

Réf : PFA1-2019- ??

Rapport de Projet de Fin d'Etude

de

troisième année en Génie Informatique

Présenté et soutenu publiquement le .././2021

Par

Wissal FERSI

Intitulé du projet

Composition du jury

Monsieur

Président

Monsieur

Encadrant

Année universitaire : 2020-2021

Dédicaces

Remerciements

Table des matières

Release 1 : Gestion d'accès, gestion des utilisateurs et gestion profil	1
Introduction	1
1. Présentation du release	1
2. Sprint 1 : Authentification et gestion d'accès	1
2.1. Mécanisme de sécurité	2
2.1.1. Json Web Token (JWT).....	2
2.1.2. Diagramme de séquence d'implémentation de la couche sécurité.....	2
2.2. Backlog du produit	3
2.3. Analyse.....	6
2.3.1. Diagrammes des cas d'utilisation.....	6
2.3.2. Raffinement des cas d'utilisation	7
2.4. Conception	11
2.4.1. Diagramme de séquence Système	11
2.4.2. Diagramme d'activité du cas d'utilisation modifier mot de passe	14
2.5. Réalisation.....	15
2.5.1. Interface d'authentification	15
2.5.2. Interface de récupération du mot de passe oublié	16
2.5.3. Interface de modification du mot de passe	17
2.5.4. Interface d'activation et de désactivation d'un compte employé.....	18
3. Sprint 2 : Gestion utilisateurs et gestion profil.....	19
3.1. Backlog du produit	19
3.2. Analyse.....	22
3.2.1. Diagramme des cas d'utilisation	22
3.2.2. Raffinement des cas d'utilisation	22
3.3. Conception	26
3.3.1. Diagramme des classes.....	26
3.3.2. Diagramme de séquence Système	26
3.3.3. Diagramme de séquence objet.....	27
3.4. Réalisation.....	29
3.4.1. Interface d'ajout d'un employé	29
3.4.2. Interface de consultation de la liste des employé.....	30
3.4.3. Interface de consultation de détail de chaque employé.....	31
3.4.4. Appliquer des recherches sur la liste employée	32
3.4.5. Gestion du rôle d'un employé	32
4. Test logiciel du release.....	34
5. Documentation	35
Conclusion.....	35

Table des figures

Figure 1 : Authentication Spring Security avec JWT	3
Figure 2: Diagramme des cas d'utilisation du premier Sprint	6
Figure 3 : Diagramme de séquence système du scénario s'authentifier	12
Figure 4 : Diagramme de séquence du système du scénario Récupérer mot de passe.....	13
Figure 5 : Diagramme d'activité du cas d'utilisation modifier mot de passe.....	14
Figure 6 : Interface d'authentification	15
Figure 7 : Les messages des cas d'erreur	16
Figure 8 : Récupération du mot de passe oublié	17
Figure 9 : Interface de modification du mot de passe	18
Figure 10 : Interface d'activation/désactivation du compte employé	18
Figure 11 : Diagramme des cas d'utilisation du Sprint numéro 2	22
Figure 12 : Diagramme des classes du sprint numéro 2.....	26
Figure 13 : Diagramme de séquence système Ajouter un compte employé	27
Figure 14 : diagramme de séquence objet du cas d'utilisation "Consulter détails employé " ..	28
Figure 15 : Interface d'ajout d'un compte employé	29
Figure 16 : Cas d'erreur d'ajout du compte employé.....	30
Figure 17 : Interface de la liste des employés	31
Figure 18 : Interface de consultation des détails d'un employé.....	31
Figure 19 : Operations de recherche appliqué sur la liste	32
Figure 20 : Interface de la liste des role d'un employé.....	33
Figure 21 : Supprimer un rôle de la liste des rôle d'un employé.....	33
Figure 22 : Ajout d'un rôle à un employée	33
Figure 23 : Application des test unitaire pour la couche user service.....	34
Figure 24 : Analyse SonarLint	34
Figure 25 : Documentation du premier release	35

Table des tableaux

Tableau 1 : Backlog Sprint 1 : Gestion d'accès	3
Tableau 2 : Raffinement du cas d'utilisation "S'authentifier"	7
Tableau 3 : Raffinement du cas d'utilisation "Modifier le mot de passe"	8
Tableau 4 : Backlog Sprint 2.....	20
Tableau 5 : Raffinement du cas d'utilisation "Ajouter un compte employé"	23
Tableau 6 : Raffinement du cas d'utilisation "Ajouter un rôle à un employé"	24
Tableau 7 : Raffinement du cas d'utilisation "Modifier les informations d'un profil"	25

Release 1 : Gestion d'accès, gestion des utilisateurs et gestion profil

Introduction

Après avoir analysé et spécifié les besoins globaux de notre client, nous détaillerons, dans ce chapitre, les différentes étapes effectuées pour le développement des deux sprints de premier release.

Nous commencerons, tout d'abord, par la présentation du backlog de chaque sprint suivi d'une analyse détaillée, une conception des fonctionnalités et finalement une présentation des interfaces homme-machine réalisées.

1. Présentation du release

Une réunion avec l'équipe Scrum s'est effectuée afin de spécifier les fonctionnalités que doit satisfaire ce release.

Notre premier release intitulé " Gestion d'accès, gestion des utilisateurs et gestion des rôles "

Comportera deux sprints qui se présentent comme suit :

- Sprint 1 : Authentification et Gestion d'accès
- Sprint 2 : Gestion des utilisateurs et Gestion des profils

Pour chaque sprint nous allons présenter son backlog produit, une analyse de chaque sprint va être explorée en présentant des diagrammes des cas d'utilisations raffiné et une description textuelles de quelques cas d'utilisation

A la fin de ce release, nous devons avoir notre premier livrable pour notre client, les utilisateurs de l'application peuvent s'authentifier, l'administrateur de l'application ("le manager") aura la possibilité de gérer les rôles, le droit d'accès et les comptes des employés.

2. Sprint 1 : Authentification et gestion d'accès

Afin de sécuriser notre application, nous devons implémenter une couche de sécurité.

Nous allons présenter dans ce qui suit, le mécanisme de sécurité de notre application, son backlog produit de ce sprint, son diagramme des cas d'utilisation, son diagramme de classe et finalement des captures écrans des interfaces.

2.1. Mécanisme de sécurité

Pour fournir une authentification sécurisée à notre application ainsi qu'un support solide d'autorisation nous avons référé à Spring Security qui a été livré avec des algorithmes de sécurité en se basant sur le json web token.

2.1.1. Json Web Token (JWT)

JSON Web Token (JWT) est un standard ouvert défini dans la RFC 75191. Il permet l'échange sécurisé de jetons (tokens) entre plusieurs parties. Cette sécurité de l'échange se traduit par la vérification de l'intégrité des données à l'aide d'une signature numérique,

Le token est composé de trois parties et chacune contient des informations différentes comme suit :

- **Un Header** : identifie l'algorithme qui a été utilisé pour générer la signature, ainsi que le type de token, dans notre application nous avons utilisé l'algorithme de hachage HS256
- **Un payload** : le payload contient les claims (les informations de l'utilisateur) que l'on souhaite transmettre.
- **Une signature** : c'est la dernière partie du token, et est générée à partir du payload et du Header.

Le jeton sera envoyé avec chaque requête que le client fera auprès de l'application, qui autorisera, ou non, le client à accéder à ses services, suivant la validité de ce dernier.

2.1.2. Diagramme de séquence d'implémentation de la couche sécurité

Le diagramme de séquence ci-après décrit en détail le séquençement du processus de la couche sécurité en utilisant Spring Security en utilisant le JWT.

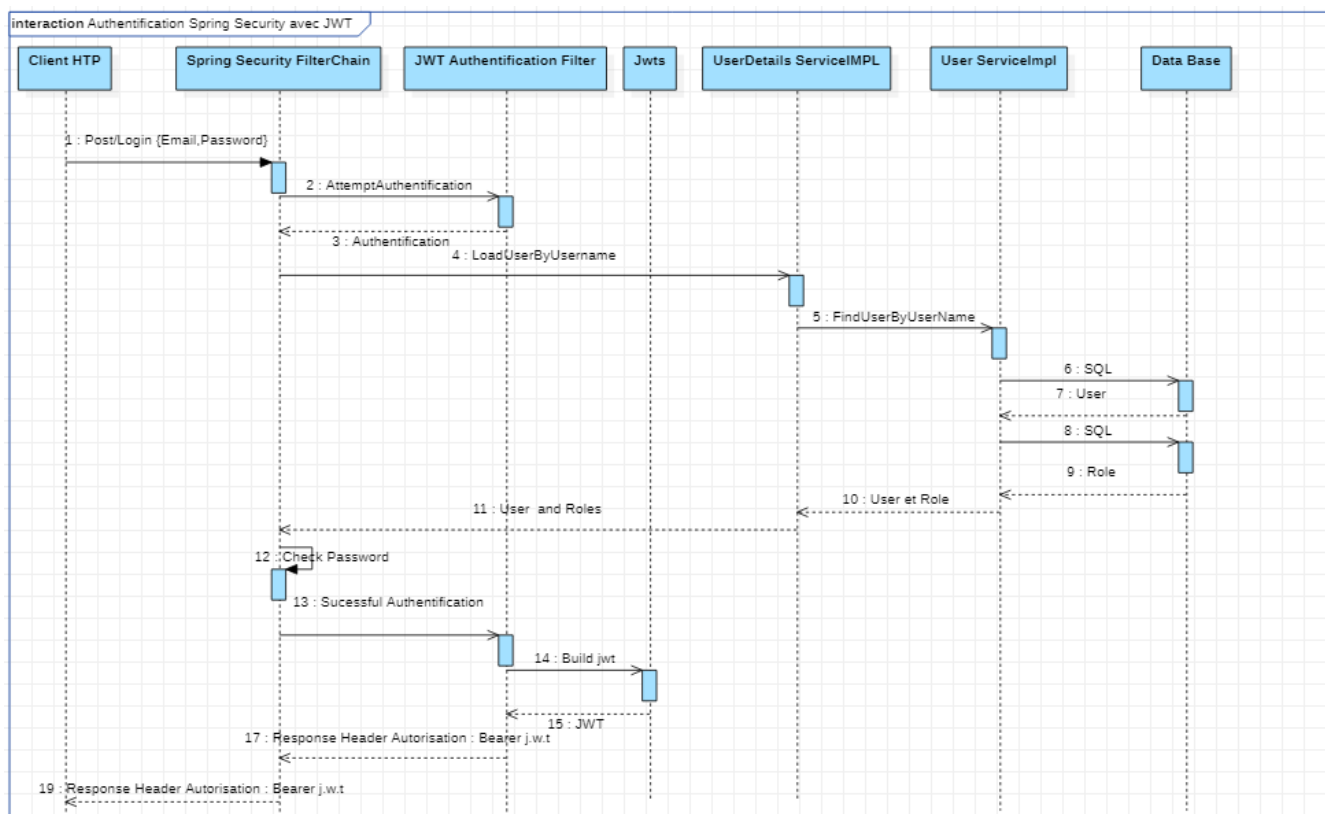


Figure 1 : Authentication Spring Security avec JWT

2.2. Backlog du produit

Nous allons énumérer les différents user story de ce premier Sprint ‘Authentification et gestion d’accès ‘ dans le backlog Sprint 1 présenté par le tableau suivant.

