République algérienne démocratique et populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université Saad Dahleb , Blida

Faculté des sciences

Département d'informatique

Projet de fin d'étude MASTER en :

Systèmes informatiques et réseaux « SIR »

Sécurité des systèmes d'informations « SSI »

Thème :

Conception et développement d'une solution automatisée pour le processus de veille sécuritaire

Réalisé par :

- Messaoun Yousra

- Nadir Maissa Ahlem

Promoteurs :

- Sahnoune Zakaria

- N. Agha

Année universitaire : 2020/2021

Résumé

Avec la croissance et l'utilisation généralisées des informations numériques, dont une grande partie est confidentielle, il y a également eu une augmentation des incidents de vol d'informations. La sécurité est très importante pour toute organisation afin d'éviter que des utilisateurs non autorisés n'accèdent aux données électroniques. La vulnérabilité est définie comme un état d'être susceptible d'être affecté par une attaque. La gestion des vulnérabilités, en d'autres termes, se définit comme la gestion de l'occurrence d'attaques avec différents outils et techniques. Pour assurer la sécurité des données, nous avons réaliser une application Web qui permet d'automatiser le processus de la veille sécuritaire d'ELIT depuis le recensement de l'actif à protéger, l'identification de la vulnérabilité touchant l'actif jusqu'au traitement de cette dernière en gardant la traçabilité et le suivi du bulletin depuis son envoie jusqu'à son classement .

Abstract

With the growth and widespread use of digital information, much of which is confidential, there has also been an increase in incidents of information theft. Security is very important to any organization to prevent unauthorized users from accessing electronic data. Vulnerability is defined as a state of being susceptible to being affected by an attack. Vulnerability management, in other words, is defined as managing the occurrence of attacks with different tools and techniques. To ensure data security, we have created a Web application that automates the process of ELIT's security watch from the inventory of the asset to be protected, the identification of the vulnerability affecting the asset until the processing of the latter while keeping the traceability and the follow-up of the bulletin from its sending until its classification.

ملخص

مع نمو المعلومات الرقمية واستخدامها على نطاق واسع ، وكثير منها سري ، كانت هناك أيضًا زيادة في حوادث سرقة المعلومات. الأمان مهم جدًا لأي منظمة لمنع المستخدمين غير المصرح لهم من الوصول إلى البيانات الإلكترونية. يتم تعريف الضعف على أنه حالة من التعرض للتأثر بالهجوم. بعبارة أخرى ، تُعرَّف إدارة الثغرات بأنها إدارة حدوث الهجمات باستخدام أدوات وتقنيات مختلفة. لضمان أمان البيانات ، قمنا بإنشاء تطبيق ويب يقوم بإتمام عملية مراقبة أمن ELIT من جرد « actif » المراد حمايته ، وتحديد الثغرة الأمنية التي تؤثر على « actif » حتى معالجته مع الحفاظ على إمكانية التتبع و متابعة النشرة من تاريخ إرسالها حتى تصنيفها.

Sommaire

Chapitre II: Présentation de l'organisme d'accueil

Chapitre III : Conception

Chapitre IV : Développement et implémentation

Liste des figures

Liste des tableaux

Remerciements

En préambule à ce mémoire, nous remercions tout d'abord ALLAH de nous avoir donné le Courage et la patience afin d'élaborer notre travail, et ainsi achever une grande partie de nos études.

Nous tenons à remercier sincèrement monsieur Sahnoune Zakaria et madame N.Agha, en tant que promoteurs, qui se sont montrés à l'écoute et étant toujours disponibles tout au long de la réalisation de ce projet, ainsi pour l'inspiration, l'aide et le temps qu'ils ont bien voulu nous consacrer.

Nous exprimons notre gratitude et reconnaissance aux professeurs de département d'informatique qui nous ont tant donné pour être ce que nous sommes aujourd'hui.

On n'oublie pas les personnes qui nous ont apporté leur aide, et leur soutien moral, nos familles pour l'amour qu'elles nous portent pendant tout le cursus de nos études, nos amis, nos proches, même par un mot d'encouragement, de loin ou de prés.

Dédicace de Messaoun Yousra

Je dédie ce mémoire à mes chers parents, mon père Djamel, ma mère Nacera et mon beau père Ahmed Pour leurpatience, leur amour, leur soutien et leurs encouragements.

Aux personnes dont j'ai bien aimé la présence dans ce jour, à mon cher mari et Mes chères sœur: Abd El-Raouf , Asma et Meriem.

Aux personnes qui m'ont toujours aidé et encouragé, qui étaient Toujours à mescôtés, et qui m'ont accompagné durant mon chemin d'études, mes aimablesamis, collègues d'étude.

Dédicace de Nadir Maissa Ahlem

je dédie ce modeste travail à mes parents que je ne pourrais jamais leurs exprimer ma reconnaissance pour leurssacrifices , conseils et encouragementstout au long de ma vie.

A l'homme, mon précieux cadeau de dieu, et a qui je dois ma réussite et mon bonheur: mon cher père Youcef.

A la femme, qui a souffert sans me laisser souffrir, qui n'a jamais dit non à mes exigences et qui n'a épargné aucun effort pour me rendre heureuse : mon adorable mère Naima.

A mes chères sœurs« Hadil,Manar et Allaa » et ma meilleure amie « Dounia ». Que Dieu les protèges et leurs offre la chance et le bonheur. A toute ma famille, mes amis et mes collègues d'étudesque j'ai connu jusqu'à maintenant. Merci pour leurs amours et leurs encouragements.

Liste des abréviations :

1. **CVE :**Common Vulnerabilities and Exposures
2. **Cvss :** Common Vulnerability Scoring System
3. **PSSI :** La politique de sécurité des systèmes d'information
4. **SI :** systèmes d'information
5. **CERT** : computer emergency response
6. **CSIRT :** computer security incident response team.
7. **SOC** : security operation center
8. **ELIT :** El Djazair information technology
9. **IT :** information technology
10. **DSSI :** direction sécurité des systèmes d'informations
11. **SSI :** Sécurité des Systèmes
12. **EDR :** détection et réponse des points de terminaison
13. **IA :** intelligence artificielle
14. **SIEM :** Security Information Event Management
15. **MVC :** Modèle-Vue-Contrôleur
16. **CSRF :** Cross-Site RequestForgery

Introduction générale

De nos jours, de nombreuses entreprises sont uniquement basées sur le stockage de toutes sortes d'informations dans des ordinateurs, à commencer par les données personnelles du personnel, les listes de clients jusqu'aux salaires, aux coordonnées bancaires et au marketing, etc.

Par conséquent, cela est considéré comme quelque chose de «souhaitable» pour de nombreuses personnes qui fera tout ce qu'il faut pour l'éclater; Les preuves de cet argument sont partout: actualités, rapports, journaux, et plus évidemment dans le fait que chaque jour il y a une nouvelle mise à jour logicielle, un patch OS et même une autre méthode de cryptage.

La sécurité de l'information consiste à faire une veille sécuritaire qui donne la capacité d'anticiper les attaques informatiques pour mieux protéger les informations sensibles et les systèmes d'information contre tout accès non autorisé et surtout contre toute utilisation, perturbation, modification ou destruction. Sans cette protection, il serait souvent très difficile pour une entreprise de fonctionner. Des systèmes de sécurité de l'information doivent être mis en œuvre et devraient normalement inclure au moins:

- Analyse des systèmes.

- Détection des vulnérabilités des systèmes.

- Gestion des solutions de vulnérabilités.

Problématique :

Dans le domaine de la sécurité SI en général, l'entreprise Elit El Djazair en particulier, l'activité de veille sécuritaire est une activité cruciale et névralgique qui consiste à collecter et à gérer les vulnérabilités qui sont des bugs ou des faiblesses dans la conception, la mise en œuvre ou la configuration d'un système. Ces faiblesses permettent à un attaquant de passer outre les politiques de sécurité et de porter atteinte à l'intégrité du système. Les vulnérabilités constituent le principal point d'entrée pour pénétrer dans les systèmes informatiques et obtenir un accès non autorisé à des actifs au sein de ces systèmes.

Dans ce travail, nous nous intéressons au processus de la gestion des vulnérabilités depuis la création des bulletins de vulnérabilités jusqu'à leurs traitement et prise en charge.

Objectifs :

Notre objectif est de concevoir et développer une application web qui prend en charge la gestion des vulnérabilités depuis la création des bulletins jusqu'à leurs classement tout en assurant une traçabilité des échanges des différents acteurs de ce processus.

Chapitre I : Etat de l’art

1. Introduction :

Dans ce premier chapitre, nous allons définir les étapes des processus de la base de notre projet : le processus de la veille et la gestion de vulnérabilités.

2. La veille :

La veille est une activité continue en grande partie itérative visant à une surveillance active de l'environnement technologique, commercial, etc., pour en anticiper les évolutions.

Cette définition met l'accent sur les finalités, la surveillance de l'environnement et la détection des évolutions, et montre la différence avec la recherche d'information ; alors que celle-ci est une activité ponctuelle, en réponse à des besoins précis**.[1]**

3. Le processus de la veille :

La veille se déroule selon un cycle de cinq étapes : le ciblage, le sourcing, la collecte et la sélection des informations, l'analyse et la synthèse, la diffusion. **[2]**

- **3.1. Le ciblage :** Le ciblage doit permettre de définir les besoins de veille de l'entreprise. Cela passe par:
  - **a.** il faut définir l'aire de veille. C'est à dire les thèmes faisant l'objet de la veille et sous quel angle les surveiller (règlementation, bons exemples, ressources humaines,…).
  - **b.** il faut ensuite désigner les personnes en charge de la récupération de l'information et celles allant exploiter les résultats de manière stratégique.
  - **c.** le choix des mots-clés pertinents.
  - **d.** déterminer les sources et les personnes ressources à éventuellement consulter, les canaux d'information et les points d'accès à utiliser.

Il faut aussi répondre aux questions suivantes :

a. ''Pourquoi'' : La compréhension du contexte du besoin de surveillance.

b. ''Quoi '' : Définir les objectifs.

c.''Pour qui'' : l'identification des cibles de la veille.

- **3.2. Le sourcing :** Le sourcing consiste en une réflexion sur les outils et canaux de veille en fonction du ciblage :

a.utilisation des sources identifiées lors du ciblage et recherche de sources complémentaires.

b.qualification des sources en fonction de leur nature, rayon de diffusion, public visé, auteur, langue, contenu/but…

c.paramétrage et configuration de l'outil de surveillance choisi.

- **3.3. La collecte et la sélection d'information :** La collecte d'informations est une opération de rassemblage des études, des opinions, des documents…etc.
- **3.4. L'analyse et la synthèse :**L'analyse et la synthèse sont activités à haut niveau de valeur ajoutée, permettent de valider les informations recueillies ; Les stocker de manière pertinente ensuite les intégrer dans un ou plusieurs documents de synthèse.
- **3.5. La diffusion :**La diffusion permet la mise à disposition des informations sous forme de livrables aux personnes concernées. L'information doit parvenir aux

intéressés par les moyens de communication qu'ils utilisent et/ou qui sont les plus adaptés à la démarche de veille : lettres d'informations, alertes, sites dynamiques, blogs, fil rss…. Il faut également qu'ils puissent interagir.

4. La veille sécuritaire :

La veille en sécurité informatique est une activité indispensable, pour tous les professionnels. Elle nous permet de rester au fait des évolutions et tendances.

Mais, le plus important, la veille nous donne la capacité d'anticiper les attaques informatiques et mieux nous préparer et donc de limiter le risque d'un incident.

Les technologies sont en évolutions permanentes, les attaques et les vulnérabilités également. C'est un vrai jeu du chat et de la souris que se livrent pirates et défenseurs chaque semaine, des vulnérabilités sont découvertes, des entreprises sont victimes de piratages, entraînant des dommages importants, voire irrémédiables.

Autant dire qu'il est indispensable :

- de se tenir au courant des vulnérabilités et des patchs.
- des tendances d'attaques des pirates.

La veille en sécurité informatique, c'est donc l'outil indispensable pour s'éviter des frayeurs**.[3]**

5. Méthodologie d'une veille sécuritaire :

Dans le contexte d'une veille en sécurité, les étapes sont à définir comme suit **:[4]**

1. Définissez d'abord vos actifs via une **analyse en gestion des risques** pour comprendre ce que vous devez protéger.

2. Rédigez la **politique de sécurité des systèmes d'information (PSSI)** permettant de définir les mesures de protection à mettre en place.

3. Faites un **inventaire de votre système d'information** et de tout ce qui est lié aux actifs à protéger.

4. Définissez les **outils** et les **processus** que vous allez mettre en place pour **gérer les vulnérabilités.**

5. Déterminez des indicateurs permettant de mesurer l'efficacité de votre veille (indice de vulnérabilité des serveurs, nombre de services vulnérables, délai entre la publication d'un patch et son application).

6. Terminologie relatives :

6.1. La vulnérabilité : est un trou ou une faiblesse dans l'application, qui peut être une faille de conception ou un bogue d'implémentation, qui permet à un attaquant de nuire aux parties prenantes d'une application. Les parties prenantes incluent le propriétaire de l'application, les utilisateurs de l'application et d'autres entités qui dépendent de l'application.**[5]**

6.2. Une menace : Le dictionnaire Cambridge définit la menace comme la possibilité que quelque chose d'indésirable se produise. Dans la terminologie des informations de sécurité, une menace est une action connue qui a le potentiel de causer des dommages. **[5]**

6.3. Le risque : Le risque est la probabilité que la vulnérabilité soit exploitée. La probabilité qu'une menace utilise la vulnérabilité pour causer un dommage crée un risque. Lorsqu'une menace utilise la vulnérabilité pour infliger un préjudice, elle a un impact et, dans le contexte de la sécurité de l'information, l'impact est une perte de disponibilité, d'intégrité et de confidentialité.

La mesure d'un risque peut être déterminée comme une combinaison de la menace, de la vulnérabilité et des actifs.

Dans les concepts d'informations de sécurité, les hôtes sont normalement la cible des attaques. Lorsqu'un hôte est opérationnel et fournit un service, il est appelé actif. **[5]**

6.4. La faille informatique : Une faille informatique désigne l'ensemble des faiblesses d'un système informatique (système d'information, composant matériel, logiciel, périphériques, etc.) qui constituent autant de portes d'entrée pour les attaques malveillantes des **malwares**. Ces vulnérabilités sont causées par des insuffisances de sécurité intervenues lors de la conception, de la mise en œuvre ou de l'utilisation du système informatique, par exemple une erreur de code faite par un programmeur. Pour les entreprises, un **audit de sécurité informatique** est d'ailleurs recommandé.**[1]**

Les différentes failles de sécurité informatique :

Les failles de sécurité informatique peuvent prendre de nombreuses formes.

Pour preuve, du 1er janvier au 20 mars 2019 (soit moins de 3 mois), le CERT Orange Cyberdefense a publié plus de 850 vulnérabilités différentes.

Ces failles de sécurité peuvent notamment être exploitées pour injecter :

- Des virus en tout genre (notamment des chevaux de Troie et des vers informatiques).
- Des tentatives **d'**hameçonnage**,** ou **d'**usurpation d'identité numérique ;
- La prise de contrôle d'ordinateurs ou de réseaux entiers pouvant donner lieu à des ransomwares ou des vols de données pour les entreprises ou les particuliers.

Les attaques résultantes de failles de sécurité peuvent être exécutées à distance (en anglais remote exploit) ou directement sur le système (local exploit).**[6]**

6.5.Les bulletins de vulnérabilités : Les bulletins de vulnérabilité nous permettent de savoir des vulnérabilités de sécurité, des stratégies de correction et des mises à jour applicables aux logiciels concernés.

Les informations qui doivent être présentes dans Les bulletins de vulnérabilité :

1. **Référence du Bulletin.**
2. **Titre du Bulletin et description.**

3. **Indice de gravité maximale.**
4. **Actifs concernés.**
5. **Interlocuteurs concernés.**
6. **Solution.**
7. **La date.**
8. **Type de vulnérabilité.**

Exemple :

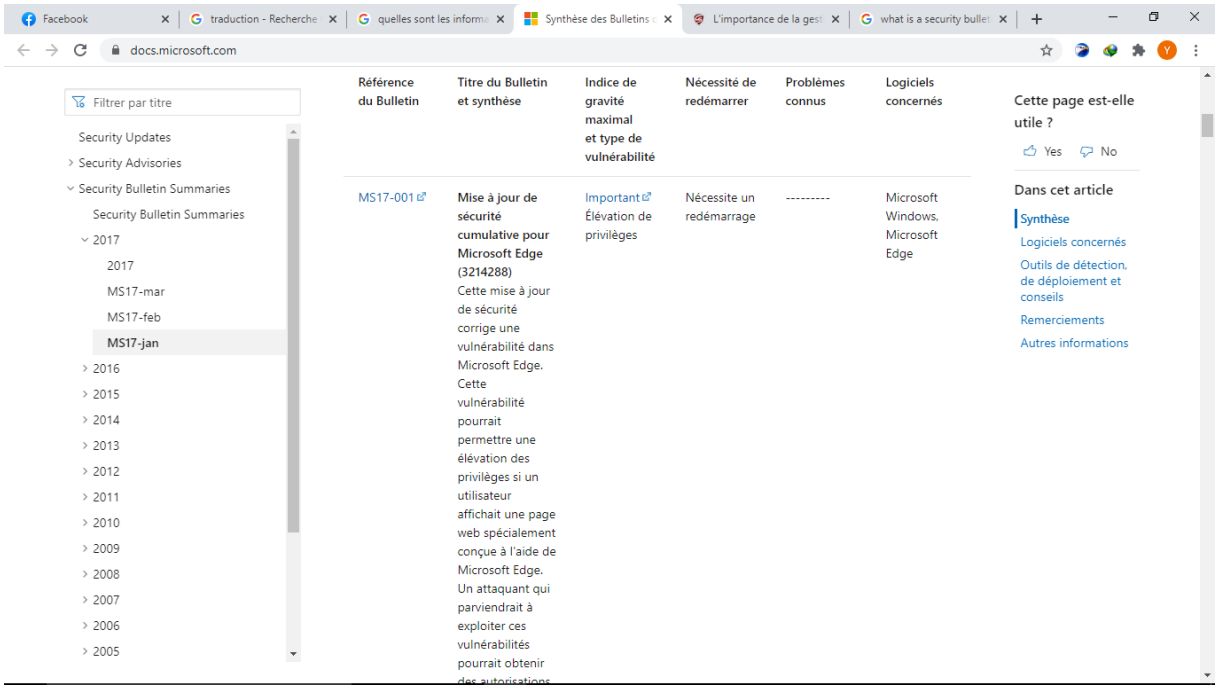


Figure 1 : Bulletin de vulnérabilité Microsoft de janvier 2017. [7]

Suite à la publication d'un bulletin de sécurité, il est nécessaire de :

- valider si la vulnérabilité concerne une solution utilisée par l'organisation.
- valider si l'actif touché par cette vulnérabilité est exposé sur Internet, depuis l'intranet, etc.
- valider la sévérité de cette vulnérabilité, c'est-à-dire de déterminer si celle-ci est exploitable à distance ou s'il est nécessaire d'être physiquement devant l'ordinateur par exemple.
- rédiger une fiche de vulnérabilité telle que définie dans le processus interne de l'organisation.
- planifier la mise en place du correctif. Si la mise à jour n'est pas possible dans un délai raisonnable en fonction de sa sévérité, il faudra mettre en place des solutions de contournement afin de réduire la surface d'attaque en attendant de pouvoir appliquer le correctif.

6.6.CVE : Common Vulnerabilities and Exposures ou **CVE** est un dictionnaire des informations publiques relatives aux vulnérabilités de sécurité. Le dictionnaire est maintenu par l'organisme MITRE.

Les identifiants CVE sont des références de la forme CVE-AAAA-NNNN (AAAA est l'année de publication et NNNN un numéro d'identifiant). Par exemple, la faille FREAK a pour identifiant CVE-2015-0204.

Le contenu du dictionnaire CVE peut être téléchargé. Cette liste contient une description succincte de la vulnérabilité concernée, ainsi qu'un ensemble de liens que les utilisateurs peuvent consulter pour plus d'informations.

Il existe de nombreux produits de sécurité qui traitent de vulnérabilités et qui utilisent donc les identifiants CVE :

- les services d'information sur les vulnérabilités,
- les IDS,IPS
- les scanneurs de vulnérabilités,

CVE fournit des détails complets sur la menace: nom commun, expositions de configuration, vue d'ensemble, description, risque, impact, solutions possibles, état, références, etc.**[5]**

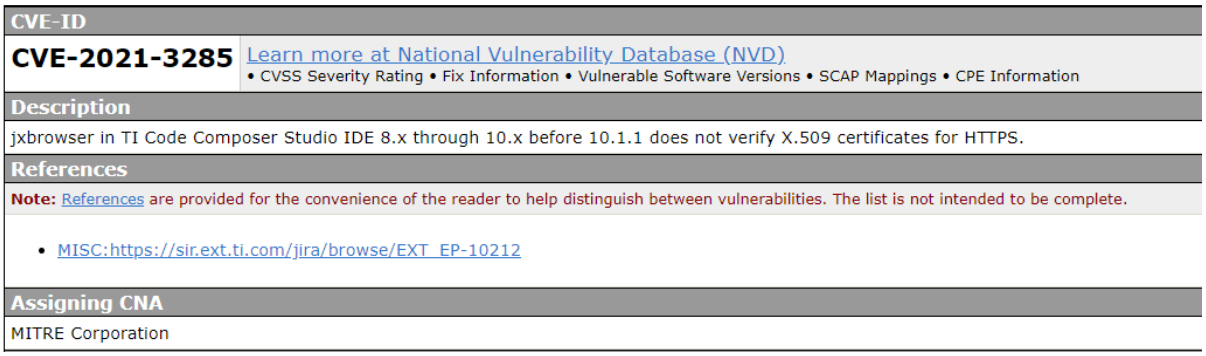


Figure 2 : exemple de CVE

6.7.Cvss :(Common Vulnerability Scoring System) est un système permettant de calculer une note évaluant la criticité d'une vulnérabilité, et de construire une chaine de caractères (un vecteur) présentant les caractéristiques de cette vulnérabilité, et les critères utilisés pour ce calcul **[8]** .

7. Gestion de vulnérabilité :

La gestion de vulnérabilité est un service de sécurité informatique. Son objectif est de garantir le traitement et la solution des vulnérabilités des infrastructures informatiques afin de minimiser les niveaux de risques.

Cette gestion garantit des méthodes et des procédures standard afin d'analyser les vulnérabilités bien connues des actifs et, si possible, de proposer l'exécution de modifications

pour les atténuer. Ce processus doit être mis en œuvre une fois que les vulnérabilités ont été détectées. Elle se fait en plusieurs étapes **[1]** :

Etape 1 : définir les règles de cybersécurité :

La politique de sécurité des systèmes d'information (PSSI) exprime la stratégie de l'entreprise et fixe les règles de cybersécurité que cette entreprise souhaite respecter. Ces règles vont couvrir différents aspects de la cybersécurité, comme par exemple, les processus de sécurité appliqués aux :

- composants sensibles,
- postes de travail,
- réseaux,
- systèmes,
- accès logiques.

La gestion des vulnérabilités commence par la définition d'un champ d'application ou va s'exercer cette politique. Elle peut toucher tout ou partie des structures de l'organisation.

Puis, on définira les différentes règles à respecter, à partir desquelles il sera possible de constituer un processus de gestion des vulnérabilités. Toutes ces règles sont compilées dans un document complémentaire à la PSSI. Les informations peuvent être regroupées sous forme de chapitres, où l'on retrouvera les étapes clés de la gestion des vulnérabilités :

- La collecte des vulnérabilités et leur analyse,
- La prise de décisions,
- L'élaboration d'un plan d'actions lorsque nécessaire,
- Le suivi de l'application des correctifs,
- Le contrôle,
- la capitalisation,la sensibilisation.

Etape 2 : collecter des données:

De nombreuses méthodes de détection des vulnérabilités des SI (systèmes d'information) existent. Elles passent par des moyens variés tels que l'activité de veille, les alertes utilisateurs, les tests d'intrusion, les audits de sécurité ou encore les scans automatiques.

a. Les audits

Un audit de sécurité est utilisé pour évaluer le niveau de sécurité d'un périmètre défini. Il permettra de donner une image à un instant T des points faibles et des points forts du périmètre ciblé.

Les auditeurs analysent :

- Les politiques,
- Les processus,
- Les procédures,
- Les pratiques,
- Les configurations
- L'architecture des logiciels, des systèmes et réseaux.

Il est également recommandé de réaliser des tests d'intrusion. A l'issue de l'audit, les consultants remettent un rapport qui propose des recommandations pour chaque vulnérabilité identifiée.

b.Les audits automatisés

Il est possible d'automatiser une recherche de vulnérabilités en utilisant des scanneurs de vulnérabilités automatisés pour détecter les failles sur un périmètre restreint.

Il existe plusieurs types de scanneurs qu'il conviendra de choisir en fonction des technologies et du volume à traiter. Bien évidemment, les scans seront bien moins pertinents qu'un audit manuel car les faux positifs sont nombreux.

Etape 3 : analyser les données :

Une fois que la phase de collecte a identifié une ou plusieurs vulnérabilités, il faut traiter cette information :

- En vérifiant qu'il ne s'agisse pas d'un faux positif (fausse alerte),
- En évaluant l'impact et la vraisemblance de l'exploitation de la vulnérabilité sur le composant,
- En évaluant les risques liés à cette vulnérabilité sur l'ensemble du SI (système d'information).

Parfois il y a des composants ont des vulnérabilités critiques et par contre d'autres n'ont aucun impact comme par exemple, un patch (mise à jour) pourrait déjà avoir été installé, ou une configuration particulière du composant pourrait faire que celui-ci n'est pas vulnérable. Donc il s'agit de faire un test on exploitant la vulnérabilité, le résultat de succès ou non permet de dire si la vulnérabilité est bien présente sur le composant. On privilégiera les environnements de recette ISO production pour ne pas impacter les environnements de production.

