République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Saad Dahlab de Blida 1
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études
présenté en vue de l'obtention du diplôme de Master en Informatique

Option : sécurité des système d information

Réalisé par :

MEKBAL Djouher Wafaa

AIBOUT Asmaa

Thème

Audit approfondi de la sécurité de l'application de agrodiv selon la RNSI 2020 au sein du ministère de l'industrie

Encadreur :	Mr	HAZAZI Faycel
Promoteur :	MAA	BENYAHIA Mohammed
Président :	Pr	Boustia Nerhimene
Examinateur :	MCB	Ghebghoub Yasmina

2024/2025

Remerciements

Au terme de ce travail, nous tenons à exprimer notre gratitude et notre reconnaissance à tous ceux qui ont contribué de près ou de loin à l'élaboration de ce mémoire. Tout d'abord, nous remercions chaleureusement le jury d'avoir accepté d'évaluer notre travail.

Nous souhaitons également exprimer notre profonde gratitude à notre encadrant, Monsieur HAZAZI, ainsi qu'à Monsieur MEDJDOUB, pour leur aide précieuse, leur disponibilité, leur suivi constant et leurs nombreux conseils, qui nous ont permis de mener à bien ce travail.

Nous tenons également à remercier notre promoteur, monsieur BENYAHIA pour l'intérêt porté à notre travail.

Nous exprimons notre reconnaissance à toutes les personnes qui ont apporté leur soutien, leurs conseils et leurs encouragements tout au long de ce parcours académique. Nous leur sommes sincèrement reconnaissants. Enfin, nous tenons à exprimer notre gratitude envers nos familles et nos proches pour leur soutien constant et leur compréhension tout au long de nos études.

Merci a tous.

Dédicace

Je dédie ce modeste travail aux deux êtres les plus chers à mon cœur : ma maman et mon papa. Vous qui m'avez élevée avec amour, guidée avec patience, soutenue sans relâche et cru en moi même dans mes doutes. Aucun mot, aucune langue ne saurait suffire à exprimer la profondeur de ma reconnaissance.

À toute la famille Mekbal et Hedibel, À mon frère adoré Ayoub et à ma chère sœur Ranime, À khaltou Aïcha, Amti Salima, khtiti Leila, À ma petite cousine Raghed, à mon cousin Aymen, et à mes cousines Hiba et Nermine, Sans oublier ma grand-mère bien-aimée, Yama Ghania, qui occupe une place irremplaçable dans mon cœur.

Je pense également à mes amis fidèles : Serine, Zahida, Imene et Youssra, À tous ceux et celles qui, de près ou de loin, ont veillé à mon éducation, m'ont encouragée, inspirée ou simplement offert un mot bienveillant.

Et bien sûr, une pensée toute particulière à mon binôme Asma, avec qui j'ai partagé cette aventure avec complicité, efforts et détermination.

À tous ceux que j'aime et qui m'aiment, Recevez ici l'expression de mon amour, de mon respect et de ma gratitude.

Wafaa

Dédicace

Je tiens à rendre hommage à mon père, mon pilier, mon repère. Par sa sagesse, son soutien constant et son amour silencieux mais immense, il a toujours cru en moi, même dans les moments de doute. Rien de tout cela n'aurait été possible sans lui. Que Dieu le protège et le récompense pour tout ce qu'il fait pour moi.

J'adresse aussi ma profonde reconnaissance à ma famille pour leur patience, leur soutien et leur amour discret mais essentiel, qui m'ont portée bien plus que je ne saurais l'exprimer.

À toutes les personnes qui m'ont tendu la main, conseillé ou simplement encouragée, je dis merci du fond du cœur. Même si je ne peux pas tous vous nommer, je n'oublie personne.

Je tiens également à exprimer ma sincère gratitude à Monsieur Hezzazi et Monsieur Medjdoub, pour leur disponibilité, leur bienveillance et la qualité de leur accompagnement.

Enfin, ce mémoire témoigne d'un parcours riche en efforts, en questionnements et en rencontres humaines précieuses. Je remercie tout particulièrement ma binôme, Mekbal Wafaa, pour sa présence et son engagement tout au long de ce chemin partagé. Merci à tous ceux qui, de près ou de loin, ont contribué à cette belle aventure.

Asmaa

Résumé

De nos jours, la sécurité des systèmes d'information constitue un enjeu stratégique crucial, notamment pour les institutions publiques confrontées à une augmentation constante des menaces cybernétiques. Ce mémoire s'inscrit dans cette problématique en présentant un audit complet de la sécurité de l'application web du group agrodiv utilisée dans un contexte réel. L'étude repose principalement sur le Référentiel National de Sécurité de l'Information *(RNSI 2020)*, tout en intégrant les bonnes pratiques internationales telles que les normes *ISO/IEC 27001.*

L'approche méthodologique adoptée dans ce travail est structurée en plusieurs phases successives : une phase de reconnaissance pour identifier les composants techniques de la cible, une analyse approfondie des vulnérabilités, une exploitation encadrée des failles détectées, puis une validation des résultats obtenus. L'ensemble de l'audit a été réalisé à l'aide d'outils professionnels et reconnus dans le domaine de la cybersécurité, notamment *Nmap* pour la cartographie réseau, *Burp Suite* pour les tests d'intrusion sur les applications web, *Metasploit* pour les simulations d'attaques, ainsi que d'autres outils complémentaires.

Les investigations ont permis d'identifier plusieurs failles critiques telles que des vulnérabilités d'injection *(SQL, XSS)*, une mauvaise gestion des sessions, ainsi que des erreurs de configuration au niveau des serveurs. Ces lacunes exposent potentiellement les données sensibles de l'organisation à des risques d'accès non autorisé ou de compromission.

En réponse à ces constats, des recommandations précises et hiérarchisées ont été formulées. Elles visent à renforcer la posture de sécurité de l'application, tout en garantissant une conformité avec les standards internationaux et les exigences nationales du RNSI. L'accent a été mis non seulement sur les aspects techniques correctifs, mais également sur l'importance d'une gouvernance de la sécurité, axée sur la prévention, la sensibilisation des utilisateurs, la gestion des risques, et l'amélioration continue des dispositifs de cybersécurité.

Ce projet nous a permis de mettre en pratique les connaissances théoriques acquises durant notre parcours universitaire, de développer une démarche rigoureuse d'audit, et de mieux comprendre les défis concrets liés à la sécurisation des systèmes d'information dans un environnement professionnel réel.

Mots-clés :

Audit de sécurité, cybersécurité, analyse de vulnérabilités, tests d'intrusion, pentest, évaluation des risques, méthodologie d'audit, conformité, normes RNSI, sécurité applicative.

Résumé

Nowadays, information systems security has become a critical strategic issue, particularly for public institutions facing an ever-growing number of cyber threats. This thesis addresses this challenge by presenting a comprehensive security audit of a real-world web application. The study is primarily based on the *National Information Security Framework (RNSI 2020)*, while also aligning with international best practices such as the *ISO/IEC 27001* standard.

The adopted methodology follows a structured, multi-phase approach: reconnaissance to identify the technical components of the target, in-depth vulnerability analysis, controlled exploitation of identified flaws, and validation of results. The audit was carried out using well-established cybersecurity tools, including *Nmap*, *Burp Suite*, *Metasploit*, and other complementary tools.

The evaluation revealed several critical vulnerabilities such as injection flaws (SQL, XSS), poor session management, and misconfigurations in the server infrastructure. These weaknesses potentially expose the organization's sensitive data to unauthorized access or compromise.

Based on these findings, detailed and prioritized recommendations were proposed to strengthen the application's security posture, while ensuring compliance with both international standards and national RNSI requirements. Emphasis was placed not only on technical remediation, but also on the importance of a security governance strategy focused on prevention, user awareness, risk management, and continuous improvement.

This project enabled us to bridge theory and practice, develop a rigorous auditing approach, and gain deeper insight into the real-world challenges of securing information systems within a professional environment.

Keywords: Security audit, cybersecurity, vulnerability analysis, penetration testing, risk assessment, audit methodology, compliance, RNSI standards, application security.

