Diplôme National D'Ingénieur en Informatique

Développement d'une Fonctionnalité d'authentification double Facteur

Réalisé par :
Oussama Rajhi

Encadré par :
-Mme. *Saida Bellafi*
-M. Lukazs Kucharweski

AU: 2016/2017

Dédicace

« Soyons reconnaissants aux personnes qui nous donnent du bonheur ; elles sont les charmants jardiniers par qui nos âmes sont fleuries. » *Marcel Proust*

Ces paroles sages me font penser aux personnes chères à mon cœur et à qui je dédie ce travaille.

Mes chers parents pour leur patience illimitée, leur encouragement contenu, leur aide, et surtout pour leur profond amour.

Mes chères sœurs, pour leur grand amour et leur soutien. A ma grand-mère pour ses précieux conseils et ses continuelles prières.

A mes chers amis et à tous ceux qui m'ont aidé et soutenus de près ou de loin pour que ce projet soit possible.

Espérant qu'ils trouvent dans cette modeste dédicace l'expression de ma haute reconnaissance.

Remerciements

J'exprime ma gratitude à toutes les personnes qui m'ont aidé à accomplir ma tâche dans de bonnes conditions et qui ont su m'accorder toute l'attention nécessaire pour élaborer le présent travail.

Je tiens d'abord à remercier mes encadreurs ***M.*** **Lukasz Kucharzewski** ***et Mme. Saida Bellafi*** *pour leur aide, leurs conseils précieux, leurs critiques constructives et leurs suggestions pertinentes qui ont été remarquables tout au long de mon stage.*

Mes remerciements les plus distingués sont adressés ensuite aux membres du jury qui m'ont fait l'honneur de bien vouloir accepter d'évaluer ce travail.

Finalement, j'exprime ma sincère reconnaissance à l'égard de tous ceux qui ont contribué à ma formation.

Signature de l'encadrant de l'entreprise : M. Lukasz Kucharzewski

Signature de l'encadrant de l'école : Mme. Saida Bellafi

Résumé

Ce travail s'inscrit dans le cadre du projet de fin d'études à l'école supérieure privée d'ingénierie et de technologie « ESPRIT » pour l'obtention du Diplôme nationale d'ingénieur.

Dans ce cadre, nous avons conçu et implémenté une fonctionnalité d'authentification double facteurs au sein de la société "Ecovadis". Notre projet gère l'authentification des employés aux plateformes de test et de production en y ajoutant un module de sécurité supplémentaire.

Le projet est basé sur les nouvelles technologies, à savoir : ASP.NET, C#, MSSQL et Twilio

MOTS CLÉS : Authentification/2FA/.Net/c#/twilio/ASP.NET

Abstract

For decades, the password has been the standard means for user authentication on computers. However, as users are required to remember more, longer, and changing passwords, it is evident that a more convenient and secure solution to user authentication is necessary.

Adding a second factor to the traditional password/username could help simplify the authentication process while securing it.

This report is the result of 6 months of the work I achieved inside the ITSECURITY team of Ecovadis.

Keywords: Authentication, 2FA, .NET, Twilio, ASP.NET

Sommaire

Liste des tableaux

Liste des figures

Introduction Générale

Depuis quelques années, de plus en plus d'entreprises investissent davantage dans la sécurité de leurs systèmes d'information. En effet, l'émergence de nouvelles menaces informatiques rend toujours les entreprises exposées à des risques de perte ou de vol de données.

Afin de renforcer leurs applications beaucoup d'entreprise ont recours à une authentification à double facteur.

Ce projet de fin d'études a été réalisé au sein de la société « Ecovadis », Une entreprise Française de classement de responsabilité sociale des entreprises.

L'objectif du projet est la conception, le développement et la mise en place d'un outil d'authentification à double facteur. Cette Fonctionnalité permet de renforcer la sécurité de l'application et la gestion de l'authentification et l'autorisation.

Ce projet est réalisé dans le cadre de la préparation d'un projet de fin d'étude présenté en vue de l'obtention du diplôme national d'ingénieur en informatique l'Ecole Supérieur Privée d'Ingénierie et de Technologie.

Comment sécuriser l'accès a plusieurs plateformes de test et de production ? Comment renforcer la sécurité de l'authentification de l'autorisation ? comment garder un œil sur le processus d'authentification ?

Afin de répondre à toutes ces questions, nous devons commencer par identifier et analyser les besoins des clients en matière de veille sur la sécurité informatique. Par la suite, nous devons spécifier les principales fonctionnalités que doit accomplir notre outil. Et enfin, nous devons entamer la partie réalisation tout en gardant le contact avec les clients pour répondre au mieux à leurs attentes.

Dans ce qui suit nous décrivons la structure de ce rapport qui comporte cinq chapitres.

Chapitre 1 intitulé «Etat de l'art» présente le cadre général du projet où nous mettons le projet dans son contexte en mettant l'accent sur l'étude de l'existant, les problématiques rencontrées et la solution proposée. Par la suite on va concentrer sur les solutions existantes sur le marché (privée et publique) avec une comparaison par notre future solution.

Le deuxième chapitre « Analyse et spécification des besoins » sera consacré pour l' analyse des besoins avec une étude de l'existant pour dégager les fonctionnalités que doit fournir notre système, les besoins fonctionnels et non fonctionnels de notre outil de veille ainsi que les principaux cas d'utilisations. Le troisième chapitre « Conception » sera dédié pour présenter une partie de la conception du projet. Et à la fin de notre rapport, nous présentons dans le

quatrième chapitre la mise en œuvre de l'application en décrivant l'environnement de travail et les étapes de préparation et de développement. Dans ce chapitre également, nous testons quelques scénarios pour valider le travail et s'assurer qu'il répond aux besoins du client.

Chapitre 1 : Présentation du cadre du projet

I. Introduction

Dans le premier chapitre, nous présentons tout d'abord l'organisme d'accueil dans lequel se déroule le projet. Ensuite, nous introduisons le cadre général et la problématique.

A la fin, nous allons élaborer une brève comparaison entre des méthodologies de développement en vue de faire le meilleur choix pour notre solution.

II. Présentation de l'organisme d'accueil

1. Présentation générale

Ecovadis est une PME française engagée dans le développement de solutions sur les achats responsables, elle fournit la première plate-forme collaborative pour les entreprises afin d'évaluer la performance environnementale et sociale de leurs fournisseurs dans le monde entier.

Elle a été créée à Paris début 2007, ayant pour objectif de devenir le partenaire de confiance des organisations achat souhaitant déployer un programme Achats Responsables qui facilite l'analyse et l'échange d'indicateurs sur les risques sociaux et environnementaux des fournisseurs. Ecovadis est en pleine expansion, elle élargit de plus en plus son périmètre d'implantation qui s'étend actuellement sur la France, la Tunisie, l'ile Maurice, la Grande Bretagne, la Pologne, les EtatsUnis et récemment la Chine. Grâce à des technologies innovantes et à un centre d'expertise mutualisé sur les problématiques environnementales et sociales dans la chaîne d'approvisionnement, Ecovadis aide les directions achat à améliorer leurs performances, tout en leur permettant de diminuer les coûts associés à l'évaluation de la performance « développement durable» de leurs fournisseurs.

En effet, Ecovadis a élaboré une méthodologie d'évaluation éprouvée, compatible avec les référentiels RSE internationaux tels que le GRI, le Pacte Mondial et la nouvelle norme ISO 26000.

2. Principaux partenaires

Figure 1 : Ecovadis

Les partenaires d'Ecovadis sont des organisations non gouvernementales, des institutions publiques et des fournisseurs de services SRM. Parmi ces partenaires, nous pouvons mentionner :

Figure 2 : Principaux partenaires

ALSTOM

Alstom est une multinationale française opérant dans le monde entier dans les marchés du transport ferroviaire , active dans les domaines du transport de passagers, de la signalisation et des locomotives, avec des produits incluant les trains à grande vitesse AGV

, TGV , Eurostar et Pendolino , en plus Aux trains de banlieue, régionaux et de métro et aux tramways Citadis .

SFR

SFR est une société française de télécommunications qui offre des services professionnels de télécommunications, de télécommunications, de données et Internet aux consommateurs et aux entreprises.

RENAULT

Groupe Renault est une française multinationale constructrice automobile établie en 1899. La société produit une gamme de voitures et de camionnettes et dans le passé a fabriqué des camions, des tracteurs, des chars, des autobus / autocars et autorail Véhicules.

III. Etude de l'existant

3.1 Fonctionnement actuel

Au sein de l'entreprise, Chaque employé se connecte a l'aide d'un nom d'utilisateur et d'un mot de passe personnelles. Pour la première connexion l'administrateur ajoute un utilisateur et lui envoie un lien pour ajouter un mot de passe. Cette prcedure est reproduite selon les besoins de l'utilisateur.

La procédure d'authentification classique est peu sécurisé surtout pour des plateformes de test distribué donc on a pensé a ajouter une autre couche de sécurité qui est l'authentification a double Facteurs.

Il existe plusieurs type d'authentification renforcé a double facteurs :

Authentification forte par certificat sur support cryptographique physique

L'authentification par certificat dont le bi-clés est tiré sur le support cryptographique physique, quel que soit le facteur de forme et avec les procédures de remise en face à face, est de loin celui qui donne le plus de garanties d'authentification mais il présente la difficulté de déploiement sur une population nombreuse et périmètre géographique étendu. Par ailleurs, il demande un déploiement sur les postes (pilote de la carte à puce) et représente un investissement financier plus élevé. Il peut permettre d'être conforme au RGS si le produit de support est qualifié. Parmi les points forts, il faut noter la possibilité de réaliser les opérations

cryptographiques (dont l'authentification du système d'exploitation du poste, la signature ou le chiffrement) en mode

Authentification forte par certificat dans un magasin cryptographique non physique

Par contre, l'authentification par certificat dont le bi-clés est tiré sur le support cryptographique non physique, dans un magasin cryptographique logiciel même avec les procédures de remise en face à face, ne donne pas les mêmes garanties d'authentification et demande une étude de qualification prévue par le RGS notamment pour les certificats une étoile. Par exemple, les magasins cryptographiques de Microsoft pour les systèmes d'exploitation depuis XP ont fait l'objet d'articles dans la presse spécialisée de manière à illustrer la possibilité d'extraire les bi-clés et les certificats à l'insu de leur porteur. Des outils logiciels ont été diffusés depuis Dès lors, les mécanismes de révocation (CRL ou même OCSP) sont eux aussi mis en échec et aucune autre protection ne pourrait contribuer à empêcher l'usage de ce certificat dérobé. L'impact de cette menace est donc très élevé. Une manière de renforcer ce service d'authentification peut être de le coupler avec un élément secret séquestré en base centralisée et de rendre l'usage du certificat plus robuste, après interrogation par un client logiciel de la base en question. Mais alors, la dépendance vis-à-vis des pilotes logiciels ainsi que de la connexion vient contrebalancer le gain en sécurité.

Authentification par génération d'authentifiant à partir d'un secret partagé sur support cryptographique physique ou logiciel sur un support tiers

L'authentification par gestion d'un secret cryptographique partagé entre le porteur et la base centralisée permet de déployer l'usage d'authentification par mot de passe à usage unique, bien connue sous le nom d'OTP (pour One Time Password). Plusieurs implémentations du générateur de mot de passe sont envisageables, les unes par logiciel, d'autres par matériel offrant des capacités variables de résistance au vol. Par rapport à l'infrastructure de gestion de clés publiques, l'infrastructure de gestion de clé privées souffre de plusieurs inconvénients qui sont inhérents à la centralisation du secret : le service d'authentification dépend d'un point unique de défaillance (SPOF), qui même s'il est répliqué demande à être synchronisé de manière fine quant à la base de temps et la base des comptes. L'autre point marquant réside dans la protection de ces secrets ou des séquestres qui peut être lacunaire (attaque du serveur central ou attaque de la base de recouvrement chez le tiers de confiance doté de celle-ci). Dans les deux cas, des renforcements sont possibles mais des exemples récents ont montré que lors d'une défaillance de grande ampleur1 , la résilience est difficilement compatible avec le renforcement de la sécurité. En effet, pour permettre le second, il est courant de mettre en œuvre

des supports cryptographiques physiques effectuant la génération des mots de passe à usage unique et d'être ainsi doté des attributs de l'authentification forte. De surcroit, il s'agit bien dans ce cas de l'authentification du porteur du token, qui doit par ailleurs connaître le code pin. Mais, en cas de compromission massive, la gestion de ceux-ci demande le retour en usine pour un changement des secrets embarqués – ce qui est coûteux en temps, en moyen, en personne – et la résilience est ainsi mise en doute. Parmi les méthodes récemment apparues au titre de l'authentification renforcée, la possibilité de disposer de logiciels OTP embarqués sur des supports mobiles pourrait permettre de pallier tous ces inconvénients et permettrait de demeurer dans le groupe de l'authentification forte au regard des trois critères (ce que je sais, ce que je possède, ce que de connais), bien que la sécurité d'un support mobile ait été mise en cause à de multiples reprises ces dernières années. Reste pourtant la difficulté d'unifier une flotte de mobiles pour une population nombreuse. Cet aspect, qui relève d'un autre volet de la gestion du système d'information, n'est pas encore optimisé d'un point de vue technique et économique. Si le support mobile est d'une origine externe au périmètre du système d'information professionnel, la maîtrise est encore moins assurée. D'autres technologies émergentes relevant du secret partagé sont apparues récemment et offre un traitement différentié de ces désagréments. Toutefois, le niveau de sécurité en est amoindri. Elles sont décrites ci-après

3.2 Critique de l'existant

Le processus actuel est inadéquat et incompatible avec la certification ISO 27001 pour plusieurs raisons :

- Risque d'attaque brute force : un hacker peut attaquer l'application en utilisant un dictionnaire de mot de passe et avoir accès a toutes les plateformes de test.
- Risque de phishing : un utilisateur malicieux peut avoir accès en envoyant un lien a un utilisateur interne.

