659321)

[Document A2 : Extrait de l’analyse des risques et menaces de l’environnement 19](#_Toc41659322)

[Documents associés au dossier B 20](#_Toc41659323)

[Document B1 : Récit utilisateur (*user story*) n°1 "Achat des billets en ligne" 20](#_Toc41659324)

[Document B2 : Représentation conceptuelle de la base de données 20](#_Toc41659325)

[Document B3 : Extrait du schéma relationnel de la base de données utile aux missions 1 et 2 21](#_Toc41659326)

[Document B4 : Contenu de la table Acheteur 22](#_Toc41659327)

[Document B5 : Mél de Denise Bradord relatif au test du récit utilisateur (*user story*) n° 5 23](#_Toc41659328)

[Document B6 : Syntaxe *MySQL* (extrait du manuel de référence de *MySQL* 8.0) 24](#_Toc41659329)

[Document B7 : Évolutions demandées par la responsable de produit (*Product Owner*) et le délégué à la protection des données (DPO) 25](#_Toc41659330)

[Document B8 : Fiche de registre établie par le délégué à la protection des données pour le traitement réservation de billet 26](#_Toc41659331)

[Documents associés au dossier C 27](#_Toc41659332)

[Document C1 : Exemple de billet produit après une réservation. 27](#_Toc41659333)

[Document C2 : Architecture et arborescence de l’application d’identification. 27](#_Toc41659334)

[Document C3 : Diagramme de classes partiel de la partie identification 28](#_Toc41659335)

[Document C4 : Diagramme de séquence de l’identification d’un visiteur par le code QR (*QRCode*) sur le compagnon de visite (CDV) 28](#_Toc41659336)

[Document C5 : Codes partiels de l’application d’identification des visiteurs : appel au service *Web*. 29](#_Toc41659337)

[Document C6 : Codes partiels de l’application d’authentification : gestion des mots de passe du guide. 32](#_Toc41659338)

[Document C7 : Scripts *PHP* de la phase d'identification du visiteur 34](#_Toc41659339)

[Document C8 : Extrait du schéma relationnel exploité par le script *getVisiteur.php* 34](#_Toc41659340)

[Document C9 : Exemple de création d'une requête préparée 35](#_Toc41659341)

[Document C10 : Descriptif classe ArrayList 35](#_Toc41659342)

[Document C11 : Documentation partielle de la classe LocalDate en *Java* 36](#_Toc41659343)

[Document C12 : Filtrage des données externes (extrait d’une formation) 36](#_Toc41659344)

[Documents associés au dossier D 37](#_Toc41659345)

[Document D1 : Liste de propositions émises lors de l’itération zéro (*sprint* 0) 37](#_Toc41659346)

[Document D2 : Risques cyber liés aux prestataires et aux sous-traitants et préconisations de la direction générale de la sécurité intérieure (DGSI) 37](#_Toc41659347)

**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, vidéoprojections, 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’offre pour 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’organisation cliente 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 – Participation à 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* (*Scrum* *Master*), 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 les acteurs 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 4 concernant 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 réserver en 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 valider la 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 de ces problèmes.

**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.

**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 – Sécurisation de 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**

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.

**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 scanner un billet trouvé par terre ou dans une poubelle et ainsi effectuer une visite avec un billet déjà utilisé.

**Mission C2 – Authentification des guides**

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.

Documents associés au dossier A

Document A1 : Besoins de sécurité pour les récits utilisateurs (user stories) de la première itération de l’application gestion des billets et des visites sur le site Web (extraits)

|  | Intitulé du récit utilisateur (*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. | |  |  | |  |  |
| 2 | En tant qu’acheteur, je veux télécharger les billets d’une de mes réservations au format *PDF* afin de les transmettre aux personnes pour lesquelles j’ai réalisé la réservation. | | *\*\** | *\*\** | | *\** | *-* |
| 5 | En tant qu’acheteur, je veux consulter les caractéristiques des seniors pour lesquels j’ai acheté un billet sur un mois donné afin de réaliser une campagne publicitaire. | | *-* | *\** | | *\*\** | *-* |
| 15 | En tant que visiteur, je veux poster un commentaire afin de donner mon avis sur la qualité de la visite organisée. | | *\** | *\*\** | | *-* | *\** |
| 22 | En tant que visiteur, je peux créer, à l’issue de ma visite, un compte afin de retrouver sur le site *Web* les photos, vidéos et expériences effectuées sur le CDV. | | *\** | *\*\** | | *\*\** | *\** |
| 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. | |  |  | |  |  |
| 27 | En tant que visiteur, je veux être déconnecté du site lorsque je clique sur le bouton déconnexion afin de ne plus être identifié. | | *\*\** | *\** | | *-* | - |
| 30 | En tant que guide, je veux modifier mon mot de passe sur l’application mobile en toute sécurité afin de sécuriser mon compte. | | \* | \*\* | | \*\* | \* |
| *- : pas de besoin* | | *\* : besoin important* | | | *\*\* : besoin très important* | | |

Disponibilité : la fonctionnalité doit être utilisée au moment voulu.

Intégrité : les données doivent être exactes et complètes.

Confidentialité : les informations ne doivent pas être divulguées.

Preuve : les traces de l’activité du système sont opposables en cas de contestation.

Document A2 : Extrait de l’analyse des risques et menaces de l’environnement

**Acteurs à l’origine de la malveillance**

|  |  |  |
| --- | --- | --- |
| Acteurs malveillants | Modes opératoires | Probabilité |
| Attaquant externe (*hacker*) | L’attaquant externe accède à la base de données. | **\*\*** |
| L’attaquant externe surcharge le système. | **\*\*\*** |
| Acheteur | L’acheteur envoie de fausses informations. | **\*\*** |
| L’acheteur surcharge le système. | **\*** |
| Visiteur | Le visiteur envoie de fausses informations. | **\*** |
| Le visiteur surcharge le système. | **\*** |

*\* : faible probabilité \*\* : forte \*\*\* : très forte probabilité*

**Impacts des événements redoutés**

|  |  |  |  |
| --- | --- | --- | --- |
| Numéro de l'événement | Événement | Impact pour l’entreprise | Gravité |
| 1 | Le système ne répond pas. |  |  |
| 2 | Un attaquant accède à la base de données et ajoute des enregistrements dans la table billet. | Perte financière pour l’entreprise. | \*\* |
| 3 | Un attaquant accède à la base de données et modifie l’affectation des guides aux visites. |  |  |
| 4 | Un acheteur accède aux billets au format *PDF* d’un autre acheteur en modifiant le numéro de réservation dans la barre d’adresse. | Problème de confiance. Désorganisation des visites | \* |

*\* : modérée \*\* : très élevée*

**Scénarios de risques (*abuser story*) et mesures à prévoir**

|  |  |  |
| --- | --- | --- |
| Numéro de l'événement | scénario de risque (*abuser story*) | Mesures à prévoir |
| 2 | En tant qu’attaquant externe, je peux ajouter des billets dans la base de données. | 2.1 Tout billet doit être obligatoirement associé à une réservation. |
| 2.2 Interdiction d’avoir deux fois le même code QR dans la table billet. |
| 2.3 Lister et contrôler le nombre de billets existants par nom et prénom de visiteur |
| 4 | En tant qu’acheteur, je peux imprimer les billets d’un autre acheteur. |  |

Documents associés au dossier B

Document B1 : Récit utilisateur (user story) n°1 "Achat des billets en ligne"

Titre : Achat des billets en ligne Valeur Métier : 15

Objectif : En tant qu’acheteur, je veux acheter en ligne les billets pour plusieurs personnes afin de pouvoir participer à une visite guidée.