Tableau 1 : Backlog Sprint 1 : Gestion d'accès

ID Module	Module	ID User Story	User Story	ID tâche	Tâche
1	Authentification et gestion d'accès	1	En tant qu'utilisateur de l'application, je veux m'authentifier à l'application via mon adresse e-mail et mon mot de passe.	1.1.	Implémenter la partie Spring security dans la partie backend.
				1.2.	Implémenter et tester les apis et les services nécessaires pour l'authentification dans la partie backend et frontend.
		2	En tant qu'utilisateur se connecte pour la première fois à l'application, je dois modifier mon mot de passe .	2.1.	Implémenter et tester les apis et les services nécessaires pour la modification du mot de passe dans la partie back end et front end.
		3	En tant qu'utilisateur, je veux récupérer l'accès à mon compte avec	3.1.	Implémenter et tester les api et les services nécessaires à la génération du reset token et son envoie par email

			l'option mot de passe oublié		de l'application à l'adresse de l'utilisateur.
				3.2.	Implémenter et tester les apis et les services nécessaire à la modification du mot de passe.
		4.	En tant que manager de l'application, je veux activer/désactiver un compte employée.	4.1.	Implémenter et tester les api et les services nécessaire à l'activation du compte employée.
				4.2.	Implémenter et tester les api et les services nécessaire à la désactivation du compte employée.

2.3. Analyse

Les “User Stories” que nous avons spécifié dans le backlog précédant nous permettent de mieux comprendre l’objectif de ce premier sprint.

Dans la section suivante, nous allons modéliser les différentes spécifications et fonctionnalités par des diagrammes de cas d’utilisation et des descriptions textuelles de quelques cas.

2.3.1. Diagrammes des cas d’utilisation

Dans le but de décrire les fonctionnalités de ce sprint d’une manière formelle, nous exposons le diagramme de cas d’utilisation dans la figure numéro 2 suivante.

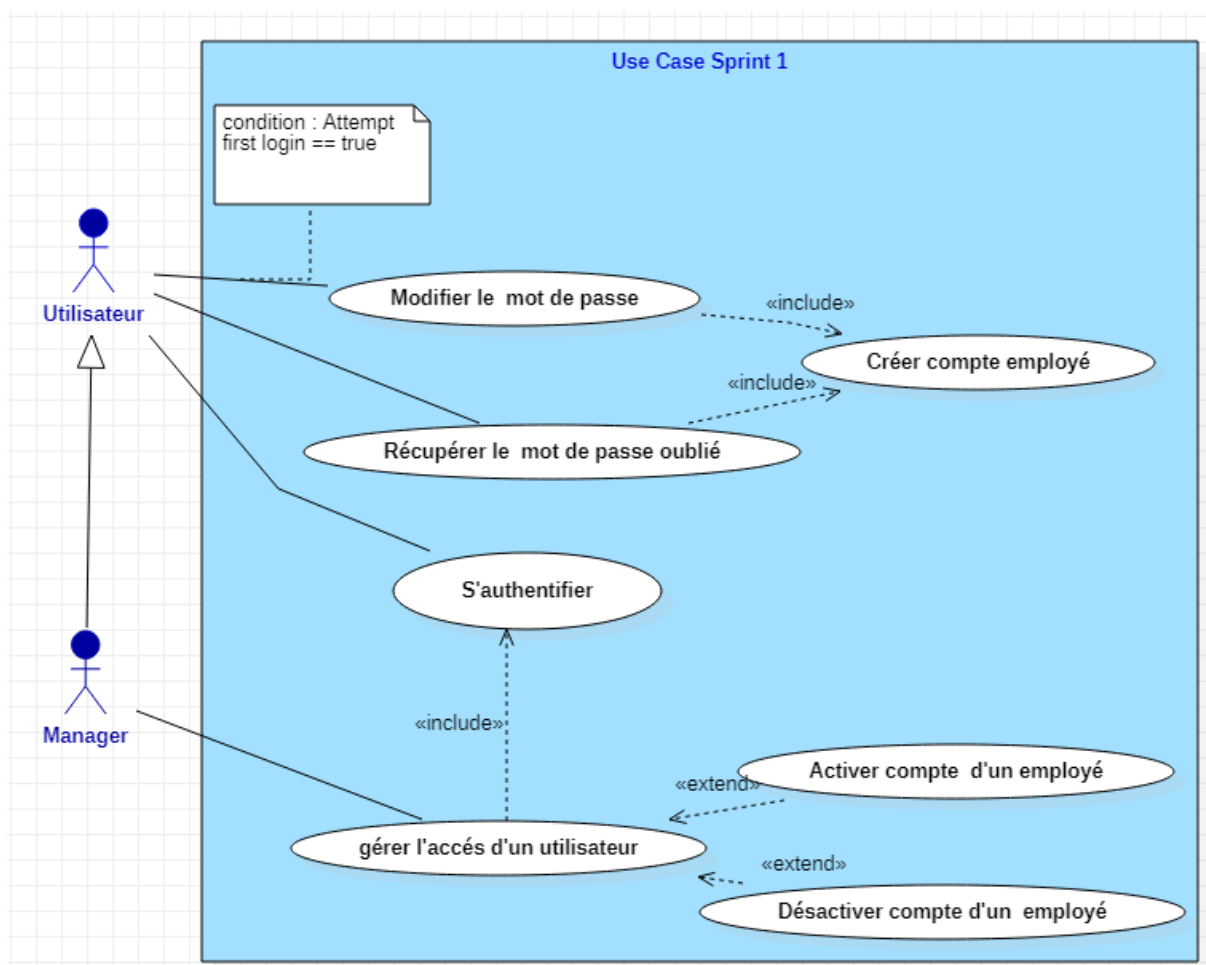


Figure 2: Diagramme des cas d'utilisation du premier Sprint

2.3.2. Raffinement des cas d'utilisation

Même si le diagramme des cas d'utilisation donne une représentation simple du système en main et montre les relations entre les acteurs et les cas d'utilisation, nous procédons dans cette partie au raffinement de quelques cas d'utilisation.

- Description textuelle du cas d'utilisation : Authentification

Le tableau numéro 2 ci-dessous, illustre le raffinement du cas d'utilisation S'authentifier, en présentant l'acteur de la fonctionnalité, les conditions, le scénario nominal et les exceptions de cette fonctionnalité.

Tableau 2 : Raffinement du cas d'utilisation "S'authentifier"

Raffinement du cas d'utilisation S'authentifier	
Cas d'utilisation	S'authentifier
Acteur	Utilisateur de l'application
Objectif	Accéder à l'application
Résumé	L'utilisateur s'authentifie afin d'accéder à l'application pour gérer ses fonctionnalités selon son rôle.(Manager/Team Leader, Team Member).
Conditions	
Préconditions	Post Conditions
<ul style="list-style-type: none">- L'utilisateur doit avoir un compte employé.- Le compte de l'employé doit avoir le statut actif.- L'utilisateur doit être connecté au moins une fois avant à l'application.- Le json web token est non expiré.	L'utilisateur se connecte à l'application.
Scénario	

1- L'utilisateur accède au formulaire d'authentification. 2- L'utilisateur saisit ses informations de login et mot de passe dans le formulaire. 3- Le système vérifie le compte depuis la base de données 4- Le système redirige l'utilisateur vers la page d'accueil selon son rôle.
Exception
1-Si les informations de connexions (login et/ou mot de passe) sont erronées, un message d'erreur s'affiche "veuillez vérifier vos coordonnées" 2-Si le compte de l'employé est désactivé, un message d'erreur s'affiche. "vous n'avez pas le droit de se connecter à l'application". 3- Si l'utilisateur se connecte pour la première fois, une redirection vers la page modifier mot de passe.

- **Description textuelle du cas d'utilisation : Modifier le mot de passe**

Le tableau numéro 3 ci-dessous, illustre le raffinement du cas d'utilisation Modifier le mot de passe, en présentant l'acteur de la fonctionnalité, les conditions, le scénario nominal et les exceptions de cette fonctionnalité.

Tableau 3 : Raffinement du cas d'utilisation "Modifier le mot de passe"

Raffinement du cas d'utilisation Modifier le mot de passe	
Cas d'utilisation	Modifier le mot de passe.
Acteur	Un utilisateur de l'application qui n'est jamais connecté.
Objectif	Se connecter à l'application.
Résumé	L'utilisateur modifie son mot de passe pour pouvoir accéder à l'application pour la première fois.

Conditions	
Préconditions	Post Conditions
<ul style="list-style-type: none"> - Un utilisateur tente de se connecter pour la première fois à l'application. - le compte de l'utilisateur doit avoir l'état actif. 	L'utilisateur accède à l'application.
Scénario	
<ol style="list-style-type: none"> 1- L'utilisateur accède au formulaire d'authentification. 2- L'utilisateur saisit ses informations de login et mot de passe dans le formulaire. 3- Le système redirige l'utilisateur à la page de modification du mot de passe. 4- L'utilisateur modifie son mot de passe. 5- Le système redirige l'utilisateur à la page du formulaire d'authentification. 6- L'utilisateur saisit ses informations de login et mot de passe dans le formulaire. 7- Le système vérifie les données depuis la base de données. 8- Le système redirige l'utilisateur vers la page d'accueil selon son rôle. 	
Exception	
<ol style="list-style-type: none"> 1-Si les deux champs du mot de passe ne sont pas identiques, un message d'erreur s'affiche "les deux champs ne sont pas identiques". 2-Si les informations de connexions (login et/ou mot de passe) sont erronées, un message d'erreur s'affiche "veuillez vérifier vos coordonnées". 3-Si le compte de l'employé est désactivé, un message d'erreur s'affiche. "vous n'avez pas le droit de se connecter à l'application". 	

- **Description textuelle du cas d'utilisation : Récupérer mot de passe oublié**

Le tableau numéro 3 ci-dessous, illustre le raffinement du cas d'utilisation récupérer mot de passe oublié, en présentant l'acteur de la fonctionnalité, les conditions, le scénario nominal et les exceptions de cette fonctionnalité.

Raffinement du cas d'utilisation Récupérer mot de passe oublié	
Cas d'utilisation	Récupérer mot de passe oublié
Acteur	Utilisateur de l'application (Manger/Team Leader/ Team Member)
Objectif	Changer le mot de passe et récupérer l'accès à l'application.
Résumé	L'utilisateur change son mot de passe afin d'accéder à l'application pour gérer ses fonctionnalité selon son rôle.(Manager/Team Leader, Team Member).
Conditions	
Préconditions	Post Conditions
- le compte de l'utilisateur doit avoir le statut actif.	L'accès à l'application est récupéré.
Scénario	
1- Le système affiche le formulaire d'authentification. 2- L'utilisateur choisit l'option mot de passe oublié. 3- Le système affiche un nouveau formulaire "mot de passe oublié". 4- L'utilisateur entre son email.	

<p>5- Le système envoie un code à l'adresse email et indique à l'utilisateur de vérifier son email.</p> <p>6- L'utilisateur saisit le code reçu par email dans le formulaire du mot de passe oublié.</p> <p>7- Le système vérifie le code et redirige l'utilisateur vers le tableau de bord.</p>
Exception
<p>1-L'utilisateur saisit un code erroné “ vous avez saisi un code erroné “</p> <p>2-L'utilisateur saisit un email qui n'existe pas dans la base de donnée, un message d'erreur s'affiche “Vous avez saisi un e-mail non valide” .</p>

2.4. Conception

Au niveau de cette section, nous allons entamer la phase de conception du premier sprint. Pour se faire, nous présentons la vue dynamique de notre application ayant recours aux diagrammes d'activités et aux diagrammes de séquence.

