TASKSTEP

RAPPORT D'AUDIT DE L'APPLICATION

D1 – BIDAUT - LAMBERT - RODRIGUES
IUT DIJON – DÉPARTEMENT INFORMATIQUE | 10 MARS 2023

Table des matières

Liste des tableaux et figures

I. Mission et périmètre

A. Cadre de la mission

Cette mission est réalisée dans le cadre de la SAE 4 du BUT2 Informatique de l'IUT de Dijon. Le début de la réalisation de ce rapport a débuté le 06 mars 2023 et a été achevée le 10 mars 2023.

B. Objectifs de la mission

L'objectif de la mission est de réaliser l'audit de l'application web « Taskstep » version 1.1.

C. Périmètre

Les domaines couverts par l'audit sont :

- La qualité logicielle
- La qualité des données
- La sécurité
- Les performances
- L'impact environnemental
- L'ergonomie
- L'accessibilité

D. Limites et contraintes

Équipe réduite (3 personnes) et un temps de réalisation assez court (16 h). De plus, étant donné que l'application n'est pas déployée certains éléments n'ont pas pu être testés.

II. Termes et définitions

Les termes et définitions feront l'objet de notes bas de page.

III. Présentation de l'application auditée

A. Description générale

L'application se nomme Taskstep, c'est une application servant à gérer sa « to do list », autrement dit, sa liste de tâches à faire. On peut donc y créer des tâches, les trier, leur donner des échéances, etc. L'accès à l'application en tant que client se fait par navigateur web. Elle a été créée en 2006.

L'application est développée avec :

- HTML
- CSS
- Javascript
- PHP
- MySQL

Trois personnes ont contribué à son développement : Rob Lowcock (2006) Ethan Romba (2008) et Thomas Hooge (2020).

L'application est à l'origine censée gérer le « multi-utilisateurs », c'est dans le cahier des charges. Cependant cette fonctionnalité n'a pas été entièrement implémentée. Un seul utilisateur est donc pris en charge mais nous allons réaliser l'audit en prenant en compte le fait qu'elle doit être « multi-utilisateurs ».

Github de l'application : https://github.com/eromba/taskstep

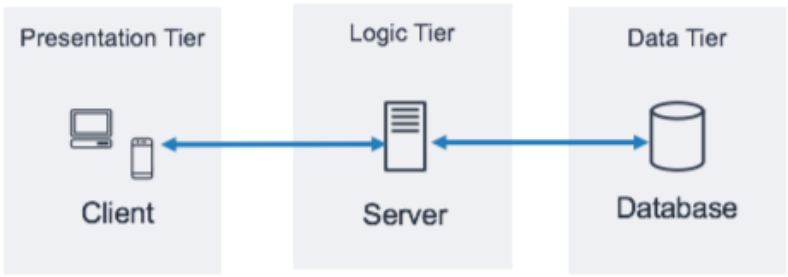
Github de notre équipe : https://github.com/dept-info-iut-dijon/S4.01_D1_AGH

B. Fonctionnalités attendues

Voir : Annexe 8 : Diagramme des cas d'utilisation

C. Architecture

L'application est structurée sous la forme d'une architecture "three tiers" donc à trois niveaux : client, serveur, base de données.



Le client est le navigateur web.

Le serveur est sous Apache, en PHP.

La base de données est en MySQL sous phpMyAdmin.

IV. Méthodologie d'audit

A. Méthodologie adoptée

Le fonctionnement de notre équipe a été de se répartir les différents domaines couverts par l'audit en faisant des duos. Nous avons ensuite défini des tâches à réaliser pour chaque domaine.

B. Outils utilisés

- Visual Paradigm 16.3 : réalisation de la rétroconception.
- Microsoft Teams : partage de documents, des tests, des checklists, KANBAN.
- Microsoft Word : rédaction du rapport d'audit.
- Google Chrome Version 111.0.5563.64 : navigation dans l'application, tests de performances avec l'outil pour développeurs.
- Firefox 110.0.1 (64 bits) : navigation dans l'application, tests de performances avec l'outil pour développeurs.
- WAVE Browser Extensions : Vérification des critères d'accessibilité.
- GreenIT-Analysis (extension de navigateur) : Vérification des critères d'impact environnementaux.

C. Checklists utilisées

- Annexe 1: Checklist qualité des données de notre cru
- nnexe 2: Checklist sécurité de notre cru
- Annexe 3: Checklist accessibilité de notre cru
- Annexe 4: Checklist performance de notre cru
- Annexe 5: Checklist qualité logicielle de notre cru
- Annexe 6 : Checklist impact environnemental d'après RGESN[1]
- Annexe 7 : Checklist ergonomie selon les critères de Bastien et Scapin[2]

[1] Référentiel général d'écoconception de services numériques
[2] Bastien, J.M.C., Scapin, D. (1993) Ergonomic Criteria for the Evaluation of Human-Computer interfaces. Institut National de recherche en informatique et en automatique, France

D. Equipe de projet

Prénom NOM	Qualité	Champs d'intervention
Adrien LAMBERT	Membre	Audit sécurité, audit performances, audit qualité logicielle, audit impact environnemental
Hugo RODRIGUES	Membre	Audit accessibilité, audit ergonomie, audit qualité des données
Ganael BIDAUT	Membre	Audit sécurité, audit qualité logicielle, audit impact environnemental, audit qualité des données

Tableau 1: Equipe de projet

E. Planning réel d'exécution

Aspect	**Objet de l'évaluation**	**Date de réalisation**	**Intervenant**	**Durée en heures**
Performance	- Etablissement de la checklist - Réalisation des tests de temps de chargement, CPU, consommation mémoire, etc. - Recherche d'axes d'amélioration - Rédaction de l'audit	09/03/2023	Ganael BIDAUT Adrien LAMBERT Hugo RODRIGUES	2 h 30 4 h 1 h 30
Qualité logicielle	- Revu du code - Rétroconception - Recherche d'axes d'amélioration - Etablissement de la checklist - Rédaction de l'audit	09/03/2023 – 10/03/2023	Ganael BIDAUT Adrien LAMBERT Hugo RODRIGUES	4 h 3 h 1 h 30
Sécurité	- Etablissement de la checklist - Identification des données et fonctionnalités ainsi que leur sensibilité - Evaluation des vulnérabilités potentielles - Recherche de démarches de sécurité correctives - Rédaction de l'audit	07/03/2023 – 08/03/2023	Ganael BIDAUT Adrien LAMBERT	7 h 6 h
Gestion des données	- Etablissement de la checklist - Evaluation des données et de la base de données actuelle - Rétroconception de la base de données - Recherche de proposition pour améliorer la base de données et les principes ACID - Proposition d'un autre modèle conceptuel des données - Rédaction de l'audit	08/03/2023	Ganael BIDAUT Adrien LAMBERT Hugo RODRIGUES	4 h 30 3 h 30 2 h 00
I A E	1 : impact environnemental	06/03/2023	Ganael BIDAUT Adrien LAMBERT	2 h 30 3 h
	2 : accessibilité	06/03/2023 – 09/03/2023	Adrien LAMBERT Hugo RODRIGUES	2 h 5 h 30
	3 : ergonomie	09/03/2023 – 10/03/2023	Hugo RODRIGUES	10 h
			Durée totale de la mission	Environ 21h/hommes

Tableau 2: Planning d'exécution

V. Synthèse des résultats

Nous avons réussi à trouver des checklists pertinentes comme RGESN pour l'impact environnemental ou encore les critères de Bastien et Scapin pour l'ergonomie. Pour le reste nous en avons créé nous-même avec nos propres ressources et nos connaissances, étoffé par de brèves recherches. Nous avons fait notre maximum compte tenu du temps donné que nous avons même largement dépassé.

La responsabilité de ces audits est à imputer à l'équipe enseignante car cela a été réalisé dans le cadre d'un exercice scolaire.

Certaines limites sont apparues car nous avons uniquement testé l'application en localhost sous XAMPP et nous avons été en effectif réduit (3 personnes).

Les tests effectués sont principalement des tests fonctionnels, ainsi que de l'observation de chaque membre avec du recoupage et de l'écrémage d'information.

L'application ne convient plus aux standards actuels, de plus, la dernière modification date de 2020 ce qui aurait dû faire l'objet d'un refactoring complet pour convenir en tous points aux normes et paradigmes actuels.

La sécurité en pâtie et reste très triviale, en plus de ne pas sécuriser la communication principale de client-serveur.

Donc les données qui transites ne sont pas sécurisées, de plus leurs gestions de données sauvegardées est fonctionnelle pour l'utilisation actuelle mais bancale car il n'y a même pas de relation. Cette gestion de données n'est cependant absolument pas adaptée à un fonctionnement multi-utilisateur.

De part plusieurs manquements, l'application ne peut qu'être peu gourmande et peu demandant en ressources, ce qui convient aussi bien en termes de performances qu'en impact environnemental.

L'application n'est pas vraiment pensée entièrement pour une accessibilité totale mais n'est pas totalement en reste là-dessus, il en va de même pour l'ergonomie. Depuis la création de l'application en 2006, tous les standards ont évolué mais celle-ci ne les a pas suivis.

VI. Présentation détaillée des résultats

A. Qualité logicielle

1. Checklist

Critères à vérifier	Conforme / Non conforme	Commentaire / Justification
L'application respecte-elle les principes SOLID[3] ?	Non conforme	Pas de classes, principe S non respecté.
Est-ce que le choix d'architecture est pertinent ?	Non conforme	Un MV[4] au lieu d'un MVC[5] pour du multi-utilisateur.
Des commentaires sont-ils présents partout et pertinents ?	Non conforme	Il y en a parfois mais pas toujours, il y a également des bouts de tests qui trainent dans le code.
De la documentation est-elle présente partout et pertinente ?	Non conforme	Aucune documentation n'est présente
Aucunes ancres identifiables dans le code ?	Non conforme	Plusieurs bouts de code inutiles
Est-ce que les technologies utilisées sont-elles aux normes ?	Non conforme	Le PHP n'est pas aux dernières normes
Les designs pattern utilisés sont-ils cohérents ?	Non conforme	Aucun design pattern n'est utilisé.
Y-a-t-il des tests unitaires et sont-ils pertinents ?	Non conforme	Aucun test unitaire n'est présent.
Est-il impossible de faire planter l'application ?	Non conforme	Oui on peut bloquer l'application dans une boucle d'alert[6]
Les packages sont-ils cohérents avec l'architecture ?	Non conforme	Il n'y a pas de package bien découper
L'application fait elle ce que nous attendons ?	Conforme	Les principales fonctionnalités marchent
L'application est-elle portable à d'autres os ?	Conforme	On peut passer sous les noyaux UNIX[7]
Les technologies utilisées sont-elles en accord avec le besoin ?	Conforme	On dispose d'une application web navigateur qui pourrait être portable en application
La nomenclature est-elle cohérente ?	Non conforme	Il y a quelques noms de balise pas professionnels.
La conception correspond-elle au code ?	Non conforme	Il n'y a pas de conception
La conception a-t-elle été pensée compte tenu des besoins ?	Non conforme	Il n'y a pas de conception
Mise à jour possible ?	Non conforme	Il n'y a pas de système de plugin
Les commentaires git sont-ils précis et utiles pour une reprise ?	Conforme	Le dernier commit a un commentaire propre

[3] Les principes SOLID sont des principes de programmation voir ici
[4] Model view : est un type d'architecture avec seulement une couche métier et une couche IHM
[5] Model view controler : est un type d'architecture avec une couche métier, une couche IHM et une couche controler, voir ici

[6] Fonction de javascript
[7] Noyaux d'une famille de système d'exploitation

2. Preuve d'audit

Nous avons réalisé la rétroconception et un cas générique de la page d'accueil en diagramme de séquence. Ainsi que ce qu'on pourrait appeler un dictionnaire de fonctionnalité qui est également présent en annexe.

Voir :

- Annexe 21 : Dictionnaire des fonctions
- Annexe 22 : Diagramme de séquence du chargement de index.php
- Annexe 23 : Rétroconception

3. Recommandations

- Revoir la conception générale de l'application en appliquant le paradigme de programmation objet afin d'avoir un code bien plus structuré, qui respecte les principes SOLID.
- Utiliser les dernières versions des technologies, notamment PHP, afin de ne plus avoir de fonctionnalités dépréciées.
- Réaliser une documentation complète de l'application ainsi qu'une conception (type diagramme des classes) afin de rendre la maintenance et la modification plus efficace.
- Réaliser des tests unitaires pour les différentes fonctionnalités afin de vérifier la conformité de leur bon fonctionnement et d'empêcher la régression lors de mise à jour.
- Mettre en place une architecture MVC afin de respecter au maximum les principes SOLID.

B. Sécurité

1. Public visé par l'application

Le public principalement visé par l'application TaskStep est le grand public. En effet, tout le monde est plus ou moins susceptible d'utiliser une application permettant de réaliser une "To do list". Ce grand public n'est en général pas sensibilisé aux problèmes de sécurité, en particulier sur une application qui n'est pas censé gérer des données très sensibles.

2. Les différents types d'utilisateurs

Dans l'idée que l'application devrait être multi-utilisateur, elle comporterait 3 types d'utilisateurs :

- Les visiteurs : qui ont seulement accès à la page de connexion
- Les utilisateurs : qui ont accès à l'ensemble de l'application mis à part la gestion des comptes.
- Les administrateurs : qui en plus d'un accès à l'ensemble de l'application ont accès à la gestion des comptes utilisateurs.

L'application n'ayant pas implémenté cet aspect multi-utilisateur, seuls les visiteurs et utilisateurs sont présents. Les utilisateurs ont accès à l'ensemble de l'application, sans restriction. En pratique, les visiteurs existent partiellement car l'utilisateur peut désactiver l'option qui permet de demander un mot de passe quand on arrive sur l'application. Il n'y a même pas de notion de "compte utilisateur", tout le monde est considéré comme étant sur la session de numéro 1, sur la base de données.

3. Ensemble des informations manipulées

Très sensible : ensemble des données qui, en cas de fuite, identifient clairement l'utilisateur et/ou sont de nature confidentielle.

Sensible : ensemble des données nécessitant l'authentification de l'utilisateur afin d'y accéder ou un utilisateur identifié.
Peu sensible : ensemble de données pas liées à l'utilisateur, ne nécessitant pas de confidentialité particulière.

Autorisation d'accès et degré de sensibilité des données		
Donnée	**Sensibilité**	**Protection à réaliser**
Titre de tâche	Sensible	Connexion à l'utilisateur
Date butoir de tâche	Sensible	Connexion à l'utilisateur
Section de la tâche	Peu sensible	Identique pour tous, donc publique. Pas de protection particulière.
Note de tâche (description)	Sensible	Connexion à l'utilisateur
URL de tâche	Sensible	Connexion à l'utilisateur
Information de complétion de tâche	Sensible	Connexion à l'utilisateur
Le nom du contexte de la tâche	Sensible	Connexion à l'utilisateur
Le nom du projet de la tâche	Sensible	Connexion à l'utilisateur
Titre de contexte	Sensible	Connexion à l'utilisateur
Titre de projet	Sensible	Connexion à l'utilisateur
Mot de passe	Très sensible	Doit être hashé[8] avec du salt[9]
Salt du mot de passe	Peu sensible	Donnée publique, pas de protection particulière

[8] Passage par une fonction mathématique le plus irréversible possible qui transforme une chaine de caractère en entré en une suite de bits
[9] salt : élément ajouté à la chaine que l'on va hacher, ce qui va éviter les attaques par dictionnaire

Numéro de session	Très sensible	Interne au serveur, ne doit pas être accessible par les utilisateurs
Stylé sélectionné par l'utilisateur	Sensible	Connexion à l'utilisateur
Préférence sur la présence de tips[10]	Sensible	Connexion à l'utilisateur

4. Ensemble des fonctionnalités

Autorisation d'accès et degré de sensibilité des fonctionnalités		
Fonctionnalité	**Sensibilité**	**Protection à réaliser**
Accéder à la page de connexion	Peu sensible	Publique, tout le monde peut y accéder. Aucune protection particulière.
Pouvoir se connecter	Sensible	Que seul un utilisateur vérifié puisse se connecter. Donc mot de passe, puis hashage de ce dit mot de passe avec un salt.
Pouvoir s'identifier une fois connecter	Très sensible	Que le serveur nous identifie avec notre session.
Accéder à l'accueil	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Accéder aux tâches du jour	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Mettre nos tâches dans un format imprimable	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Voir toutes les tâches	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Pouvoir valider une tache	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Pouvoir modifier une tâche	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Pouvoir supprimer une tâche	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Pouvoir hiérarchiser des tâches	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Pouvoir trier les tâches par, date, projet, contexte, valider, titre	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Ajouter un contexte/projets	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Modifier un contexte/projets	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Supprimer un contexte/projets	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Consulter les contextes/projets	Sensible	Nécessite l'authentification de l'utilisateur spécifique.
Consulter les paramètres	Très sensible	Car il comporte des
Changer de style	Sensible	Nécessite l'authentification de l'utilisateur spécifique.

