1

Je m’appelle Sophie. Pendant près d’1 an, j’ai suivi un cursus de formation pour apprendre le métier de développeur en informatique.

Cette formation était un partenariat entre l’Ecole Efrei Paris et mon employeur, SG

Aujourd’hui je vais vous présenter mon projet de fin d’étude.

Il s’agit d’un outil de gestion de tickets. Ces tickets sont des incidents techniques pouvant survenir dans un immeuble de bureau de grande taille.

Je vous parlerais de l’aspect technique (l’architecture de l’outil),

Des fonctionnalités, avec un focus sur les éléments les plus importants (l’incident, l’utilisateur, l’authentification),

Un point sur la sécurité

Et pour finir une petite démonstration.

click

2

SG

Tout d’abord, un peu de contexte.

Société Générale est une des plus importantes banques françaises.

Comme toutes grandes entreprises, elle a un besoin grandissant de savoir-faire en informatique.

click

Parallèlement, d’autres métiers de plus en plus automatisés nécessitent moins de personnel.

Elle a donc eu l’idée de vastes plans de formation afin d’adapter une partie de son personnel à ces nouveaux besoins.

click

Les formations de reconversion, ou reskilling, permettent à des salariés motivés de changer de parcourt professionnel, de découvrir un nouveau métier, de passer un diplôme d’Etat.

En intégrant une de ces formations, j’ai rejoint il y quelques mois une équipe de développeurs.

click

FixedIncome

S’occupe à la fois de support et de développement.

click

En tant que débutante je ne fais pas encore de support. Mais je fais du développement.

3 SOS Immo

Tout à l’heure j’ai dit que l’appli gérait les incidents dans un immeuble de bureau de grande taille.

Dans immeuble de ce genre, l’entreprise occupante (proprio ou locataire de l’immeuble) ne s’occupe pas elle-même de ce genre de choses. Elle passe des contrats avec d’autres entreprises prestataires spécialisées dans leur domaine (plomberie, ascensoriste, ménage, etc.).

Ces entreprises emploient des techniciens sur place, à demeure, pour pouvoir intervenir à tout moment, dans un délai convenu.

Classiquement la centralisation des incidents est assurée par un standard téléphonique, des cahiers et des post’it, dash board.

click

Dans un contexte de digitalisation des process, l’idée est venue d’une plateforme unique pour tous les occupants de l’immeuble, qu’ils soient employés de bureau, intervenants extérieur ou responsables d’immeuble.

Je dois dire qu’une plateforme de ce genre a été mise en place SG. Je reprends l’idée à mon compte.

Pour construire ce projet, je suis allée rencontrer des responsables d’immeuble Société Générale, à la Défense.

Ils m’ont expliqué comment ils utilisent l’outil et leurs besoins en la matière.

click

L’objectif principal de l’application est bien sûr d’aider au suivi des incidents.

Les objectifs secondaires : aider les services techniques à identifier les points de vigilances : prestaires potentiellement en sous-effectif, étages ou types d’incidents particulièrement récurrents

*Satisfaction des usagers.*

J’en ai déterminé les fonctionnalités suivantes.

click

4 diagramme de Use case

Après avoir défini les besoins, j’en suis arrivée à définir 4 profils différents.

click

2 internes et 2 externes

Interne => entreprise occupante

Externe => entreprise prestataire sous contrat

click

Usager dont le rôle se borne à signaler l’incident et valider la fin d’intervention.

click

Admin, c’est à la fois le service immobilier, responsable d’immeuble, et l’administrateur de l’appli et qui a donc tous les droits.

click

Technicien qui résout les problèmes

click

Valideur qui est le chef du technicien. Il utilise l’outil pour coordonner son équipe.

Ces 2 profils externes ne travaillent que pour une seule entreprise prestataire chacun.

click

5

J’ai conçu SOS Immo avec une architecture web client-serveur classique.

Il est développé comme 2 projets indépendants.

Le Front end qui est l’interface utilisateur et qui permet de naviguer entre les différentes fonctionnalités.

La partie visible du programme.

Les Back end en est partie invisible.

Il fait les calculs et garde la mémoire.