Table des matières

1 Sécurité des applications web et audit informatique . . . 3
1.1 Introduction . . . 4
1.2 Définition de l'audit de sécurité . . . 4
1.3 Objectifs et enjeux de l'audit de sécurité . . . 4
1.3.1 Objectifs principaux de l'audit de sécurité . . . 4
1.3.2 Enjeux de l'audit de sécurité . . . 4
1.4 Méthodologie d'audit . . . 5
1.4.1 Types d'audits de sécurité . . . 5
1.4.1.1 Audit organisationnel . . . 5
1.4.1.2 Audit technique . . . 5
1.4.1.3 Audit de conformité . . . 6
1.4.1.4 Autres audits spécifiques . . . 6
1.4.2 Types de test . . . 7
Black-box : . . . 8
Gray-box : . . . 8
White-box : . . . 8
1.4.3 Tableau comparatif des types d'audit de sécurité . . . 9
1.4.4 Étapes de l'audit . . . 9
1.4.4.1 Reconnaissance et collecte d'informations . . . 9
1.4.4.2 Tests de sécurité et exploitation des vulnérabilités . . . 10
1.4.4.3 Analyse des résultats et évaluation des risques . . . 10
1.4.4.4 Rapport d'audit et recommandations . . . 10
1.5 Composants de sécurité périmétrique dans les architectures web . . . 10
1.5.1 Pare-feu (Firewall) . . . 11
1.5.2 IDS (Intrusion Detection System) . . . 11
1.5.3 IPS (Intrusion Prevention System) . . . 11
1.5.4 GEO-IP / IP Reputation . . . 11
1.5.5 WAF (Web Application Firewall) . . . 11
1.5.6 V-IP (IP virtuelle) . . . 12
1.6 Vulnérabilités fréquentes dans les applications web . . . 12
1.6.1 Vulnérabilités liées aux sessions, mots de passe, etc. . . . 15
1.7 Bonnes pratiques de sécurité applicative . . . 15
1.7.1 Validation et filtrage des entrées . . . 15
1.7.2 Utilisation du chiffrement . . . 15
1.7.3 Gestion sécurisée des sessions et des cookies . . . 16
1.7.4 Mise en œuvre de contrôles d'accès rigoureux . . . 16
1.7.5 Surveillance et journalisation . . . 16

1.7.6 Tests de sécurité et audits réguliers . . . 16
1.8 Conclusion . . . 16

2 Contexte Institutionnel et Réglementaire . . . 17
2.1 Introduction . . . 18
2.2 Présentation du Ministère de l'Industrie . . . 18
2.2.1 Structure organisationnelle . . . 18
2.2.2 Objectifs et rôle du ministère . . . 18
2.3 Importance des systèmes d'information et de la digitalisation . . . 19
2.4 Enjeux liés à la cybersécurité . . . 19
2.5 Risques et défis pour un organisme gouvernemental . . . 20
2.6 Cadre réglementaire . . . 21
2.6.1 Normes internationales : ISO/IEC 27001 . . . 21
2.6.2 OWASP Top 10 . . . 21
2.6.2.1 Statut et autorité . . . 21
2.6.2.2 Objectifs . . . 21
2.6.2.3 Contenu . . . 21
2.6.2.4 Complémentarité avec le RNSI . . . 22
2.6.3 Référentiel National de la Sécurité de l'Information (RNSI) . . . 22
2.6.3.1 Objectifs du RNSI 2020 . . . 22
2.6.3.2 Champ d'application . . . 22
2.6.4 Lois algériennes applicables . . . 23
2.6.4.1 Décret présidentiel n° 20-05 du 24 Joumada El Oula 1441 (20 janvier 2020) . . . 23
2.6.4.2 Loi n° 09-04 du 5 août 2009 sur la cybersécurité et la lutte contre la cybercriminalité . . . 23
2.6.4.3 Décret exécutif n° 16-61 du 2 Joumada El Oula 1437 (11 février 2016) . . . 24
2.6.4.4 Loi n° 18-04 du 24 Chaâbane 1439 (10 mai 2018) . . . 24
2.6.4.5 Loi n° 18-07 du 25 Ramadhan 1439 (10 juin 2018) . . . 24
2.7 Conclusion . . . 24

3 Planification et déroulement de l'audit . . . 26
3.1 Introduction . . . 27
3.2 Définition du périmètre et des objectifs . . . 27
3.2.1 Délimitation du périmètre de l'audit . . . 27
3.2.2 Objectifs de l'audit de sécurité . . . 27
3.3 Méthodologie et approche adoptée . . . 28
3.3.1 Cadres de référence utilisés . . . 28
3.3.2 Type d'audit . . . 29
3.3.3 Type de test . . . 29
3.4 Plan d'audit et organisation des étapes . . . 30
3.4.1 Phases principales de l'audit . . . 30
3.4.2 Tableau récapitulatif des étapes de l'audit . . . 30
3.5 Outils et technologies mobilisés . . . 31
3.5.1 Présentation des outils d'audit utilisés . . . 31

Cartographie et analyse réseau : 31
Tests de sécurité des applications web : 31
Analyse du trafic et inspection des paquets : 31
Outils système et réseau : 31
Évaluation des vulnérabilités et exploitation : 31
Outils de détection de malwares ou rootkits : 31
3.5.1.1 Outils utilisés dans un audit EXTERNE 32
3.5.1.2 Outils utilisés dans un audit INTERNE 32
3.5.1.3 Outils hybrides (interne / externe selon le contexte) 33
3.6 Topologie de l'infrastructure auditée 34
3.6.1 Schéma de topologie 34
3.7 Contexte de l'application web auditée 35
3.8 Points d'entrée et structure applicative 35
3.9 Critères d'évaluation des vulnérabilités 36
Impact 38
Exploitabilité 38
Score de base final 38
3.10 Limitations ou périmètre hors scope 38

4 Résultats de l'audit et recommandations 39
4.1 Introduction 40
4.2 Constatations techniques détaillées 40
4.2.1 Vulnérabilités critiques identifiées 40
4.2.2 Risques associés 40
4.2.3 Recommandations principales 40
4.3 Constatations techniques détaillées 41
4.3.1 Services en écoute réseau 41
4.3.2 Configuration et sécurité du service SSH 41
4.3.3 Analyse de la configuration du serveur 42
4.3.3.1 Évaluation de la sécurité de l'application Laravel (Backend) 43
4.3.3.2 Sécurisation des entêtes HTTP et des sessions 43
4.3.3.3 Analyse des privilèges et des outils système 44
4.4 Analyse de l'exposition Réseau 44
4.4.0.1 Cartographie des ports internes (IP privée) 44
4.4.0.2 Cartographie des ports exposés (IP publique) 45
4.4.1 Évaluation du frontend web 45
4.4.1.1 Absence de chiffrement TLS entre frontend et backend . . 45
4.4.1.2 Sécurité des cookies et des sessions 45
4.4.1.3 En-têtes HTTP manquants 46
4.4.1.4 Code exposé côté client 46
4.4.2 Analyse de la base de données 46
4.4.2.1 Système de gestion et structure 46
4.4.3 4.4.2 Cartographie des données sensibles 47
4.4.3.1 Comptes et politique d'accès 47
4.5 Plan de Recommandations Aligné au RNSI 2020 49
4.6 Conclusion 51

Références bibliographiques **59**

Bibliographie **60**

Table des figures

1.1 Répartition des vulnérabilités selon OWASP Top 10 (2021) 14

3.1 Topologie du système audité 35
3.2 Répartition des vulnérabilités par niveau de criticité (CVSSv3) 37

1 Exemple de code source contenant des informations sensibles 55
2 Vulnérabilité clickjacking 56
3 Présence d'un service IKEv1 exposant un équipement de sécurité réseau utilisant une version obsolète de son système. 56
4 Analyse Wireshark d'un échange IKEv1 en mode agressif 57
5 Attaque Force Brute via SSH 57