[10] Élément de l'application

Afficher ou non le bloc de “tips”	Sensible	Nécessite l’authentification de l’utilisateur spécifique.
Changer de mot de passe	Très sensible	
Choisir de désactiver les mots de passes et les sessions	Très sensible	Nécessite une autorisation spéciale. Ex : compte administrateur. Mais en soit ne devrait même pas exister
Supprimer toutes les tâches terminées	Très sensible	
Faire tourner le script update	Très sensible	Nécessite une autorisation spéciale. Ex : compte administrateur.
Exporter en csv	Sensible	Nécessite l’authentification de l’utilisateur spécifique.
Mettre en favori grâce à du drag and drop	Sensible	Nécessite l’authentification de l’utilisateur spécifique.
Consulter le forum d’aide	Peu sensible	Forum public, tout le monde y a accès. Pas de protection particulière.
Déconnexion	Sensible	Nécessite l’authentification de l’utilisateur spécifique.
Ajouter une tâche	Sensible	Nécessite l’authentification de l’utilisateur spécifique.
Ajouter une note à la tâche	Sensible	Nécessite l’authentification de l’utilisateur spécifique.
Ajouter une section à la tâche	Sensible	Nécessite l’authentification de l’utilisateur spécifique.
Ajouter un contexte et un projet à la tâche	Sensible	Nécessite l’authentification de l’utilisateur spécifique.
Ajouter une date de fin à la tâche	Sensible	Nécessite l’authentification de l’utilisateur spécifique.

5. Les vulnérabilités structurelles

- Vulnérabilité potentielle à l’attaque DDOS[11].
- Vulnérabilité potentielle à la non-gestion des codes d’erreurs.
- Possibilité d’injections SQL dans les champs d’entrée.
- Possibilité d’injection XSS[12]
- Vulnérabilité potentielle sur l’obsolescence des technologies utilisées.
- Vulnérabilité potentielle sur les mots de passes, leur gestion, éviter les “rainbow table”[13].
- Est-il possible à partir du client d’avoir les clés du royaume de l’application.
- La base de données est-elle chiffrée et anonymisé ?
- Est-ce qu'une démarche d'OSINT[14] ne met pas en péril la sécurité de l'application ?

6. Démarche de sécurité réalisée par l’existant pour chaque vulnérabilité potentielle

- L'application n’inclus pas de protection d’attaque par dénis de services, elle est alors très sensible en cas d’attaque.

[11] Une attaque DDoS, ou par déni de service distribué : Type d’attaque avec de nombreuse requêtes simultané, voir ici
[12] Cross-Site Scripting : vulnérabilité permettant d'injecter du contenu dans une page, voir ici
[13] Type d’attaque à partir de données publiques dans de grands tableau de mot de passe simple et connu, voir ici
[14] Open Source **Intelligence :** désigne toutes les informations qui peuvent être trouvées publiquement, voir ici

- L'application ne gère pas les codes d'erreurs, ils sont gérés par le navigateur. Aucune page n'est prévue à cet effet.
- Les langages utilisés, notamment PHP, sont dans des versions dépréciés
- Les attaques par injection SQL ne sont pas gérées partout dans l'application mais possible à certains endroits.
- Les attaques par injection XSS ne sont pas gérées mais peu fonctionnel ici.
- Lors du changement de mot de passe il n'y a pas de contrainte, de plus il y a une option de non-utilisation de mot de passe et de section.
- Etant donné que nous avons une version http sans un tunnel SSL et que le mot de passe transite en claire, cela pose un problème de sécurité.
- Le mot de passe est hasher au MD5[15] qui est déprécier et de plus on ne fait qu'ajouter le salt à la fin du hash au lieu de le faire l'ajouter avant de hasher.
- Il y a la présence d'un flux RSS[16] qui n'est jamais utilisé.

7. Evaluation de la pertinence et la suffisance de la démarche de sécurité réalisée par l'existant

- Concernant de dénis de services l'application n'est pas prévue pour de grand nombre d'utilisateur de base mais est prévu à être déployer donc cette protection peut passer par le serveur en amont. Donc pas pertinent
- La non-gestion des codes d'erreurs n'est pas réellement une vulnérabilité mais c'est géré par le navigateur peuvent être géré par le routeur en avance.
- Des mises à jour sont nécessaires pour passer aux paradigmes plus récents notamment la POO[17], arrêter d'utiliser mysqli pour avoir réellement des PDO, les dernières normes PHP8, HTML5, CSS3 et JS ECMA-262 sans compter que nous ne sommes pas vraiment en PHP7 malgré ce qui est noté.
- Avec les nouvelles versions de PHP il est possible de faire rapidement les vérifications pour éviter les injections.
- Les mots de passes transitent en claire sans forcément avoir un tunnel SSL[18], s'assuré d'être en https et dans le cas du http créer de quoi faire transiter de manière sécurisée.
- De plus aucune contrainte et/ou rappel de sécurité sur les mots de passes des changements, pas de changement du mot de passe par défaut lors de la connexion.
- Changer de fonction de hachage pour du plus récent et ajouter le "salt" avant de hasher.

8. Démarches de sécurité adaptées pour corriger l'existant

- Retirer l'option de possibilité de retrait des mots de passes et sessions ne devrait même pas être une option, même par un administrateur.
- Mettre tout à jour tout le code, aux dernières normes avec des versions non dépréciées.
- Passer l'ensemble de l'application en https et les dernières normes.
- Rajouter des contraintes sur le mot de passe et un rappel de sécurité sur les mots de passes lors des changements.
- Changement du mot de passe par défaut lors de la connexion.

[15] Message Digest 5 : fonction connue de hashage, voir ici
[16] *Really simple syndication*, litt. « syndication vraiment simple » : flux qui envoie des données au client, voir ici
[17] Programmation orienté objet : paradigme de programmation, voir ici
[18] Secure Sockets Layer : évolution de TSL sert à sécuriser des communication, voir ici

9. Checklist

Critères à vérifier	Conforme / Non conforme	Justifications/ Commentaires
Est-ce que l'application a conscience de son public cible ?	Non conforme	Car des éléments restent très spécifiques alors que le public cible est le grand public.
Ont-ils une approche pertinente des problèmes de sécurité informatique compte tenu de leur public cible ?	Non conforme	Aucune sécurité minimale requise sur les mots de passe. Possibilité de désactiver les sessions et mots de passe.
Y a-t-il différents rôles, une fois identifié, gérés par l'application ?	Non conforme	Non on n'a pas de rôles différents une fois identifié
Ces rôles ont-ils les permission minimums compte tenu des fonctionnalités proposées par la solution ?	Non conforme	Nous avons un seul utilisateur qui à toutes les permissions, aucune ségrégation par rapport à différents rôles
Les données manipulées ont-elles toutes un effort suffisant de sécurité par rapport à leur sensibilité ?	Non conforme	Les mots de passe sont hashé avec l'algorithme MD5, déprécié depuis 2008.
Les fonctionnalités proposées ont-elles toutes un effort suffisant de sécurité par rapport à leur sensibilité ?	Non conforme	Possibilité de désactiver les sessions et mots de passe.
Le serveur communique-t-il sous un tunnel SSL avec le client ?	Non conforme	Aucun chiffrement, les mots de passe et données transitent en clair entre le client et le serveur.
Le serveur communique-t-il de manière sécurisée avec la base de données ?	Non conforme	Non nous ne sommes pas en https sous les dernières normes mais sous http1.1
Le serveur possède-t-il des sécurités comme un anti-DDOS ?	Non conforme	Aucune sécurité de ce type.
Est-ce que les mots de passe sont bien hachés ?	Conforme	Oui mais avec l'algorithme MD5, déprécié depuis 2008.
Est-ce que la fonction de hachage est toujours aux normes ?	Non conforme	MD5 déprécié depuis 2008
Est-ce que le mot de passe de la base de données est changée ? (Plus par défaut)	Non conforme	Le script de base ne le fait pas
Est-ce que le mot de passe de base est changé ?	Non conforme	Ce n'est pas fait
Est-ce que l'on change de mot de passe lors de la première connexion ?	Non conforme	On ne demande pas à l'utilisateur de le faire
Est-ce que la force des mots de passes est cohérent compte tenu de leur utilisation ?	Non conforme	Non car on ne vérifie pas la force du mot de passe alors qu'ont à accès à tout directement
L'application utilise-t-elle les dernières normes de sécurité pour les communications ?	Non conforme	Non nous ne sommes pas en https sous les dernières normes mais sous http1.1
L'application utilise-t-elle les dernières normes de sécurité dans le code ?	Non conforme	Non par exemple MD5 déprécié depuis 2008
L'application est protégée contre les injections SQL ?	Non conforme	Vérification des chams d'entrées utilisateurs avec la fonction PHP "addslashes()" qui n'est pas

		adaptée à la prévention d'injections SQL. Cf. addslashes
L'application est protégée contre le XSS (Cross-Site Scripting)	Conforme	Ça ne marche pas partout
Y-a-il des protections sur la création de comptes anti-bot ?	Non conforme	Aucune protection ni vérification à ce propos.
Existe-il un manuel d'administration de l'application, comprenant notamment : mode d'emploi du manuel, présentation du module d'administration de l'application, droits d'accès « type » par poste, procédure de création / modification / suppression de droits d'accès, …	Non conforme	Il n'y a rien
Existe-il un guide utilisateurs / manuel de procédures, comprenant notamment : mode d'emploi du manuel, présentation de l'application, mode opératoire, règles de gestion, écrans et zones de saisie, liste des messages d'erreurs, états de contrôle et d'exception.	Non conforme	Il n'y a rien, hormis les README.
Existe-t-il une procédure de gestion des profils utilisateurs de l'application placée sous la responsabilité du propriétaire de l'application (procédure de création / modification et suppression des droits d'accès) ? Un dispositif de SSO[19] est-il mis en œuvre ?	Non Conforme	Il n'y a rien hormis un système SSO avec les sessions PHP.
Chaque utilisateur possède-t-il un identifiant qui lui est propre ? Vérifier qu'il n'existe pas de compte « générique » et que l'informatique (chef de projet) n'a que des accès en lecture au même titre que d'éventuels sous-traitants et éditeurs.	Non conforme	Il n'y a qu'il seul utilisateur, donc un seul mot de passe, qui a accès à toutes les fonctionnalités.
Le mot de passe associé à l'identifiant permet-il d'assurer une protection d'accès efficace (7 caractères minimum, gestion de l'historique des mots de passe sur 2 ans, contrôle de « trivialité », changement trimestriel des mots de passe, etc.) ?	Non conforme	L'application ne vérifie pas la force du mot de passe.
Les tentatives de connexions infructueuses à l'application sont-elles enregistrées et contrôlées par le propriétaire de l'application ? Sont-elles limitées ?	Non conforme	Aucun contrôle ou limite sur les connexions infructueuses.
Les procédures de transmission de fichiers en entrée assurent-elles l'exhaustivité et l'exactitude des informations transmises (contrôles systèmes) ?	Non conforme	Non nous ne sommes pas en https sous les dernières normes mais sous http1.1
Les contrôles mis en œuvre lors de l'intégration des données par fichiers à l'application sont-ils suffisants et identiques à ceux mis en œuvre dans le cadre d'une saisie transactionnelle (contrôles applicatifs) ?	Non applicable	
L'intégrité et l'exhaustivité des données transmises entre les différents modules de l'application et/ou à des applications en aval sont-elles assurées ?	Non conforme	Non pas de vérification
Existe-t-il une procédure formalisée et standard de maintenance de l'application ?	Non conforme	Aucune procédure de maintenance définit.

[19] Single Sign-On : On se connecte qu'une seule fois à un système et on reste identifier, voir ici

La documentation de l'application est-elle systématiquement mise à jour après chaque intervention de maintenance ?	Non conforme	Aucune documentation mis à part les instructions d'installation.
La documentation d'exploitation est-elle à jour, dupliquée, protégée et inclut-elle les procédures de gestion des incidents et de reprise / redémarrage ?	Non conforme	Aucune documentation mis à part les instructions d'installation.
Évaluer le niveau de service par l'analyse des tableaux de bord.	Non applicable	
Les procédures de sauvegarde et de reprise de l'application sont-elles satisfaisantes et répondent-elles aux enjeux de l'application et aux engagements de service de l'informatique ?	Non applicable	
Une partie des sauvegardes est-elle stockée à l'extérieur de l'organisation (banque, société spécialisée) selon une périodicité adaptée aux enjeux ?	Non applicable	
En cas de sinistre grave, existe-t-il un plan de secours en adéquation avec les besoins et les enjeux (plan d'urgence, plan de repli, plan de reprise) ?	Non conforme	Aucun plan de secours définit.
La base de données est-elle chiffrée ?	Non conforme	Aucun chiffrement pour la base de données. Il est donc encore plus nécessaire que son accès soit protégé par un mot de passe fort.
Est-ce qu'une démarche d'OSINT ne met pas en péril la sécurité de l'application ?	Non conforme	Le dépôt git est public, une démarche d'OSINT est alors possible.

C. Gestion des données

1. Checklist

Paramètres à vérifier	Conforme / Non conforme	Commentaire / Justification
Est-ce que la base de données respecte la troisième forme normale ?	Non conforme	Dépendances fonctionnelles non conformes
Est-ce que toutes les données misent en base de données sont pertinentes ?	Non conforme	Une énumération est là, les sessions sont en dur
Est-ce que les données sont sécurisées ?	Non conforme	Protocole de hashage de mot passe déprécier (MD5)
Est-ce que la base de données respecte le RGPD[20] et/ou la réglementation étatique ?	Non conforme	Pas de CGU[21]
Est-ce que l'application respecte le RGPD et/ou la réglementation étatique ?	Non conforme	Pas de CGU
L'utilisateur accepte-il avec consentement éclairé le stockage de ses données ?	Non conforme	Rien n'est fait
L'utilisateur accepte-il avec consentement éclairé l'utilisation de ses données ?	Non conforme	Rien n'est fait
L'utilisateur peut-il demander la suppression des informations le concernant ?	Non conforme	Rien n'est prévu pour
Peut-on récupérer toutes nos données ?	Non conforme	Rien n'est prévu pour
Est-ce que le typage est cohérent avec les données ?	Non conforme	Le typage en texte sur des varchar connu, des integer qui sont des bytes, cela ressemble trop à des anciennes normes
Est-ce que le typage est le plus restrictif possible ?	Non conforme	Le typage en texte sur des varchar connu, des integer qui sont des bytes, cela ressemble trop à des anciennes normes
N'y a-t-il pas de relations inutiles ?	Non applicable	
Les relations sont-elles pertinentes ?	Non applicable	
Est-ce que les table ont une fonction distincte ?	Non conforme	La table "settings" gère les préférences utilisateurs, ainsi que les mots de passes, les sessions, etc.
Y-a-t-il des doublons qui sont inutiles ?		Il n'y a pas de doublon
Y-a-t-il des redondances inutiles ?		Il n'y a pas de redondances
Les données inutilisées sont-elles supprimées au bout d'un moment ?	Non conforme	Rien n'est fait
Les cookies[22] font-ils l'objet de consentement éclairé de l'utilisateur ?	Non applicable	Pas de cookies
Le refus de ses cookies n'est-il pas bloquant ?	Non applicable	Pas de cookies
En cas de changement de politique est-ce que l'utilisateur en est informé et accepte ces changements ?	Non conforme	Rien n'est prévu pour
La base de données est-elle chiffrée ?	Non conforme	Rien n'est prévu pour

[20] Règlement général sur la protection des données
[21] Conditions générales d'utilisation
[22] Cookie : donnée stockées chez l'utilisateur relatif au site, voir ici

Protection DDOS présente ?	Non conforme	Rien n'est prévu pour mais peut se mettre en amont sur le serveur
Est-ce que l'application gère les exceptions liées à nos données ?	Non conforme	La date d'échéance saisie lors de la création d'une tâche n'est pas vérifiée.
Les technologies utilisées sont-elles cohérentes ?	Conforme	
Les technologies utilisées ne sont-t-elles pas obsolètes ?	Non conforme	
Le model des données est-il optimisé compte tenu de nos besoins ?	Non conforme	Rien n'est réellement optimisé
Est-ce que les différents utilisateurs ont les permissions minimums ?	Conforme	Pas de multi utilisateur ni différent rôle en base de données
Est-ce qu'un Deadlock[23] est possible ? Si Conforme leur gestion est-elle pertinente et convenable ?	Conforme	Tout se fait en 1 transaction auto-commité[24] et sur 1 utilisateur

2. Commentaires

La base de données est suffisante pour ce que fait l'application maintenant mais cela reste une base de données relationnel sans relation et ne gère pas le multi-utilisateurs.

Les taches utilisent un texte qui est le titre des contextes et des projets comme clé étrangère pour la gestion des taches.

La table section est une énumération qui n'est même pas vouée à évoluer.

La table settings est juste un tableau associatif de clé/valeur.