Le tout est codé en JavaScript.

Front

Est géré par la librairie React.

Le concept de React est assez simple : 1 page pour le site et une multitude de composants pour l’habiller qui sont déclenchés selon certaines conditions.

Un composant est donc un élément de page. Il contient

* du code html qui lui-même peut appeler d composants : parents => enfants
  + visuellement : tableau, bouton, formulaire, etc.
* des fonctions qui lui permettent d’interagir avec le Back
* d’autres éléments propres à React à mi-chemin entre variables et fonctions qu’on appelle useState.

Variables pour simplifier de n’importe quel type. Ont la particularité d’être transmissibles d’un composant parent à un composant enfant, et leur valeur mises par un enfant.

Quand un useState est mise à jour par un compo enfant, le compo parent dans lequel il a été déclaré est recalculé.

Et c’est ça qui fait fonctionner le tout.

click

6

Voici la page et son seul composant. Par convention « App.js »

Gare de triage pour tous les autres composants.

Dans App.js, j’ai déclaré plusieurs useState dont le premier, nommé « ecran », string initialisé « login ».

Le code HTML de Apps.js lance systématiquement 2 composants :

* 1 composant « Bandeau.js »
* 1 autre composant qui dépendra de la valeur du useState « ecran ».

1/ Le contenu de « Bandeau.js » est lui-même conditionné à « ecran ».

Systématiquement « Bandeau.js » affiche le logo de l’application.

Si « ecran » !== « login », authentification réussie, il affichera aussi d’autres éléments, nom et profil de l’utilisateur.

2/ Le 2nd composant est donc conditionné à la valeur « ecran ».

Au démarrage, « Login.js ».

Contient le formulaire d’authentification – id + mdp.

Il contient aussi la fonction qui va communiquer ces éléments au Back et récupérer les données utilisateurs.

Quand l’authentification est validée, la valeur d’« ecran » est mise à jour à « menu ».

Comme « ecran » est un useState, le composant dans lequel il a été déclaré (App.js donc) est recalculé.

Le composant « Login.js » n’est plus affiché. A la place, le composant « Accueil.js ».

« Accueil.js » contient toutes les fonctionnalités de l’application, accessibles par des boutons.

L’affichage ou non de ces boutons est conditionné au « profil » de l’utilisateur.

Pour ce qui est du Back

click

7

Le back est un serveur NodeJS contrôlé par la librairie Express.

Le controller c’est le cerveau de l’application.

Son rôle est de recevoir les requêtes/demandes du Front (via des adresses url) et de les traiter avec les fonctions adéquates.

Ces fonctions sont des services que j’ai regroupés par catégorie (login, utilisateurs, incidents).

Chaque catégorie de services est logée dans un fichier .js distinct.

Pour fonctionner, le Back a besoin d’une mémoire. Celle-ci est stockée dans une base de données MySQL.

Les services ne vont pas interroger directement la base de données.

L’interaction entre les 2 est assuré par un ORM, Object Relational Mapping.

C’est un système qui converti les tables de la base de données en autant de classes objets.

Chaque table est une classe d’objet.

Chacun colonne est 1 attribut de l’objet.

Ce sont les fichiers Models.

J’ai choisi la librairie Sequelize de NodeJS.

Sequelize possède ces propres fonctions pour récupérer les données de la base, les convertir en objet et vice versa.

Il évite au maximum les requêtes SQL. Et, quand ces requêtes sont inévitables, il empêche les problèmes d’injections SQL.

J’ai mis ces fonctions dans des fichiers DAO (Data Access Object) distincts des Models, pour clarifier le code.

Ce sont les fonctions DAO qui sont utilisées par les services.

Ainsi, chaque couche a son propre rôle dans l’organisation global du Back.

Passons aux fonctionnalités.

click

8

Pour en finir avec la technique, j’ai réparti toutes les données nécessaires pour ce projet en 9 catégories.

Le résultat est une base de données de 9 tables.

Les plus importantes sont les tables incidents, utilisateurs et habilitations.

J’en parlerais plus un peu plus tout à l’heure.

click

9

Voici le menu complet des actions.

