République Algérienne Démocratique et Populaire

Ministère de l’Enseignement Supérieur et de la Recherche Scientifique

A picture containing logo

Description automatically generatedUniversité Benyoucef Benkhedda-Alger1

Faculté des sciences

Département Informatique

Projet de Fin d’Etudes pour l’obtention du diplôme de la Licence en Informatique

**Spécialité :** Systèmes Informatiques (SI)

**Thème**

**Conception et Développement d’une Plateforme en ligne pour les Statistiques et Veille Sécuritaire en Algérie**

Encadré par : Réalisé par :

- Mr. Rahmani Amine - Feddane Chaima

- Mr. Abdelli Aniss - Hamidani Khalil

**2022/2023**

**Remerciement**

**Dédicaces**

**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.

Nous avons réalisé une application Web qui permet de collecter des données sur les incidents liés à la sécurité, de les traiter et de les analyser pour fournir des statistiques précises sur la criminalité et la sécurité dans l'Algérie. En outre, notre plateforme dispose également d'une fonctionnalité de scan de services web pour détecter les vulnérabilités potentielles et renforcer la sécurité de ces services. Le mémoire présente les étapes clés de la conception et du développement de la plateforme, ainsi que les techniques utilisées et les résultats obtenus.

**Abstract**

Information theft occurrences have increased along with the broad proliferation and use of digital information, much of which is sensitive. Any organization that wants to prevent unauthorized people from obtaining electronic data must prioritize security.

To give reliable statistics on crime and security in Algeria, we have created a web application that enables the gathering, processing, and analysis of data on security-related incidents. To further reinforce the security of these services and find any potential flaws, our platform now includes a web service scanning functionality.

The study outlines the crucial phases of the platform's design and development, the technologies employed, and the outcomes.

**ملخص**

مع تزايد أهمية المعلومات الرقمية وارتفاع شعبيتها، يتزايد معها معدل سرقة المعلومات، ولذلك يتحتم على المؤسسات ضمان الأمان الكافي لمنع المستخدمين غير المصرح لهم من الوصول إلى البيانات الإلكترونية. ومن أجل تحقيق هذا الهدف، قمنا بتطوير تطبيق ويب يقوم بجمع ومعالجة وتحليل البيانات الأمنية لتقديم إحصائيات دقيقة عن الجريمة والأمن في الجزائراضافة الى تحليل خدمات الويب لتحديد نقاط الضعف وتحسين أمان هذه الخدمات، وذلك لتحقيق أفضل مستويات الحماية الممكنة. يحتوي هذا التقرير على مراحل التصميم والتطوير الرئيسية للمنصة، بالإضافة إلى تفاصيل التقنيات المستخدمة والنتائج المحققة.

**Table de matières**

**Liste de figures**

***Figure 1 :***

***Figure 2 : Site de l’Agence de cybersécurité et de sécurité des infrastructures***

***-CISA-***

***Figure 3 : Le formulaire de déclaration d'incident du site CISA***

**Liste des abréviations**

**IOC** Indicator of Compromise

**UML** Unified Modeling Language

**CISA** Cybersecurity and Infrastructure Security Agency

**Introduction générale**

La sécurité en ligne est un enjeu de plus en plus important dans notre société numérique. Les utilisateurs d'Internet sont confrontés à de nombreux problèmes de sécurité, tels que les attaques de phishing, les virus informatiques, les logiciels malveillants, les attaques par déni de service (DDoS), et bien d'autres. Ces menaces peuvent causer des dommages importants, tels que la perte de données, le vol d'identité, le piratage de comptes en ligne et bien d'autres.

En Algérie, les utilisateurs d'Internet sont confrontés à ces mêmes problèmes de sécurité. Les cybercriminels utilisent des techniques sophistiquées pour exploiter les vulnérabilités des sites web et des applications, et pour compromettre la sécurité des utilisateurs algériens. C'est pourquoi il est important de mettre en place des mesures de sécurité adéquates pour protéger les utilisateurs et les sites web algériens.

La plateforme en ligne pour les statistiques et la veille sécuritaire en Algérie est une solution pour aider les utilisateurs algériens à se protéger contre les menaces en ligne. En permettant de scanner les sites web à la recherche de vulnérabilités potentielles, cette plateforme peut aider les administrateurs de sites à détecter et à corriger les failles de sécurité avant qu'elles ne soient exploitées par des cybercriminels.

