

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 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 :

Mr. Rahmani Amine
Mr. Abdelli Aniss

Réalisé par :

Feddane Chaima
Hamidani Khalil

2022/2023

Remerciement

*Nous souhaitons exprimer nos sincères remerciements à **Dieu**, qui nous a accordé la guidance et la force nécessaires pour mener à bien ce mémoire de fin d'études. Sans son soutien infaillible, rien n'aurait été possible.*

*Nous aimerais également adresser nos profonds remerciements à nos encadreurs, **Monsieur Rahmani Amine** et **Monsieur Abdelli Aniss**, pour leur expertise, leur patience et leur précieuse contribution tout au long de notre parcours. Leurs conseils éclairés et leur disponibilité ont été d'une aide inestimable, nous permettant d'atteindre nos objectifs de recherche.*

*Nos remerciements vont également à l'organisme d'accueil, le **Ministère de la Numérisation et des Statistiques**, pour avoir offert un environnement propice à notre apprentissage et à nos travaux de recherche. Leur collaboration et leur soutien ont grandement enrichi notre expérience.*

*Enfin, nous tenons à exprimer nos sincères remerciements aux **membres du jury** qui ont accepté d'honorer notre travail en évaluant notre mémoire.*

Dédicaces

Avec une profonde gratitude et une humble reconnaissance, je souhaite dédier ce modeste travail à ceux qui, peu importe les mots choisis, restent indescriptibles dans leur importance.

À ma chère maman,

Qui a été ma source inépuisable d'amour, de soutien et d'encouragement tout au long de ce parcours académique. Tes mots doux et ton inébranlable croyance en moi m'ont donné la force de persévérer et de réaliser ce mémoire de fin d'étude.

À mon cher papa,

Dont la sagesse et les valeurs m'ont inspiré chaque jour. Tu as été mon modèle de détermination et de travail acharné. Je te remercie du fond du cœur pour ta présence et ta confiance en moi.

À mes frères et sœurs,

Mes compagnons de vie et mes alliés inébranlables. Votre soutien inconditionnel, vos encouragements et votre compréhension ont été d'une valeur inestimable. Vos mots d'encouragement et votre présence ont allégé les moments de doute et ont renforcé ma détermination. Merci d'avoir toujours été là pour moi.

À mon binôme de travail Khalil,

Qui a partagé cette aventure académique avec moi. Notre collaboration étroite, notre échange d'idées et notre soutien mutuel ont été essentiels pour mener à bien ce mémoire. Ta perspicacité, ton engagement et ton travail assidu ont été une véritable source de motivation. Merci d'avoir été un partenaire de confiance et de m'avoir accompagné tout au long de ce parcours.

Enfin, à mes amis fidèles,

Qui ont été présents à chaque étape de ma vie étudiante. Votre soutien inconditionnel, votre écoute bienveillante et vos encouragements ont illuminé les moments de stress et de doute. Merci d'avoir partagé mes joies, mes peines et mes réussites. Vous êtes une source d'inspiration et de bonheur inestimable.

Dédicaces

Je dédie humblement ce travail avec un amour profond à ceux qui sont au-delà des mots, dont aucune expression ne pourra jamais rendre justice à l'immensité de ce que vous représentez pour moi.

À ma chère maman, qui a été ma plus grande source d'amour, de soutien et d'inspiration. Ta bienveillance inconditionnelle et tes encouragements constants ont été les piliers de ma réussite académique. Je te dédie ce mémoire avec une profonde gratitude pour tout ce que tu as fait pour moi.

À mon cher papa, dont la force, et les conseils avisés ont été une boussole tout au long de mon parcours. Ta présence constante et ton soutien inébranlable m'ont donné la confiance nécessaire pour aller de l'avant. Je t'exprime ma reconnaissance éternelle pour ton amour et ton soutien indéfectibles.

À mon frère et ma sœur, mes compagnons de vie et mes amis les plus proches. Votre présence, vos encouragements et votre complicité ont été une source de réconfort et de motivation. Je vous suis reconnaissant pour votre soutien inébranlable.

À mes chers grands-parents, qui m'ont transmis leur sagesse, leur expérience et leur amour inconditionnel. Vos valeurs, vos récits inspirants et votre soutien indéfectible ont été une source d'inspiration et de motivation tout au long de ce parcours académique. Je vous dédie ce mémoire avec une profonde gratitude.

À mon binôme de travail Chaïma, qui a partagé cette aventure académique avec moi. Je te souhaite le meilleur pour tes futurs projets, tant sur le plan personnel que professionnel. Que nos chemins se croisent à nouveau et que nos collaborations continuent d'apporter des fruits dans le futur. Merci encore pour cette formidable aventure.

Et, à mes amis chers, qui ont été mes piliers de soutien tout au long de ce parcours. Votre présence joyeuse, vos encouragements constants et vos moments de détente ont rendu cette expérience inoubliable. Je vous suis profondément reconnaissant pour votre amitié sincère et votre soutien indéfectible.

HAMIDANI KHALIL

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. L'objectif final de notre application est de faciliter la collecte d'information auprès des secteurs publics et privés afin de tenir à jour une cartographie nationale des risques liés au numérique. 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 analyzing data on security-related incidents. Our platform now includes a web service scanning functionality to reinforce these services' security further and find any potential flaws. Our app aims to facilitate the collection of information from the public and private sectors to keep the national digital risk map up to date. 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 لمنع المستخدمين غير المصرح لهم من الوصول إلى البيانات الإلكترونية. وأجل هذا قمنا بتطوير تطبيق ويب يقوم بجمع وتحليل البيانات الأمنية لتقديم إحصائيات دقيقة عن الجريمة والأمن في الجزائر إضافة إلى تحليل خدمات الويب لتحديد نقاط الضعف وتحسين أمان هذه الخدمات، وذلك لتحقيق أفضل مستويات الحماية. الهدف النهائي للتطبيق هو تسهيل جمع المعلومات من القطاع العام والخاص من أجل تحديث قواعد بيانات المخاطر الرقمية. يحتوي هذا التقرير على مراحل التصميم والتطوير الرئيسية للمنصة، بالإضافة إلى تفاصيل التقنيات المستخدمة والنتائج المحققة.

Table de matières

Introduction générale	1
Plan du mémoire	2
Chapitre I : Organisme d'accueil.....	3
I.1 Introduction	3
I.2 Présentation du ministère.....	3
I.3 Composition du Ministère.....	3
I.3.1 Organigramme du ministère	3
I.3.2 La direction des technologies de la numérisation	5
I.3.3 La sous-direction de la cybersécurité.....	5
I.4 La sécurité informatique et la matrice ATT&CK de MITRE	5
I.5 Conclusion.....	6
Chapitre II : Introduction à la sécurité informatique	7
II.1 Introduction	7
II.2 Définitions	7
II.3 Analyse vulnérabilités	8
II.4 Exemple d'étude.....	8
II.5 Conclusion.....	9
Chapitre III : Conception	10
III.1 Introduction	10
III.2 Analyse des besoins	10
III.2.1 Les besoins fonctionnels	10
III.2.2 Les besoins non fonctionnels	10
III.3 Conception	11
III.3.1 Le diagramme de cas d'utilisation.....	11
III.3.2 Le diagramme de classe	14
III.3.3 Le diagramme de séquence	14
III.4 Conclusion.....	16
Chapitre IV: Implémentation	17
IV.1 Introduction.....	17
IV.2 Technologies et APIs.....	17
IV.2.1 Les langages utilisés	17
IV.2.2 Outils de développement.....	18
IV.2.3 APIs.....	19

IV.3 L'outil Nmap.....	19
IV.4 Structure de la base de données.....	19
IV.5 Présentation des fonctionnalités générales de l'application.....	20
IV.5.1 La page d'accueil	20
IV.5.2 Remplir un formulaire d'incident.....	21
IV.5.3 Signaler un indicateur de compromission.....	23
IV.5.4 Scanner un service web	24
IV.6 Conclusion	24
Conclusion générale	25
Annexe.....	26
Bibliographie	32

Liste de figures

<i>Figure 1: Orgaigramme de l'organisme d'accueil</i>	4
<i>Figure 2: Matrice des menaces accusatoires des algorithmes d'apprentissage</i>	6
<i>Figure 3: Site de l'Agence de cybersécurité -CISA-</i>	8
<i>Figure 4: Le formulaire de déclaration d'incident du site CISA</i>	9
<i>Figure 5: Diagramme de cas d'utilisation.....</i>	11
<i>Figure 6: Diagramme de classe</i>	14
<i>Figure 7: Diagramme de séquence pour remplir un formulaire d'incident.....</i>	15
<i>Figure 8: Diagramme de séquence pour signaler un indicateur de compromission.....</i>	15
<i>Figure 9: Diagramme de séquence pour scanner un service web.....</i>	16
<i>Figure 10: La page d'accueil.....</i>	20
<i>Figure 11: Le formulaire d'incident.....</i>	21
<i>Figure 12: Autres sections du formulaire d'incident</i>	22
<i>Figure 13: Le formulaire d'IOC.....</i>	23
<i>Figure 14: Scanner un service web.....</i>	24

Liste des abréviations

ATT&CK Adversarial Tactics, Techniques, and Common Knowledge

IOC Indicator of Compromise

CISA Cybersecurity and Infrastructure Security Agency

UML Unified Modeling Language

HTML Hypertext Markup Language

CSS Cascading Style Sheets

SQL Structured Query Language

API Application Programming Interface

CVE Common Vulnerabilities and Exposures

Nmap Network Mappe

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

Chapitre I : Organisme d'accueil

I.1 Introduction

Dans ce chapitre, on présentera le Ministère de la Numérisation et des Statistiques (MNS) et ses fonctions, ainsi que la direction qui a fait l'objet de notre stage, à savoir la Direction des Technologies de la Numérisation (DTN) et de sa Sous-Direction de Cybersécurité (SDCSI).