Aucun profil n’a accès à l’ensemble de ces actions.

Le profil avec les plus de fonctionnalités est bien sûr Admin, que je vais détailler tout de suite.

La seule action à laquelle il n’a pas accès est Suivi d’incident.

Qui liste les interventions non terminées de l’entreprise prestataire pour laquelle travaille l’utilisateur.

click

10

Admin a donc accès aux différents écrans de gestion de données.

Comme tous les profils, il peut créer et suivre ses propres signalements.

Il peut consulter l’écran pilotage qui contient tous les incidents listés par catégories.

Il a alors la possibilité de sélectionner 1 des incidents pour en consulter le détail.

Suivant le status de l’incident, il pourra ou non agir dessus.

Je vous explique cette notion de status.

click

11 diagramme état-transition

Tous les incidents suivent le même parcourt.

Ils passent linéairement par 4 états, ou statuts.

A sa création, 1 inc est en attente d’affection.

Personne ne s’occupe encore de lui.

Puis un technicien lui est affecté. Il est donc pris en charge.

A la fin de l’intervention, l’inc est en attente de validation par l’utilisateur auteur du signalement.

Puis l’utilisateur valide la clôture.

Après clôture, l’incident est mort.

Si l’utilisateur est mécontent de l’intervention, il le signale et un nouvel inc est automatiquement généré à l’identique du premier, avec le motif d’insatisfaction.

Le cycle de vie recommence avec ce nouvel inc.

Les écrans relatifs à ce cycle.

click

12 signalement

Au lancement de cet écran, il y a échange front/back.

Le back envoie la liste de tous les emplacements possibles dans l’immeuble avec tous les types d’incidents possible dans chacun de ces emplacements.

Puisque que tout ne peut pas arriver n’importe où.

Un premier menu déroulant s’affiche pour sélectionner l’étage.

Une fois l’étage renseigné, le deuxième menu déroulant propose les emplacements possibles de cet étage précis.

Ensuite, le dernier menu déroulant propose tous les types d’incidents pouvant survenir dans cet emplacement.

Le commentaire est facultatif.

A la validation, le tout est envoyé au Back.

Celui-ci détermine quelle entreprise prestataire doit être attribuée à cet incident suivant le type d’incident renseigné.

Puis sauvegarde en base.

L’utilisateur est redirigé vers l’écran de suivant d’avancement de ses propres signalements.

Click suivi d’avancement

Chaque signalement est une vignette.

La couleur de ces vignettes indique le statut actuel de l’incident.

Bien sûr l’utilisateur peut consulter le détail d’une de ces vignettes puisqu’il s’agit de ses propres incidents.

click

13 détail

Une fiche incident est partagée en 3 parties.

En haut/ Cartouche, sorte de carte d’identité. Quand, où et quoi.

En bas/ Commentaire associé à cet incident précis.

Au milieu/ le status

Tout le monde peut le connaitre. Mais les fonctionnalités qui le concerne ne sont accessibles que selon le profil.

Par exemple, l’usager ne peut agir qu’après la fin de l’intervention.

Le technicien peut prendre en charge et terminer une intervention.

Pour développer le projet, j’ai commencé par faire un diagramme de useCase. Ensuite, j’ai constitué un dictionnaire de données. Je les ai triés par catégorie, ce qui m’a permis de concevoir la base de données de mon application.

click

14 bd

A présent vous avez toutes les clés en main. Voici les données nécessaire au cycle de vie d’un incident.

* Clé primaire en auto-incrément
* Emp et tinc fournis par l’auteur du signalement.
* Le presta est calculé. Cela pourrait faire doublon avec le tinc.

Il arrive que le type d’incident soit mal défini lors du signalement.

Le profil Admin a la possibilité d’attribuer l’incident à un autre prestataire que celui calculé en premier lieu.

* Identifiant de l’auteur du signalement. Indispensable car c’est lui qui devra faire la clôture.
* Identifiant du technicien. Pour savoir qui fait quoi.
* Dates et heures de chaque étape/statut. Pour savoir où on en est..
* Enquête de satisfaction.

click

15 diagramme de séquence

SOS Immo est conçu pour un usage professionnel au sein d’1 immeuble de bureaux.