Pas de gestion des utilisateurs pour du multiutilisateur

La session est saisie en dur lors de l'installation.

Le typage à l'air fait selon d'ancien standard et n'est pas restrictif.

Voici la conception actuelle de la base de données avec son MCD[25], voir : Annexe 9 : Qualité des données - MCD actuel

3. Recommandations

- Nous proposons un MCD, voir : *Annexe :10 Qualité des données - MCD proposé*. Il permettrait de respecter la troisième forme normale et de notamment rendre la base de données réellement relationnelle. De plus avec ce modèle, le multiutilisateur devient implémentable.
- Déploiement sur un serveur protégé qui communique par des tunnels SSL avec un nombre restreint de personne.
- La présence de différents rôles avec des permissions minimums.
- Présence d'un mot de passe fort pour accéder à la base de données, qui change régulièrement.
- Faire des sauvegardes ou même dupliquer la base pour toujours être opérationnel en cas d'incidents sur un serveur.
- Prévenir les utilisateurs pour éviter au maximum les failles non contrôlables, ce qui revient à respecter les réglementations et lois.

[23] Deadlock ou Interblocage : phénomène qui peut bloquer une transaction base de données lors que plusieurs transactions demandent des actions spécifiques aux mêmes enregistrements voir ici
[24] Va valider la transaction à chaque requête.
[25] Model Conceptuel des données

- Mettre à jour l’ensemble des systèmes.
- Nettoyer régulièrement la base de données.

D. Performance

1. Checklist

Critères à vérifier	Conforme / Non conforme	Commentaire / Justification
Les traitements sont-ils performants (vitesse d'exécution, réactivité) ?	Conforme	Les traitements sont performants. Aucun temps d'attente visible à déplorer durant l'utilisation de l'application. En moyenne, sur une minute d'utilisation intensive, on a deux secondes de proccess système. Cela fait une moyenne de 33ms par secondes, ce qui est très correct. Voir : Annexe 17 : Preuve d'audit - Analyse de la répartition du temps sur une minute d'utilisation
La consommation mémoire est-elle optimisée ?	Non conforme	Certes l'application consomme très peu de mémoire, généralement entre 2mB et 7mB, jamais plus. Ce qui est extrêmement faible. Cependant, de nombreuses variables sont déclarés mais jamais utilisées. Il y a également un tunnel RSS qui n'est jamais utilisé. Voir : Annexe 18 : Preuve d'audit - Consommation mémoire sur une minute d'utilisation Annexe 19 : Preuve d'audit - Code inutile et inutilisé Annexe 20 : Flux RSS jamais utilisé
La consommation CPU[26] est-elle optimisée ?	Non conforme	Bien que les traitements soient performants, la consommation CPU pourrait être mieux optimisée (surtout au niveau du serveur) en optimisant notamment les requêtes à la base de données.
La consommation énergie est-elle optimisée ?	Non conforme	Car optique de multi utilisateur, donc là pas adaptée et pas optimisée
L'architecture technique est-elle adaptée ?	Conforme	Utilisation d'une architecture dites "three tiers" : Client – Serveur - BDD[27]
Les technologies utilisées sont-elles pertinentes par rapport au besoin de l'application ?	Conforme	Utilisation du HTML, CSS, JavaScript, PHP, MySQL, phpMyAdmin. Ce sont les technologies les plus utilisées afin de réaliser des applications web.
Le logiciel est-il de conception récente et fondé sur des technologies portables, non	Non conforme	La conception initiale date de 2006, l'application n'est pas en paradigme objet (pas de classes), la version de PHP utilisée est dépréciée.

[26] *Central Processing unit*
[27] Base de données

obsolètes et évolutives (matériel, OS, SGBD[28], outils de développements, …) ?		
Les technologies utilisées sont-elles matures et suffisamment répandues sur le marché (Linux, J2EE, .NET, etc.) ?	Conforme	Utilisation du HTML, CSS, JavaScript, PHP, MySQL, phpMyAdmin. Ce sont toutes des technologies extrêmement rependues et matures, qui sont encore misent à jour régulièrement.
Les technologies utilisées ont-elles suffisamment de marge pour faire face à un nombre croissant d'utilisateurs et de transactions	Conforme	Utilisation du HTML, CSS, JavaScript, PHP, MySQL, phpMyAdmin. Ce sont toutes des technologies extrêmement rependues et matures, qui sont encore misent à jour régulièrement. Elles sont utilisées sur tous types d'application web et peuvent gérer de nombreux utilisateurs si bien utilisées.
L'application évolue-t-elle régulièrement par versions successives ?	Non conforme	Crée en 2006 et mise à jour en 2008 et 2020. C'est une maintenance très irrégulière.

2. Recommandations

- Il serait pertinent de nettoyer les variables non utilisées dans le code afin de libérer de l'espace mémoire.
- De plus une actualisation serai nécessaire pour plus d'imperméabilité et une optimisation certaine.
- L'application devrait être mise à jour de façon bien plus régulière afin d'éviter les problèmes de dépréciations des versions/technologies utilisées.
- Revoir toutes la conception de l'application ainsi que celle de la base de données. Implémentation en paradigme objet ainsi que création de réelles relations dans la base de données. Cela permettrait d'alléger certains traitements et de gagner en performance.

[28] Système de Gestion de Base de Données

E. Impact environnemental, Accessibilité, Ergonomie

1. Impact environnemental

1. Checklist

ID	Thématique	Libellé du critère	Évaluation	Commentaire
1.1	Stratégie	Le service numérique a-t-il été évalué favorablement en termes d'utilité en tenant compte de ses impacts environnementaux ?	Non conforme	Pas d'évaluation
1.2	Stratégie	Le service numérique a-t-il défini ses cibles utilisatrices ?	Non conforme	Rien que le multiutilisateur et le fait qu'une telle application a été déployer
1.3	Stratégie	Le service numérique a-t-il défini les besoins métiers et les attentes réelles des utilisateurs cibles ?	Non conforme	Rien que le multiutilisateur et le fait qu'une telle application a été déployer
1.4	Stratégie	Le service numérique a-t-il défini la liste des profils de matériel que les utilisateurs vont pouvoir employer pour y accéder ?	Non conforme	L'application demande peu de ressources, y compris pour le host.
1.5	Stratégie	Le service numérique est-il utilisable sur des terminaux âgés de 5 ans ou plus ?	Conforme	L'application demande peu de ressources, y compris pour le host.
1.6	Stratégie	Le service numérique est-il utilisable sur des terminaux âgés de 5 ans ou plus ?	Non conforme	Ce n'est pas adapté au mobile first et n'est pas responsive
1.7	Stratégie	Le service numérique a-t-il été conçu avec des technologies standard interopérables plutôt que des technologies spécifiques et fermées ?	Conforme	Les technologies HTML/CSS/JS/PHP correspondes
1.8	Stratégie	Le service numérique a-t-il au moins un référent identifié en écoconception numérique ?	Non conforme	Il n'y a pas de référent identifié en écoconception
1.9	Stratégie	Le service numérique a-t-il identifié des indicateurs pour mesurer ses impacts environnementaux ?	Non conforme	Aucune présence d'indicateurs
1.10	Stratégie	Le service numérique s'est-il fixé des objectifs en matière de réduction ou de limitation de ses propres impacts environnementaux ?	Non conforme	Cela n'est pas préciser.
1.11	Stratégie	Le service numérique réalise-t-il régulièrement des revues pour s'assurer du respect de la réduction ou de la limitation de ses impacts environnementaux ?	Non conforme	Non car l'application date de Mathusalem
1.12	Stratégie	Le service numérique publie-t-il une déclaration ou une politique d'écoconception ?	Non conforme	Il n'y a rien de préciser
2.1	Spécifications	Le service numérique a-t-il été conçu avec une revue de conception et une revue de code en ayant pour un des objectifs de réduire les impacts environnementaux de chaque fonctionnalité ?	Non conforme	Aucune revue de conception ou de code dans cette optique
2.2	Spécifications	Le service numérique a-t-il prévu une stratégie de décommissionnement pour ses fonctionnalités, ses composants ou ses environnements non utilisés ?	Non conforme	Aucune stratégie de décommissionnement n'est prévue.

2.3	Spécifications	Le service numérique impose-t-il à ses fournisseurs de garantir une démarche de réduction de leurs impacts environnementaux ?	Non applicable	Pas de réel fournisseur
2.4	Spécifications	Le service numérique a-t-il pris en compte les impacts environnementaux des composants d'interface prêts à l'emploi utilisés ?	Non conforme	Ils n'ont pas réduit au maximum ce qu'ils envoient
2.5	Spécifications	Le service numérique a-t-il pris en compte les impacts environnementaux des services tiers utilisés lors de leur sélection ?	Non applicable	Pas de services tiers
3.1	Architecture	Le service numérique repose-t-il sur une architecture, des ressources ou des composants conçus pour réduire leurs propres impacts environnementaux ?	Non conforme	Non car ils ont fait comme ils ont pu
3.2	Architecture	Le service numérique fonctionne-t-il sur une architecture pouvant adapter la quantité de ressources utilisées en fonction de la consommation du service ?	Non conforme	Ce n'est pas le cas
3.3	Architecture	Le service numérique a-t-il pris en compte l'évolution technique des protocoles ?	Non conforme	Pas de passage à PHP8 ni à l'évolution du web
3.4	Architecture	Le service numérique utilise-t-il un protocole d'échange adapté aux contenus transférés ?	Non conforme	Certes ça passe sur le flux RSS mais pas sur mysqli pour la liaison BDD
3.5	Architecture	Le service numérique garantit-il la mise à disposition de mises à jour correctives pendant toute la durée de vie prévue des équipements et des logiciels liés au service ?	Non applicable	Peut-être pendant leur déploiement
3.6	Architecture	Le service numérique propose-t-il d'installer des mises à jour correctives indépendamment des mises à jour évolutives ?	Non conforme	Ce n'est plus suivie depuis longtemps
4.1	UX/UI[29]	Le service numérique est-il utilisable via une connexion bas débit ?	Non conforme	Ne passe pas avec la limitation de bande passante d'un navigateur
4.2	UX/UI	Le service numérique comporte-t-il uniquement des éléments animations, vidéos et sons dont la lecture automatique est désactivée ?	Conforme	Il n'y en a pas donc conforme.
4.3	UX/UI	Le service numérique affiche-t-il uniquement des contenus sans défilement de page infini ?	Conforme	Il n'y a pas de page infini
4.4	UX/UI	Le service numérique optimise-t-il le parcours de navigation pour chaque fonctionnalité principale ?	Non conforme	Non car des éléments fonctionnels important ne sont pas en avant
4.5	UX/UI	Le service numérique permet-il à l'utilisateur de décider de l'activation d'un service tiers ?	Non applicable	Il n'y en a pas
4.6	UX/UI	Le service numérique utilise-t-il majoritairement des composants fonctionnels natifs du système d'exploitation, du navigateur ou du langage utilisé ?	Conforme	Pas vraiment de librairie externe utilisées
4.7	UX/UI	Le service numérique utilise-t-il uniquement du contenu vidéo, audio et animé porteur d'informations ?	Non conforme	Il n'y en a pas
4.8	UX/UI	Le service numérique utilise-t-il du texte ou de l'image au lieu de contenu vidéo, audio ou animé lorsque cela est possible ?	Conforme	Oui car pas de vidéo
4.9	UX/UI	Le service numérique permet-il de mettre en pause les animations, défilement ou clignotement ?	Non applicable	Il n'y a rien de cela.

[29] Expérience utilisateur / Interface utilisateur

4.10	UX/UI	Le service numérique utilise-t-il majoritairement des polices de caractères du système d'exploitation ?	Conforme	Helvetica, Arial, Sans-Serif
4.11	UX/UI	Le service numérique limite-t-il les requêtes serveur lors de la saisie utilisateur ?	Non conforme	Pas vraiment, pas de buffer pour les loads
4.12	UX/UI	Le service numérique informe-t-il l'utilisateur du format de saisie attendu avant sa validation ?	Non conforme	Pas de texte précisant les formats attendus, notamment pour les dates
4.13	UX/UI	Le service numérique vérifie-t-il les saisies et les formats de données obligatoires à la soumission d'un formulaire sans requête serveur lorsque c'est possible ?	Non conforme	Pas de vérification poussée
4.14	UX/UI	Le service numérique informe-t-il l'utilisateur, avant le transfert, des poids et formats de fichier attendus ?	Non conforme	Aucune information donnée
4.15	UX/UI	Le service numérique vérifie-t-il des limites de poids et de formats sur les fichiers pouvant être transmis par l'utilisateur ?	Non conforme	Volume non mais format oui
4.16	UX/UI	Le service numérique indique-t-il à l'utilisateur que l'utilisation d'une fonctionnalité a des impacts environnementaux importants ?	Non conforme	Aucune information à propos des impacts environnementaux
4.17	UX/UI	Le service numérique propose-t-il des notifications uniquement lorsque c'est nécessaire ?	Non conforme	Alerte qui ne devrait pas exister car vérification des saisies
4.18	UX/UI	Le service numérique permet-il à l'utilisateur de contrôler les notifications qu'il reçoit ?	Non conforme	Nous n'avons pas l'action sur les alertes
4.19	UX/UI	Le service numérique fournit-il à l'utilisateur un moyen de contrôle sur ses contenus et ses services afin de réduire les impacts environnementaux ?	Conforme	Il est possible de supprimer toutes les données des tâches terminées
5.1	Contenus	Le service numérique utilise-t-il un format de fichier adapté au contenu et au contexte de visualisation de chaque image ?	Conforme	Oui même si on pourrait compresser
5.2	Contenus	Le service numérique propose-t-il des images dont le niveau de compression est adapté au contenu et au contexte de visualisation ?	Non conforme	Fichiers non compressés mais ils ont essayé de réduire leur poids a maximum
5.3	Contenus	Le service numérique utilise-t-il un format de fichier adapté au contenu et au contexte de visualisation pour chaque vidéo ?	Non applicable	Pas de vidéo
5.4	Contenus	Le service numérique propose-t-il des vidéos dont le niveau de compression est adapté au contenu et au contexte de visualisation ?	Non applicable	Pas de vidéo
5.5	Contenus	Le service numérique utilise-t-il un format de fichier adapté au contenu et au contexte d'écoute de chaque contenu audio ?	Non applicable	Pas d'audio
5.6	Contenus	Le service numérique propose-t-il des contenus audios dont le niveau de compression est adapté au contenu et au contexte d'écoute ?	Non applicable	Pas d'audio
5.7	Contenus	Le service numérique utilise-t-il un format de fichier adapté au contenu et au contexte d'utilisation pour chaque document ?	Conforme	Utilisation du format PNG sur les images quand cela est nécessaire.
5.8	Contenus	Le service numérique propose-t-il des documents dont le niveau de compression est adapté au contenu et au contexte d'utilisation ?	Non conforme	Aucune compression