Ainsi le processus semble dépassé d'un point d vue sécuritaire et présente plusieurs vulnérabilités et autant d'opportunité pour un utilisateur malicieux.

3.3 Présentation du travail demandé

Dans un souci de concevoir une application aussi sécurisée que possible et de pour se conformer aux normes de la certification ISO 27001. Nous avons conçu une extension au système d'authentification existant. Le travail réalisé se résume dans les fonctionnalités suivantes :

- Demander un code supplémentaire lors de l'authentification.

- Resilier l'accès après une période déterminé ou par l'interface d'administration.
- Visualiser les statistiques d'utilisation dans le backend.
- Choisir la méthode de réception des codes pour l'utilisateur

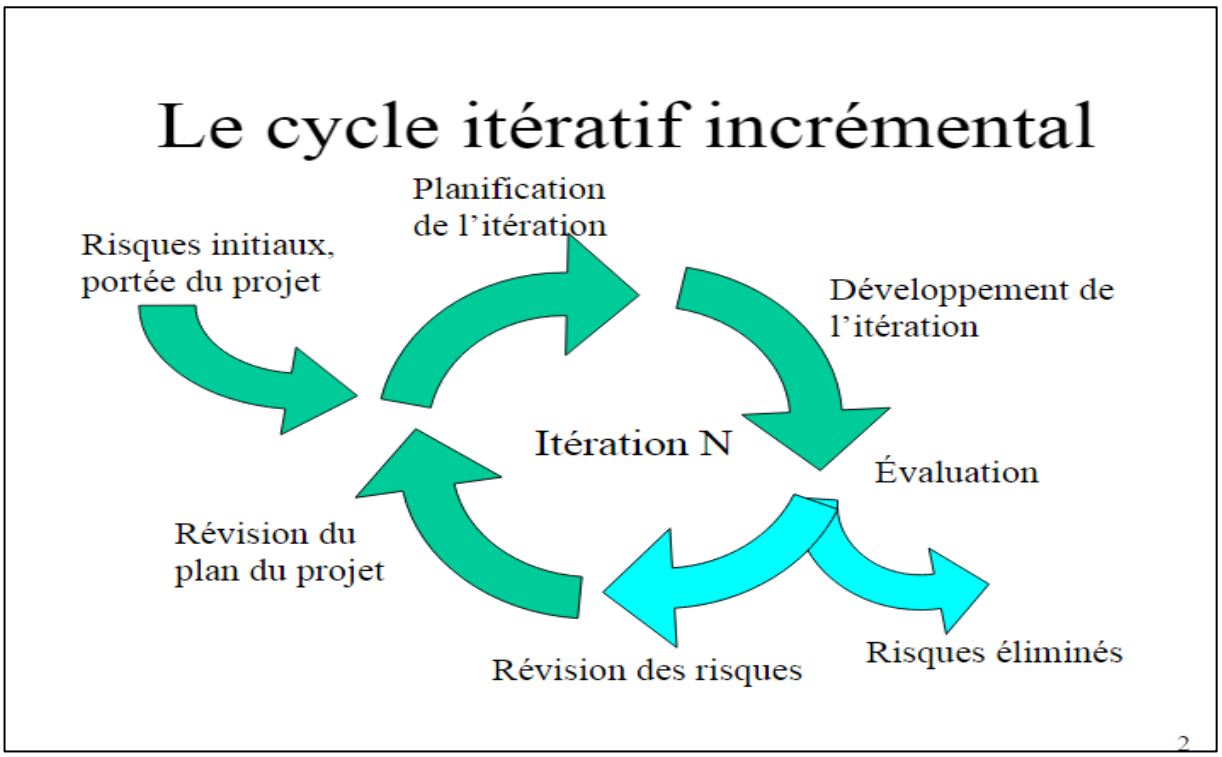
IV. Méthodologie adoptée

Pour l'analyse et la conception de notre application on optera pour la méthode **du Processus Unifié** (UP pour Unifie Process), qui est un processus de développement itératif et incrémental.

On a opté pour cette démarche parce qu'elle s'appuie essentiellement sur la modélisation UML pour la description de l'architecture (fonctionnelle, logicielle et physique) et la mise au point de cas d'utilisation qui permettent de décrire les besoins et exigences des utilisateurs.

Le projet est découpé en itérations qui permettent de mieux suivre l'avancement globale. A la fin de chaque itération une partie exécutable du système finale est produite, de façon incrémentale (par ajout)

Le schéma ci-dessous (Figure 7) représente les phases d'un processus unifié :



- **Figure 1 : Les phases d'un processus unifié**

Expression des besoins :

Cette étape nous permet de :

- Comprendre les besoins principaux et obtenir l'ensemble de ses fonctions,
- Evaluer les besoins fonctionnels (du point de vue de l'utilisateur) qui conduisent par la suite à la réalisation des modèles de cas d'utilisation,
- Prendre en compte l'ensemble des besoins non fonctionnels et livrer une liste des exigences techniques.

☞ **Analyse :**

Il s'agit d'analyse et de comprendre les besoins et les exigences du client afin de choisir la conception de la solution. On livre une spécification complète des besoins issus des cas d'utilisation sous une forme plus compréhensible par le client (via l'élaboration de scénarios) pour enfin pourvoir bien maintenir notre futur système.

☞ **Conception :**

Il s'agit de concevoir l'ensemble de composants de l'application en utilisant le langage de modélisation UML.

☞ **Implémentation :**

C'est le fait d'implémenter le système sous formes de (code source, scripts.).

Les objectifs fondamentaux de l'implémentation sont de planifier les intégrations des composants pour chaque itération, et de produire les classes sous formes de codes sources.

☞ **Test :**

Les tests permettent de vérifier des résultats de l'implémentation.

Pour conclure, il faut savoir que pour mener efficacement un tel cycle, on doit avoir besoin d'un :

- Modèle de cas d'utilisation.
- Modèle d'analyse : détailler les cas d'utilisation.
- Modèle de conception : finissant la structure statique du système sous forme de sous-systèmes, de classes et interfaces.
- Modèle d'implémentation : présentant les composants en code source.
- Modèle de déploiement : définissant l'architecture de déploiement adopté.
- Un modèle de test.

Conclusion :

Dans ce chapitre, on a mis le projet dans son contexte. On a précisé également la méthodologie qu'on va adopter afin de bien mener le déroulement de ce projet.

Dans le chapitre suivant, on va spécifier et analyser les besoins et les fonctionnalités du système a développer.

Chapitre 2 : Spécification des besoins

Introduction :

La spécification des besoins sert essentiellement à identifier l'ensemble des acteurs du système et leur associer chacun l'ensemble d'actions avec lesquelles ils pourront intervenir dans l'objectif de donner un résultat optimal et satisfaisant au client.

On va commencer en premier lieu par une spécification des besoins auxquels doit répondre l'application, passant ensuite à l'analyse de ces besoins à travers l'introduction des acteurs et les diagrammes des cas d'utilisations relatifs à ces acteurs.

I.Etude des besoins

Cette étape consiste à comprendre le contexte du système, Il s'agit de déterminer les fonctionnalités et les acteurs et d'identifier les cas d'utilisation initiaux.

- Besoins fonctionnels : doivent être réalisés à la fin de la phase de développement (cas d'utilisation, scénarios).
- Besoins non fonctionnels : performance, etc.

Nous présentons dans ce qui suit tous les besoins fonctionnels classés par acteur ainsi que les besoins non fonctionnels communs à tous ces acteurs.

I.1 Besoins Fonctionnels

Le système doit permettre de :

- S'authentifier avec un code valable une seule fois.
- Choisir comment recevoir le code de sécurité.
- Activer et désactiver l'authentification à double facteurs par l'administrateur.
- Visualiser les statistiques d'utilisations.

I.2 Besoins non Fonctionnels

Il s'agit des besoins qui caractérisent le système. Ces derniers représentent les exigences implicites auquel le système doit répondre. Parmi ces besoins on cite :

- L'utilisabilité : les interfaces doivent être simples et claires. Elles ne doivent pas être trop complexes pour gagner du temps lors de l'utilisation du système.

- La sécurité : pour pouvoir accéder aux interfaces du système chaque utilisateur doit saisir son login et son mot de passe.

- La cohérence : le système doit être capable de maintenir une cohérence entre les différentes informations qui le composent.

- La maintenabilité : le code source du système doit être clair et commenté afin de faciliter la maintenance et la modification.

II. Identifications des acteurs et des cas d'utilisations

Les acteurs sont des entités externes qui interagissent avec le système et ils sont décrits par leur rôle. Ce rôle définit les besoins et les capacités de l'acteur vis-à-vis au système. Les acteurs en interaction avec notre système sont :

Administrateur : L'acteur qui a le plus de permissions dans le système il active/désactive l'authentification à double facteur, choisi la méthode pour délivrer le code et visualise les statistiques d'utilisation.

Utilisateur (Tous les utilisateurs interne de EcoVadis) : ils reçoivent un code pour s'identifier et peuvent changer comment est délivré le code.

II.1 Diagramme de cas d'utilisation initiale

Les cas d'utilisation sont une technique de description du système étudié privilégiant le point de vue de l'utilisateur. Les cas d'utilisation décrivent, sous la forme d'actions, le comportement d'un système du point de vue d'un utilisateur. Ils servent à structurer les besoins des utilisateurs et les objectifs correspondants du système . Le diagramme de la figure suivante présente les principales fonctionnalités offertes par l'application pour les acteurs.

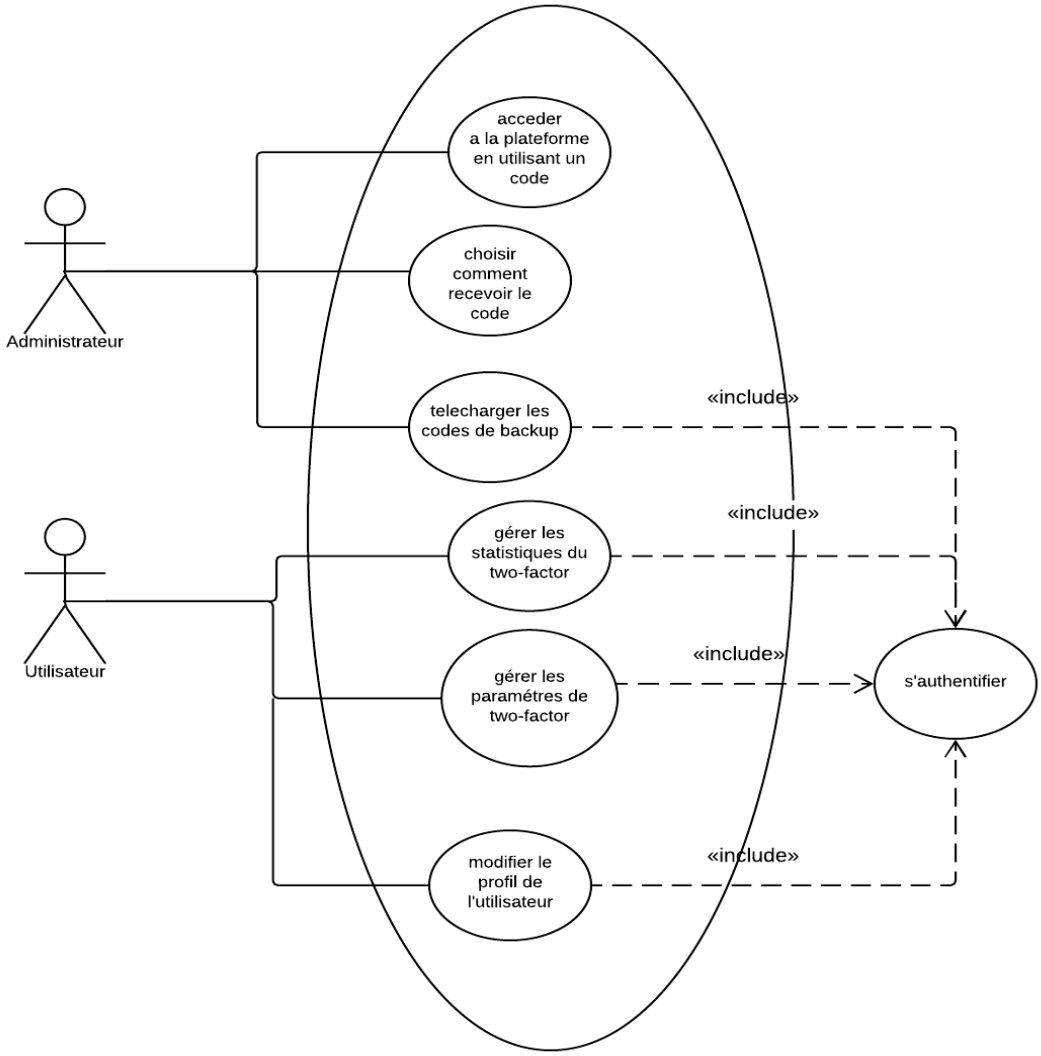


Figure 2 Diagramme de cas d'utilisation initiale

II.2 Raffinement des cas d'utilisations

A partir du diagramme des cas d'utilisation et de l'identification des besoins et des acteurs, nous avons élaboré une vision générale des cas d'utilisation métiers du futur système. Ensuite, nous raffinerons les cas d'utilisation prioritaires puisque nous allons passer à une phase d'analyse qui correspond à une vision informatique du système.