I.2 Présentation du ministère

Le Ministère de la Numérisation et des Statistiques (MNS) s'inscrit comme un leader et décideur important dans le domaine du numérique en Algérie, et créé en vertu du décret exécutif n° 20-363 du 19 Rabie Ethani 1442 Correspondant au 5 décembre 2020 fixant les attributions du ministère. [\[1\]](#)

I.3 Composition du Ministère

I.3.1 Organigramme du ministère

Le ministère de la Numérisation et des Statistiques se compose d'un secrétariat général, deux (02) directions générales qui se déclinent en directions centrales et sous-directions selon le champ de compétences défini par les missions et attributions conformément au décret susmentionné, et le cabinet du Ministre. Le schéma suivant présente l'organigramme général du Ministère.

Notre stage de fin d'étude s'effectue au niveau de la *Sous-Direction de la Cybersécurité* au sein de la Direction des Technologies de la Numérisation.

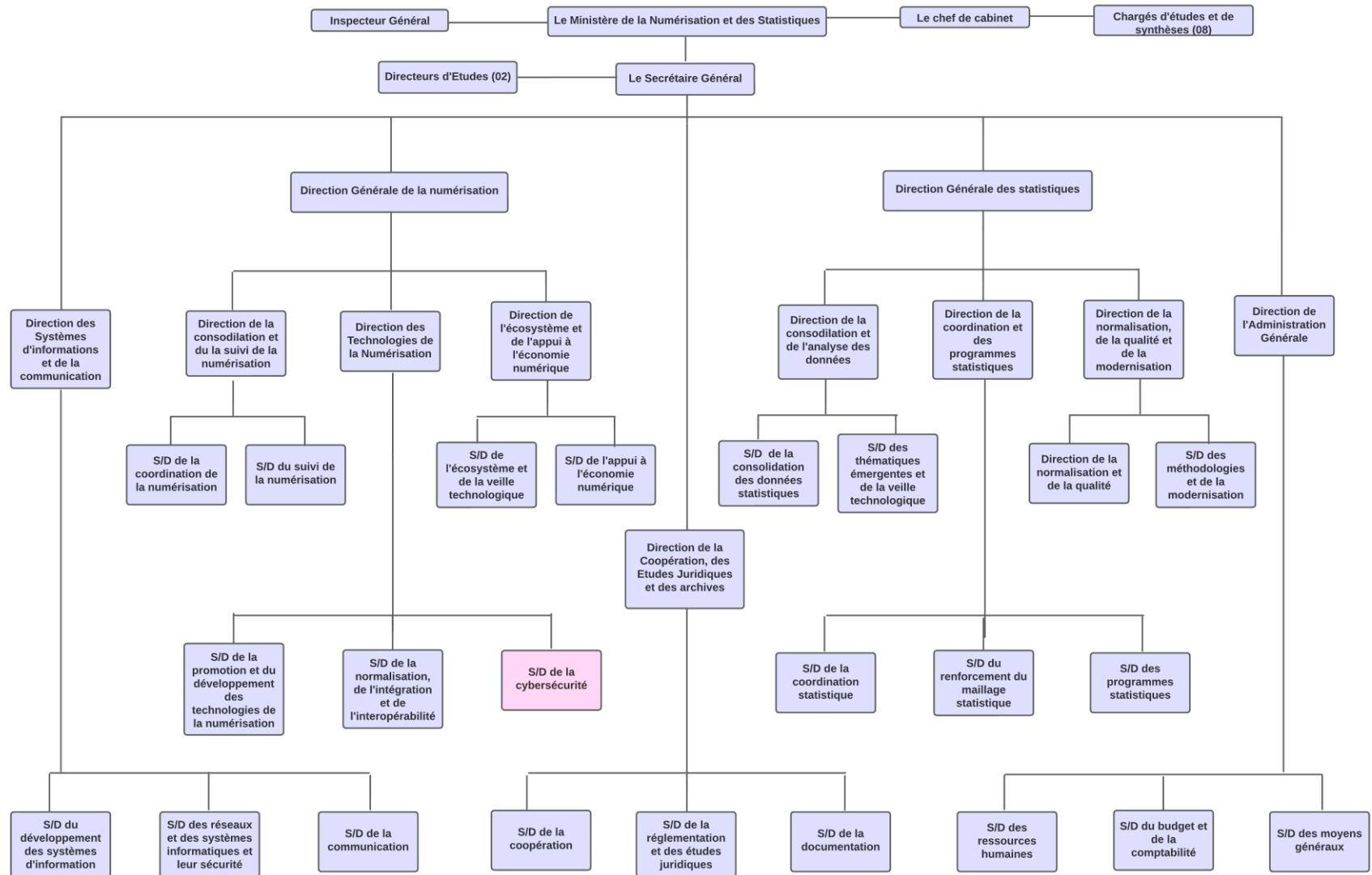


Figure 1: Orgaigramme de l'organisme d'accueil

I.3.2 La direction des technologies de la numérisation

Cette direction est chargée notamment :

- De promouvoir l'usage des technologies du numérique ;
- D'œuvrer, de concert avec les départements ministériels, à la mise en place d'un système d'information gouvernemental intégré d'aide à la décision ;
- De proposer toute action visant le développement du capital humain et des compétences nationales requises pour le développement du numérique ;
- De mener les études nécessaires à l'élaboration du cadre légal et réglementaire relatif au développement de la numérisation ;

Elle comprend trois (3) sous-directions

- a) La sous-direction de la promotion et du développement des technologies de la numérisation,
- b) La sous-direction de la normalisation, de l'intégration et de l'interopérabilité,
- c) La sous-direction de la cybersécurité.

I.3.3 La sous-direction de la cybersécurité

Elle est notamment chargée de :

- De participer à l'élaboration et à la mise en œuvre de la politique nationale de sécurité des systèmes d'information ;
- De participer à la mise à jour du référentiel national de la sécurité de l'information et de veiller à son application, au sein du secteur ;
- De participer à l'élaboration de la stratégie nationale du développement de la certification électronique et de participer à sa mise en œuvre ;

Ce stage de fin d'étude s'inscrit dans le cadre du programme de la sous-direction concernant l'élaboration et la tenue à jour de la cartographie des risques et menaces encourus par les systèmes d'information et du secteur de la numérisation en général.

I.4 La sécurité informatique et la matrice ATT&CK de MITRE

La sécurité informatique est devenue une préoccupation majeure dans le monde d'aujourd'hui en raison de l'évolution constante des attaques informatiques sophistiquées. Pour faire face à ces menaces, de nombreux pays, dont les États-Unis, ont développé des matrices

des risques et des attaques informatiques pour identifier et répertorier les vulnérabilités potentielles pouvant affecter l'économie, la sécurité et la politique du pays. Un exemple notable est la matrice ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

Contrairement aux approches antérieures axées sur les outils et les logiciels malveillants, la matrice ATT&CK se concentre sur les actions offensives et les tactiques utilisées par les adversaires pour interagir avec les systèmes informatiques. Elle classe ces actions en techniques et tactiques, offrant une vue d'ensemble des objectifs et des méthodes des attaquants.[\[2\]](#)

Reconnaissance	Initial Access	Execution	Persistence	Model Evasion	Exfiltration	Impact
Acquire OSINT information: (Sub Techniques) 1. Arxiv 2. Public blogs 3. Press Releases 4. Conference Proceedings 5. Github Repository 6. Tweets	Pre-trained ML model with backdoor	Execute unsafe ML models (Sub Techniques) 1. ML models from compromised sources 2. Pickle embedding	Execute unsafe ML models (Sub Techniques) 1. ML models from compromised sources 2. Pickle embedding	Evasion Attack (Sub Techniques) 1. Offline Evasion 2. Online Evasion	Exfiltrate Training Data (Sub Techniques) 1. Membership inference attack 2. Model inversion	Defacement
ML Model Discovery (Sub Techniques) 1. Reveal ML model ontology – 2. Reveal ML model family –	Valid account	Execution via API	Account Manipulation		Model Stealing	Denial of Service
Gathering datasets	Phishing	Traditional Software attacks	Implant Container Image	Model Poisoning	Insecure Storage 1. Model File 2. Training data	Stolen Intellectual Property
Exploit physical environment	External remote services			Data Poisoning (Sub Techniques) 1. Tainting data from acquisition – Label corruption 2. Tainting data from open source supply chains 3. Tainting data from acquisition – Chaff data 4. Tainting data in training environment – Label corruption		Data Encrypted for Impact Defacement
Model Replication (Sub Techniques) 1. Exploit API – Shadow Model 2. Alter publicly available, pre-trained weights	Exploit public facing application			Stop System Shutdown/Reboot		
Model Stealing	Trusted Relationship					

Figure 2: Matrice des menaces accusatoires des algorithmes d'apprentissage

En Algérie, il existe actuellement une lacune en termes de matrice générale des risques et des attaques informatiques. La présente étude constitue une première étape cruciale vers la résolution de cette lacune en Algérie, en établissant les fondements nécessaires pour la création d'une matrice nationale des risques et des attaques informatiques. Cette initiative vise à renforcer la sécurité de l'information.