En fournissant des statistiques sur les types d'attaques les plus courantes et les méthodes les plus efficaces pour s'en protéger, cette plateforme peut également aider les utilisateurs algériens à mieux comprendre les risques potentiels et à prendre des mesures pour renforcer la sécurité de leurs systèmes. En fin de compte, cette plateforme peut contribuer à améliorer la sécurité en ligne en Algérie, en offrant une solution pratique et efficace pour la veille et la surveillance de la sécurité informatique.

**Plan du mémoire**

En vue d'atteindre cet objectif, la structure suivante a été retenue :

* **Le premier chapitre**, intitulé « Introduction à la sécurité informatique », présente le domaine d'étude et explore les aspects liés à la sécurité informatique.
* **Le deuxième chapitre**, intitulé « Conception », présente les différentes étapes du processus de conception, de la collecte des besoins à la conception détaillée.
* **Enfin, le troisième chapitre**, intitulé « Implémentation », porte sur la réalisation et l’implémentation de l’application ainsi que son fonctionnement.

**Chapitre I : Introduction à la sécurité informatique**

**I.1.** **Introduction**

L'objectif de ce chapitre est de fournir un aperçu de la sécurité informatique, d'examiner ses concepts fondamentaux et de souligner son importance dans le monde numérique actuel.

**I.2. L’organisme d’accueil**

Le Ministère de la Numérisation et des Statistiques en Algérie créé en janvier 2020, est le département ministériel chargé de la mise en place de politiques et de programmes visant à améliorer l'utilisation des technologies de l'information et de la communication (TIC) dans les différents secteurs de la société, ainsi que la production et la gestion des données statistiques.

Ce ministère a pour mission de moderniser l'administration publique en favorisant la numérisation de ses procédures, en facilitant l'accès aux services publics en ligne, en renforçant la sécurité des données numériques, et en encourageant l'innovation dans le domaine des TIC.

Il est également responsable de la production et de la diffusion de données statistiques fiables et pertinentes, qui sont nécessaires pour la prise de décisions éclairées en matière de planification, de suivi et d'évaluation des politiques économiques, sociales et environnementales en Algérie.

**I.2.1 Service de Sous-direction de la Cybersécurité**

Est une entité chargée de la sécurité informatique et de la protection des données numériques au sein du ministère. Elle est responsable de la mise en place de mesures visant à protéger les systèmes d'information et les données électroniques contre les cyberattaques, les virus informatiques, le piratage et les autres menaces liées à la sécurité numérique.

**I.3. Définitions**

1. IOC :

Est l'acronyme de "Indicator of Compromise" ou "Indicateur de compromission" en français. Il s'agit d'un élément de preuve qui indique qu'un système informatique a été compromis ou qu'une activité malveillante a eu lieu. Les IOC peuvent prendre diverses formes, notamment des fichiers de logs, des adresses IP, des noms de domaine, des signatures de virus, des hash de fichiers, des comportements suspects, des identifiants de connexion, des emails suspects, etc. Les IOC sont utilisés par les professionnels de la sécurité informatique pour détecter, prévenir et enquêter sur les incidents de sécurité, ainsi que pour mettre en place des mesures de protection et de remédiation. Les IOC sont également largement utilisés dans les systèmes de détection et de réponse aux incidents de sécurité (SIEM), qui permettent aux organisations de surveiller en temps réel les activités suspectes sur leurs réseaux et de détecter les menaces potentielles.

1. Sécurité informatique :

Ensemble de mesures de sécurité physiques, logiques et administratives, et de mesures d'urgence, mises en place dans une organisation, en vue d'assurer la protection de ses biens informatiques, la confidentialité des données de son système d'information et la continuité de service. La sécurité informatique comporte trois aspects : la protection physique des installations, la protection des données contre la consultation, la modification ou la dégradation, effectuées de façon volontaire ou accidentelle par des personnes non autorisées, et la protection de la fiabilité de ces données (c'est-à-dire la conservation de leur contenu au fil du temps ou lors de leur traitement).

1. Vulnérabilité :

Est une faiblesse ou une lacune dans un système informatique ou dans une application qui peut être exploitée par des attaquants pour pénétrer ou perturber le système. Les vulnérabilités peuvent être causées par des erreurs de conception, des défauts de codage, des configurations inappropriées, ou des problèmes de mise à jour. Les attaquants exploitent souvent les vulnérabilités pour accéder à des données sensibles, installer des logiciels malveillants ou perturber le fonctionnement normal du système.

