Droit du numérique

IN3SA01 2022-2023

Groupe 7 :
Samir Subra
Nino Pires
Antoine Bazire
Alexis Araujo

Les mesures impliquées

Il est important de procéder à des analyses pour que l'on puisse traiter les données qui nous seront utiles avant de développer l'application. La création de la base de données passera par cette phase d'analyse et contiendra les données utiles à l'application, elles seront catégorisées puis stockées (: "**Cartographiez et catégoriser les données et les traitements de votre système"**). Cela nécessite un travail en amont qui correspond à la mesure "priorisez les actions à mener".

Les mesures : "Gérez les risques" et "Documenter la conformité de vos développements" ont aussi une place importante dans la conception de l'application. La gestion des risques a été réalisée avant le développement (notamment via la matrice de gestion des risques).
Les documentation technique et non-technique sont réalisées et actualisées au cours du développement.

Dans notre application nous récoltons des données à caractère personnel comme l'adresse email et le pseudonyme. Ces données sont nécessaires pour la connexion à l'application en tant qu'utilisateur. Elles ont donc un sens utile et pertinent. Nous avons limité le nombre de données à caractère personnel, nous n'en récoltons que deux et ce sont des données non sensibles.
Elles sont récupérées lors de l'inscription à l'application d'un visiteur.

Il est nécessaire de réfléchir aux données ainsi qu'à leur sécurisation dès la phase de conception pour ainsi protéger les données personnelles des utilisateurs que nous stockons ("**Mettez la protection de la vie privée au cœur de vos développements")** . Nous pouvons prendre les exemples du mot de passe. Nous récoltons les mots de passe lors de l'inscription d'un visiteur pour qu'il passe utilisateur ce mot de passe sera stocké pour pouvoir faire la connexion. Ce mot de passe est hashé (=crypté) ce qui permet de ne pas rendre "publique" la diffusion de cette donnée sensible. Ce mot de passe est modifiable pour plus de sécurité.
Les utilisateurs seront avertis si leur mot de passe entré est faible d'un point de vue sécurité conformément aux recommandations de la CNIL ("exigences de sécurité des données").
Cela à été préparé dans la conception et grâce à la méthode *agile*. La méthode *agile* permet de mieux connaître les exigences du client et de lui permettre de participer/suivre la conception du produit. Nous avons donc défini cette protection du mot de passe dès le début avant le développement.

Nous utilisons plusieurs technologies dans notre projet comme github qui permet de faire de la gestion de version de notre application via des *clés ssh* (permet de créer une connexion sécurisée sur un réseau non sécurisé) qui répond à la mesure du CNIL : "Sécurisez vos serveurs et vos postes de travail" mais nous utilisons aussi un serveur pour pouvoir mettre en ligne l'application. Le serveur interagit avec les pages codées, la vue de l'utilisateur mais aussi la base de données. Il est donc nécessaire que ce serveur soit sécurisé pour faire face à toutes intrusions qui pourraient mettre en danger l'intégrité de l'application et de ses données.

Comme cités précédemment, nous utilisons git comme gestionnaire de code source et gitlab pour versionner et stocker notre projet. Sur Git, le projet est sécurisé via clés ssh. Sur Gitlab, uniquement les 4 membres du projet peuvent accéder au fichiers et les modifier (les 2 clients ont accès uniquement en visionnage avec des droits limités ("attribution des niveaux d'accès et des permissions")).
Évidemment les membres ont conscience des mesures de sécurité et font attention à ne pas publier en ligne des contenus sensibles et/ou personnelles.

Le serveur est installé par nous-même, nous pouvons donc nous assurer de la localisation géographique des serveurs qui vont héberger nos données.
Comme expliqué auparavant, les mots de passe seront hachés et donc **jamais stockés en clair.**
Enfin, l'accès aux outils et interfaces d'administration seront utilisables uniquement aux seules personnes habilitées. C'est-à- dire aux comptes que nous désignons comme gestionnaire.