Un environnement de recette ressemble à celui de production mais est utilisé pour passer en revue les fonctionnalités d'un composant. Un environnement ISO production est un

environnement identique à l'environnement de production mais n'impacte pas les systèmes, les réseaux, les services et les applications qui sont utilisés en production.

Une fois la menace est présente, l'analyse de risque encouru par l'entreprise il faut savoir comment la réduire .donc l'objectif de cette analyse est de limiter l'exposition aux risques afin de mieux les maîtriser. Nous pouvons représenter le processus d'analyse à l'aide du diagramme ci-dessous**[9]**:

Figure 3 : Processus d'analyse des vulnérabilités

Dans l'analyse des vulnérabilités, il faut aussi déterminer les conséquences d'un correctif sur les autres briques du SI. Sur un périmètre donné, notamment quand l'exploitation de la vulnérabilité reste faible, il est parfois plus risqué de corriger. Une analyse en profondeur permet alors de prendre les bonnes décisions.

Etape 4 : prendre les bonnes décisions :

Les informations et rapports doivent être rendus à des comités. Les décisionnaires se réunissent périodiquement pour traiter les vulnérabilités (faibles ou modérées) dont le risque pour le SI reste mineur. Pour les vulnérabilités majeures, des comités exceptionnels (les officiers de sécurité, le RSSI* opérationnel, le RSSI d'une filiale, …) peuvent avoir lieu.

Ces comités sont prévus pour :

- informer et consulter les participants,
- analyser les risques et la faisabilité des remédiations,
- prendre les décisions pour traiter les vulnérabilités,
- valider un plan d'action.

Etape 5: Plan Do Check Act:

Le plan d'action est fait par les différentes équipes responsables des composants impactés. Pour chaque action, doivent figurer au minimum :

- Le ou les composants cibles,
- Le responsable et les différents acteurs,
- L'action à mener (de manière suffisamment détaillée pour empêcher toute mauvaise interprétation).

Il est recommandé de suivre l'avancement du plan d'action dans un tableau de bord de la sécurité afin notamment de pouvoir en reporter l'état aux différents comités et responsables.

Le risque zéro n'existant pas, une attaque peut arriver alors que le plan d'action est en train d'être mis en œuvre. Savoir quels systèmes sont mis a jours et quels autres sont encore faillibles est très important. Pour cela le suivi doit s'accompagner d'un contrôle qui vise à vérifier si les mesures sont correctement appliquées et ne présentent pas de régression en matière de sécurité. Ces contrôles sont appliqués sur les composants vulnérables. Un audit (ou contre-audit s'il a déjà eu lieu), peut être un moyen adéquat pour effectuer cette vérification et identifier les éléments qui permettront d'agir en conséquence.

Etape 6 : apprendre et devenir meilleur :

Les vulnérabilités détectées doivent intégrées au programme des équipes techniques pour éviter de reproduire les mêmes erreurs à l'avenir. Ces équipes sont par exemple :

- Les auditeurs, qui pourront rejouer ces tests sur d'autres composants ou s'en inspirer pour mener des attaques plus élaborées,
- Les équipes CERT/CSIRT***, qui, dans leurs activités de « threathunting » auront de nouveaux scénarios à explorer et de nouvelles traces à analyser,
- Les équipes SOC****, qui pourront travailler sur l'intégration de nouveaux indicateurs de compromission ou affiner ceux existants.

***__CERT__ : computer emergency response team / CSIRT : computer security incident response team.

****__SOC__ : security operation center.

8.La gestion des bulletins des vulnérabilités :

Les vulnérabilités d'un système d'exploitation ou d'une application peuvent avoir différentes causes par exemple des erreurs de programmations, des vulnérabilités intentionnelles…etc. Si des vulnérabilités ont été identifiées dans un système, qu'elles soient intentionnelles ou non, le logiciel sera exposé aux attaques des programmes malveillants. Pour cela, il existe des entreprises qui utilisent les bulletins de vulnérabilités qui fournissent des résumés et des

nouvelles vulnérabilités.
Ces résumés contiennent des informations concernant les vulnérabilités comme le nom, la date d'apparition, le correctif, les systèmes touchés, cvss, la description des vulnérabilités...etc.

8.1. Pré requis :

- **Actif :** Tout élément représentant de la valeur pour l'entreprise.

- **Correctif :** Un programme qui sert à corriger une erreur ou un disfonctionnement dans un logiciel ou un autre programme, ou encore à effectuer une mise à jour d'un logiciel, dans le mais y remédier à la vulnérabilité identifiée.

- **Impact :** Changement négatif pénalisant le niveau des objectifs métiers atteints**.[10]**

9. Etude sur quelque solution existante dans le domaine de la gestion de vulnérabilités :

9.1.ManageEngine Vulnerability Manager Plus[11]

9.1.1. Description de ManageEngine Vulnerability Manager Plus :

Avec Vulnerability Manager Plus, de la détection et l'évaluation des vulnérabilités à leur élimination avec un flux de travail de correction automatisé, tous les aspects de la gestion des vulnérabilités sont facilités avec une console centralisée. Vous pouvez également gérer les configurations de sécurité, renforcer les serveurs web, atténuer les vulnérabilités zero-day, exécuter des audits de fin de vie et éliminer les logiciels risqués. Simplifier la gestion des vulnérabilités grâce à un agent déployable à distance, une interface web et une évolutivité infinie.

9.1.2. Les utilisateurs de ManageEngine Vulnerability Manager Plus :

Toutes les grandes entreprises, p. ex., les banques, les établissements d'enseignement, les institutions gouvernementales, les secteurs financiers ou encore les établissements de santé stockant des données sensibles dans leurs systèmes.

9.2. Syxsense :[12]

9.2.1. Description de Syxsense

Syxsense Secure propose une analyse des vulnérabilités, une gestion des correctifs, ainsi que l'EDR (détection et réponse des points de terminaison), le tout dans une solution performante. Syxsense Secure utilise l'IA (intelligence artificielle) pour aider les équipes de sécurité à prévoir et éliminer les menaces. Bénéficiez d'une surveillance en temps réel des processus malveillants, de la quarantaine automatisée des appareils et des données en temps réel pour avoir un aperçu de l'intégrité de chaque point de terminaison sur votre réseau.

9.2.2. Les utilisateurs de Syxsense

Les professionnels de l'informatique, les départements SecOps et les prestataires d'infogérance dotés de 100 à 100 000 terminaux ayant besoin d'une gestion avancée des points de terminaison et d'une sécurité des points de terminaison dans une seule solution.

9.3. Netsurion Managed Threat Protection :[13]

9.3.1. Description de Netsurion Managed Threat Protection :

Netsurion EventTracker, la plateforme phare de sécurité gérée, est conçue pour s'adapter aux organisations de toutes tailles et de tous stades de maturité. Que vous ayez besoin d'un complément ciblé à vos capacités et employés existants ou d'une solution externalisée complète, la plateforme EventTracker est personnalisable de manière unique en fonction de vos besoins. Cette architecture vous permet d'activer des fonctionnalités telles que la protection des points de terminaison, la SIEM (Security Information Event Management), la gestion des vulnérabilités, la recherche des menaces, etc., le tout au sein d'une console gérée de manière centralisée.

9.3.2. Les utilisateurs de Netsurion Managed Threat Protection :

Les organisations qui ont besoin de fonctionnalités avancées de détection des menaces et de neutralisation, qui veulent des capacités proactives de chasse aux menaces et qui cherchent également à rationaliser la gestion de la conformité.

9.4. Intruder[14]

9.4.1. Description de Intruder

Solution pour trouver les faiblesses dans votre domaine numérique en ligne, expliquer les risques et aider à la remédiation avant qu'une violation ne puisse se produire.

9.4.2. Les utilisateurs de Intruder

Intruder est un logiciel de gestion des vulnérabilités facile à utiliser pour les entreprises disposant de ressources internes limitées afin de répondre aux exigences d'exécution d'un programme efficace de gestion des vulnérabilités.

9.5. Les différentes fonctionnalités de ces logiciels :

	ManageEngine Vulnerability Manager Plus	Syxsense	Netsurion Managed Threat Protection	Intruder
Alertes/Notifications	X	X	X	X
Analyse de la vulnérabilité	X	X		X
Authentification à 2 facteurs	X			
Contrôles/Permissions d'accès	X	X		X
Cryptage	X			
Gestion des appareils	X			
Gestion des correctifs	X			
Gestion des menaces web	X			
Gestion des stratégies	X			
Notifications en temps réel	X			
Rapports et analyses.	X			
Rapports et statistiques	X			
Rapports personnalisables	X			
Suivi des activités	X			
Surveillance en temps réel	X			
Sécurité des applications	X			
Tableau de bord d'activités	X			
API		X		X
Analyse de code source		X		
Analyse des risques		X		
Analyse en temps réel		X		
Analyse web		X		X
Détection de ressources		X		X
Injections SQL		X		
Password Protection		X		
Protection contre les failles		X		X
Protection contre les menaces		X		
Rapports et analyses		X		X
Runtime Container Security		X		
Sécurité SSL		X		
Sécurité des applications web		X		X
Sécurité réseau		X		
Threat intelligence		X		
Évaluation des vulnérabilités		X		X
Analyse d'événements			X	
Analyse des causes profondes			X	
Analyse des comportements			X	
Définition des priorités			X	
Détection d'anomalies et malware			X	
Gestion de remédiation			X	
Gestion des points de terminaison			X	
Liste blanche et liste noire			X	
Monitoring en continu			X	
Vulnerability / Threat Prioritization				X

Tableau 1 : tableau des fonctionnalités

9.6. Déploiement et prise en charge de ces logiciels :

	Ressources d'aide	Déploiement	Formation
ManageEngine Vulnerability Manager Plus	• Service client/e-mail • FAQ/forums • Base de connaissances • Support téléphonique • Service de support 24/7 (réponse directe) • Chat	• Cloud, SaaS, web • Mac (ordinateur) • Windows (ordinateur)	• Formation présentielle • En ligne en direct • Webinaires • Documentation • Vidéos
Syxsense	• Service client/e-mail • FAQ/forums • Base de connaissances • Support téléphonique • Service de support 24/7 (réponse directe) • Chat	• Cloud, SaaS, web • Mac (ordinateur) • Windows (ordinateur) • Linux (ordinateur)	• Formation présentielle • En ligne en direct • Webinaires • Documentation • Vidéos
Netsurion Managed Threat Protection	• Service client/e-mail • FAQ/forums • Base de connaissances • Support téléphonique • Service de support 24/7 (réponse directe) • Chat	• Cloud, SaaS, web • Mac (ordinateur) • Windows (ordinateur) • Linux (ordinateur) • Windows (sur site) • Linux (sur site) • Chromebook	• Formation présentielle • En ligne en direct • Webinaires • Documentation • Vidéos

		(ordinateur) • Android (mobile) • iPhone (mobile) • iPad (mobile)	
Intruder	• Service client/e-mail • FAQ/forums • Base de connaissances • Chat	Cloud, SaaS, web	• En ligne en direct

Tableau 2 : tableau de déploiement et prise en charge

10. Conclusion:

En fin de compte, la mesure de la préparation d'une organisation à faire face aux vulnérabilités dépend de la solidité de son programme de sécurité, des politiques qui régissent la gestion des vulnérabilités, ainsi que de la réactivité et du respect des politiques de l'organisation.

Au fil de e chapitre, nous avons fait une étude préalable sur la veille sécuritaire et le processus de la gestion de vulnérabilités. Dans le deuxième chapitre, nous allons parler sur l'organisation d'accueil ELIT.

Chapitre II: Présentation de l’organisme d’accueil

1. Introduction :

Dans ce chapitre nous allons faire une petite présentation sur l'entreprise ELIT, plus tôt sur la direction sécurité des systèmes d'informations.

2. L'entreprise ELIT :

El Djazair information technology"ELIT" est une société algérienne comptant plus de 300 ingénieurs informaticiens, plus de 40 clients et des infrastructures hautement disponibles et sécurisées.

Au-delà des aspects reconnus au domaine IT, les réseaux informatiques, le développement des sites web, la messagerie électronique, etc., ELIT assure la sécurité des systèmes d'information via une plateforme de sécurité à la pointe de la technologie et ce, avec une ressource humaine 100% algérienne.**[15]**

3. Organisation de la direction Sécurité des systèmes d'information:

ELIT dispose d'une Direction Sécurité des Systèmes d'information pour veiller à préserver le capital informationnel du groupe Sonelgaz et améliorer le niveau de sécurité des données ainsi que garantir l'intégrité, la confidentialité, la disponibilité et la traçabilité des systèmes d'information de l'entreprise.

Elle se compose de trois départements :

3.1. Département normes et conformité qui compte:

- des ingénieurs sécurité chargé des normes et de la conformité.
- des ingénieurs sécurité chargé de l'audit.
- des ingénieurs sécurité chargé de la veille technologique.

3.2. Département réseaux et infrastructure qui compte :

- des ingénieurs sécurité chargé des réseaux.
- des ingénieurs sécurité chargé des infrastructures.

3.3. Département systèmes et données qui compte :

- des ingénieurs sécurité chargé des systèmes.
- des ingénieurs sécurité chargé des données et applications.

4. Les rôles de direction sécurité des systèmes d'informations (DSSI):

Cette direction est chargée de :

- ✓ Assurer une veille technologique constante dans le domaine SSI .
- ✓ Réaliser des audits de SSI.

- ✓ Identifier les besoins et les risques informatiques empêchant le bon fonctionnement de l'entreprise.
- ✓ Mettre en œuvre la stratégie SSI groupe Sonelgaz et veiller au respect de la politique de sécurité.
- ✓ Etablir et maintenir la politique de sécurité du Groupe Sonelgaz et veiller à son application
- ✓ Sensibiliser les différents acteurs des SI sur la SSI.
- ✓ Surveiller et détecter les vulnérabilités du SI .

5. La Réalisation :

Pour la réalisation des missions, DSSI a attribué des missions à chacun de ses composantes.

5.1. Missions de département de normes et conformité :

- ✓ L'élaboration d'un référentiel de sécurité des documents applicable au niveau de groupe SONELGAZ, ainsi que sa mise en œuvre, le contrôle de son application et de veiller à son évolution.
- ✓ La réponse aux exigences de sécurité au niveau du groupe SONELGAZ.
- ✓ La veille juridique.
- ✓ La veille sécuritaire.
- ✓ La gestion des vulnérabilités.
- ✓ La réalisation des audits de conformité.
- ✓ La classification et la gestion des risques SI.

Pour que le département puisse accomplir ses missions il doit faire :

- Elaboration un document « politique de sécurité des systèmes d'information »et veiller a son évolution.
- Rédaction des procédures techniques et de gestions de sécurité des systèmes d'information.
- Définir les critères de diffusion externe des informations.
- Elaboration d'un plan gestion des incidents.
- Rédaction des chartes d'usages des ressources informatique.
- Identifier et classer les actifs qui ont une importance en termes de sécurité.
- Communication des référentielles sécurités des systèmes d'information.
- Mettre en place des moyens de contrôle de l'application de la politique de sécurité au niveau du groupe SONELGAZ.
- Rédaction des procédures d'audits sécurité des SI.
- Réalisation d'audits sécurité aux niveau des directions et filiales du groupe SONELGAZ.
- Proposition de solutions de sécurité applicables.
- Proposition de livres, documents…etc. ayant trait la sécurité des systèmes d'information.

5.2. Missions de département de réseaux et infrastructures :

Ce département doit veiller a la sécurité des moyens de communications et la sécurité physiques des SI.

Pour cela il faut:

- Elaborer des procédures de contrôles.
- Configurer les équipements techniques et vérifier la bonne configuration des routeurs et Switch.
- Détecter les vulnérabilités des réseaux et traiter les attaques .
- Etablir les normes et contrôler la conformité des salles hébergeant les serveurs ainsi que leurs procédures d'accès.
- Appliquer la politique de sécurité dans les réseaux et les infrastructures.
- Participer dans l'élaboration des CDC sur les réseaux ainsi que sur la construction des sites abritant des plateformes importantes.
- Contribuer dans le choix de l'architecture réseaux et l'emplacement physique des équipements informatique.
- Empêcher les accès non autorisés depuis des réseaux publics (Internet, réseau téléphonique).

5.3. Missions de département systèmes et données :

- ✓ Veiller aux droits d'accès aux données et ressources d'un système.

Pour que le département puisse accomplir ses missions il doit :

- Participer dans l'élaboration des CDC pour l'acquisition ou le développement de SI.
- Contrôler la sécurité des applications informatique avant leurs mises en production.
- Elaboration d'un standard de programmation pour la prise en charge des règles de sécurité applicative.
- Définir les règles de haute disponibilité des serveurs.
- Elaborer une stratégie et des procédures de sauvegardes.
- Mettre en place un système d'authentification.
- Elaboration des procédures de gestion des mots du passe des serveurs.
- Participer au choix, achat et réception des serveurs pour la vérification de leur conformité.
- Veiller à la MAJ des dernières versions des correctifs ou des OS.
- Définir et diffuser les standards de sécurisation pour la configuration des serveurs.
- Sensibiliser les utilisateurs sur les risques.

6.Le processus existant au niveau d'ELIT:

Au niveau de département de sécurité d'ELIT , ils n'utilisent pas ce genre de logiciel qui font la détection des vulnérabilités et l'application de correctif automatiquement ,par contre ils utilisent la gestion des bulletins de vulnérabilités.

La gestion des bulletins de vulnérabilités sur ELIT VEILLE se faisait manuellement en utilisant des fichiers word, ce qui provoquait :

- Le non suivi des bulletins.
- La non traçabilité du processus.
- La perte de temps.
- La perte de ressource.

Pour cela, ils veulent faire l'automatisation de ce processus de la veille sécuritaire de la société.

7. Conclusion :

Pour terminer, ELIT est une société Spécialisée dans les technologies de l'information et de la communication.

Dans ce chapitre, nous avons présenté quelques aspects concernant notre organisme d'accueil.

Dans le prochain chapitre,On va faire la conception, la présentation des objectifs et des fonctionnalités de l'application et utiliser l'UML (les diagrammes de séquences, cas d'utilisation etc…).

Chapitre III : Conception

1. Introduction

Nous arrivons dans ce chapitre à la partie qui concerne la conception de notre Solution. Pour cela nous allons utiliser la méthode de conception UML. Au cours de ce chapitre, nous allons tout d'abord établir la spécification et l'analyse des besoins pour voir par la suite, la partie conception avec les différents diagrammes d'UML.

2. L'automatisation du processus d'ELIT :

Notre travail est d'avoir une solution Web qui automatise le processus de la veille sécuritaire depuis le recensement de l'actif à protéger, l'identification de la vulnérabilité touchant l'actif jusqu'au traitement de cette dernière.
. Notre application doit avoir :

- ✓ Une partie de gestion des actifs de sécurité (création, Màj, suppression ...) avec la possibilité de l'alimentation des actifs à partir des fichiers excel.
- ✓ Une partie de gestion des bulletins de vulnérabilités (création, envoie, suivi des bulletins).
- ✓ Une partie pour l'affichage des statistiques sur les vulnérabilités touchant la société.
- ✓ Un mécanisme d'authentification.
- ✓ Un manuel d'exploitation des espaces utilisateurs.

3. La procédure de La gestion des bulletins des vulnérabilités :

La procédure de la gestion de vulnérabilité implique 4 principaux intervenants au niveau du groupe Sonelgaz :

- Responsable de la veille.
- Veilleur (administrateur de l'outil).
- Auditeur.
- Interlocuteur (Propriétaire de l'actif).

Il faut bien définir le rôle et la responsabilité pour chacun pour le bon fonctionnement de l'activité de gestion des vulnérabilités.

4. Définition des rôles et responsabilités :

- **Responsable de la veille:** est un responsable de la Direction Sécurité des SI qui est responsable de la gestion de l'activité de la veille.
- **Veilleur:** est désigné par le responsable de veille, sa mission est d'analyser l'existant, de collecter et de diffuser l'information pertinente sur les vulnérabilités ainsi que l'administration et l'exploitation de l'outil Elit- Veille. Il doit savoir :

- ✓ Construire une méthodologie de recueil et d'analyse des événements de sécurité.
- ✓ Renseigner la base de données par des actifs SI à jour et des sites fiables de sécurité
- ✓ Communiquer dans les délais les résultats de la veille aux bons destinataires.
- ✓ Posséder des connaissances techniques liées à la sécurité informatique.
- ✓ Le sens toujours en éveil et avoir une forte réactivité.

- **Auditeur:**est responsable de la vérification du prix en charge de la découverte par l'interlocuteur.
- **Interlocuteurs (Propriétaires des actifs):**Sont les responsables des systèmes ou administrateurs des applications qui ont comme responsabilité la prise en charge des vulnérabilités.

Pour le déroulement de cette procédure il faut avoir :

- ✓ le Canevas de recensement des actifs.
- ✓ Le Bulletin de vulnérabilités.
- ✓ Le Rapport d'audit.
- ✓ Le Manuel d'utilisation de l'outil de veille.

5. Séquencement des phases :

Le processus de gestion de vulnérabilités se fait en cinq étapes principales :

5.1. Recensement des Actifs:cette phase consiste au catalogage de l'existant, des actifs, des ressources du système d'information ainsi que les sources affichant les vulnérabilités sur les actifs

5.2. Collecte des vulnérabilités:se fait au niveau de deux activités différentes qui sont :

- **Veille sécuritaire:** l'outil de veille permet de rechercher les vulnérabilités qui touchent les actifs insérés dans la base de données des actifs par la voie des flux RSS .
- **Les audits:** les audits permettent aux auditeurs de déceler les vulnérabilités sur les systèmes et les applications.

5.3.Analyse des vulnérabilités: On peut définir le niveau de critique d'une vulnérabilité par deux moyens qui sont la matrice de risque pour les vulnérabilités provenant de l'activité de veille ou sera calculé directement par l'outil d'audit dans le cas d'activité d'audit.

Etude et analyse des vulnérabilités de la veille:

Après la détection de vulnérabilité, le veilleur doit analyser la criticité de la vulnérabilité qui doit être évaluée par rapport à sa probabilité d'occurrence et son impact métier.

		Probabilité d'occurrence		
		Faible	Moyen	Elevé
Impact métier	Elevé	Moyenne	Elevé	Très élevé
	Moyen	Faible	Moyenne	Elevée
	Faible	Faible	Faible	Moyenne

Tableau 3 : tableau de la criticité de la vulnérabilité

Délais de résolution de la vulnérabilité suivant son niveau de critique:

Criticité de la vulnérabilité	Détails
Extrême	Doit être traitée dans les 72 heures jours après sa découverte
Elevée	Doit être traitée dans les 7 jours après sa découverte
Moyenne	Doit être traitée dans les 30 jours après sa découverte
Faible	Doit être traitée dans les 60 à 90 jours après sa découverte

Tableau 4 : tableau de délais de résolution de la vulnérabilité

5.4. Test et application des correctifs :

a. Test du correctif de la vulnérabilité :

Après avoir le bulletin de vulnérabilités ou le rapport d'audit renseigné par le veilleur où l'auditeur, l'interlocuteur doit tester le fonctionnement du correctif[1] dans un environnement de test avant de l'appliquer dans l'environnement de production.

b. Application du correctif de la vulnérabilité :

Après le test, l'interlocuteur passe à l'application des correctifs sur l'environnement de production et renseigne le bulletin de vulnérabilité pour l'envoyer au veilleur dans le cas de veille ou envoi directement un message à l'auditeur s'il s'agit d'un audit.

5.5. Vérification des correctifs : Dans cette étape, l'équipe de sécurité doit vérifier l'application des correctifs de sécurité sur le système touché par la vulnérabilité après la réception du bulletin de vulnérabilité. Une fois les vulnérabilités ont été résolues, une itération du processus est considérée clôturée.

Si le correctif n'est pas appliqué, une autre itération du processus sera exécutée jusqu'à ce que les vulnérabilités ont corrigées.

Il est possible d’avoir des vulnérabilités ne pouvant pas être corrigés pour diverses raisons :

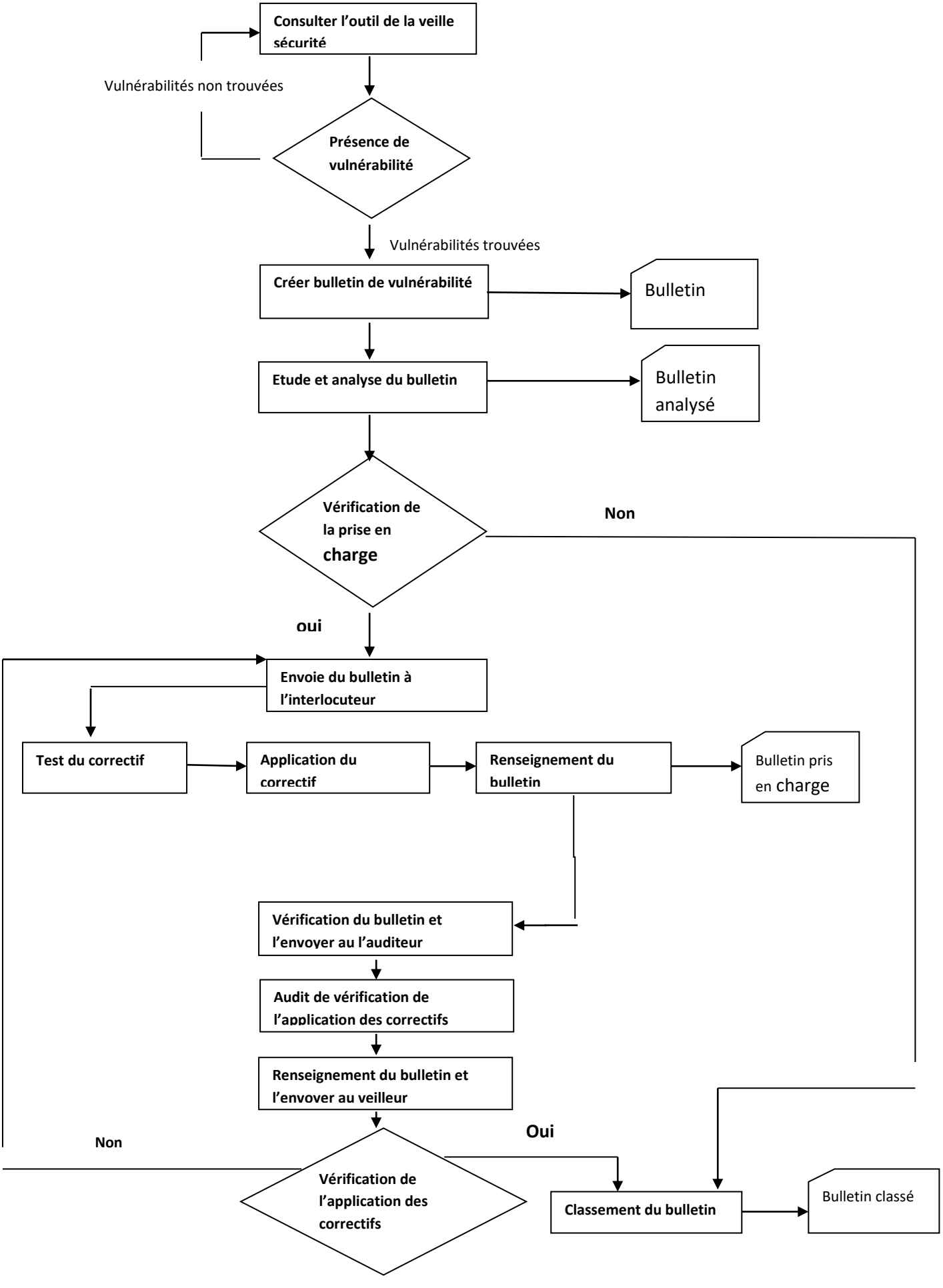
- Ressources humaines ou financières insuffisantes ;

- Correctifs non disponibles ;

- Contraintes techniques spécifiques.