1. Attaque :

En informatique, est un acte malveillant visant à compromettre ou à perturber un système informatique, un réseau ou une application. Les attaques peuvent prendre de nombreuses formes, notamment des virus, des malwares, des tentatives d'intrusion, des attaques par déni de service, des attaques de phishing, etc. Les attaquants peuvent chercher à voler des données sensibles, à perturber les opérations normales du système, à détruire des informations ou à compromettre la sécurité des utilisateurs.

**I.4. Analyse vulnérabilités**

L'analyse de vulnérabilités est un processus visant à identifier les vulnérabilités dans un système informatique, une application ou un réseau, afin de les corriger avant qu'elles ne soient exploitées par des attaquants. Le processus commence généralement par une évaluation de la sécurité du système, qui peut comprendre des tests de pénétration, des analyses de configuration, des scans de vulnérabilités et d'autres techniques. Les vulnérabilités identifiées sont ensuite évaluées en termes de leur impact potentiel sur le système et de la probabilité qu'elles soient exploitées. Une fois les vulnérabilités prioritaires identifiées, des correctifs sont appliqués pour réduire les risques. L'analyse de vulnérabilités est un processus continu, car de nouvelles vulnérabilités peuvent apparaître en raison de changements dans les systèmes, les applications ou les menaces. Par conséquent, il est important de maintenir les systèmes à jour et de réaliser des analyses de vulnérabilités régulières pour maintenir une posture de sécurité optimale.

**I.5. Exemple d’étude**

À titre d'exemple pour cette étude, on a opté pour le site CISA qui est un site d'une agence gouvernementale américaine chargée de protéger l'infrastructure critique des États-Unis contre les menaces de cybersécurité.

***Figure 2 : Site de l’Agence de cybersécurité et de sécurité des infrastructures***

***-CISA-***

Ce site propose plusieurs formulaires à remplir pour signaler différents types de problèmes de cybersécurité. La figure suivante, représente le formulaire de déclaration d'incident (Incident Reporting Form), qui se compose de plusieurs sections. Les sections du formulaire incluent des informations sur l'organisation signalant l'incident, des détails sur l'incident ou la vulnérabilité, et des informations sur les mesures de sécurité en place.

En remplissant le formulaire, l'utilisateur peut fournir à la CISA des informations détaillées sur l'incident ou la vulnérabilité, ce qui permet à l'agence de fournir rapidement une assistance technique et opérationnelle pour atténuer les risques.

Graphical user interface, text, application, email

Description automatically generated

***Figure 3 : Le formulaire de déclaration d'incident du site CISA***

**I.6. Conclusion**

A la fin du présent chapitre, nous avons constaté que la sécurité informatique est un domaine crucial dans le monde numérique actuel. Nous avons défini on quoi consiste la sécurité informatique, ainsi que les indicateurs de compromission (IOC), les vulnérabilités et les attaques. Nous nous sommes aussi penchés sur l'analyse des vulnérabilités, une méthode d'identification et de correction des vulnérabilités dans les systèmes informatiques.

**Chapitre II : Conception**

**II.1. Introduction**

La conception est une étape clé dans tout projet de développement logiciel. Afin de la réussir, il est nécessaire de suivre une méthodologie rigoureuse et structurée. Ce chapitre se concentre sur les différentes étapes de la conception, en mettant l'accent sur l'analyse des besoins et la conception avec les diagrammes de cas d’utilisation, de classe et de séquence. Les différentes techniques utilisées pour collecter, analyser et formaliser les besoins des utilisateurs sont détaillées, et les différents types de diagrammes utilisés en conception logicielle sont présentés pour concevoir une solution adaptée.

**II.2. Analyse des besoins**

Cette étape consiste à identifier et comprendre les besoins des utilisateurs ainsi que les exigences du système, afin de définir les fonctionnalités et les caractéristiques nécessaires pour répondre à ces besoins.

**II.2.1 Les besoins fonctionnels**

Il s'agit des tâches ou des actions que les utilisateurs doivent pouvoir accomplir avec notre système :

* Un citoyen peut déclarer, en anonyme, un acte suspect de piratage ou de tentative d’attaque.
* Une administration peut suivre l’état d’actualité de sécurité en Algérie avec les nouvelles vulnérabilités liées aux équipements et applications utilisés.
* Un tableau de bord des statistiques officielles de nombres d’attaques par type et par cible au service de l’état pour le suivi et la veille sécuritaire.