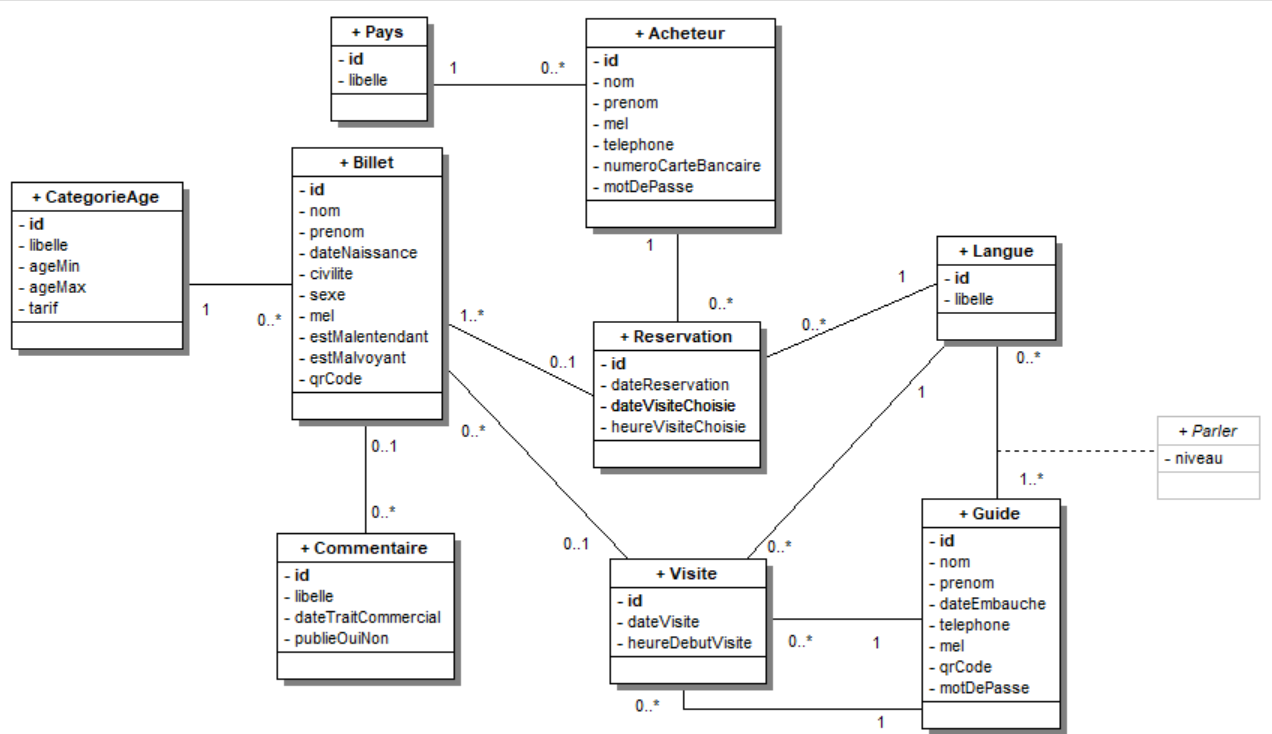
Rattachement : itération (*sprint*) n°1

Critères d’acceptation:

* Pour réserver des billets sur internet, une personne (appelée acheteur) devra créer un compte en fournissant son adresse mél qui sera utilisée comme identifiant, et un mot de passe.
* Une fois connecté, l’acheteur obtiendra un premier formulaire lui proposant de renseigner les informations utiles à la réservation de billets : son nom, son prénom, son mél, son numéro de téléphone. Puis, il devra choisir la date et l’heure souhaitées pour la visite, la langue dans laquelle il souhaite que la visite se déroule et le nombre de billets désirés.
* Ensuite, pour chacun des billets qu’il souhaite réserver, un deuxième formulaire de saisie lui demandera de fournir, pour chaque personne destinatrice d’un billet : son nom, son prénom, sa civilité, son sexe, son adresse mél, si elle est ou non malentendante, si elle est ou non malvoyante et sa date de naissance. La date de naissance est utilisée uniquement pour déterminer la tranche d’âge de la personne ; elle est déterminante pour connaître le tarif du billet. La connaissance du/des handicaps (malentendance, malvoyance) du visiteur permettra de lui préparer un compagnon de visite adapté.
* Suite à la validation des données saisies, l’acheteur est invité à saisir ses données bancaires. Un paiement sécurisé est effectué.

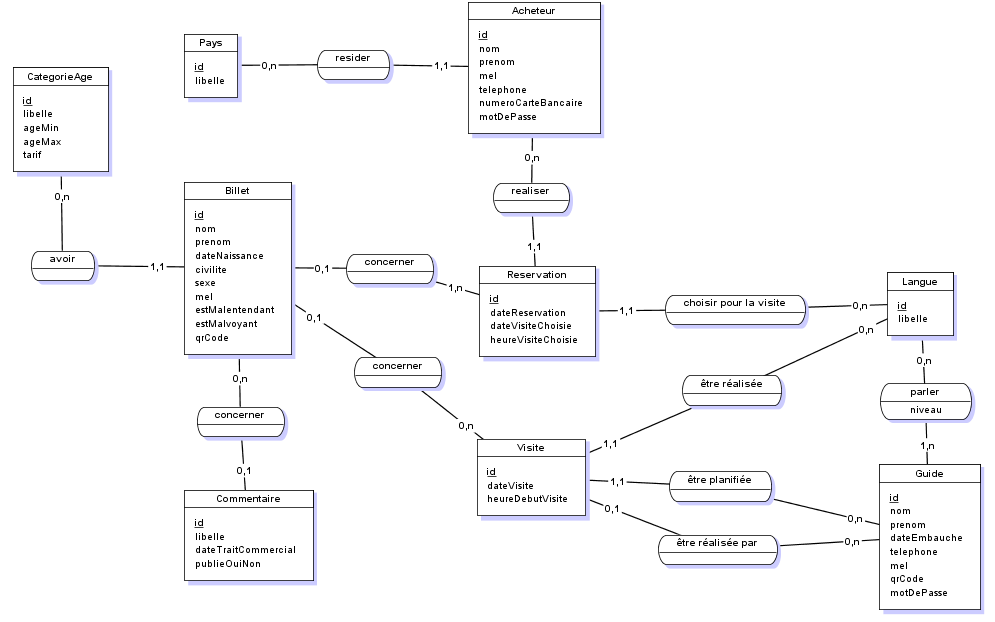
Document B2 : Représentation conceptuelle de la base de données

Représentation conceptuelle de la base de données avec un diagramme UML :