2.4.1. Diagramme de séquence Système

Les diagrammes de séquences système offrent une description des scénarios des cas d'utilisations en mettant l'accent sur la chronologie des interactions entre les acteurs et le système. Dans cette partie, nous allons exposer quelques scénarios dans des diagrammes de séquence système. [1]

- **Diagramme de séquence système du scénario s'authentifier**

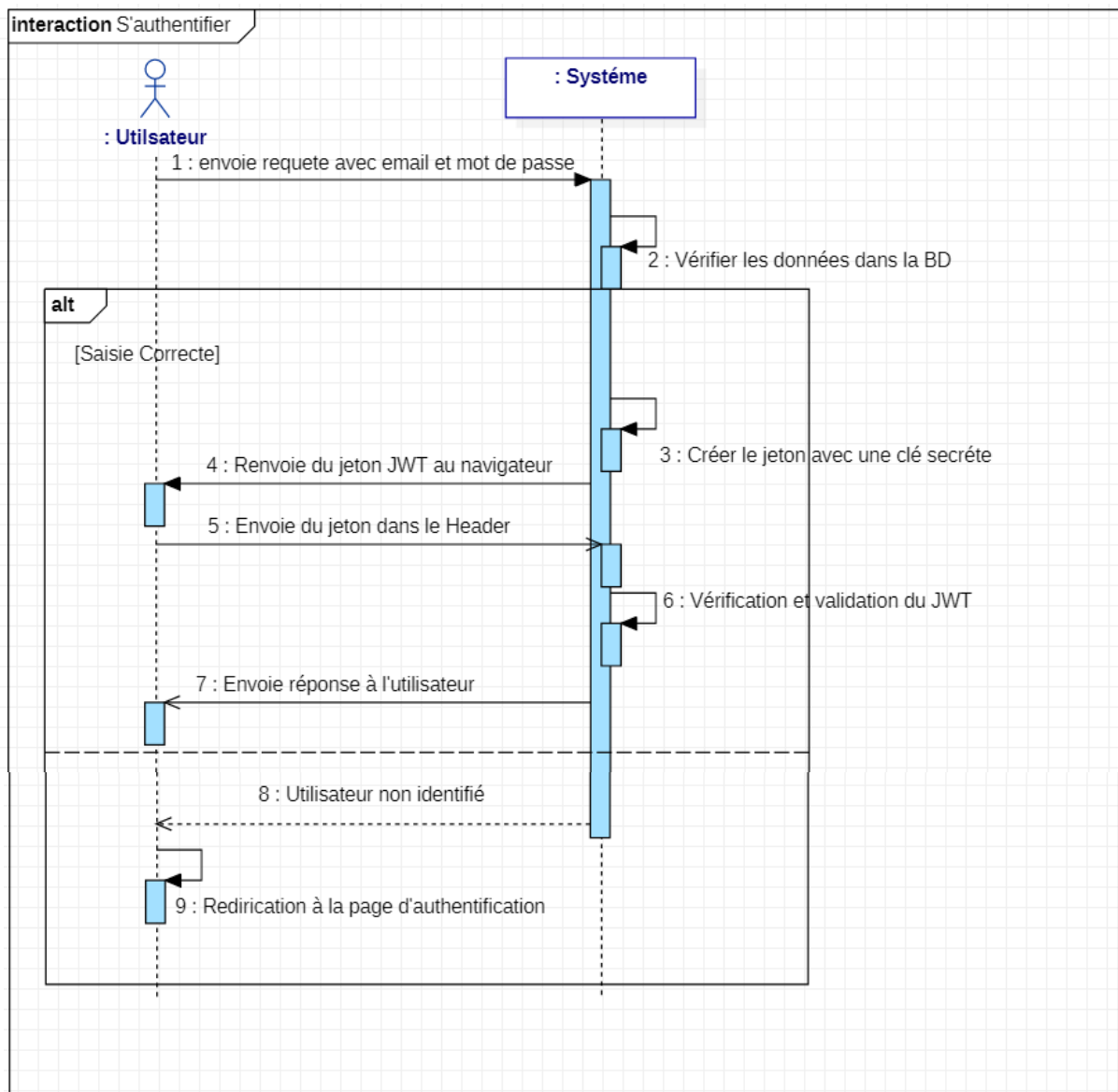


Figure 3 : Diagramme de séquence système du scénario s'authentifier

- Diagramme de séquence système du scénario récupérer mot de passe oublié

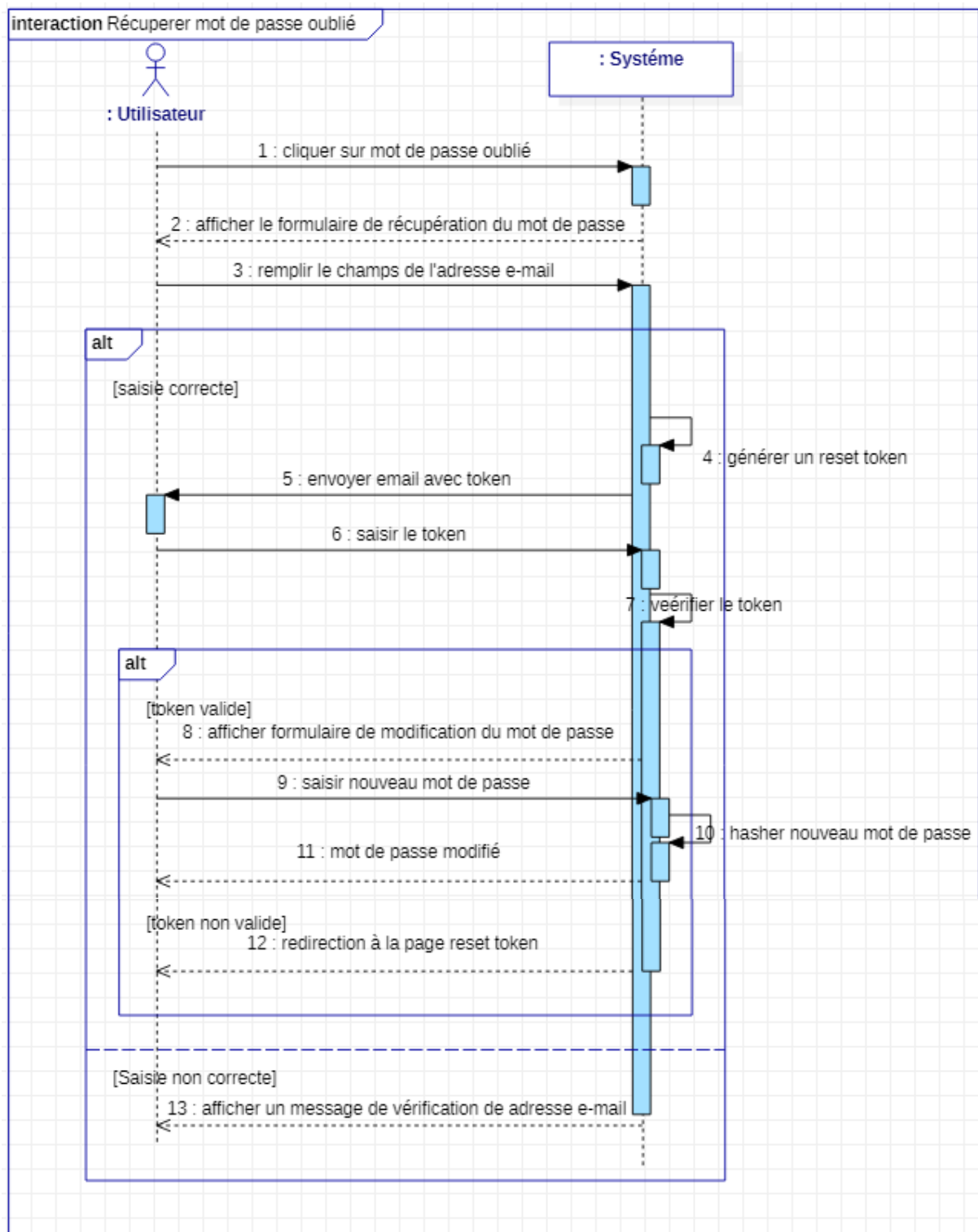


Figure 4 : Diagramme de séquence du système du scénario Récupérer mot de passe

2.4.2. Diagramme d'activité du cas d'utilisation modifier mot de passe

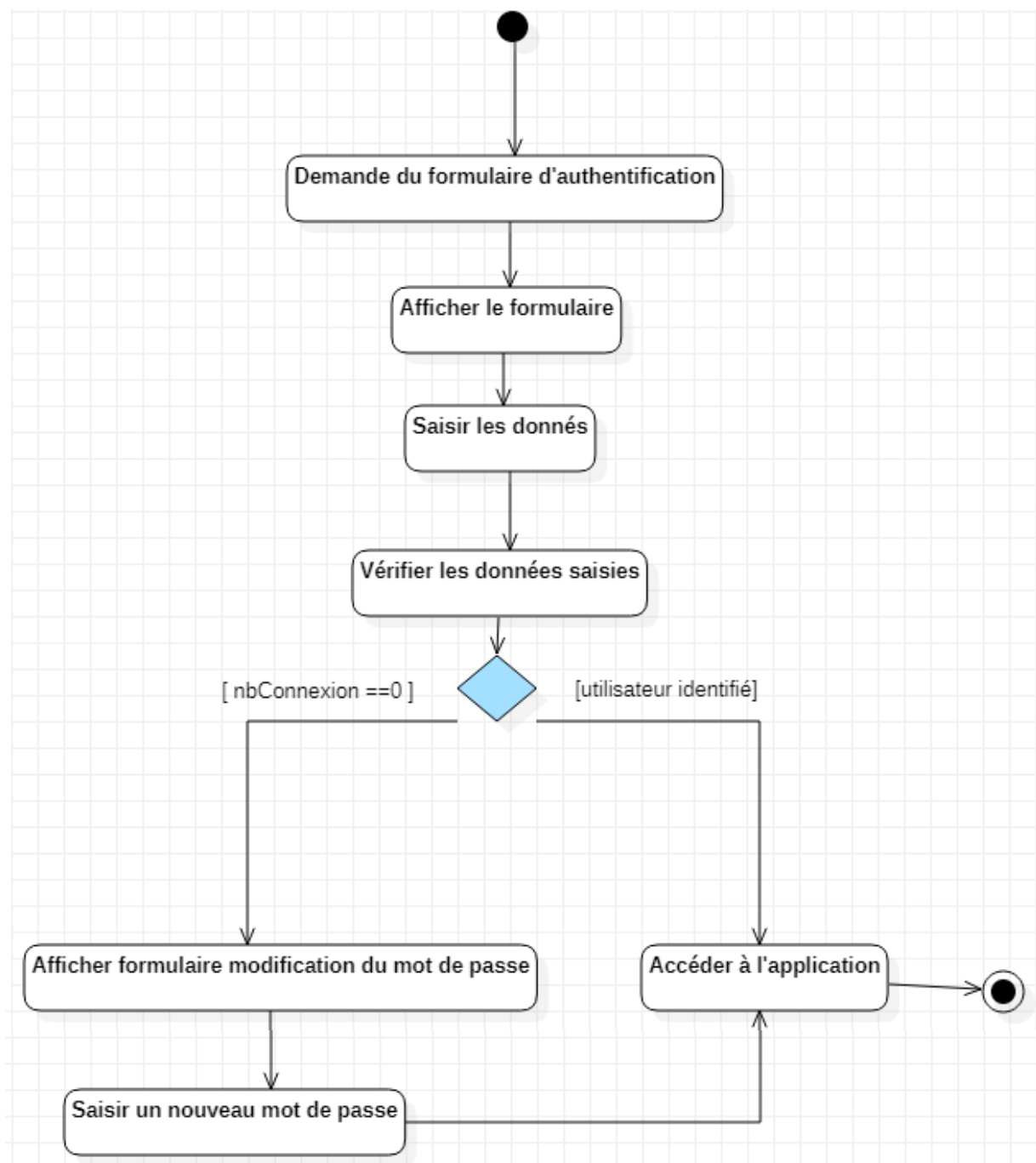


Figure 5 : Diagramme d'activité du cas d'utilisation modifier mot de passe

2.5. Réalisation

Dans cette partie nous présenterons les interfaces Homme/Machine IHM de notre premier sprint, qui est le module Authentification et gestion d'accès, afin de montrer le mode de fonctionnement de ce dernier.