Cas d'utilisation UC-2FA-0001 : Authentification avec un code double Facteur

Acteur principale	Utilisateur EcoVadis
Autre Acteur	System
Cas d'utilisation	S'authentifier au système a l'aide d'un code second facteur
Préconditions	● L'utilisateur existe dans le système. ● L'authentification double facteur est configuré. ● Le numéro de téléphone de l'utilisateur existe dans le système
Postcondition	Utilisateur authentifié dans le système
Déclencheur	Action Utilisateur
Scenario Principal	1. L'utilisateur accède au Backoffice 2. Le système demande un nom d'utilisateur et un mot de passe 3. L'utilisateur entre un nom d'utilisateur et un mot de passe valide 4. Le système demande un code unique a l'utilisateur et lui envoie un sms contenant le code 5. L'utilisateur introduit le code et valise 6. Si le code est valide l'utilisateur est redirigé vers la page d'accueil
Scenario alternatif	6a.Si le code est erroné l(utilisateur est redirigé vers cas d'utilisation 2 : utilisilateur introduit un code erroné
Règles Métiers	● Chaque intervalle préconfiguré l'utilisateur doit introduire le code de nouveau. ● L'intervalle peut être change par l'administrateur ● L'authentification double facteur pourrait être activer/désactiver par l'administrateur ● Le système peut envoyer 1000 sms par mois

Tableau 1 Cas d'utilisation UC-2FA-0001 : Authentification avec un code double Facteur

Cas d'utilisation UC-2FA-0002: Utilisateur intrduit un code invalide

Utilisateur Principale	Utilisateur Ecovadis
Niveau Utilisateur	Utilisateur Normale
Autre Acteur	Système
Contexte	Si un utilisateur introduit un code invalide il doit être averti.
Preconditions	• L'utilisateur existe dans le système • L'authentification double facteur est configuré • Un numéro de téléphone est configuré dans le système.
PostCondition	Un message d'erreur est affiché
Succés	L'utilisateur est averti que le code introduit est erroné.
Déclencheur	Action Utilisateur
Scénario principal	1. Dans la 5eme etape du cas d'utilisation UC-2FA-0001 : Authentification avec un code double Facteur l'utilisateur introduit un code invalide 2. Le système affiche le message: ***Invalid code. Please try again.***
Règle Metiers	• Dans le cas ou un utilisateur introduit un code invalide l'utilisateur doit être averti par un message explicite

Tableau 2 Cas d'utilisation UC-2FA-0002: Utilisateur intrduit un code invalide

Cas d'utilisation UC-2FA-0003: Gérer les options de l'authentification double facteur

Acteur Principale	Administrateur
Autre Acteur	Système
Stakeholders & Interests	Administrateur, Utilisateur
Contexte	L'administrateur Système doit gérer les paramètres de l'authentification double système.
Préconditions	● L'utilisateur existe dans le système
Postcondition	L'administrateur change les paramètres de la fonctionnalité authentification double facteur y compris l'activer/desactiver
Déclencheur	Action Utilisateur
Scenario de succès	1. L'administrateur s'authentifie au Backoffice. 2. L'administrateur se dirige vers General/User Role/Two Factor 3. Le système affiche une liste d'utilisateurs. 4. L'administrateur sélectionne un ou plusieurs utilisateurs. 5. L'administrateur active/désactive l'option double facteurs et enregistre les modifications. 6. En cas d'activation le système envoie une liste de code de backup aux utilisateurs
Règles Metiers	● Le changement prend effet immédiatement ● L'accès aux paramètres est réservé aux utilisateurs avec le rôle administrateur ● L'onglet doit être cache aux utilisateurs n'ayant pas le rôle administrateur

Tableau 3 Cas d'utilisation UC-2FA-0003: Gérer les options de l'authentification double facteur

Cas d'utilisation UC-2FA-0004: Le numéro du téléphone de l(utilisateur n'est pas dans la base de donnée.

Acteur principal	Système
Niveau d'objectif	Niveau d'objectif de l'utilisateur
Autres acteurs	Administrateur
Les intervenants et les intérêts	Administrateur, l'utilisateur EcoVadis
objectif primordial	• Le système Administrateur doit etre capable de gérer la configuration de l'authentification à 2 facteurs sur demande. • Le système Administrateur doit recevoir une alerte quand l'un des utilisateurs n'a pas configuré son numéro de téléphone.
Conditions préalables	• L'utilisateur existe dans le système. • Quelques utilisateurs n'ont pas configuré leurs numéros de téléphone.mobile.
Garantie de succès	Chaque fois qu'un ou plusieurs utilisateurs dont administrateur permet l'authentification à 2 facteurs, n'ont pas leur numéro de téléphone mobile configuré, le système informe l'administrateur.
Déclencheur	Action de l'utilisateur
Le scénario de succès principal	1. Dans la 5e étape de l'histoire de l'utilisateur UC-2FA-0003 : scénario de la gestion des options de l'authentification à 2 facteurs, administrateur essaie d'activer l'authentification à 2 facteurs pour les utilisateurs ne disposant pas de numéro de téléphone mobile configuré. 2. le Système affiche un message d'avertissement de popup pour informer l'administrateur : ***certains utilisateurs i.e. username1, username2, username3, n'ont pas leurs numéros de téléphone mobile configurés. Souhaitez-vous continuer?*** avec options, oui, enregistrer les utilisateurs avec des numéros mobiles, annuler.
Extensions	
Les règles opérationnelles	• Si les utilisateurs pour lesquels l'administrateur permet l'authentification à 2 facteurs, n'ont pas leurs numéros de téléphone mobile configurés, le système informe l'administrateur. • Choisir **Oui** pour enregistrer toutes les modifications – active les 2-facteurs pour tout le monde quelle que soit la configuration du numéros mobile. • Choisir **Enregistrer les utilisateurs avec les numéros mobiles** pour activer 2-facteur uniquement pour les utilisateurs avec le numéro de téléphone mobile configuré . • Choisir **annuler** pour revenir à la configuration des 2-facteurs.

Tableau 4 Cas d'utilisation UC-2FA-0004: Le numéro du téléphone de l(utilisateur n'est pas dans la base de donnée.

Cas d'utilisation UC-2FA-0005: Choix du méthode du livraison du code.

Acteur principal	L'Utilisateur d'EcoVadis
Niveau d'objectif	Niveau d'objectif de l'utilisateur
Autres acteurs	Le système
Les intervenants et les intérêts	L'utilisateur d'EcoVadis
objectif primordial	Permettre aux utilisateurs de choisir la méthode de livraison d'OTP qui leur convient.
Conditions préalables	● L'utilisateur existe dans le système. ● L'utilisateur a l'autehentification à 2-facteurs configurée. ● L'utilisateur a son numéro de téléphone mobile configuré..
Minimal Guarantee	
Garantie de succès	l'utilisateur peut choisir l'une des options de livraison d'OTP.
Déclencheur	Action de l'utilisateur
Le scénario de succès principal	1. Dans la 5eme étape du scenario de l'histoire de l'utilisateur UC-2FA-0001: la connexion de l'utilisateur avec l'authetification à 2 facteurs,l'utilisateur choisit de recevoir l'OTP via application authentification de google. 2. Retour à la 5eme étape du scenario de l'histoire de l'utilisateur UC-2FA-0001: la connexion de l'utilisateur avec l'authetification à 2 facteurs.
Extensions	1. Dans la 5eme étape du scenario de l'histoire de l'utilisateur UC-2FA-0001: la connexion de l'utilisateur avec l'authetification à 2 facteurs,l'utilisateur choisit d'introduire un code de secours. 2. Retours à la 5 eme étape du scenario de l'histoire de l'utilisateur UC-2FA-0001: la connexion de l'utilisateur avec l'authetification à 2 facteurs.
Les règles opérationnelles	● Le code de secours ne peut etre utilisé qu'une seule fois. ● Quand un code est utilisé il devient inactive. ● pour obetenir de nouveaux codes de secours,l'utilisateur doit aller à sa page de profil et générer de nouveaux codes. Voir le récit utilisateur UC-2FA-0008 : Générer des codes de sauvegarde.

Tableau 5 Cas d'utilisation UC-2FA-0005: Choix du méthode du livraison du code.

Cas d'utilisation UC-2FA-0006: No mobile number configured for the given user

Acteur principal	Système
Niveau d'objectif	Niveau d'objectif de l'utilisateur
Autres acteurs	L'utilisateur d'EcoVadis
Les intervenants et les intérêts	l'utilisateur d'EcoVadis
objectif primordial	Si aucun numéro de téléphone mobile est fourni dans le profil de l'utilisateur, alors l'utilisateur doit être averti que le mot de passe d'application ne peut pas être envoyé par SMS.
Conditions préalables	● L'utilisateur existe dans le système. ● L'utilisateur a l'autehentification à 2-facteurs configurée. ● L'utilisateur n'a pas son numéro de téléphone mobile configuré..
Minimal Guarantee	
Garantie de succès	l'utilisateur est informé qu'il n'y a aucun numéro de téléphone mobile fourni dans son profil utilisateur.
Déclencheur	Action de l'utilisateur.
Le scénario de succès principal	1. Dans la 4eme étape du scenario de l'histoire de l'utilisateur UC-2FA-0001: la connexion de l'utilisateur avec l'authetification à 2 facteurs,l'utilisateur, le système vérifie que l'utilisateur n'a aucun numéro de téléphone mobile fourni dans son profil. **2.** Le système affiche un message d'erreur : **le *numéro de téléphone Mobile n'a pas été configuré dans votre profil utilisateur. Veuillez essayer une autre méthode de livraison du mot de passe d'application*.** 3. Le système reste dans le message pop-up et permet à utilisateur de choisir une autre méthode de livraison des OTP.
Extensions	
Les règles opérationnelles	● i un utilisateur n'a pas un numéro de téléphone mobile, sous réserve, le système est obligé d'afficher un message d'erreur. ● Texte du message d'erreur : ***le numéro de téléphone Mobile n'a pas été configuré dans votre profil utilisateur. Veuillez essayer une autre méthode de livraison du mot de passe d'application.***

Tableau 6 Cas d'utilisation UC-2FA-0006: No mobile number configured for the given user

Cas d'utilisation UC-2FA-0007: l'utilisateur entre un code erroné plusieurs fois de suite.

Acteur principal	Système
Niveau d'objectif	Niveau d'objectif de l'utilisateur
Autres acteurs	L'utilisateur d'EcoVadis
Les intervenants et les intérêts	L'utilisateur d'EcoVadis
objectif primordial	Si l'utilisateur essaie de se connecter et échoue plusieurs fois d'affilée (5 fois), puis son compte est désactivé.
Conditions préalables	● L'utilisateur existe dans le système. ● L'utilisateur a l'autehentification à 2-facteurs configurée.
Garantie de succès	L'utilisateur est informé que le compte a été désactivé en raison du nombre élevé de tentatives de connexion incorrecte.
Déclencheur	Action de l'utilisateur.
Le scénario de succès principal	1. In 6th dans la 6eme étape de l'histoire de l'utilisateur UC-2FA-0001: la connexion de l'utilisateur avec l'authetification à 2 facteurs l'utilisateur essaye plusieurs fois d'ouvrir une session mais fournit un mot de passe d'application incorrecte (5 fois de suite). ***2.*** Le système affiche un message d'erreur : ***votre compte a été désactivé en raison du nombre élevé de tentatives de connexion incorrectes. Veuillez contacter un administrateur.*** 3. Système de désactivé le compte.
Extensions	
Les règles opérationnelles	● Nombre de tentatives de login incorrectes subséquentes autorisées : 4 ● Après la 5eme tentative de connexion incorrecte le compte est désactivé et l'utilisateur est informé par rapport à la situation et aux actions possibles pour annuler la désactivation.

Tableau 7 Cas d'utilisation UC-2FA-0007: l'utilisateur entre un code erroné plusieurs fois de suite.

Cas d'utilisation UC-2FA-0008: Téléchargement des codes de backup

Acteur principal	L'utilisateur d'EcoVadis
Niveau d'objectif	Niveau d'objectif de l'utilisateur
Autres acteurs	Système
Les intervenants et les intérêts	L'utilisateur d'EcoVadis
objectif primordial	Tout utilisateur pouvant accéder à BackOffice devrait être en mesure de télécharger ses codes de secours ou les envoyer par mail.
Conditions préalables	• L'utilisateur existe dans le système. • L'utilisateur a l'autehentification à 2-facteurs configurée.
Garantie de succès	L'utilisateur télécharge le fichier ou envoye à lui meme un mail avec les cods de secours.
Déclencheur	Action de l'utilisateur.
Le scénario de succès principal	1. L'utilisateur se connecte au BackOffice. 2. L'Utilisateur clique sur le lien du profil à modifié , i.e. 3. L'utilisateur séléctionne éditer de l'authentification à 2-facteurs. 4. Dans la fenêtre pop-up, l'utilisateur sélectionne onglet code de secours. 5. L'utilisateur clique sur télécharger les codes de secours 6. Le système appelle le téléchargement du fichier de codes de secours.
Extensions	5a. Utilisateur clique sur envoyer par mail. 6a. e système envoie un mail contenant le fichier de codes de secours, à l'adresse de messagerie configuré dans le profil de l'utilisateur.
Les règles opérationnelles	• L'utilisateur doit être ecapable de télécharger le fichier contenant les codes de secours de sa page de profil • L'utilisateur doit être capable d'envoyer des codes de secours à l'adresse de messagerie configuré dans son profil.