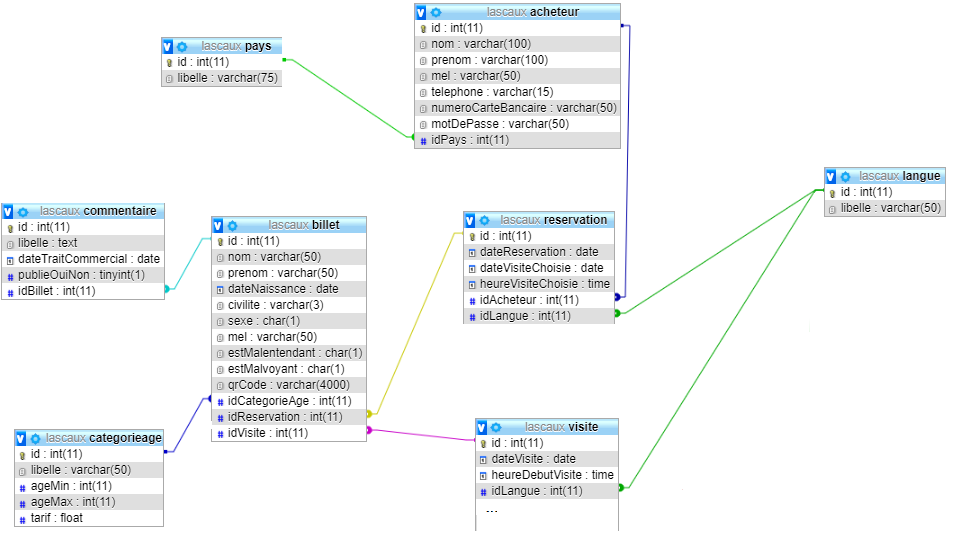
*Remarque : les attributs nommés ‘id’ sont des identifiants*

Représentation conceptuelle de la base de données avec un schéma entité-association :



Document B3 : Extrait du schéma relationnel de la base de données utile aux missions 1 et 2

Extrait du schéma relationnel sous forme graphique :



Extrait du schéma relationnel sous forme textuelle :

**Pays** (id, libelle)

Clé primaire : id

**CategorieAge** (id, libelle, ageMin , ageMax, tarif)

Clé primaire : id

**Langue** (id, libelle)

Clé primaire : id

**Acheteur** (id, nom, prenom, mel, telephone, numeroCarteBancaire, motDePasse, idPays)

Clé primaire : id

Clé étrangère : idPays en référence à id de Pays

**Reservation** (id, dateReservation, dateVisiteChoisie,heureVisiteChoisie, idAcheteur, idLangue)

Clé primaire : id

Clés étrangères : idAcheteur en référence à id de Acheteur

idLangue en référence à id de Langue

**Visite** (id, dateVisite, heureDebutVisite, idLangue, ...)

Clé primaire : id

Clés étrangères : idLangue en référence à id de Langue

…

**Billet** (id, nom, prenom, dateNaissance, civilite, sexe, mel, estMalentendant, estMalvoyant, qrCode, idCategorieAge, idReservation, idVisite)

Clé primaire: id

Clés étrangères : idCategorieAge en référence à id de CategorieAge

idReservation en référence à id de Reservation

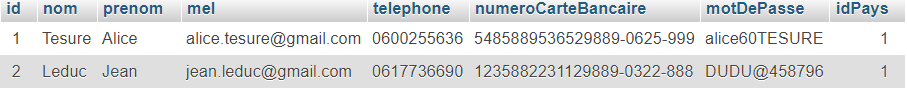
idVisite en référence à id de Visite

**Commentaire** (id, libelle, dateTraitCommercial, publieOuiNon, idBillet)

Clé primaire : id

Clé étrangère : idBillet en référence à id de Billet

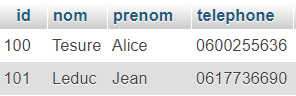
Document B4 : Contenu de la table Acheteur



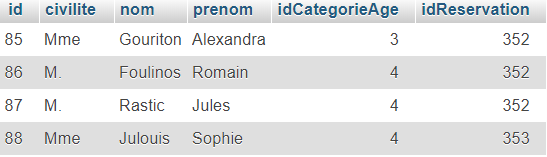
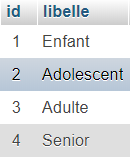
Document B5 : Mél de Denise Bradord relatif au test du récit utilisateur (user story) n° 5

Bonjour,

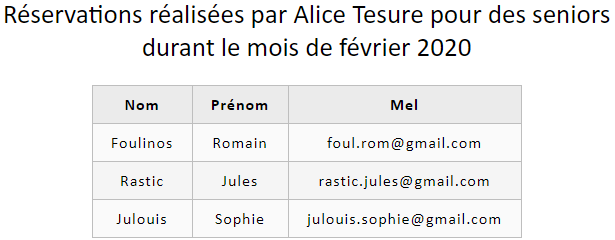
Je viens de tester la fonctionnalité décrite dans le récit utilisateur (*user story*) n° 5 qui permet à l’acheteur connecté de visualiser le nom, le prénom et l’adresse mél des séniors pour lesquels il a réalisé des réservations sur un mois et une année sélectionnés.

Afin de tester cette fonctionnalité, j’ai créé deux comptes acheteur : le premier au nom d’Alice Tesure, le deuxième au nom de Jean Leduc. Voici un extrait des caractéristiques de ces deux comptes :

J’ai ensuite saisi deux réservations sur le mois de février 2020 : la première avec le compte d’Alice Tesure et la deuxième avec celui de Jean Leduc :

Puis, j’ai renseigné les caractéristiques des personnes associées aux réservations comme ceci :

Pour rappel, voici les enregistrements existants dans la table CategorieAge :

Connectée avec le compte d’Alice Tesure, j’ai demandé la liste des caractéristiques des réservations réalisées pour les seniors durant le mois de février 2020 et voici ce que j’ai obtenu :

Comme tu peux le constater, Alice Tesure visualise une réservation réalisée par un autre acheteur, alors qu’elle ne devrait pouvoir consulter que ses propres réservations.

Les données affichées proviennent de la requête SQL paramétrée suivante qui est responsable de ce problème de confidentialité :

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

Peux-tu corriger cette requête pour régler le problème de confidentialité que je t’ai soumis ?

Par ailleurs, peux-tu optimiser la requête pour éviter qu’elle ne consomme des ressources inutiles ?

Bon courage !

Cordialement

Denise Bradord.

Document B6 : Syntaxe MySQL (extrait du manuel de référence de MySQL 8.0)

L’instruction CREATE USER permet la création d’un nouveau compte utilisateur sur *MySQL*. Pour chaque compte, cette instruction crée une nouvelle ligne dans la table système *mysql.user*.

Format général de l’instruction CREATE USER :

*CREATE USER*  *'nom\_de\_compte'* IDENTIFIED BY *'password'*;

*nom\_de\_compte* respecte la syntaxe suivante 'user\_name'@'host\_name' où le ‘user\_name’ est le nom de l’utilisateur et le 'host\_name' est l’adresse IP de la machine. Un nom de compte composé uniquement d’un nom d’utilisateur est équivalent à 'user\_name'@'%'.

Un compte créé pour la première fois n’a pas de privilèges et pas rôle par défaut. Pour attribuer des privilèges ou des rôles, il faudra utiliser l’instruction GRANT.