Dans ce cas, les interlocuteurs devront mettre en place des mesures de sécurité palliatives (pour contrôler ou atténuer les risques).

6. Le processus de la gestion des bulletins des vulnérabilités :



Notre processus à développer est comme suit :

1. **consultation de la veille sécuritaire :** c'est le travail du veilleur qui doit récolter l'information de la vulnérabilité touchant l'actif, l'étudier et l'analyser.
2. **Création du bulletin :** c'est le travail du veilleur, quand il trouve une vulnérabilité qui touche un des actifs de la société, il doit créer un bulletin de vulnérabilité.
3. **L'envoie du bulletin à l'interlocuteur :** c'est le travail du veilleur, après la création du bulletin et le remplissage de toutes les informations nécessaires de la vulnérabilité, il doit envoyer le bulletin aux interlocuteurs concernés.
4. **Test et application du correctif :** c'est le travail d'interlocuteur, après la réception de bulletin, il doit tester et appliquer le correctif si c'est possible.
5. **Renseignement et l'envoie du bulletin :** c'est le travail d'interlocuteur, après le test du correctif, il doit écrire sa réponse sur le bulletin (est-ce-qu'il a appliqué le correctif ou non) et l'envoyer par la suite à l'auditeur.
6. **Audit de vérification de l'application des correctifs :** c'est le travail d'auditeur qui va vérifier la prise en charge de la vulnérabilité.
7. **Renseignement du bulletin et l'envoyer au veilleur :** après la vérification d'application du correctif, l'auditeur doit aussi écrire sa réponse sur le bulletin et l'envoyer au veilleur.
8. **Classement du bulletin :** après la réception du bulletin de la part d'auditeur, le veilleur va classer le bulletin par rapport ces trois états :
    - Corrigé : correctif appliqué.
    - Bloqué : correctif non appliqué.
    - A renvoyé: renvoie des bulletins l'interlocuteur.

7. Présentation de notre approche de conception

L'objectif de l'approche orienté objet est de décomposer le système informatique en un ensemble d'objets en interactions. Cette approche objet requiert de modéliser avant de concevoir pour apporter plus de rigueur au système, elle offre aussi une meilleure compréhension des logiciels. Cette démarche se fonde sur des langages de modélisation UML.

Le langage UML est une notion graphique conçue pour représenter, spécifier, construire et documenter les systèmes logiciels. Ses deux principaux objectifs sont la modélisation de systèmes utilisant les techniques orientées objet, depuis la conception jusqu'à la maintenance, et la création d'un langage abstrait compréhensible par l'homme et interprétable par les machines. **[16]**

8. Analyse des besoins

8.1. Besoins fonctionnels:

8.1.1. Pour un interlocuteur :

-Connecter.

-Remplir la base d'actifs.

-Tester et appliquer les correctifs.

-Renseigner et envoyer le bulletin au veilleur.

8.1.2. Pour un veilleur :

-Connecter.

-Détecter les vulnérabilités.

-Créer et renseigner le bulletin.

-Envoyer le bulletin aux interlocuteurs concernés et au veilleur.

8.1.3. Pour un auditeur :

-Connecter.

- Tester la prise en charge des vulnérabilités.

-Renseigner le bulletin.

-Envoyer le bulletin au veilleur.

8.2. Besoins non fonctionnels :

- **Ergonomie :** Design très confortable et élégant.
- **La performance :** Pas d'erreurs.
- **Simplicité :** L'interface doit être simple et lisible.
- **Fiabilité :**Notre application doit garantir la fiabilité de l'utilisation.
- **Rapidité :** Le système doit assurer la rapidité dans la navigation de notre application.
- **Facilité :**La manipulation de notre application doit être facile.

9. Diagramme de cas d'utilisation

9.1. Définition

Les diagrammes de cas d'utilisation permettent d'effectuer l'analyse des besoins du système à concevoir. Ils peuvent aussi être ensuite utilisés comme moyen d'organisation et de structuration de développement du logiciel. **[16]**

Un cas d'utilisation est une description de l'interaction entre les acteurs et le système.

9.2. A-Acteur

Un acteur représente un rôle joué par une personne qui interagit avec le système. Par définition, les acteurs sont à l'extérieur du système et se recrutent parmi les utilisateurs de l'application et aussi parmi les responsables de sa configuration et de sa maintenance. D'où, les acteurs potentiels qui risquent d'interagir avec l'application sont :

- ✓ Client
- ✓ Administrateur

- **Client**

Désigne la personne ou l'entité qui exploite l'application (nos acteurs). Il rentre dans l'interaction du système tel qu'il peut consulter le catalogue des actifs, des vulnérabilités, renseigner bulletin, créer un compte…etc.

- **Administrateur**

C'est lui qui gère l'application de façon régulière, son rôle est :

- Gérer les publicités.
- Faire des mises à jour au niveau de la base de données.
- Gérer les entrés.

9.3. Cas d'utilisation

Un cas d'utilisation (en anglais use case) permet de mettre en évidence les relations fonctionnelles entre les acteurs et le système étudié. Le format de représentation d'un cas d'utilisation est complètement libre mais UML propose un formalisme et des concepts issus de bonnes pratiques. **[16]**

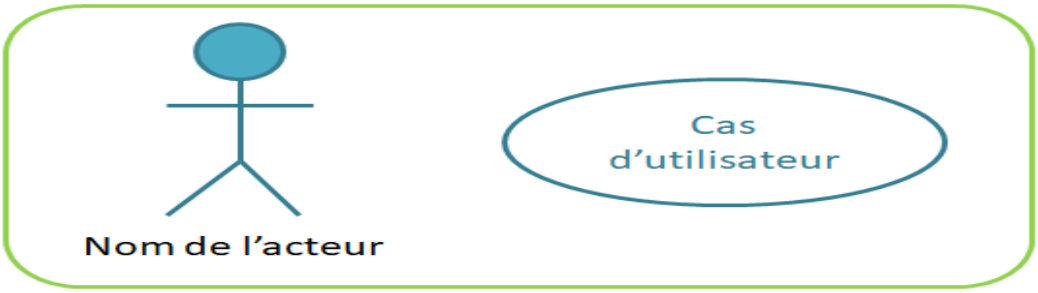


Figure 4 :Eléments d'un diagramme de cas d'utilisation.

9.4. Relations entre cas d'utilisation

Trois types de relation standard entre cas d'utilisation sont proposés par UML :

- **Include :** Le cas d'utilisation incorpore explicitement et de manière obligatoire un autre cas d'utilisation à l'endroit spécifié.
- **Extend :** Le cas d'utilisation incorpore implicitement de manière facultative un autre cas d'utilisation à l'endroit spécifié.
- **Généralisation (héritage)** : les cas d'utilisation descendants héritent des propriétés de leurs parents.

9.5. Représentation des diagrammes de cas d'utilisation

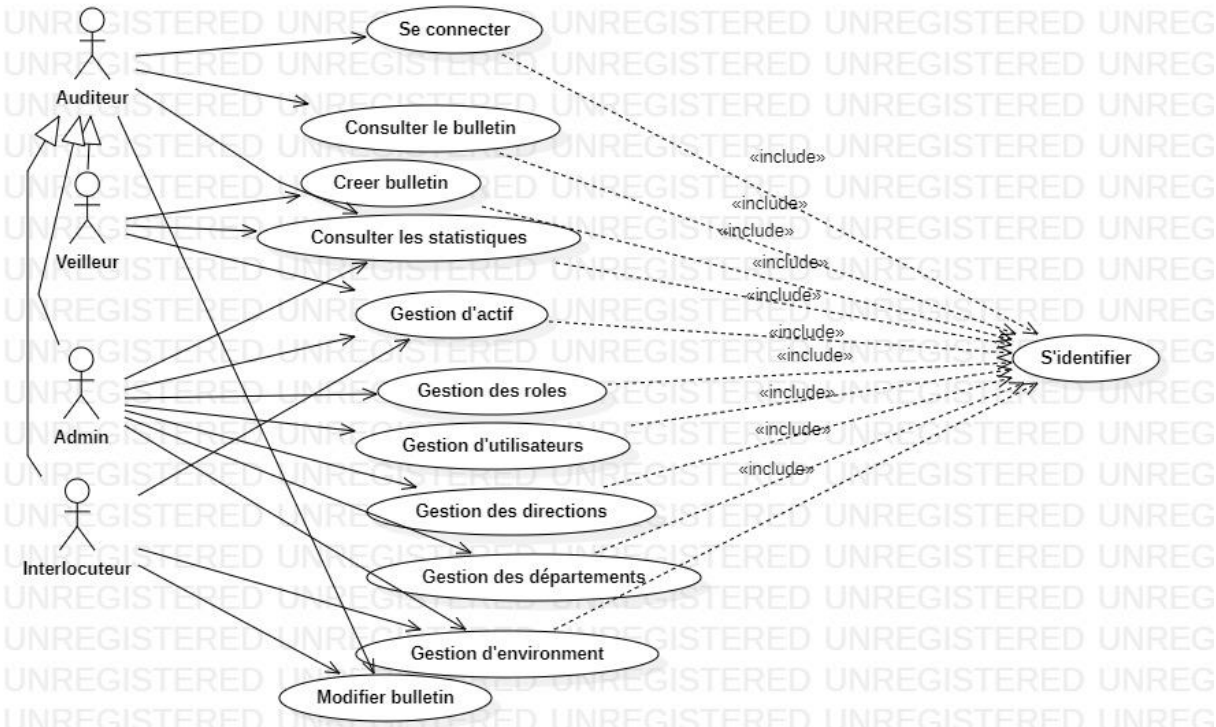


Figure 5 :Diagramme de cas d'utilisation général

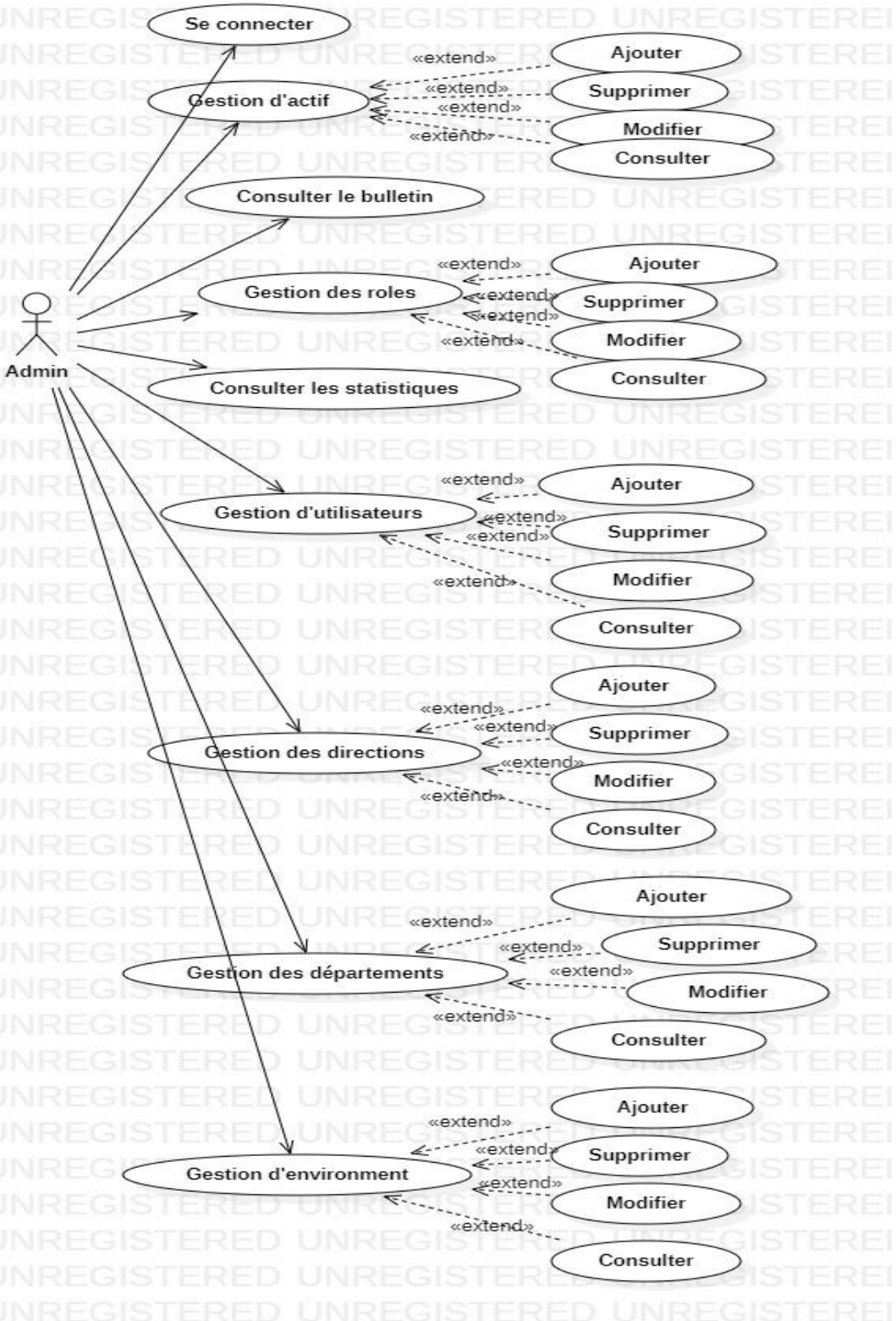


Figure 6 :Diagramme de cas d'utilisation d'admin

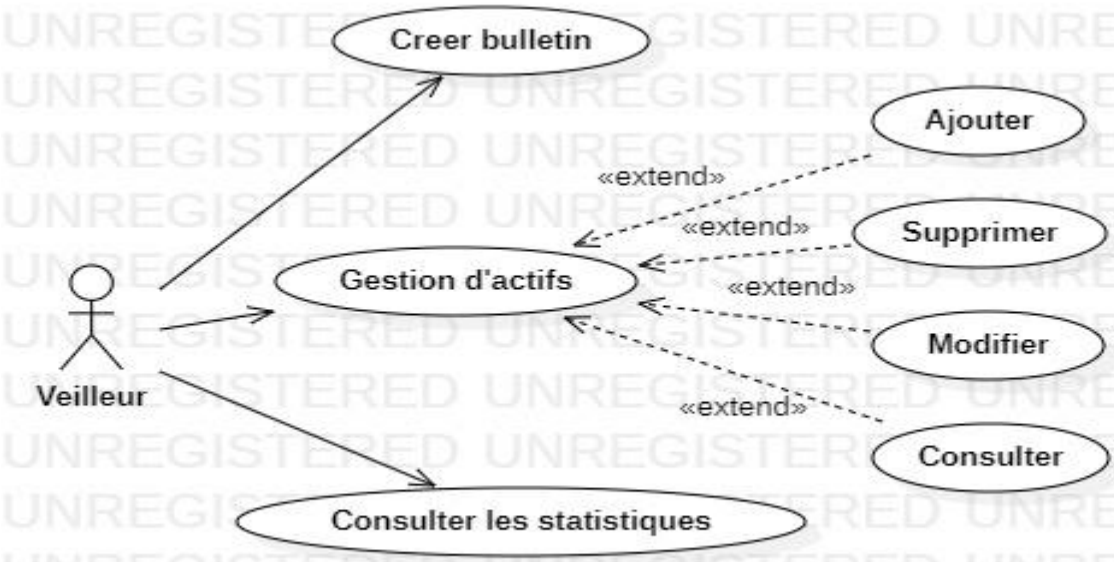


Figure 7 :Diagramme de cas d'utilisation du veilleur

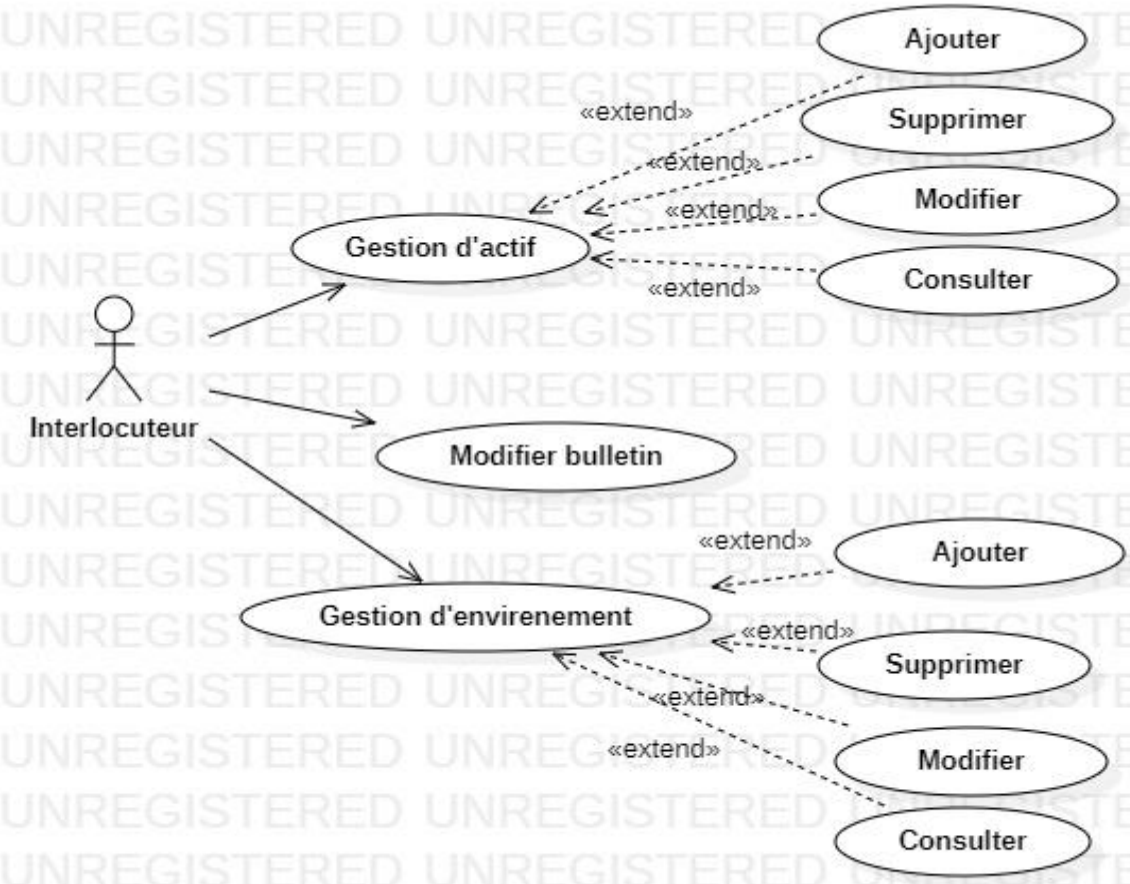


Figure 8 :Diagramme de cas d'utilisation d'interlocuteur

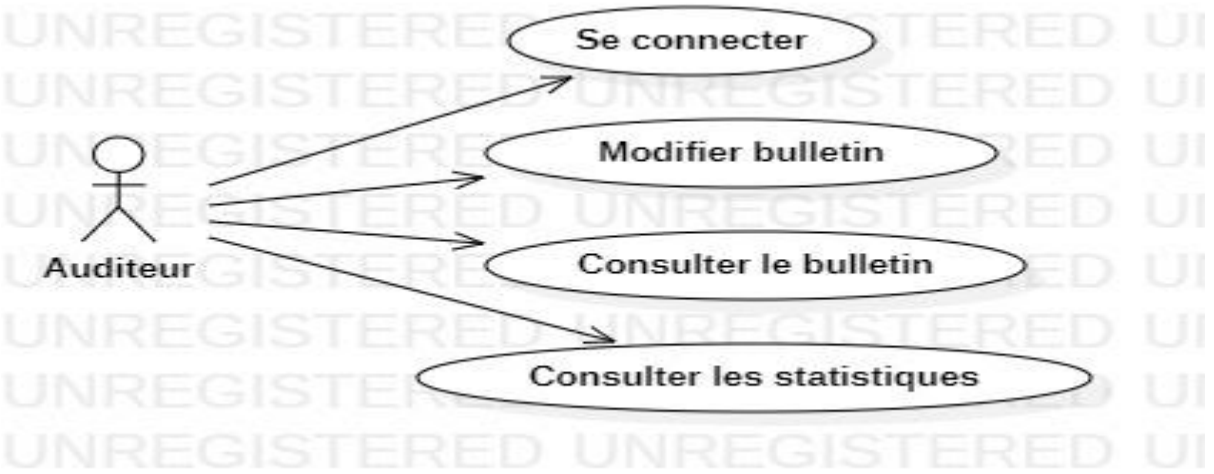


Figure 9 :Diagramme de cas d'utilisation d'auditeur

10. Diagramme de séquence

Un diagramme de séquence est un diagramme d'interaction qui expose en détail la façon dont les opérations sont effectuées : quels messages sont envoyés et quand ils le sont. Les diagrammes de séquences sont organisés en fonction du temps. Le temps s'écoule au fur et à mesure que vous parcourez la page. Les objets impliqués dans l'opération sont répertoriés de gauche à droite en fonction du moment où ils prennent part dans la séquence de message. **[16]**

10.1. Représentation des diagrammes de séquence

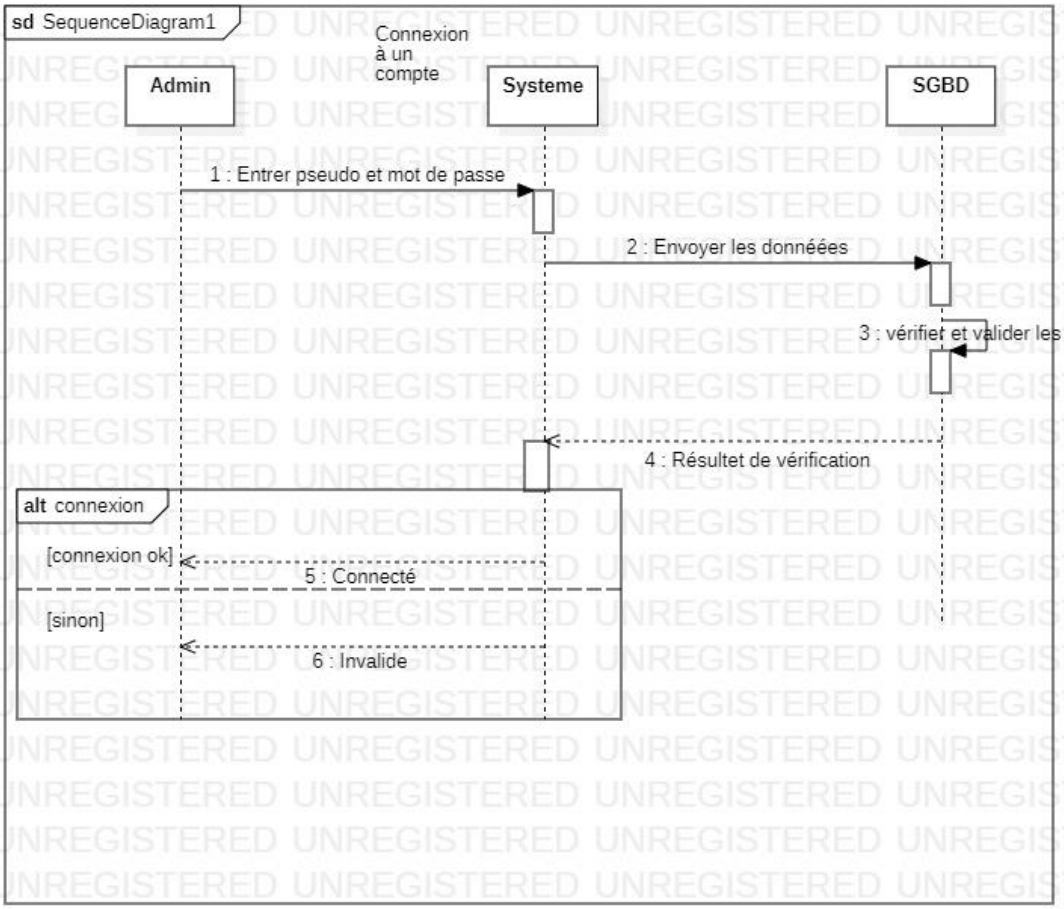


Figure10:Diagramme de séquence de la connexion à un compte

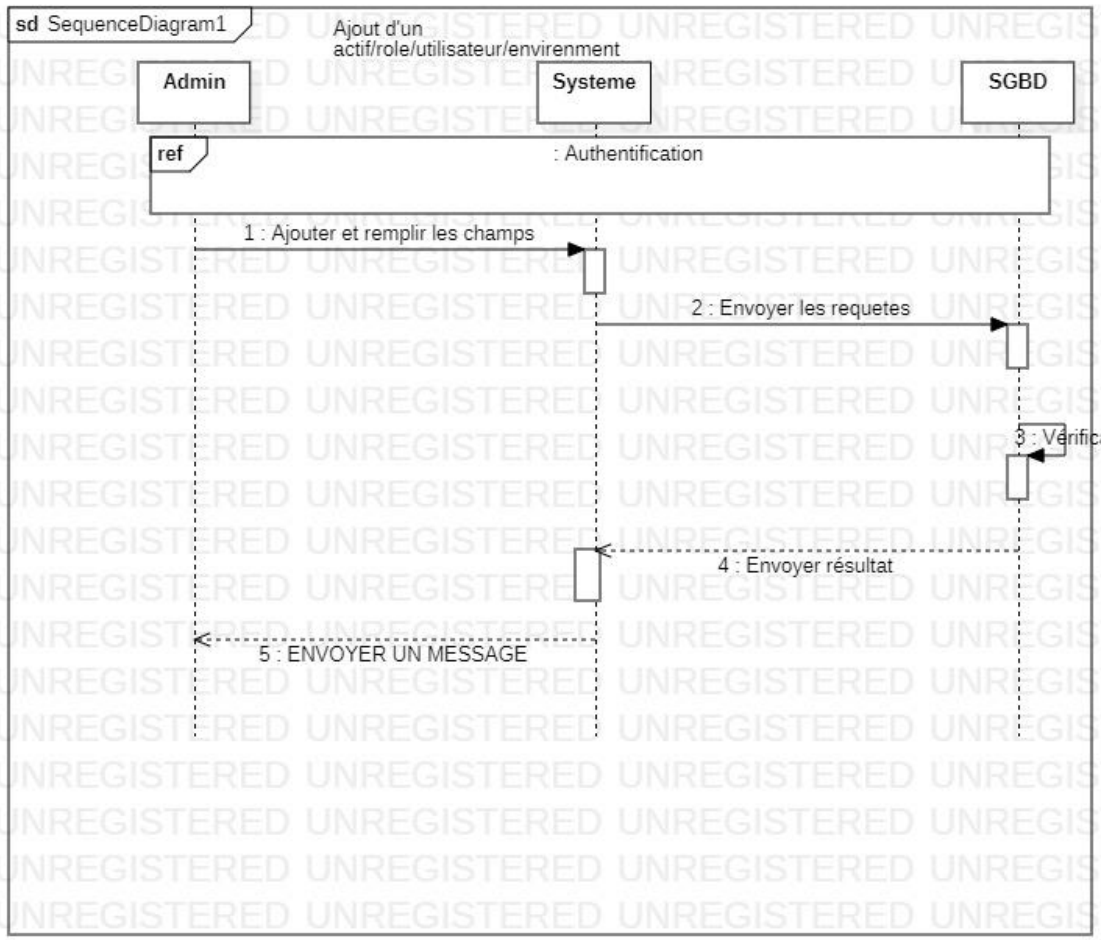


Figure 11 :Diagramme de séquence d'ajout d'un actif/rôle/utilisateur/environnement /département/direction.