2.5.1. Interface d'authentification

La figure ci-dessous présente l'interface d'authentification. L'utilisateur saisit son adresse e-mail et son mot de passe, s'ils sont corrects, il aura la permission d'accéder aux différentes fonctionnalités de l'application selon son rôle si non un message d'erreur s'affiche.

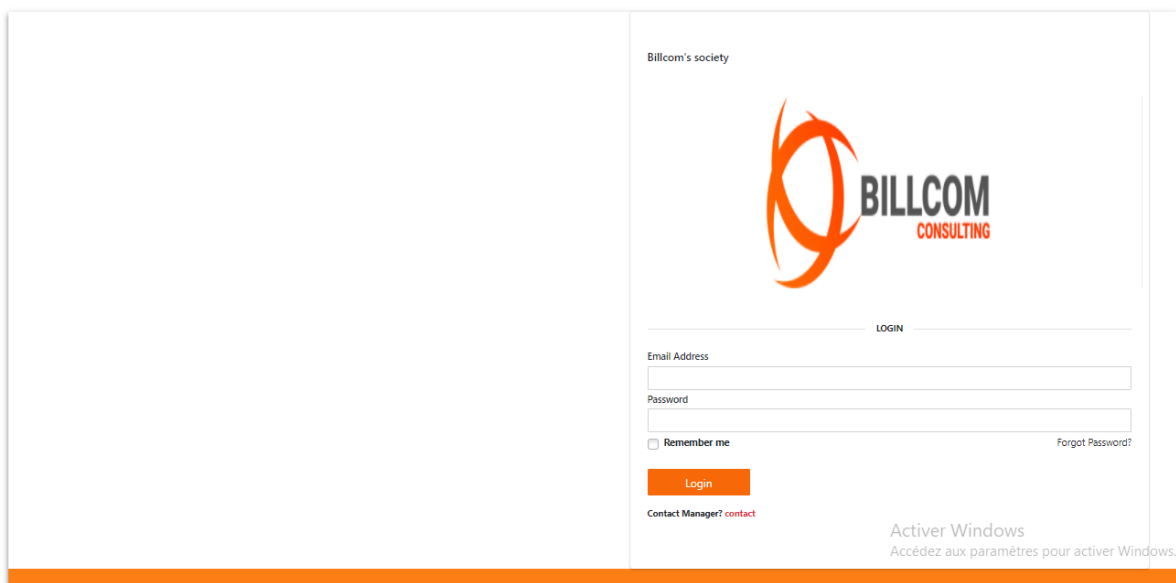
The image shows a web-based login interface for 'Billcom's society'. At the top, the text 'Billcom's society' is displayed. Below it is the company logo, which consists of an orange stylized circular graphic followed by the text 'BILLCOM CONSULTING' in black and red. Under the logo, the word 'LOGIN' is centered. There are two input fields: 'Email Address' and 'Password'. Below the 'Email Address' field is a checkbox labeled 'Remember me'. To the right of the 'Password' field is a link that says 'Forgot Password?'. A red 'Login' button is positioned below the 'Remember me' checkbox. At the bottom left, there is a link 'Contact Manager? contact'. At the bottom right, there is a Windows watermark that says 'Activer Windows' and 'Accédez aux paramètres pour activer Windows.'.

Figure 6 : Interface d'authentification

Les cas d'erreurs

- Si l'utilisateur saisit une adresse e-mail non valide
- Si un utilisateur ne remplit pas un des champs obligatoires
- Si les données ne sont pas valides

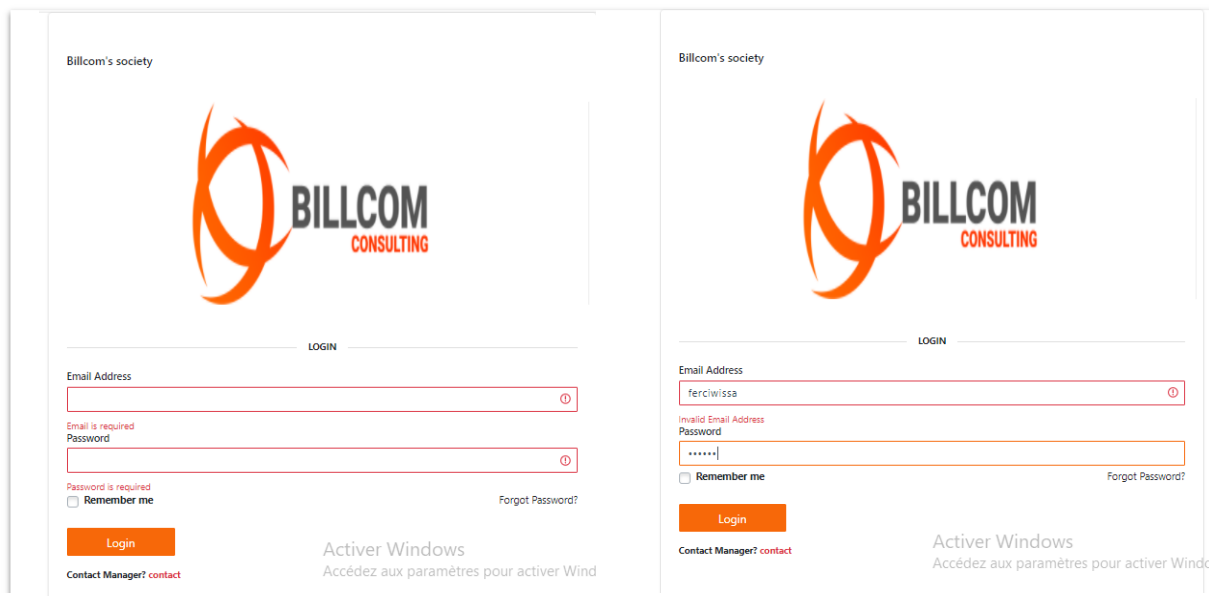



Figure 7 : Les messages des cas d'erreur

2.5.2. Interface de récupération du mot de passe oublié

Pour récupérer son mot de passe l'utilisateur doit écrire son e-mail, attendre la réception d'un token et puis il doit saisir le code envoyé.

Reset Password



Enter Your Email Address

[Get Code](#)

Contact Manager? [contact](#)

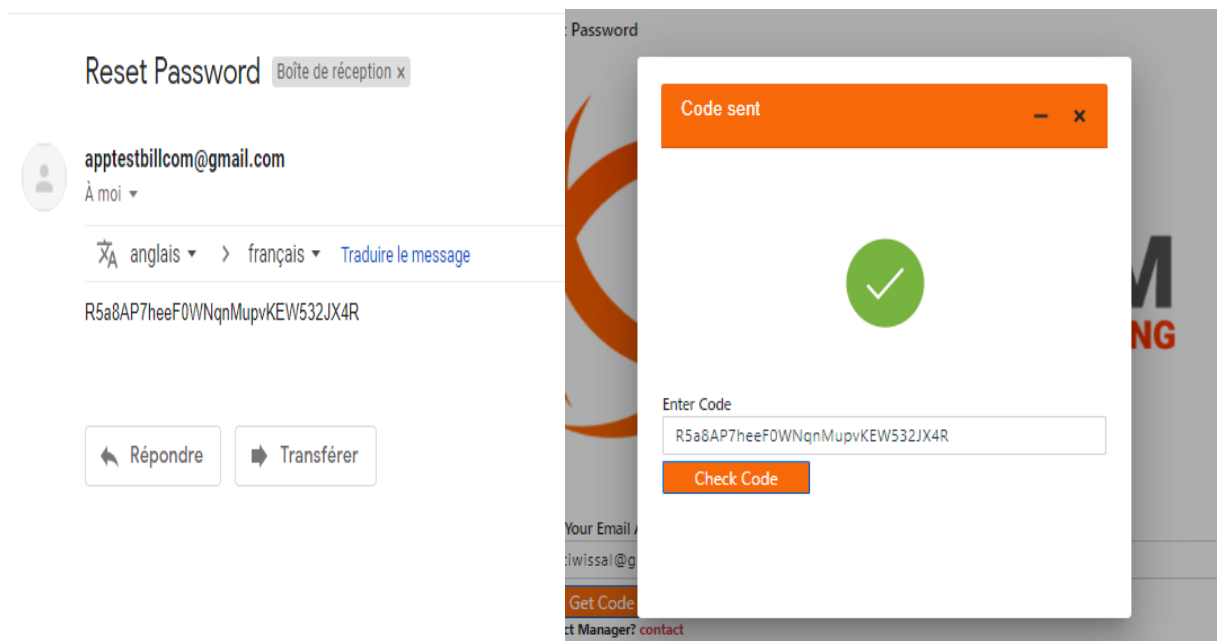
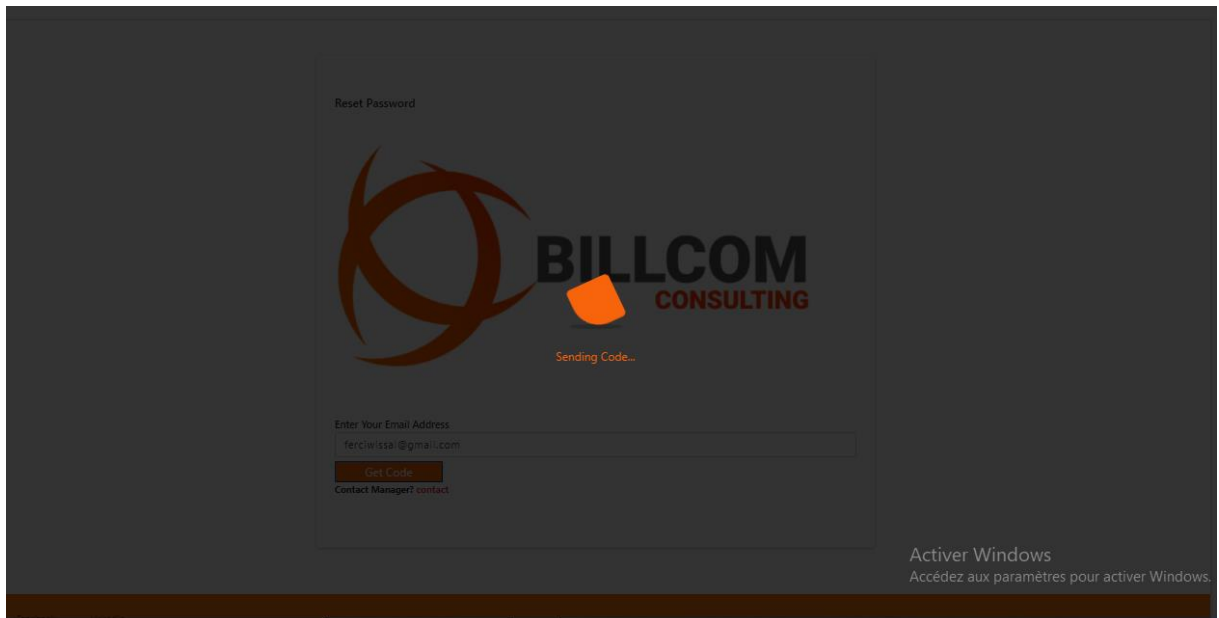


Figure 8 : Récupération du mot de passe oublié

2.5.3. Interface de modification du mot de passe

Si l'utilisateur se connecte pour la première fois, il va recevoir un e-mail de ses coordonnées et pour se connecter à l'application il doit modifier son mot de passe pour des raisons de confidentialités de ses données.