Format général de l’instruction GRANT :

*GRANT priv\_type [(column\_list)][, priv\_type [(column\_list)]] …*

*ON [object\_type] priv\_level*

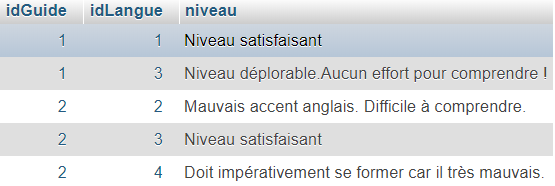
*TO user\_or\_role [, user\_or\_role] ...*

*priv\_type* contient les privilèges attribués. Les valeurs autorisées sont : ALTER, CREATE VIEW, CREATE, DELETE, DROP, GRANT OPTION, INDEX, INSERT, SELECT, SHOW VIEW, TRIGGER et UPDATE et ALL

*ON*  contient le nom de la base de données suivi du nom de la table : db\_name.tbl\_name

*TO*  contient le nom du compte

Document B7 : Évolutions demandées par [la responsable de produit (Product Owner) et le délégué à la protection des données](#_tt21a5954py3) (DPO)

Appréciation du niveau linguistique des guides

Lors de la première itération (*sprint*), une employée du service administratif a porté une appréciation sur le niveau de chaque langue parlée par un guide. Voici ci-contre un extrait des appréciations enregistrées dans la table LangueParlee.

Au regard des valeurs saisies, la responsable de produit (PO) souhaite que le niveau de langue ne soit plus un texte libre, mais qu’il soit sélectionné dans une liste déroulante dont les valeurs seront gérées via une fonctionnalité de l’application développée dans une prochaine itération (*sprint*).

Authentification et renouvellement des mots de passe

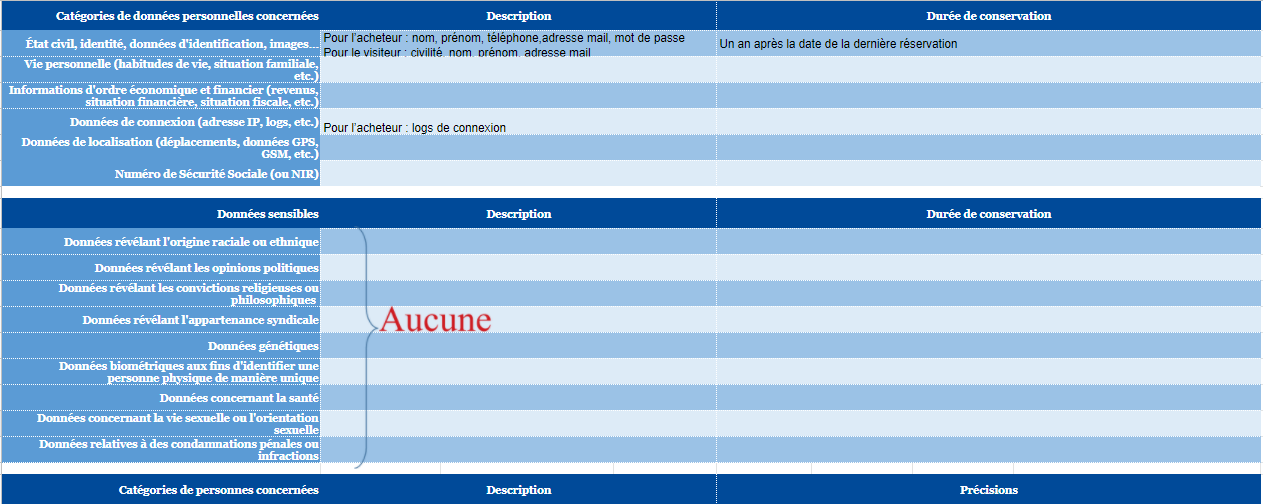
Pour des raisons de sécurité, le compte d’un acheteur doit être verrouillé après quatre échecs de connexion. Par ailleurs, les acheteurs devront changer leur mot de passe tous les quinze jours : le nouveau mot de passe choisi ne devra pas avoir déjà été utilisé par l’acheteur.

Les données sensibles

La connaissance du/des handicaps du visiteur (malentendance, malvoyance) permet de lui préparer un compagnon de visite (CDV) adapté. Lors de la première itération (*sprint*), ces indications ont été enregistrées à tort dans la base de données. Le délégué à la protection des données (DPO) vous demande de retirer ces informations sensibles et de proposer un moyen d’enregistrer pour le visiteur les caractéristiques du CDV à préparer. Plusieurs caractéristiques sont possibles :

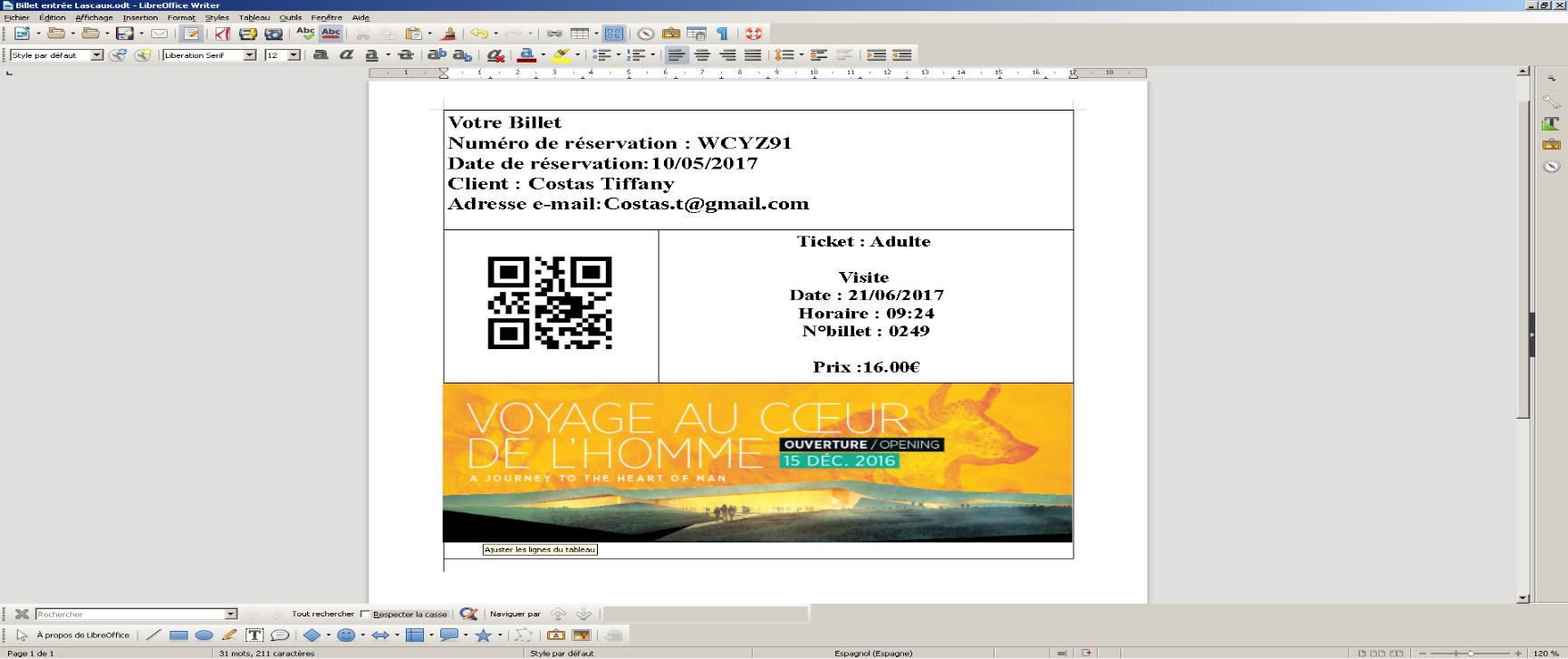
* 1 : taille de la police de caractères moyenne ;
* 2 : taille de la police de caractères grande ;
* 3 : volume sonore élevé ;
* 4 : CDV clavier braille.