I.5 Conclusion

Ce chapitre nous a permis de prendre connaissance de la composition du ministère et de mieux assimiler les différentes tâches de la sous-direction de la cybersécurité (SDSCI).

Chapitre II : Introduction à la sécurité informatique

II.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.

II.2 Définitions

1. Indicateur de compromission (IOC)

Est l'acronyme de "Indicator of Compromise". Ils sont utilisés en sécurité informatique pour détecter et prévenir les activités malveillantes sur un système informatique. Ils peuvent prendre différentes formes telles que des fichiers de logs, des adresses IP, des noms de domaine, etc. Les professionnels de la sécurité informatique les utilisent pour surveiller les réseaux en temps réel et détecter les menaces potentielles.

2. 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 a trois volets : la protection physique des installations, la sécurité des données contre les atteintes volontaires ou accidentelles de personnes non autorisées, et la préservation de la fiabilité des données dans le temps et lors de leur traitement.

3. 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.

4. Attaque

Une attaque informatique est une action malveillante visant à nuire un système, un réseau ou une application, prenant diverses formes telles que virus, malwares, intrusions, phishing, etc. Les attaquants cherchent à voler des données, perturber les opérations, détruire des informations ou compromettre la sécurité des utilisateurs. [3]

II.3 Analyse vulnérabilités

L'analyse de vulnérabilités est un processus qui identifie les failles d'un système informatique, les évalue et les corrige pour empêcher les attaques. Ce processus comprend une évaluation de la sécurité du système, l'identification des vulnérabilités prioritaires et l'application de correctifs pour réduire les risques. Comme de nouvelles vulnérabilités peuvent survenir, il est essentiel de maintenir les systèmes à jour et de réaliser des analyses de vulnérabilités régulières pour assurer une sécurité optimale.

II.4 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. [4]

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.



Figure 3: Site de l'Agence de cybersécurité -CISA-

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.

* Required fields

I am: the impacted user reporting on behalf of the impacted user

1. Your Contact Information

First Name	Last Name	Telephone	Email Address * Required
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

2. Organization Details

What type of organization are you? * Required

Select One

3. Incident Description

When, approximately, did the incident start?

06/20/2023 10:19:26 AM

When was this incident detected? * Required

06/20/2023 10:19:26 AM

From what timezone are you making this report?

Select One

Please enter a brief description of the incident: * Required

4. Impact Details

Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised? * Required

Yes
 No

Figure 4: Le formulaire de déclaration d'incident du site CISA

II.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 ce qu'est 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 III : Conception

III.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.

III.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.

III.2.1 Les besoins fonctionnels

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

- L'utilisateur peut déclarer 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.
- Présentation des dernières informations sur les vulnérabilités pertinentes.

III.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.

III.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 :

III.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.

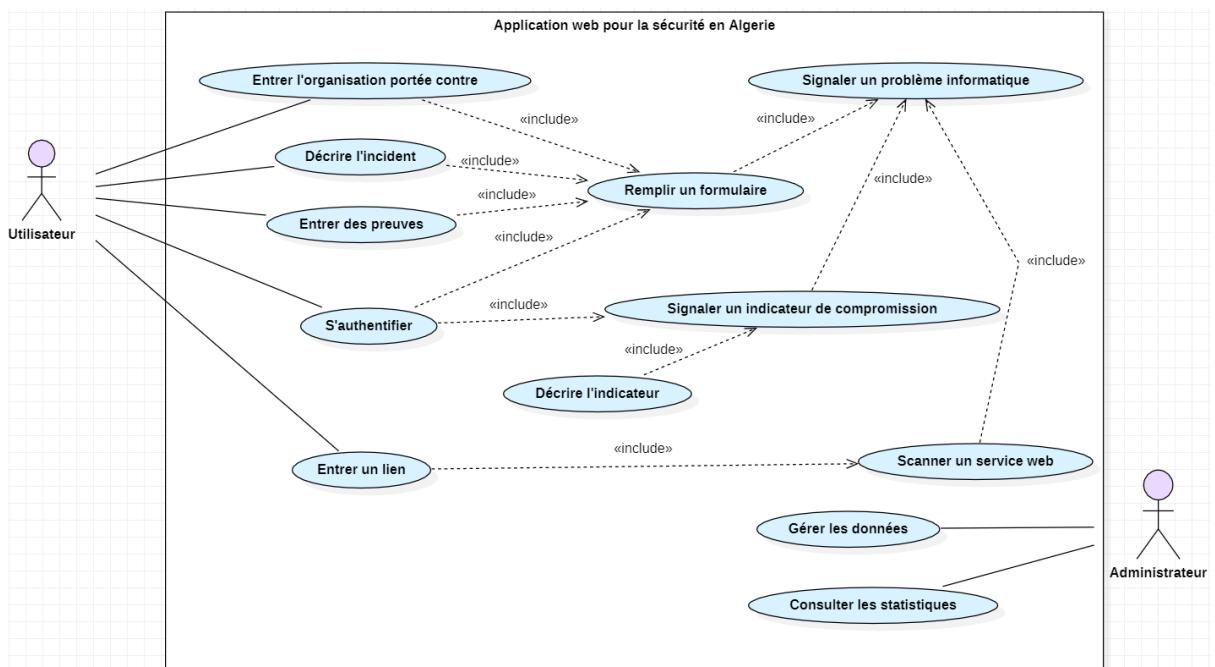


Figure 5: Diagramme de cas d'utilisation

A. 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 agence ou une organisation.
- **Administrateur** : il représente l'informaticien de l'organisme.

B. 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**

1. **Description textuelle de « Remplir un formulaire »**

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 fournit ses informations de contact.
Scénario nominal : 1-L'utilisateur s'authentifie en entrant ses informations de connexion. 2-L'utilisateur entre le nom de l'organisation portée contre laquelle l'incident est signalé. 3-L'utilisateur fournit une description détaillée de l'incident de sécurité, y compris la date et l'heure à laquelle il s'est produit, ainsi que toute information pertinente sur sa nature. 4-L'utilisateur est invité à ajouter des preuves supplémentaires, telles que des documents, des photos ou des vidéos, pour étayer le signalement de l'incident, puis il le soumet pour un traitement. 5-L'administrateur collecte les informations fournies et traite les données conformément aux procédures établies.

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.
Scénario nominal : 1-Le système affiche une page de formulaire de rapport de problème IOC. 2-L'utilisateur s'authentifie en entrant ses informations d'identification. 3-L'utilisateur sélectionne le type d'organisation parmi les options disponibles : individu, secteur privé ou secteur gouvernemental. 4-L'utilisateur entre le lien du site. 5-L'utilisateur sélectionne une catégorie de problème dans une liste déroulante prédefinie. 6-L'utilisateur fournit une description détaillée du problème dans le champ de texte prévu à cet effet, puis il soumet le formulaire. 7-Le système enregistre le rapport de problème IOC dans la base de données.

3. 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.
Scénario nominal : 1-Sur la page de scan, l'utilisateur trouve un champ de texte où il peut entrer le lien du service web qu'il souhaite scanner. 2-L'utilisateur saisit le lien du service web cible dans le champ de texte. 3-Une fois que le lien est saisi, l'utilisateur clique sur le bouton "Scan" pour lancer le processus de scan. 4-Le système commence à analyser le service web spécifié en utilisant des techniques de scan de sécurité.

- 5-Pendant le processus de scan, le système identifie les vulnérabilités, les failles de sécurité et d'autres problèmes potentiels liés au service web.
- 6-Le système génère un rapport détaillé contenant les résultats du scan.
- 7-Le rapport du scan est affiché à l'utilisateur, fournissant des informations sur les vulnérabilités et les problèmes de sécurité identifiés.

III.3.2 Le diagramme de classe

Est l'un des types de diagrammes UML les plus utiles, car il décrit clairement, la structure interne d'un système particulier en modélisant ses classes, ses attributs, ses opérations ainsi que les relations entre la vue statique des objets et leurs comportements.