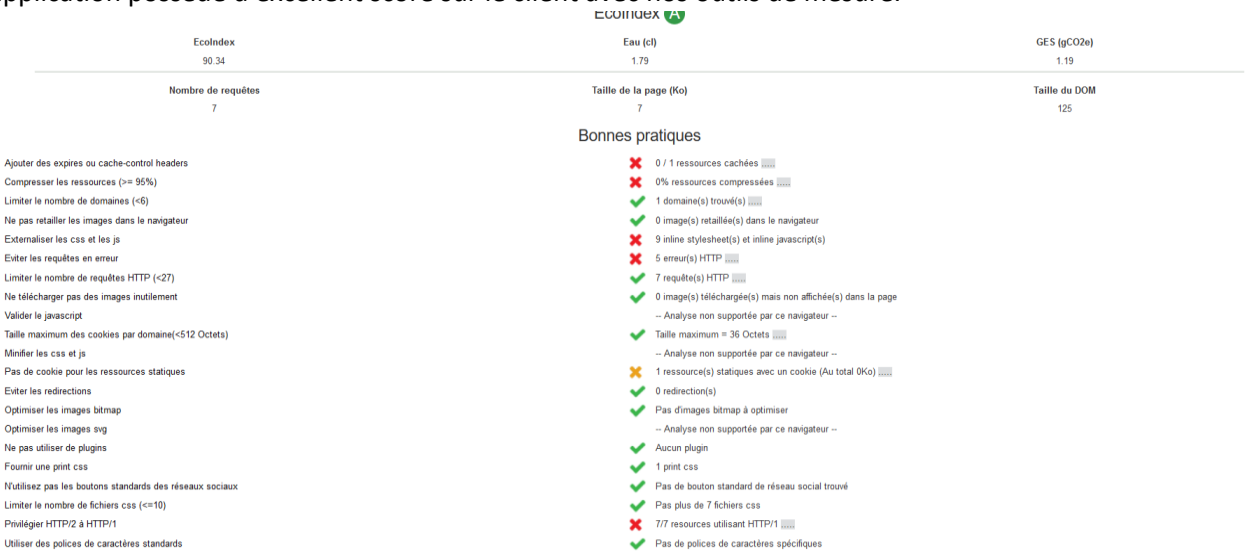
5.9	Contenus	Le service numérique a-t-il une stratégie d'archivage et de suppression, automatiques ou manuelles, des contenus obsolètes ou périmés ?	Non conforme	Pas de suppression automatique
6.1	Frontend	Le service numérique s'astreint-il à un poids maximum par écran ?	Conforme	Il est fait que pour un écran
6.2	Frontend	Le service numérique s'astreint-il à une limite de requêtes par écran ?	Non conforme	Il fait beaucoup de requêtes
6.3	Frontend	Le service numérique utilise-t-il des mécanismes de mises en cache pour la totalité des contenus transférés dont il a le contrôle ?	Non conforme	Duplication du CSS qui sera en cache
6.4	Frontend	Le service numérique a-t-il mis en place des techniques de compression sur la totalité des ressources transférées dont il a le contrôle ?	Non conforme	Aucune compression
6.5	Frontend	Le service numérique affiche-t-il majoritairement des éléments graphiques et des médias dont les dimensions d'origine correspondent aux dimensions du contexte d'affichage ?	Conforme	Tout est au bon format
6.6	Frontend	Le service numérique propose-t-il un mécanisme de chargement progressif pour les éléments graphiques et les médias le nécessitant ?	Non applicable	Rien ne le nécessite
6.7	Frontend	Le service numérique se limite-t-il au chargement des composants utilisés au sein des bibliothèques lorsque cela est possible ?	Non applicable	Pas de librairie externe
6.8	Frontend	Le service numérique évite-t-il de déclencher le chargement de ressources et de contenus inutilisés pour chaque fonctionnalité ?	Non conforme	Plusieurs CSS pas toujours utiles
6.9	Frontend	Le service numérique utilise-t-il un stockage côté client de certaines ressources afin d'éviter des échanges réseaux inutiles ?	Non conforme	Pas de cookies
6.10	Frontend	Le service numérique restreint-il l'usage des capteurs des terminaux utilisateur au besoin du service plutôt qu'en permanence ?	Non applicable	Pas d'utilisation des capteurs chez le client
6.11	Frontend	Le service numérique héberge-t-il les ressources statiques transférées dont il est l'émetteur sur un même domaine ?	Non applicable	
7.1	Backend	Le service numérique a-t-il recours à un système de cache serveur pour les données les plus utilisées ?	Non conforme	Aucun système de cache n'est utilisé, toutes les données sont stockées en BDD.
7.2	Backend	Le service numérique est-il configuré pour transmettre depuis le serveur des contenus compressés au client qui les accepte ?	Non conforme	Le fichier de données exportées en .csv n'est pas compressé.
7.3	Backend	Le service numérique définit-il des durées de conservation sur les données et documents qui le nécessitent ?	Non conforme	La seule donnée qui pourrait est la session utilisateur, cependant elle est stockée dans la base de données et n'expire jamais.
7.4	Backend	Le service numérique archive-t-il ou supprime-t-il les données et documents après expiration de leur durée de conservation ?	Non conforme	La seule donnée qui pourrait est la session utilisateur, cependant elle est stockée dans la base de données et n'expire jamais.
7.5	Backend	Le service numérique informe-t-il l'utilisateur d'un traitement en cours en arrière-plan ?	Non conforme	L'utilisateur n'est jamais tenu au

				courant des traitements en arrière-plan.
8.1	Hébergement	Le service numérique utilise-t-il un hébergement signataire du Code de Conduite européen sur les Datacentres ?	Non applicable	Le service numérique est open source et mis à disposition de tout le monde. La gestion de l'hébergement est donc propre à chaque entité utilisant le service.
8.2	Hébergement	Le service numérique utilise-t-il un hébergement ayant une démarche de réduction de son impact écologique ?	Non applicable	Le service numérique est open source et mis à disposition de tout le monde. La gestion de l'hébergement est donc propre à chaque entité utilisant le service.
8.3	Hébergement	Le service numérique utilise-t-il un hébergement qui fournit une politique de gestion durable des équipements ?	Non applicable	Le service numérique est open source et mis à disposition de tout le monde. La gestion de l'hébergement est donc propre à chaque entité utilisant le service.
8.4	Hébergement	Le service numérique utilise-t-il un hébergement qui fournit des indicateurs d'impacts environnementaux liés à son activité ?	Non applicable	Le service numérique est open source et mis à disposition de tout le monde. La gestion de l'hébergement est donc propre à chaque entité utilisant le service.
8.5	Hébergement	Le service numérique utilise-t-il un hébergement dont le PUE (Power Usage Effectiveness) est communiqué ?	Non applicable	Le service numérique est open source et mis à disposition de tout le monde. La gestion de l'hébergement est donc propre à chaque entité utilisant le service.
8.6	Hébergement	Le service numérique utilise-t-il un hébergement dont son WUE (Water Usage Effectiveness) est communiqué ?	Non applicable	Le service numérique est open source et mis à disposition de tout le monde. La gestion de l'hébergement est donc propre à chaque

				entité utilisant le service.
8.7	Hébergement	Le service numérique utilise-t-il un hébergement dont la consommation d'électricité est majoritairement d'origine renouvelable ?	Non applicable	Le service numérique est open source et mis à disposition de tout le monde. La gestion de l'hébergement est donc propre à chaque entité utilisant le service.
8.8	Hébergement	Le service numérique utilise-t-il un hébergement dont la localisation géographique est en cohérence avec celle de ses utilisateurs et de ses activités ?	Non applicable	Le service numérique est open source et mis à disposition de tout le monde. La gestion de l'hébergement est donc propre à chaque entité utilisant le service.
8.9	Hébergement	Le service numérique héberge-t-il de façon distincte les données « chaudes » et « froides » ?	Non conforme	Toutes les données sont gérées de la même façon : sur la base de données.
8.10	Hébergement	Le service numérique duplique-t-il les données uniquement lorsque cela est nécessaire ?	Non conforme	Certaines images / icones sont présentes deux fois dans deux dossier différents (/images et /styles/images)
8.11	Hébergement	Le service numérique utilise-t-il une redondance uniquement lorsque cela est nécessaire ?	Non conforme	Le service numérique est open source et mis à disposition de tout le monde. La gestion de l'hébergement est donc propre à chaque entité utilisant le service.
8.12	Hébergement	Le service numérique utilise-t-il un hébergement qui récupère la chaleur fatale produite par les serveurs ?	Non applicable	Le service numérique est open source et mis à disposition de tout le monde. La gestion de l'hébergement est donc propre à chaque entité utilisant le service.
		Taux de conformité sur 79 critères évalués	**43%**	

2. *Recommandations*

L'application possède d'excellent score sur le client avec nos outils de mesure.



Date	Nombre requêtes	Taille(kb)	Taille du dom	GES[30]	Eau	ecoIndex	Note
07/03/2023 10:46:00	0	0	120	1.13	1.69	93.66	A
07/03/2023 10:45:00	13	8	122	1.21	1.81	89.65	A

Il faudrait augmenter le nombre des bonnes pratiques de l'application afin d'obtenir encore de meilleurs scores. Ce pourrait être le fait de compresser les données qui peuvent l'être, utiliser le cache ou encore définir dates d'expiration sur des données temporaires dans le temps afin de les supprimer.

[30] Gaz à effet de serre

2. Accessibilité

3. Checklist

N°	Paramètres à vérifier	Vérifié / Pas vérifié	Commentaire / Justification
A1	Chaque image porteuse d'information a-t-elle une alternative textuelle ?	Pas vérifié	Car nous retrouvons des images n'ayant pas de "alt" comme descriptif tel que le drapeau jaune et le drapeau rouge pour signifier l'état de votre tâche. Voir : Annexe 11 : Preuve d'audit - A1 - Textes alternatifs
A2	Chaque image de décoration est-elle correctement ignorée par les technologies d'assistance ?	Vérifié	Aucune image de décoration n'est vu par le narrateur.
A3	Dans chaque page web, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle respectée ?	Pas vérifié	Dans la "sidebar", les couleurs rouges et vertes pour préciser les tâches validées et à réaliser ne respectent pas cette règle. Voir : Annexe 12 : Preuve d'audit - A3 - Représentation d'information par couleur
A4	Dans chaque page web, le contraste entre la couleur du texte ou image et la couleur de son arrière-plan est-il suffisamment élevé ?	Pas vérifié	Certaines images ne correspondent pas à l'accessibilité.
A5	Chaque lien est-il explicite ?	Vérifié	Le nom des alternatives textuelles des liens est en général très explicite : "home", "settings", etc.
A6	Dans chaque page web, chaque lien a-t-il un intitulé ?	Vérifié	Tous les liens ont une alternative textuelle, aucun lien en dur dans le site.
A7	Chaque script est-il contrôlable par le clavier et par tout dispositif de pointage ?	Pas vérifié	L'application est globalement gérable rien qu'à l'aide du clavier. Cependant il n'est pas possible de sélectionner une date dans le calendrier, le format n'étant pas précisé, il n'est pas possible de saisir une date seulement au clavier. Voir : Annexe 13 : Preuve d'audit - A7 - Calendrier
A8	Chaque page web est-elle définie par un type de document ?	Vérifié	Chaque page web à bien à faire à une doctype.
A9	Dans chaque page web, la langue par défaut est-elle présente ?	Vérifié	Oui, la langue par défaut est bien précisée sur chaque page web.
A10	Chaque page web a-t-elle un titre de page ?	Pas vérifié	Car sur chaque page on retrouve TaskStep en titre de page ce qui n'est pas explicite. Voir : Annexe 14 : Preuve d'audit - A10 - Titres non adaptés
A11	Dans chaque page web, chaque changement de langue est-il indiqué dans le code source ?	Pas vérifié	Lorsque nous changeons de langues dans la config.php, la valeur de l'attribut "lang" dans le code source reste "en".

			Voir : Annexe 15 : Preuve d'audit - A11 - Changement de langue en config ne change pas la balise
A12	Les textes sont-ils bien tous de la langue indiquée ?	Pas vérifié	Car ça ne change pas de langue pour la page elle-même, de plus certains textes ne sont pas traduits comme le pied de page ou même le style du CSS.
A13	Dans chaque page web, pour chaque élément recevant le focus, la prise de focus est-elle visible ?	Vérifié	Oui le focus est visible pour chaque élément du site.
A14	Pour chaque page web, les contenus cachés ont-ils vocation à être ignorés par les technologies d'assistance ?	Vérifié	Exemple : les champs “hidden”(caché), qui servent uniquement les développeurs et ont vocations à être ignorés par les technologies d’assistance.
A15	La taille des caractères permet-elle une lecture aisée ?	Pas vérifié	Car à l’aide de l’extension WAVE, nous retrouvons des alertes nous indiquant que le texte est très petit à certains endroits.
A16	L’espacement des caractères permet-il une lecture aisée ?	Vérifié	L’espacement des caractères permet une lecture aisée
A17	La hauteur de ligne permet-elle une lecture aisée ?	Vérifié	L’espacement des caractères permet une lecture aisée
A18	La lecture des blocs de texte est-elle accessible ?	Vérifié	La lecture des blocs de texte est accessible.
A19	La page 404 est-elle personnalisée ?	Pas vérifié	Non, l’erreur 404 est celle proposée de base.
A20	Sur chaque page, les textes importants sont pris en compte par les technologies d'assistance ?	Pas vérifié	Nous retrouvons des balises <select> lors de la création d’une tâche, ces balises sont les choix que l’on doit faire pour choisir la section/ contexte / projet et ne sont pas prisent en compte par le narrateur. Voir : Annexe 16 : Preuve d'audit - A20 - Eléments non pris en charge par le narrateur

4. Recommandations

- Ajouter des textes alternatifs (attribut “alt”) à toutes les images porteuses d’information, tels que les drapeaux de couleur représentants l’état d’une tâche. (Cf. A1)
- Donner une alternative textuelle à toutes les informations, notamment celles représentées uniquement par des couleurs comme dans la sidebar. (Cf. A3)
- Rendre l’application intégralement navigable au clavier ou avec tout autre dispositif de pointage, notamment le choix des dates dans le calendrier. (Cf. A7)
- Donner un titre pertinent à chaque page afin de pouvoir se situer plus facilement sur le site. (Cf. A10)
- Faire en sorte que le changement de langue dans la configuration change également la valeur de l’attribut “lang” sur toutes les pages, afin d’orienter le narrateur sur la langue dans laquelle est la page. (Cf. A11)
- Adapter la taille des caractères lorsqu’elle est jugée inadaptée selon les normes. (Cf. A15)

- Faire en sorte que l'entièreté des information importantes soient lues par le narrateur, notamment les différents éléments dans les balises <select>, ce qui n'est pas le cas actuellement. (Cf. A.20)

3. Ergonomie

Identification du logiciel/site testé : Taskstep 1.1

Identification du navigateur et du système d'exploitation avec lequel le test s'est déroulé : Windows 10 – Google Chrome, Mozilla Firefox, Edge

Description des parcours utilisateur testés :

Scénario n°1 :

- L'utilisateur se connecte
- Il crée un item
- Il va voir la liste de ces items sur la page "All Items"
- Il se déconnecte

1. *Le guidage*

Description :

- Ensemble des moyens mis en œuvre pour conseiller, orienter, informer et conduire l'utilisateur lors de ses interactions avec l'ordinateur.

- D'un point de vue général, il s'agit d'évaluer la façon dont le système prend en charge l'utilisateur.

- L'utilisateur doit comprendre clairement ce qu'il peut faire et comment il peut le faire. Le système doit donc le prendre en main pour le conduire efficacement.
- Un guidage trop présent peut devenir gênant lorsque la population à laquelle on s'adresse est experte avec l'outil informatique ou avec le système. En effet, certains des procédés permettant d'améliorer le guidage vont de pair avec une réduction de la vitesse d'exécution des actions.
- On ne peut cependant pas remettre en cause l'objectif du guidage. Il s'agit seulement de réfléchir en fonction de la population cible. Si elle est experte, on devra veiller à ne pas entraver ses actions et à lui permettre de les exécuter rapidement.

(1) 1.1 Incitation

Note : 1 /4

(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

- Inciter l'utilisateur à effectuer des actions spécifiques en lui fournissant des indices. Par exemple, guider les entrées de données en indiquant le format adéquat et les valeurs acceptables (ex : date (aaaa-mm-jj) _ _ _ _ / _ _ / _ _). Le mieux étant de proposer des contrôles spécifiques à l'entrée désirée (ex : une entrée calendrier pour choisir une date).

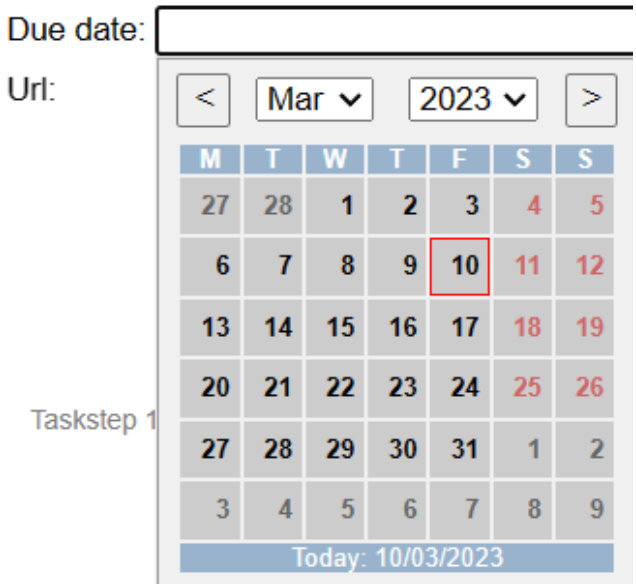
- Le critère d'incitation permet de juger des moyens mis en œuvre pour faire connaître à l'utilisateur le contexte dans lequel il se trouve et les actions qu'il peut effectuer. Par exemple, dans le domaine du web, il s'agit par exemple d'indiquer à l'utilisateur où il se trouve dans le site web et quels éléments sont cliquables.

Les + :

- Indication du nom pour chaque champ où des actions peuvent être faites.

Les - :

- Pas de précision pour le format de la date dans la création de l'item :



Nous voyons en bas du calendrier le format possible attendu, or lors du choix de la date, on ne retrouve pas le même format de date :

Ce qui n'est vraiment pas claire.

- N'indique pas que l'utilisateur doit obligatoirement sélectionner une section / un contexte / un projet pour créer sa tâche.
- Aucun titre de page n'est proposé.

(2) 1.2 Groupement/Distinction entre Items

Note : **3 /4**

(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

- Groupement des différents éléments visuels de façon cohérente et ordonnée.