Tableau 8 Cas d'utilisation UC-2FA-0008: Téléchargement des codes de backup

Cas d'utilisation UC-2FA-0009: Générer les codes de backup

Acteur principal	L'utilisateur d'EcoVadis
Niveau d'objectif	Niveau d'objectif de l'utilisateur
Autres acteurs	Système
Les intervenants et les intérêts	L'utilisateur d'EcoVadis
objectif primordial	Tout utilisateur pouvant accéder BackOffice devrait être capable de générer de nouveaux codes de secours.
Conditions préalables	• L'utilisateur existe dans le système. • L'utilisateur a l'authentification à 2-facteurs configurée.
Garantie de succès	Nouveaux codes de secours sont crées.
Déclencheur	Action de l'utilisateur.
Le scénario de succès principal	1. L'utilisateur se connecte au BackOffice. 2. L'Utilisateur clique sur le lien du profil 3. L'utilisateur séléctionne éditer de l'authentification à 2-facteurs. 4. Dans la fenêtre pop-up, l'utilisateur sélectionne onglet code de secours. 5. L'utilisateur clique sur génèrer nouveaux codes de secours.. 6. Le système génère une nouvelle liste de codes de secours.
Extensions	
Les règles opérationnelles	

Tableau 9 Cas d'utilisation UC-2FA-0009: Générer les codes de backup

Cas d'utilisation UC-2FA-0010: Accéder aux statistiques

Acteur principal	Administrator
Niveau d'objectif	Niveau d'objectif de l'utilisateur
Autres acteurs	Système
Les intervenants et les intérêts	L'utilisateur d'EcoVadis
objectif primordial	L'administrateur doit etre capable de verifier les statistiques de l'utilisation de l'authentification à 2-facteurs.
Conditions préalables	L'un des utilisateurs a déja utilisé l'authetification à 2-facteurs.
Garantie de succès	L'administrateur est capable de verifier les statistiques de l'utilisation de l'authentification à 2-facteurs.
Déclencheur	Action de l'utilisateur.
Le scénario de succès principal	1. L'administrateur se connecte à BackOffice. 2. Administrateu sélectionne Général-> rôles/ utilisateur-> onglet double facteurs 3. le système affiche une liste d'utilisateurs. 4. L'administrateur clique sur le sous-menu statistiques de l'authentification à 2-facteurs. 5. Le système présente des statistiques des messages envoyés et non envoyés de l'OTP.
Extensions	6. Administrateur clique sur le lien des connexions détaillés.. 7. Système utilise un filtre pour le nom d'utilisateur et le type de connexion. 8. Administrateur de recherche par le nom d'utilisateur et/ou le type de connexion. 9. le système renvoie des informations filtrés.
Les règles opérationnelles	• Statistiques disponibles dans le module: • Un diagramme pour la somme des SMS envoyés et des SMS échoués. • Un diagramme pour l'accés mensuel de la plateforme de l'authentification à 2-facteurs. • Les connexions détaillés par utilisateur, contenant la date de chaque sms envoyé au téléphone de portable de l'utilisateur, date de chaque accès à la plate-forme via l'authentification à 2 facteurs • Statistiques concernant le pourcentage d'utilisateurs avec l'authentification à 2-facteurs active. également • L'accés à l'authentification à 2-facteurs n'est disponible qu'en mode administrateur. • L'onglet 2 facteurs doit être masqué pour tous les rôles qui ne sont pas autorisés à l'utiliser

Tableau 10 Cas d'utilisation UC-2FA-0010: Accéder aux statistiques

III. Diagrammes de séquences

Après avoir décrit les cas d'utilisation, nous présentons les diagrammes de séquences, Ces diagrammes permettent de représenter graphiquement la chronologie des interactions entre les acteurs et le système vu comme une boîte noire, dans le cadre du scénario nominal.

Le schéma ci-dessous représente le diagramme de séquence du cas d'utilisation « inscription d'un simple utilisateur »

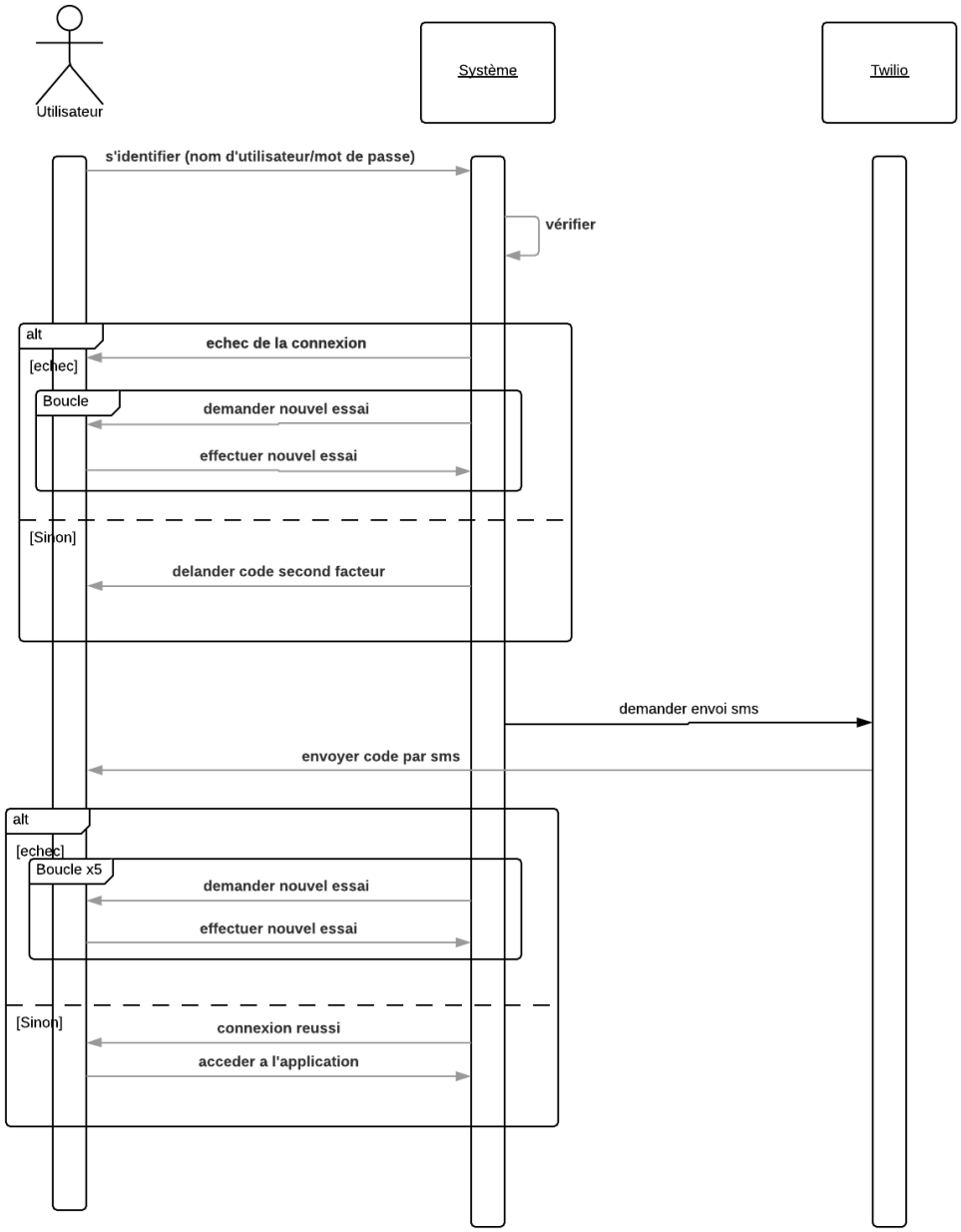


Figure 3 Diagramme de séquence globale

Conclusion

On est parvenu à travers ce chapitre de spécifier les besoins du système, et cela, en déterminant les différents acteurs principales du système et en déterminant leur différents rôles à traves la réalisation d'un ensemble de diagrammes de cas d’utilisations et de séquences qui nous permettront dans le chapitre suivant de bien concevoir notre future application.

Chapitre 3 : Conception

Introduction

La conception d'une application est une partie très importante du processus de développement web afin de mettre en œuvre l'application avant son implémentation.

Nous avons consacré ce chapitre à la modélisation de notre système en utilisant la méthode de conception UML, en définissant tout d'abord l'architecture de notre application, en élaborant ensuite le diagramme de classe.

I. Architecture de l'application

Dans les phases préliminaires du développement d'une application ou de la refonte d'un système d'information, la définition de l'architecture technique consiste à faire les choix de technologies et d'organisation de composants logiciels les plus adaptés aux besoins et aux contraintes de l'organisation d'accueil. Ces choix sont ensuite relayés au sein de notre projet, guidant la conception et permettant la transformation d'un modèle fonctionnel en application performante et robuste.

La figure ci-dessous représente l'architecture utilisée :

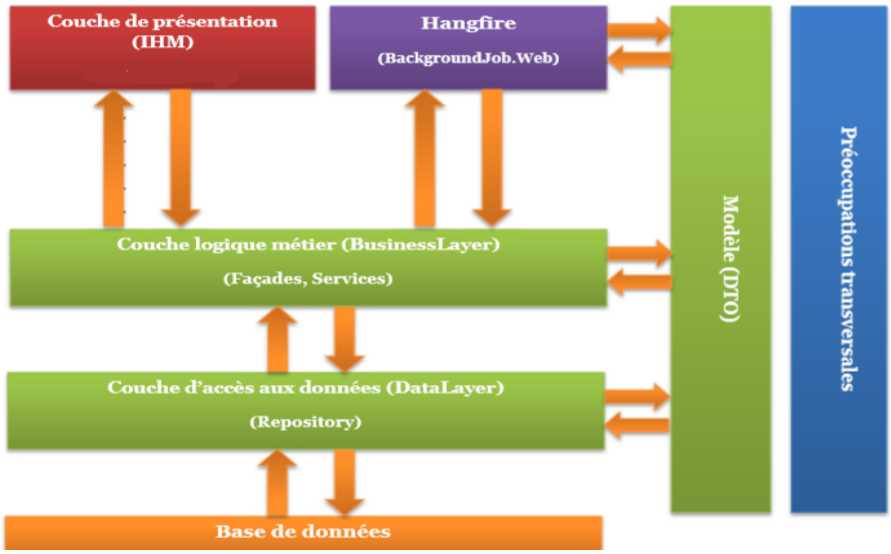


Figure 4 Architecture Logique

En effet, le développement en couche adopté est très intéressant dans la communication entre les couches et aussi dans le découpage net et précis des étapes de développement de l'application. Ainsi, nous allons développer chacune d'entre elle proprement selon le modèle multicouche.

II. Diagramme de classe d'analyse

Dans cette partie, on va représenter une perspective de l'application à travers une modélisation statique de notre système en utilisant un diagramme de classes.

Commençons tout d'abord par une description de chaque classe :

Classes	Description
User	C'est la classe de base de notre système. Un Utilisateur : • s'authentifie au système • possede plusieurs code
UserFailedTwoFActor	C'est une autre classe de base de notre Système contenant les données de l'utilisateur dont le processus d'authentification a echoué
BackupCode	C'est une classe contenant un groupement Des code secours.
Code	Contient toutes le code de l'authentification
TwoFactorLog	C'est une classe qui contient les logs de la fonctionnalité.

Le diagramme de classes représente les classes constituant le système et les associations entre elles. Les diagrammes de classes expriment de manière générale la structure statique d'un système, en termes de classe et de relations entre ces classes. De même qu'une classe décrit un ensemble d'objets, une association décrit un ensemble de liens ; les objets sont des instances de classes et les liens sont des instances de relations.