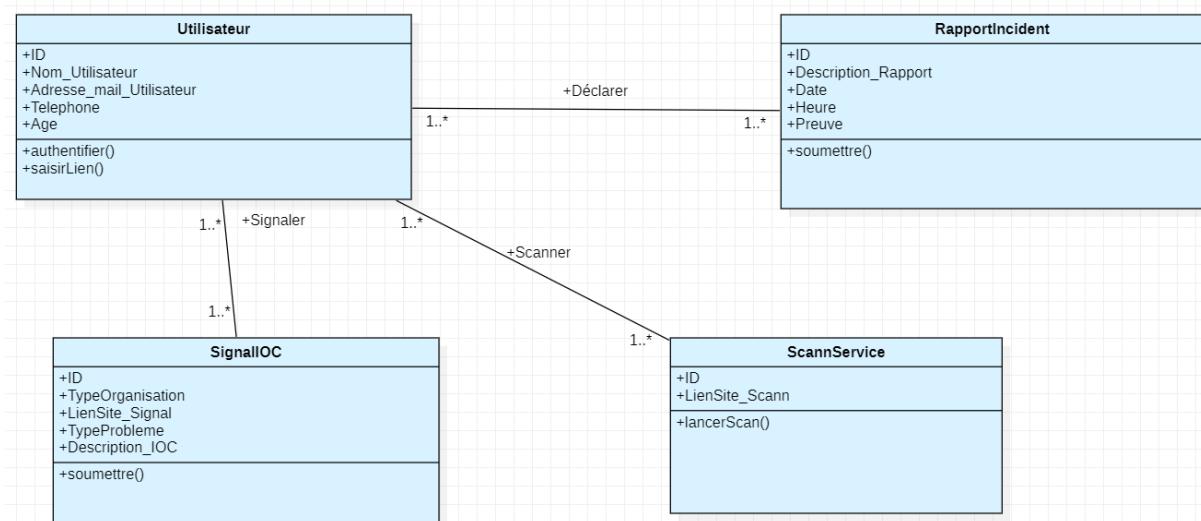


Figure 6: Diagramme de classe

III.3.3 Le diagramme de séquence

C'est un diagramme d'interaction qui met l'accent sur le classement des messages en ordre chronologique. Il contient la reformulation du texte du cas d'utilisation décrite par les scenarios.

1. Diagramme de séquence pour remplir un formulaire d'incident

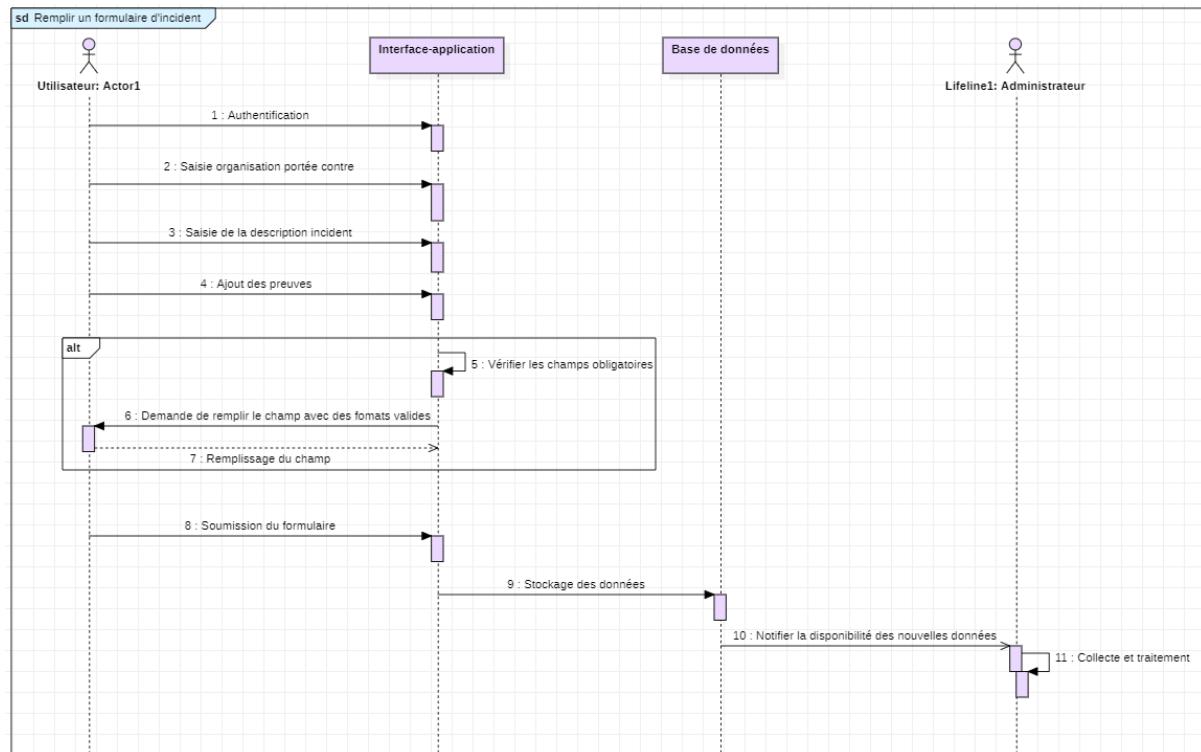


Figure 7: Diagramme de séquence pour remplir un formulaire d'incident

2. Diagramme de séquence pour signaler un indicateur de compromission

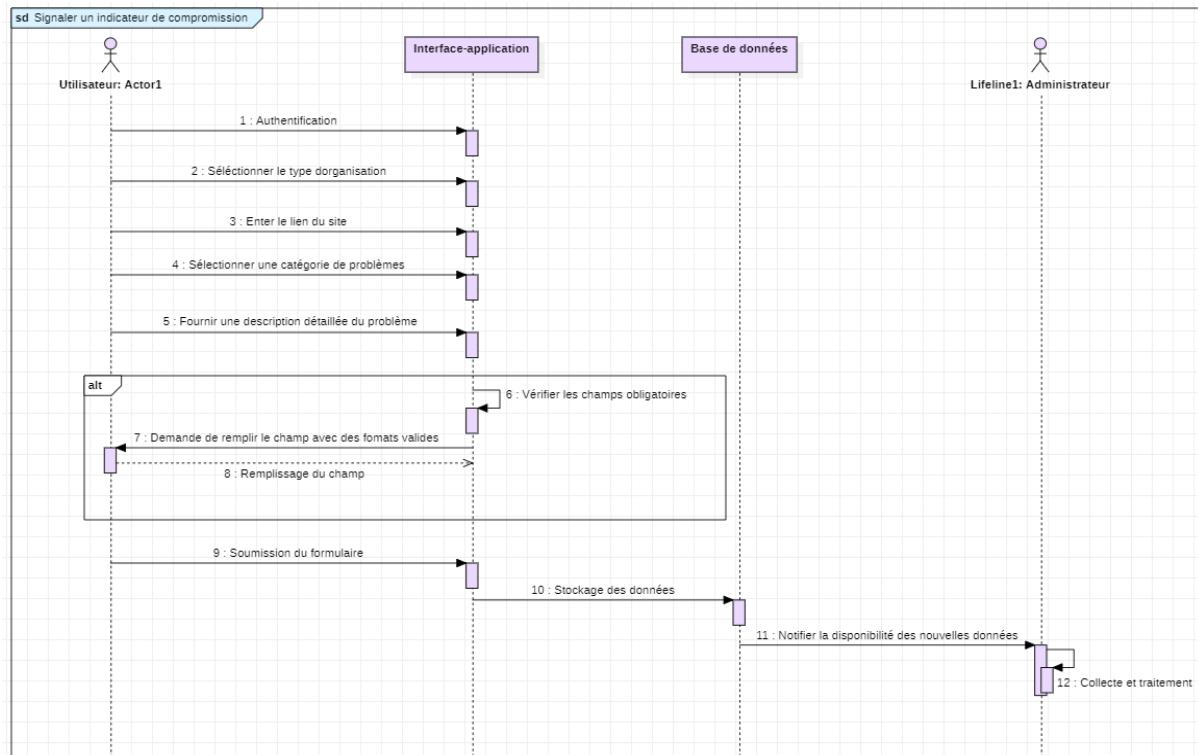


Figure 8: Diagramme de séquence pour signaler un indicateur de compromission

3. Diagramme de séquence pour scanner un service web

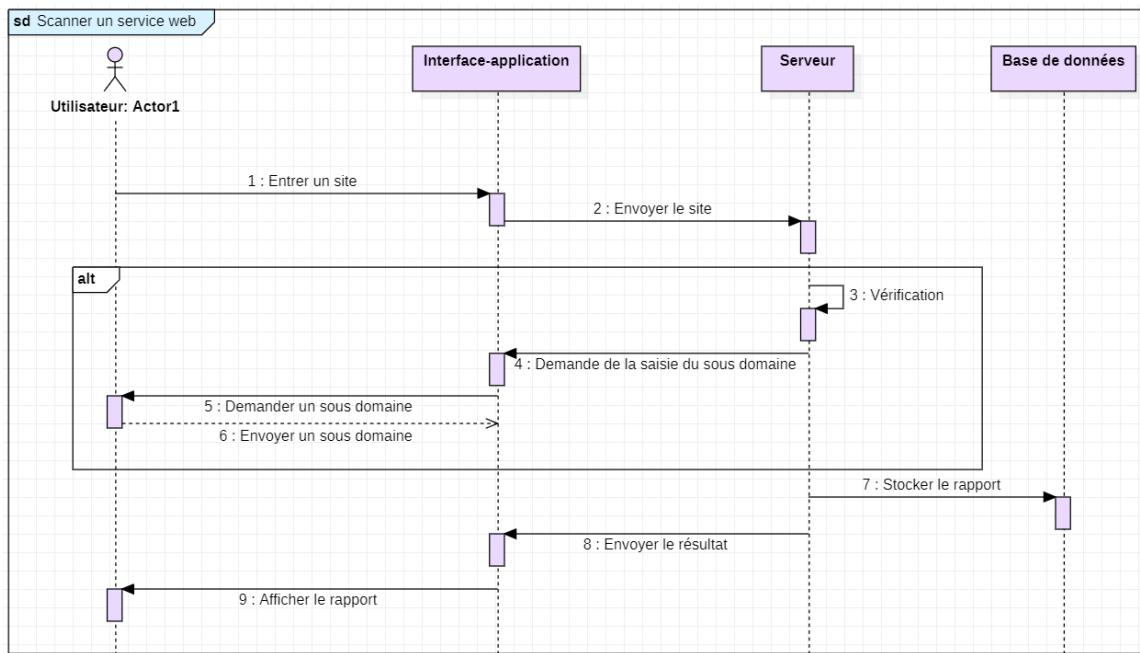


Figure 9: Diagramme de séquence pour scanner un service web

III.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.