On peut grouper les items de 2 manières :

1.3.1 Groupement/Distinction par la Localisation

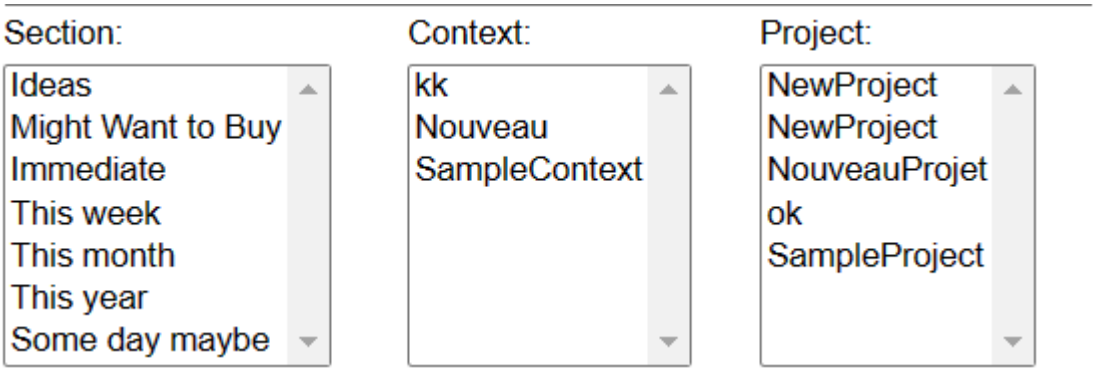
Positionner les items les uns par rapport aux autres afin d'indiquer leur appartenance, ou non, à une classe donnée d'objets. Par exemple, grouper les options de menus en fonction des objets sur lesquels elles s'appliquent.

1.3.2 Groupement/Distinction par le Format

Donner aux éléments des caractéristiques graphiques particulières afin d'indiquer leur appartenance, ou non, à une classe donnée d'objets. Par exemple : utiliser un symbole et la couleur rouge pour les boîtes de dialogue d'alerte ou d'erreur.

Les + :

- Les différents blocs ont un titre, nous permettant de les identifier

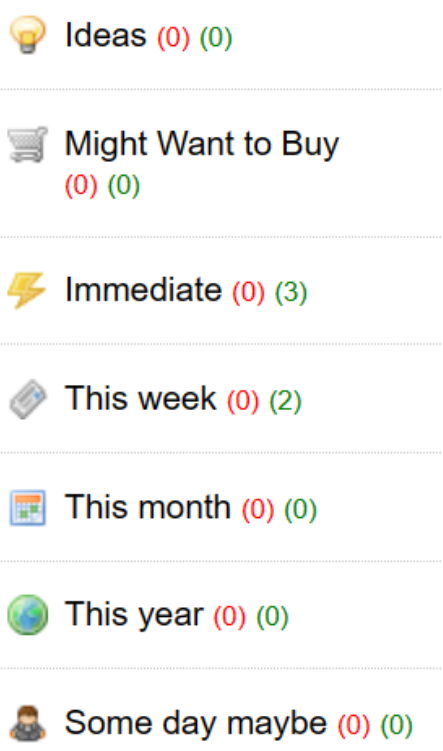


- Présence de caractéristiques graphiques particulières afin d'indiquer leur appartenance.

Les - :

- Manque de couleurs pour pouvoir les différencier.

- Couleurs du menu de gauche mal choisies (inverser les couleurs : il faut la couleur rouge pour “tâche à faire” et la couleur verte pour “tâche validée”).



(3) 1.3 Feedback Immédiat

Note : **3 /4**

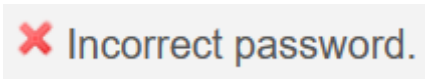
(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

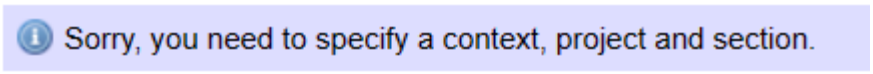
Dans tous les cas, l'ordinateur doit répondre à l'utilisateur en fonction des actions et des requêtes de ce dernier. Par exemple, dans les cas où les traitements sont longs, une information indiquant à l'utilisateur que les traitements sont en cours devrait lui être fournie.

Les + :

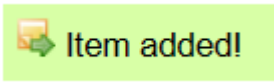
- Affichage du mot de passe incorrect



- Affichage de ce qu'il manque pour créer la tâche :



- Affichage permettant d'indiquer que la tâche à bien été créée :



Les - :

- Ne nous affiche pas le fait qu'une action se fait ou non.

(4) 1.4 Lisibilité

Note : **3 /4**

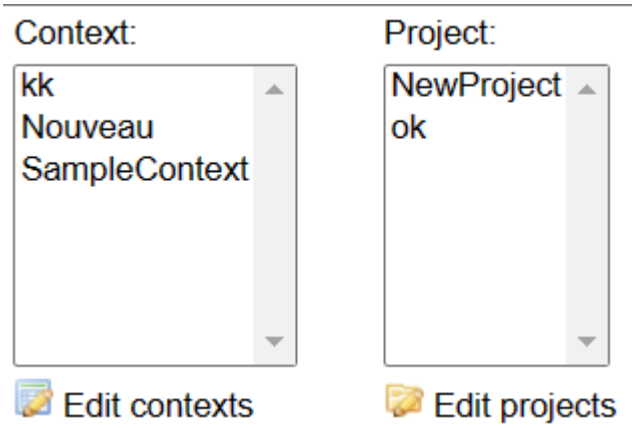
(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

Le critère Lisibilité concerne les caractéristiques de présentation des informations (éventuellement multimodales) dans un environnement visuel pouvant entraver ou faciliter la lecture de ces informations (luminance, contraste, dimension des objets, espacement entre les objets, fréquence sonore, intensité, timbre, etc.). Par convention, le critère Lisibilité ne concerne ni le feedback ni les messages d'erreurs.

Les + :

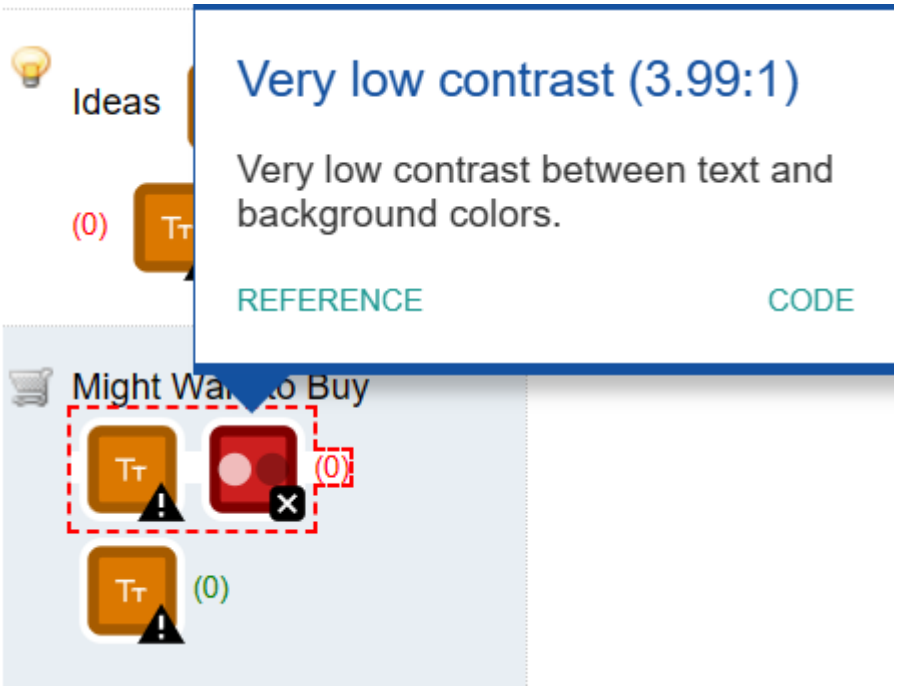
- Les textes sont bien lisibles.
- La dimension des objets est respectée.



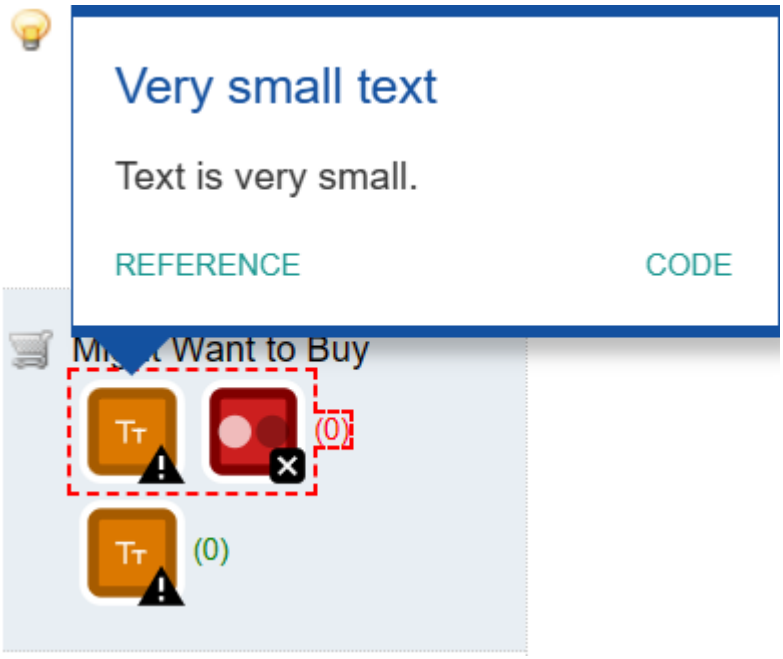
- Les espacements des objets sont aussi respectés.

Les - :

- Pour le menu de gauche, nous retrouvons des erreurs de contraste pour la valeur affichant le nombre de tâche terminée/validée en rouge.



- Nous retrouvons en plus de cette erreur de contraste pour la couleur rouge une alerte concernant la taille des valeurs affichant le nombre de tâche terminée/validée en rouge puis celles à réaliser en vert.



2. *Charge de travail*

Description :

L'ensemble des éléments de l'interface qui a un rôle dans la réduction de la charge perceptive ou mnésique des utilisateurs, de même que dans l'augmentation de l'efficacité du dialogue.

(5) 2.1 Brièveté

Note : **3 /4**

(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

Limiter le travail de lecture, d'entrée et les étapes par lesquelles doivent passer les usagers.

Cela se réalise en faisant attention essentiellement à 2 points :

2.1.1 Concision

Réduire la charge de travail au niveau perceptif et mnésique pour ce qui est des éléments individuels d'entrée ou de sortie. Par exemple, lorsqu'une unité de mesure est associée à un champ de données, celle-ci doit faire partie du label du champ plutôt qu'être saisie par l'utilisateur.

2.1.2 Actions Minimales

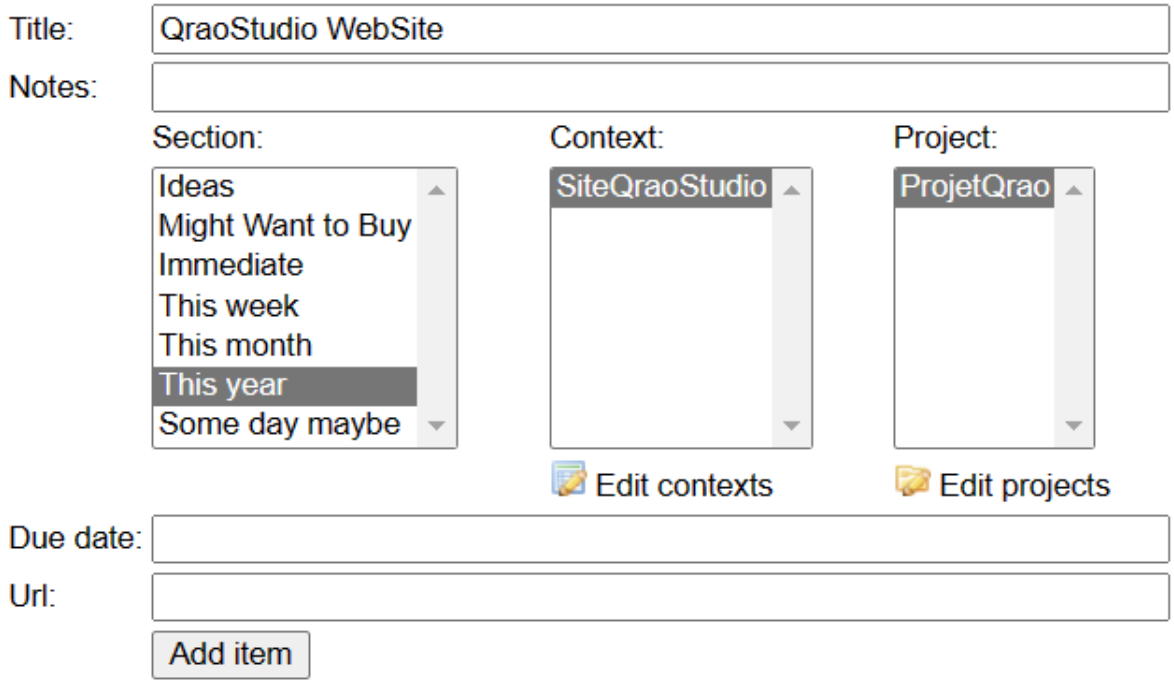
Limiter les étapes par lesquelles doivent passer les utilisateurs. Par exemple, ne pas demander aux utilisateurs d'entrer des données qui peuvent être déduites par le système.

Les + :

- Les différents champs d'entrer ne sont pas obligatoire pour la création d'une tâche.
  - Hormis la section / le contexte / le projet qui eux sont obligatoire pour savoir où placer la tâche donc c'est à nous de décider ce qu'on souhaite remplir.
- Le choix de la date sous forme de calendrier est intéressant pour avoir un visuel direct avec le temps qu'il reste pour réaliser la tâche.

Les - :

- Lorsque nous avons qu'un seul contexte ou qu'un seul projet, l'utilisateur sera quand même obligé de le sélectionner, Or ce n'est pas nécessaire.



(6) 2.2 Densité Informationnelle

Note : **2 /4**

(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

Réduire la charge de travail du point de vue perceptif et mnésique, pour des ensembles d'éléments et non pour des items. Par exemple, limiter la densité informationnelle de l'écran, en affichant seulement les informations nécessaires.

Les + :

- Les notes et l'url ne sont pas nécessaire mais peuvent être très utiles, autrement, le reste des éléments sont nécessaires donc n'ont pas à être enlever. Hormis ceux indiqués dans les -.

Les - :

- Des éléments ne sont pas nécessaires dans la page d'ajout de tâches :

Puisque nous pouvons retrouver ceux-ci autrement.

3. *Contrôle explicite*

Description :

Prise en compte par le système des actions explicites des utilisateurs et le contrôle qu'ont les utilisateurs sur le traitement de leurs actions.

(7) 3.1 Actions Explicites

Note : **2 /4**

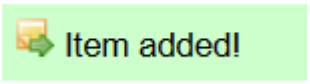
(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

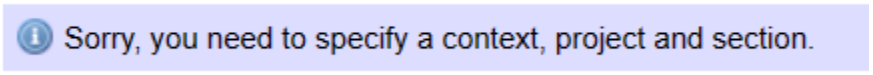
Expliciter la relation entre le fonctionnement de l'application et les actions des utilisateurs. Par exemple, l'entrée de commandes doit se terminer par une indication de fin (« Enter », « OK ») à laquelle des possibilités d'édition doivent être préalables.

Les + :

- Nous avons l'indication lorsque l'utilisateur à réussie à créer une tâche.



- Appuyer sur "Enter" est un réflexe normal dans un formulaire mais l'application gère le cas où nous n'avons pas les informations requises et avec un feedback.



Les - :

- Aucun élément visuel nous montre ce qui est obligatoire ou non avant de valider, pourrait mettre un (*) pour le montrer.
- Pas de changement d'état pour le bouton "update settings" sur la page settings lorsque quelque chose a été changé.

(8) 3.2 Contrôle Utilisateur

Note : **1 /4**

(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

L'utilisateur doit pouvoir contrôler le déroulement des traitements informatiques en cours. Par exemple, autoriser l'utilisateur à interrompre tout traitement en cours.

Les + :

- L'utilisateur peut à tout moment changer de page ou la mettre à jour ce qui permet d'interrompre ce qu'il allait faire.

Les - :

- Ne le fait pas s'il a déjà validé ou s'il revient en arrière.
- Lorsqu'un problème survient, l'utilisateur ne pourra l'enlever puis continuer ce qu'il à faire seulement s'il met à jour la page en faisant un rafraîchissement de la page, pour les moins calé en informatique, le problème pourrait ne pas être compris et forcerait l'utilisateur à fermer son navigateur carrément, ce qui le déconnecterait complétement.

4. *Adaptabilité*

Description :

Capacité à réagir selon le contexte et selon les besoins et les préférences des utilisateurs.