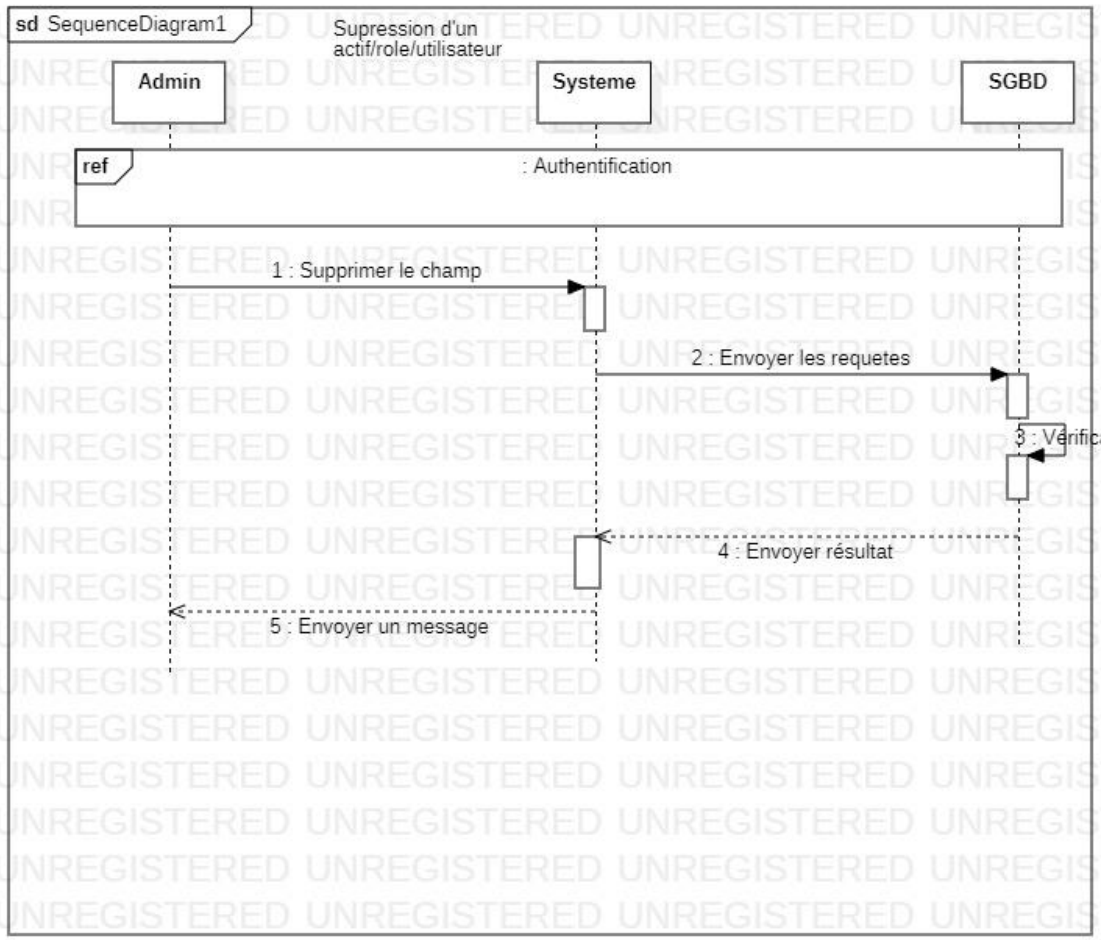


Figure 12 :Diagramme de séquence de la suppression d'un rôle/actif/utilisateur/environnement/département/direction

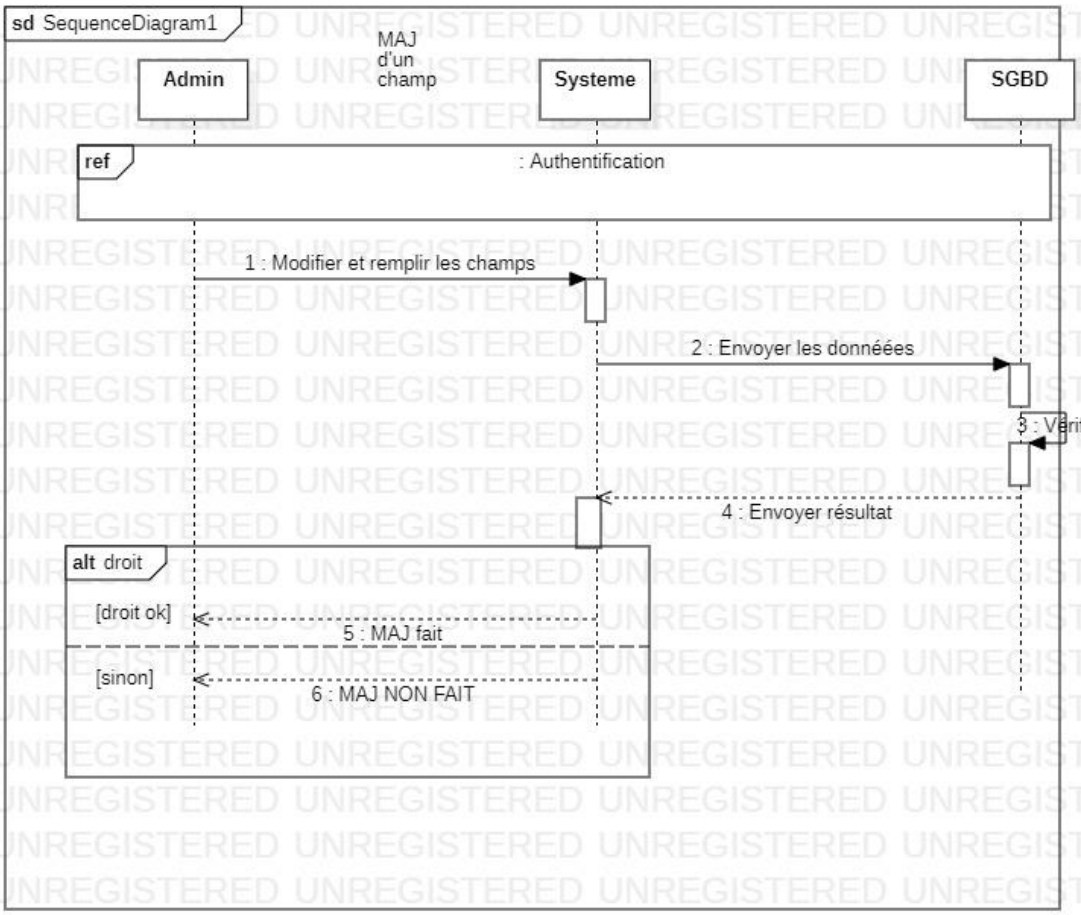


Figure 13 :Diagramme de séquence de la mise à jour d'un champ

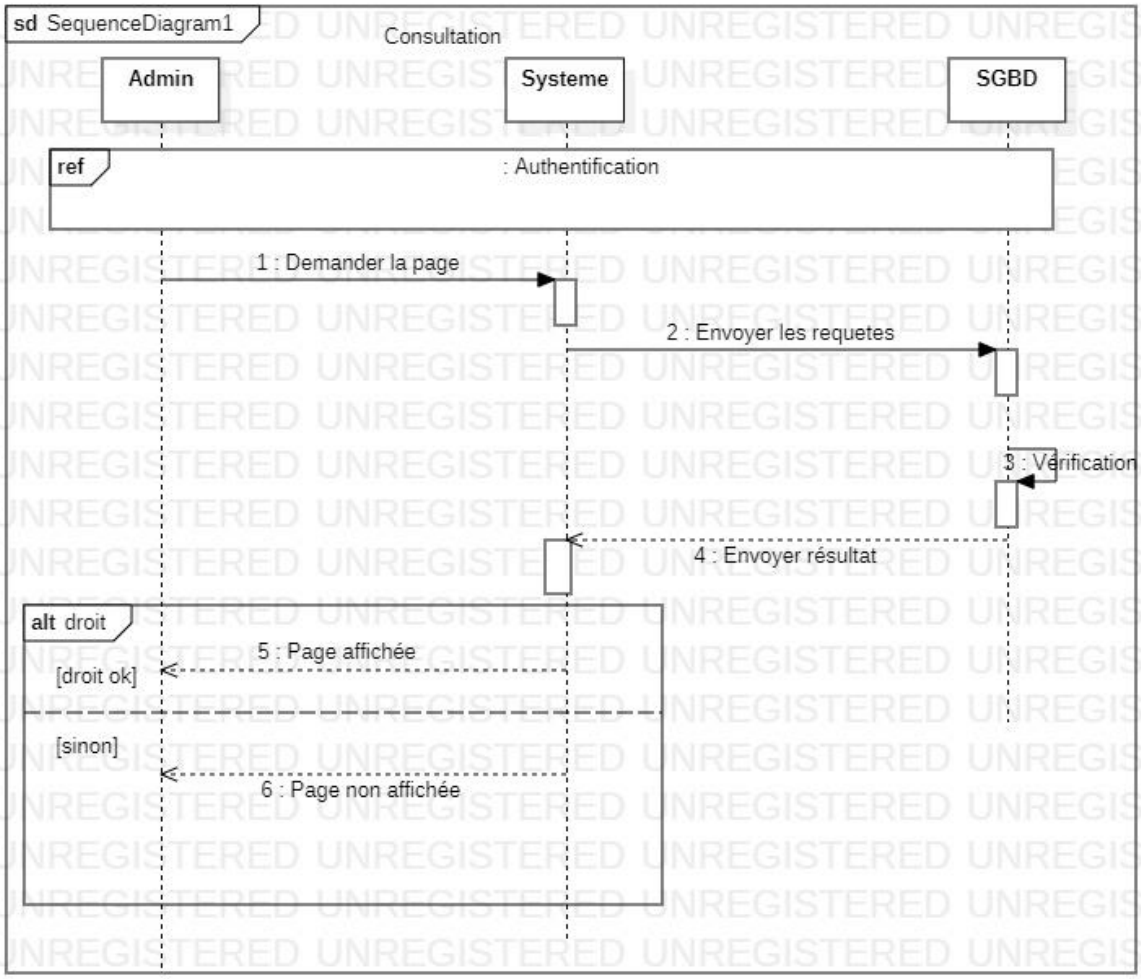


Figure 14 :Diagramme de séquence de la consultation des données.

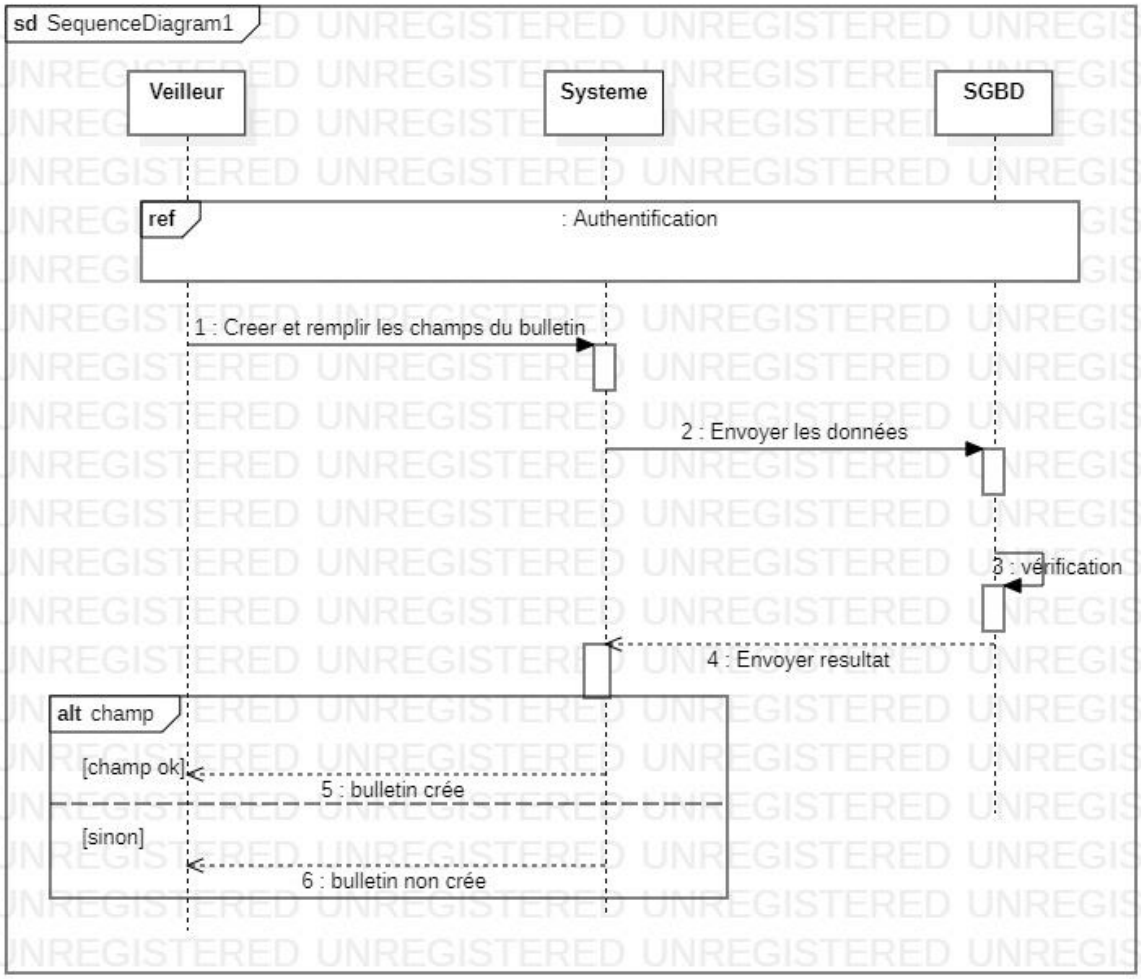


Figure 15:Diagramme de séquence de la création d'un bulletin

11. Diagramme de classe

Un diagramme de classes fournit une vue globale d'un système en présentant ses classes, interfaces et collaborations, et les relations entre elles. Les diagrammes de classes sont statiques : ils affichent ce qui interagit mais pas ce qui se passe pendant l'interaction.

En notation UML, une classe est représentée sous la forme d'un rectangle divisé en plusieurs parties : le nom de la classe, les attributs (champs) et les opérations (méthodes) **: [17]**

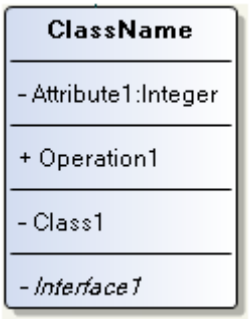


Figure 16 : représentation de la classe

11.1. Représentation de diagramme de classe :

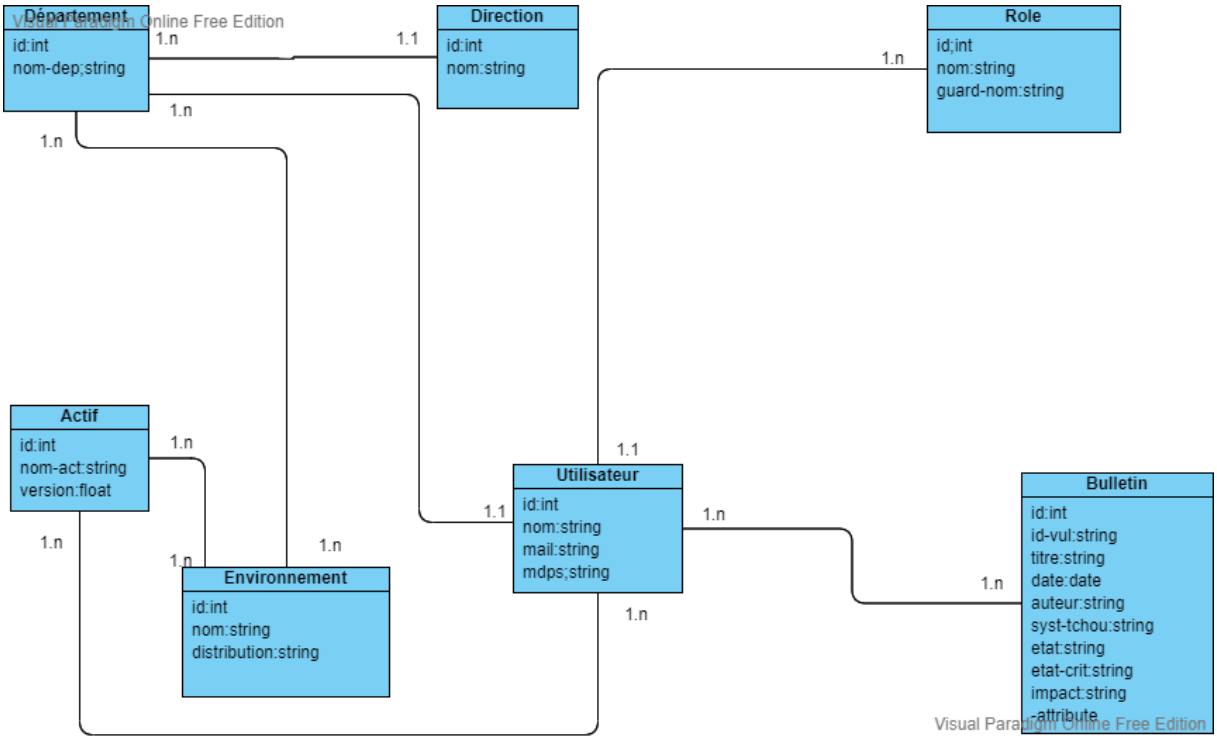


Figure 17 : Diagramme de classe

12. Architecture du système :

L'outil fondamental de la gestion de ce projet est Framework nommé «LARAVEL » gérant une base de données sous « MySQL ».

Nous avons proposé l'architecture de notre application comme suit :

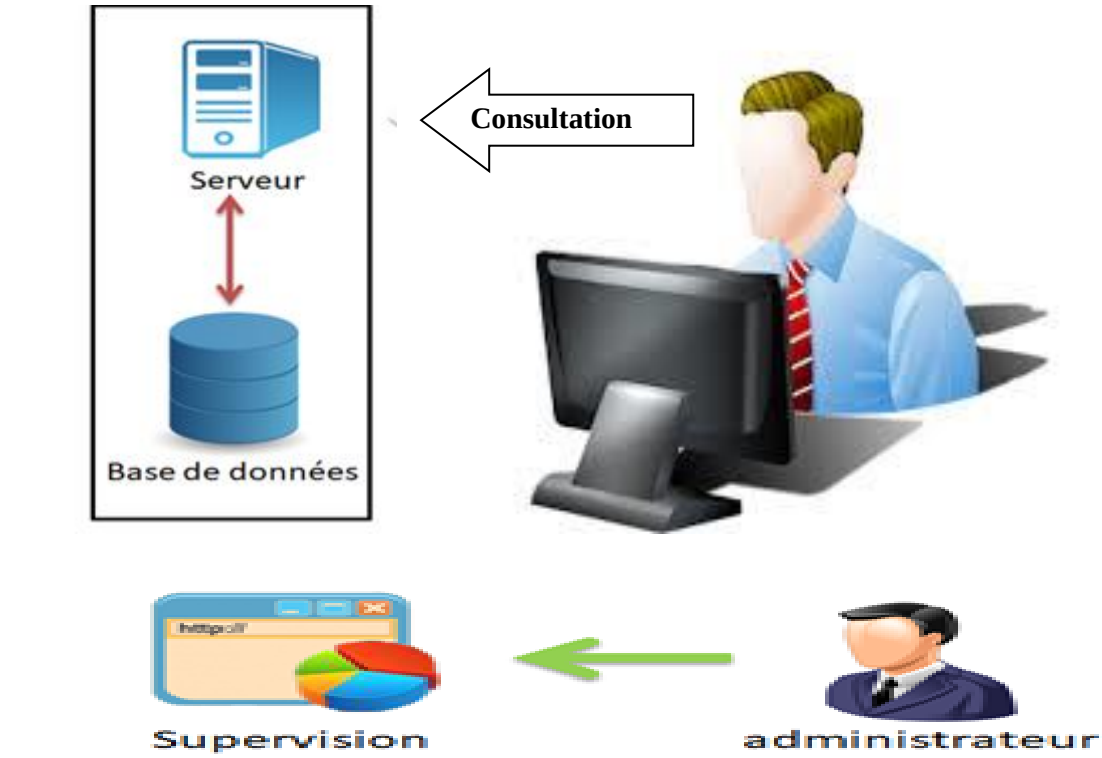


Figure 18 : Architecture du système

13. Conclusion

Au fil de ce chapitre, nous avons fait une présentation de notre conception en passant par les objectifs et les fonctionnalités de l'application et nous avons fini par le passage au modèle relationnel. Dans le chapitre suivant, nous nous intéresserons à la réalisation de ce qui a été présenté dans ce chapitre.

Chapitre IV : Développement et implémentation

1. Introduction

Dans cette partie, nous allons détailler les étapes du développement du site, le choix des outils dans un premier temps ainsi que les démonstrations des interfaces de notre application et les déférentes fonctionnalités des utilisateurs.

2. Les outils utilisés :

2.1. XAMP Server :

Est un ensemble de logiciels permettant de mettre en place facilement un serveur web local, un serveur FTP et un serveur de messagerie électronique**. [18]**

2.2. Visual Studio Code :

Est un éditeur de code source conçu par Microsoft pour Windows, Linux et macOS. Les fonctionnalités incluent la prise en charge du débogage, de la mise en évidence de la syntaxe, de la complétion intelligente du code, des extraits de code, de la refactorisation du code et de Git intégré. Il peut être utilisé avec une variété de langages de programmation, notamment Java, JavaScript, Go, Node.js, Python et C++.

Au lieu d'un système de projet, il permet aux utilisateurs d'ouvrir un ou plusieurs répertoires, qui peuvent ensuite être enregistrés dans des espaces de travail pour une réutilisation future. Cela lui permet de fonctionner comme un éditeur de code indépendant de la langue pour n'importe quelle langue. Il prend en charge un certain nombre de langages de programmation et un ensemble de fonctionnalités qui diffèrent selon le langage.**[19]**

2.3.Laravel :[20]

Est un Framework d'application Web avec une syntaxe expressive et élégante écrit en PHP.Laravel tente de simplifier le développement en facilitant les tâches courantes utilisées dans la majorité des projets Web, telles que l'authentification, le routage, les sessions et la mise en cache.

Laravel vise à rendre le processus de développement agréable pour le développeur sans sacrifier les fonctionnalités de l'application.il fournit des outils puissants nécessaires pour des applications volumineuses et robustes.

On peut difficilement parler d'un Framework sans évoquer :

a.MVC (Modèle-Vue-Contrôleur):

C'est un modèle d'organisation du code :

- Le modèle est chargé de gérer les données.
- La vue est chargée de la mise en forme pour l'utilisateur.
- Le contrôleur est chargé de gérer l'ensemble.