Document B8 : Fiche de registre établie par le délégué à la protection des données pour le traitement réservation de billet



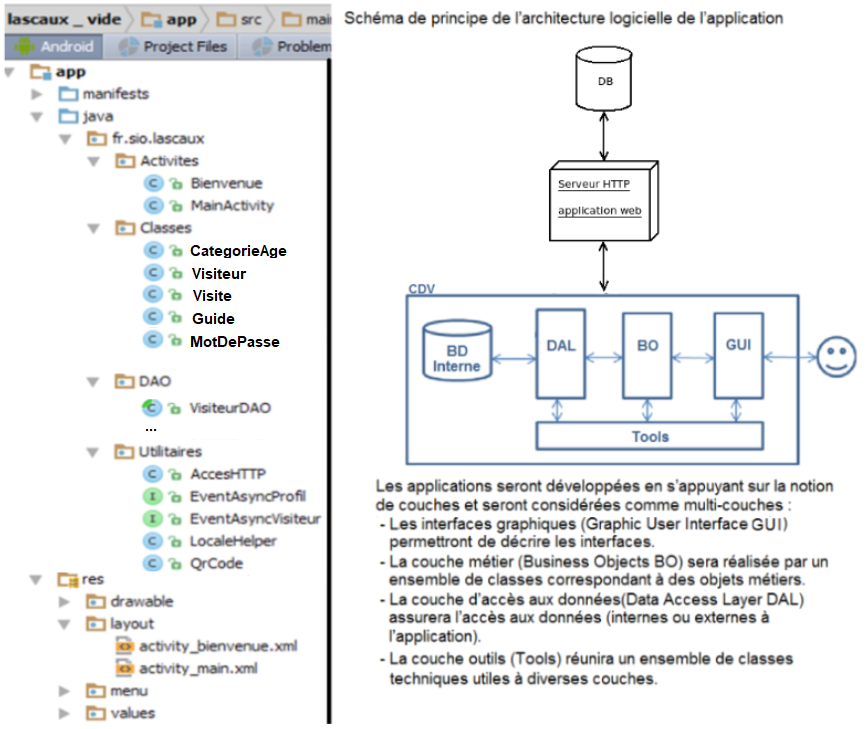
Documents associés au dossier C

Document C1 : Exemple de billet produit après une réservation.

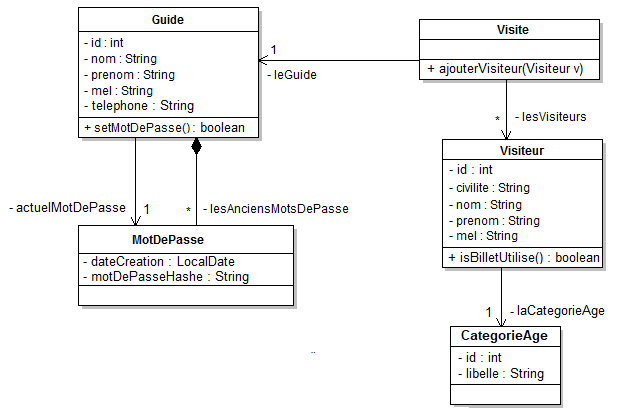


Ce billet a été attribué pour un adulte identifiable via le code QR (*QrCode)* figurant sur le billet. Le flashage de ce dernier permettra de déterminer l’identité du visiteur.

Document C2 : Architecture et arborescence de l’application d’identification.

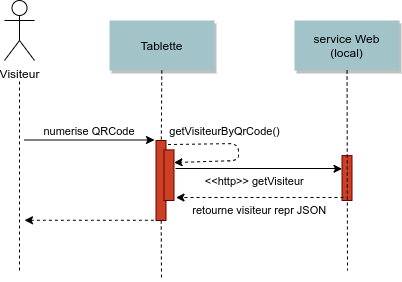


Document C3 : Diagramme de classes partiel de la partie identification



**Remarque :** les accesseurs de l’ensemble des attributs ne sont pas représentés sur le diagramme.

Document C4 : Diagramme de séquence de l’identification d’un visiteur par le code QR (QRCode) sur le compagnon de visite (CDV)



Document C5 : Codes partiels de l’application d’identification des visiteurs : appel au service Web.

*MainActivity.java*

|  |
| --- |
| */\*\**  *\* Classe principale de l’application du CDV*  *\*/*  public class MainActivity extends Activity {  private Button btnIdentifier;  private QrCode unQrCode;  private Visiteur leVisiteur;  private Visite laVisite;  */\*\**  *\* Initialise l’activité avec le français comme langue par défaut.*  *\* @param savedInstanceState l’instance en cours*  *\*/*  *@*Override  protected void onCreate(Bundle savedInstanceState) {  super.onCreate(savedInstanceState);  Context context = LocaleHelper.setLocale(this, "fr");  Resources resources = context.getResources();  setContentView(R.layout.activity\_main);  btnIdentifier = (Button) findViewById(R.id.buttonidentifier);  btnIdentifier.setOnClickListener(new View.OnClickListener() {  */\*\**  *\* Gère l’événement clic sur l’activité.*  *\* Récupère la valeur du code QR de la vue*  *\* puis appelle identifierUtilisateur.*  *\* @param v la vue de l’activité*  *\*/*  @Override  public void onClick(View v) {  String idQrCode;  unQrCode = new QrCode(); *// lit le code QR sur la vue v*  idQrCode = unQrCode.getIdentifiant();  identifierUtilisateur(idQrCode);  }  });  }  */\*\**  *\* Construit le Visiteur à partir du code QR scanné*  *\* Initialise le connecteur à la base de données distante*  *\* @param idQrCode le code QR du billet scanné*  *\*/*  private void identifierUtilisateur(String idQrCode)**{**  …  *// partie traitant des visiteurs*  */\*\**  *\* Recueille les informations nom, prenom, civilite du visiteur et construit leVisiteur*  *\*/*  VisiteurDAO visiteurAcces = new VisiteurDAO(){  @Override  public void onTacheTerminee(Visiteur resultat) {  *// une fois la tâche terminée le visiteur est accessible*  this.leVisiteur = resultat;  if (this.leVisiteur != null) {  *// la visite ‘laVisite’* *a été initialisée préalablement*  this.laVisite.ajouterVisiteur(this.leVisiteur);  *// transmission à l'activité Bienvenue du visiteur identifié*  Intent intent = new Intent(getBaseContext(), Bienvenue.class);  intent.putExtra("monVisiteur", leVisiteur);  startActivity(intent);  Toast.makeText(getApplicationContext(), "Chargement des données",  Toast.LENGTH\_LONG).show();  }  else{  Toast.makeText(getApplicationContext(), "QrCode incorrect”,  Toast.LENGTH\_LONG).show();  }  } *// fin de onTacheTerminee*  }; *// fin de new VisiteurDAO()*  *//appel de la méthode getVisiteurByQrCode dans VisiteurDAO*  visiteurAcces.getVisiteurByQrCode(idQrCode);  **}**  **}** |