(9) 4.1 Flexibilité

Note : **2 /4**

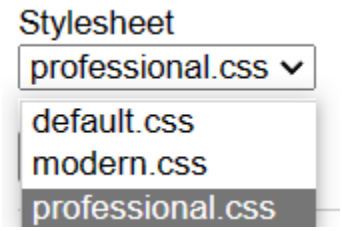
(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

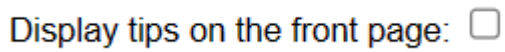
Mettre à la disposition des utilisateurs des moyens pour personnaliser l'interface afin de rendre compte de leurs stratégies ou habitudes de travail et des exigences de la tâche. Par exemple, les utilisateurs doivent pouvoir désactiver des affichages inutiles.

Les + :

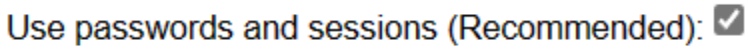
- Il peut choisir un style particulier dans les paramètres au préalable :



- Dans les paramètres il peut également retirer la fenêtre tips de l'accueil :



- Il peut également retirer les mots de passe et les sessions pour se connecter directement



Les - :

- Les interfaces ne sont pas modulables aux bons vouloir de l'utilisateur

(10) 4.2 Prise en Compte de l'Expérience de l'Utilisateur

Note : **1 /4**

(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

Le système doit respecter le niveau d'expérience de l'utilisateur. Par exemple, prévoir des choix d'entrées pas-à-pas ou multiples selon l'expérience des utilisateurs.

Les + :

- Feedback permettant d'avancer
- Tous les champs sont brièvement expliqués avec le mot qui le représente

Les - :

- Pas d'aide particulière à la navigation
- Pas de placeholder(Marque substitutive)
- Pas d'indication permettant de savoir ce qui est obligatoire ou non

5. *Gestion des Erreurs*

Description :

Moyens permettant d'une part d'éviter ou de réduire les erreurs, d'autre part de les corriger lorsqu'elles surviennent.

(11) 5.1 Protection Contre les Erreurs

Note : **1 /4**

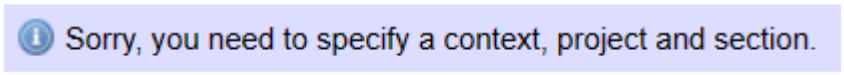
(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

Mettre en place des moyens pour détecter et prévenir les erreurs. Par exemple, toutes les actions possibles sur une interface doivent être envisagées et plus particulièrement les appuis accidentels des touches du clavier afin que les entrées non-attendues soient détectées.

Les + :

- Un affichage est présenté lorsque des champs obligatoires n'ont pas été sélectionnés et que l'on souhaite valider nos options.



Les - :

- Possède des failles n'ayant pas d'indication de ce qu'il faut faire.
- Devrait obliger l'utilisateur à sélectionner une date même si elle ne lui convient pas puis modifier par la suite s'il le souhaite car trop d'erreurs possibles.

(12) 5.2 Qualité des Messages d'Erreurs

Note : **1 /4**

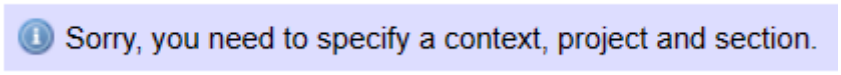
(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

S'assurer que l'information donnée aux utilisateurs sur la nature des erreurs commises (syntaxe, format, etc.) et sur les actions à entreprendre pour les corriger, soit pertinente, facile à lire et exacte. Par exemple, utiliser un vocabulaire neutre, non-personnalisé, non réprobateur dans les messages d'erreurs ; éviter l'humour.

Les + :

- Message d'erreurs assez compréhensible



Les - :

- Aucune solution pour expliquer comment régler le problème n'est proposée lorsqu'un problème apparait. Ne peut pas satisfaire le client s'il n'a pas l'habitude d'utiliser l'application.

(13) 5.3 Correction des Erreurs

Note : **2 /4**

(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

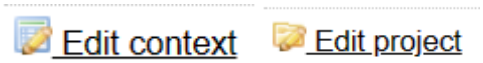
Description :

Mettre à la disposition des utilisateurs des moyens pour corriger leurs erreurs. Par exemple, fournir la possibilité de modifier les commandes lors de leur saisie.

Les + :

- Possibilité de modifier toutes les tâches ajoutées :

- Possibilité de modifier tous les contextes ou projets ajoutés :



Les - :

- Aucune information pour régler le problème n'est proposée lorsqu'il survient ne permettant pas à l'utilisateur d'être guider pour gérer ce problème.

6. *Homogénéité/Cohérence*

Note : **3 /4**

(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

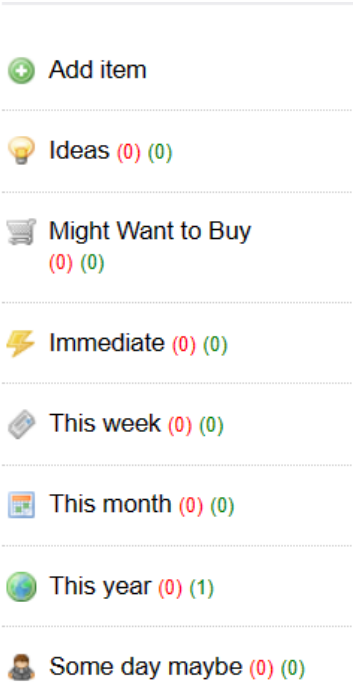
Les choix de conception d'interface doivent être conservés pour des contextes identiques, et doivent être différents pour des contextes différents. Par exemple, toujours afficher au même endroit l'incitation pour la saisie des données ou des commandes.

Les + :

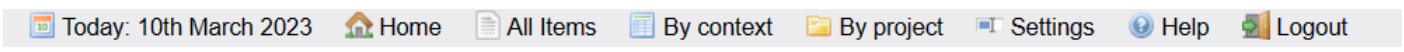
- Nous retrouvons le même style de pages pour chaque page.
- Le menu ne change jamais hors choix de l'utilisateur sur le "tips" :

  Display tips on the front page: ☐

- La barre latérale est toujours là même sur chaque page :

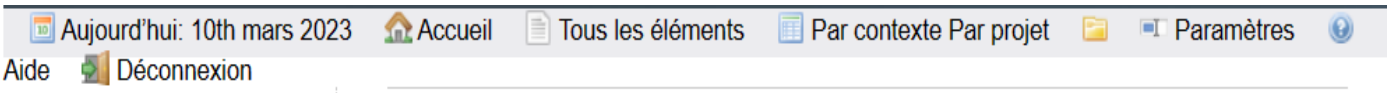


- De même pour la barre de navigation :



Les - :

- Lorsque nous traduisons la page à l'aide de l'outils du navigateur, les éléments changent et ne permettent pas à l'utilisateur d'être dans les meilleures conditions :



7. *Signifiance des Codes et Dénominations*

Note : **1 /4**

(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

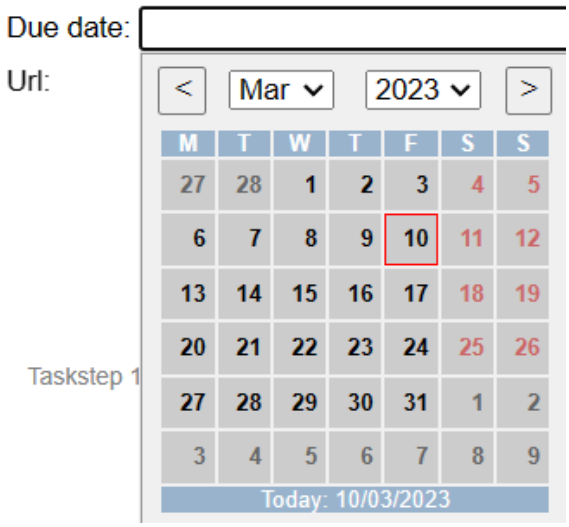
Il doit y avoir adéquation entre l'objet ou l'information affichée ou entrée, et son référent. Par exemple, rendre les règles d'abréviation explicites.

Les + :

- Chaque élément à un mot qui lui est associé pour permettre à l'utilisateur d'en déduire ce qu'il pourrait faire ou mettre.

Les - :

- Pas de précision pour le format de la date dans la création de l'item.



- Nous voyons en bas du calendrier le format possible attendu, hors lors du choix de la date, on ne retrouve pas le même format de date :

8. *Compatibilité*

Note : **3 /4**

(0 = très mauvais, 1 = mauvais, 2 = moyen, 3 = bon, 4 = très bon)

Description :

Il faut qu'il y ait accord entre les caractéristiques des utilisateurs et des tâches, d'une part, et l'organisation des sorties, des entrées et du dialogue d'une application donnée, d'autre part. Par exemple, les termes employés doivent être familiers aux utilisateurs, et relatifs à la tâche à réaliser.

Les + :

- Les mots employés dans l'application sont très clairs.
- Ainsi que les erreurs affichées.

Les - :

- Des indications pourraient quand même être différentes comme :

Où le "By" n'est pas nécessaire et pourrait porter à confusions.

9. *Synthèse*

Ici est présenté un bilan général du site ainsi que les remarques les plus importantes en faisant référence précisément aux sections du document concernées

TaskStep contient des fonctionnalités claires et des indications précises et faciles à comprendre.

Chaque champ contient un titre pour nous permettre de connaitre l'information recherchée.

Des choses peuvent être ajoutées ou améliorées sur le site, telles que :

- Des indications permettant à l'utilisateur d'apprendre facilement et rapidement les différentes fonctionnalités du site. (4. Adaptabilité).
- Des indications permettant à l'utilisateur de gérer facilement les problèmes qui apparaissent. (5. Gestion des Erreurs)
- Régler les erreurs de contrastes pour certaines catégories sur le site. (1.4 Lisibilité).
- Régler la taille de certains caractères. (1.4 Lisibilité).
- L'utilisateur peut changer le style de page de son compte puis enlever les tips affichés sur la page d'accueil ainsi que de ne pas être obligé de mettre un mot de passe, cependant, il ne peut pas changer le reste de l'interface du site. (4.1 Flexibilité).

VII. Plan d'action

A. Synthèse des actions à mener par un Plan d'action

Projet	Action	Priorité	Responsable de l'action	Charge (homme/heure)	Planification
Phase 1 : Refaire les architectures	Faire une conception en pensant MVC	1	L'ensemble des membres	2h	Début : 06/04/2023 fin : 2h plus tard
	Refaire la base de données	3	2 membres	1h	Début : 06/04/2023 fin : 1h plus tard
Phase 2 : Refaire le code de l'application, en respecter la nouvelle conception et les fonctionnalités	Implémenter notre conception avec comme cahier des charges l'ensemble des fonctionnalités de l'application actuelle	4	L'ensemble des membres	12h	Début : 24/04/2023 fin : 27/04/2023
	Tests unitaires	2	L'ensemble des membres	3h	Début : 06/04/2023 fin : 24/04/2023
Phase 3 : Refaire la partie graphique / UI de l'application	Arranger les éléments graphiques en se basant sur les précédentes versions et l'accessibilité	5	L'ensemble des membres	2h	Début : 27/04/2023 fin : 28/04/2023
Phase 4 : Réalisation de tests comparatifs et sessions correctives	Faire un avant/après de l'application	6	L'ensemble des membres	1h	Début : 28/04/2023 fin : 28/04/2023
	Préparation du déploiement	7	2 membres	2h	Début : 28/04/2023 fin : 02/05/2023

Tableau 3: Plan d'action

VIII. Références

Référentiel général d'écoconception de services numériques
Qu'est-ce qu'une attaque DDoS ?
Qu’est-ce qu’une attaque XSS (Cross-Site Scripting) ?
Les Rainbow Tables
Qu’est ce que l’OSINT et comment est-il utilisé en cybersécurité ?
MD5
Que sont SSL, TLS et HTTPS ?
What is Object-Oriented Programming?
Règlement général sur la protection des données
Conditions générales d'utilisation
Model Conceptuel des données

Vous retrouverez notamment en bas de pages des liens de références sur les mots clés de vocabulaire qui ont aidé la rédaction de l’audit.

Annexes

Annexe 1: Checklist qualité des données

Critères à vérifier	Conforme / Non conforme
Est-ce que la base de données respecte la troisième forme normale ?	
Est-ce que toutes les données misent en base de données sont pertinentes ?	
Est-ce que les données sont sécurisées ?	
Est-ce que la base de données respecte le RGPD et/ou la réglementation étatique ?	
Est-ce que l'application respecte le RGPD et/ou la réglementation étatique ?	
L'utilisateur accepte-il avec consentement éclairé le stockage de ses données ?	
L'utilisateur accepte-il avec consentement éclairé l'utilisation de ses données ?	
L'utilisateur peut-il demander la suppression des informations le concernant ?	
Peut-on récupérer toutes nos données ?	
Est-ce que le typage est cohérent avec les données ?	
Peut-on rendre le typage plus strict ?	
N'y a-t-il pas de relations inutiles ?	
Les relations sont-elles pertinentes ?	
Est-ce que les table ont une fonction distincte ?	
Y-a-t-il des doublons qui sont inutiles ?	
Y-a-t-il des redondances inutiles ?	
Les données inutilisées sont-elles supprimées au bout d'un moment ?	
Les cookies font-ils l'objet de consentement éclairé de l'utilisateur ?	
Le refus de ses cookies n'est-il pas bloquant ?	
En cas de changement de politique est-ce que l'utilisateur en est informé et accepte ces changements ?	
La base de données est-elle chiffrée ?	
Protection DDOS présente ?	
Est-ce que l'application gère les exceptions liées à nos données ?	
Les technologies utilisées sont-elles cohérentes ?	
Les technologies utilisées ne sont-t-elles pas obsolètes ?	
Le model des données est-il optimisé compte tenu de nos besoins ?	
Est-ce que les différents utilisateurs ont les permissions minimums ?	
Est-ce qu'un Deadlock est possible ? Si Conforme leur gestion est-elle pertinente et convenable ?	

nnexe 2: Checklist sécurité

Critères à vérifier	Conforme / Non conforme
Est-ce que l'application a conscience de son public cible ?	
Ont-ils une approche pertinente des problèmes de sécurité informatique ?	
Y a-t-il différents rôles gérés par l'application ?	
Ces rôles ont-ils les permission minimums compte tenu des fonctionnalités proposées par la solution ?	
Les données manipulées ont-elles toutes un effort suffisant de sécurité par rapport à leur sensibilité ?	
Les fonctionnalités proposées ont-elles toutes un effort suffisant de sécurité par rapport à leur sensibilité ?	
Le serveur communique-t-il sous un tunnel SSL avec le client ?	
Le serveur communique-t-il de manière sécurisée avec la base de données ?	
Le serveur possède-t-il des sécurités comme un anti-DDOS ?	
Est-ce que les mots de passe sont bien hachés ?	
Est-ce que la fonction de hachage est toujours aux normes ?	
Est-ce que le mot de passe de la base de données est changée ? (Plus par défaut)	
Est-ce que le mot de passe de base est changé ?	
Est-ce que l'on change de mot de passe lors de la première connexion ?	
Est-ce que la force des mots de passes est cohérent compte tenu de leur utilisation ?	
L'application utilise-t-elle les dernières normes de sécurité pour les communications ?	
L'application utilise-t-elle les dernières normes de sécurité dans le code ?	
Les injections SQL sont-elles possibles ?	
Y-a-il des protections sur la création de comptes anti-bot ?	
Existe-il un manuel d'administration de l'application, comprenant notamment : mode d'emploi du manuel, présentation du module d'administration de l'application, droits d'accès « type » par poste, procédure de création / modification / suppression de droits d'accès, …	
Existe-il un guide utilisateurs / manuel de procédures, comprenant notamment : mode d'emploi du manuel, présentation de l'application, mode opératoire, règles de gestion, écrans et zones de saisie, liste des messages d'erreurs, états de contrôle et d'exception.	
Existe-t-il une procédure de gestion des profils utilisateurs de l'application placée sous la responsabilité du propriétaire de l'application (procédure de création / modification et suppression des droits d'accès) ? Un dispositif de SSO est-il mis en œuvre ?	
Chaque utilisateur possède-t-il un identifiant qui lui est propre ? Vérifier qu'il n'existe pas de compte « générique » et que l'informatique (chef de projet) n'a que des accès en lecture au même titre que d'éventuels sous-traitants et éditeurs.	
Le mot de passe associé à l'identifiant permet-il d'assurer une protection d'accès efficace (7 caractères minimum, gestion de l'historique des mots de passe sur 2 ans, contrôle de « trivialité », changement trimestriel des mots de passe, etc.) ?	
Les tentatives de connexions infructueuses à l'application sont-elles enregistrées et contrôlées par le propriétaire de l'application ? Sont-elles limitées ?	
Les procédures de transmission de fichiers en entrée assurent-elles l'exhaustivité et l'exactitude des informations transmises (contrôles systèmes) ?	
Les contrôles mis en œuvre lors de l'intégration des données par fichiers à l'application sont-ils suffisants et identiques à ceux mis en œuvre dans le cadre d'une saisie transactionnelle (contrôles applicatifs) ?	