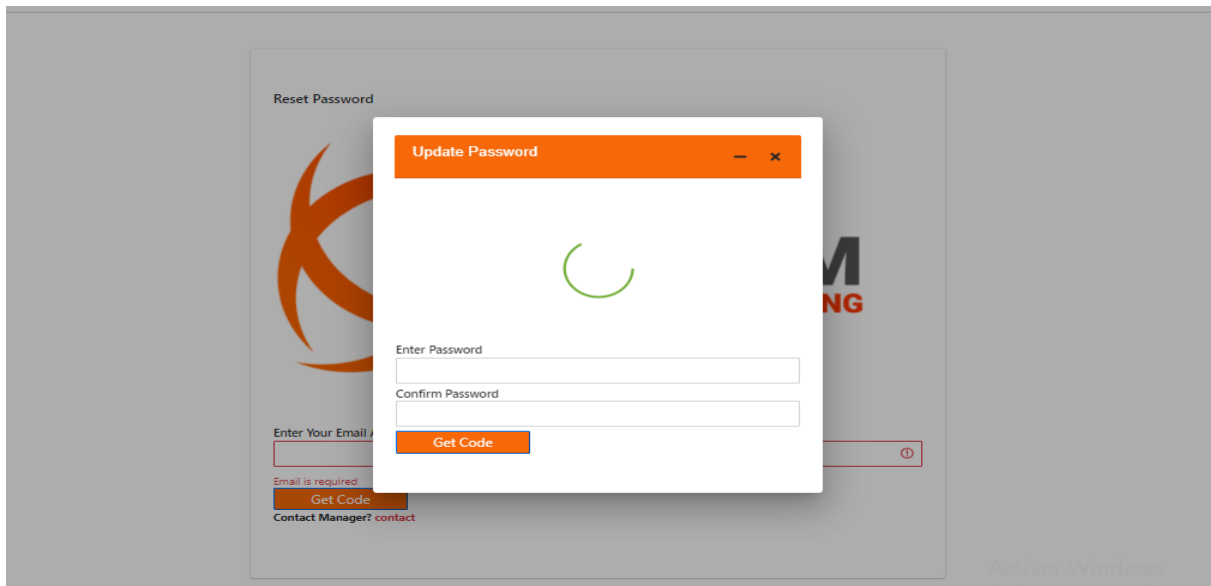


Figure 9 : Interface de modification du mot de passe

2.5.4. Interface d'activation et de désactivation d'un compte employé

En se connectant à son application, un manager peut activer ou désactiver un compte employé.

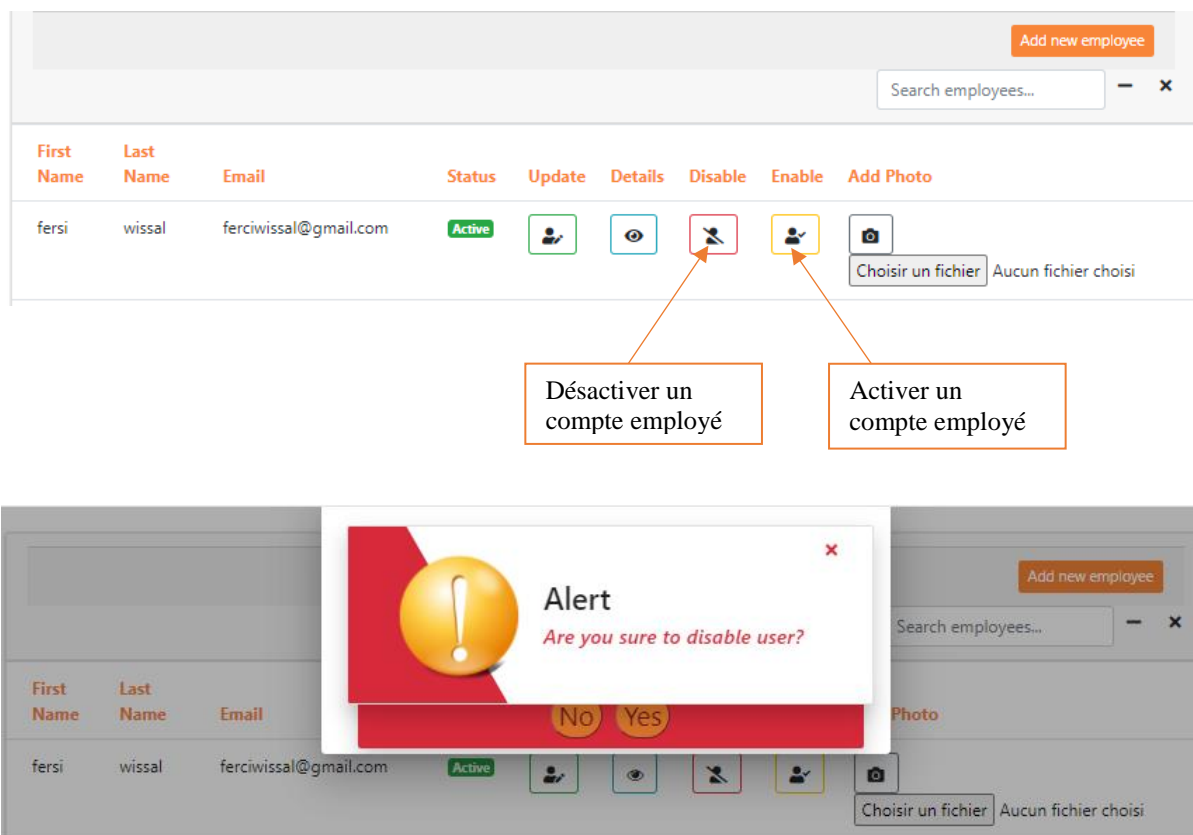


Figure 10 : Interface d'activation/désactivation du compte employé

3. Sprint 2 : Gestion utilisateurs et gestion profil

Pour pouvoir accéder à l'application et gérer les fonctionnalités suivant le rôle, une gestion des utilisateurs et de leurs rôles doit être exploitée ainsi qu'une gestion de leurs profils. Dans ce deuxième Sprint du premier release nous allons traiter et développer deux modules :

- Gestion utilisateurs
- Gestion profil

3.1. Backlog du produit

Le tableau numéro 4 ci-après représente le backlog de notre deuxième sprint "Gestion utilisateurs et gestion du profil". Nous exposons dans cette partie les user stories liés à ce sprint pour pouvoir les analyser dans la suite de ce chapitre

Tableau 4 : Backlog Sprint 2

ID Module	Module	ID User Story	User Story	ID tâche	Tâche
2	Gestion des comptes employés et leurs rôles	1	En tant que manager, je veux créer des comptes employés	1.1.	Implémenter et tester les apis et les services nécessaires pour l'ajout des comptes dans la partie backend et frontend.
		2.	En tant que manager, je veux Consulter les détails des employés.	2.1.	Implémenter et tester les apis et les services nécessaires pour la consultation de la liste des employés des comptes dans la partie backend et frontend.
				2.2.	Implémenter et tester les apis et les services nécessaires pour la consultation de détail de chaque employée dans la partie backend et frontend.
		3.	En tant que manager, je veux Appliquer des recherches sur la liste des employés.	2.2.	Implémenter et tester la méthode de recherche par nom de l'employé.
				3.2.	Implémenter et tester la méthode de recherche par numéro de téléphone de l'employé.

				3.3.	Implémenter et tester la méthode de recherche par l'e-mail de l'employé
		4.	En tant que manager, je veux ajouter/supprimer un ou plusieurs rôles pour les employés.	4.1.	Implémenter et tester les api et services pour la fonctionnalité ajouter rôle à l'employé.
				4.2.	Implémenter et tester les api et services pour la fonctionnalité supprimer un rôle associé à l'employé.
3	Gestion des profils	1.	En tant qu'employé, je veux modifier mon profil.	1.1.	Implémenter et tester les apis et les services nécessaires à la modification du profil dans la partie backend et frontend.
			En tant qu'employé je veux modifier mon mot de passe	1.2.	Implémenter et tester les apis et les services nécessaires à la modification du mot de passe dans la partie backend et frontend.

3.2. Analyse

Au niveau de cette section, nous avons commencé par l'exposition du Backlog du sprint. Ensuite, nous passons à la phase d'analyse de ce sprint dans laquelle nous présentons le diagramme de cas d'utilisation ainsi, des descriptions textuelles de quelques cas d'utilisation.

3.2.1. Diagramme des cas d'utilisation

La figure numéro 6 ci-après présente le diagramme des cas d'utilisation du deuxième Sprint.

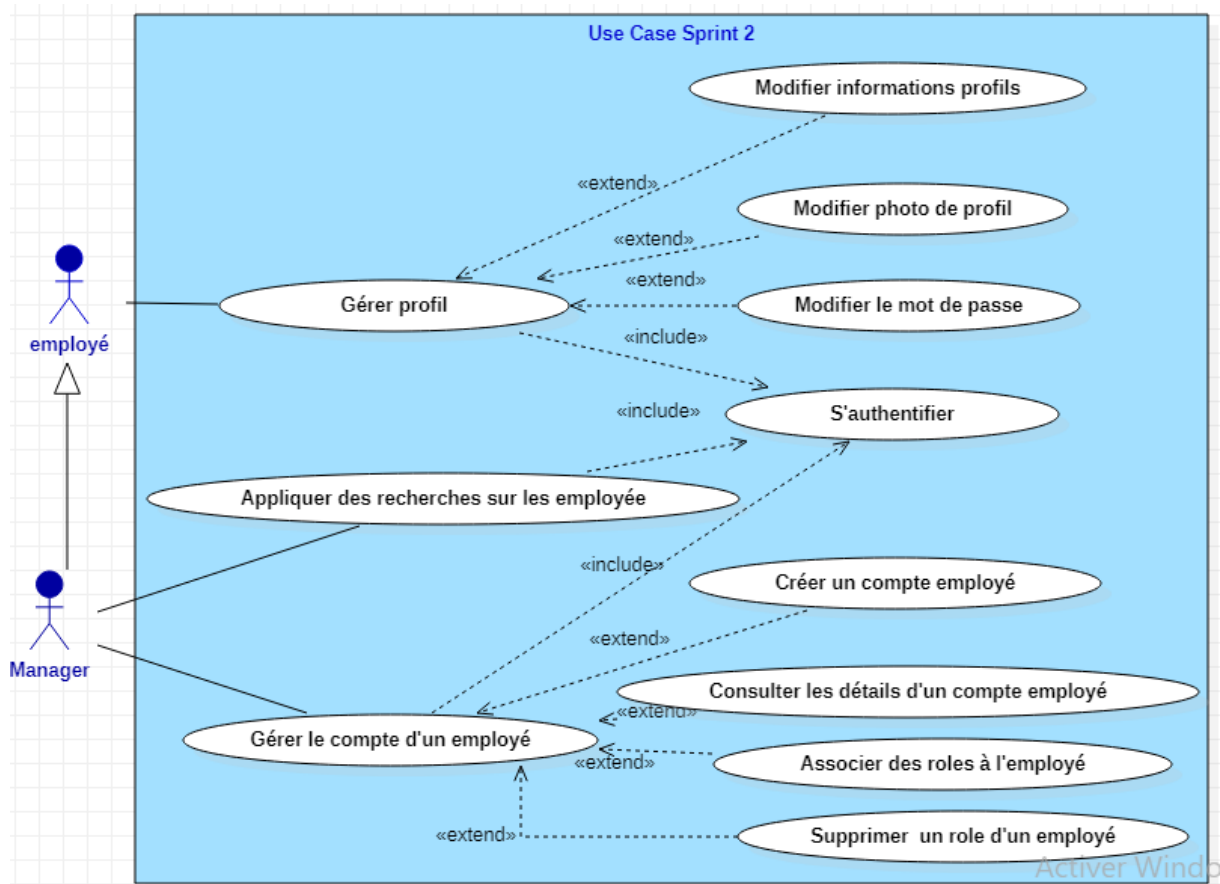


Figure 11 : Diagramme des cas d'utilisation du Sprint numéro 2

3.2.2. Raffinement des cas d'utilisation

Dans cette partie, nous allons raffiner les cas d'utilisation de notre diagramme en présentant une description textuelle de quelques cas.