*VisiteurDAO.java*

|  |
| --- |
| */\*\*\* Classe permettant l'accès aux données (data access object) \*/*  public abstract class VisiteurDAO implements EventAsyncVisiteur {  private static final String serveur="www.Lascaux.artparietal.fr";  private static final String chemin="/lascaux/";  public VisiteurDAO(){ … }  *//Constructeur*  */\*\**  *\* Envoie une requête HTTP pour récupérer les données du visiteur à partir du QrCode scanné*  *\* @param unQrCode chaîne contenant le code QR du billet*  *\*/*  public void getVisiteurByQrCode(String unQrCode){  *// declenche la requete HTTP http://www.Lascaux.artparietal.fr/lascaux/getVisiteur.php*  AccesHTTP requeteHttp = new AccesHTTP(){  *[... récupère l’information reçue dans this.ret … ]*  @Override  protected void onPostExecute(Long result) {  *// une fois le Post réalisé, analyse et récupération des informations json*  onTacheTerminee(jsonStringToVisiteur(this.ret));  }  };   requeteHttp.addParam("qrcode",unQrCode);  requeteHttp.execute("http://" + serveur + chemin + "getVisiteur.php");  }  */\*\**  *\* Crée un objet visiteur à partir du flux json reçu en paramètre*  *\* @param jsonString chaîne Json en provenance du serveur*  *\* @return un visiteur correctement initialisé ou null si échec*  *\*/*  private Visiteur jsonStringToVisiteur(String jsonString){  Visiteur unVisiteur = null;  CategorieAge laCategorieAge,  String nomV,civiliteV, prenomV,melV, libCategorieAgeV;  int idV, idCategorieAgeV;  try {  JSONObject objJson = new JSONObject(jsonString);  idV = Integer.parseInt(objJson.getString("id"));  civiliteV = objJson.getString("civilite");  nomV = objJson.getString("nom");  prenomV = objJson.getString("prenom");  melV = objJson.getString("mel");  idCategorieAgeV = Integer.parseInt(objJson.getString("idCategorieAge"));  libCategorieAgeV = objJson.getString("libCategorieAge");  laCategorieAge= new CategorieAge(idCategorieAgeV, libCategorieAgeV);  unVisiteur = new Visiteur(idV,civiliteV,nomV,prenomV,melV, laCategorieAge);  }  catch (JSONException e){  Log.d("log","pb decodage JSON");  }  return unVisiteur;  }  } |

Document C6 : Codes partiels de l’application d’authentification : gestion des mots de passe du guide.

*Guide.java*

|  |
| --- |
| */\*\* \* Classe Guide\*/*  publicclassGuide {  private int id;  private String nom;  private String prenom;  private String mel;  private String telephone;  private MotDePasse actuelMotDePasse;  private ArrayList <MotDePasse> lesAnciensMotsDePasse;  /\*\*  \* *Ce constructeur valorise l’ensemble des attributs.*  \*/  public Guide(int id, String nom, String prenom, String mel, String telephone,  MotDePasse actuelMotDePasse, ArrayList <MotDePasse> lesAnciensMotsDePasse ) {  *...*  this.lesAnciensMotsDePasse = lesAnciensMotDePasse;  this.actuelMotDePasse = actuelMotDePasse;  }  ***// Méthode à compléter pour être conforme à l’évolution demandée***  */\*\**  *\* Vérifie si le nouveau mot de passe reçu en paramètre est conforme aux spécifications.*  *\* Si le nouveau mot de passe est différent du mot de passe actuel, on mémorise l’instance de*  *\* l’ancien mot de passe dans l’historique des anciens mots de passe, puis on crée une instance*  *\* pour le nouveau mot de passe qui devient l’actuel mot de passe du guide (déjà hashé).*  *\* @param unMotDePasse le mot de passe hashé*  *\* @return true (vrai) si la modification a été effectuée ou false (faux) sinon*  *\*/*  public boolean setMotDePasse(String unMotDePasse) {  boolean modifARealiser = true;  if(unMotDePasse.equals(this.actuelMotDePasse.getMotDePasseHashe()){  modifARealiser = false;  } else{  this.lesAnciensMotsDePasse.add(this.actuelMotDePasse);  this.actuelMotDePasse = new MotDePasse( LocalDate.now(), unMotDePasse);  }  return modifARealiser;  }  ***// Méthode à écrire***  */\*\**  *\* Vérifie si le mot de passe est périmé, c’est-à-dire s’il a plus de trois mois*  *\* @return true (vrai) si le mot de passe a plus de trois mois, false (faux) sinon*  *\*/*  public boolean doitChangerMdP() {**...**}  } |

*MotDePasse.java*

|  |
| --- |
| */\*\**  *\* Classe MotDePasse*  *\* mémorise un mot de passe avec sa date de création. Le mot de passe est réputé hashé.  \* @version 2.0*  *\*/*  public class MotDePasse {  private LocalDate dateCreation;  private String motDePasseHashe;  */\*\**  *\* constructeur de la classe  \* @param dateCrea date de début d’utilisation*  *\* @param motDePasse le mot de passe hashé*  *\*/*  public MotDePasse(LocalDate dateCrea, String motDePasse) {  this.dateCreation = dateCrea;  this.motDePasseHashe = motDePasse;  }  */\*\**  *\* accesseur de la date de création*  *\* @return la date de la création du mot de passe*  *\*/*  public LocalDate getDateCreation() {  return dateCreation;  }  */\*\**  *\* accesseur du mot de passe*  *\* @return le mot de passe*  *\*/*  public String getMotDePasseHashe() {  return motDePasseHashe;  }  } |

### 

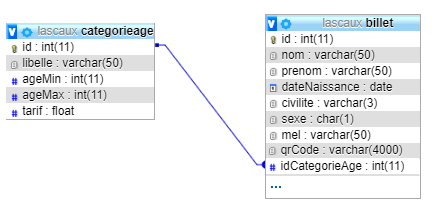
Document C7 : Scripts PHP de la phase d'identification du visiteur