Conformément au recommandations de la CNIL, nous allons **imposer une authentification** avant tout accès à des données personnelles, en effet les utilisateurs pourront accéder à la page profil uniquement s' ils se sont authentifié avec succès sur l'application.
Pour implémenter certaines fonctionnalités de *SimFast*, nous avons recours à certaines bibliothèques comme par exemple "matplotlib". Les outils choisis ont été pris avec précaution et sont toujours **maintenus à ce jour.**

Il est indispensable d'adopter au plus tôt une bonne hygiène d'écriture de code, c'est en suivant cette règle que nous avons construit la partie développement de l'application. Ainsi la documentation du code ainsi que des tests sont créés et maintenus en même temps que l'écriture du code. Le versionnage du code est lui aussi suivi via des "commit" clairs et reguliés sur gitlab. les environnements de développement intégrés nous aident à avoir un code structuré (indentation, sauts de ligne, accolades etc…) et à éviter les redondances.
Les tests (unitaire d'intégration et d'acceptation) ont un rôle très important dans la mise en place d'une application. Ainsi les tests et leurs documentations sont faits en même temps que la programmation. Ils sont disponibles dans les

dossiers “Test” de chaque livrables sur notre Gitlab. En respect des mesures du CNIL, nous n’utilisons pas de jeu de données d’utilisateurs réels pour réaliser nos tests.

Pour suivre adéquatement le principe de transparence du RGPD, nous allons informer les utilisateurs (sur la page d’inscription) de la finalité des données (= à quelles fin elles seront utilisées), le caractère obligatoire des données, la durée de conservation des données ainsi que le destinataire des données récoltées.
Les utilisateurs de *Simfast* pourront aussi faire valoir leur **Droits d’accès** au données en se rendant sur leur page de profil qui affichera toutes les données leurs appartenant.
Le droit à l’effacement est aussi respecté car toutes les données stockées sur nos serveurs sont effacées lors de la suppression du compte de l’utilisateur le souhaite.

Pour ce qui est des traceurs (ou cookies), nous ne sommes pas soumis à l’obligation de recueil de consentement car nous utilisons seulement ceux nécessaire à l’ouverture et au maintien d’une séssion ouverte temporairement (**Certains traceurs peuvent être exemptés du recueil de consentement** : les traceurs destinés à l’authentification auprès d’un service(...). Source : *Guide-RGPD-du-developpeur*).

Les comptes possédant les droits “Gestionnaire” auront accès à des statistiques d’utilisation des différents modules de Simfast par les utilisateurs inscrits sur la plateforme. Ces données sont anonymes et uniquement récoltées à des fins de suivi de statistiques / performances de l’application. Cette limitation nous exempte également de demander leur consentement à nos utilisateurs.

Enfin, nous avons décidé de prendre plusieurs mesures pour prémunir notre application contre les différents types d’attaques informatiques malveillantes qui pourraient survenir :

Ainsi, pour les attaques de type Manipulation d’URL, nous avons fait en sorte que la partie “Utilisateur” et “Gestionnaire” de l’application ne soit pas accessible si il n’y a pas eu d’authentification valide au préalable (utilisation des sessions / cookies).

Pour les attaques de type “Credential Stuffing” (ou Bourrage d'identifiants), un captcha a été mis en place lors de l’authentification des utilisateurs pour empêcher des potentiels robots de multiplier les requêtes et de trouver des mots de passe valides.

Comme précisé plus tôt, les mots de passe devront respecter des normes minimales de sécurité ce qui limitera les attaques de type “Brute Force” et par dictionnaire. Nous allons également implémenter un délai si un utilisateur fait un trop grand nombre d’essais infructueux de connexion.

Pour les attaques par “Injection de code Indirecte”, les risques sont diminués car nous n’avons pas d’options de téléversement de fichier (par exemple upload de fichiers / images) sur *Simfast*. Nous allons tout de même renforcer notre

protection en neutraliser les caractères utilisés pour l'insertion de script (cf. nettoyage « HTML escape »).

Les attaques par Injections SQL font partie des plus grands risques sur notre application. Pour tenter de limiter ce risque, nous allons implémenter un maximum de requêtes SQL préparées et affiner notre gestion des droits d'accès à la base de données utilisée.

Enfin pour la protection contre les logiciels malveillants / ransomware, notre équipe est formée aux risques que forment le téléchargement de fichiers dont on n'est pas sûr de la provenance. Nous évitons également d'utiliser les comptes possédants les droits "Administrateurs" sur des machines qui ne nous appartiennent pas et pour notre usage quotidien.

Bibliographie :

Auteur : Commission nationale de l'informatique et des libertés
Source : *Guide RGPD de l'équipe de développement* (https://lincnil.github.io/Guide-RGPD-du-developpeur/)