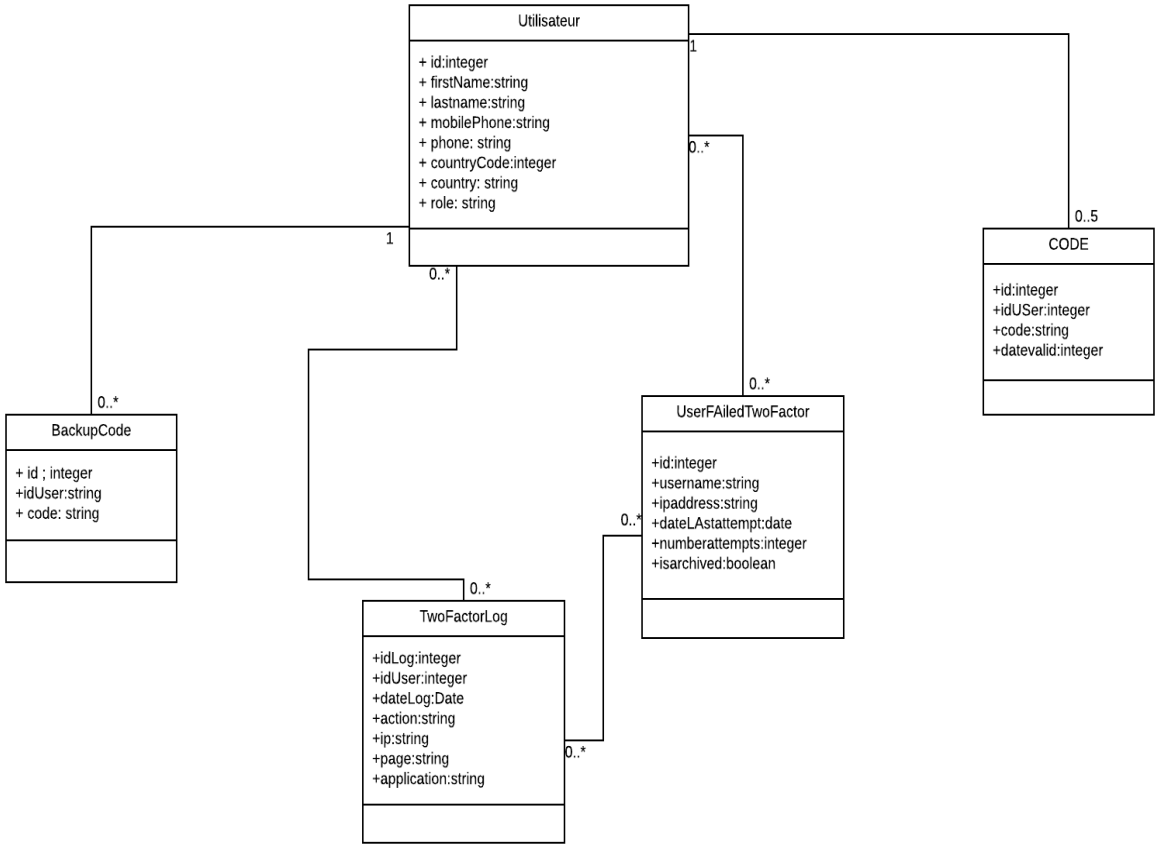


Figure 5 Diagramme de classe d'analyse

III. Diagramme d’activité relatif a l’authentification

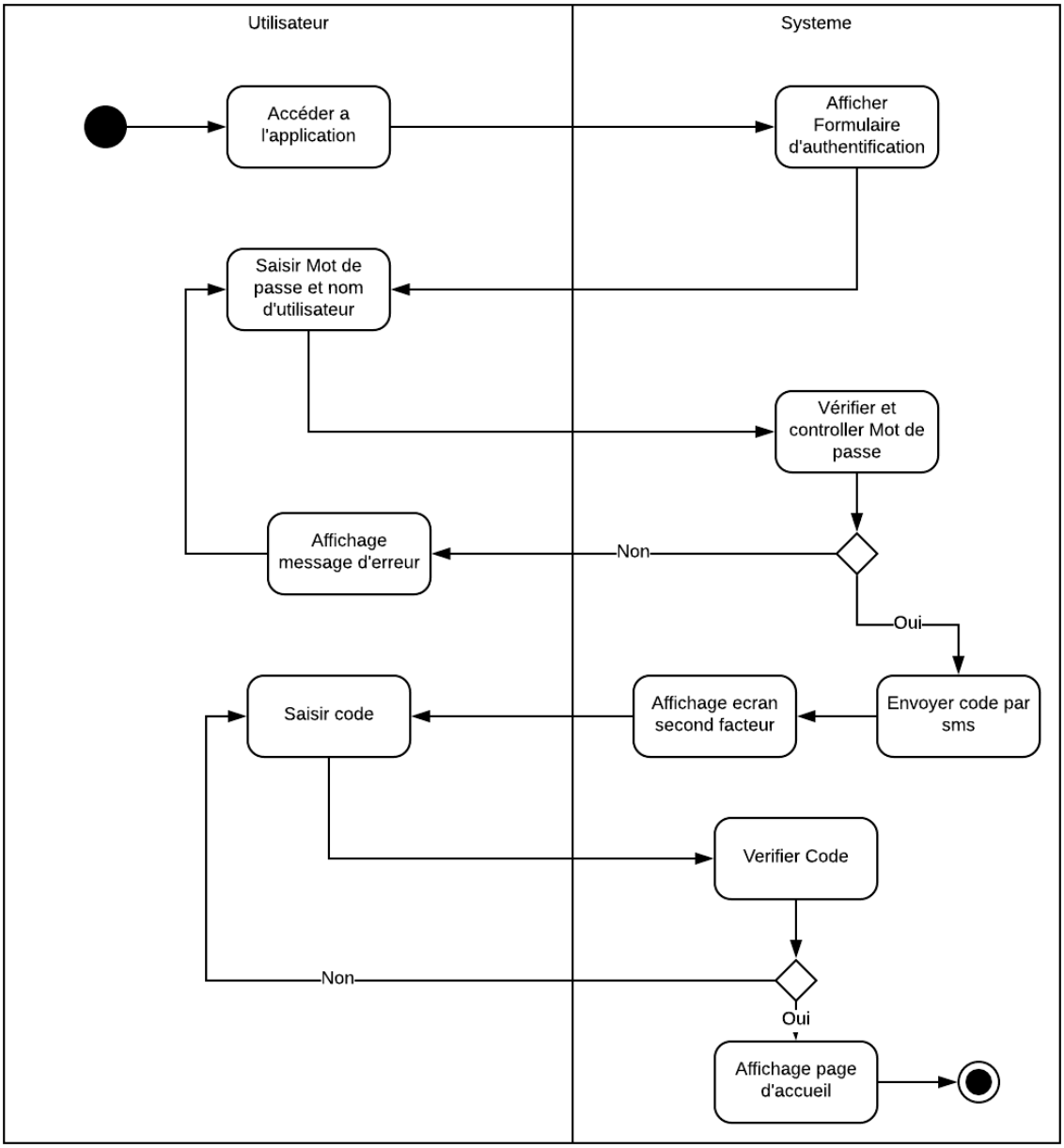


Figure 6: Diagramme d'activité relatif a l’authentification

Cette figure représente le diagramme d’activités relatif à l’authentification. Comme nous avons expliqué, après avoir rempli le formulaire d’authentification, le système vérifie si les paramètres introduits correspondent à un utilisateur dans la base de données puis vérifie le code d’authentification double facteur.

Conclusion

Dans ce chapitre, on a commencé par présenter l'architecture logicielle de l'application. Ensuite, on a présenté le diagramme de classes entités de notre application et on a décrit les différentes relations entre eux.

Par la suite, on a expliqué à travers des diagrammes d'activités et de séquences quelques cas d'utilisations de notre plateforme. Le prochain chapitre présentera la partie réalisation de notre Fonctionnalité.

Chapitre 4 : Réalisation et Test

Introduction

Dans ce dernier chapitre on présente la partie réalisation de notre plateforme. On commence par présenter l'environnement de travail et les outils utilisés. On présente ensuite les principales fonctionnalités implémentées tout au long de ce travail.

La dernière partie de ce chapitre sera consacrée pour les tests du bon fonctionnement de notre solution ainsi que son hébergement.

I. Environnement de travail

L'environnement de travail est constitué des deux parties nommées environnement matériel et environnement logiciel.

I.1 L'environnement matériel

Le développement de ce projet a été réalisé sur un PC ayant les caractéristiques suivantes :

- Modèle : HP
- Processeur : Intel Core i7 CPU M 380 @ 2.50GHz 2.50 GHz
- Mémoire : 8 Go
- Disque dur : 500 Go SSD

I.2 L'environnement logiciel

Nous avons énuméré au cours de cette partie les différents outils utilisés tout au long de ce projet pour l'étude et la mise en place de notre application.

a. Système d'exploitation

Nous avons utilisé comme système d'exploitation Microsoft Windows 8 Edition Professionnel Premium.

b. Outils de développement

- **LucidChart :**

Nous avons exploité pour la modélisation UML de notre application la plateforme Cloud LucidChart. Nous l'avons utilisé pour réaliser les diagrammes de cas d'utilisation et les diagrammes de séquences.

- **Visual Studio 2017 :**

Microsoft Visual Studio est une collection des logiciels de développement pour Windows, conçue par Microsoft. Visual Studio est un ensemble complet d'outils de développement permettant de construire des applications principalement utilisant les technologies .NET entre autres : WinForm, WPF (des applications bureautiques), Web ASP.NET, Windows Phone, des Services Web XML WCF ou ASMX. Visual Basic, Visual C++, Visual C# et Visual J# utilisent tous le même environnement de développement intégré qui leur permet de partager des outils et facilite la création de solutions interopérable avec plusieurs langages.

Ainsi, nous avons choisis Microsoft Visual Studio comme l'environnement de développement intégré, les raisons de cette version se présentent d'une part, par de nouvelles fonctionnalités pour le Web ayant une assistance totale pour les nouvelles règles sur HTML5, CSS3, JavaScript, ainsi que les nouvelles avancées pour l'ASP.NET. D'autre part, l'intégration des outils de gestion du cycle de vie des applications et de modélisation de quelques diagrammes UML. Le débogage est plus facile pendant les tests et la maintenance. Il intègre directement les outils de mises en œuvre des services web, donc pas besoin des applications tiercesSQL Server Management Studio : C'est un logiciel utilisé pour configurer, gérer et administrer toutes les fonctionalités de Microsoft SQL server.

- **IIS express** : c 'est un serveur Web intégré à Visual studio.
- **Chrome Developer Tools** :

Le Google Chrome Developer Tools, nous l'avons utilisé pour déboguer le code JQuery à l'aide du débogueur graphique et les points d'arrêts. C'est un outil le mieux adapté pour déboguer le code JQuery.

Google Chrome Developer Tools est un environnement intégré pour le débogage,

l'optimisation et la compréhension d'une application Web, exécuté depuis le navigateur Google Chrome. Les outils de développement sont développés en partie par le projet open source WebKit, où les outils sont appelés Web Inspector.

- **CheckMarx** : c'est un scanner de vulnérabilité statique du code pour les application .NET.
- **Twilio** : c'est le leader de marché des appels et sms. Il propose une API bien documenté qui permet d'envoyer/recevoir des sms et des appels en masse facilement.

I.3 Technologie et langage de développement

Les technologies et langage utilisés pour le développement de ce projet sont :

- ✓ **ASP.NET (MVC) :** ASP.NET est un ensemble de technologies de programmation web, crée par Microsoft. ASP.NET fait partie de la plateforme Microsoft .NET et est le successeur de la technologie Active Server Pages (ASP). Il est donc un Framework de développement d'application web, basé sur le motif de conception Modèle-Vue-Contrôleur aussi nommé MVC. ASP.NET MVC est une infrastructure de présentation simple et facilement testable, qui (comme celle des applications utilisant des Web Forms) est intégrée aux fonctionnalités ASP.NET existantes.

- ✓ **CSharp** : (C#) C'est un nouveau langage développé par Microsoft. Il s'inspire notamment de Java, C++ et Delphi. C# a été conçu spécifiquement pour la plateforme .NET, il est donc généralement considéré comme le langage le plus adapté pour le développement .NET.

- ✓ **jQuery** : C'est un Framework JavaScript open source, implanté coté client, qui porte sur l'interaction entre DOM, JavaScript, AJAX et le HTML. Cette bibliothèque JavaScript est destinée à simplifier les commandes courantes de JavaScript. La devise de jQuery est en effet « Ecrire moins pour faire plus ». Les spécificités de jQuery sont nombreuses, mais l'essentiel est certainement la flexibilité qu'il apporte pour accéder à tous les éléments du document Html. Cette caractéristique est d'ailleurs retenu pour donner un nom à ce Framework : j pour JavaScript et Query pour chercher ou accéder aux éléments.

II Présentation des interfaces

Dans ce qui suit, on va présenter quelques scénarios d'utilisation via des interfaces graphiques de notre application.

II.1 Interface d'authentification

Chaque utilisateur doit s'authentifier afin d'accéder à son espace. Il doit introduire son identifiant et son mot de passe.

L'accès aux ressources de la plateforme nécessite une sécurisation des données basée sur les techniques d'authentification de l'utilisateur.

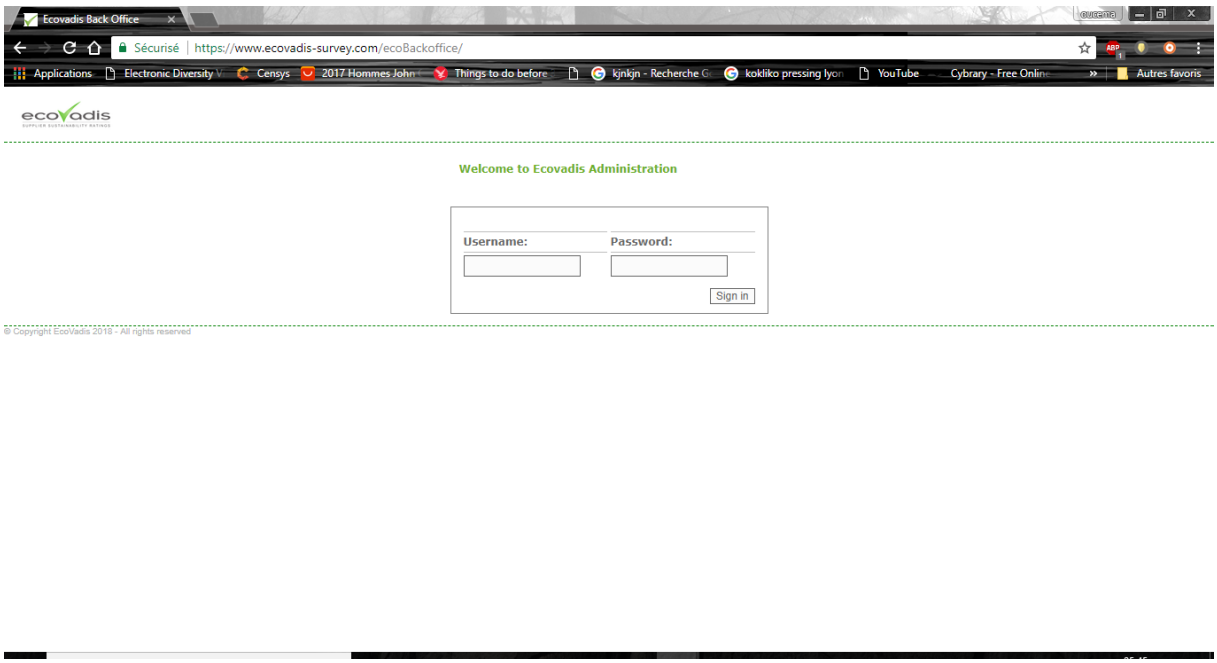


Figure 7 Interface d'authentification

II.2 Interface du code second facteur

Après la réussite de la première étape l'utilisateur reçoit le code soit par un sms soit sur l'application Google Auth et il est redirigé vers l'interface de connexion.