Liste des tableaux

1.2 Classification des vulnérabilités OWASP Top 10 (2021) 13

3.1 Correspondance entre les domaines RNSI et l'audit – Partie 1 28
3.2 Correspondance entre les domaines RNSI et l'audit – Partie 2 29
3.3 Résumé des étapes de l'audit de sécurité 30
3.4 Outils utilisés et leur rôle dans l'audit de sécurité 32
3.5 Outils d'analyse de la sécurité Web 32
3.6 Outils d'exploitation et de tests automatisés 32
3.7 Outils système pour l'analyse locale 33
3.8 Outils d'analyse locale et de sécurité système 33
3.9 Utilisation de Metasploit pour les élévations de privilèges 33
3.10 Comparaison des cas d'usage des outils en audit externe et interne 33

4.1 Ports ouverts et services associés 41
4.2 Évaluation des paramètres SSH 41
4.3 Analyse de la configuration du serveur 42
4.4 Évaluation de sécurité Laravel (backend) 43
4.5 Évaluation des entêtes HTTP et de la gestion de session 43
4.6 Analyse des privilèges et outils de surveillance 44
4.7 Ports internes détectés sur l'interface privée 44
4.8 Ports détectés sur l'interface publique 45
4.9 Absence de chiffrement entre frontend et backend 45
4.10 Évaluation des cookies et des sessions 45
4.11 En-têtes HTTP manquants 46
4.12 Éléments sensibles exposés côté client 46
4.13 Tables contenant des données sensibles 47
4.14 État des éléments liés à la gestion des comptes et des accès 47
4.15 Présentation des failles liées à la gestion des jetons et au hachage des données sensibles 48
4.16 Présentation des failles liées aux scripts SQL 48
4.17 Présentation des failles liées à la journalisation et aux mécanismes d'audit . 48
4.18 Présentation des failles liées à configuration MySQL 49

Introduction générale

Dans un monde en plein développement numérique, la sécurité des systèmes d'information est devenue un enjeu strategique pour les organisations, soient elle privées ou publiques. Les cyberattaques se multiplient, les vulnérabilités logicielles sont exploitées avec une sophistication croissante, et les conséquences d'une faille de sécurité peuvent être fatales : perte de données sensibles, interruption des services, atteinte à la réputation, ou encore sanctions réglementaires. Face à ces menaces, l'audit de sécurité informatique s'avère essentiel pour évaluer, renforcer et garantir la robustesse des infrastructures technologiques.

Ce mémoire s'inscrit dans cette perspective en explorant les fondements, les méthodologies et les bonnes pratiques de l'audit de sécurité, avec une mise en œuvre réelle au sein Ministère de l'Industrie. En tant qu'institution gouvernementale, ce ministère gère des données stratégiques et sensibles, dont la protection est cruciale pour la souveraineté nationale et la continuité des services publics. Cependant, comme toute entité connectée, il est exposé à des risques croissants de cybersécurité, notamment à travers ses applications web, souvent ciblées par les attaquants en raison de leur accessibilité et de leur complexité.

L'objectif de ce travail est double :

Théorique : Présenter une synthèse complète des principes de l'audit de sécurité, des normes en vigueur (telles que l'ISO/CEI 27001 et le Référentiel National de Sécurité des Systèmes d'Information – RNSI), ainsi que des vulnérabilités spécifiques aux applications web (OWASP Top 10).

Pratique : Décrire la planification et la réalisation d'un audit de sécurité au sein du Ministère de l'Industrie, en mettant en lumière les outils utilisés, les vulnérabilités identifiées et les recommandations proposées pour y remédier.

Problématique

Les applications web, bien qu'elles rendent les échanges et services en ligne plus facile, forment une surface d'attaque importante pour les cybercriminels. Des failles comme les injections SQL, les attaques XSS (Cross-Site Scripting) ou les erreurs de configuration peuvent compromettre l'intégrité du système et la confidentialité des données. Pour un

ministère, dont les activités reposent sur des plateformes numériques, une faille de sécurité pourrait avoir des répercussions politiques, économiques et sociales majeures.

Comment, donc, renforcer la sécurité des applications web d'une institution publique ? Quelles méthodologies et quels outils employer pour identifier les vulnérabilités et proposer des correctifs adaptés ? Enfin, comment rendre ces pratiques conformes avec le cadre réglementaire algérien et les standards internationaux ?

Organisation du Mémoire

Pour répondre à ces questions, ce mémoire est structuré en cinq chapitres :

Chapitre 1 : Fondements de l'audit de sécurité informatique – Définition, objectifs, types d'audits (organisationnel, technique, conformité) et méthodologies (tests black-box, gray-box, white-box).

Chapitre 2 : Contexte Institutionnel et Réglementaire – Présentation du Ministère de l'Industrie, analyse des risques cybernétiques et cadre légal (RNSI, lois algériennes sur la cybersécurité).

Chapitre 3 : Applications Web et Enjeux de Sécurité – Évolution des technologies web, vulnérabilités courantes (OWASP Top 10) et bonnes pratiques de sécurisation.

Chapitre 4 : Planification et Déroulement de l'Audit – Périmètre, outils (Nmap, Burp Suite, Metasploit), étapes (reconnaissance, tests, analyse) et critères d'évaluation.

Chapitre 5 : Rapport d'Audit – Synthèse des résultats, vulnérabilités critiques détectées et recommandations pour renforcer la sécurité.

Chapitre 1

Sécurité des applications web et audit informatique

1.1 Introduction

Les applications web occupent aujourd'hui une place centrale dans les systèmes d'information modernes. Cependant, cette forte exposition les rend particulièrement vulnérables aux attaques. Protéger ces applications est donc devenu un enjeu crucial pour les organisations.Ce chapitre présente les bases de la sécurité des applications web, les vulnérabilités les plus courantes, ainsi que les outils et méthodes utilisés pour les détecter. Il expose également les principes de l'audit de sécurité, indispensable pour évaluer et renforcer la protection des systèmes.

1.2 Définition de l'audit de sécurité

L'audit de sécurité correspond à une revue et un examen indépendants des enregistrements et des activités, visant à évaluer l'efficacité des contrôles de cybersécurité et à garantir la conformité aux politiques établies, aux procédures opérationnelles ainsi qu'aux exigences standard, légales et réglementaires pertinentes [21, p. 83].

1.3 Objectifs et enjeux de l'audit de sécurité

Les objectifs et enjeux de l'audit de sécurité des systèmes d'information, tels que présentés ci-dessous, sont issus d'une synthèse de plusieurs sources, notamment le guide pratique d'audit des systèmes d'information [18] et les principes fondamentaux exposés par Stallings [29].

1.3.1 Objectifs principaux de l'audit de sécurité

Les objectifs principaux de l'audit de sécurité consistent à analyser les vulnérabilités des systèmes d'information, évaluer l'efficacité des dispositifs de sécurité et proposer des actions correctives.

- Identifier les vulnérabilités et failles de sécurité dans les systèmes d'information.
- Évaluer le niveau de conformité aux politiques de sécurité internes et aux normes réglementaires.
- Proposer des recommandations visant à améliorer la sécurité et réduire les risques.
- Assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données.

1.3.2 Enjeux de l'audit de sécurité

Les enjeux de l'audit de sécurité incluent la protection des informations sensibles, la gestion des risques liés aux menaces informatiques et la conformité aux exigences légales et normatives.

- Protéger les données sensibles contre les accès non autorisés et les fuites d'information.

— Assurer la continuité des activités en évitant les interruptions de service.
— Réduire les risques financiers, légaux et liés à la réputation associés aux événements de sécurité.
— Renforcer la gouvernance et la gestion globale de la sécurité au sein de l'organisation.
— Favoriser une culture de sécurité et une démarche d'amélioration continue.
— Une faille de sécurité peut compromettre la réputation d'une organisation ; l'audit permet d'anticiper ce risque en identifiant les vulnérabilités pouvant nuire à la confiance et à la crédibilité, comme le souligne Olanrewaju [25].

1.4 Méthodologie d'audit

L'audit de la sécurité des systèmes d'information repose sur une méthodologie afin d'identifier, d'analyser et de corriger les vulnérabilités potentielles pour garantir l'intégrité et la résilience d'un système. Cette méthodologie est essentielle pour protéger les infrastructures d'informations critiques, améliorer les postures de cybersécurité et garantir la conformité aux exigences légales et réglementaires.