En général on résume en disant que le modèle gère la base de données, la vue produit les pages HTML et le contrôleur fait tout le reste.

Dans Laravel :

- Le modèle correspond à une table d'une base de données. C'est une classe qui étend la classe Model qui permet une gestion simple et efficace des manipulations de données et l'établissement automatisé de relations entre tables.
- Le contrôleur se décline en plusieurs catégories : contrôleur classique, contrôleur RESTfull et contrôleur de ressource.
- La vue est soit un simple fichier avec du code HTML, soit un fichier utilisant le système de template Blade de Laravel.

b.ORM Eloquent :

Le Framework PHP Laravel est fourni avec Eloquent Object Relational Mapper (ORM), qui fait référence à une implémentation avancée du PHP Active Record Pattern, ce qui facilite l'interaction avec la base de données de l'application. Comme les développeurs doivent créer des sites Web complexes et d'autres applications, ils préfèrent un temps de développement plus court. Les exigences commerciales variables sont traitées avec un développement plus rapide, ainsi qu'un code bien organisé, réutilisable, maintenable et évolutif. Il fonctionne avec des applications Web personnalisées car il peut gérer plusieurs bases de données et effectuer des opérations de base de données courantes.

Les développeurs peuvent travailler efficacement dans Eloquent avec plusieurs bases de données à l'aide d'une implémentation ActiveMethod. Il s'agit d'un modèle architectural où le modèle créé dans la structure Modèle-Vue-Contrôleur (MVC) correspond à une table dans la base de données.

L'avantage est que les modèles effectuent des opérations de base de données courantes sans coder de longues requêtes SQL. Les modèles permettent l'interrogation de données dans vos tables, ainsi que l'insertion de nouveaux enregistrements dans les tables. Le processus de synchronisation de plusieurs bases de données s'exécutant sur différents systèmes est simplifié. Il n'est pas du tout nécessaire d'écrire des requêtes SQL. Tout ce que vous avez à faire est de définir les tables de la base de données et les relations entre elles, et Eloquent fera le reste du travail.

c. Json

Est un format de fichier standard ouvert et un format d'échange de données qui utilise du texte lisible par l'homme pour stocker et transmettre des objets de données constitués de paires attribut-valeur et de tableaux (ou d'autres valeurs sérialisables). C'est un format de données très courant, avec une gamme variée d'applications, un exemple étant les applications Web qui communiquent avec un serveur.

JSON est un format de données indépendant de la langue. Il est dérivé de JavaScript, mais de nombreux langages de programmation modernes incluent du code pour générer et analyser des données au format JSON. **[21]**

d.Middleware :

Le middleware agit comme un pont entre une demande et une réponse. C'est un type de mécanisme de filtrage. Par exemple, Laravel inclut un middleware qui vérifie que l'utilisateur de votre application est authentifié. Si l'utilisateur n'est pas authentifié, le middleware redirigera l'utilisateur vers l'écran de connexion de votre application. Cependant, si l'utilisateur est authentifié, le middleware permettra à la demande de continuer dans l'application. Et comme un autre exemple il permet de filtrer les sessions si un client se connecter et il veut accéder a l'espace d'un autre rôle comme « administrateur » ,le middleware ne le permet pas d'accéder car c'est un espace réservé juste pour l'administrateur . et ça permet de réduire le risque pour la sécurité.

Un middleware supplémentaire peut être écrit pour effectuer diverses tâches en plus de l'authentification. Par exemple, un middleware de journalisation peut journaliser toutes les demandes entrantes dans votre application. Il existe plusieurs middleware inclus dans le Framework Laravel, y compris un middleware pour l'authentification et la protection CSRF.**[22]**

e. Csrf :

La forme complète de CSRF est Cross-Site RequestForgery. Il s'agit d'un type d'attaque en ligne dans lequel l'attaquant envoie des demandes en tant qu'utilisateur autorisé à un système en obtenant des informations d'accès d'un utilisateur particulier de ce système et effectue différents types d'activités malveillantes en utilisant l'identité de cet utilisateur.

L'impact de cette attaque dépend des privilèges de la victime sur le système. Si la victime est un utilisateur normal, cela affectera uniquement les données personnelles de la victime. Mais si la victime est l'administrateur du système, l'attaquant peut endommager l'ensemble du système. Les utilisateurs de n'importe quel site Web d'entreprise, les réseaux sociaux peuvent être affectés par cette attaque. Cette attaque peut être facilement évitée en utilisant la protection Laravel CSRF pour rendre le système plus sécurisé. il génère automatiquement des jetons CRSF pour chaque session utilisateur active. Ces jetons vérifient que les opérations ou demandes sont envoyées par l'utilisateur authentifié concerné.**[23]**

2.4 Bootstrap :

Est une collection d'outils utiles à la création du design (graphisme, animation et interactions avec la page dans le navigateur, etc.) de sites et d'applications web. C'est un ensemble qui contient des codes HTML et CSS, des formulaires, boutons, outils de navigation et autres éléments interactifs, ainsi que des extensions JavaScript en option. C'est l'un des projets les plus populaires sur la plate-forme de gestion de développement GitHub.**[24]**

3. Procédure d’exécution :[25]

1. Le point d'entrée pour toutes les requêtes vers une application Laravel est le fichier public/index.php. Toutes les requêtes sont dirigées vers ce fichier par la configuration de votre serveur web (Apache / Nginx).

2. Le fichier index.php charge la définition du chargeur automatique générée par Composer, puis récupère une instance de l'application Laravel à partir de bootstrap/app.php. La première action entreprise par Laravel lui-même est de créer une instance du conteneur d'application / service.

3.la demande entrante est envoyée au noyau HTTP ou au noyau de la console, selon le type de demande qui entre dans l'application.

4. Le noyau HTTP étend la classe Illuminate\Foundation\Http\Kernel, qui définit un tableau d'amorceurs qui seront exécutés avant l'exécution de la requête. Ces amorceurs configurent la gestion des erreurs, configurent la journalisation, détectent l'environnement d'application et effectuent d'autres tâches qui doivent être effectuées avant que la demande ne soit réellement traitée.

5.Le noyau HTTP définit également une liste de middleware HTTP que toutes les requêtes doivent traverser avant d'être traitées par l'application. Ces middleware gèrent la lecture et l'écriture de la session HTTP, déterminent si l'application est en mode maintenance, vérifient le jeton CSRF, etc.

6.La signature de méthode pour la méthode handle du noyau HTTP est assez simple : elle reçoit une requête et renvoie une réponse. Considérez le noyau comme une grande boîte noire qui représente l'ensemble de votre application. Nourrissez-le de requêtes HTTP et il renverra des réponses HTTP.

7.L'une des actions d'amorçage du noyau les plus importantes est le chargement des fournisseurs de services pour votre application. Tous les fournisseurs de services de l'application sont configurés dans le tableau des fournisseurs du fichier de configuration config/app.php.

8.L'un des fournisseurs de services les plus importants de votre application est App\Providers\RouteServiceProvider. Ce fournisseur de services charge les fichiers de route contenus dans le répertoire de routes de l’application.

9.Une fois que la méthode de route ou de contrôleur renvoie une réponse, la réponse reviendra vers l'extérieur via le middleware de la route, donnant à l'application la possibilité de modifier ou d'examiner la réponse sortante.

4. Procédure de travail :

L’application donne des fonctionnalités à 4 utilisateurs qui sont:

A.Interlocuteur :

L’application affiche une page qui contient un menu où l’interlocuteur :

1. va remplir ses actifs et ses environnements.

2. recevoir et renseigner le bulletin.

3. appliquer le correctif.

4. envoyer le bulletin à l’auditeur.

B.Veilleur :

L’application affiche une page qui contient un menu où le veilleur:

1. va créer les bulletins.

2. renseigner le bulletin.

3. envoyer le bulletin aux interlocuteurs concernés.

4. recevoir le bulletin et les classer.

C.Auditeur :

L’application affiche une page qui contient un menu où l’auditeur:

1. va recevoir le bulletin.

2. vérifier l’application des correctifs.

3. envoyer le bulletin au veilleur.

D.Admin :

L’application affiche une page qui contient un menu où l’admin :

1. peut gérer les utilisateurs.

2. gérer les actifs.

3. gérer les environnements.

4. consulter tous ce qu’il ya dans la base de donnée.

5. Implémentation :

Dans cette partie, nous allons détailler notre application en présentant les différentes fonctionnalités proposées.

Lors du lancement de l'application, la page principale s'affiche :

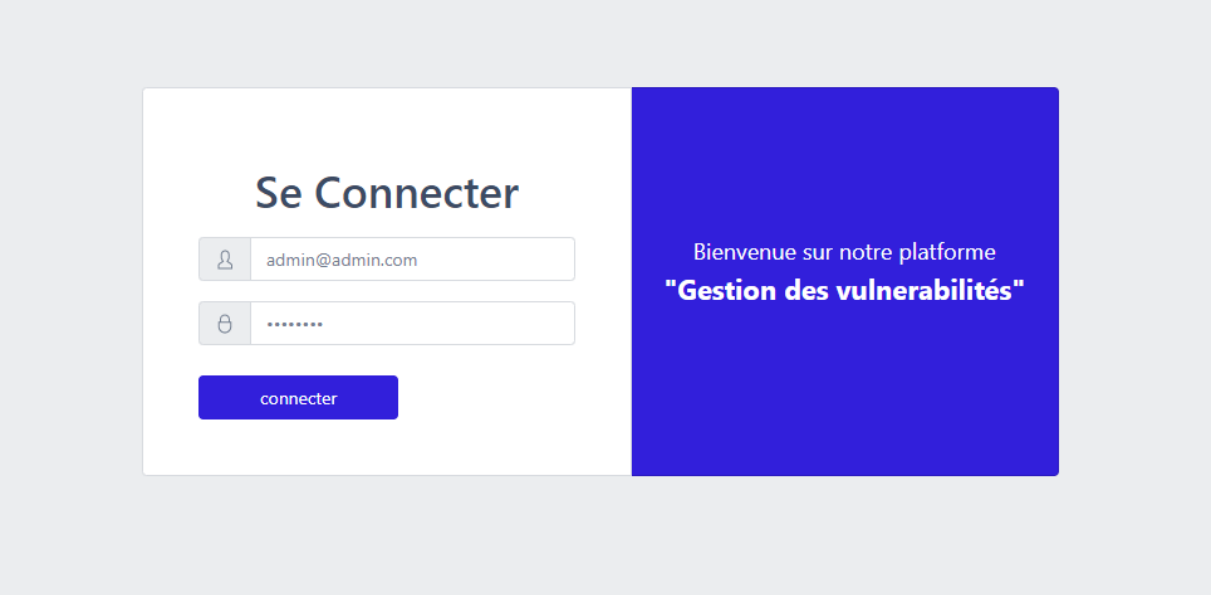


Figure19 : La page principale.

Quand l'utilisateur va se connecter, il y a quatre possibilités, soit il se connecte comme étant un :

1. Admin

Ici le tableau de bord qui s'affiche avec le menu des options

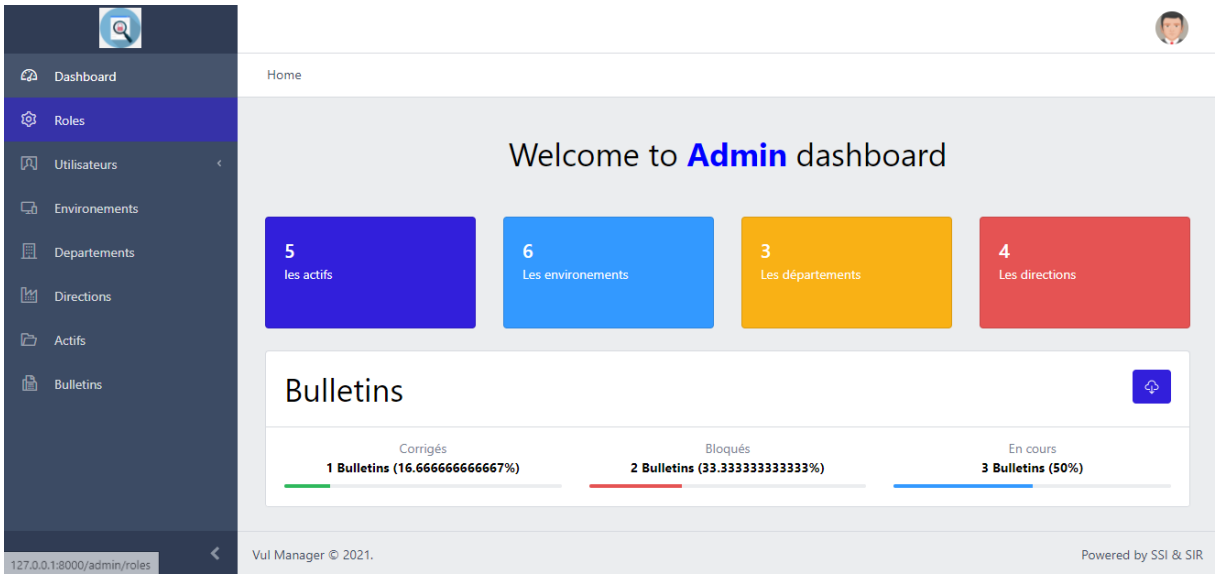


Figure 20 : Tableau de bord d'admin.

A ce niveau,

- **Il peut ajouter**

a. un utilisateur :

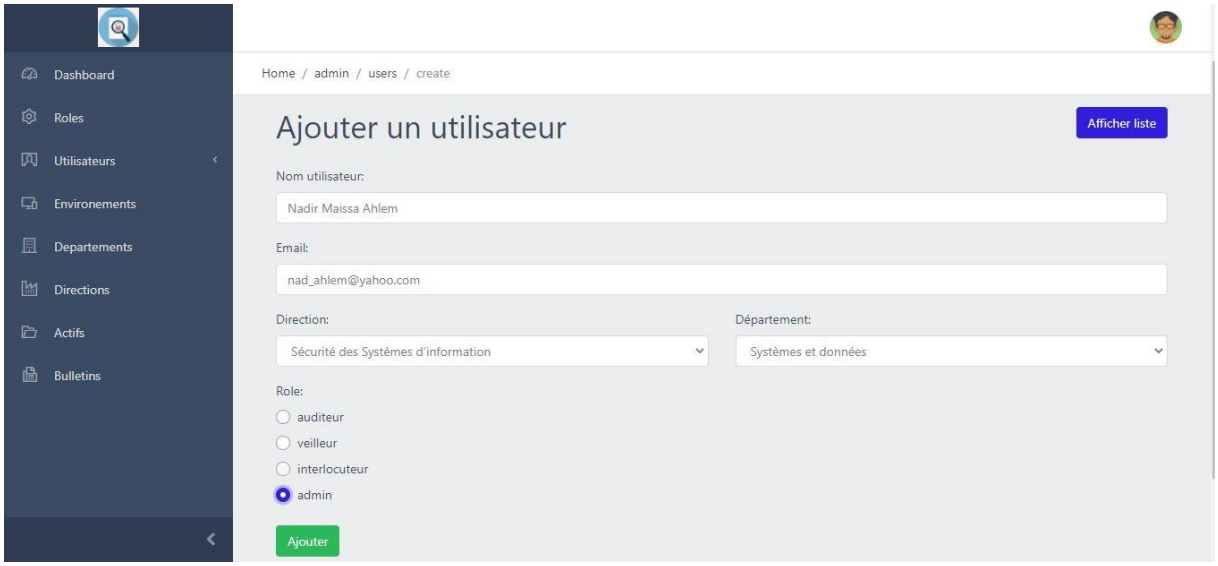


Figure 21 :l'ajout d'un utilisateur.

Lorsque l'administrateur va ajouter un utilisateur, le mot de passe va se générer automatiquement et doit être envoyé a l'interlocuteur ajouté pour qu'il puisse accède a

soncompte , on a utilisé « mailTrap » :

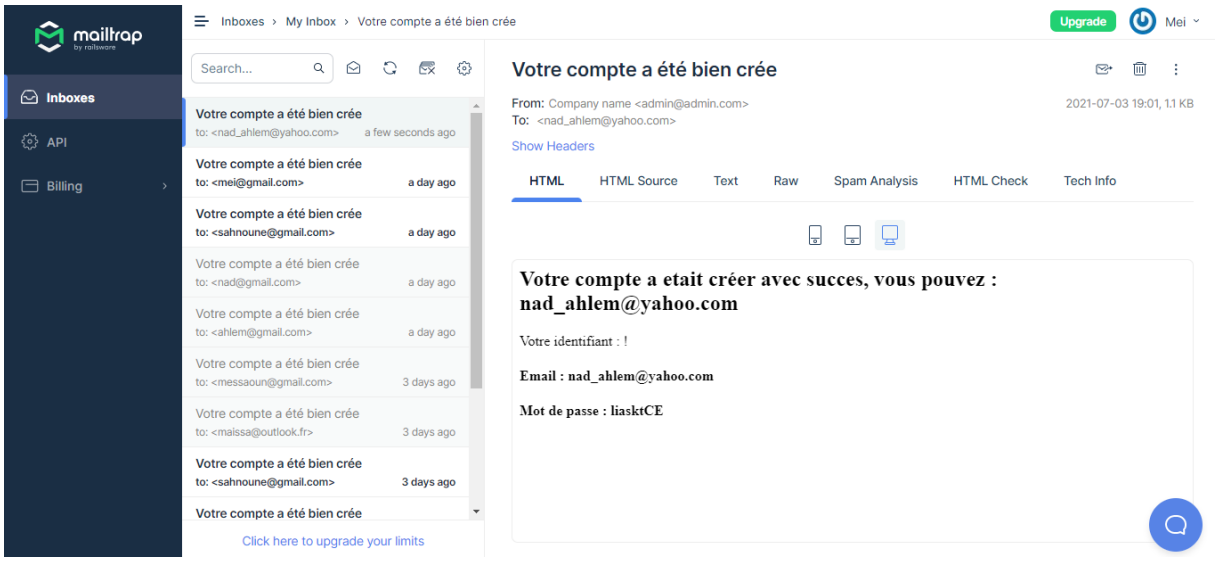


Figure 22 : génération du mot de passe.

b. un environnement :

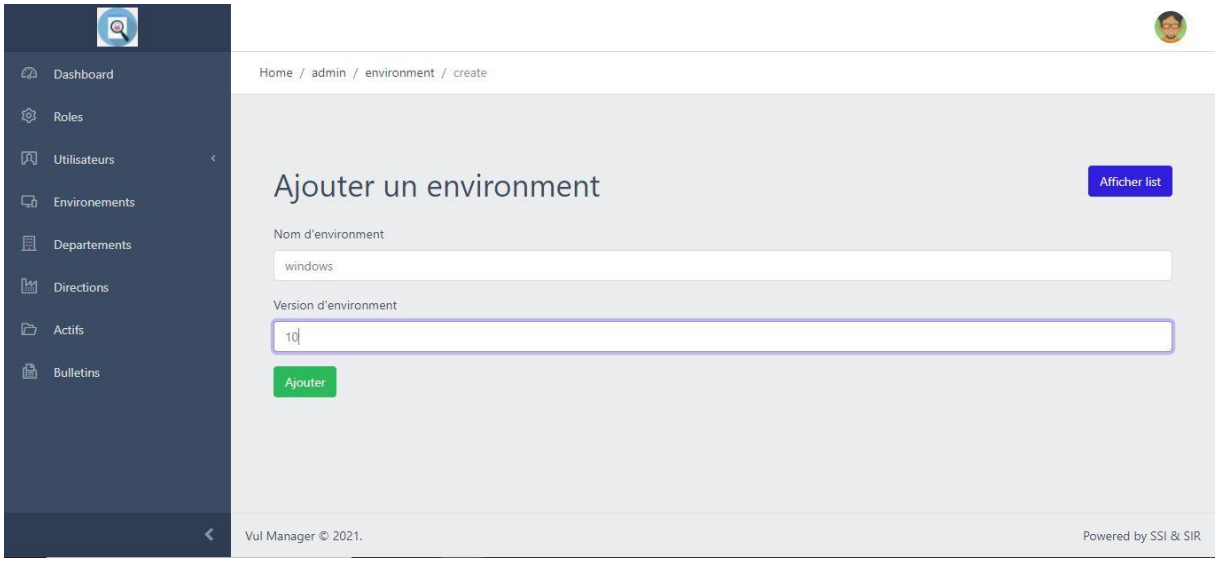


Figure 23:l'ajout d'un environnement.

c. un département :

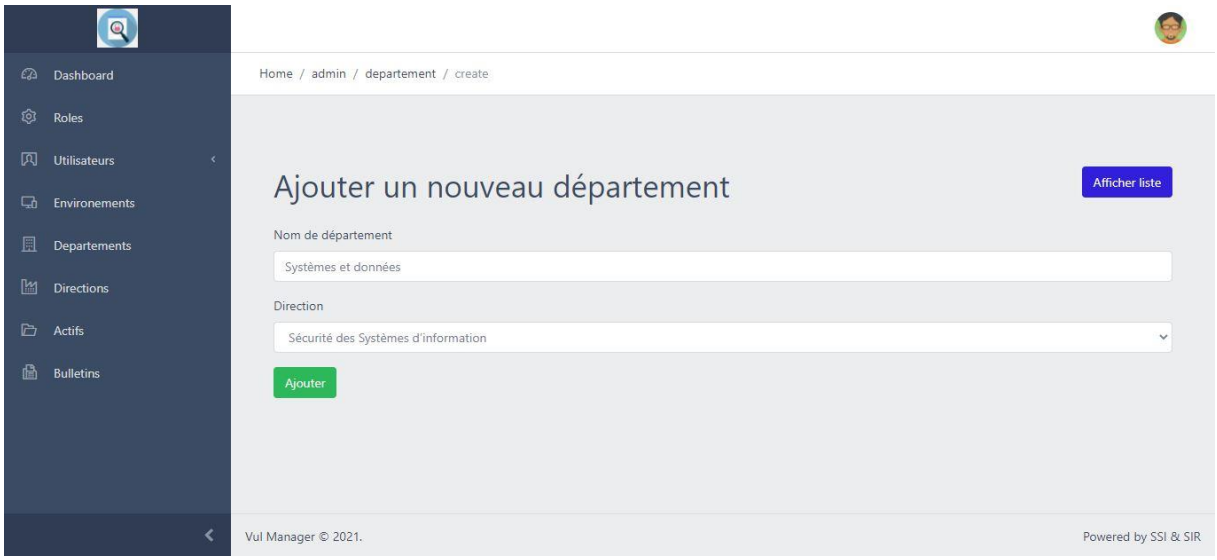


Figure 24 :l'ajout d'un département.

d. une direction :

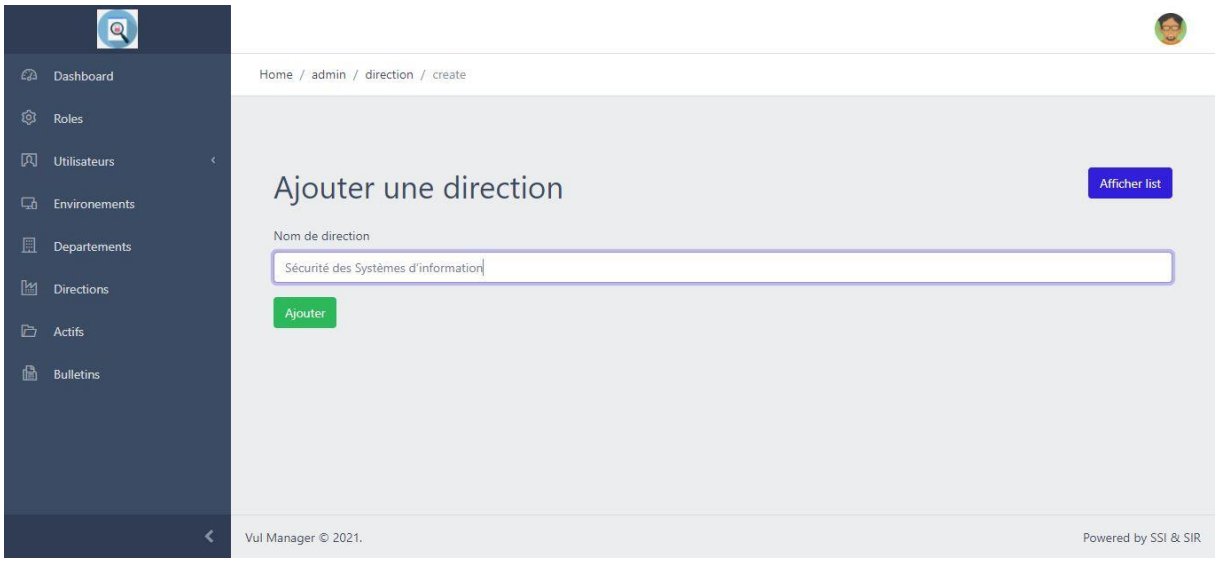


Figure 25:l'ajout d'une direction.

e.un actif :

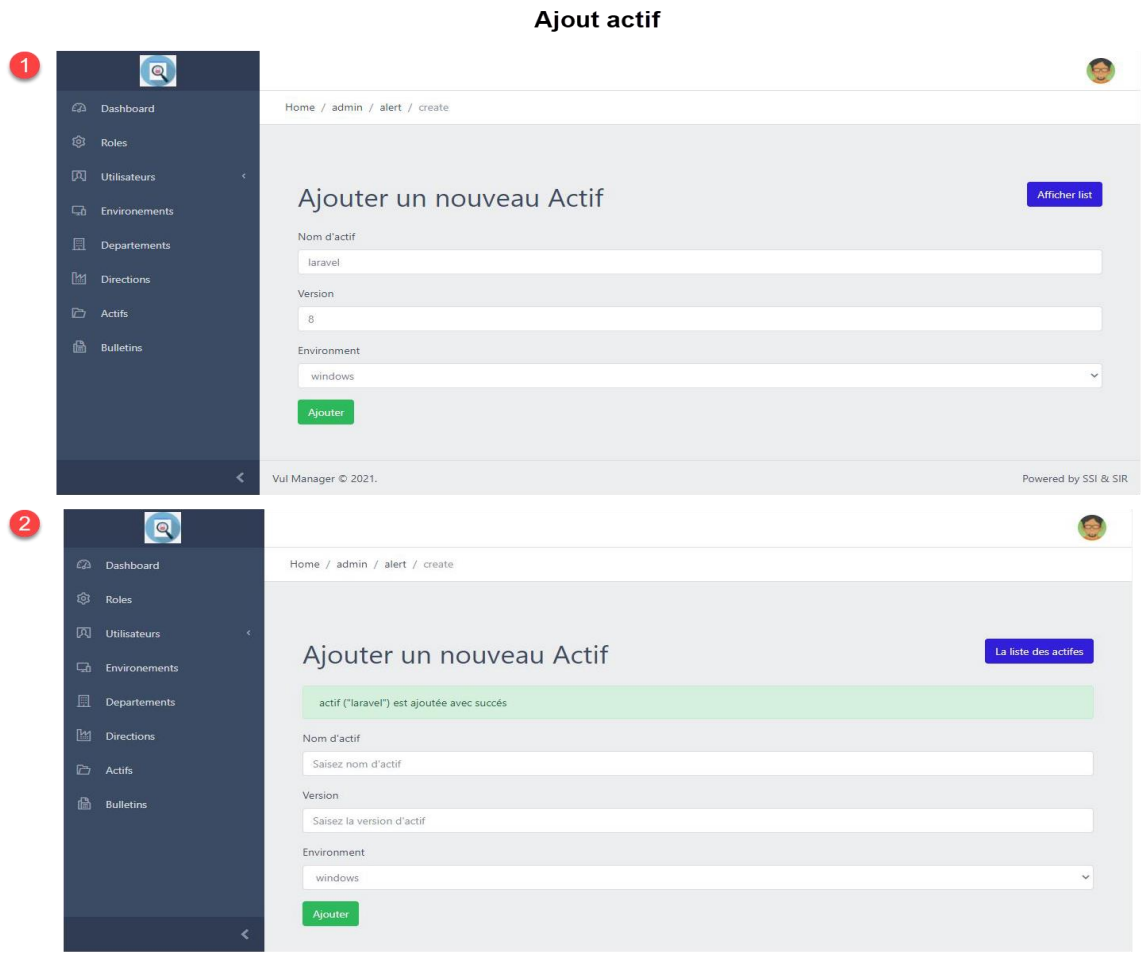


Figure 26 :l'ajout d'un actif.