*getVisiteur.php*

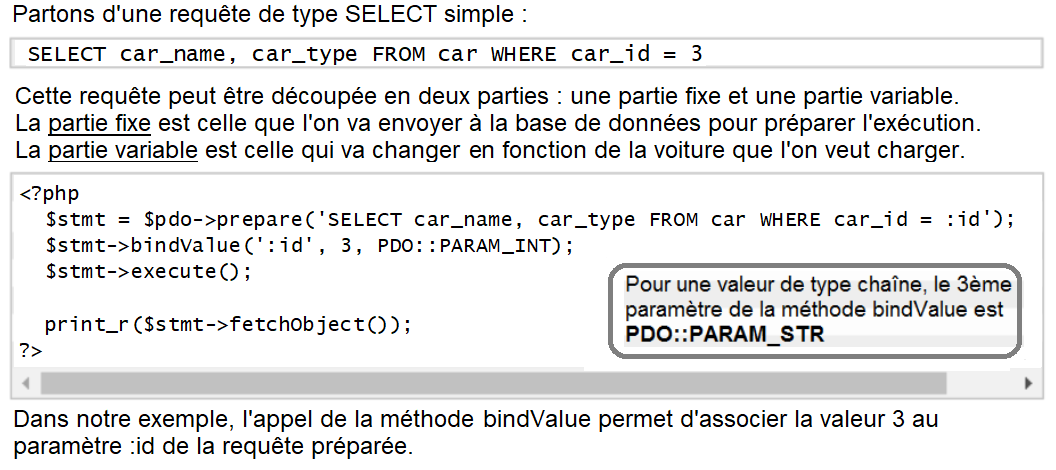
|  |
| --- |
| <?php  *// Le code du script de connexion a été testé et approuvé au niveau de la sécurité*  *// il initialise la variable globale $pdo*  require\_once 'connect-db.php';  */\*\**  *\* Obtenir les informations du visiteur, en représentation JSON, à partir d’une valeur de qrCode d’un billet*  *\* @param string $qrCode*  *\* @global PDO $pdo une référence PDO de connexion à la base de données*  *\* @return string JSON représentation du visiteur ou la cause de l'erreur*  *\*/*  function getVisiteurByQrCode($qrCode) {  global $pdo;  try {  $sql = "  SELECT billet.id as id, civilite, nom, prenom, mel,  categorieAge.id as idCategorieAge, libelle AS libCategorieAge  FROM Billet  JOIN CategorieAge ON idCategorieAge = CategorieAge.id  WHERE qrCode = '" . $qrCode . "'";  $req = $pdo->prepare($sql);  $req->execute();  *// retourne la ligne suivante en tant qu'un tableau indexé par le nom des colonnes*  *// ou retourne false si aucune ligne n'est retournée*  $ligne = $req->fetch(PDO::FETCH\_ASSOC);  return json\_encode($ligne);  } catch (PDOException $e) {  $erreur = array();  *// obtient la raison technique de l'erreur*  $erreur['erreur'] = $e->getMessage();  return json\_encode($erreur);  }  }  header("content-type: application/json; charset=utf-8");  echo getVisiteurByQrCode($\_POST['qrcode']); |

*Remarque : La balise fermante php (?>) est volontairement absente en fin de script.*

Document C8 : Extrait du schéma relationnel exploité par le script getVisiteur.php

****

Document C9 : Exemple de création d'une requête préparée



Document C10 : Descriptif classe ArrayList

|  |
| --- |
| public class ArrayList {  public ArrayList() { … } *// Construit une liste vide*  public boolean add(E e) { … } *// Ajoute un élément dans la liste*  public void clear() { … } *// Supprime tous les éléments de la liste*  public boolean contains(E e) { … } *// Retourne vrai si l’objet passé en paramètre existe*  *dans la liste*  public E get(int index) { … } *// Retourne l’élément positionné à l’emplacement index*  public int size() { … } *// Retourne le nombre d’éléments contenus dans la liste*  public boolean remove(int index) { … } *//* S*upprime l’élément positionné à l’emplacement index*  }  L’exemple ci-dessous permet de manipuler une collection de chaînes de caractères. Le principe est le même quel que soit le type des éléments.  ArrayList<String> mesChaines; *// Déclaration d'une collection de chaînes de caractères*  mesChaines = new ArrayList<String>(); *// Instanciation de la collection*  mesChaines.add("un"); *// Ajout d'une chaîne à la collection*  mesChaines.add("deux");  for (String uneChaine : mesChaines) { *// Parcours de la collection*  System.out.println(uneChaine); *// Affichage de l'élément courant*  }  mesChaines.remove(1); *// Suppression du 2ème élément (indice 1)*  System.out.println(mesChaines.get(0)); *// Affichage du 1er élément (indice 0)*  System.out.println(mesChaines.size()); *// Affichage du nombre d'éléments de la collection* |

Document C11 : Documentation partielle de la classe LocalDate en Java

* + 1. *//pour obtenir l’année en cours*
    2. LocalDate aujourdhui = LocalDate.now();
    3. int anneeEnCours = aujourdhui.getYear();
    4. System.out.println(anneeEnCours);
    5. LocalDate uneDate = LocalDate.now();
    6. LocalDate uneAutreDate ;
    7. *// pour soustraire un mois à une date*
    8. uneAutreDate = uneDate.minusMonths(1);
    9. *// pour soustraire une année à une date*
    10. uneAutreDate = uneAutre.minusYears(1);
    11. *// pour ajouter un mois à une date*
    12. uneAutreDate = uneAutreDate.plusMonths(1);
    13. *// pour comparer deux dates*
    14. if (aujourdhui.isAfter(uneAutreDate)) {
        1. System.out.println("aujourd’hui se situe après l'autre date");
    15. } else {
    16. System.out.println("aujourd’hui se situe avant l'autre date");
    17. }

Document C12 : Filtrage des données externes (extrait d’une formation)

Les variables super globales $\_POST, $\_GET, $\_COOKIE, et $\_REQUEST détiennent des informations transmises via une requête *HTTP* déclenchée par un utilisateur.

Ces informations peuvent potentiellement provenir d’un utilisateur malintentionné. Il existe deux manières de filtrer : soit on valide le contenu de ces informations car on en connaît le type (URL, mél, tél, date par exemple), soit on nettoie le contenu en supprimant ou transformant ce qui pourrait être malicieux comme des apostrophes ou la présence de balises par exemple.

On utilise donc deux types de filtres :

* les filtres de validation (VALIDATE), qui ne modifient pas les données transmises, mais qui cherchent à vérifier qu'ils correspondent à un format. Si ce n'est pas le cas, ils renvoient FALSE.
* Les filtres de conversion (SANITIZE) qui suppriment ou transforment les caractères ou expressions qui ne sont pas conformes à un format sans forcément s'assurer que le résultat soit effectivement valide (par exemple suppression de balises et encodage de caractères spéciaux).

Quelques exemples :

* pour valider un champ ‘mel’ contenant une adresse courriel via la méthode POST :

$mel = filter\_input(INPUT\_POST, 'mel', FILTER\_VALIDATE\_EMAIL) ;

* pour nettoyer un champ ‘mdp’ contenant un mot de passe via la méthode POST

$mdpSaisi = filter\_input(INPUT\_POST, 'mdp', FILTER\_SANITIZE\_STRING) ;

* pour valider un champ ‘quantité’ contenant une valeur entière via la méthode POST pour laquelle on souhaite vérifier qu’elle est comprise entre 1 et 999:

$qteCom = filter\_input(INPUT\_POST, 'quantite', FILTER\_VALIDATE\_INT, array("options" => array("min\_range"=>1, "max\_range"=>999))) ;

Pour résumer : les filtres sont l’ultime évolution de la chasse à l’option guillemet magique (magic quote).