Chapitre IV: Implémentation

IV.1 Introduction

Ce chapitre se concentre sur la réalisation de notre site web et couvre les aspects techniques liés à sa mise en œuvre. Nous discuterons des choix des technologies et des outils que nous avons utilisés pour développer notre application, ainsi que de la représentation des interfaces qui reflètent les scénarios décrits dans le chapitre précédent. Cette section est cruciale car elle permettra de mieux comprendre la façon dont notre application a été construite et comment elle fonctionne.

IV.2 Technologies et APIs

IV.2.1 Les langages utilisés

1. HTML

HTML, en anglais (Hypertext Markup Language), est un langage de balisage utilisé pour représenter les pages web en structurant sémantiquement et logiquement le contenu des pages, incluant des ressources multimédias et des formulaires. Il est conforme aux exigences d'accessibilité du web et est souvent utilisé avec JavaScript et CSS. HTML est un format ouvert inspiré du SGML(Standard Generalized Markup Language). [\[5\]](#)



2. CSS

Les feuilles de style en cascade, généralement appelées CSS de (Cascading Style Sheets), forment un langage informatique qui décrit la présentation des documents HTML et XML(Extensible Markup Language). Les standards définissant CSS sont publiés par le World Wide Web Consortium (W3C). Introduit au milieu des années 1990, CSS devient couramment utilisé dans la conception de sites web et bien pris en charge par les navigateurs web dans les années 2000. [\[6\]](#)



3. JavaScript

JavaScript est un langage de programmation de scripts principalement utilisé pour les pages web interactives, ainsi que pour les serveurs avec l'utilisation de Node.js. Il est orienté objet à prototype et supporte les paradigmes objet, impératif et fonctionnel. Avec son gestionnaire de dépendances npm (Node Package Manager), JavaScript possède le plus large écosystème avec environ 500 000 paquets en août 2017. [\[7\]](#)



4. Python

Python est un langage de programmation interprété, orienté objet et multi-paradigme. Il est conçu pour être simple à lire et à écrire, ce qui le rend très populaire pour les projets de développement logiciel. [\[8\]](#)



4.1 Flask

Flask est un micro-framework Web pour Python qui permet de créer rapidement et facilement des applications Web. Il est léger, flexible et facile à apprendre, ce qui en fait un choix populaire pour les petits projets et les prototypes.



5. SQL

SQL (Structured Query Language) est un langage de programmation utilisé pour la gestion de bases de données relationnelles. Il permet de créer, modifier et interroger des données stockées dans une base de données. Les commandes SQL sont utilisées pour effectuer des opérations telles que la sélection, l'insertion, la mise à jour et la suppression de données dans une base de données. [\[9\]](#)



IV.2.2 Outils de développement

1. Le WampServer

WampServer est une plateforme de développement Web de type WAMP, permettant de faire fonctionner localement des scripts PHP. WampServer n'est pas en soi un logiciel, mais un environnement comprenant trois serveurs, un interpréteur de script, ainsi que phpMyAdmin pour l'administration Web des bases MySQL. [\[10\]](#)



2. MySQL

MySQL est un système de gestion de bases de données relationnelles (SGBDR) open source. Il fait partie des logiciels les plus utilisés au monde, autant par le grand public (applications web principalement) que par des professionnels, et cela grâce à sa performance, sa haute fiabilité et sa simplicité. [\[11\]](#)



IV.2.3 APIs

Un API (Application Programming Interface) est un ensemble de règles, protocoles et outils qui permettent à différentes applications de communiquer entre elles de manière standardisée et automatisée.

Pour afficher les vulnérabilités sur notre site, l'API CVE (Common Vulnerabilities and Exposures) est utilisée. C'est une base de données publique qui recense les informations sur les vulnérabilités connues dans les logiciels et les systèmes. Grâce à cette API, il est possible d'interroger la base de données pour obtenir les dernières informations sur les vulnérabilités pertinentes pour le site. Une fois les données récupérées, elles sont traitées et affichées de manière claire et concise sur le site afin d'informer les utilisateurs des vulnérabilités potentielles. Cette approche permet de maintenir la sécurité du site en restant à jour sur les vulnérabilités connues. [\[12\]](#)

IV.3 L'outil Nmap

Nmap (Network Mapper) est un outil de sécurité informatique utilisé pour l'exploration de réseau et la découverte d'hôtes. Il permet de scanner des réseaux et des ports pour identifier les services en cours d'exécution sur des machines distantes, ainsi que d'autres informations telles que les systèmes d'exploitation utilisés. Nmap est largement utilisé par les professionnels de la sécurité pour évaluer les vulnérabilités d'un réseau et identifier les éventuelles failles de sécurité. [\[13\]](#)



IV.4 Structure de la base de données

La base de données comprend cinq tables distinctes. Ce choix s'explique par des raisons de sécurité. Trois d'entre eux (déclarations personnelles, professionnelles et gouvernementales) sont utilisés pour le service de signalement des incidents. Une autre table (IOC) stocke les indicateurs de compromission, et la dernière table (scan_reports) enregistre les rapports de scan pour le service web. Cette structure permet une organisation efficace des données et facilite la gestion des incidents, des indicateurs de compromission et des résultats de scan.

Pour l'observation de la structure détaillée de la base de données, voir [annexe](#).

IV.5 Présentation des fonctionnalités générales de l'application

IV.5.1 La page d'accueil

The screenshot shows the main landing page of the Algerian Cyber Security Center (ACSC). At the top, there's a dark blue header with the ACSC logo, the Ministry of Digitalization And Statistics logo, and navigation links for HOME, REPORT AN INCIDENT, REPORT AN IOC, and SCAN A SERVICE. Below the header is a banner with the text "The Algerian Cyber Security Center" and "Helping to make Algeria the safest place to live and work online." A large call-to-action button says "REPORT A CYBER INCIDENT" with the subtext "JOIN THE FIGHT AGAINST CYBERCRIME." and "Don't let cyber threats go undetected." A button labeled "Start Reporting Now" leads to the reporting form. To the right is an illustration of two people analyzing a clipboard with charts and a magnifying glass. Below the banner is a section titled "Discover The Last 20 Scored Vulnerability IDs & Summaries From NIST Database" showing three recent vulnerabilities:

- CVE-2023-2237** (High): The WP Replicate Post plugin for WordPress is vulnerable to SQL Injection via the post_id parameter in versions up to, and including, 4.0.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing queries that can be used to extract sensitive informations... [source: Wordfence](#) →
- CVE-2023-2305** (Medium): The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpdm_members', 'wpdm_login_form', 'wpdm_reg_form' shortcodes in versions up to, and including, 3.2.70 due to insufficient input sanitization and output escaping on user supplied attributes... [source: Wordfence](#) →
- CVE-2023-3173** (Critical): The GitHub repository for froxlor/froxlor prior to version 2.0.20 had a vulnerability related to improper restriction of excessive authentication attempts, which can be exploited by an attacker and allow unauthorized access to the system via brute-force attacks. [source: huntr.dev](#) →

At the bottom of the section, there's a link "See all the CVEs" with a right-pointing arrow.

Figure 10: La page d'accueil

IV.5.2 Remplir un formulaire d'incident

La figure suivante représente le formulaire d'incident, qui est le même pour tous les utilisateurs, qu'ils soient citoyens, agence ou organisations. D'autres informations sont affichées selon l'utilisateur, voir [annexe](#).

The screenshot shows the 'Report Personal cyber issue Form' interface. At the top, there is a header with the logo of the Ministry of Digitalization and Statistics, the text 'ACSC Algerian Cybersecurity Center', and navigation links for 'HOME', 'REPORT AN INCIDENT', 'REPORT AN IOC', and 'SCAN A SERVICE'. Below the header, the main form title is 'Report Personal cyber issue Form'. There is a back button and a section titled 'Section 1 Complaintant's Informations'. A note states: 'How much personal information you provide is up to you, however too little information may impact our ability to properly respond to or handle your request.' A blue bar at the bottom of this section indicates that mandatory fields are marked with an asterisk (*). The form fields include: 'First Name *' (text input), 'Last Name *' (text input), 'Email *' (text input), 'Telephone' (text input), 'Age' (text input), 'Gender' (radio buttons for Male and Female), 'Which option best describes you?' (radio buttons for Student, Employee, Retiree, and Other), and an 'Address' field (text input). Below this, 'Section 2 Company or Person Complained Against' is shown, with fields for 'First Name', 'Last Name', 'Company Name', 'Country' (dropdown menu), 'Email Address', and 'Website' (text input). A note in this section says: 'Tell us about the company, organization or individual that you have a complaint against. Please provide as much information as possible and attach all documents you might have on hand to support your complaint. Any empty field will be considered as unknown information.'