S'il ne remplit pas tous les champs, on aurra un message d'erreur :

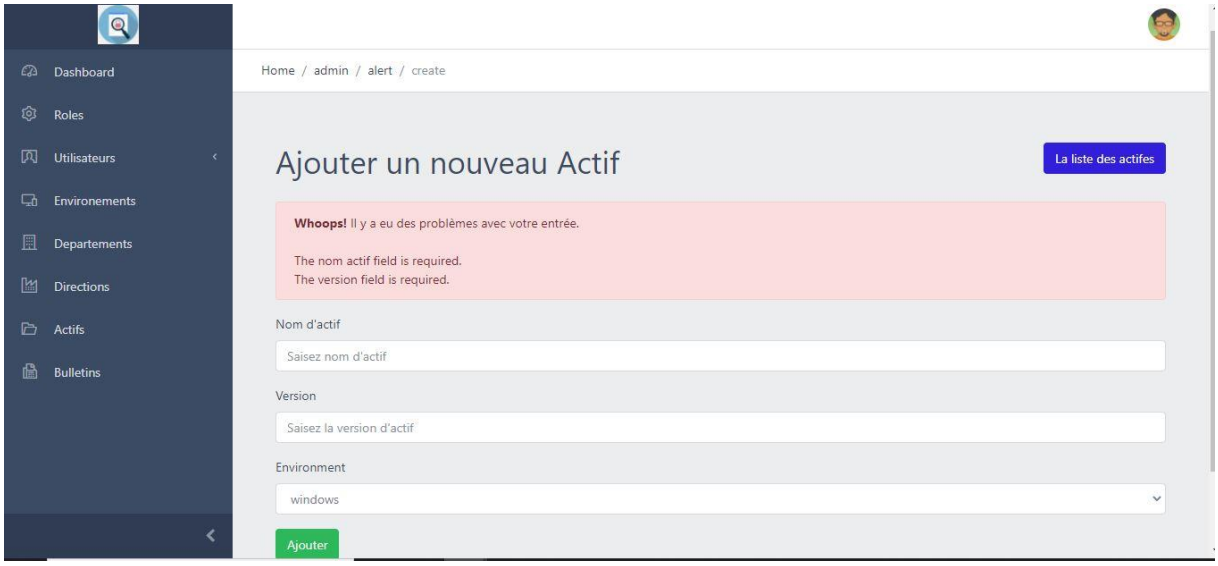


Figure 27 : échec d'ajout d'un actif.

- **Il peut mettre à jour**

a.Un actif :

Ici comme vous voyez,on a les selctions des utilisateurs , c'est-à-dire l'administrateur peut affecter l'actif aux utilisateurs ,dans cet exemple on a affecté l'actif « JavaEE » aux utilisateurs « Messaoun Youssra, Ahlem, Nad ».

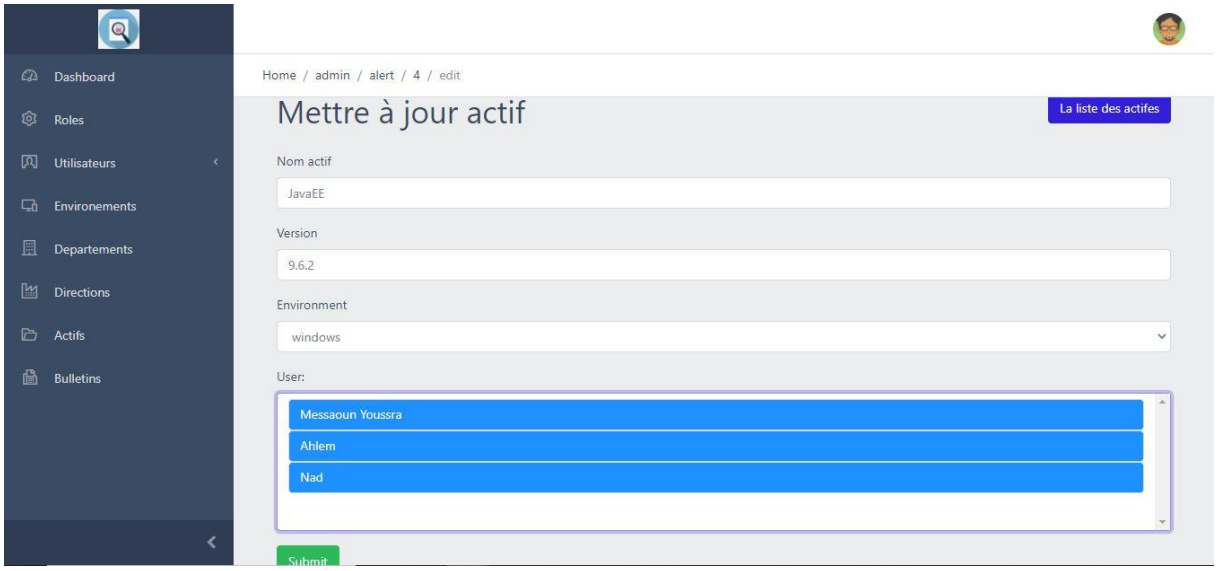


Figure 28 : Mis à jour d'un actif.

- **Il peut consulter**

a.la liste des rôles :

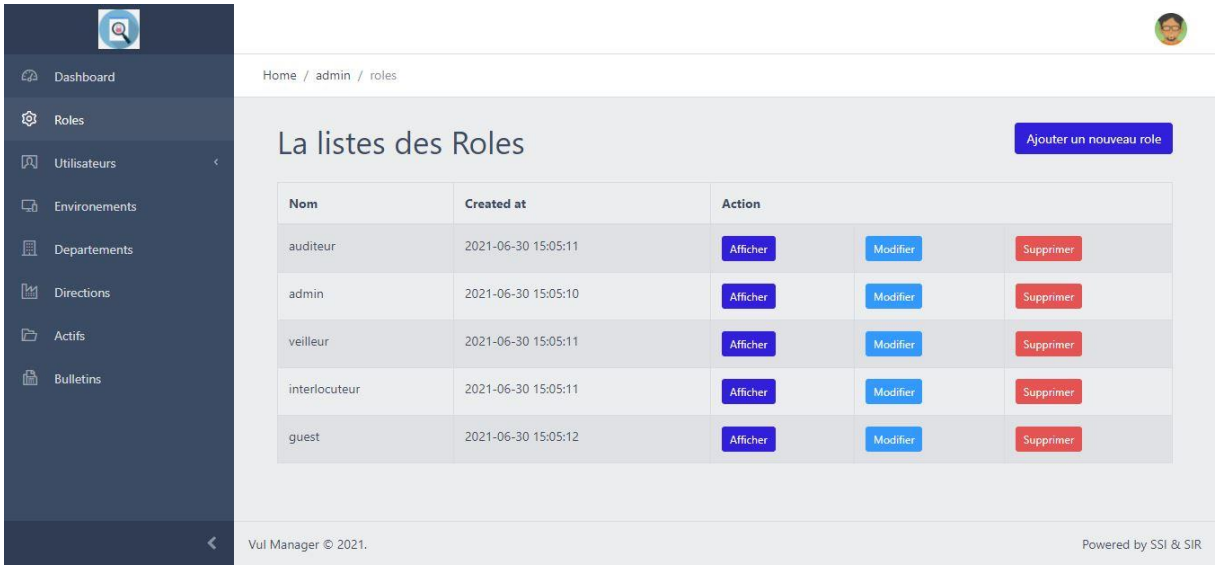


Figure 29 : Consultation de la liste des rôles.

b.la liste des départements :

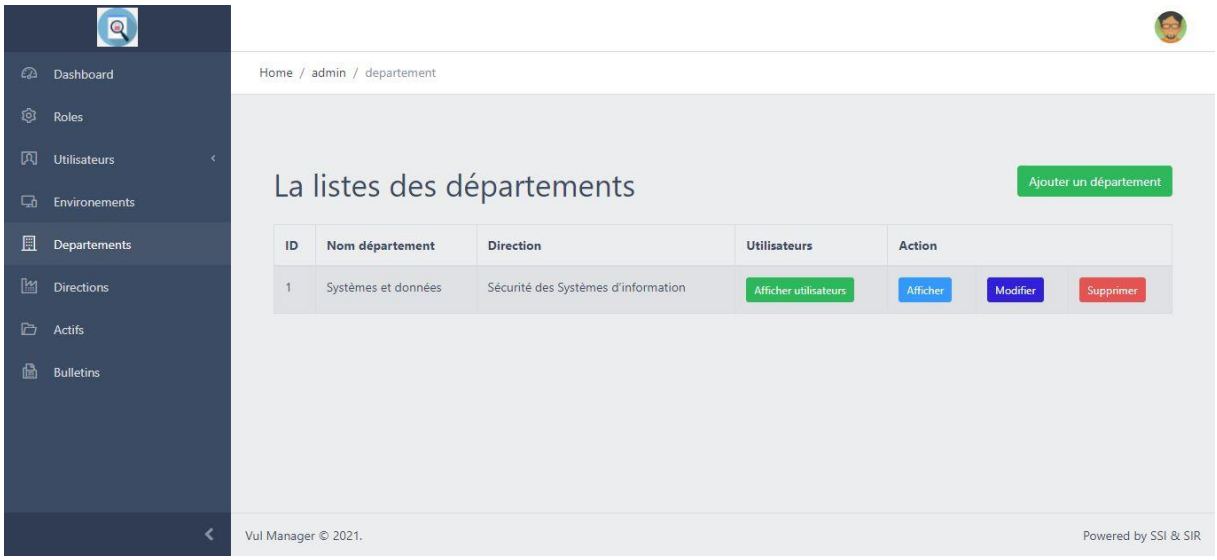


Figure 30 : Consultation de la liste des départements.

c.la liste des directions :

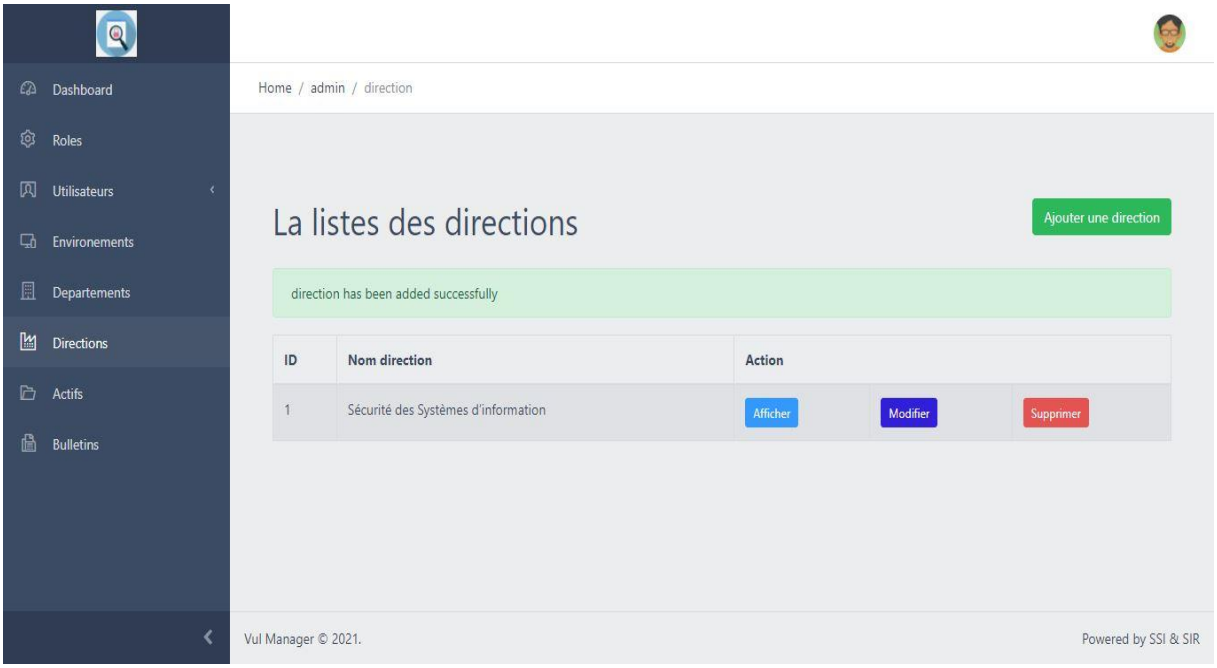


Figure 31 : Consultation de la liste des directions.

d.la liste des actifs :

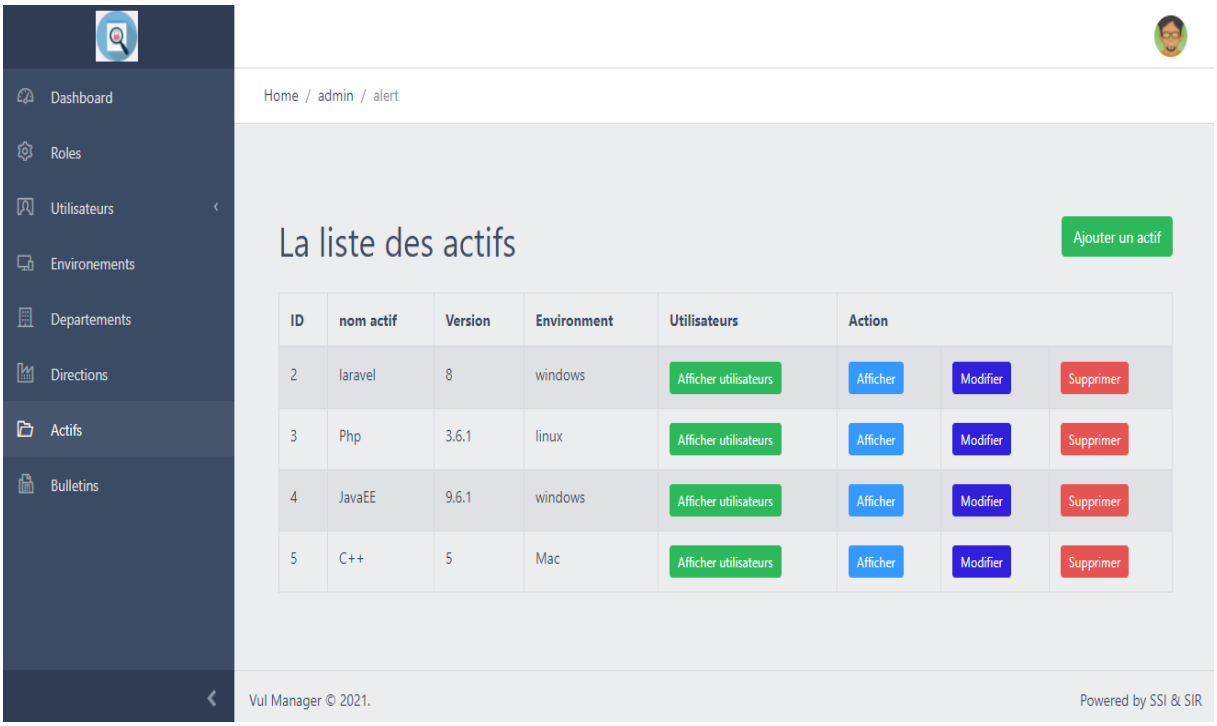


Figure 32 : Consultation de la liste des actifs.

e.la liste des environnements :

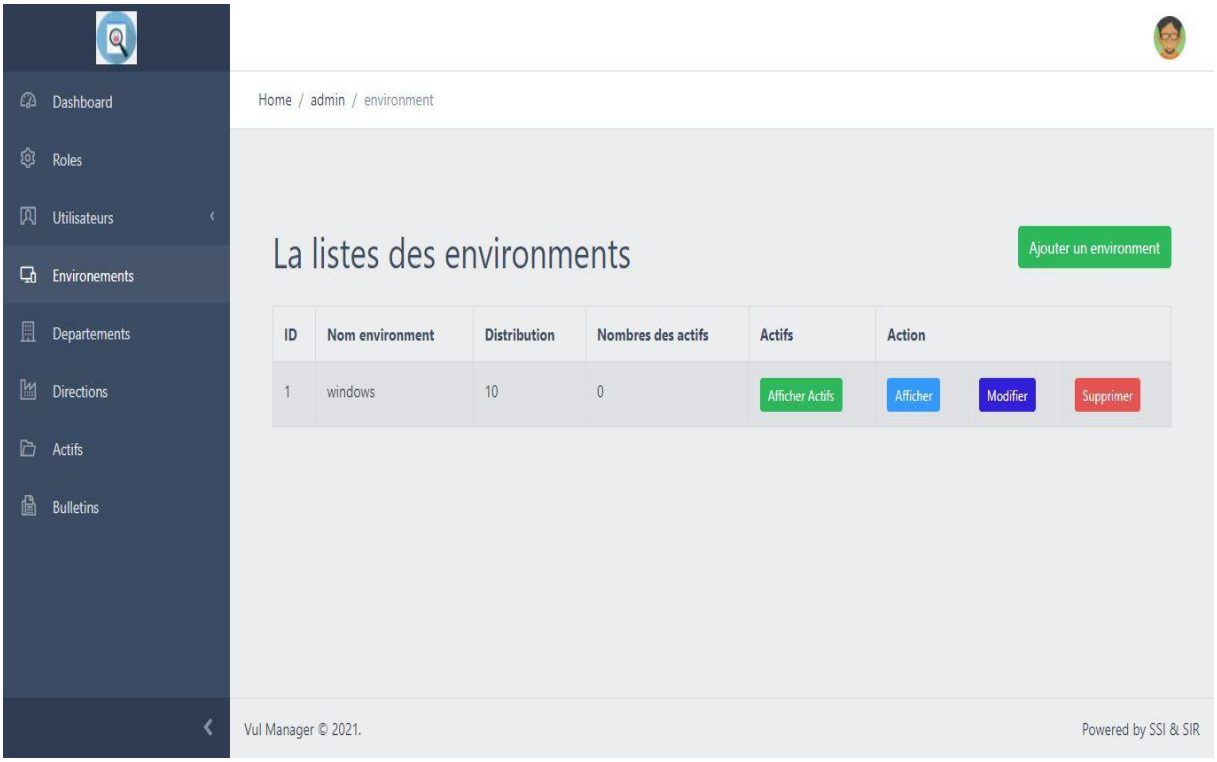


Figure 33 : Consultation de la liste des environnements.

f.les actif d'un environnement spécifié :

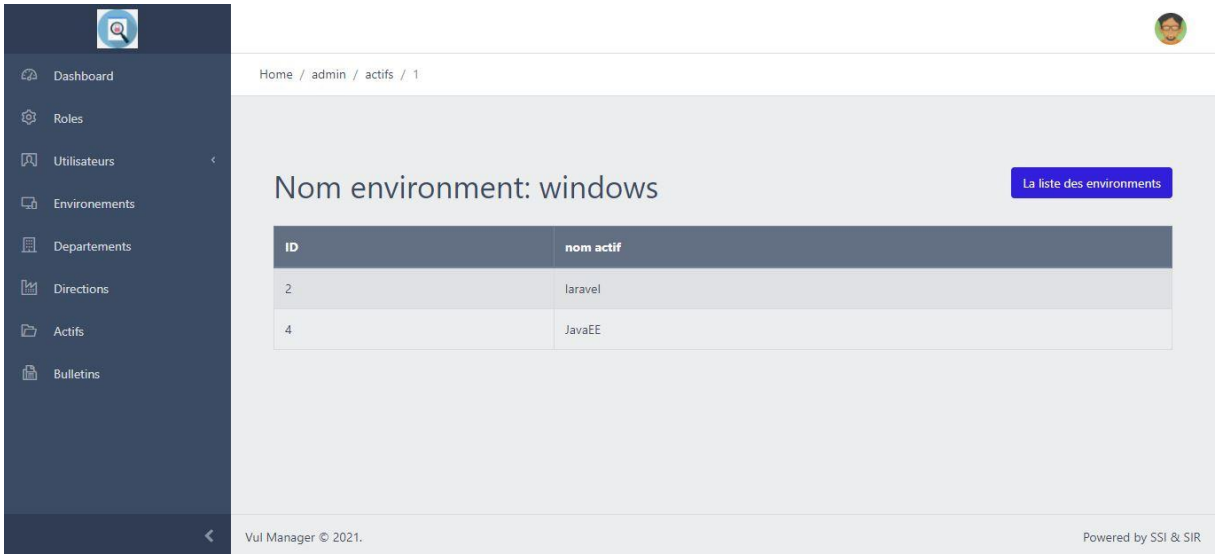


Figure 34 : Consultation des actifs d'un environnement spécifié.

g.les utilisateurs d'un actif spécifié :

Figure 35 : Consultation des utilisateurs d'un actif spécifié.

h.les utilisateurs d'un environnement spécifié :

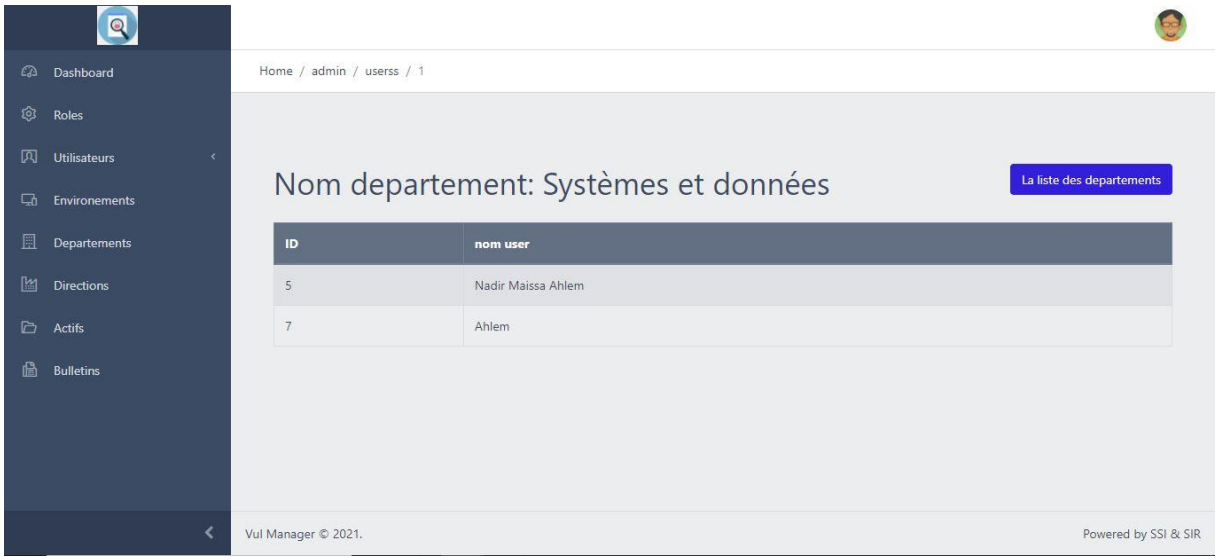


Figure 36 : Consultation des utilisateurs d'un environnement spécifié.

i. la liste des utilisateurs spécifiés (interlocuteurs) :

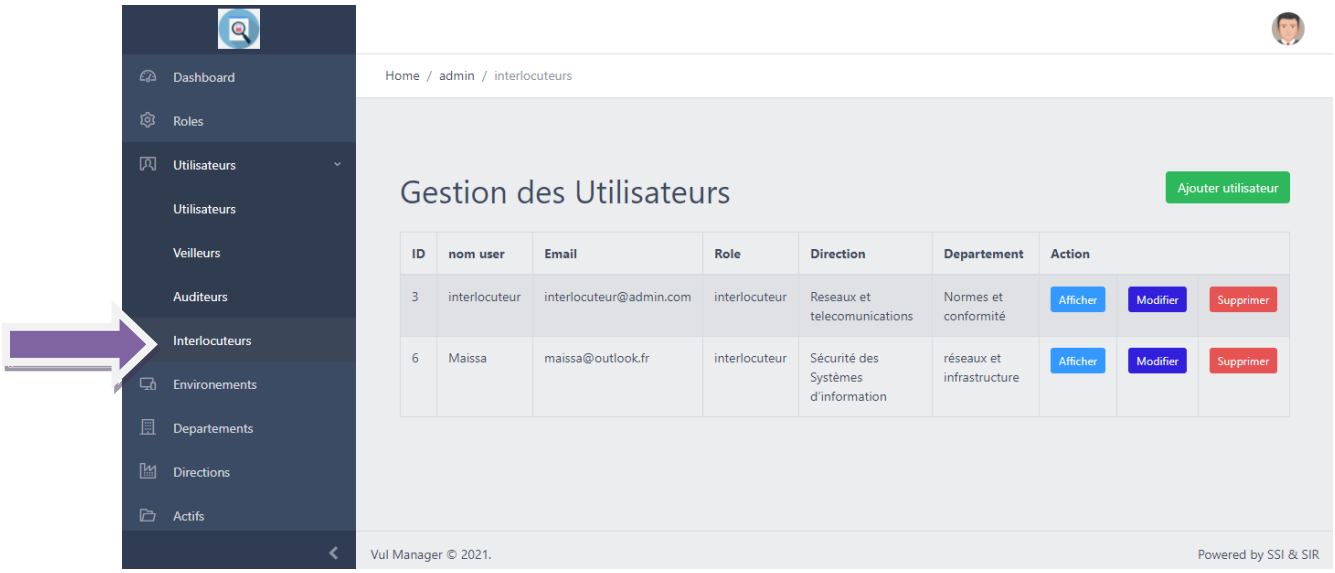


Figure 37: Consultation de la liste des utilisateurs spécifiés.