Ce n’est ni un réseau social ni pas un site marchand.

Tous les occupant doivent pouvoir y accéder mais ce sont les services immobiliers qui gèrent les comptes.

click

Chaque nouvelle arrivée est signalée par RH (int) ou par presta directement au service d’immeuble. Ce procès n’est pas géré dans SOS Immo.

Pour créer 1 compte : Nom prenom mail tel – presta : fonction

click

L’admin saisi ces données + identifiant unique dans l’application.

Et celle-ci se charge de générer un mot de passe aléatoire à expiration immédiate.

Elle transmet l’id+mdp par mail à ce nouvel l’utilisateur.

Tout à l’heure, focus mdp

Click

A la demande de connexion, le Back contrôle que l’identifiant + mdp fournis appartiennent à 1 même utilisateur.

Click

A chaque connexion, la date d’expiration du mot de passe est contrôlée.

Le cas échéant, l’utilisateur est redirigé vers l’écran de changement de mot de passe.

Ce sera le cas systématiquement à la première connexion.

Le nouveau mdp aura lui une validité de 90 jours.

Par la suite, l’utilisateur peut changer son mdp quand ça lui chante.

L’utilisateur a aussi le droit d’avoir des trous de mémoire.

Click

En cas d’oubli d’id/mdp, l’utilisateur est invité à renseigner son mail.

L’appli contrôle que l’adresse existe en base.

S’il s’agit de l’identifiant, il sera juste transmis par mail.

Si c’est le mdp qui est demandé, c’est un nouveau mdp aléatoire à expiration immédiate qui sera envoyé.

Voici les écrans

click

16 authentification

Click oubli

Click changement mdp

Mdp actuel

Nouveau 1 – différent mdp actuel et satisfaire aux caractéristiques minimums requises.

Nouveau 2 – identique nouveau 1

Le Back contrôle que l’ancien mdp est associé à l’utilisateur en cours et fait la maj en base.

Je vais revenir sur le diagramme de séquence de tout à l’heure

click

17 diagramme

On voit qu’admin connaît l’identifiant.

Le programme génère un mdp et le communique à l’utilisateur.

Il ne garde pas ce mdp en mémoire.

click hashage

Auparavant ce mdp est hashé.

Le hachage est un moyen de crypter un message.

C’est une fonction transforme une chaine de caractères en un nombre hexadécimal de 32 caractères.

Ce système a 2 particularités :

Sens unique – Il ne peut pas être décrypté.

Une même chaîne ou document ne produira qu’1 seul résultat de hash et ce résultat lui est totalement spécifique.

*Librairie « sha1 ».*

Mais c’est pas tout.

click salage

Pour encore plus de sécurité, on procède au salage du mdp.

C’est un procédé purement mécanique : on ajoute à la chaine à crypter une autre chaine (de préférence unique) avant le hashage.

J’ai concaténé le mdp avec l’identifiant, puisqu’il est unique.

Hashé le tout.

click fin

C’est ce hash qui est sauvegardé en base.

*Ainsi 2 utilisateurs peuvent avoir le même mdp sans risque.*

Le mdp original est totalement inaccessible, personne ne peut pas le reconstituer.

click fin

18 données

Pas de données vraiment confidentielles

Num ss, adresse, siret, âge…

Mais tout de même sensibles

Nom mail telephone, niveau d’habilitation

7 des 9 tables ont pour clé primaire un entier en auto incrément.

Pour Utilisateurs et Habilitations, pour lesquels j’ai choisi une clé plus sécurisée, un Uuid.

click

Universally Unique Identifier

Nombre hexadécimal de 32 caractères généré aléatoirement par une fonction ad oc.

La fonction garantie que ce nombre tout à fait unique.

Il n’apparait sur aucun écran de l’interface.

*Librairie « uuidv4 ».*

Avec les uuid pour les tables les plus sensibles et hasher/saler , j’ai voulu sécuriser les données.

Mais il faut aussi sécuriser l’accès à ces données.