Figure 11: Le formulaire d'incident

Section 3

Details of Your Complaint

Please describe briefly what happened. Try and put the elements in the order in which they happened. Refer to a person, company or financial transaction which you have not already reported in the Suspect and Payment sections. Please provide us with information on the incident, along with a detailed description of the events, business conduct observed and any additional information you feel is pertinent to your complaint.

When was this incident detected *

mm/dd/yyyy

What is the type of the incident

- Online abuse and threats
- Identity fraud and identity theft
- Money loss or compromised accounts
- Vulnerability

If you select "Other", what is your issue ?

Description of the incident*

Type here...

Section 4

Evidences

Attach any and all documents you might have on hand to support your complaint.
Electronic files can be submitted by clicking the "Attach files" button. You can attach pictures, documents and spreadsheets.

Note that combined file size cannot exceed 10 MB in size.



Browse File to Upload

[Submit The Report](#)

Help us to help others

Sharing informative reports is crucial for us to comprehend the threat landscape and enhance the cyber intelligence capabilities. This subsequently improves our ability to help protect other Algerian organisations.



Ministry Of
Digitalization
And Statistics

ACSC
Algerian
Cybersecurity
Center

Algerian Cybersecurity Center © 2023. All Rights Reserved

Quick Links

- [HOME](#)
- [REPORT AN INCIDENT](#)
- [REPORT IOC](#)
- [SCAN A SERVICE](#)

Get In Touch

email@gmail.com

0543392605

53 lot vincent bouzareah 53 lot
vincent bouzareah

Figure 12: Autres sections du formulaire d'incident

IV.5.3 Signaler un indicateur de compromission

The screenshot shows the 'Report an IOC' page of the ACSC website. At the top, there's a header with the Ministry of Digitalization and Statistics logo, the ACSC logo, and navigation links for HOME, REPORT AN INCIDENT, REPORT AN IOC, and SCAN A SERVICE. Below the header, the main title 'Report an IOC' is displayed. A 'Back' button is located at the top left of the form area. The form is divided into two sections: Section 1 (Submitter's Contact Informations) and Section 2 (IOC Description). Section 1 contains fields for First Name, Last Name, Email, and Telephone. Section 2 contains fields for website type (Private or Government), website URL, IOC detection types (checkboxes for various anomalies like Unusual Outbound Network Traffic, Anomalies in Privileged User Account Activity, etc.), Other IOC details, and a large Description area. A 'Submit' button is at the bottom left, and a note about sharing reports for intelligence is at the bottom right.

Report an IOC

← Back

Section 1

Submitter's Contact Informations

How much personal information you provide is up to you, however too little information may impact our ability to properly respond to or handle your request.

Mandatory fields are marked with an asterisk (*).

First Name *

Last Name *

Email *

Telephone

Section 2

IOC Description

What is the type of the website ?

Private website

Government website

Enter the website URL:

example.com

What are the IOCs you detect in this website :

Unusual Outbound Network Traffic

Anomalies in Privileged User Account Activity

Geographical Irregularities

Log-In Red Flags

Increases in Database Read Volume

HTML Response Sizes

Large Numbers of Requests for the Same File

Mismatched Port-Application Traffic

Suspicious Registry or System File Changes

Unusual DNS Requests

Unexpected Patching of Systems

Mobile Device Profile Changes

Bundles of Data in the Wrong Place

Web Traffic with Unhuman Behavior

Signs of DDoS Activity

Other IOC

Description

provide more details ...

Submit

Help us to help others

Sharing informative reports is crucial for us to comprehend the threat landscape and enhance the cyber intelligence capabilities. This subsequently improves our ability to help protect other Algerian organisations.

Figure 13: Le formulaire d'IOC

IV.5.4 Scanner un service web

La figure suivante représente l'interface pour scanner un service. Pour observer le résultat du scan ,voir [annexe](#).

The screenshot shows the 'Scan A Service' interface from the ACSC (Algerian Cybersecurity Center) website. At the top, there is a logo for the Ministry Of Digitalization And Statistics and the ACSC logo. The main heading is 'Scan A Service'. Below it, a box contains the text: 'What does the scan service provide ?' followed by a note: 'The scan service provides a detailed report of the domain name you want to scan to help you identify potential security threats or attacks.' Another box below says 'Before you start scanning' with instructions: 'Before scanning, please ensure that you enter a valid domain name in the input field. The scan input will only accept the root URL without the http:// or https:// prefix and without the Folder name and Web page name.' A link 'Click See The correct domain form' is provided. The URL input field is annotated with labels: 'Hypertext Protocol' (red bracket), 'Domain Name' (blue bracket), 'Folder Name' (green bracket), and 'Web page Name' (purple bracket). The URL entered is 'https://example.com/folder/file.html'. Below the input field, a large arrow points to a 'Domain Name' label and the 'example.com' part of the URL. To the right of the input field is a button labeled 'Scan The Domain' with a hand cursor icon. At the bottom left, there is a 'Enter The Target Domain Name' input field containing 'survey.mjs.gov.dz' and a 'Scan The Domain' button. A section titled 'How the scan is working ?' explains the process: 'The scan service is done using the nmap tool to perform a port scan on the domain specified, this will detect the open ports and vulnerabilities on the target domain. This type of scan can be useful for identifying potential security vulnerabilities in a network or host, and can help system administrators take steps to secure their systems against potential attacks.' A link 'Click to understand more about the Nmap scan process' is provided. Another section titled 'Terms and conditions' notes: 'Note that it's important to consider that the scan should only be used for legitimate purposes and with the permission of the target network or host owner. The unauthorized use of these tools can be illegal and can result in serious consequences.' At the bottom, a 'Help us to help others' section encourages sharing reports: 'Sharing informative reports is crucial for us to comprehend the threat landscape and enhance the cyber intelligence capabilities. This subsequently improves our ability to help protect other Algerian organizations.'

Figure 14: Scanner un service web

IV.6 Conclusion

En conclusion, ce chapitre de réalisation nous a permis de concrétiser notre projet en développant un site web fonctionnel et efficace. Nous avons présenté les différentes technologies et outils que nous avons utilisés pour la mise en place de notre application, ainsi que les interfaces qui reflètent les fonctionnalités décrites dans les chapitres précédents.

Conclusion générale

Au cours de ce mémoire de fin d'études, nous avons abordé un aspect critique de l'environnement numérique moderne : la sécurité de l'information. Alors que l'utilisation des données numériques continue de croître à un rythme exponentiel, la protection de ces informations confidentielles est devenue une préoccupation majeure pour les organisations. Notre objectif principal était de concevoir et de développer une application Web capable de collecter, traiter et analyser les incidents liés à la sécurité afin de fournir des statistiques précises sur la criminalité et la sécurité en Algérie.

Dans le premier chapitre, nous avons présenté l'organisme d'accueil, soulignant ainsi l'importance de la sécurité de l'information pour son fonctionnement efficace.

Dans le deuxième chapitre, nous avons exploré les bases de la sécurité informatique, en mettant l'accent sur les menaces et les risques auxquels sont confrontées les organisations. Cette section nous a permis de mieux comprendre les enjeux auxquels nous étions confrontés dans le développement de notre application.

Le troisième chapitre se concentre sur la conception de l'application. Il détaille les différentes étapes du processus de conception, en mettant l'accent sur l'analyse des besoins et l'utilisation de diagrammes UML. L'objectif est de définir une solution logicielle répondant aux attentes des utilisateurs tout en garantissant la confidentialité et l'intégrité des données collectées.

Enfin, le quatrième chapitre a présenté l'implémentation de notre application, détaillant les choix technologiques et les fonctionnalités mises en œuvre pour renforcer la sécurité des services web.

Grâce à notre application, les utilisateurs pourront désormais signaler et analyser les incidents de sécurité, ce qui permettra de mieux comprendre les tendances et d'élaborer des stratégies de prévention plus efficaces.

En conclusion, cette expérience nous a permis d'acquérir une compréhension approfondie des défis liés à la sécurité de l'information et de développer des compétences pratiques dans la conception et le développement d'une application web sécurisée. Nous espérons que notre application pourra être utilisée de manière proactive pour prévenir les incidents de sécurité et assurer la confidentialité des données dans l'environnement numérique actuel.

Annexe

Cette annexe représente les détails des images présentes sur notre site web dans le chapitre d'implémentation.

- La suite de la page d'accueil

The screenshot shows the 'About Us' section of the ACSC website. It features a header with three people in professional attire standing next to a globe, followed by social media icons for Instagram, Facebook, and LinkedIn. Below this is a large blue arrow pointing right. The main content area is titled 'WHO WE ARE' and describes ACSC as a website dedicated to promoting cyber security awareness and offering resources and solutions for individuals and businesses in Algeria. It covers topics like latest threats, best practices for securing networks, and tools for detecting cyber-attacks. The 'WHAT WE DO' section lists services such as reporting cyber issues, reporting IOCs, website scanning, and data collecting. Each service is accompanied by an illustration and a brief description. At the bottom, there's a 'Help us to help others' section encouraging sharing of reports, and a footer with links to quick pages and contact information.