- Description textuelle du cas d'utilisation : Ajouter un compte employé

Le tableau numéro 5 ci-dessous, illustre le raffinement du cas d'utilisation Ajouter un compte employé, en présentant l'acteur de la fonctionnalité, les conditions, le scénario nominal et les exceptions de cette fonctionnalité.

Tableau 5 : Raffinement du cas d'utilisation "Ajouter un compte employé"

Raffinement du cas d'utilisation	
Cas d'utilisation	Ajouter un compte employé
Acteur	Manager de l'application
Objectif	Créer un compte employé
Résumé	Un utilisateur ayant le rôle manager ajoute un compte d'un employé avec succès.
Conditions	
Préconditions	Post Conditions
<ul style="list-style-type: none"> - S'authentifier en tant que manager. - l'email du nouveau compte est inexistant dans la base. - Saisir des informations valide. 	Le compte de l'employé est créé avec succès.
Scénario	
1- Le manager s'authentifie avec son compte. 2- Le manager accède à la partie ajout d'un employé. 3- Le manager remplit les champs de l'employé à ajouter. 4- Le système vérifie la validité des données. 5- le système valide la création du compte de l'employé. 6- Le système affiche une notification de création avec succès.	
Exception	
1-Si les informations de saisie ne sont pas valides, un message d'erreur s'affiche en spécifiant le problème.	

2-Si l'adresse e-mail de l'employé existe dans la base de donnée un message d'erreur s'affiche.

- **Description textuelle du cas d'utilisation : Ajouter un rôle à l'employé**

Le tableau numéro 6 ci-dessous, illustre le raffinement du cas d'utilisation Ajouter un rôle à un employé, en présentant l'acteur de la fonctionnalité, les conditions, le scénario nominal et les exceptions de cette fonctionnalité.

Tableau 6 : Raffinement du cas d'utilisation "Ajouter un rôle à un employé"

Raffinement du cas d'utilisation	
Cas d'utilisation	Ajouter un rôle à un employé
Acteur	Manager de l'application
Objectif	Un employé aura la possibilité de manipuler les fonctionnalités en tant que Leader et team member.
Résumé	Un rôle ajouté à un employé.
Conditions	
Préconditions	Post Conditions
- S'authentifier en tant que manager.	Le nouveau rôle est associé à l'employé.
Scénario	
1- Le manager s'authentifie avec son compte. 2- Le manager sélectionne l'employé a lequel va ajouter le rôle. 3- Le manager clique sur le bouton ajouter rôle. 4- Le système affiche la liste des rôles. 5- Le manager choisit le rôle à partir d'une liste.	

6- Le système affiche une notification d'ajout avec succès.
Exception
Un employé possède déjà le rôle qui a été sélectionné alors il y'aura un retour à l'étape numéro 4.

- **Description textuelle du cas d'utilisation : Modifier les informations d'un profil**

Le tableau numéro 7 ci-dessous, illustre le raffinement du cas d'utilisation Modifier les information d'un profil, en présentant l'acteur de la fonctionnalité, les conditions, le scénario nominal et les exceptions de cette fonctionnalité.

Tableau 7 : Raffinement du cas d'utilisation "Modifier les informations d'un profil"

Raffinement du cas d'utilisation	
Cas d'utilisation	Modifier les informations d'un profi.
Acteur	Utilisateur de l'application(Manager/Team Leader/Team Member).
Objectif	Un profil utilisateur modifié.
Résumé	Un utilisateur authentifié peut modifier des informations de son profil.
Conditions	
Préconditions	Post Conditions
- Un utilisateur authentifié.	Un profil mis à jour.
Scénario	
1- L'utilisateur accède à la page informations utilisateurs. 2- L'utilisateur clique sur le bouton modifier. 3- Le formulaire des informations s'affiche en format input.	

4- L'utilisateur entre des modifications sur son profil.

5- L'utilisateur valide son choix.

6- Le système affiche un message de succès.

Exception

Un employé possède déjà le rôle qui a été sélectionné alors il y'aura un retour à l'étape numéro 4.

3.3. Conception

La conception est une étape critique dans le cycle de vie d'une application, elle vise à développer des modèles détaillés de l'architecture du système et de réduire sa complexité. Elle nous permet de représenter une vue dynamique du système en se référant à un diagramme de classe et une vue statique en présentant des diagrammes de séquences de quelques cas.

3.3.1. Diagramme des classes

La figure numéro 7 ci-après présente le diagramme de classe de ce sprint.

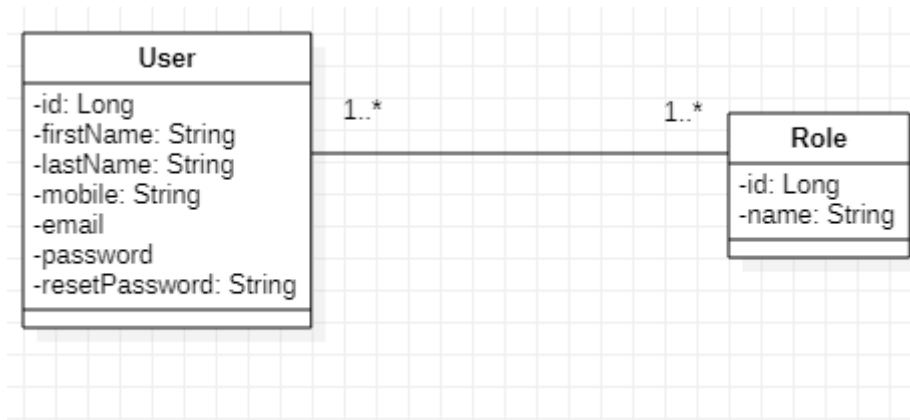


Figure 12 : Diagramme des classes du sprint numéro 2

3.3.2. Diagramme de séquence Système

- Diagramme de séquence système `Ajouter un compte employé`

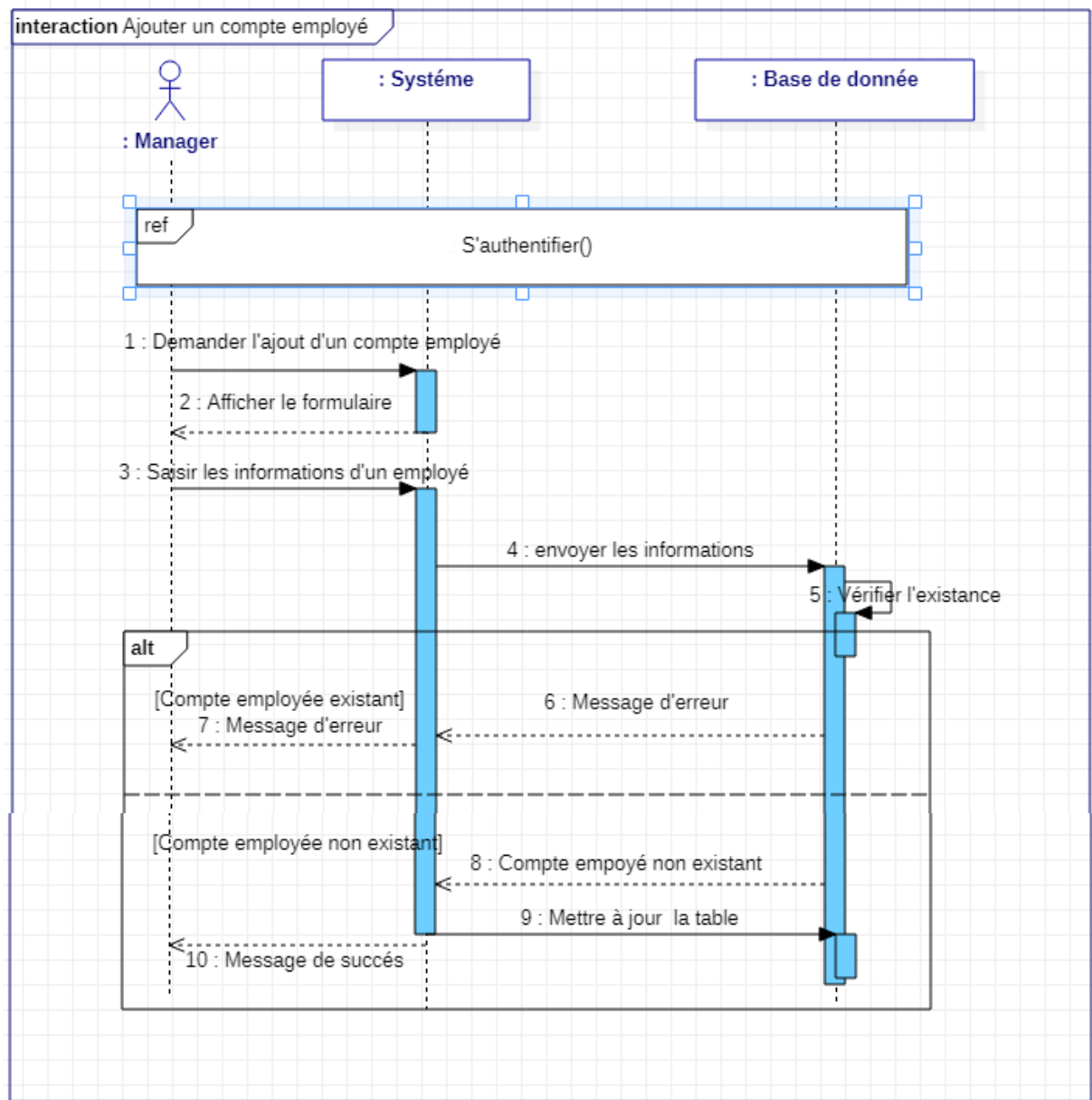


Figure 13 : Diagramme de séquence système Ajouter un compte employé

3.3.3. Diagramme de séquence objet

Les diagrammes de séquence Objet offrent une description des scénarios des cas d'utilisations en mettant l'accent sur la chronologie des opérations en interaction avec les objets. Dans cette partie, nous allons exposer quelques scénarios dans des diagrammes de séquence objet