Un premier filtre est fait par l’appli web, puisque que c’est le profil de l’utilisateur qui lui donne accès ou non aux différentes fonctionnalités.

click

19 cookie

Mais c’est pas suffisant.

Il faut qu’à chaque service sollicité par le serveur, contrôle soit fait : le demandeur est-il autorisé à demander ?

Pour cela, j’ai choisi d’utiliser un cookie de session.

Ce cookie est un petit fichier créé par le serveur et stocké dans le navigateur.

Il est donc créé après la réussite de l’authentification.

Je l’ai paramétré pour stocker certaines infos sur l’utilisateur.

isId – signale réussite de la connexion

Quand un service est appelé par le serveur, il va commencer par contrôler la validité de la demande.

Exemples d’utilisations différentes

* Je veux créer un nouvel utilisateur
  + Le serveur appelle le service de création d’ut.
  + La première chose que fait ce service, c’est de contrôler grâce au cookie
    - Que l’auteur la requête est bien identifié et connecté
    - Qu’il a le bon profil
* Je veux la liste des incidents que j’ai moi-même déclarés.
  + Le serveur appelle le service adéquat.
  + Ce service contrôle que l’auteur la requête est bien connecté.
    - Le profil n’a pas d’importance.
  + Ensuite, le service récupère la liste des incidents (via DAO) et fait un filtre. Ne garde que ceux déclaré par l’utilisateur identifié par le cookie.

Cookie peut être appelé à tout moment.

Durée de vie limitée.

click

20 organisation

Pour ce qui est des outils utilisés pour l’élaboration de ce projet

J’ai créé 2 dépôts sur outil de versioning GitHub.

Pour le suivi d’avancement du projet j’ai utilisé Trello, surtout au début.

Lister et trier les tâches à effectuer.

Eviter de se disperser.

Pour tester le code, j’ai utilisé la librairie Jest, pour le javaScript.

Mise en page css

Et utilisé PostMan pour tester les services Back.

Démo

Il est temps de vous présenter de visu SOS Immo.

Je ne vais pas pouvoir vous montrer toutes les fonctionnalités.

Je vais donc me concentrer sur le cycle de vie de l’incident.

click

21 bref

Année particulièrement enrichissante, éprouvante certes, mais passionnante.

click

De par ma formation initiale et mon expérience professionnelle et personnelle, j’avais déjà des notions :

conception

recueil leurs besoins

Détermination des fonctionnalités nécessaires et leur priorisation

Etablir un dictionnaire de données et en faire une base de données SQL

Ici c’est moi qui ai assuré à peu près tous les rôles : Product owner, conceptrice, codeuse, testeuse, valideuse…

click

Au cours de l’année écoulée, j’ai appris énormément de choses que j’ai pu mettre en pratique pour ce projet :

Web => quelques notions HTLM => Application client/serveur

La POO : t les classes d’objets et leurs méthodes.

Langages

Devops – qui m’a permis d’automatiser les tests unitaires et qui va me servir au déploiement sur un serveur distant

click

J’ai bien sûr dû compléter par des recherches personnelles.

Principalement pour comprendre l’ORM. Qui fait le lien entre et base de données et classes objets.

Beaucoup de temps aussi notamment pour les tests.

Mais là c’était beaucoup plus un problème de codage que compréhension du concept.

click

Aujourd’hui SOS Immo est opérationnel.

La mission principale de (suivi des incidents) est remplie.

Et la partie authentification est terminée.

click

Il me reste à finaliser l’administration de certaines données.

Je souhaite également déployer l’appli sur une machine distante.

On peut aussi envisager d’autres évolutions comme l’archivage des incidents clôturés, la production de kpi, etc.

click

22 enfin

Je tiens à remercier bien sûr les professeurs et les autres élèves de ce rekilling. Nous avons tous accomplie un travail énorme.

Merci aussi au manager FixedIncome, qui a fait confiance à une débutante de 48 ans, ainsi qu’à toute l’équipe pour son soutien et sa patience.

Enfin, je ne veux pas oublier les responsables du service immobilier de l’immeuble Basalte de la Défense. Dont l’aide m’a été très précieuse pour ce projet. Définition des fonctionnalités.