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**

With the widespread growth and use of digital information, much of which is confidential, there has also been an increase in incidents of information theft. Security is very important for any organization to prevent unauthorized users from accessing electronic data.

We have developed a web application that allows for the collection, processing, and analysis of data on security-related incidents to provide accurate statistics on crime and security in Algeria. Additionally, our platform also features a web service scanning functionality to detect potential vulnerabilities and strengthen the security of these services.

The report presents the key steps in the design and development of the platform, as well as the technologies used, and the results obtained.

**ملخص**

مع نمو واستخدام المعلومات الرقمية الشائعة، والتي يتم جزء كبير منها بسرية، زادت أيضًا حوادث سرقة المعلومات. الأمان مهم للغاية لأي منظمة لتجنب وصول المستخدمين غير المصرح لهم إلى البيانات الإلكترونية.

لقد قمنا بتطوير تطبيق ويب يتيح جمع البيانات المتعلقة بحوادث الأمن، ومعالجتها وتحليلها لتوفير إحصائيات دقيقة حول الجريمة والأمن في الجزائر. بالإضافة إلى ذلك، تتميز منصتنا أيضًا بوظيفة فحص خدمات الويب لاكتشاف الثغرات المحتملة وتعزيز أمان هذه الخدمات.

يقدم التقرير الخطوات الرئيسية في تصميم وتطوير المنصة، بالإضافة إلى التقنيات المستخدمة والنتائج المحققة.

**Table de matières**

**Liste de figures**

**Liste des abréviations**

**IOC** Indicator of Compromise

**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. 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.3. 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.4. Exemple d’étude**

**I.5. 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.

**Bibliographie**

https://lesdefinitions.fr/