- Diagramme de séquence objet `Consulter détails Employé`

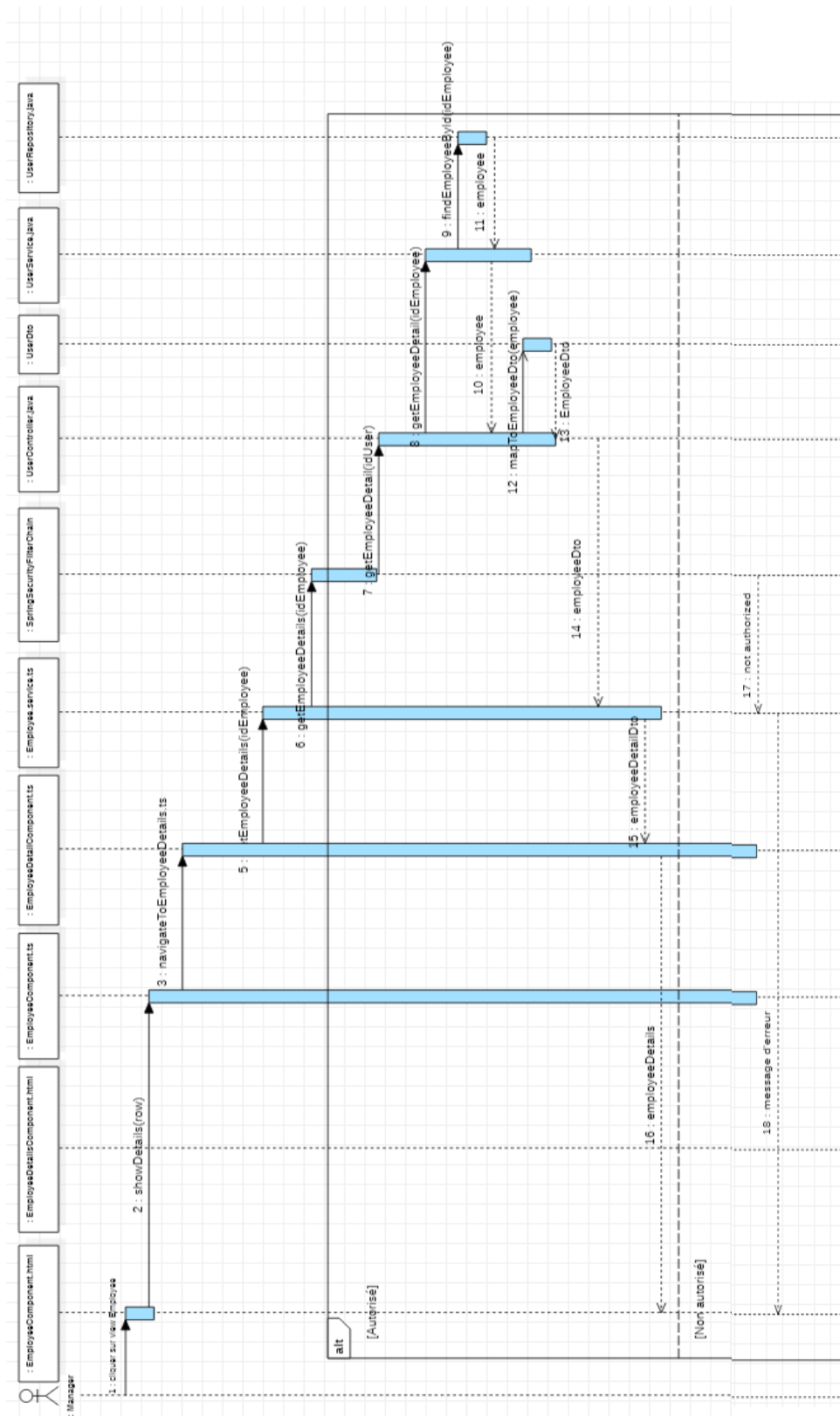


Figure 14 : diagramme de séquence objet du cas d'utilisation "Consulter détails employé "

3.4. Réalisation

Après avoir traité la partie conception, nous exposerons dans ce qui suit quelques interfaces de notre système réalisées au cours de ce deuxième sprint.

3.4.1. Interface d'ajout d'un employé

Pour ajouter des utilisateurs à son application un manager authentifié aura le droit de créer des comptes employé en respectant les contraintes de validation d'un compte. La figure numéro 14 ci-dessous présente le formulaire de création du compte employé.

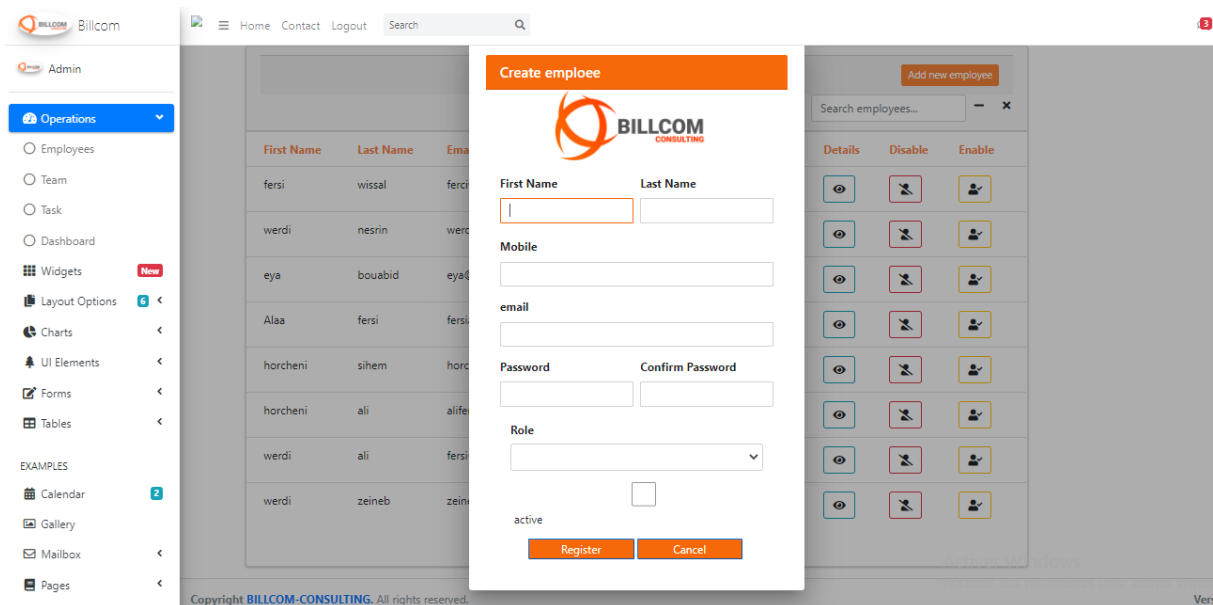



Figure 15 : Interface d'ajout d'un compte employé

Les cas d'erreurs

- Si un manger ne respecte pas les validateurs
- Si une adresse email existe dans la base de donnée

Create employee



First Name

marwa

Last Name

hamdi

Mobile

98688815

email

hamdimarwa

Format Email Invalid

Password

.....

Confirm Password

.....

Passwords must match

Role

manager

active

☒

Register

Cancel

Create employee



First Name

marwa

Last Name

hamdi

Mobile

98688815

email

hamdimarwa@gmail.com

Password

.....

Confirm Password

.....

Passwords must match

Role

manager

active

☒

Register

Cancel

Figure 16 : Cas d'erreur d'ajout du compte employé

3.4.2. Interface de consultation de la liste des employé

Cette interface, numéro 17, ne peut être visible que par le manager de l'application, il aura le droit de consulter la liste de ses employés.

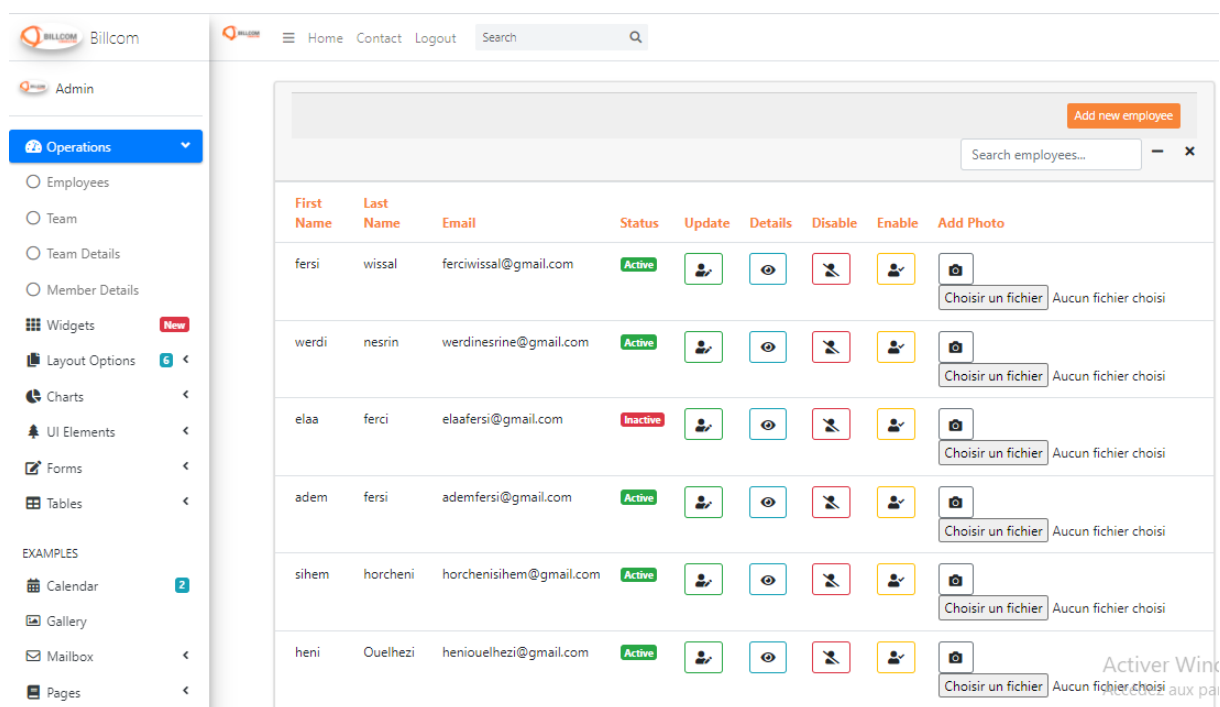


Figure 17 : Interface de la liste des employés

3.4.3. Interface de consultation de détail de chaque employé

En cliquant sur l'icône visualiser d'un employé, le manager peut consulter les détails de l'employé.

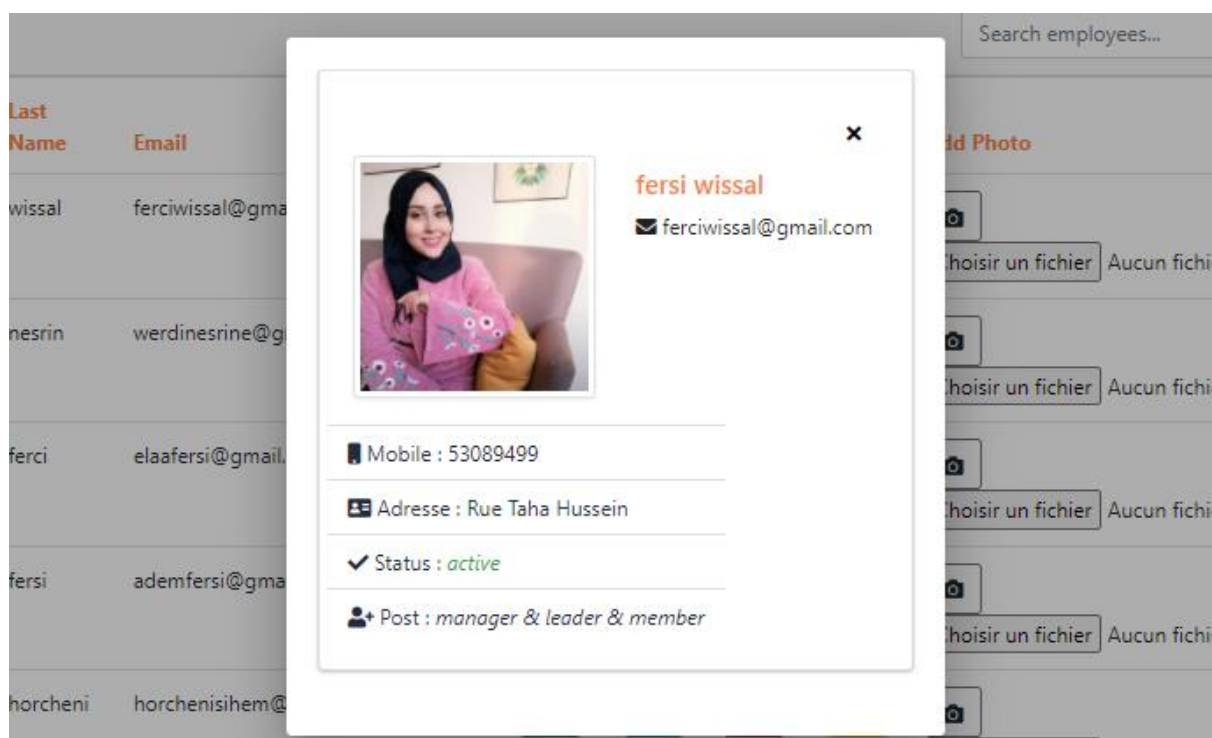


Figure 18 : Interface de consultation des détails d'un employé

3.4.4. Appliquer des recherches sur la liste employée

- Recherche par nom

First Name	Last Name	Email	Status	Update	Details	Disable	Enable	Add Photo
fersi	wissal	ferciwissal@gmail.com	Active					 Choisir un fichier Aucun fichier choisi
fersi	wissal	ferciwissal@gmail.com	Active					 Choisir un fichier Aucun fichier choisi