1.4.1 Types d'audits de sécurité

Les audits de sécurité peuvent être classés en plusieurs catégories en fonction de leurs objectifs, de leur portée et de leurs méthodologies. Voici les principaux types d'audits de sécurité :

1.4.1.1 Audit organisationnel

Définition : un audit organisationnel évalue les politiques, les processus et les contrôles de sécurité mis en place au sein d'une organisation.

Objectifs :

— Vérifier la conformité aux réglementations et aux normes.
— Identifier les lacunes dans la gestion des risques et la gouvernance de la sécurité.
— Évaluer l'efficacité des politiques de sécurité de l'information.

Domaines couverts :

— Politiques de sécurité de l'information.
— Gestion des ressources humaines (formation, sensibilisation).
— Contrôle d'accès physique et logique.
— Gestion des incidents de sécurité.
— Plan de continuité d'activité (PCA).

1.4.1.2 Audit technique

Définition : un audit technique se concentre sur l'évaluation des vulnérabilités techniques des systèmes, des réseaux et des applications.

Objectifs :

— Identifier les failles de sécurité dans les infrastructures et les applications.
— Tester la résistance des systèmes face à des attaques simulées.
— Proposer des correctifs pour renforcer la sécurité.

Méthodologies :

— **Tests d'intrusion (pentest)** : Simulation d'attaques pour évaluer la résistance des systèmes.
  — Approches : Boîte noire, boîte grise, boîte blanche.
— **Audit des vulnérabilités** : Utilisation d'outils automatisés pour détecter les failles connues.
— **Audit de configuration** : Vérification des configurations des systèmes et des équipements pour s'assurer qu'elles respectent les bonnes pratiques.

Domaines couverts :

— Sécurité des serveurs et des réseaux.
— Sécurité des applications web et mobiles.
— Sécurité des bases de données.
— Sécurité des API et des services cloud.

1.4.1.3 Audit de conformité

Définition : un audit de conformité vise à vérifier que l'organisation respecte les réglementations, les normes et les politiques internes en matière de sécurité.

Objectifs :

— S'assurer du respect des obligations légales et réglementaires (ex : RGPD, NIS 2).
— Obtenir ou renouveler des certifications (ex : ISO 27001, SOC 2).
— Éviter les sanctions financières et les pertes de réputation.

Normes et réglementations courantes :

— RGPD : Protection des données personnelles.
— ISO/IEC 27001 : Management de la sécurité de l'information.
— NIS 2 : Sécurité des réseaux et des systèmes d'information.
— DORA : Résilience opérationnelle dans le secteur financier.

1.4.1.4 Autres audits spécifiques

Audit de sécurité web Définition : évaluation des vulnérabilités des sites web et des applications web.

Objectifs :

— Identifier les failles techniques et logiques.
— Protéger contre les attaques courantes (ex : injections SQL, XSS, CSRF).
— Améliorer la sécurité des données et des utilisateurs.

Méthodologies :

- Analyse de la configuration des serveurs web.
- Tests d'injection (SQL, XSS, HTML).
- Examen des composants tiers (bibliothèques, frameworks).
- Vérification des contrôles d'accès et des mécanismes d'authentification.

Audit de sécurité mobile Définition : évaluation de la sécurité des applications mobiles (iOS, Android) et de leur environnement.

Objectifs :

- Identifier les vulnérabilités spécifiques aux applications mobiles.
- Assurer la protection des données stockées et transmises.
- Respecter les normes de sécurité (ex : MASVS de l'OWASP).

Domaines couverts :

- Stockage sécurisé des données.
- Communications chiffrées.
- Authentification et gestion des sessions.
- Protection contre le reverse engineering.

Audit de sécurité IoT Définition : évaluation de la sécurité des objets connectés et de leur écosystème.

Objectifs :

- Identifier les vulnérabilités matérielles et logicielles.
- Protéger les données transmises par les objets connectés.
- Assurer la sécurité des protocoles de communication.

Domaines couverts :

- Analyse du hardware (reverse engineering, dumps de mémoire).
- Analyse du firmware (ports ouverts, cryptographie).
- Sécurité des protocoles de communication (écoute des échanges, déni de service).
- Sécurité des services associés (interfaces web, API).

1.4.2 Types de test

Les types de sécurité peuvent varier en fonction des méthodes, des objectifs et du niveau d'accès accordé aux auditeurs. Les trois principaux types d'audits sont le *Black-box*, le *Gray-box* et le *White-box*. Chaque type présente des caractéristiques, des avantages et des limites spécifiques, et leur usage combiné est souvent recommandé pour garantir une évaluation rigoureuse de la sécurité.

Comme le souligne Casper [3], une approche exclusivement *Black-box* est insuffisante pour effectuer des tests de sécurité fiables sur des systèmes complexes. En effet, le manque de transparence et d'accès interne limite fortement la capacité à détecter certaines vulnérabilités systémiques. Cela justifie l'usage complémentaire des tests *Gray-box* et *White-box* dans une démarche d'audit approfondi.

Black-box : Un test *Black-box* est une méthode où l'auditeur n'a aucune connaissance préalable du système, de l'application ou de l'infrastructure examinée. L'auditeur agit comme un attaquant externe, essayant de découvrir les vulnérabilités à partir d'une position sans accès privilégié.

Caractéristiques :

— Absence d'accès aux codes sources, à la documentation ou aux informations internes.
— Le test se concentre sur les interfaces externes et les points d'entrée.
— Outils : scanners de vulnérabilités, analyseurs de trafic, outils de pentest.

Avantages :

— Simulation réaliste d'une attaque externe.
— Identification de failles visibles depuis l'extérieur.

Limites :

— Ne permet pas d'identifier des failles internes ou logiques plus subtiles.
— Moins efficace pour détecter les erreurs de conception ou de configuration interne.

Applications :

— Test de pénétration externe.
— Évaluation de la sécurité périmétrique.
— Contrôle de conformité vis-à-vis des exigences des partenaires externes.

Gray-box : Le testt *Gray-box* combine les approches Black-box et White-box. L'auditeur a un accès partiel aux informations internes, ce qui permet de cibler des zones critiques tout en conservant une certaine objectivité.

Caractéristiques :

— Accès limité au code, à la documentation ou aux schémas d'architecture.
— Connaissance partielle des processus métiers ou techniques.

Avantages :

— Meilleur compromis entre réalisme de l'attaque et profondeur d'analyse.
— Moins coûteux et plus ciblé qu'un audit White-box complet.

Applications :

— Audit d'applications critiques.
— Audit de sécurité sur les réseaux hybrides ou distribués.

White-box : Un test *White-box* donne un accès total à toutes les informations internes du système : code source, configurations, bases de données, etc. C'est l'approche la plus complète pour identifier les vulnérabilités.

Caractéristiques :

— Accès intégral au système audité.
— Analyse poussée du code, des configurations et des flux de données.

Avantages :

— Permet une analyse exhaustive des failles de sécurité, même les plus subtiles.
— Favorise la mise en conformité avec les normes de sécurité internes.

Applications :

— Évaluation de la sécurité logicielle.
— Audit de conformité interne (ISO 27001, etc).
— Analyse de la qualité du code et des processus de développement sécurisé.

1.4.3 Tableau comparatif des types d'audit de sécurité

Critère	**Audit Black-box**	**Audit Gray-box**	**Audit White-box**
Connaissance système	Nulle	Partielle	Complète
Accès ressources	Aucun	Limité	Total
Objectif	Simulation externe	Analyse ciblée réaliste	Analyse exhaustive
Approche	Externe – boîte noire	Semi-interne – boîte grise	Interne – boîte blanche
Avantages	Réalisme, surface externe	Ciblage précis, coût modéré	Profondeur, conformité, exhaustivité
Limites	Vision limitée, pas d'accès interne	Vision partielle, biais possible	Long, coûteux, moins réaliste
Applications typiques	Pentest externe, sécurité périmètre	Audit app critiques, réseaux mixtes	Audit code, normes internes, ISO

1.4.4 Étapes de l'audit

La réalisation d'un audit de sécurité suit une méthodologie structurée en plusieurs étapes interdépendantes. Ces étapes permettent d'identifier les vulnérabilités, de les évaluer et de proposer des solutions adaptées [22].