2. veilleur

Cet utilisateur a les mêmes fonctionnalités comme l'admin sauf la consultation de la liste des rôles et l'ajout des utilisateurs, des départements et des directions mais il a au plus :

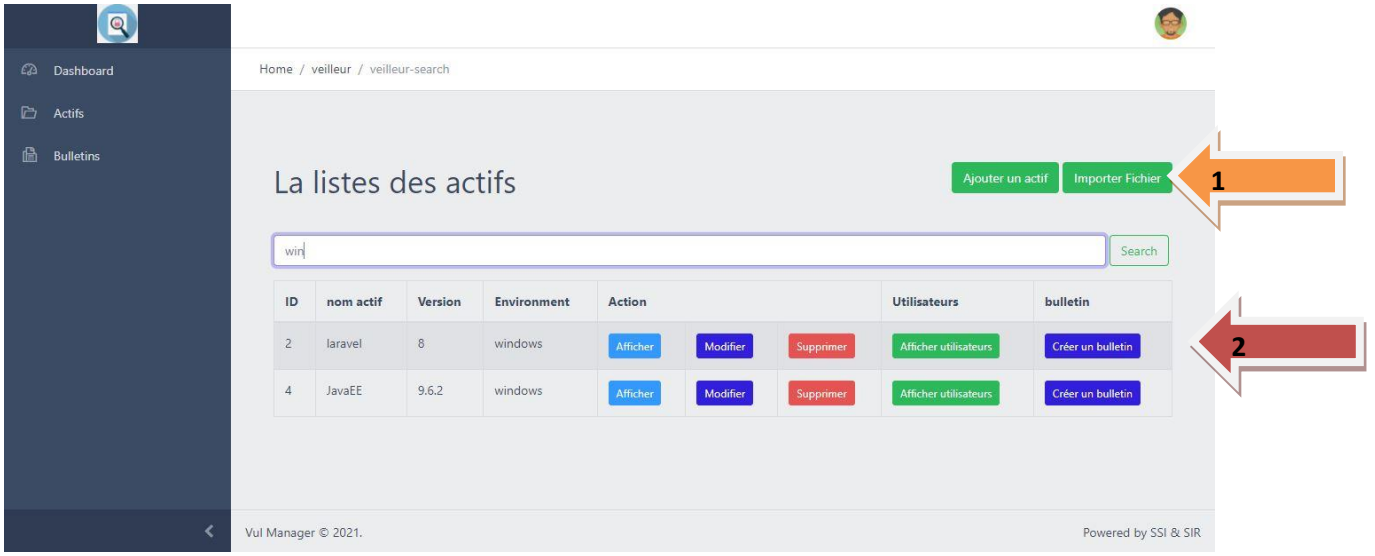


Figure 38 : Les fonctionnalités du veilleur.

2.1. L'importation des fichiers **EXCEL** contenant des actifs :

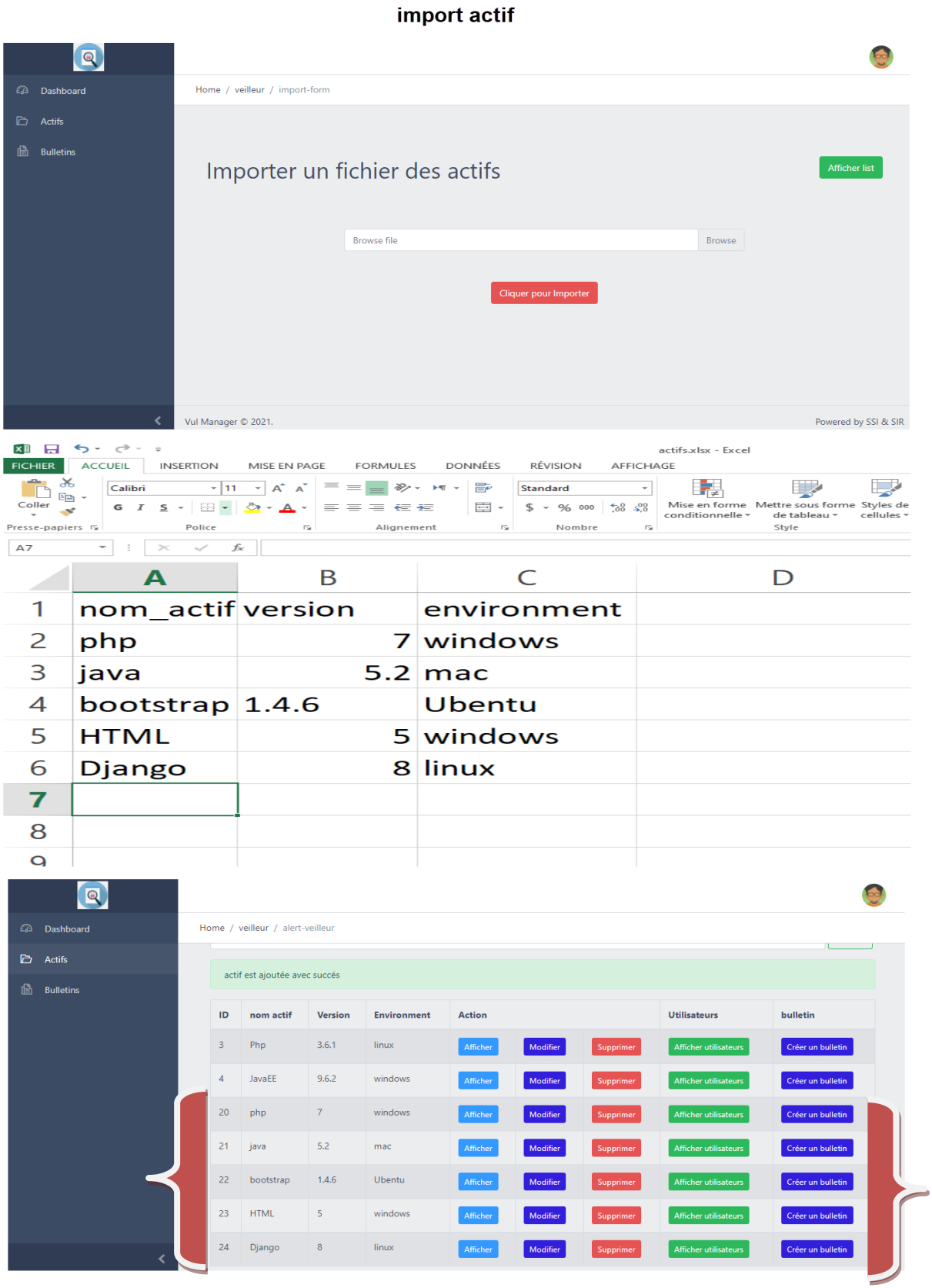


Figure 39 : L'importation de la liste des actifs.

2.2. La gestion de bulletin, donc seulement le veilleur qui peut créer le bulletin qui concerne un actif en cliquant sur « créer bulletin ». (nous allons détailler cette tache).

3. Interlocuteur :

Cet utilisateur a les mêmes fonctionnalités du veilleur sauf la création et le classement et la consultation des statistiques du bulletin.

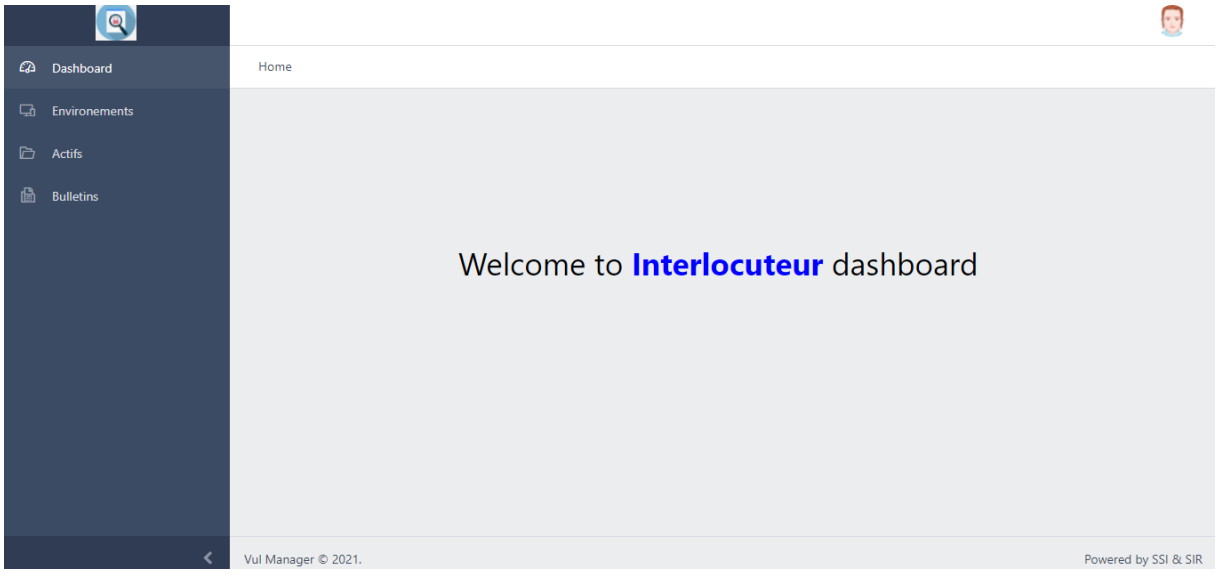


Figure 40: Tableau de bord d'interlocuteur.

Ce dernier alors va recevoir le bulletin, appliquer le correctif, remplir sa partie dans le bulletin et l'envoyer à l'auditeur.

4. l'auditeur

L’auditeur peut consulter les statistiques des bulletins existants et renseigner le bulletin après sa réception de la part d’interlocuteur.

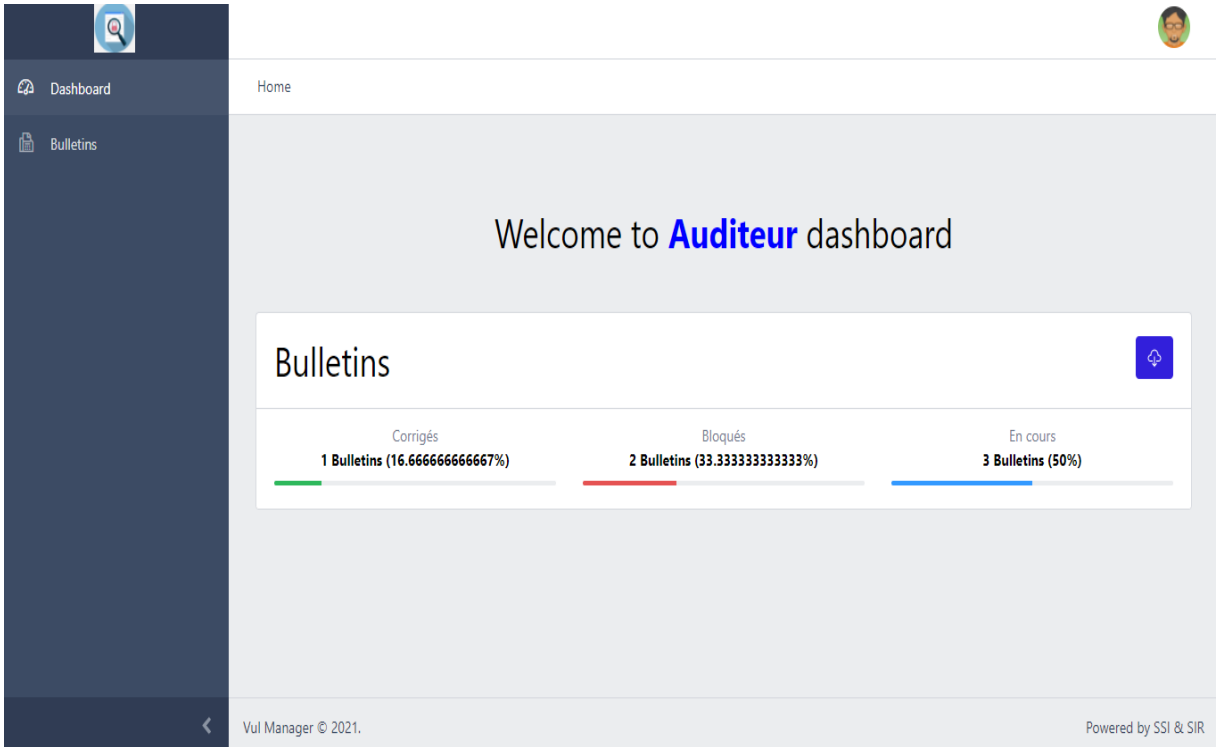


Figure 41 : Tableau de bord d’auditeur.

5. La gestion du bulletin :

1. Comme on a mentionné au dessus, le veilleur doit sélectionner l’actif vulnérable pour envoyer le bulletin aux interlocuteurs concernés en cliquant sur le bouton « créer

bulletin », par la suite il doit remplir les champs :

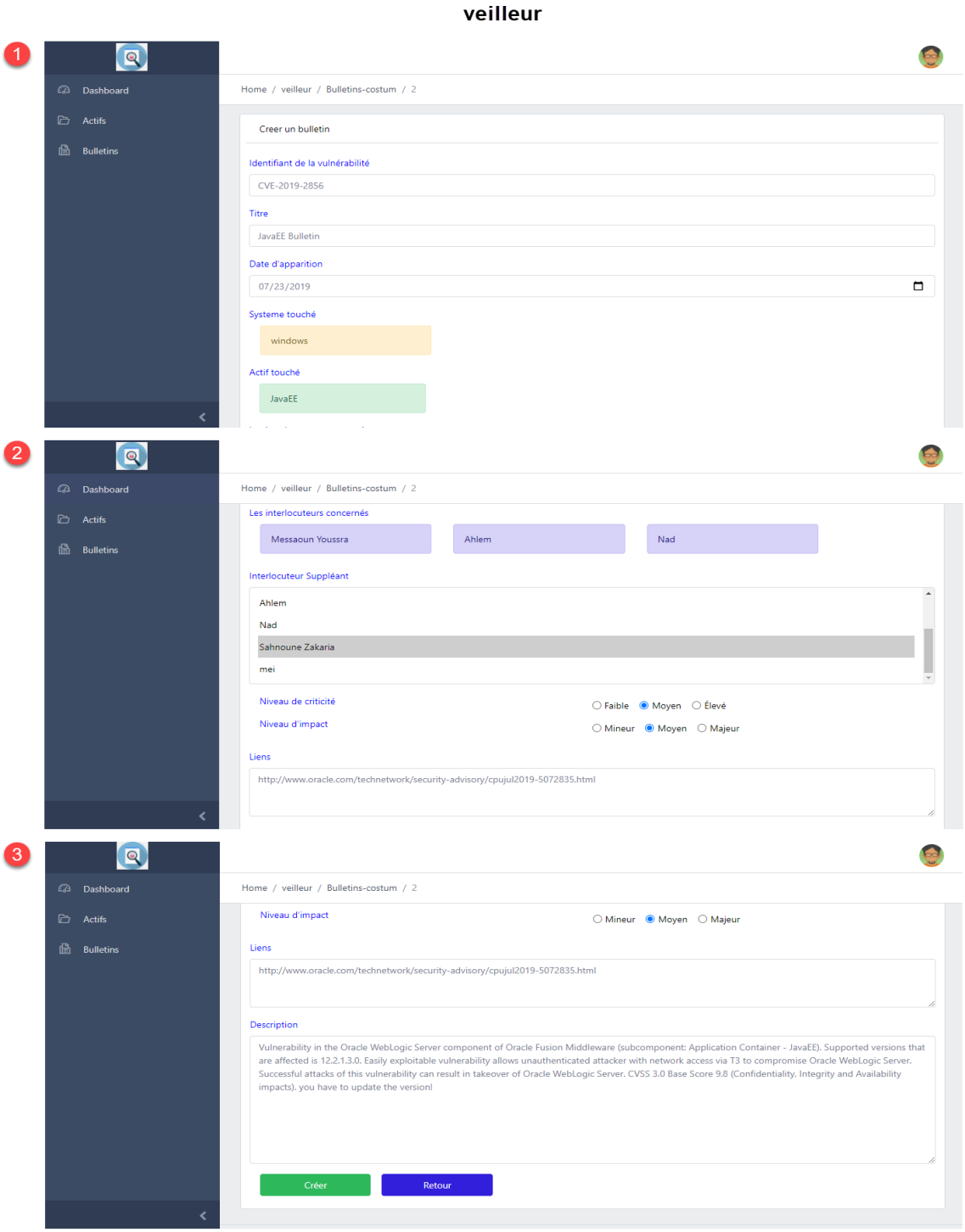


Figure 42 : Création du bulletin.

Sachant que les systèmes touchés et les interlocuteurs concernés vont se sélectionner automatiquement.

Comme vous voyez, dans cet exemple on a trois interlocuteurs concernées, donc le bulletin doit être dupliqué pour les trois car c'est la même vulnérabilité d'un actif « JavaEE », mais

c’est le même bulletin pour chaque personne

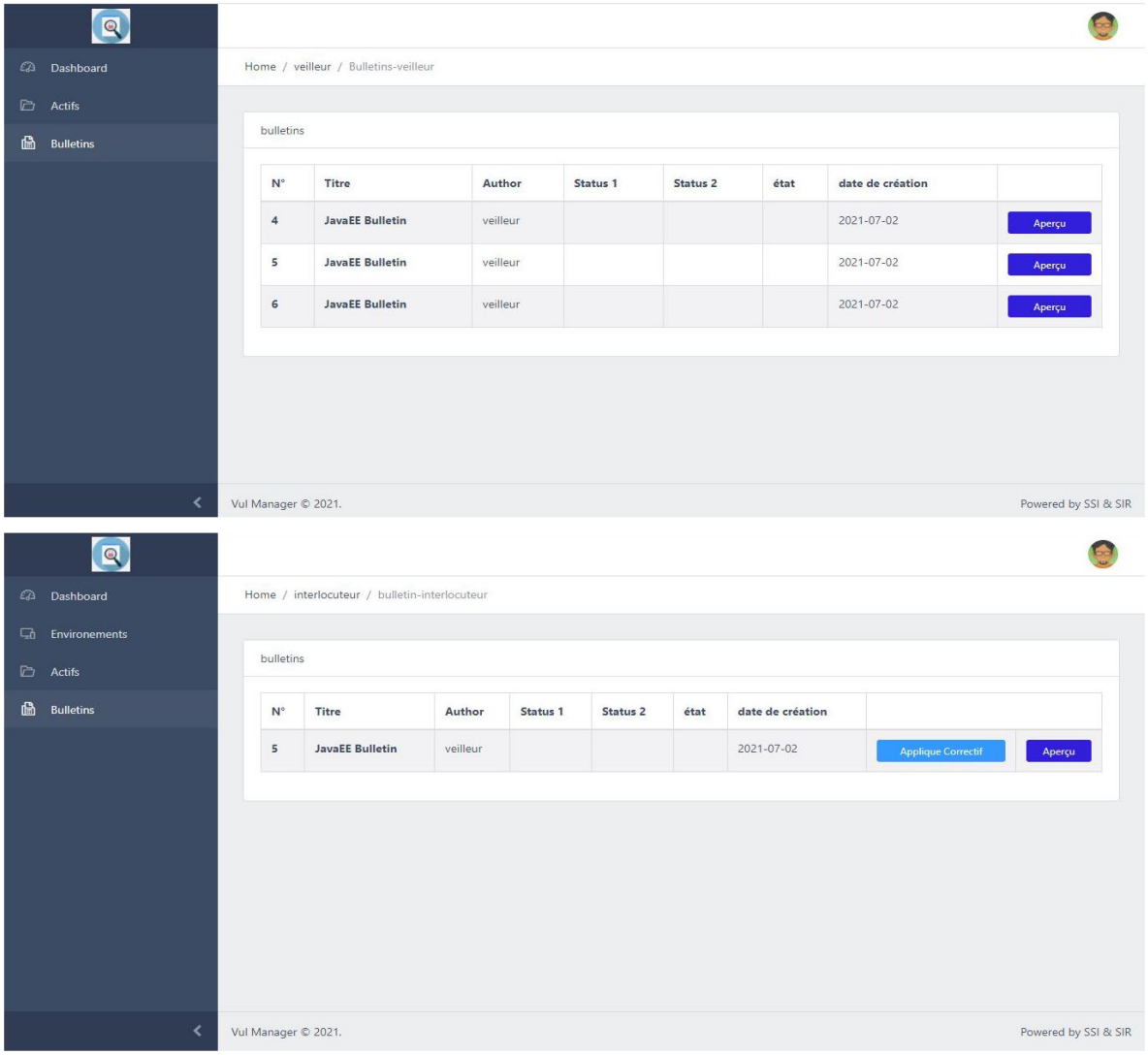


Figure 43 : La duplication du bulletin.

Voila le bulletin après la création :

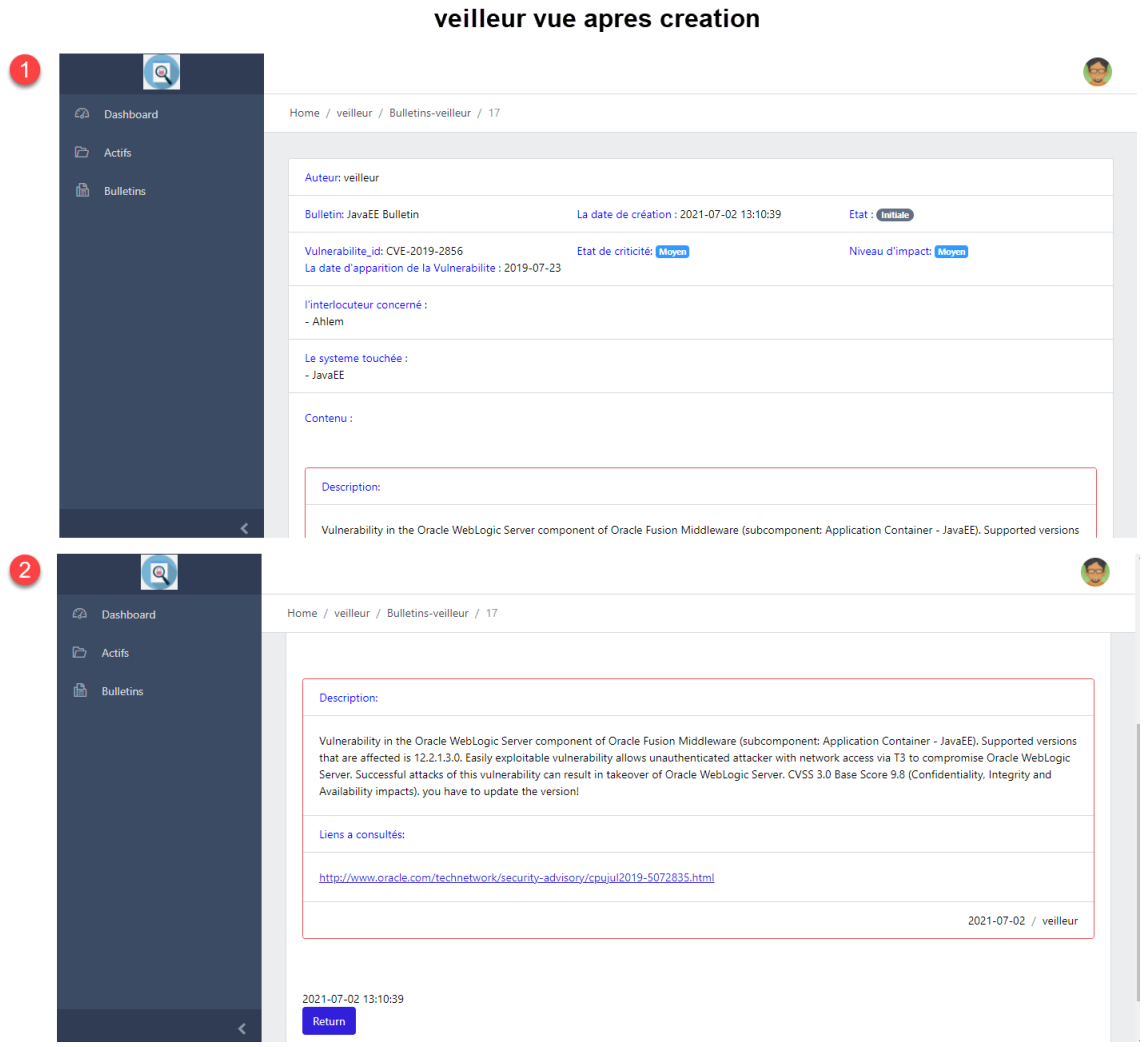


Figure 44 : Aperçu du bulletin après création.