- Recherche par prénom

First Name	Last Name	Email	Status	Update	Details	Disable	Enable	Add Photo
heni	Ouelhezi	heniouelhezi@gmail.com	Active					 Choisir un fichier Aucun fichier choisi

- Recherche par numéro de téléphone

First Name	Last Name	Email	Status	Update	Details	Disable	Enable	Add Photo
elaa	ferci	elaafersi@gmail.com	Inactive					 Choisir un fichier Aucun fichier choisi

Figure 19 : Operations de recherche appliqué sur la liste

3.4.5. Gestion du rôle d'un employé

Chaque employée aura une liste des rôles. En consultant cette liste un manager peut appliquer des opérations sur cette liste suivant son besoin. Dans la section ci-après, nous allons présenter la partie gestion des rôles

- Consulter la liste du rôle d'un employé

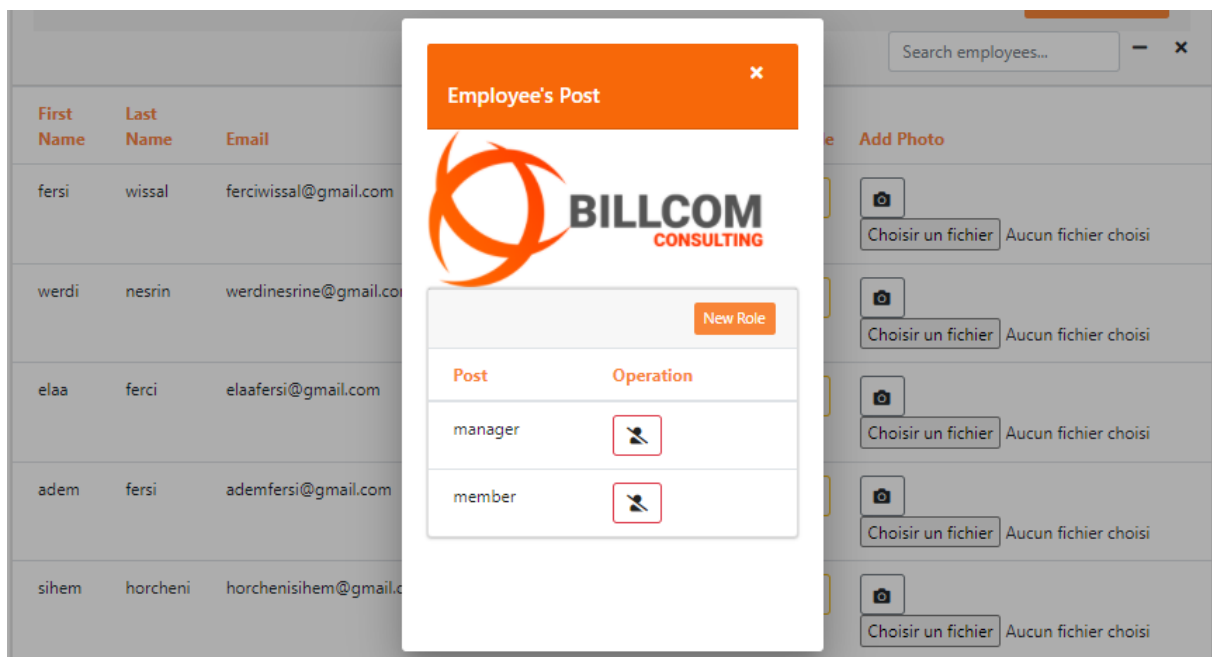


Figure 20 : Interface de la liste des role d'un employé

- Opération sur la liste

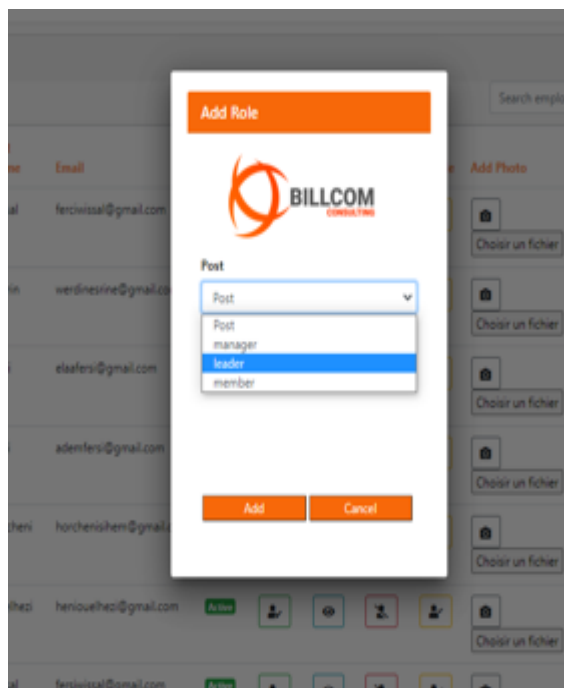


Figure 22 : Ajout d'un rôle à un employée

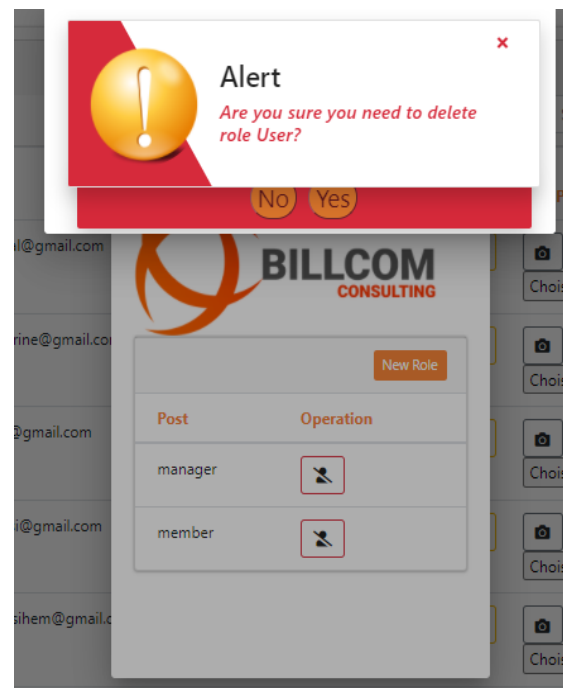


Figure 21 : Supprimer un rôle de la liste des rôle d'un employé

4. Test logiciel du release

Le test du logiciel fait partie du cycle de vie du développement, son objectif est de s'assurer que le code à déployer est de haute qualité, sans bugs ni erreurs logiques.

Pour ce faire nous avons utilisé le Framework Junit 5. La figure qui suit, montre le succès d'exécution des tests développés pour ce release.

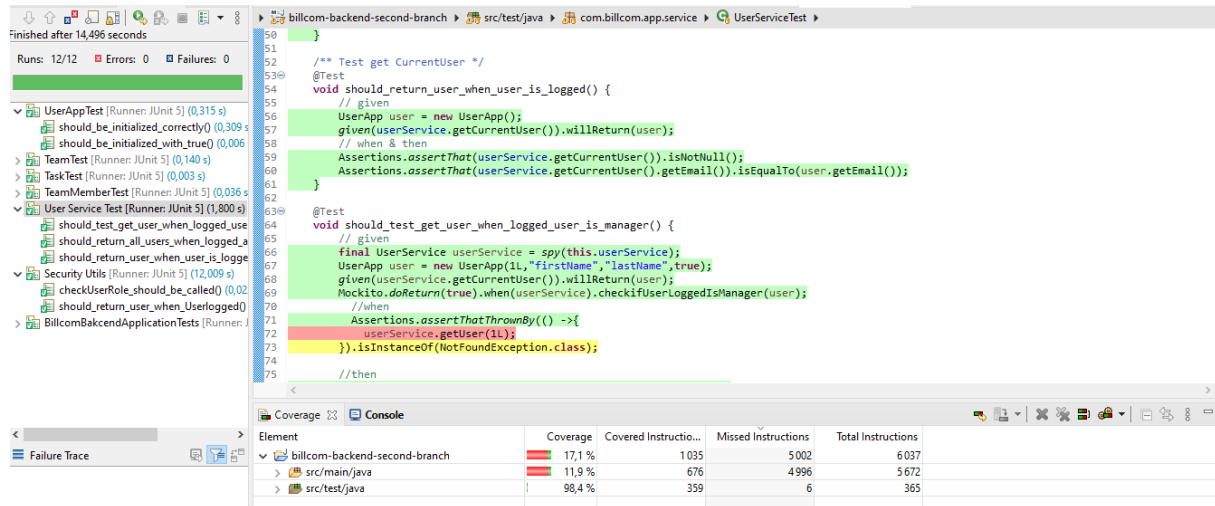


Figure 23 : Application des test unitaire pour la couche user service

En plus que les test logiciel effectué, nous avons utilisé SonarLint qui est une extension IDE que nous utilisons afin de détecter et résoudre les problèmes de qualité du code. La figure suivante montre une analyse que nous avons lancée à l'aide de SonarLint pour le premier release.

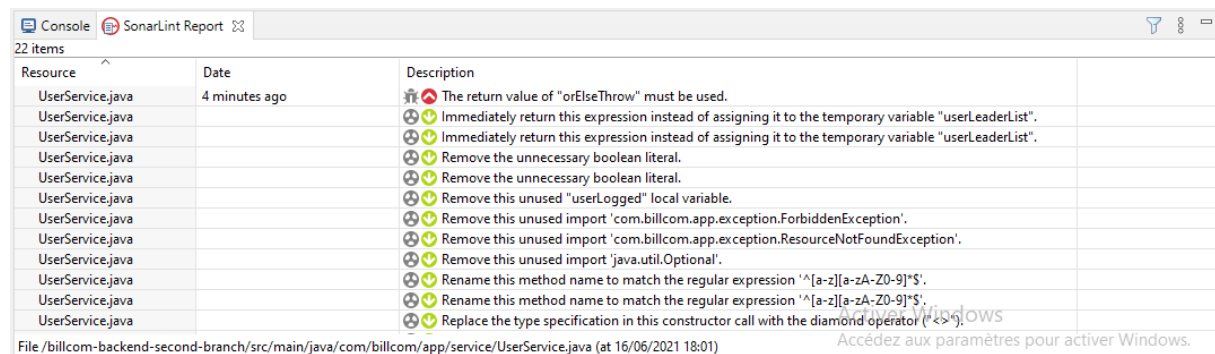


Figure 24 : Analyse SonarLint

5. Documentation

Nous utilisons SwaggerUI pour partager la documentation des contrôleurs entre le chef de produit, les testeurs et les développeurs.

La figure, numéro 24, ci-dessous représente un exemple de documentation de quelques contrôleurs de ce release.



Figure 25 : Documentation du premier release

Conclusion

Au niveau de ce chapitre, nous avons présenté le premier release de notre application qui comporte deux sprint.

Pour chaque Sprint, nous avons présenté le backlog produit en premier temps. Ensuite nous avons présenté les différentes fonctionnalités réalisées à travers le diagramme de cas d'utilisation raffiné, avec des descriptions textuelles de quelques cas. Puis nous avons mis en disposition la conception en présentant des diagrammes de séquence objet, de séquence système et d'activité. Après, nous avons exposé quelques interfaces graphiques. Et finalement, nous avons présenté la partie test et documentation du release. Dans le chapitre suivant, nous allons présenter le deuxième release.

Bibliographie

Glossaire / Acronymes

Annexes

Résumé

Mots clés :.

Abstract

Keywords:

الملخص

الكلمات المفتاحية :