1.4.4.1 Reconnaissance et collecte d'informations

Cette phase consiste à rassembler un maximum d'informations sur la cible de l'audit, sans nécessairement interagir directement avec elle. Elle peut inclure une collecte passive (recherche sur les DNS, WHOIS, moteurs de recherche, réseaux sociaux) et une collecte active (scans de ports, détection de services).

Objectifs :

— Identifier les systèmes, adresses IP, domaines, technologies utilisées.
— Cartographier les services disponibles et les points d'entrée potentiels.
— Préparer les phases de test ultérieures de manière efficace.

1.4.4.2 Tests de sécurité et exploitation des vulnérabilités

Cette étape consiste à détecter, valider et potentiellement exploiter les vulnérabilités découvertes à l'aide d'outils automatisés et de techniques manuelles. Elle inclut les tests d'injection, l'analyse des configurations, l'évaluation des mécanismes d'authentification et la simulation d'attaques.

Méthodes courantes :

— Scans de vulnérabilités (Nessus, OpenVAS, etc.).
— Tests d'intrusion ciblés (ex : SQLi, XSS, CSRF).
— Exploitation assistée par des frameworks comme Metasploit.

1.4.4.3 Analyse des résultats et évaluation des risques

Les résultats collectés sont ensuite analysés pour comprendre la portée des failles identifiées. Chaque vulnérabilité est évaluée en fonction de sa gravité, de sa probabilité d'exploitation et de son impact sur le système ou les données.

Référentiels d'évaluation utilisés :

— CVSS (Common Vulnerability Scoring System).
— OWASP Risk Rating Methodology.
— Normes de classification internes ou sectorielles.

Objectif : Prioriser les vulnérabilités en fonction du risque réel pour l'organisation.

1.4.4.4 Rapport d'audit et recommandations

Enfin, un rapport est rédigé pour présenter les constats, les preuves collectées, les niveaux de risques, et les recommandations correctives. Le rapport peut être technique ou exécutif selon le public visé.

Contenu typique :

— Résumé exécutif pour la direction.
— Détail technique des vulnérabilités avec preuves (screenshots, logs...).
— Recommandations de correction et de renforcement de la sécurité.
— Priorisation des actions à mener (court/moyen/long terme).

Un bon rapport doit être clair, factuel, et orienté vers l'amélioration continue de la posture de sécurité de l'organisation.

1.5 Composants de sécurité périmétrique dans les architectures web

La sécurité périmétrique constitue la première ligne de défense des architectures web contre les menaces extérieures. Elle regroupe un ensemble de dispositifs techniques permettant de filtrer, surveiller et contrôler les flux réseau à l'entrée de l'infrastructure. Ces

mécanismes visent à prévenir les intrusions, à détecter les comportements malveillants et à limiter les risques d'attaques ciblées.

1.5.1 Pare-feu (Firewall)

Le pare-feu constitue le composant fondamental de la sécurité périmétrique. Il agit comme un filtre réseau, en autorisant ou bloquant les flux selon des règles définies par l'administrateur. Il permet de restreindre l'accès aux services exposés, de limiter les connexions à certaines plages d'adresses IP ou ports, et de bloquer les tentatives de connexions non autorisées. Les pare-feux peuvent être matériels ou logiciels, et fonctionner à différents niveaux (niveau réseau, transport ou application).

1.5.2 IDS (Intrusion Detection System)

Un système de détection d'intrusion est conçu pour surveiller les activités réseau et système afin d'identifier des comportements suspects ou des signatures connues d'attaques. Fonctionnant de manière passive, un IDS ne bloque pas les flux, mais génère des alertes permettant aux équipes de sécurité d'intervenir rapidement. Il est particulièrement utile pour repérer des scans de port, des tentatives d'accès non autorisé ou des anomalies dans les paquets réseau.

1.5.3 IPS (Intrusion Prevention System)

Contrairement à l'IDS, l'IPS intervient de manière active pour bloquer les menaces en temps réel. Il agit comme un pare-feu intelligent, capable d'analyser le trafic en profondeur et de prendre des mesures immédiates (blocage, déconnexion, réécriture de paquets) face à une attaque détectée. L'IPS peut être intégré au pare-feu ou déployé en tant que composant distinct.

1.5.4 GEO-IP / IP Reputation

Ces techniques permettent d'ajouter une couche de filtrage basée sur l'origine du trafic. Le filtrage GEO-IP restreint ou autorise l'accès à l'application en fonction de la localisation géographique des adresses IP, utile notamment pour limiter l'exposition à des zones à risque. Le filtrage basé sur la réputation IP repose quant à lui sur des bases de données de menaces connues (listes noires), permettant de bloquer les adresses IP associées à des activités malveillantes ou à des botnets.

1.5.5 WAF (Web Application Firewall)

Le pare-feu applicatif web est un composant spécialisé dans la protection des applications web contre les attaques courantes telles que l'injection SQL, les scripts intersites (XSS), le cross-site request forgery (CSRF), etc. Contrairement aux pare-feux traditionnels, le WAF fonctionne au niveau de la couche HTTP/HTTPS et analyse les requêtes

applicatives en profondeur. Il peut appliquer des règles personnalisées pour détecter des comportements anormaux, bloquer les tentatives d'exploitation ou masquer certaines erreurs côté serveur.

1.5.6 V-IP (IP virtuelle)

Une adresse IP virtuelle permet de masquer la véritable localisation des services internes en faisant transiter le trafic par une IP intermédiaire. Ce mécanisme est souvent utilisé dans des architectures avec équilibrage de charge (load balancing) ou dans des environnements virtualisés ou conteneurisés. Il renforce la sécurité en dissimulant les adresses IP réelles des services critiques et en limitant leur exposition directe à Internet.

1.6 Vulnérabilités fréquentes dans les applications web

Le développement intensif des applications web expose les systèmes d'information à un ensemble de vulnérabilités connues et récurrentes. Le référentiel *OWASP Top 10*, publié par l'*Open Web Application Security Project*, constitue une classification de référence des dix catégories de vulnérabilités les plus critiques affectant les applications web [26]. Ce référentiel repose sur l'analyse de données issues de plusieurs centaines de milliers d'applications à l'échelle mondiale.

L'édition 2021 du *OWASP Top 10* établit la liste suivante :

TABLE 1.2 – Classification des vulnérabilités OWASP Top 10 (2021)

Code	Nom	Description
A01	Contrôles d'accès défaillants	Défaillances dans les mécanismes de contrôle d'accès permettant l'accès non autorisé à des ressources
A02	Défaillances cryptographiques	Mauvaise protection des données sensibles (manque de chiffrement, protocoles faibles)
A03	Injections	Insertion de code malveillant via les champs d'entrée (SQL, LDAP, etc.)
A04	Conception non sécurisée	Défauts d'architecture logicielle introduisant des risques structurels
A05	Configuration incorrecte	Paramétrages incorrects des composants logiciels ou des services
A06	Composants vulnérables	Utilisation de bibliothèques ou frameworks obsolètes ou vulnérables
A07	Défaillances d'authentification	Faiblesses dans la gestion de l'authentification et des sessions
A08	Défaillances d'intégrité	Manque de vérification d'intégrité dans les mises à jour
A09	Journalisation insuffisante	Absence de mécanismes de détection d'incidents adéquats
A10	SSRF (Server-Side Request Forgery)	Détournement des serveurs pour requêtes non autorisées

FIGURE 1.1 – Répartition des vulnérabilités selon OWASP Top 10 (2021)

1.6.1 Vulnérabilités liées aux sessions, mots de passe, etc.

Au-delà des failles identifiées par l'OWASP, certaines vulnérabilités récurrentes concernent directement la gestion de l'authentification et des sessions :

— **Sessions non sécurisées** : L'usage de cookies non protégés (sans attributs Secure ou HttpOnly) ou l'absence de renouvellement de session après authentification peut faciliter les détournements de session [27].
— **Mots de passe faibles ou mal stockés** : Le choix de mots de passe peu complexes ou l'absence de hachage sécurisé (comme Argon2 ou bcrypt) peut mener à des compromissions rapides en cas de fuite de la base d'utilisateurs [11].
— **Temps de session trop long** : Un délai d'expiration trop élevé pour une session peut permettre à un attaquant d'accéder au compte d'un utilisateur inactif [30].
— **Absence de politique de verrouillage de compte** : Cela facilite les attaques par force brute sur les identifiants.