Après ca, l'interlocuteur reçoit le bulletin et il doit remplir sa partie :

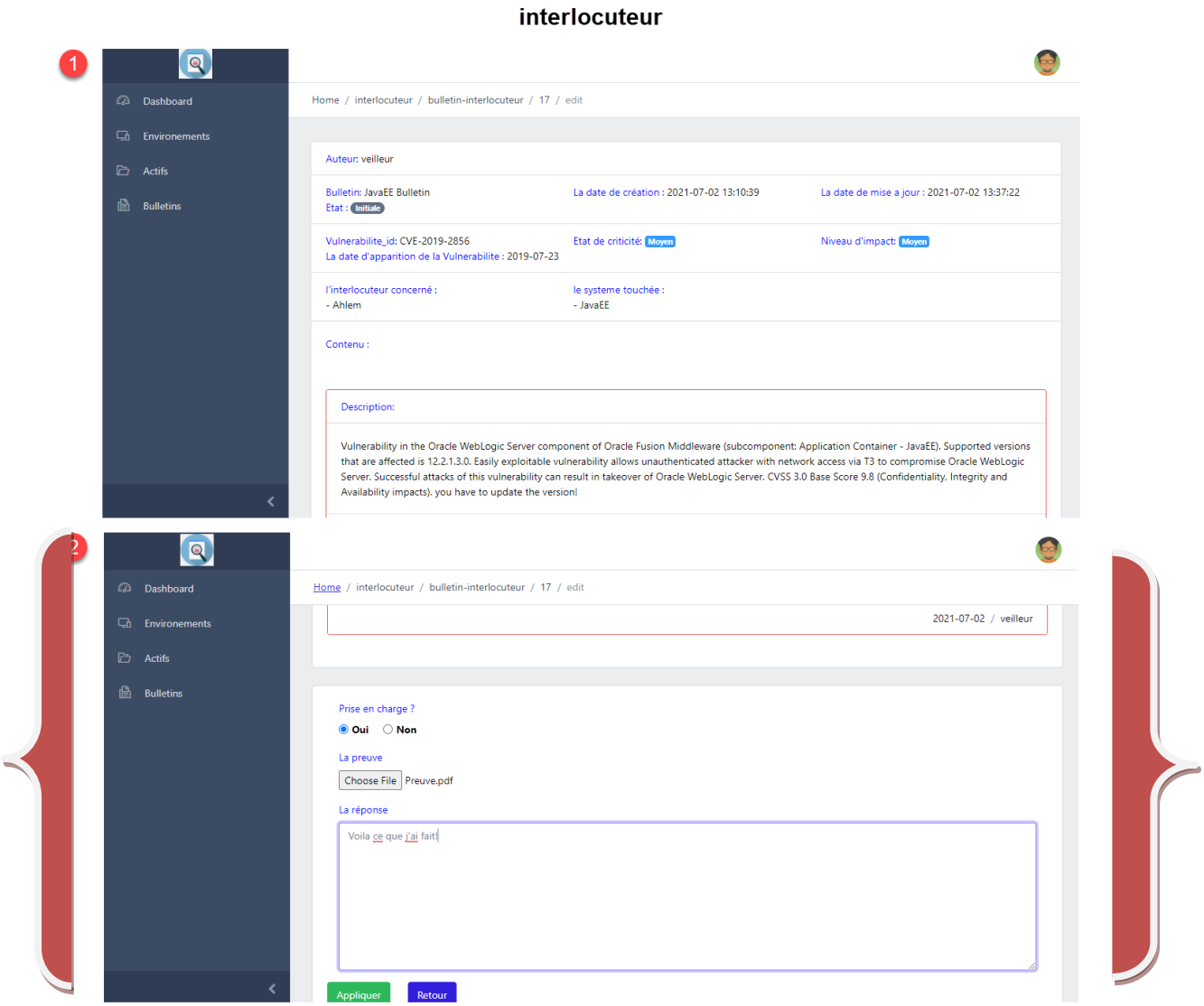


Figure 45: La partie de remplissage d'interlocuteur.

Ensuite l'auditeur doit consulter la réponse avec une preuve envoyée par l'interlocuteur et vérifier la prise en charge de la vulnérabilité :

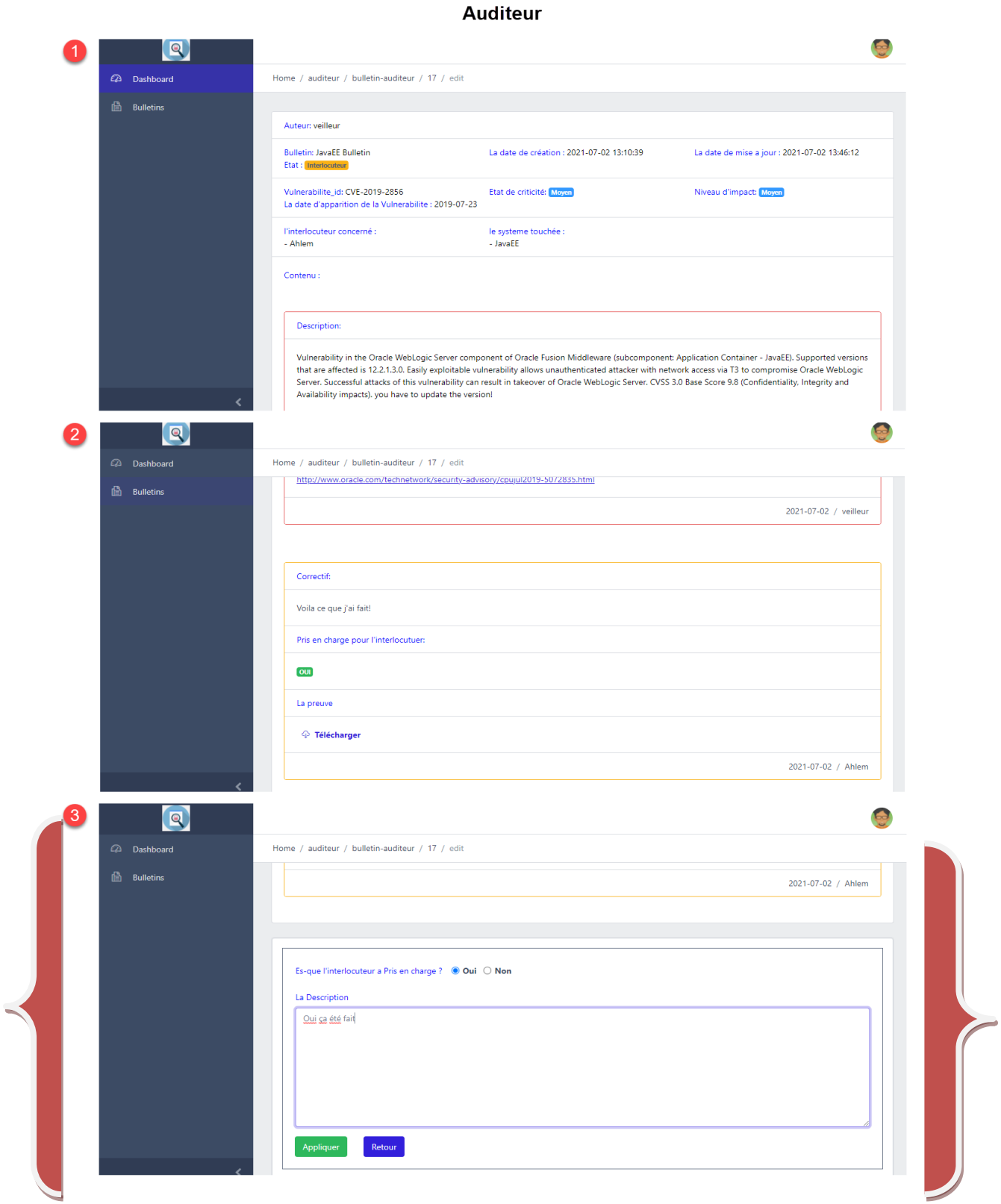


Figure 46: La partie de remplissage d'auditeur.

Apres la vérification de l'auditeur, maintenant c'est le rôle d'un veilleur qui va classer le bulletin selon ces trois choix **(corrigé, bloqué, relancé le processus):**

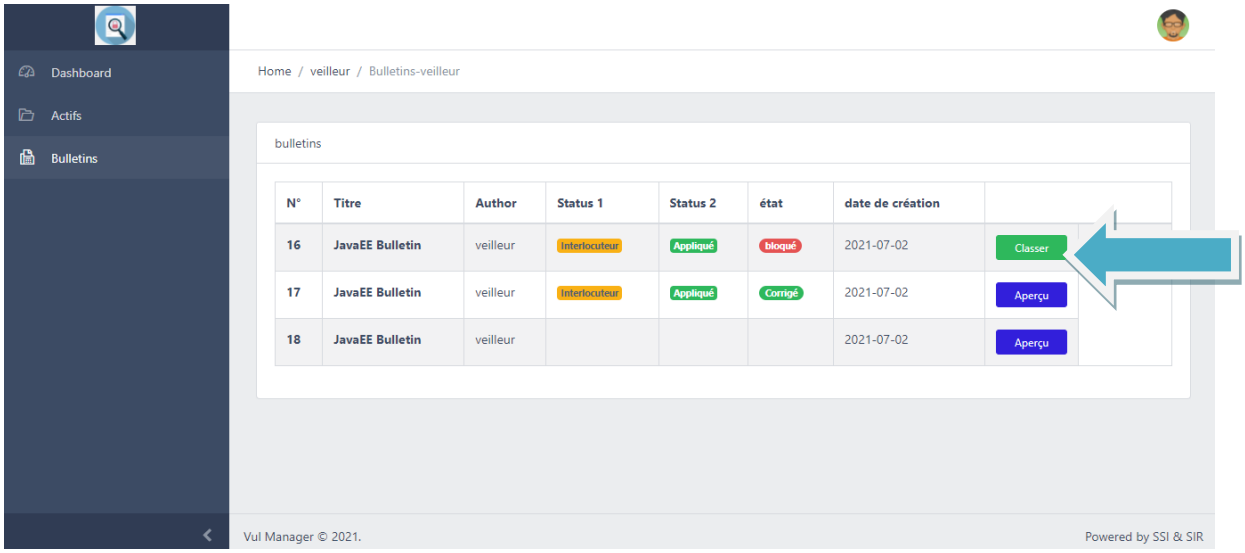


Figure 47 : Lé classement du bulletin.

Sinon, il peut consulter juste les bulletins déjà crées en cliquant sur ''Aperçu''.

- On a un autre exemple dans le cas où le bulletin a été classe « bloqué » pour l'interlocuteur « MessaounYoussra » :

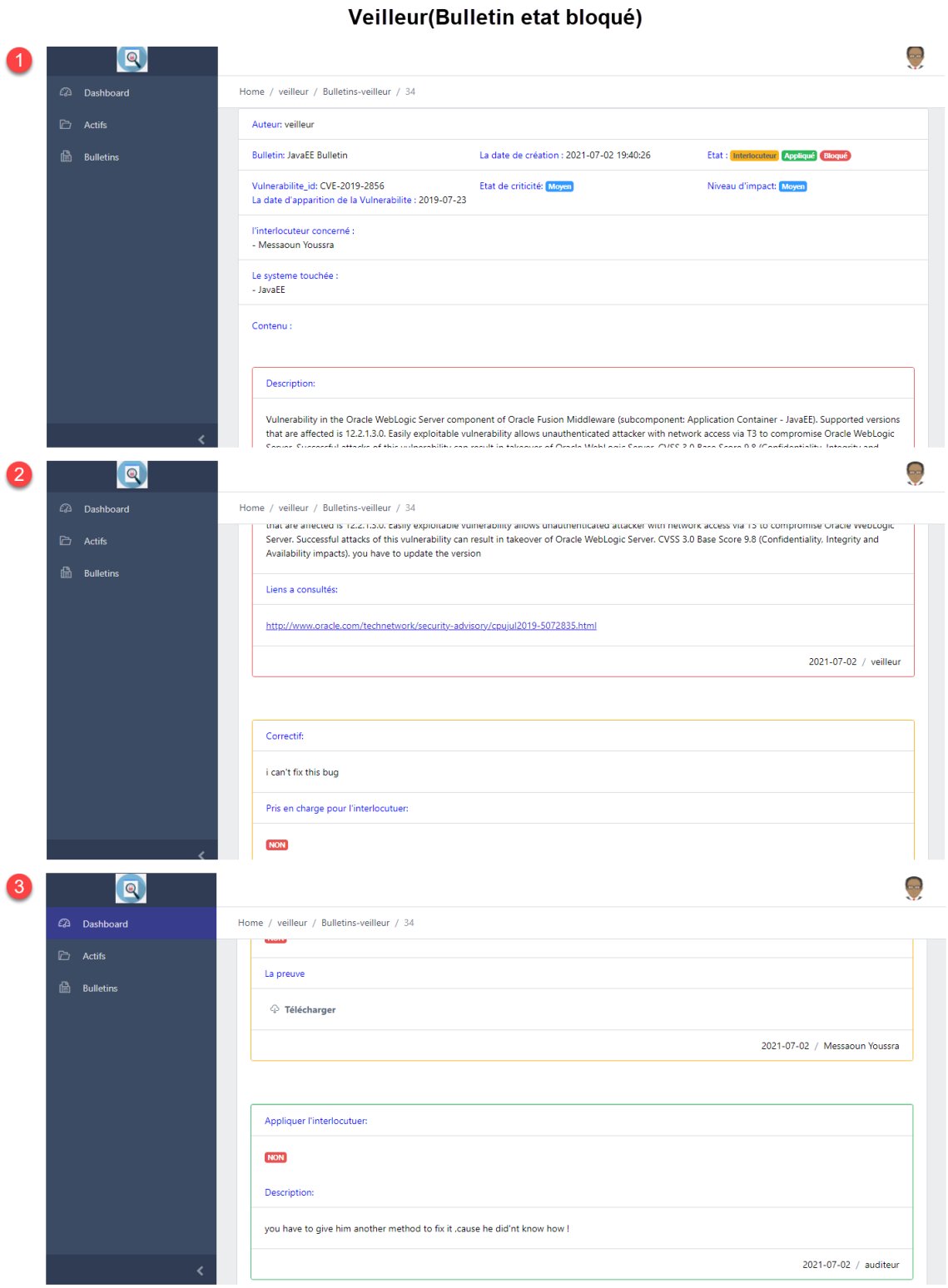


Figure 48 : Exemple d'un bulletin classé bloqué.

- Dans la figure suivante on a deux bulletins classés comme ‘’bloqué’’, un bulletin comme ‘’corrigé’’ et les trois bulletins en cours :

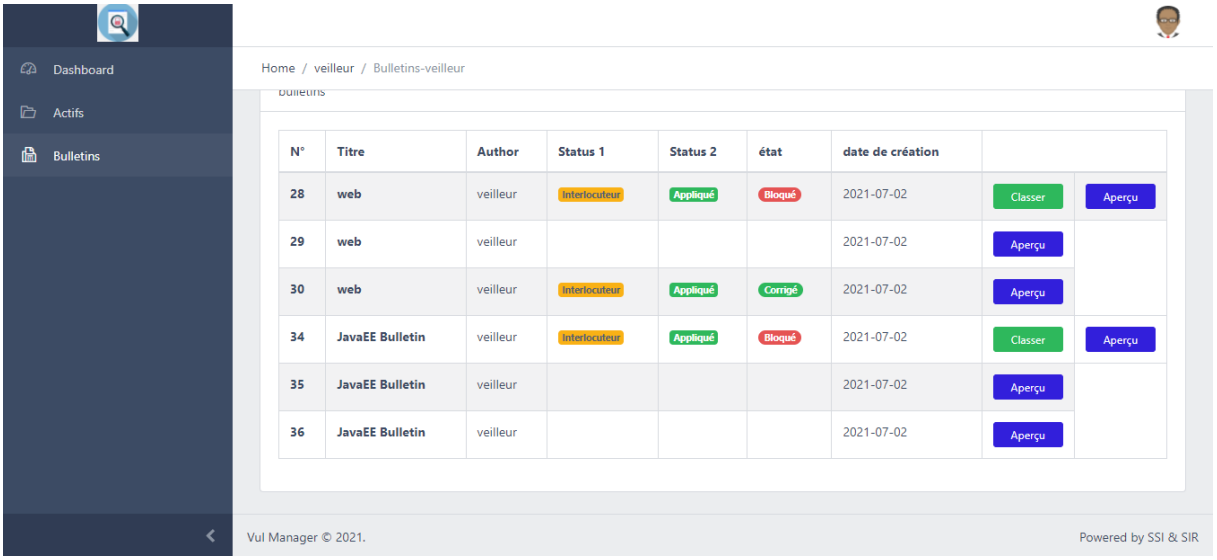


Figure 49 : La liste de bulletins classés.

- Finalement, on aura ces statistiques là :

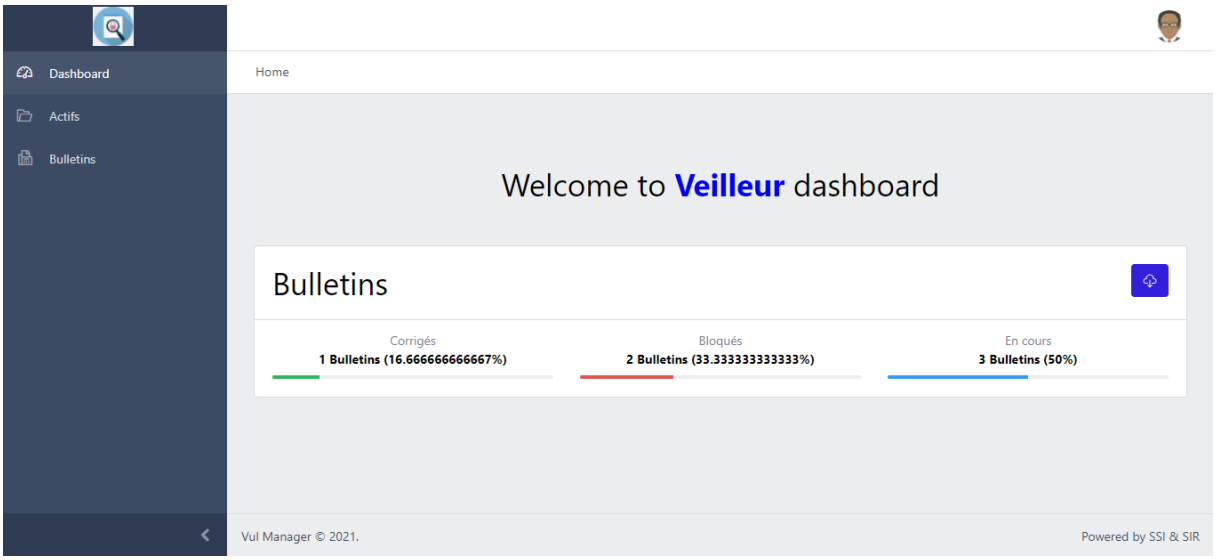


Figure 50: Tableau de bord du veilleur.

6. Conclusion :

Dans ce dernier chapitre, l’étude était basée sur la réalisation et l’implémentation de L’application par une présentation des outils de développement et des interfaces les plus Significatives de l’application.

Conclusion et perspectives

Les vulnérabilités, ainsi que leur exploitation, sont encore aujourd'hui la cause profonde de la plupart des atteintes à la sécurité des données personnelles c'est pour ça, il faut mettre en place des processus de la gestion de vulnérabilités pour protéger les données.

La mise en place d'un processus efficace de gestion des vulnérabilités allant de leurs identifications à leurs corrections est une des mesures phare pour se prémunir des différentes menaces grandissantes.

Ce projet nous a permis d'étendre et améliorer nos connaissances et nos compétences dans le domaine de la programmation Web qui est un domaine en perpétuel changement depuis la commercialisation d'internet, qui a commencé au début des années 90. Il est aujourd'hui devenu un standard pour soigner les présentations, qui est souvent élaboré et met en avant de nombreux contenus multimédias.

Nous avons rencontré beaucoup de problèmes et malgré le peu de temps que nous avions, nous avons réussi à réaliser notre application. Nous envisageons de l'améliorer dans l'avenir proche en ajoutant par exemple un script pour récupérer les vulnérabilités directement à partir d'internet, l'application automatique des correctifs, la vérification automatique d'application des correctifs...etc.

En outre, nous souhaitons que ce travail soit utile à d'autres personnes désirant aborder des sujets pareils et que notre application puisse être utilisée réellement par beaucoup de gens.

Bibliographie

[1]:Sans auteur. « Définition de la veille ».En ligne :http://www.ressources.univ-rennes2.fr/cultures-numeriques-dans-l-enseignement/veille/1-quest-ce-que-la-veille/1-1-definitions-de-la-veille/ (consulté le 04-Mars-2021)

[2]:Sans auteur. « Les étapes de la veille ».En ligne :https://conseils-infodoc.fr/les-5-etapes-de-la-veille/(consulté le 04-Mars-2021)

[3] :https://www.torii-security.fr/blog/la-veille-securite-informatique-activite-indispensable

[4]:Sans auteur.«La méthodologie de la veille».En ligne:https://openclassrooms.com/fr/courses/1733741-effectuez-votre-veille-en-cybersecurite/6032022-mettez-en-place-un-processus-de-veille-en-securite(consulté le 06-Mars-2021)

[5] : Eliana Karina González Suárez ,Barcelona, 2011 ,*University Politècnica de Catalunya*, Vulnerability Management Expert System– Design Development and Implementation – (consulté le 06-Mars-2021)

[6] : Sans auteur. « Les failles de la sécurité informatique ».En ligne :https://blog.antivirus-pas-cher.com/2020/07/15/faille-de-securite-informatique-quest-ce-que-cest%E2%80%89-comment-se-proteger%E2%80%89/#:~:text=Les%20diff%C3%A9rentes%20failles%20de%20s%C3%A9curit%C3%A9,plus%20de%20850%20vuln%C3%A9rabilit%C3%A9s%20diff%C3%A9rentes(consulté le 06-Mars-2021)

[7] :Microsoft,Publie le 10 janvier 2017. « Synthèse des bulletins de sécurité ».En ligne :https://docs.microsoft.com/fr-fr/security-updates/securitybulletinsummaries/2017/ms17-jan(consulté le 07-Mars-2021)

[8] : Sans auteur, « Définition CVSS 'Common Vulnerability Scoring System' ».En ligne :https://www.certist.com/public/fr/SO_detail?code=cvss%20v3&format=html#:~:text=CVSS%20(Common%20Vulnerability%20Scoring%20System,crit%C3%A8res%20utilis%C3%A9s%20pour%20ce%20calcul.3(consulté le 10-Avril-2021)

[9] :Sans auteur, « Gestion de vulnérabilité ».En ligne :https://www.cyberswat.ca/importance-gestion-vulnerabilites-processus/(consulté le 15-Mars-2021)

[10]:ISO 27000, (Clause 3.1).En ligne: https://www.slideshare.net/PabloBlanco10/new-iso27002-2013(consulté le 21-Avril-2021)

[11]:Sans auteur,«Description de logiciel 'Manage-Engine-VMPLUS'».En ligne :https://www.capterra.fr/software/185510/manageengine-vulnerability-manager-plus(consulté le 20-Juin-2021)

[12]:Sans auteur,« Description de logiciel 'Syxsense' ».En ligne : https://www.capterra.fr/software/141605/patch-manager(consulté le 20-Juin-2021)

[13]:Sans auteur, « Description de logiciel 'Netsurion Managed Threat Protection' ».En ligne : https://www.capterra.fr/software/80473/eventtracker(consulté le 20-Juin-2021)

[14]:Sans auteur, « Description de logiciel 'Intruder' ».En ligne : https://www.capterra.fr/software/161379/intruder(consulté le 20-Juin-2021)

[15]:ELITE .juillet2021https://www.elit.dz/639/qui-sommes-nous(consulté le 22-Avril-2021)

[16] :Sans auteur,4janvier 2016, « Définition diagramme de classes UML ».En ligne http://docwiki.embarcadero.com/RADStudio/Sydney/fr/D%C3%A9finition_des_diagrammes_de_classes_UML_1.5(consulté le 10-Juin-2021)

[17] :Sans auteur,4janvier 2016, « Définition diagramme de classes UML ».En ligne http://docwiki.embarcadero.com/RADStudio/Sydney/fr/D%C3%A9finition_des_diagrammes_de_classes_UML_1.5(consulté le 10-Juin-2021)

[18] :TéléchargerXampp, « Definition XAMPP ».En ligne : https://french-mortgage-advice.com/xampp-en-francais-24/

[19] : Lardinois, Frederic (April 29, 2015). "Microsoft Launches Visual Studio Code, A Free Cross-Platform Code Editor For OSX, Linux And Windows".« Definition Visual Studio Code ».En ligne:https://techcrunch.com/2015/04/29/microsoft-shocks-the-world-with-visual-studio-code-a-free-code-editor-for-os-x-linux-and-windows/(consulté le 22-Juin-2021)

[20]:Laravel documentation,«Definition Laravel».En ligne :https://laravel.com/docs/4.2/introduction(consulté le 22-Juin-2021)

[21]:Sans auteur, « Définition JSON ».En ligne :https://www.json.org/json-en.html

[22]:Sans auteur,«Definition Middleware».En ligne :https://www.tutorialspoint.com/laravel/laravel_middleware.htm(consulté le 22-Juin-2021)

[23]:Fahmida Yesmin,Septembre2020,«Definition CSRF».En ligne https://linuxhint.com/laravel_csrf_protection/(consulté le 22-Juin-2021)

[24]:Sans auteur, « Définition Bootstrap».En ligne:https://diallorama.wordpress.com/conception-web/

[25]:Laravel documentation,«Procédure d'excution».En ligne :https://laravel.com/docs/8.x/lifecycle. (consulté le 22-Juin-2021)