About Us
Learn about who we are and what we do.
Follow on social media

WHO WE ARE
ACSC, or the Algerian Cyber Security Center, is a website dedicated to promoting cyber security awareness and offering resources and solutions for individuals and businesses in Algeria. The site covers a broad range of topics related to cyber security, including information on the latest threats, best practices for securing networks and devices, and tools and techniques for detecting and responding to cyber-attacks.

WHAT WE DO
ACSC offers a variety of services to help individuals and organizations in Algeria better protect themselves from online threats, our key services include:

Reporting Cyber Issues

ACSC provides a platform for Algerian citizens and organizations to report cyber security issues they have encountered. This includes incidents such as hacking attempts, phishing scams, and malware infections. Our reporting system helps individuals and organizations quickly and easily report cyber security issues so we can investigate and take appropriate action.

Reporting IOC

ACSC also offers a platform for individuals and organizations to report indicators of compromise (IOCs). This includes IP addresses, domain names, and other data related to known or suspected cyber threats. By collecting and analyzing this data, we can better understand the threat landscape in Algeria and take proactive measures to protect our users.

Website Scanning

ACSC provides a website scanning service that helps individuals and organizations identify vulnerabilities in their web applications and websites. Our scanning tools analyze websites for common security issues, such as SQL injection and cross-site scripting (XSS) vulnerabilities. We then provide detailed reports and recommendations to help website owners mitigate these risks.

Data collecting

ACSC collects and analyzes data related to cyber threats targeting Algeria. we aim to gain valuable insights into security-related incidents, enabling us to identify trends, patterns, and potential vulnerabilities. Through our data-driven approach, we strive to enhance security measures and proactively address emerging threats, ultimately promoting a safer digital environment for our users and stakeholders.

Help us to help others
Sharing informative reports is crucial for us to comprehend the threat landscape and enhance the cyber intelligence capabilities. This subsequently improves our ability to help protect other Algerian organizations.

Quick Links
[HOME](#)
[REPORT AN INCIDENT](#)
[REPORT IOC](#)
[SCAN A SERVICE](#)

Get In Touch
ACSC@gmail.com
[023 50 59 82](tel:023505982)
[Boulevard Mohamed 5, Alger Centre](#)

Algerian Cybersecurity Center © 2023. All Rights Reserved

- La page d'accueil pour choisir le type de formulaire à remplir



**Ministry Of
Digitalization
And Statistics**

ACSC | Algerian
Cybersecurity
Center

HOME REPORT AN INCIDENT REPORT AN IOC SCAN A SERVICE

Report a Cyber Incident

What is a cybercrime ?

Cyber Incident or a cybercrime refers to criminal activities that are carried out using a computer or an online network. These criminal activities may include fraud, online image abuse, shopping, and investment scams, ransomware or malware attacks, identity theft, as well as threats and intimidation.

As cyber crime becomes more sophisticated, criminals are targeting individuals, businesses, critical infrastructure organizations, education institutes, and governments agencies or departments, All the reports submissions are useful and will aid the ACSC .

You should NOT Report when:

- A physical crime has been committed, such as your debit or credit card or computer has been stolen
- You have received a scam call, and no loss of personal information or money has occurred

Select the option which best describes the affected entity

Select the option that best describes the entity that has been affected by the incident from the list below

👤 An Individual

Select this option to report a cybercrime that has affected you personally or someone that you know or if you wish to report a cyber security vulnerability.

🏢 Business or a company

Select this option to report an event that has affected an ABN-registered business or if you wish to report a cyber security vulnerability.

-government department or agency

Select this option to report an event that has affected a Government department or agency entity or if you wish to report a cyber security vulnerability.

Help us to help others

Sharing informative reports is crucial for us to comprehend the threat landscape and enhance the cyber intelligence capabilities. This subsequently improves our ability to help protect other Algerian organizations.



**Ministry Of
Digitalization
And Statistics**

ACSC | Algerian
Cybersecurity
Center

HOME REPORT AN INCIDENT REPORT IOC SCAN A SERVICE

Get In Touch

✉ ACSC@gmail.com

📞 023 50 59 82

📍 Boulevard Mohamed 5, Alger Centre

Algerian Cybersecurity Center © 2023. All Rights Reserved

- La page d'accueil pour signaler un indicateur de compromission

The screenshot shows the ACSC website's 'Report an IOC' page. At the top, there's a header with the Ministry of Digitalization and Statistics logo, the ACSC logo, and navigation links for HOME, REPORT AN INCIDENT, REPORT AN IOC, and SCAN A SERVICE. Below the header, a large blue banner features the title 'Report an IOC'. Underneath, a light blue box contains the heading 'What is an IOC ?' followed by a detailed explanation of what Indicators of Compromise (IOCs) are and how they are used. Another section, 'What Are Cyber Threat Indicators and Defensive Measures?', provides a list of eight items defining various types of cyber threats and vulnerabilities. Further down, a 'Report The IOC' section discusses the importance of sharing IOCs to combat cybercrime. At the bottom of the page, there's a 'Start Reporting' button, a 'Help us to help others' section, and footer information including the Ministry of Digitalization and Statistics logo, a list of quick links, and contact details for the ACSC.

What is an IOC ?

Indicators of Compromise (IOCs) are pieces of information that can help detect and identify potential security threats or attacks. IOCs can include any data that suggests malicious activity in IP addresses or domain names. By collecting and analyzing IOCs reports, security professionals can identify patterns and trends in attacks and develop strategies to protect against future threats. These reports will be shared within the security community to improve threat intelligence and response efforts.

What Are Cyber Threat Indicators and Defensive Measures?

The term "cyber threat indicator" means information that is necessary to describe or identify

- Malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability
- A method of defeating a security control or exploitation of a security vulnerability
- A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability
- A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability
- Malicious cyber command and control

Report The IOC

Reporting Indicators of Compromise (IOCs) to the appropriate authorities or security teams is crucial in the fight against cybercrime and other security threats. By sharing IOCs, security professionals can collaborate and coordinate efforts to identify, investigate, and respond to potential attacks.

[Start Reporting](#)

Help us to help others

Sharing informative reports is crucial for us to comprehend the threat landscape and enhance the cyber intelligence capabilities. This subsequently improves our ability to help protect other Algerian organizations.

Quick Links

[HOME](#)
[REPORT AN INCIDENT](#)
[REPORT IOC](#)
[SCAN A SERVICE](#)

Get In Touch

ACSC@gmail.com
[023 50 59 82](tel:023505982)
[Boulevard Mohamed 5, Alger Centre](#)

Algerian Cybersecurity Center © 2023. All Rights Reserved

- Le rapport du scan d'un service :


**Ministry Of
Digitalization
And Statistics**
ACSC
Algerian
Cybersecurity
Center

[HOME](#) [REPORT AN INCIDENT](#) [REPORT AN IOC](#) [SCAN A SERVICE](#)

Nmap Scan Report - Scanned at Tue Jun 20 15:19:01 2023

Scan Summary | [survey.mjs.gov.dz \(41.111.142.149\)](#)
[← Go Back](#)

Scan Summary

Nmap 7.80 was initiated at Tue Jun 20 15:19:01 2023 with these arguments:

```
nmap -sV --script nmap-vulners --resolve-all -oX /tmp/survey.mjs.gov.dz.xml survey.mjs.gov.dz
```

Verbosity: 0; Debug level 0

Nmap done at Tue Jun 20 15:19:45 2023; 1 IP address (1 host up) scanned in 43.95 seconds

41.111.142.149 / survey.mjs.gov.dz

Address

- 41.111.142.149 (ipv4)

Hostnames

- survey.mjs.gov.dz (user)

Ports

The 996 ports scanned but not shown below are in state: **filtered**

- 996 ports replied with: **no-responses**

Port	State (toggle closed [1] filtered [0])	Service	Reason	Product	Version	Extra info
25/tcp	open		smtp	syn-ack		
	fingerprint-strings		Hello: 452 syntax error (connecting)			
80/tcp	open		http	syn-ack		
	fingerprint-strings		DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, RTSPRequest, X11Probe: HTTP/1.1 400 Bad request: Content-length: 90 Cache-Control: no-cache Connection: close Content-Type: text/html <html><body><h1>400 Bad request</h1> Your browser sent an invalid request. </body></html> FourOhFourRequest: HTTP/1.1 301 Moved Permanently content-length: 0 location: https://nicer/20ports%2c/1ri%6Eity.txt%zebak connection: close GetRequest, HTTPOptions: HTTP/1.1 301 Moved Permanently content-length: 0 location: https:/// connection: close			
443/tcp	closed		ident	reset		
	https-redirect		ERROR: Script execution failed (use -d to debug)			
113/tcp	closed					
	443/tcp	open		https	syn-ack	Apache
	fingerprint-strings		DNSStatusRequestTCP, DNSVersionBindReqTCP, RPCCheck, RTSPRequest, tor-versions: HTTP/1.1 400 Bad request: Content-length: 90 Cache-Control: no-cache Connection: close Content-Type: text/html <html><body><h1>400 Bad request</h1> Your browser sent an invalid request. </body></html> FourOhFourRequest, GetRequest, HTTPOptions: HTTP/1.0 503 Service Unavailable cache-control: no-cache content-type: text/html <html><body><h1>503 Service Unavailable</h1> server is available to handle this request. </body></html>			
	http-server-header	Apache				