Pour prévenir ces risques, il est essentiel de suivre des pratiques de sécurité strictes : validation côté serveur des entrées utilisateur, chiffrement des communications (HTTPS), protection des cookies, limitation des tentatives de connexion, journalisation des accès, et mises à jour régulières des composants utilisés.

1.7 Bonnes pratiques de sécurité applicative

La sécurité des applications web est essentielle pour prévenir les attaques potentielles et protéger les données sensibles des utilisateurs. Pour cela, plusieurs bonnes pratiques doivent être suivies tout au long du cycle de développement des applications, de la conception à la mise en production. Voici quelques-unes des pratiques de sécurité les plus importantes à appliquer dans le développement d'applications web .

1.7.1 Validation et filtrage des entrées

La validation des entrées est une étape cruciale pour prévenir les attaques par injection (par exemple, injection SQL, XSS). Il est essentiel de valider et de filtrer toutes les données provenant des utilisateurs avant de les traiter ou de les utiliser dans des requêtes. Les entrées doivent être filtrées pour s'assurer qu'elles ne contiennent aucun code malveillant et doivent être validées en fonction de leur type, longueur, format et plage de valeurs [9].

1.7.2 Utilisation du chiffrement

Le chiffrement des données sensibles est un pilier fondamental de la sécurité des applications web. Les informations telles que les mots de passe, les données personnelles, et les communications doivent être chiffrées à l'aide de protocoles de sécurité forts (par exemple, TLS pour les communications et AES pour les données au repos). De plus, il est important d'utiliser des méthodes de hachage sécurisées pour le stockage des mots de passe, comme bcrypt ou Argon2 [8].

1.7.3 Gestion sécurisée des sessions et des cookies

Les sessions doivent être sécurisées pour éviter les détournements de session. Cela inclut l'utilisation de cookies sécurisés, la mise en place de mécanismes de renouvellement des sessions après authentification et la limitation de la durée de vie des sessions. Les cookies doivent être configurés avec les attributs Secure et HttpOnly pour empêcher leur vol via des attaques XSS [27].

1.7.4 Mise en œuvre de contrôles d'accès rigoureux

Un contrôle d'accès correct est essentiel pour s'assurer que seuls les utilisateurs autorisés peuvent accéder à des ressources ou exécuter des actions spécifiques. Il est important de mettre en place un système de gestion des rôles (RBAC) et de s'assurer que les utilisateurs n'ont accès qu'aux informations et aux fonctionnalités nécessaires à leur rôle. Les mécanismes de contrôle d'accès doivent être basés sur les principes de moindre privilège et de séparation des tâches [7].

1.7.5 Surveillance et journalisation

La surveillance continue des applications et la journalisation des événements de sécurité sont essentielles pour détecter et répondre rapidement à des incidents de sécurité. Les journaux doivent être protégés contre les modifications non autorisées et être suffisamment détaillés pour permettre une analyse efficace en cas d'attaque. La journalisation des actions des utilisateurs, des erreurs du système et des tentatives d'accès non autorisées peut fournir des informations cruciales pour l'identification et la résolution des problèmes de sécurité [10].

1.7.6 Tests de sécurité et audits réguliers

Les tests de sécurité doivent être réalisés régulièrement pour identifier les vulnérabilités dans l'application. Ces tests incluent des tests de pénétration, des analyses de vulnérabilités automatiques et des revues de code. L'objectif est de repérer les failles potentielles avant qu'elles ne soient exploitées par des attaquants. En outre, des audits de sécurité réguliers doivent être effectués pour garantir que les pratiques de sécurité sont maintenues au fil du temps [12].

1.8 Conclusion

Ce chapitre a permis de poser les bases essentielles de la Sécurité des applications web ansi que l'audit informatique en présentant ses définitions, objectifs, types et méthodologies. Il a offert une vue d'ensemble sur les différentes approches possibles selon les contextes organisationnels et techniques. Ces fondements théoriques constituent un point de départ nécessaire pour aborder, dans le prochain chapitre, Contexte institutionnel et réglementaire.

Chapitre 2

Contexte Institutionnel et Réglementaire

2.1 Introduction

Les applications web constituent aujourd'hui une composante incontournable des systèmes d'information. Leur complexité croissante et leur exposition permanente à Internet en font des cibles privilégiées pour les cyberattaques. Ce chapitre s'attache à expliquer le fonctionnement général des applications web, de leur architecture aux méthodes de traitement des données, tout en identifiant les failles potentielles qui peuvent compromettre leur sécurité. Une compréhension fine de ces mécanismes est indispensable à toute démarche d'audit ciblée et pertinente.

2.2 Présentation du Ministère de l'Industrie

Le Ministère de l'Industrie et de la Production Pharmaceutique est un organisme gouvernemental chargé de la gestion et de l'organisation du secteur industriel en Algérie. Ses missions principales incluent le développement et la compétitivité industriels, la promotion de l'investissement, et le suivi des contributions de l'État au secteur public industriel. Le ministère est également responsable de la promotion des petites et moyennes entreprises (PME) et de la restructuration du secteur industriel pour répondre aux besoins économiques actuels.

2.2.1 Structure organisationnelle

Le ministère est organisé autour de plusieurs directions générales et structures spécialisées, notamment :

Cabinet du ministre : chargé de l'accompagnement politique et administratif du ministre dans les instances gouvernementales.

Direction des ressources humaines : élabore et applique la politique des ressources humaines du ministère.

Direction de l'administration et des moyens : responsable de la gestion du budget, de la comptabilité, et des services généraux.

Direction générale du secteur public marchand : s'occupe des participations de l'État, des partenariats, et du développement des entreprises publiques.

Direction générale de l'investissement industriel : pilote les politiques d'investissement, d'aménagement foncier, et la promotion des petites et moyennes entreprises (PME).

2.2.2 Objectifs et rôle du ministère

— Renforcer la compétitivité des industries nationales.
— Promouvoir l'investissement dans le secteur industriel.
— Moderniser les infrastructures industrielles et technologiques.
— Assurer la sécurité et la fiabilité des systèmes d'information

2.3 Importance des systèmes d'information et de la digitalisation

Les systèmes d'information jouent un rôle crucial dans la gestion et le fonctionnement du ministère. Ils permettent une meilleure coordination entre les différentes directions, une gestion efficace des données, et une prise de décision plus rapide et plus précise. La digitalisation des processus administratifs et industriels est essentielle pour améliorer l'efficacité opérationnelle et répondre aux exigences modernes de gestion.

Gestion des données :

- La centralisation des données améliore la sécurité et l'accessibilité, permettant une gestion efficace des informations industrielles et économiques [20].
- L'intégration efficace des données permet également aux organisations d'identifier les tendances, d'optimiser les processus, de réduire le gaspillage et d'améliorer les performances [4].

Communication interne et externe :

- Le SI met en place des réseaux sécurisés pour l'échange d'informations, favorisant la collaboration entre les différents services et les entités externes [20].
- L'amélioration des canaux de communication favorise également le partage des connaissances et la coordination, qui sont essentiels pour l'efficacité opérationnelle [4].

Aide à la décision :

- Le développement d'outils analytiques facilite la prise de décisions stratégiques, en fournissant des informations fondées sur des données fiables [23].
- Les systèmes d'information rationalisent le processus décisionnel, en augmentant la précision et la rapidité pour répondre aux besoins évolutifs [23].

Services en ligne :

- Les services numériques simplifient les procédures administratives pour les entreprises et les investisseurs, en promouvant la transparence et l'efficacité de l'administration publique [20].