L'intégrité et l'exhaustivité des données transmises entre les différents modules de l'application et/ou à des applications en aval sont-elles assurées ?	
Existe-t-il une procédure formalisée et standard de maintenance de l'application ?	
La documentation de l'application est-elle systématiquement mise à jour après chaque intervention de maintenance ?	
La documentation d'exploitation est-elle à jour, dupliquée, protégée et inclut-elle les procédures de gestion des incidents et de reprise / redémarrage ?	
Évaluer le niveau de service par l'analyse des tableaux de bord.	
Les procédures de sauvegarde et de reprise de l'application sont-elles satisfaisantes et répondent-elles aux enjeux de l'application et aux engagements de service de l'informatique ?	
Une partie des sauvegardes est-elle stockée à l'extérieur de l'organisation (banque, société spécialisée) selon une périodicité adaptée aux enjeux ?	
En cas de sinistre grave, existe-t-il un plan de secours en adéquation avec les besoins et les enjeux (plan d'urgence, plan de repli, plan de reprise) ?	
La base de données est-elle chiffrée ?	
Est-ce qu'une démarche d'OSINT ne met pas en péril la sécurité de l'application ?	

Annexe 3: Checklist accessibilité

N°	Paramètres à vérifier	Vérifié / Pas vérifié	Commentaire / Justification
1	Chaque image porteuse d'information a-t-elle une alternative textuelle ?		
2	Chaque image de décoration est-elle correctement ignorée par les technologies d'assistance ?		
3	Dans chaque page web, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle respectée ?		
4	Dans chaque page web, le contraste entre la couleur du texte ou image et la couleur de son arrière-plan est-il suffisamment élevé ?		
5	Chaque lien est-il explicite ?		
6	Dans chaque page web, chaque lien a-t-il un intitulé ?		
7	Chaque script est-il contrôlable par le clavier et par tout dispositif de pointage ?		
8	Chaque page web est-elle définie par un type de document ?		
9	Dans chaque page web, la langue par défaut est-elle présente ?		
10	Chaque page web a-t-elle un titre de page ?		
11	Dans chaque page web, chaque changement de langue est-il indiqué dans le code source ?		
12	Les textes sont-ils bien tous de la langue indiquée ?		
13	Dans chaque page web, pour chaque élément recevant le focus, la prise de focus est-elle visible ?		
14	Pour chaque page web, les contenus cachés ont-ils vocation à être ignorés par les technologies d'assistance ?		
15	La taille des caractères permet-elle une lecture aisée ?		
16	L'espacement des caractères permet-il une lecture aisée ?		
17	La hauteur de ligne permet-elle une lecture aisée ?		
18	La lecture des blocs de texte est-elle accessible ?		
19	La page 404 est-elle personnalisée ?		
20	Sur chaque page, les textes importants sont pris en compte par les technologies d'assistance ?		

Annexe 4: Checklist performance

Critères à vérifier	Conforme / Non conforme	Commentaire / Justification
Les traitements sont-ils performants (vitesse d'exécution, réactivité) ?		
La consommation mémoire est-elle optimisée ?		
La consommation CPU est-elle optimisée ?		
La consommation énergie est-elle optimisée ?		
L'architecture technique est-elle adaptée ?		
Les technologies utilisées sont-elles pertinentes par rapport au besoin de l'application ?		
Le logiciel est-il de conception récente et fondé sur des technologies portables, non obsolètes et évolutives (matériel, OS, SGBD, outils de développements, …) ?		
Les technologies utilisées sont-elles matures et suffisamment répandues sur le marché (Linux, J2EE, .NET, etc.) ?		
Les technologies utilisées ont-elles suffisamment de marge pour faire face à un nombre croissant d'utilisateurs et de transactions		
L'application évolue-t-elle régulièrement par versions successives ?		

Annexe 5: Checklist qualité logicielle

Critères à vérifier	Conforme / Non conforme	Commentaire / Justification
L'application respecte-elle les principes SOLID ?		
Est-ce que le choix d'architecture est pertinent ?		
Des commentaires sont-ils présents partout et pertinents ?		
De la documentation est-elle présente partout et pertinente ?		
Y-a-t-il des ancres identifiables dans le code ?		
Est-ce que les technologies utilisées sont-elles aux normes ?		
Les designs pattern utilisés sont-ils cohérents ?		
Y-a-t-il des tests unitaires et sont-ils pertinents ?		
Est-il possible de faire planter l'application ?		
Les packages sont-ils cohérents avec l'architecture ?		
L'application fait elle ce que nous attendons ?		
L'application est-elle portable à d'autres os ?		
Les technologies utilisées sont-elles en accord avec le besoin ?		
La nomenclature est-elle cohérente ?		
La conception correspond-elle au code ?		
La conception a-t-elle été pensée compte tenu des besoins ?		
Mise à jour possible ?		
Les commentaires git sont-ils précis et utiles pour une reprise ?		

Annexe 6 : Checklist impact environnemental

ID	Thématique	Libellé du critère	Évaluation	Commentaire
1.1	Stratégie	Le service numérique a-t-il été évalué favorablement en termes d'utilité en tenant compte de ses impacts environnementaux ?		
1.2	Stratégie	Le service numérique a-t-il défini ses cibles utilisatrices ?		
1.3	Stratégie	Le service numérique a-t-il défini les besoins métiers et les attentes réelles des utilisateurs cibles ?		
1.4	Stratégie	Le service numérique a-t-il défini la liste des profils de matériel que les utilisateurs vont pouvoir employer pour y accéder ?		
1.5	Stratégie	Le service numérique est-il utilisable sur des terminaux âgés de 5 ans ou plus ?		
1.6	Stratégie	Le service numérique est-il utilisable sur des terminaux âgés de 5 ans ou plus ?		
1.7	Stratégie	Le service numérique a-t-il été conçu avec des technologies standard interopérables plutôt que des technologies spécifiques et fermées ?		
1.8	Stratégie	Le service numérique a-t-il au moins un référent identifié en écoconception numérique ?		
1.9	Stratégie	Le service numérique a-t-il identifié des indicateurs pour mesurer ses impacts environnementaux ?		
1.10	Stratégie	Le service numérique s'est-il fixé des objectifs en matière de réduction ou de limitation de ses propres impacts environnementaux ?		
1.11	Stratégie	Le service numérique réalise-t-il régulièrement des revues pour s'assurer du respect de la réduction ou de la limitation de ses impacts environnementaux ?		
1.12	Stratégie	Le service numérique publie-t-il une déclaration ou une politique d'écoconception ?		
2.1	Spécifications	Le service numérique a-t-il été conçu avec une revue de conception et une revue de code en ayant pour un des objectifs de réduire les impacts environnementaux de chaque fonctionnalité ?		
2.2	Spécifications	Le service numérique a-t-il prévu une stratégie de décommissionnement pour ses fonctionnalités, ses composants ou ses environnements non utilisés ?		
2.3	Spécifications	Le service numérique impose-t-il à ses fournisseurs de garantir une démarche de réduction de leurs impacts environnementaux ?		
2.4	Spécifications	Le service numérique a-t-il pris en compte les impacts environnementaux des composants d'interface prêts à l'emploi utilisés ?		
2.5	Spécifications	Le service numérique a-t-il pris en compte les impacts environnementaux des services tiers utilisés lors de leur sélection ?		
3.1	Architecture	Le service numérique repose-t-il sur une architecture, des ressources ou des composants conçus pour réduire leurs propres impacts environnementaux ?		
3.2	Architecture	Le service numérique fonctionne-t-il sur une architecture pouvant adapter la quantité de ressources utilisées en fonction de la consommation du service ?		
3.3	Architecture	Le service numérique a-t-il pris en compte l'évolution technique des protocoles ?		
3.4	Architecture	Le service numérique utilise-t-il un protocole d'échange adapté aux contenus transférés ?		

3.5	Architecture	Le service numérique garantit-il la mise à disposition de mises à jour correctives pendant toute la durée de vie prévue des équipements et des logiciels liés au service ?		
3.6	Architecture	Le service numérique propose-t-il d'installer des mises à jour correctives indépendamment des mises à jour évolutives ?		
4.1	UX/UI	Le service numérique est-il utilisable via une connexion bas débit ?		
4.2	UX/UI	Le service numérique comporte-t-il uniquement des éléments animations, vidéos et sons dont la lecture automatique est désactivée ?		
4.3	UX/UI	Le service numérique affiche-t-il uniquement des contenus sans défilement de page infini ?		
4.4	UX/UI	Le service numérique optimise-t-il le parcours de navigation pour chaque fonctionnalité principale ?		
4.5	UX/UI	Le service numérique permet-il à l'utilisateur de décider de l'activation d'un service tiers ?		
4.6	UX/UI	Le service numérique utilise-t-il majoritairement des composants fonctionnels natifs du système d'exploitation, du navigateur ou du langage utilisé ?		
4.7	UX/UI	Le service numérique utilise-t-il uniquement du contenu vidéo, audio et animé porteur d'informations ?		
4.8	UX/UI	Le service numérique utilise-t-il du texte ou de l'image au lieu de contenu vidéo, audio ou animé lorsque cela est possible ?		
4.9	UX/UI	Le service numérique permet-il de mettre en pause les animations, défilement ou clignotement ?		
4.10	UX/UI	Le service numérique utilise-t-il majoritairement des polices de caractères du système d'exploitation ?		
4.11	UX/UI	Le service numérique limite-t-il les requêtes serveur lors de la saisie utilisateur ?		
4.12	UX/UI	Le service numérique informe-t-il l'utilisateur du format de saisie attendu avant sa validation ?		
4.13	UX/UI	Le service numérique vérifie-t-il les saisies et les formats de données obligatoires à la soumission d'un formulaire sans requête serveur lorsque c'est possible ?		
4.14	UX/UI	Le service numérique informe-t-il l'utilisateur, avant le transfert, des poids et formats de fichier attendus ?		
4.15	UX/UI	Le service numérique vérifie-t-il des limites de poids et de formats sur les fichiers pouvant être transmis par l'utilisateur ?		
4.16	UX/UI	Le service numérique indique-t-il à l'utilisateur que l'utilisation d'une fonctionnalité a des impacts environnementaux importants ?		
4.17	UX/UI	Le service numérique propose-t-il des notifications uniquement lorsque c'est nécessaire ?		
4.18	UX/UI	Le service numérique permet-il à l'utilisateur de contrôler les notifications qu'il reçoit ?		
4.19	UX/UI	Le service numérique fournit-il à l'utilisateur un moyen de contrôle sur ses contenus et ses services afin de réduire les impacts environnementaux ?		
5.1	Contenus	Le service numérique utilise-t-il un format de fichier adapté au contenu et au contexte de visualisation de chaque image ?		
5.2	Contenus	Le service numérique propose-t-il des images dont le niveau de compression est adapté au contenu et au contexte de visualisation ?		
5.3	Contenus	Le service numérique utilise-t-il un format de fichier adapté au contenu et au contexte de visualisation pour chaque vidéo ?		

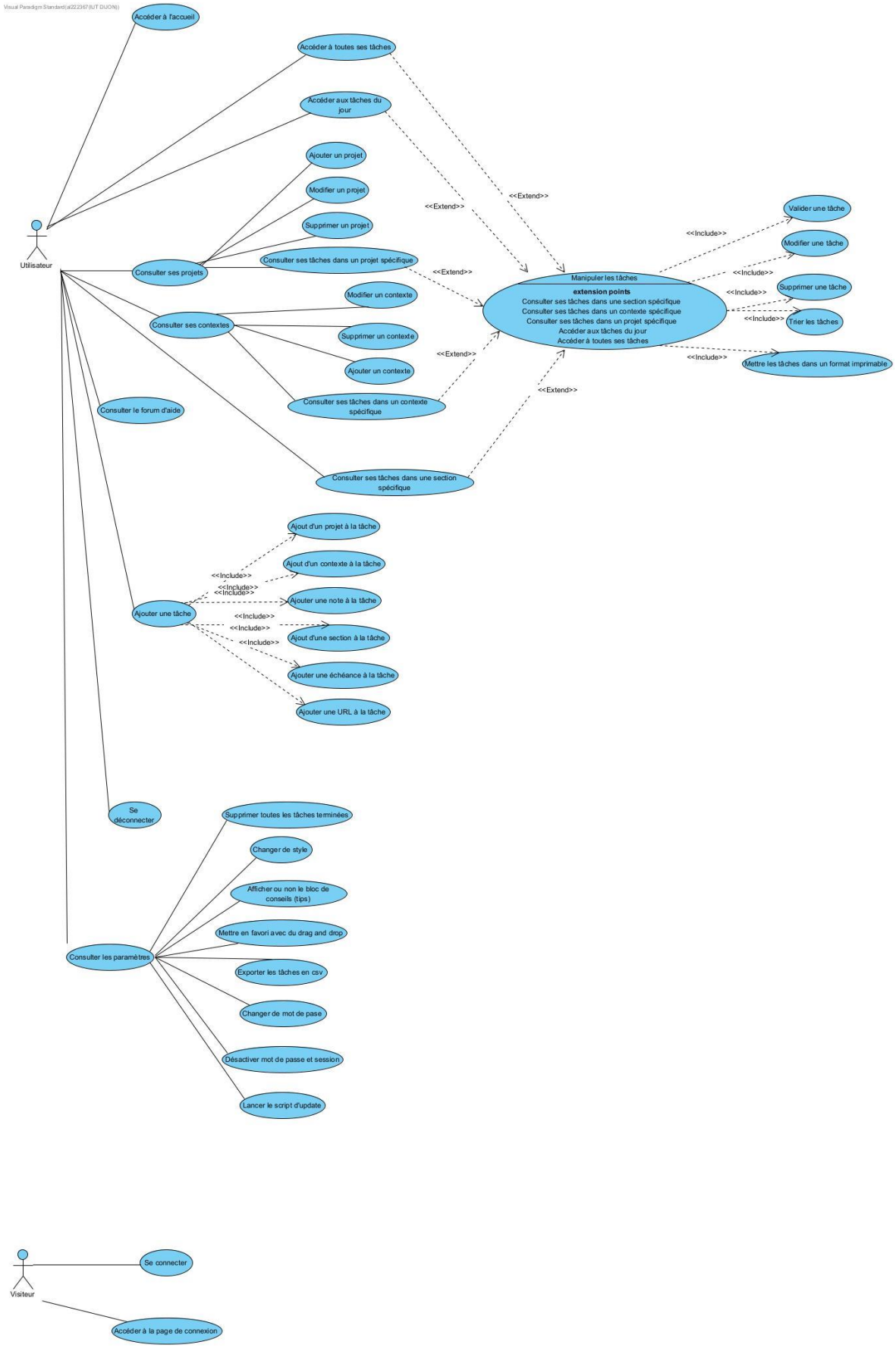
5.4	Contenus	Le service numérique propose-t-il des vidéos dont le niveau de compression est adapté au contenu et au contexte de visualisation ?		
5.5	Contenus	Le service numérique utilise-t-il un format de fichier adapté au contenu et au contexte d'écoute de chaque contenu audio ?		
5.6	Contenus	Le service numérique propose-t-il des contenus audios dont le niveau de compression est adapté au contenu et au contexte d'écoute ?		
5.7	Contenus	Le service numérique utilise-t-il un format de fichier adapté au contenu et au contexte d'utilisation pour chaque document ?		
5.8	Contenus	Le service numérique propose-t-il des documents dont le niveau de compression est adapté au contenu et au contexte d'utilisation ?		
5.9	Contenus	Le service numérique a-t-il une stratégie d'archivage et de suppression, automatiques ou manuelles, des contenus obsolètes ou périmés ?		
6.1	Frontend	Le service numérique s'astreint-il à un poids maximum par écran ?		
6.2	Frontend	Le service numérique s'astreint-il à une limite de requêtes par écran ?		
6.3	Frontend	Le service numérique utilise-t-il des mécanismes de mises en cache pour la totalité des contenus transférés dont il a le contrôle ?		
6.4	Frontend	Le service numérique a-t-il mis en place des techniques de compression sur la totalité des ressources transférées dont il a le contrôle ?		
6.5	Frontend	Le service numérique affiche-t-il majoritairement des éléments graphiques et des médias dont les dimensions d'origine correspondent aux dimensions du contexte d'affichage ?		
6.6	Frontend	Le service numérique propose-t-il un mécanisme de chargement progressif pour les éléments graphiques et les médias le nécessitant ?		
6.7	Frontend	Le service numérique se limite-t-il au chargement des composants utilisés au sein des bibliothèques lorsque cela est possible ?		
6.8	Frontend	Le service numérique évite-t-il de déclencher le chargement de ressources et de contenus inutilisés pour chaque fonctionnalité ?		
6.9	Frontend	Le service numérique utilise-t-il un stockage côté client de certaines ressources afin d'éviter des échanges réseaux inutiles ?		
6.10	Frontend	Le service numérique restreint-il l'usage des capteurs des terminaux utilisateur au besoin du service plutôt qu'en permanence ?		
6.11	Frontend	Le service numérique héberge-t-il les ressources statiques transférées dont il est l'émetteur sur un même domaine ?		
7.1	Backend	Le service numérique a-t-il recours à un système de cache serveur pour les données les plus utilisées ?		
7.2	Backend	Le service numérique est-il configuré pour transmettre depuis le serveur des contenus compressés au client qui les accepte ?		
7.3	Backend	Le service numérique définit-il des durées de conservation sur les données et documents qui le nécessitent ?		
7.4	Backend	Le service numérique archive-t-il ou supprime-t-il les données et documents après expiration de leur durée de conservation ?		
7.5	Backend	Le service numérique informe-t-il l'utilisateur d'un traitement en cours en arrière-plan ?		