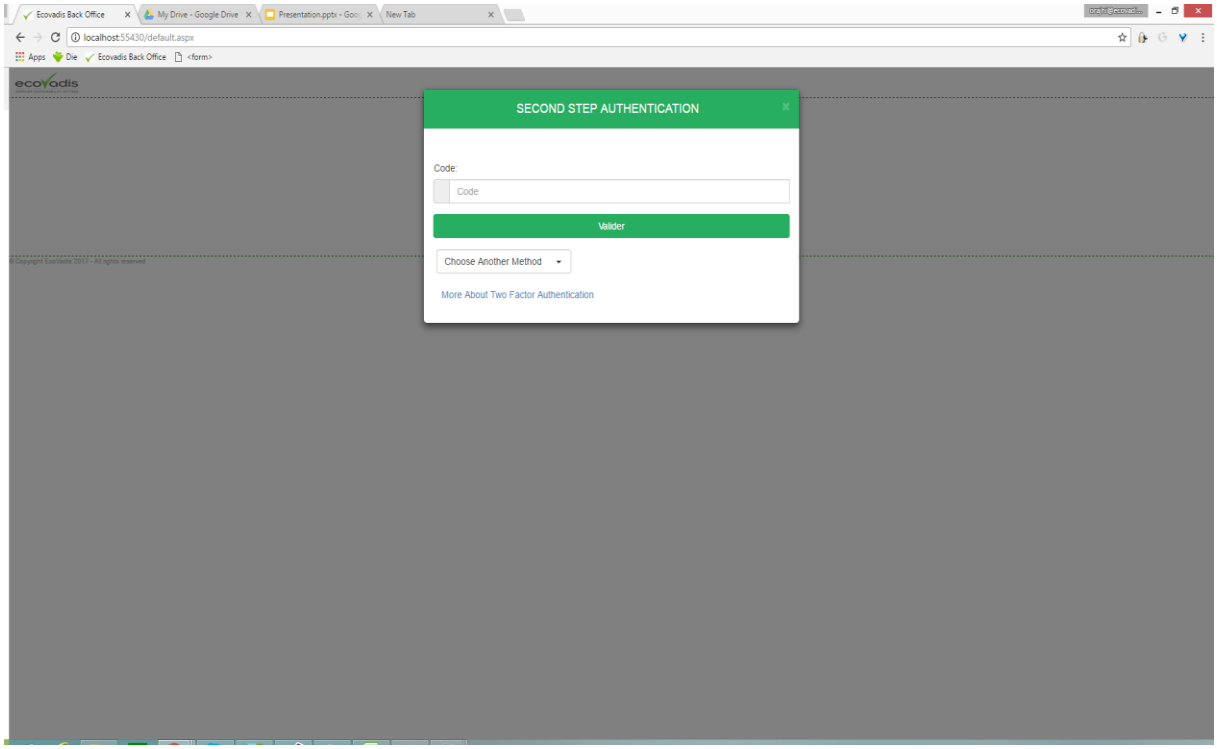


Figure 8 Interface d'authentification

II.3 Interface de gestion des options double facteur

Sur cette interface l'administrateur peut modifier les utilisateurs et activer/désactiver l'authentification double facteur pour un ou plusieurs utilisateurs. Il peut aussi sélectionner un utilisateur et visualiser ses paramètres ou modifier certains paramètres.

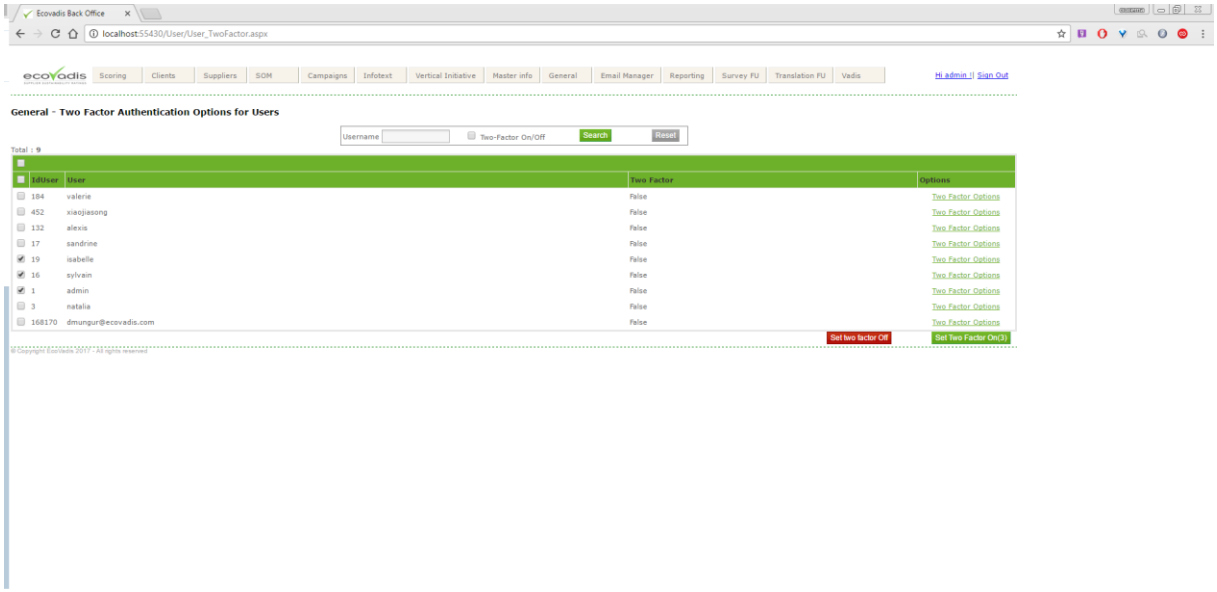


Figure 9 Interface de gestion des la fonctionnalité authentification double facteur

II.4 Options de double facteur

Sur cette interface l'administrateur peut envoyer les paramètre double facteurs aux utilisateurs finaux et modifier certains paramètre comme le numéro du téléphone.

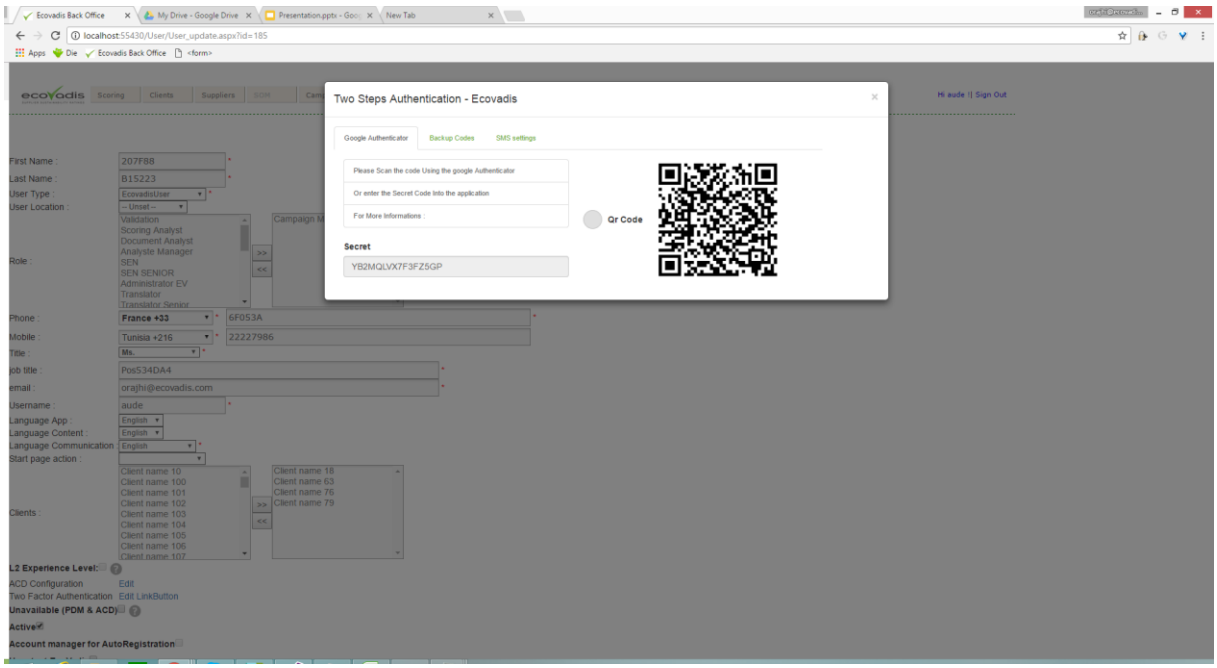


Figure 10 Interface des options personalisé double facteur

II.5 interface de logs double facteur

L'administrateur peut accéder aux logs détaillés de la fonctionnalité sur cette interface par type et par date.

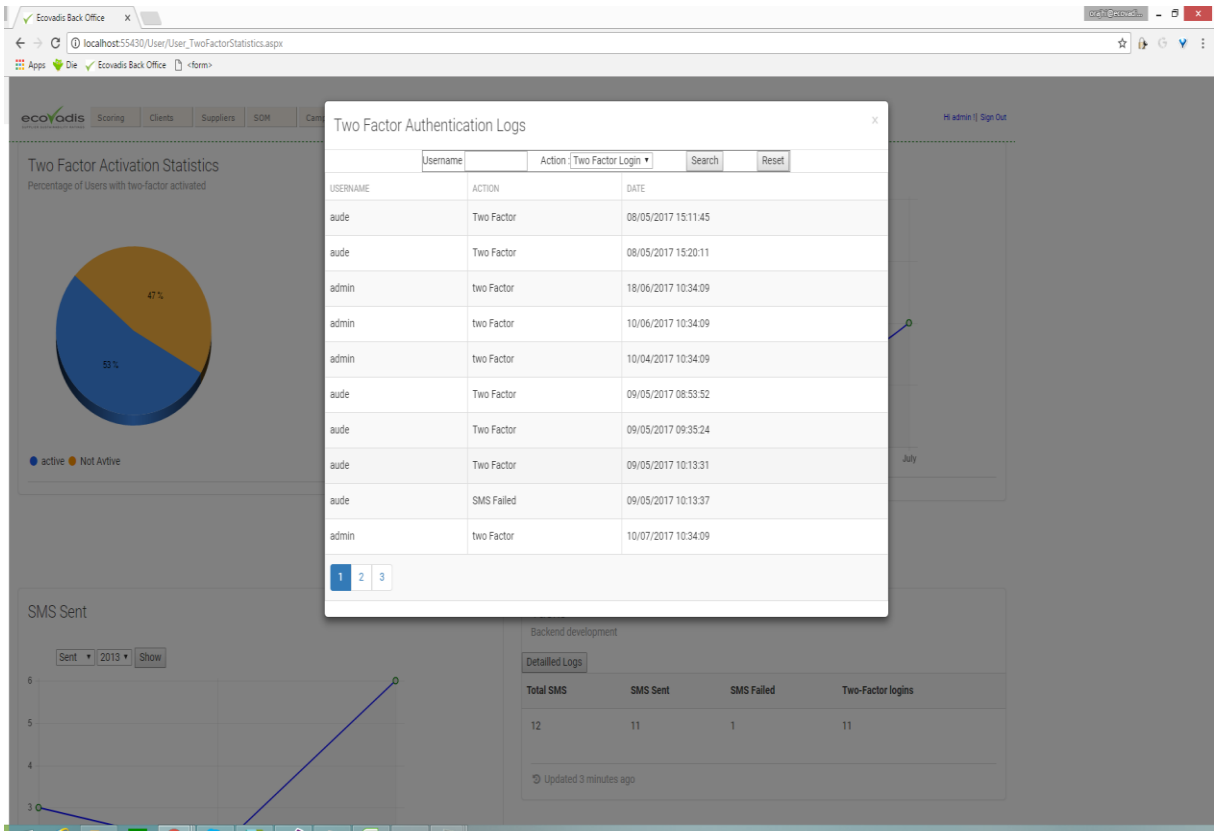


Figure 11 Interfaces des logs double Facteur

II.6 Interface de statistiques double facteur

L'administrateur peut accéder aux statistique d'utilisation de la fonctionnalité d'authentification et de l'envoi des sms détaillé ainsi que e pourcentage d'activation de la fonctionnalité.

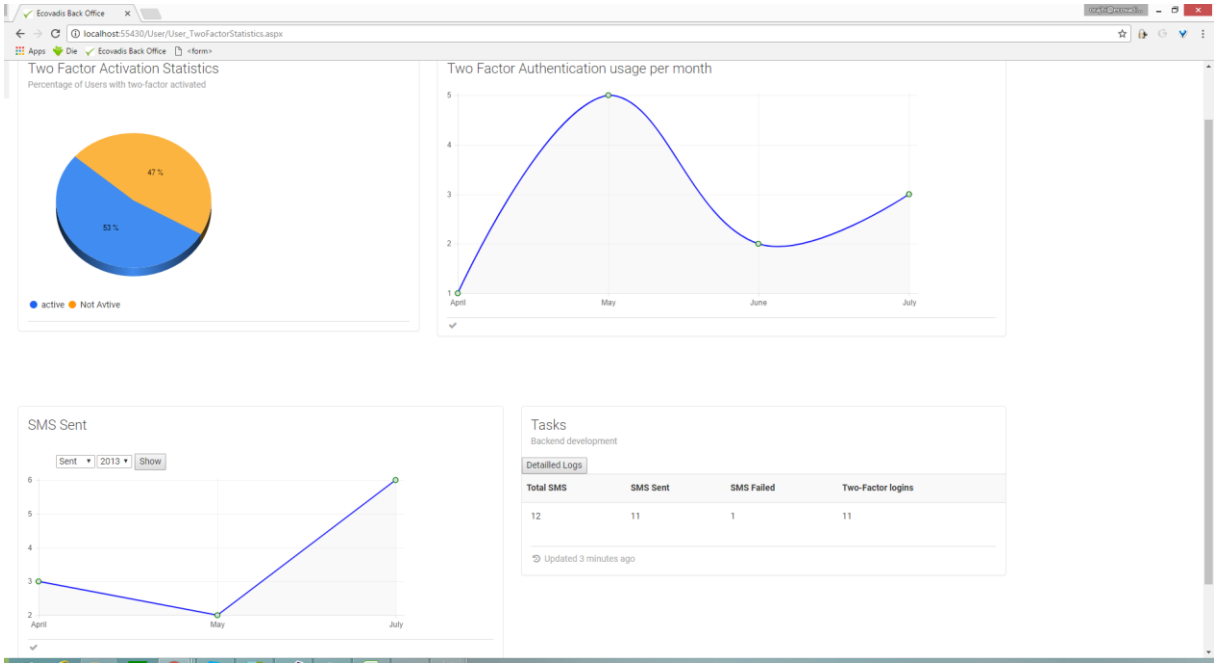


Figure 12 Interface des Statistiques double Facteur

III.Test de sécurité

Pour le test de sécurité, on a utilisé l'outil de scan CheckMarx. C'est est un scanner de sécurité pour le code source des applications supportant plus de 20 Langages de programmation.