Documents associés au dossier D

Document D1 : Liste de propositions émises lors de l’itération zéro (sprint 0)

1. Le compte administrateur de *MySQL* (*root*) sera utilisé par tous les scripts *PHP* de l’application ayant besoin de se connecter à la base de données *MySQL*. Il faudra cependant veiller à changer le mot de passe par défaut de ce compte.
2. L’administrateur *Scrum* (*Scrum Master*) définira l’identifiant et le mot de passe de l’administrateur de l’application en production. Ce dernier aura tous les droits sur le contenu des tables utilisées par l’application. Un fichier contenant l’identifiant et le mot de passe de l’administrateur sera remonté dans le référentiel (*repository*) utilisé par l’équipe *Scrum*.
3. Un référentiel (*repository*) privé sera utilisé pour la gestion de versions (*versioning*) des fichiers contenant le code source des applications.
4. Les développeurs pourront tester l’application en utilisant directement les bases de production.
5. Il est indispensable de vérifier qu’il n’y a pas de vulnérabilités connues sur les dernières versions des bibliothèques logicielles (*librairies*) et des infrastructures logicielles (*frameworks)* libres (*open source*) avant de les utiliser.
6. Les caractéristiques de chaque connexion et déconnexion (*user*, IP, date et heure, etc.) seront conservées dans un fichier des événements (fichier *log*). L’écriture dans ce fichier ne sera effective que du lundi au vendredi.

Document D2 : Risques cyber liés aux prestataires et aux sous-traitants et préconisations de la direction générale de la sécurité intérieure (DGSI)

*extrait de DGSI Ingérence économique : https://www.economie.gouv.fr/files/dgsi-special-cybersecurite.pdf*

Les entreprises et administrations, indépendamment de leur taille, mission ou secteur d’activité, sont de plus en plus fréquemment amenées à confier à des tiers tout ou partie de la gestion de leurs systèmes d’information. Ces prestations peuvent induire des risques sur l’intégrité, la disponibilité ou la confidentialité desdits systèmes.

Pour mener à bien ces missions, les prestataires disposent, en particulier, de connexions informatiques aux réseaux de l’entreprise cliente. Ces accès peuvent être internes lorsqu’un sous-traitant est physiquement sur le site, ou à distance, notamment dans le cas d’infogérance ou de supervision des réseaux. Indifféremment de la méthode de connexion au réseau utilisée, l’entreprise est exposée à de nouvelles vulnérabilités.

Dans le cadre de ses missions de sécurité économique et de protection du patrimoine, la DGSI a traité plusieurs cas d’atteintes à des systèmes d’information perpétrés par un prestataire, au cours ou à l’issue de sa mission. D’autres cas relèvent d’intrusions dans les systèmes d’information du prestataire en vue d’atteindre l’entreprise ou l’administration ayant sollicité le sous-traitant.

**1er exemple : les problèmes liés à un sous-traitant durant une prestation**

Une administration a accueilli dans ses locaux les employés du sous-traitant pour un projet de refonte de son système d’information. Les accès informatiques nécessaires pour mener à bien la mission leur ont été octroyés. Après avoir constaté des irrégularités dans le système d’information, l’équipe de sécurité de l’administration cliente a découvert que l’un de ces employés ne respectait pas la charte informatique et utilisait du matériel informatique personnel non déclaré.

Après enquête, il s’est avéré que ce prestataire exfiltrait de l’information sensible et menait des actions informatiques au sein de l’administration elle-même, afin d’augmenter ses privilèges au sein du système d’information de celle-ci.

**2ème exemple : malveillance d’un sous-traitant à l’issue d’un contrat de prestation non renouvelé**

Une entreprise a subi des attaques provoquant l’indisponibilité de son système d’information, ainsi que la perte de données sauvegardées. Après investigations techniques, il a été démontré que le dysfonctionnement provenait d’un compte administrateur mis à disposition de prestataires.

Il est apparu que l’ancien sous-traitant, dont le contrat était arrivé à terme et n’avait pas été renouvelé, disposait toujours des droits d’accès au réseau du client et au compte administrateur.

Animé par un esprit de vengeance, ce prestataire a exfiltré des données sensibles et mené des actions de sabotage (suppression de données).

**3ème exemple : Ingérence à l’encontre d’un prestataire pour compromettre le système d’information de l’entreprise cliente**

Une entreprise ayant fait appel à un prestataire pour mener à bien des projets d’ingénierie, a interconnecté une partie de son réseau avec celui du sous-traitant afin de permettre des opérations à distance. Quelques mois après, l’entreprise a été victime d’une compromission importante de son système d’information.

Après enquête, il s’est avéré que le prestataire avait fait l’objet d’une compromission de son système d’information, dont l’objectif était d’accéder au système d’information du client final afin d’en exfiltrer des données sensibles.

**Préconisations de la DGSI**

Afin de réduire les risques d’atteintes aux systèmes d’information, dont ceux de captation et d’exfiltration de données sensibles, la DGSI recommande d’appliquer les bonnes pratiques suivantes :

**En amont d’une prestation :**

Bien définir le périmètre et les modalités d’interconnexion :

* Cloisonner au maximum le réseau informatique accueillant les prestataires ;
* Créer des comptes utilisateurs temporaires pour les prestataires et ne leur octroyer que les droits strictement nécessaires aux missions confiées.

Bien définir les modalités contractuelles de la prestation :

* Prévoir contractuellement et de manière précise les missions et obligations des prestataires ;
* Inclure une clause de confidentialité dans les contrats de prestation, couvrant toutes les informations et données relatives à l’entreprise, dont le prestataire pourrait être amené à prendre connaissance ;
* Privilégier le recours à des entreprises ayant leur siège social dans l’Union Européenne afin de ne pas s’exposer à des législations étrangères défavorables et à portée extraterritoriale ;
* Assurer le suivi des informations et données détenues par le prestataire ; s’assurer, le cas échéant, que ces dernières sont stockées sur des serveurs situés dans l’Union Européenne ;
* Procéder à toute vérification qui paraîtrait utile pour vérifier le respect de la clause de confidentialité prévue par le contrat ;
* Exiger un niveau de sécurité informatique minimal du prestataire (dispose-t-il d’une politique de sécurité des systèmes d’information ? réalise-t-il des audits de ses systèmes informatiques régulièrement ? Ses salariés sont-ils sensibilisés à la sécurité informatique ?).

**Durant la prestation :**

* Superviser la sécurité, le maintien en condition opérationnelle et de sécurité des équipements utilisés par le prestataire ;
* Surveiller l’ensemble des activités du prestataire (accès, changement de personnels, journaux d’événements réseau) ;
* Nommer un référent pour assurer le bon déroulement du projet et veiller à ce que les règles informatiques et contractuelles soient appliquées.

**Après la prestation :**

* Couper l’ensemble des flux réseaux et interconnexions avec le prestataire ;
* Suspendre l’ensemble des accès et comptes utilisateurs utilisés par les sous-traitants avant de les supprimer, le cas échéant ;
* Superviser les équipements du réseau ayant été utilisés par le prestataire afin d’exclure toute malveillance potentielle ;
* Rapporter aux responsables de l’entreprise et de l’administration et, le cas échéant, aux autorités, les incidents constatés.