Misc Metrics (click to expand)

Metric	Value
Ping Results	syn-ack

[Go to top](#) [Toggle Closed Ports](#) [Toggle Filtered Ports](#)


**Ministry Of
Digitalization
And Statistics**

ACSC
Algerian
Cybersecurity
Center

Quick Links

- [HOME](#)
- [REPORT AN INCIDENT](#)
- [REPORT IOC](#)
- [SCAN A SERVICE](#)

Get In Touch

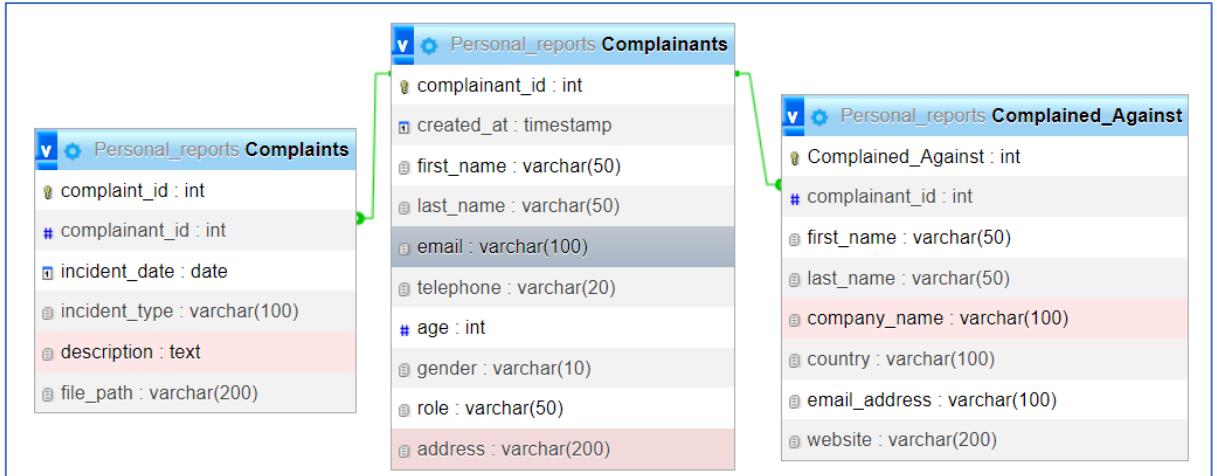
- [✉ ACSC@gmail.com](mailto:ACSC@gmail.com)
- [📞 023 50 59 82](tel:023505982)
- [📍 Boulevard Mohamed 5, Alger Centre](#)

Algerian Cybersecurity Center © 2023. All Rights Reserved

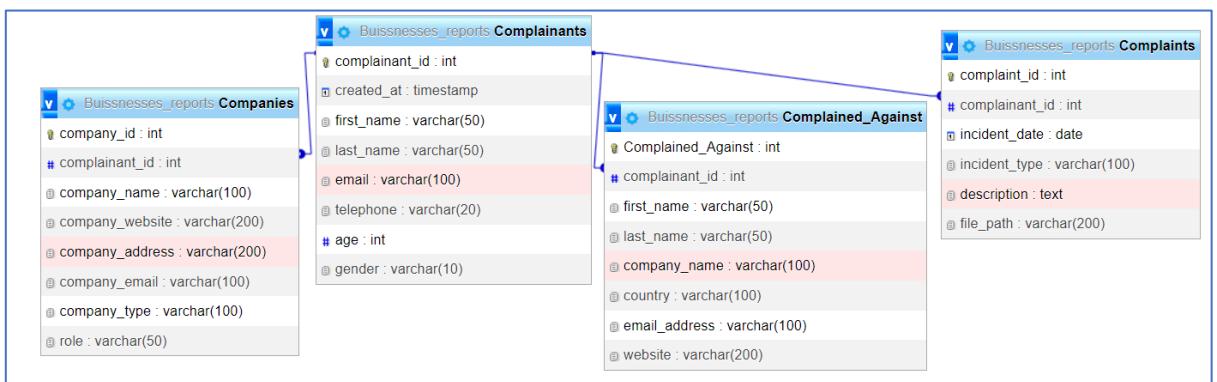
29

- La structure de la base de données

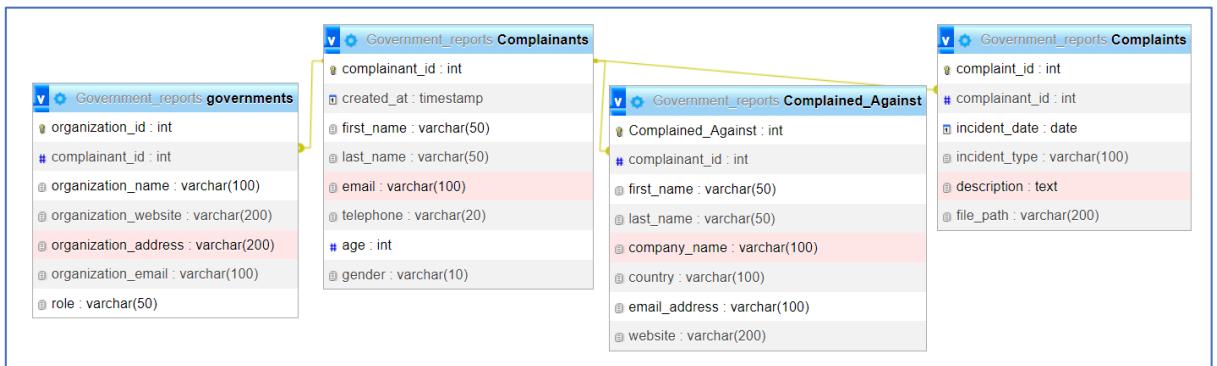
1. La table « Personal_reports » pour signaler un incident personnel



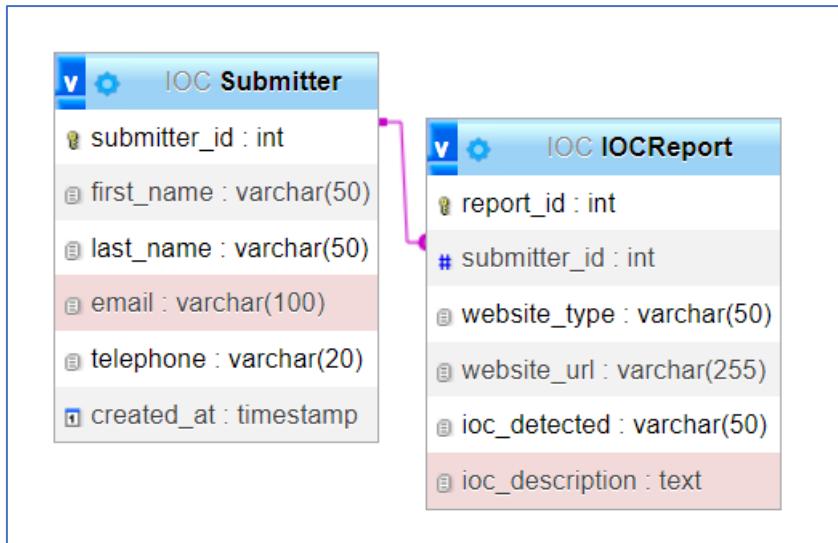
2. La table « Business_reports » pour signaler un incident d'une agence



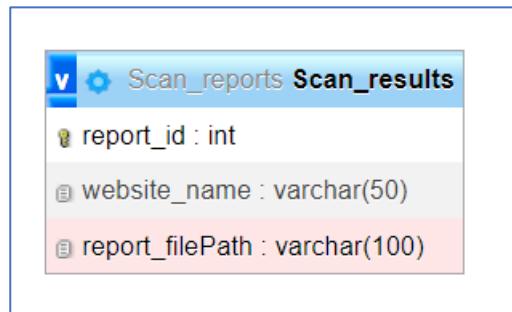
3. La table « Government_reports » pour signaler un incident d'une organisation



4. La table « IOC » pour signaler un indicateur de compromission



5. La table « Scan_reports» pour scanner un service web



Bibliographie

- [1] « L'organisme d'accueil» <https://mns.gov.dz/>
- [2] « Matrice ATT&CK» <https://thehackernews.com/2020/10/adversarial-ml-threat-matrix.html>
- [3] « Les définitions» <https://lesdefinitions.fr/>
- [4] « CISA» <https://www.cisa.gov/forms/report>
- [5] « HTML» <https://www.clubic.com/telecharger-fiche227868-html-executable.html>
- [6] « CSS» <https://developer.mozilla.org/fr/docs/Web/CSS>
- [7] « Javascript» <https://grafikart.fr/tutoriels/javascript>
- [8] « Python» <https://pythonbasics.org/what-is-flask-python/>
- [9] « SQL» <https://datascientest.com/sql-tout-savoir>
- [10] « Wampserver» <https://www.wampserver.com/>
- [11] « MySQL» <https://kinsta.com/fr/base-de-connaissances/qu-est-ce-que-mysql/>
- [12] « National Institute of Standards and Technology Databases» <https://nvd.nist.gov/>
- [13] « Nmap» <https://nmap.org/>