Contrairement à beaucoup de outils de scan Web, CheckMarx fait un scan sur le code source de votre application.

Une fois CheckMarx analyse le code de l'application, il produit un rapport sur toutes les failles de sécurité qu'il a trouvée.

- **Avantages :** Aucune configuration nécessaire. Il suffit de l'exécuter.
- **Exécution à tout moment :** Parce que tous les besoins de CheckMarx sont un code source, CheckMarx peut être exécuté à n'importe quel stade de développement.
- **Les meilleures pratiques :** CheckMarx peut être exécuté de façon itérative a chaque fois qu'on effectue une correction.
- **Test flexibles :** Chaque vérification effectuée par CheckMarx est indépendante, de sorte que les tests peuvent être limités à un sous-ensemble de tous les contrôles auxquels CheckMarx est livré.
- **La vitesse :** Bien que CheckMarx ne soit pas exceptionnellement rapide, il est beaucoup plus rapide que les scanners de sites Web .Même les grandes applications ne devraient pas prendre plus de quelques minutes pour numériser.

L'outil génère un rapport détaillé en format HTML,JSON et PDF avec des vulnérabilités détectés qu'il convient de vérifier manuellement par le développeur.

Rapport générale des vulnérabilités

Checkmarx produit un rapport détaillé des vulnérabilités classé selon l'impact donné par l'OWASP TOP 10 et affiche des graphiques sur l'impact de ces dernières sur différents parties du système et leur distribution dans la solution.

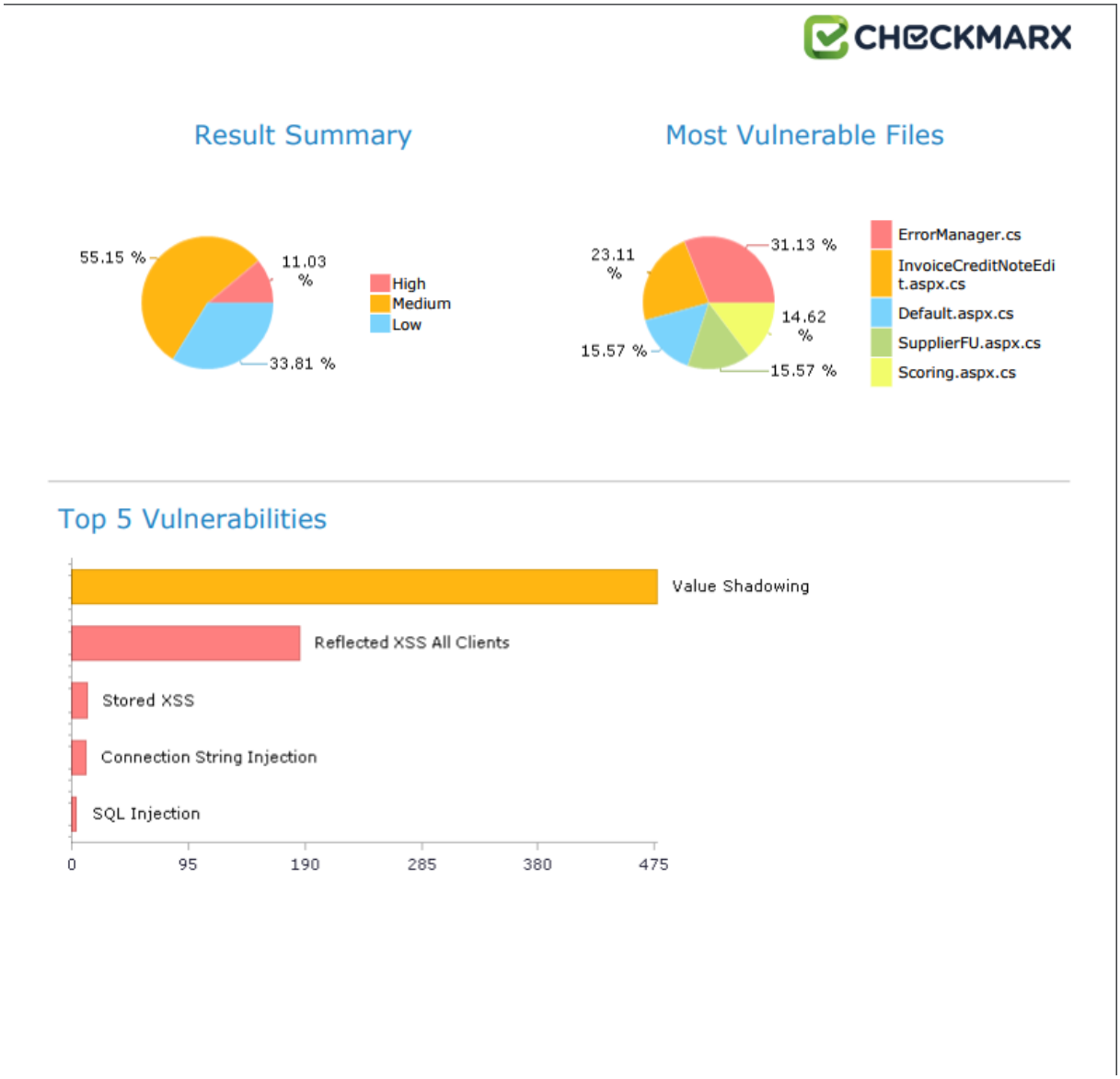


Figure 13 Rapport Générale des vulnérabilités

CHECKMARX

Results Distribution By Status First scan of the project

	High	Medium	Low	Information	Total
New Issues	214	1,070	656	0	1,940
Recurrent Issues	0	0	0	0	0
Total	214	1,070	656	0	1,940
Fixed Issues	0	0	0	0	0

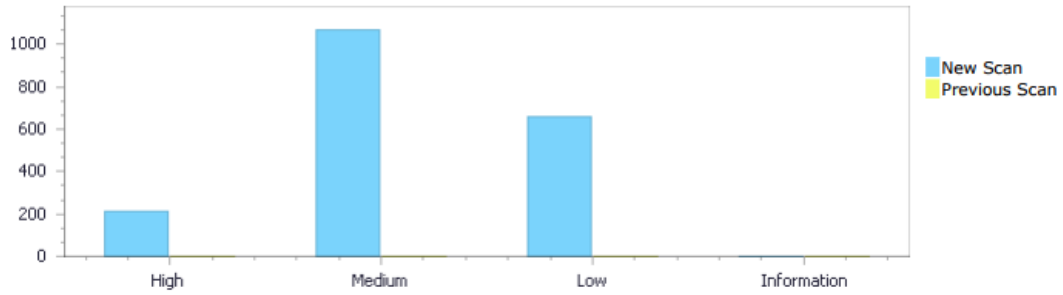
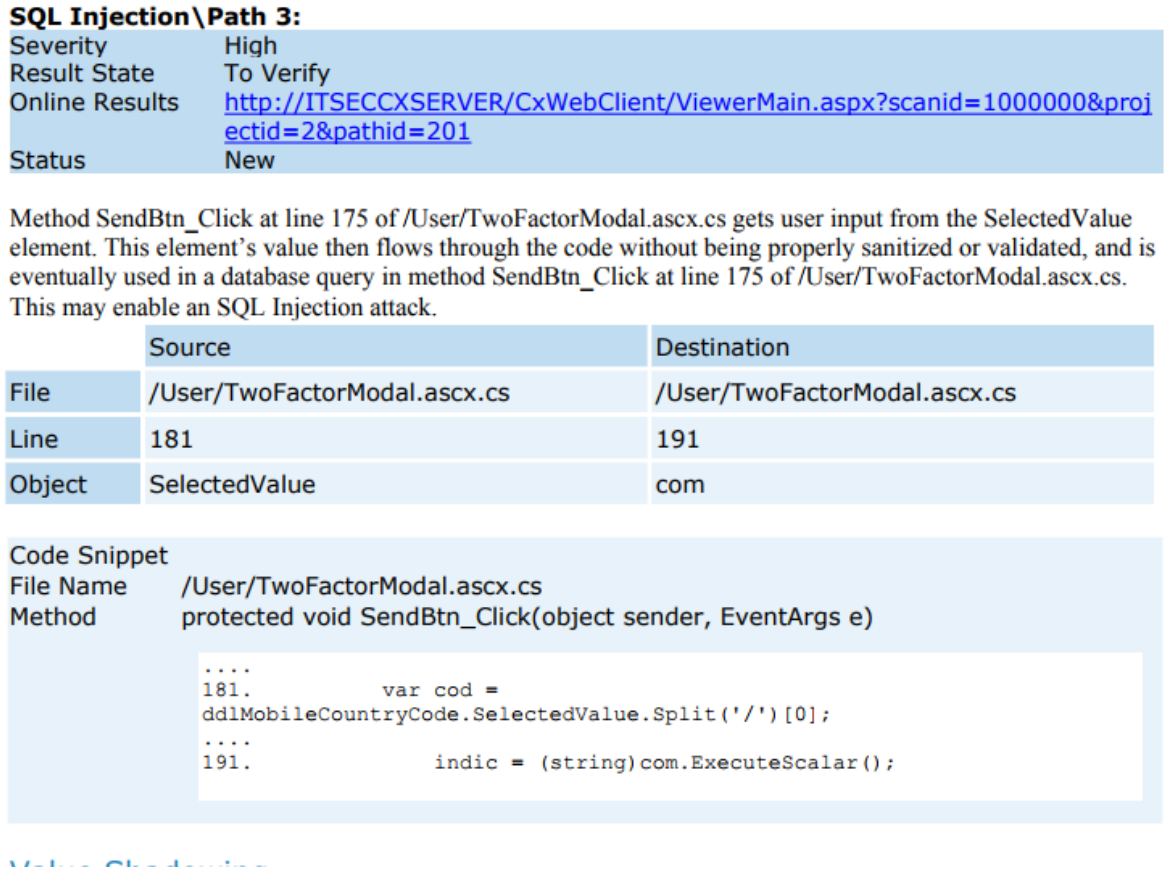


Figure 14 Rapport des vulnérabilités par catégorie

Chaque vulnérabilité détecté dans le code est décrite et l'emplacement ou elle a été détecté est signalé. Pour une vérification manuelle sur le code et en utilisant des outils de test de vulnérabilité specialisé tel que Burpsuite ou Fiddler.



SQL Injection\Path 3:

Severity	High
Result State	To Verify
Online Results	http://ITSECCXSERVER/CxWebClient/ViewerMain.aspx?scanid=1000000&projectid=2&pathid=201
Status	New

Method SendBtn_Click at line 175 of /User/TwoFactorModal.ascx.cs gets user input from the SelectedValue element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method SendBtn_Click at line 175 of /User/TwoFactorModal.ascx.cs. This may enable an SQL Injection attack.

	Source	Destination
File	/User/TwoFactorModal.ascx.cs	/User/TwoFactorModal.ascx.cs
Line	181	191
Object	SelectedValue	com

Code Snippet
File Name /User/TwoFactorModal.ascx.cs
Method protected void SendBtn_Click(object sender, EventArgs e)

```
....
181.          var cod =
ddlMobileCountryCode.SelectedValue.Split('/')[0];
....
191.              indic = (string)com.ExecuteScalar();
```

Figure 15 Example de vulnérabilité détecté par Checkmarx

VI. Planification du projet

Afin de schématiser l'évolution de notre projet nous avons utilisé l'outil en ligne Tom's Planner qui permet de schématiser des diagrammes de Gantt en toute simplicité.

Le schéma ci-dessous représente le diagramme de Gantt qu'on a établi pour la planification de notre projet :

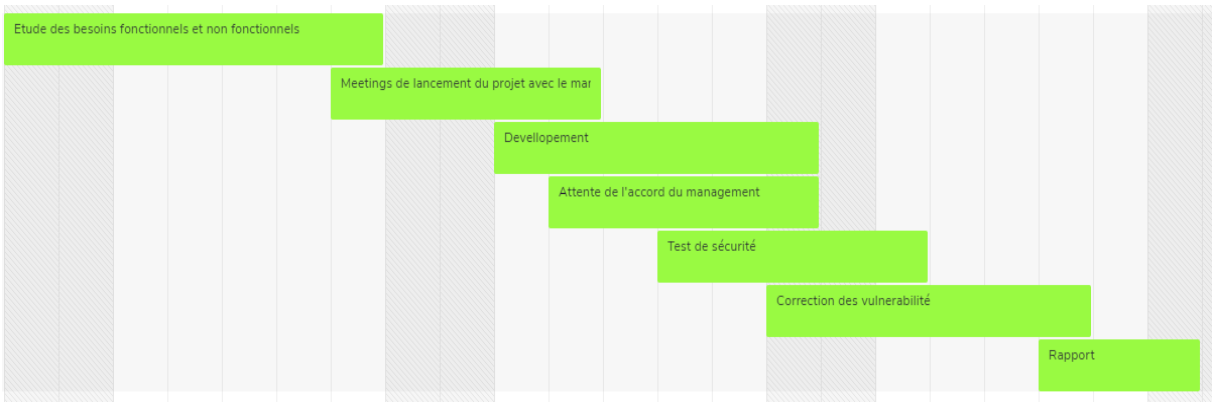


Figure 16 Diagramme de Gannt

Conclusion :

Au cours de ce chapitre, nous avons essayé de présenter notre environnement de travail matériel et logiciel, pour terminer par un balayage des différentes interfaces développées et des tests de sécurité de qualité effectués.