2.4 Enjeux liés à la cybersécurité

Dans le contexte de la digitalisation, la cybersécurité est devenue un défi crucial pour les institutions publiques,qui sont de plus en plus ciblés par des cyberattaques sophistiquées. Ces défis touchent aussi bien les aspects stratégiques, opérationnels, juridiques qu'humains.

Protection des données sensibles [31] : — Les services publics traitent des informations critiques, y compris des données personnelles et stratégiques, qui, si elles sont compromises, peuvent menacer la souveraineté nationale.
— La mise en œuvre de systèmes de cryptage, de pare-feu et de détection d'intrusion est essentielle pour protéger ces données contre tout accès non autorisé.

Maintien de la continuité du service [28] : — Les cyberattaques, telles que les attaques DDoS et les rançongiciels, peuvent perturber des services essentiels, nécessitant des mesures de cybersécurité robustes pour garantir la disponibilité en cas d'incident.

Conformité aux obligations légales [2] : — Les organismes publics doivent respecter les réglementations nationales et internationales ; ne pas le faire peut entraîner des sanctions légales et porter atteinte à la crédibilité des institutions.
— Une gestion efficace de la cybersécurité est essentielle à la conformité et au maintien de la confiance du public.

Préserver la confiance des citoyens [24] : — Les violations très médiatisées peuvent gravement endommager les relations entre les citoyens et les institutions publiques, ce qui souligne l'importance de la sécurité numérique pour renforcer la confiance.
— La transparence et une communication efficace sur les mesures de cybersécurité peuvent renforcer la confiance du public.

Maîtrise des risques technologiques [19] : — L'adoption rapide de technologies telles que le cloud computing et l'IoT introduit de nouveaux risques, nécessitant une surveillance continue et des stratégies proactives.

2.5 Risques et défis pour un organisme gouvernemental

En tant qu'organisme gouvernemental, le ministère est exposé à plusieurs risques en matière de cybersécurité, notamment :

— **Attaques par déni de service (DDoS)** : Ces attaques visent à rendre les services en ligne indisponibles en surchargeant les serveurs avec un volume important de requêtes malveillantes [1].
— **Usurpation d'identité (spoofing)** : Les pirates peuvent falsifier des adresses IP ou des identifiants pour se faire passer pour des utilisateurs ou systèmes légitimes et ainsi accéder aux systèmes internes [1].
— **Vol de données sensibles** : Les informations confidentielles, telles que les données industrielles, les informations personnelles ou les plans stratégiques, peuvent être ciblées par des cybercriminels à des fins d'espionnage ou de sabotage [1].
— **Phishing et attaques par ingénierie sociale** : Ces techniques consistent à tromper les employés via des courriels ou des messages frauduleux afin d'obtenir des informations sensibles ou un accès non autorisé aux systèmes [1].

Outre ces risques, le ministère doit également relever plusieurs défis majeurs pour renforcer sa posture en cybersécurité :

— **Sécurisation des réseaux** : assurer la protection des réseaux internes contre les intrusions et les attaques externes.
— **Formation des employés** : sensibiliser le personnel aux bonnes pratiques en matière de cybersécurité pour réduire les risques liés à l'erreur humaine.
— **Mise à jour des systèmes** : maintenir les systèmes d'information à jour avec les derniers correctifs de sécurité pour éviter les vulnérabilités connues.

2.6 Cadre réglementaire

La sécurité des systèmes d'information ne peut être dissociée de son cadre réglementaire. Celui-ci énonce les normes auxquelles les entreprises doivent adhérer pour garantir la sécurité de leurs actifs informationnels.

2.6.1 Normes internationales : ISO/IEC 27001

L'ISO/IEC 27001 est une norme internationale, elle est la plus reconnue au monde en matière de système de management de sécurité de l'information (SMSI), elle fournit aux entreprises des lignes directrices pour l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue d'un système de management de la sécurité de l'information [6, page 2584].

2.6.2 OWASP Top 10

L'OWASP Top 10 est un référentiel technique publié par l'*Open Web Application Security Project* (OWASP), une communauté internationale spécialisée en sécurité applicative. Ce document recense les 10 risques de sécurité les plus critiques affectant les applications web.

2.6.2.1 Statut et autorité

— Référentiel technique non normatif mais largement reconnu.
— Utilisé comme standard de facto dans les audits de sécurité web.
— Mis à jour tous les 3 ans (dernière version : 2021) [26].

2.6.2.2 Objectifs

— Identifier les vulnérabilités web les plus critiques.
— Prioriser les corrections lors des audits de sécurité.
— Guider les développeurs vers des bonnes pratiques [9].

2.6.2.3 Contenu

Le référentiel classe les risques de A01 à A10, incluant :

— Injections (A03).
— Contrôles d'accès défaillants (A01).
— Configuration incorrecte (A05) [26].

2.6.2.4 Complémentarité avec le RNSI

— Le RNSI fournit le cadre organisationnel (Domaines 5 et 6) [21].
— L'OWASP Top 10 apporte les spécificités techniques pour les applications web.
— Utilisation conjointe recommandée par l'ANSSI [1].

2.6.3 Référentiel National de la Sécurité de l'Information (RNSI)

Le Référentiel National de Sécurité de l'information (RNSI 2020) est un document élaboré par le Ministère de la Poste, des Télécommunications, des Technologies et du Numérique (MPTTN) de l'Algérie. Il vise à établir une gouvernance et une approche commune de la sécurité de l'information au sein des organismes publics. Il définit aussi les exigences minimales en matière de sécurité qui permettent de gérer, résister et réduire l'impact des menaces qui peuvent survenir. Le RNSI présente aussi les contrôles de sécurité et les bonnes pratiques à adopter par les organismes publics tels que l'ISO/IEC 27001 et le NIST, tout en focalisant sur la formation et la sensibilisation des usagers aux risques encourus, et l'évaluation périodique des contrôles afin d'assurer la satisfaction continue des exigences de sécurité et la conformité aux obligations réglementaires [21].

2.6.3.1 Objectifs du RNSI 2020

Les objectifs du référentiel perceptibles à travers ses différents domaines sont :

— Augmenter le niveau de sécurité des systèmes d'information et la protection des informations des organismes par la mise en place des contrôles de sécurité adéquats.
— Adopter une approche basée sur l'appréciation des risques lors de l'implémentation des contrôles de sécurité.
— Définir les rôles et responsabilités appropriées en matière de protection des informations.

2.6.3.2 Champ d'application

Le champ d'application du RNSI couvre l'ensemble des administrations et entités du secteur public, ainsi que toute infrastructure informatique hébergée sur le territoire national traitant des informations sensibles, conformément aux législations algériennes en vigueur. Ce référentiel constitue ainsi un socle commun pour renforcer la résilience numérique de l'État et harmoniser les pratiques de sécurité au sein des institutions publiques.

2.6.4 Lois algériennes applicables

En Algérie, la protection des données personnelles et de la cybersécurité est supervisée par des documents législatifs spécifiques pour garantir la sécurité, l'intégrité et la disponibilité des informations.

2.6.4.1 Décret présidentiel n° 20-05 du 24 Joumada El Oula 1441 (20 janvier 2020)

Ce décret met en œuvre un dispositif national de sécurité du système d'information (DNSSI) en Algérie. Il définit le cadre organisationnel et stratégique pour améliorer la protection de l'infrastructure numérique nationale [14].

Les principaux points mentionnés sont :

— Création du Conseil national de la sécurité des systèmes d'information (CNSSI) : Il élabore la stratégie nationale et assure la coordination des efforts de cybersécurité.
— Mise en place de l'Agence de la sécurité des systèmes d'information (ASSI) : Responsable de la mise en œuvre des politiques de cybersécurité, de l'audit des systèmes importants et de la coordination des réactions aux incidents.
— Obligations pour les organisations et entreprises de nommer un responsable de la sécurité de l'information (RSSI) dans un délai maximum d'un an après l'annonce du décret.
— Supervision de l'audit de sécurité et classification des systèmes d'information pour assurer une meilleure protection des infrastructures critiques.
— Renforcement de la coopération nationale et internationale en cybersécurité.