**II.2.2 Les besoins non fonctionnels**

Afin d’assurer le bon fonctionnement de notre application et pour garantir la satisfaction de l’utilisateur, des contraintes doivent être prises en compte tout au long du développement du notre projet :

* **Sécurité** : La plateforme doit fournir un haut niveau de sécurité afin de protéger les données et les utilisateurs contre les attaques malveillantes.
* **Performance** : L’application doit être rapide et réactive pour permettre aux utilisateurs de naviguer rapidement à travers les différentes sections.
* **Accessibilité** : L’application doit être conçue pour être accessible à tous les utilisateurs, y compris ceux ayant des besoins particuliers en termes d'accessibilité.
* **Fiabilité** : La plateforme doit être fiable et offrir une grande disponibilité afin que les utilisateurs puissent l'utiliser sans interruption.

**II.3. Conception**

Dans cette section, nous avons choisi de travailler avec **UML**, qui est un langage de modélisation graphique servant à décrire les processus et les structures des systèmes logiciels. Le modèle UML est composé de plusieurs diagrammes, chacun ayant une fonction spécifique. Les diagrammes suivants sont présentés dans le cadre de cette étude :

**II.3.1 Le diagramme de cas d’utilisation :**

Le diagramme de cas d'utilisation de cette application permettra de visualiser les différentes actions et interactions possibles entre les utilisateurs et le système.

1. **Spécification des acteurs du système :**

Dans le contexte d'un diagramme de cas d'utilisation, un acteur représente un utilisateur externe au système ou une entité qui interagit avec le système.

Voici les acteurs principaux impliqués dans notre application :

* **Utilisateur :** il peut être un citoyen, une entreprise ou une organisation.
* **Administrateur :** il représente l’informaticien de l’organisme d’accueil.

1. **Spécification des tâches associées aux acteurs du système :**

**Une tâche :** représente l'ensemble des différentes fonctions auxquelles un acteur peut accéder.

* **Les descriptions textuelles des cas d’utilisation :**

|  |
| --- |
| **Cas :** Remplir un formulaire de déclaration d’incident. |
| **Résumé :** Procédure de signalement d’un problème informatique à l’aide du remplissage d’un formulaire d’incident. |
| **Acteur primaire :** L’utilisateur. |
| **Acteur secondaire :** L’administrateur. |
| **Pré-conditions:** L'utilisateur fournisse ses informations de contact. |
| **Scénario nominal :**   1. L’utilisateur doit s'authentifier en entrant ses informations de connexion. 2. L'utilisateur fournit une description détaillée de l'incident de sécurité, y compris la date et l'heure à laquelle l'incident s'est produit, ainsi que toute information pertinente sur la nature de l'incident. 3. L'utilisateur est également invité à déclarer l'impact de l'incident, en évaluant le niveau de gravité et les conséquences potentielles pour l'organisation. 4. Une fois que le formulaire est rempli, l'utilisateur peut le soumettre pour examen et traitement ultérieur. 5. L’administrateur collecte les informations et traite les données. |

1. **Description textuelle de « Remplir un formulaire » :**
2. **Description textuelle de « Signaler un indicateur de compromission » :**

|  |
| --- |
| **Cas :**  Signaler un indicateur de compromission. |
| **Résumé :** Compléter un formulaire afin de signaler un indicateur de compromission. |
| **Acteur primaire :** L’utilisateur. |
| **Acteur secondaire :** L’administrateur. |
| **Pré-conditions :** |
| **Scénario nominal :** |

1. **Description textuelle de « scanner un service web » :**

|  |
| --- |
| **Cas :**  Scanner un service web. |
| **Résumé :** Permet de rechercher activement des vulnérabilités potentielles dans les applications web. |
| **Acteur primaire :** L’utilisateur. |
| **Acteur secondaire :** L’administrateur. |
| **Pré-conditions:** |
| **Scénario nominal :** |

**II.3.2 Le diagramme de classe :**

**II.3.3 Le diagramme de séquence :**

**II.4. Conclusion**

Pour conclure, le chapitre consacré à la conception a souligné l'importance de cette phase dans le processus de développement logiciel. Nous avons vu comment l'analyse des besoins est un élément fondamental pour définir une solution logicielle qui répond de manière optimale aux attentes des utilisateurs. Les différents types de diagrammes UML, tels que les diagrammes de classe, de séquence et de cas d'utilisation, ont été présentés comme des outils indispensables pour modéliser les différentes vues et interactions entre les éléments du système.

**Bibliographie**

<https://lesdefinitions.fr/>

<https://www.microsoft.com/fr-ca/security/business/security-101/what-is-malware>

https://www.cisa.gov/forms/report