Volet architecture sécurité

Sommaire

Dernière modification : 2021-04-28

1. Introduction

Ceci est le point de vue sécurité. Il décrit l'ensemble des dispositifs mis en œuvre pour empêcher l'utilisation non-autorisée, le mauvais usage, la modification illégitime ou le détournement des modules applicatifs.

Les autres volets du dossier sont accessibles d'ici.

1.1. Documentation de Référence

Table 1. Références documentaires sécurité

N°	Version	Titre/URL du document	Détail
1	1	Cahier des charges	Cahier des charges transmis par le client regroupant toutes les informations relatives au projet
2	n/a	Sécurité : Sécuriser les sites web	Recommandations faites par la CNIL au niveau de la sécurisation des donées des utilisateurs

2. Non statué

2.1. Points soumis à étude complémentaire

N/A

2.2. Hypothèses

Table 2. Hypothèses

ID	Détail
1	Aucune solution n'est actuellement en place il conviendra donc d'en créer une respectant les normes minimales de sécurités recommandées par la CNIL

3. Contraintes

- Mettre en oeuvre le protocole TLS
- Rendre l'utilisation de TLS obligatoire pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques.
- Limiter les ports de communication strictement nécessaires au bon fonctionnement de l'application
- Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
- Si des cookies non nécessaires au service sont utilisés, recueillir le consentement de l'internaute.
- Limiter le nombre de composants mis en œuvre, en effectuer une veille et les mettre à jour.
- Utiliser des outils de détection des vulnérabilités (logiciels scanners de vulnérabilité tels que nmap, nessus, nikto, etc.) pour les traitements les plus critiques afin de détecter d'éventuelles failles de sécurité.

4. Exigences

4.1. Exigences d’intégrité

Table 3. Niveau d’intégrité exigée par classe de données

Classe de données	Niveau « Non intègre » (La donnée peut ne pas être intègre)	Niveau « Détectable » (La donnée peut ne pas être intègre si l’altération est identifiée dans un délai raisonnable)	Niveau « Maîtrisé » (La donnée peut ne pas être intègre, si l’altération est identifiée et l’intégrité du bien essentiel retrouvée)	Niveau « Intègre » (La donnée doit toujours être rigoureusement intègre)
Données utilisateur				x
Données prduits			x	
Données statistiques			x	
Données archivées		x		

4.2. Exigences de confidentialité

Table 4. Niveau de confidentialité exigée par classe de données

Classe de données	Niveau « Public » (Tout le monde peut accéder à la donnée)	Niveau Limité » (La donnée n’est accessible qu’aux personnes habilitées)	Niveau « Réservé » (La donnée n’est accessible qu’au personnel interne habilité)	Niveau « Privé » (La donnée n’est visible que par l’intéressé(e))
Données utilisateur				x

4.3. Exigences d’identification

- Un utilisateur ne peut avoir qu’un seul identifiant
- Chaque identifiant sera fait avec une adresse email
- Chaque nouvel email sera tester pour voir si il existe deja en base avant insértion
- Chaque email ser testé avec une regex pour voir si il est valide

4.4. Exigences d’authentification

Table 5. Exigence d’authentification par cas d’utilisation

Cas d'authentification	Mot de passe respectant la politique de mot de passe	Clé publique ssh connue	OTP par Token	Biométrie	Connaissance de données métier	E-mail d'activation	Délégation authentification
Connexion	x						x
Modification compte	x						x
Création compte						x	

4.5. Exigences de fédération d'identité

L'identification et l'authentification seront externalisés au fournisseur d'identité Auth0 pour simplifier la gestion de la sécurité et réduire les coûts de développement et d'exploitation.

4.6. Exigences de SSO et SLO

N/A

4.7. Exigences de non répudiation

Table 6. Besoins de non-répudiation

Donnée signée	Origine du certificat client	Origine du certificat serveur
pièce d'identitée	Administration publique	
Justificatif de domicile	Administration pblique, prestataire de service	

4.8. Exigences d'anonymat et de respect de la vie privée

- Aucunes données relatives à la santé ne seront enregistrées
- Aucune donnée raciale, politique, syndicales, religieuse ou d'orientation sexuelle ne pourra être stockée sous quelque forme que ce soit dans le SI.
- En application de la directive européenne « paquet telecom », un bandeau devra informer l'usager de la présence de cookies.
- En application du RGPD, un consentement explicite des utilisateurs dans la conservation de leurs données personnelles de santé sera proposé.

4.9. Exigences sur les habilitations

Table 7. Matrice de rôles

Groupe ou utilisateur	Rôle `consultation`	Rôle `modification`	Rôle `suppression`	Rôle `asministration`
Admin	x	x	x	x
Utilisateur	x			
Client	x	x	x	

4.10. Exigences de traçabilité et d'auditabilité

- Pour les connections administrateur, il parait necessaire de garder pour chaque connexions : le nom, la date et en cas de modification l'ancienne et la nouvelle valeur.
- Toute tentative d'intrusion dans le SI devra être détectée (dans la mesure du possible).
- L'historique des commandes de chaque client devra etre tracable

Table 8. Données à conserver pour preuves

Donnée	Objectif	Durée de rétention
Log complet (IP, heure GMT, détail) des commandes passées sur le site	Prouver que la commande a été passée	1an
Log complet (User, heure GMT, Ancienne/Nouvelle modification) des modifications faites sur le site	Eviter perte de données	1 an
Date et contenu du mail de confirmation de commande	Prouver que le mail de validation de commande a été envoyé	2 ans
Date et contenu du mail de cofirmation de paiement	Prouver que le mail de validation de paiement a été envoyé	2 ans

5. Mesures de sécurité

5.1. Intégrité

Dispositifs répondant aux exigences d'intégrité :

TBD

5.2. Confidentialité

Dispositifs répondant aux Exigences de confidentialité :

TBD

5.3. Identification

Dispositifs répondant aux exigences d'identification :

- Pour assurer la non réutilisation des ID des comptes supprimés, une table d'historique sera ajoutée dans l'application et requêtée avant toute création de nouveau compte.

5.4. Authentification

Dispositifs répondant aux exigences d'authentification :

- L'authentification des internautes inscrits se fera par login/mot de passe (respectant la politique de mot de passe P)
- L'accès aux pages paniers et paiment des internautes inscrits se fera par l'utilisation d'un token Auth
- L'authentification des internautes à l'inscription se fera via la validation d'un email de confirmation
- Les mots de passe ne seront en aucun cas conservés mais stockés sous la forme de digest bcrypt.

6. Auto-contrôles

6.1. Auto-contrôle RGPD

Table 9. Checklist d'auto-contrôle de respect du RGPD

Exigence RGPD	Prise en compte ?	Mesures techniques entreprises
Registre du traitement de données personnelles	x	Liste des traitements et données personnelles dans le document XYZ
Pas de données personnelles inutiles	x	Vérifié, la rétention de numéro de CB a été supprimée car inutile.
Droits des personnes (information, accès, rectification, opposition, effacement, portabilité et limitation du traitement.)	x	Oui, traitement manuel sur demande depuis le formulaire, traitement en 1 mois max

Sécurisation des données	x	Oui, voir les mesures listées dans ce document notamment sur la confidentialité, audibilité et intégrité.