8.1	Hébergement	Le service numérique utilise-t-il un hébergement signataire du Code de Conduite européen sur les Datacentres ?		
8.2	Hébergement	Le service numérique utilise-t-il un hébergement ayant une démarche de réduction de son impact écologique ?		
8.3	Hébergement	Le service numérique utilise-t-il un hébergement qui fournit une politique de gestion durable des équipements ?		
8.4	Hébergement	Le service numérique utilise-t-il un hébergement qui fournit des indicateurs d'impacts environnementaux liés à son activité ?		
8.5	Hébergement	Le service numérique utilise-t-il un hébergement dont le PUE (Power Usage Effectiveness) est communiqué ?		
8.6	Hébergement	Le service numérique utilise-t-il un hébergement dont son WUE (Water Usage Effectiveness) est communiqué ?		
8.7	Hébergement	Le service numérique utilise-t-il un hébergement dont la consommation d'électricité est majoritairement d'origine renouvelable ?		
8.8	Hébergement	Le service numérique utilise-t-il un hébergement dont la localisation géographique est en cohérence avec celle de ses utilisateurs et de ses activités ?		
8.9	Hébergement	Le service numérique héberge-t-il de façon distincte les données « chaudes » et « froides » ?		
8.10	Hébergement	Le service numérique duplique-t-il les données uniquement lorsque cela est nécessaire ?		
8.11	Hébergement	Le service numérique utilise-t-il une redondance uniquement lorsque cela est nécessaire ?		
8.12	Hébergement	Le service numérique utilise-t-il un hébergement qui récupère la chaleur fatale produite par les serveurs ?		
		Taux de conformité sur 79 critères évalués		

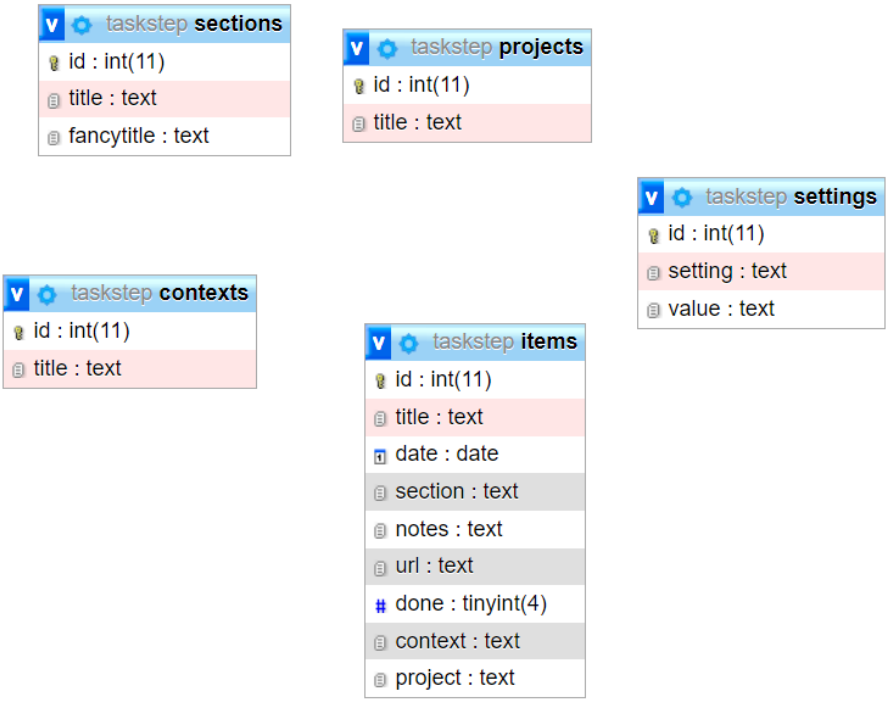
Annexe 7 : Checklist ergonomie

1. Guidage	
1.1 Lisibilité	
1.2 Incitation	
1.2 Groupement/Distinction entre Items	
1.3 Feedback immédiat	
2. Charge de travail	
2.1 Brièveté	
2.2 Densité Informationnelle	
3. Contrôle explicite	
3.1 Actions Explicites	
3.2 Contrôle Utilisateur	
4. Adaptabilité	
4.1 Flexibilité	
4.2 Prise en Compte de l'Expérience de l'Utilisateur	
5. Gestion des Erreurs	
5.1 Protection Contre les Erreurs	
5.2 Qualité des Messages d'Erreurs	
5.3 Correction des Erreurs	
6. Homogénéité/Cohérence	
7. Signifiance des Codes et Dénominations	
8. Compatibilité	
Moyenne :	

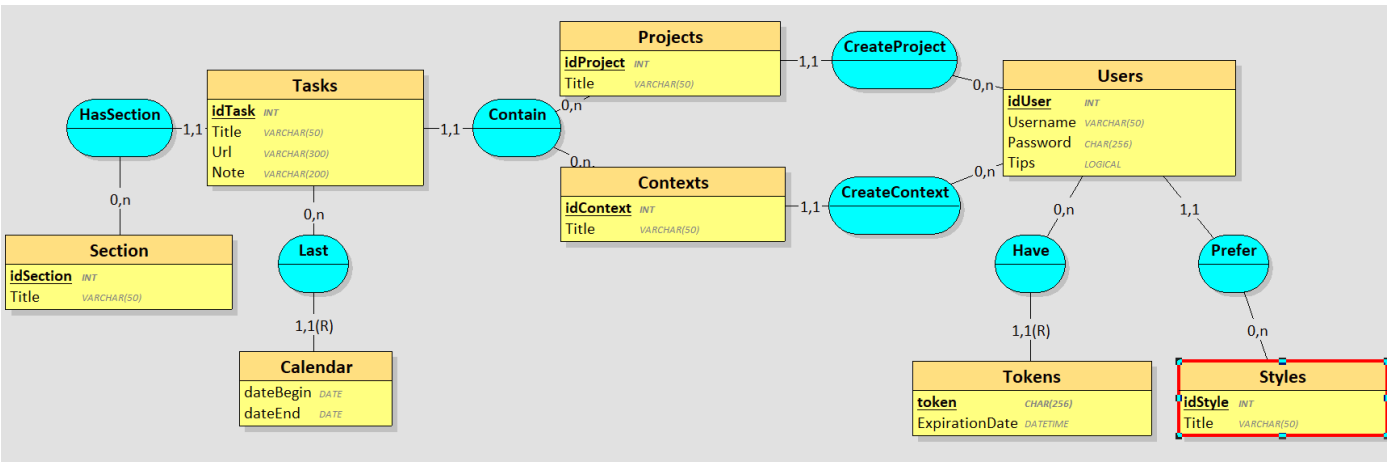
Annexe 8 : Diagramme des cas d'utilisation



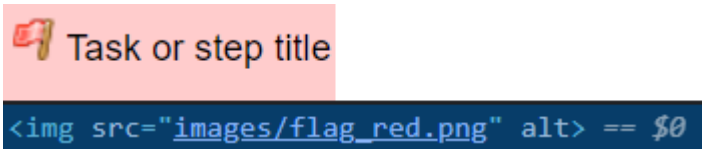
Annexe 9 : Qualité des données - MCD actuel



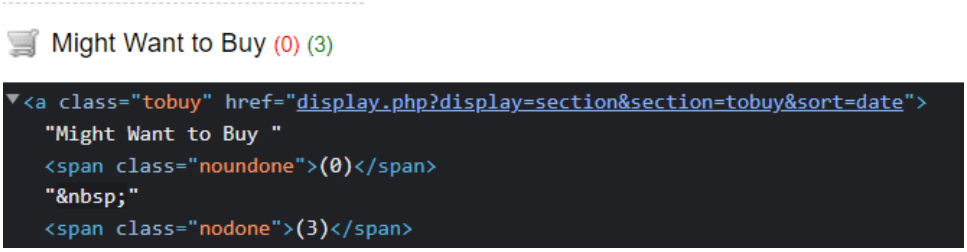
Annexe :10 Qualité des données - MCD proposé



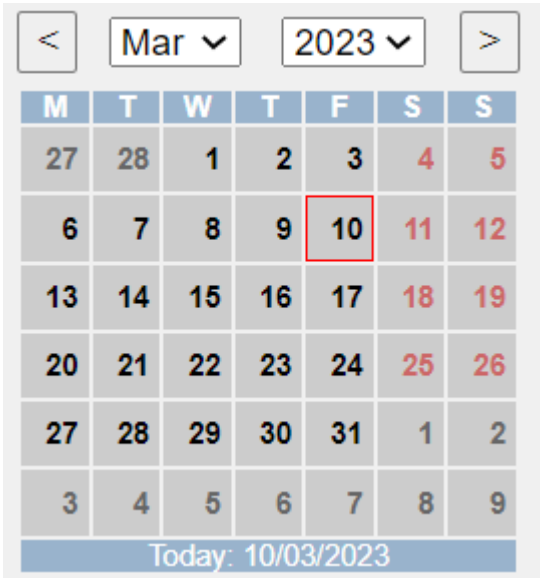
Annexe 11 : Preuve d'audit - A1 - Textes alternatifs



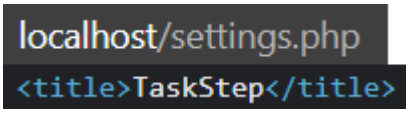
Annexe 12 : Preuve d'audit - A3 - Représentation d'information par couleur



Annexe 13 : Preuve d'audit - A7 - Calendrier



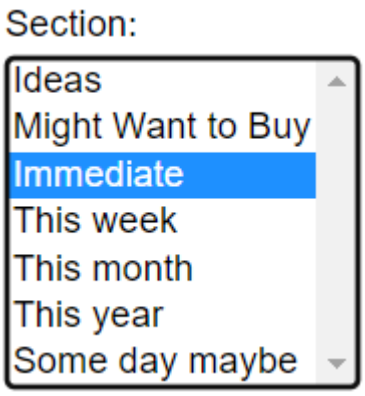
Annexe 14 : Preuve d'audit - A10 - Titres non adaptés



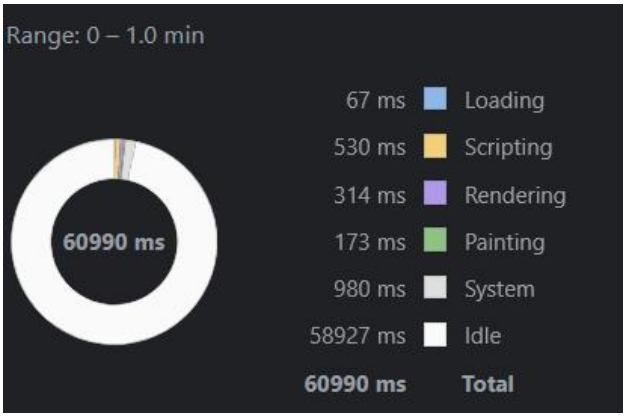
Annexe 15 : Preuve d'audit - A11 - Changement de langue en config ne change pas la balise

```
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
$language = 'ru';    // GUI language
```

Annexe 16 : Preuve d'audit - A20 - Eléments non pris en charge par le narrateur



Annexe 17 : Preuve d'audit - Analyse de la répartition du temps sur une minute d'utilisation



Annexe 18 : Preuve d'audit - Consommation mémoire sur une minute d'utilisation

Annexe 19 : Preuve d'audit - Code inutile et inutilisé

```
<body>
  <!--Open container-->
  <div id="sexyBG"></div>
  <div id="sexyBOX" onmousedown="document.onclick=function(){};" onmouseup="setTimeout('sexyTOG()',1);"></div> event
  <div id="container">…</div>
 </body>
</html>
```

Annexe 20 : Flux RSS jamais utilisé

```
<link rel="alternate" type="application/rss+xml" title="RSS" href="<?php selfref_url(); ?>rss.php" />
```

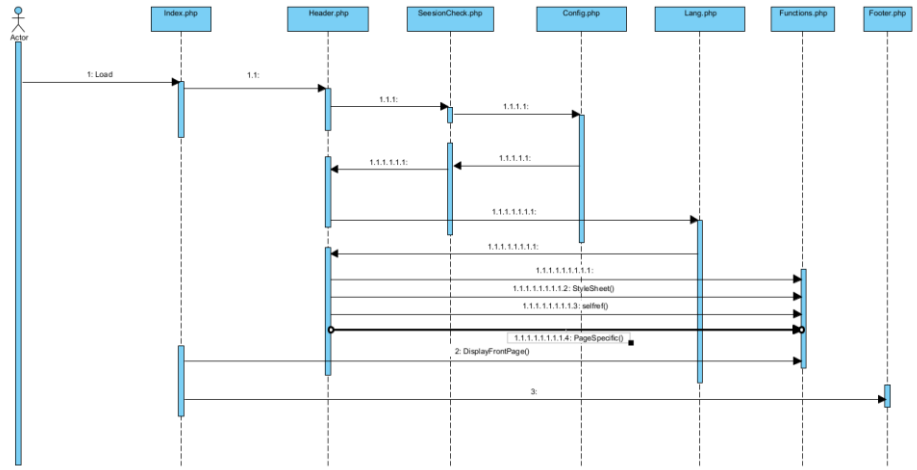
Annexe 21 : Dictionnaire des fonctions

NOM / EMPLACEMENT	Où c'est utilisé	Ce que ça fait
Function.php	RSS, Header,Login et leurs dérivés	Objet divin qui recueille les fonctions
Connect():mysqli	Login	Fait un mysqli avec les informations de config.php
Pagespecific()	Header,RSS	Affiche le contenue nécessaire (html/js) en fonction d'un paramètre en fonction du fichier où on appelle la fonction
Stylesheet()	Header,login	Affiche le style de préférence de l'utilisateur
Display_items(display = "", section = "", tid = "", sortby = "")	Display	Affiche toute les taches d'une section donner
Displayfrontpage()	Index	Affiche les taches mis en avant ou mettre en avant sur la page d'accueil
Selfref_url()	Header	Donne l'url de lui-même qui est calculer de manière dynamique de là où il est host
Sort_form(type = "", section="",tid="",sortby="")	Display	Définit le paramètre de tri avant d'afficher et met en bonne disposition la liste
Rss.php	Header	
Main()	Header	Définit le xml du flux rss et récupère les données puis les met en forme
Login.php	Header et sessioncheck	
Main()	Lien header, Redirection par sessioncheck	Si elle ne l'a pas fait, effectue le test de vérification Affiche la page de login Le log out
Sessioncheck.php	Header	
Main()	Header	Vérifie si la personne n'était pas déjà connectée grâce aux sessions en php
Config.php		
Main()	Sessioncheck, Install (supprimer), Update, Login, print, rss	Donne les informations de connexion à la bdd, les formats de date et la langue du texte
Header.php		

Main()	Display_type, Display, edit_type, edit, Index, Settings	Demande les vérifications, Affiche l'entête navigable, Initialise tout, Ouvre des choses inutilisés, Affiche la sidebar (les sections à gauche)
Footer.php		
Main()		Affiche le pied de page
Settings.php		
Main()	Settings, un case de function.pagespecific, Lien header	Initialise les formulaires de changement de paramètre, affiche les formulaires de changement de paramètre, Fait des boutons pour update le logiciel, exporter en csv et suppression des taches fini Affiche le formulaire de changement de mot de passe
Index.php		
Main()	Header en lien, sur la fin de install, pareil pour update, login formulaire/lien	Affiche / commande l'affiche globale.
Display.php		
Main()	Function.display_items (lien), Function.frontpage (lien), function.sort_form, Header plusieurs fois en lien, Display_type en lien	Récupère les formulaires ou alors des variables en url et fait les actions qui correspondent ou prépare l'espace pour les affichages. Principalement les affichages d'items
Display_types.php		
Main()	Header en lien	Affichage pour les projets et les contextes
Print.php		
Main()	Function.sort_form	Fait l'affichage du près à l'impression
Edit_types.php		
Main()	Edit_types, display_types, edit	Affiche la page de modification des projets et des contextes
Edit.php		

Main()	Edit, header.pagespecific, header.displayfrontpage, header.display_items	Affiche la page de modification pour les items
Lang/		
En.php,es.php,de.php.ru.php	Header	Sert à charger du vocabulaire dans des variables
Update.php		
Main()	Settings	Sert à choisir si on veut remettre une version particulière de l'application avec les modifications apportées

Annexe 22 : Diagramme de séquence du chargement de index.php



Annexe 23 : Rétroconception