Conclusion Générale

La sécurité des systèmes d'information est devenue une préoccupation accrue pour la plupart des entreprises. En effet, l'émergence de nouvelles menaces informatiques rend toujours ces dernières exposées à des risques de perte ou de vol de données.

Le premier rempart pour une application web est l'authentification qui doit être sécurisé au moyen d'une authentification sécurisé et bien développé.

A cet effet, Ecovadis a pensé à introduire un système d'authentification à double facteur a sa plateforme.

Il s'agit d'un service de sécurisation des applications web par l'ajout d'un facteur supplémentaire au couple nom d'utilisateur/mot de passe classique.

Afin d'atteindre cet objectif, nous avons commencé par identifier et analyser les besoins des clients en matière d'authentification double facteur. Par la suite, nous avons spécifié les principales fonctionnalités que doit accomplir notre outil et nous avons choisi de nous focaliser principalement sur sept critères pour offrir une meilleure solution qui répond aux besoins des utilisateurs.

Enfin, nous avons réalisé une fonctionnalité d'authentification simple pour l'utilisateurs et des options de gestions pour l'administrateur.

En effet, cette plateforme offre une interface cohérente et personnalisée, des tableaux de bord et statistiques et un service de SMS.

De plus, elle permet une surveillance pertinente et personnalisée des éditeurs et produits composant le système d'information de l'entreprise avec une gestion des vulnérabilités et un suivi des solutions correctives à déployer à travers un outil de workflow.

Dans le cadre de perspectives, nous envisageons d'ajouter des fonctionnalités supplémentaires pour le code second facteur comme des générateurs de mot de passe matériel et des cartes d'accès a puce

Annexes

➢ Logiciel de gestion de projet TFS

Les figures ci-dessous montrent des interfaces du logiciel de gestion de projet TFS, TFS permet la gestion des sources, la gestion des builds, le suivi des éléments de travail, la planification, la gestion de projet et l'analyse des performances. Il a pour but d'augmenter la productivité des développeurs.

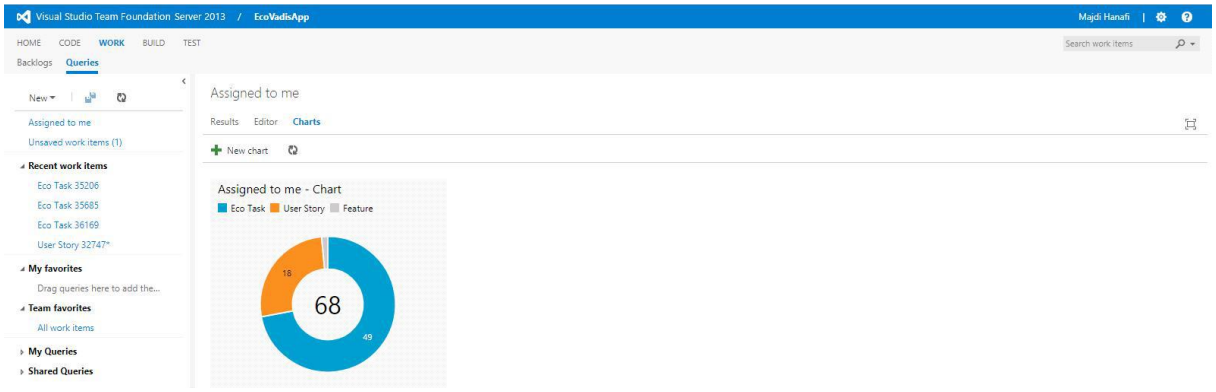


Figure 17 Chart du projet

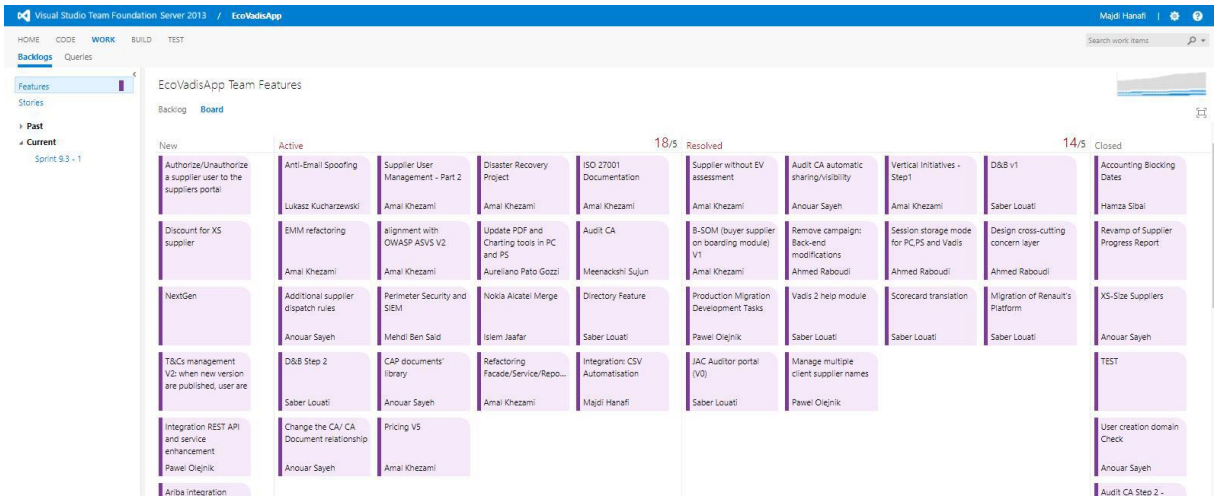


Figure 18 TFS Board

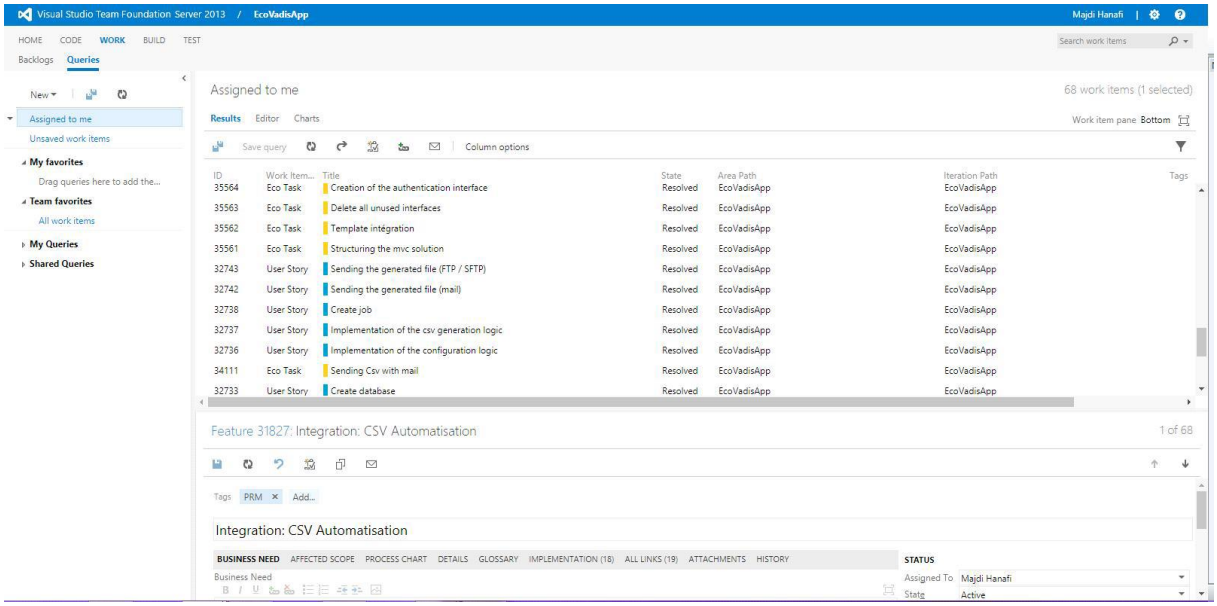


Figure 19 Liste des taches

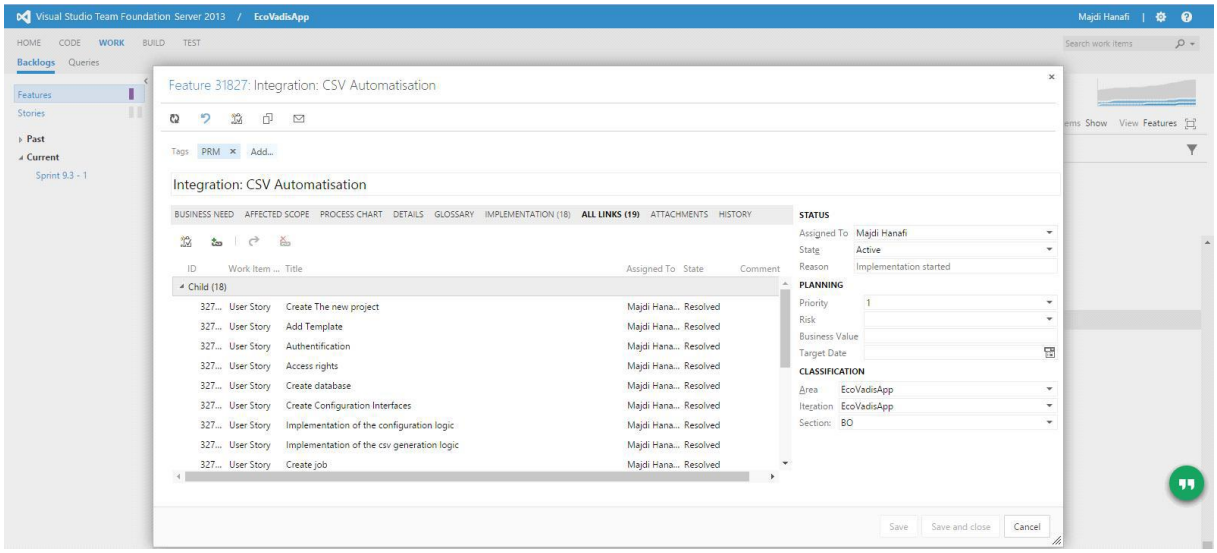


Figure 20 Liste des User Stories

➢ Test unitaire

L'objectif d'un test unitaire est de permettre au développeur de s'assurer qu'une unité de code ne comporte pas d'erreur de programmation. C'est un test, donc les vérifications sont faites en exécutant une petite partie (une « unité ») de code.

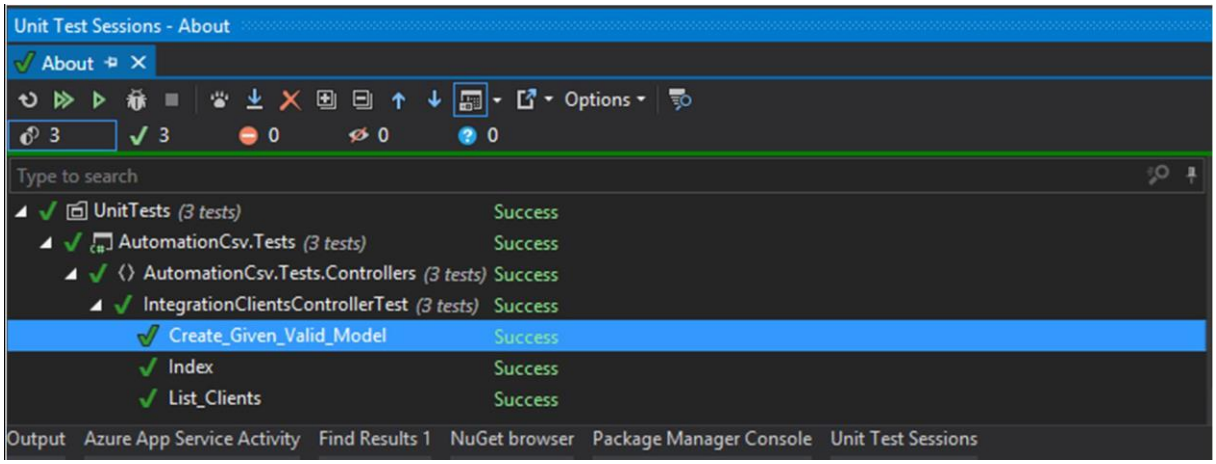


Figure 21 Example de test unitaire

Néttographie

[W1]. http://www.ecovadis.com

[W2]. http://testrelease.ecovadis-itlab.com

[W3]. https://www.ecovadis-itsecurity.com/ecoBackOffice

[W4]. http://www.lucidcharts.com

[W5]. https://technet.microsoft.com/en-us/library/security/MS17-023

[W6].http://laurent-audibert.developpez.com/Cours-UML/html/Cours-UML.html#htoc23

[W7]. https://www.twilio.com/docs/tutorials/two-factor-authentication-csharp-mvc

[W8]. https://www.vmware.com

[W9].https://docs.microsoft.com/en-us/aspnet/identity/overview/features-api/two-factor-authentication-using-sms-and-email-with-aspnet-identity

[W10]. http://winscp.net/eng/docs/lang:fr

Glossaire

2

- 2FA: 2 Factor Authentiaction

A

- API: Application Programming Interface

B

- BD: Base de Données
- BO : BackOffice

H

- HTML: Hypertext Markup Language
- HTTP: Hypertext Transfer Protocol

I

- IDE: Integrated Development Environment

J

- JSON: JavaScript Object Notation

M

- MsSQL: Micraosoft Structured Query Language

S

- SGBDR: Système de Gestion de Base de Données Relationnelle
- SI : Système d'Information
- SQL: Structured Query Language

U

- UML: Unified Modeling Language

esprit

esprit

18, rue de l'Usine - ZI Aéroport
Charguia II - 2035 Ariana
Tél. : +216 71 941 541 (LG)
Fax. : +216 71 941 889
e-mail : contact@esprit.ens.tn
www.esprit.ens.tn