Ce cadre juridique vise à améliorer la résilience des systèmes d'information en Algérie contre les cybermenaces et à assurer la protection des données sensibles des organisations et des citoyens.

2.6.4.2 Loi n° 09-04 du 5 août 2009 sur la cybersécurité et la lutte contre la cybercriminalité

Cette loi établit un cadre juridique pour la prévention et la lutte contre les infractions liées aux technologies de l'information et de la communication. Elle définit les règles spécifiques applicables aux crimes numériques et les moyens de surveillance et d'investigation autorisés par les autorités compétentes [15].

Principaux axes :

— Définition des infractions numériques : accès illégal, atteintes aux données, cyberfraude, diffusion de contenus illicites, etc.
— Surveillance des communications électroniques : possibilité d'interception en cas de menace pour la sécurité nationale ou enquête judiciaire.
— Perquisitions et saisies numériques encadrées légalement.
— Obligations des fournisseurs de services : conservation des données de connexion, assistance judiciaire.

— Coopération internationale en matière de cybercriminalité transnationale.

Cette loi est essentielle pour sécuriser les infrastructures numériques en Algérie et renforcer la lutte contre la cybercriminalité.

2.6.4.3 Décret exécutif n° 16-61 du 2 Joumada El Oula 1437 (11 février 2016)

Ce décret modifie et complète le décret n° 09-410 du 10 décembre 2009, fixant les règles de sécurité applicables aux équipements sensibles [13].

Principaux points :

— Définition des équipements sensibles (télécommunications, surveillance, etc.)
— Obligation d'agrément pour opérateurs manipulant ces équipements.
— Exigences de sécurité physique et logique des infrastructures.
— Restrictions sur l'accès, importation, utilisation, cession.
— Interdiction de connexion internet des systèmes de vidéosurveillance.

2.6.4.4 Loi n° 18-04 du 24 Chaâbane 1439 (10 mai 2018)

Cette loi fixe les règles générales relatives à la poste et aux communications électroniques en Algérie [16].

Points principaux :

— Sécurité et intégrité des réseaux.
— Création d'une autorité de régulation indépendante.
— Surveillance stricte des communications électroniques.
— Protection des données et cybersécurité.
— Garantie du service universel sur le territoire national.

2.6.4.5 Loi n° 18-07 du 25 Ramadhan 1439 (10 juin 2018)

Cette loi porte sur la protection des personnes physiques dans le traitement des données à caractère personnel [17].

Principaux points :

— Consentement et transparence pour la collecte et l'utilisation des données personnelles.
— Droits d'accès, correction, suppression, opposition pour les citoyens.
— Obligations des responsables de traitement en matière de confidentialité et sécurité.
— Encadrement strict des transferts internationaux de données.
— Sanctions en cas de non-conformité.

2.7 Conclusion

Ce chapitre a présenté le ministère, son organisation, ainsi que l'importance des systèmes d'information et des enjeux de cybersécurité qui y sont liés. Il a aussi détaillé le cadre

réglementaire qui encadre la sécurité des systèmes d'information. Ces éléments posent les bases pour mieux comprendre, dans le chapitre suivant, l'évolution des applications web, leurs architectures et les vulnérabilités associées, afin d'aborder les bonnes pratiques de sécurité applicative indispensables aujourd'hui.

Chapitre 3

Planification et déroulement de l'audit

3.1 Introduction

La conduite d'un audit de sécurité efficace repose sur une planification rigoureuse et une démarche structurée. Ce chapitre détaille les étapes clés de l'audit réalisé, depuis la définition du périmètre et des objectifs jusqu'à la cartographie du système audité. Il présente la méthode adoptée, les types de tests effectués ainsi que les outils mobilisés, en s'appuyant sur des référentiels reconnus tels que l'ISO 27001 et le RNSSI. Ce cadre méthodologique permet d'assurer la cohérence de l'audit, la pertinence des observations formulées et la fiabilité des résultats obtenus.

3.2 Définition du périmètre et des objectifs

3.2.1 Délimitation du périmètre de l'audit

Le périmètre de l'audit couvre l'ensemble des composants techniques sur lesquels repose l'application web étudiée. L'environnement cible est un serveur Linux (Ubuntu 22.04.2 LTS) sur lequel est déployée une application développée avec le framework Laravel. L'analyse englobe à la fois les éléments d'infrastructure et les aspects applicatifs. L'audit s'est concentré sur les points suivants :

— Le serveur Ubuntu hébergeant l'application web.
— L'analyse locale du code source de l'application Laravel afin d'en identifier les potentielles failles de sécurité.
— Les services réseau exposés, notamment :

HTTP (port 80/443) : interface web accessible publiquement
SSH (port 22) : accès distant pour l'administration
MySQL (port 3306) : base de données relationnelle.

— La base de données : structure, droits d'accès, configuration de sécurité.
— La configuration globale du système et des services applicatifs installés.

3.2.2 Objectifs de l'audit de sécurité

L'objectif principal de cet audit est d'évaluer le niveau de sécurité de l'application web ainsi que de l'environnement serveur sur lequel elle est déployée. Il s'agit d'identifier les vulnérabilités techniques, les erreurs de configuration et les mauvaises pratiques susceptibles de compromettre la confidentialité, l'intégrité ou la disponibilité des données.

Plus précisément, les objectifs poursuivis sont les suivants :

— Identifier les failles de sécurité présentes dans le code source de l'application Laravel (injections, failles XSS, mauvaise gestion des sessions, etc.).
— Vérifier la sécurisation des services exposés (HTTP, SSH, MySQL), en portant une attention particulière à la configuration par défaut, aux ports ouverts et aux mécanismes d'authentification.

— Évaluer la configuration du système d'exploitation et des composants logiciels installés (droits d'accès, journalisation, mises à jour, etc.).
— Analyser la structure de la base de données et les droits d'accès associés, en vue de détecter d'éventuelles failles ou élévations de privilèges.
— Émettre des recommandations concrètes visant à renforcer la sécurité globale du système audité.

3.3 Méthodologie et approche adoptée

3.3.1 Cadres de référence utilisés

Dans le cadre de cet audit, plusieurs référentiels reconnus ont été mobilisés pour guider l'analyse technique et orienter les recommandations de sécurité.

RNSSI (Référentiel National de Sécurité des Systèmes d'Information – Algérie, 2020) :
Utilisé comme référentiel principal pour la conduite de l'audit et l'élaboration des recommandations, Fournit un ensemble d'exigences en matière de sécurité adaptées aux SI algériens.
→ Sert de référence pour les bonnes pratiques en contexte institutionnel algérien.
Le tableau ci-dessous synthétise les domaines du RNSI les plus pertinents par rapport au périmètre audité, et précise leur lien avec nos constats :

TABLE 3.1 – Correspondance entre les domaines RNSI et l'audit – Partie 1

Domaine RNSI	**Titre du domaine**	**Lien avec l'audit et les recommandations**
Domaine 1	Gestion des actifs	Inventaire des services exposés, identification des composants sensibles.
Domaine 3	Gestion et contrôle des accès	Recommandations sur l'accès SSH, les droits `sudo`, et la gestion des comptes MySQL.
Domaine 5	Sécurité des réseaux	Analyse des ports ouverts, durcissement des services accessibles, filtrage recommandé.
Domaine 6	Sécurité des systèmes d'information	Vérification de la configuration du système Linux, des permissions critiques et des mises à jour.

TABLE 3.2 – Correspondance entre les domaines RNSI et l'audit – Partie 2

Domaine RNSI	Titre du domaine	Lien avec l'audit et les recommandations
Domaine 7	Sécurité liée à l'exploitation	Analyse des processus actifs, fichiers sensibles, configuration du serveur web.
Domaine 8	Sécurité des systèmes critiques	Application Laravel en développement : attention portée aux modules fonctionnels sensibles.
Domaine 13	Surveillance et journalisation	Recommandations sur la journalisation des accès et événements (`auth.log`, `nginx`, `mysql`).
Domaine 14	Gestion des incidents de sécurité	Propositions d'activation des mécanismes de détection et de réaction (IDS, alertes système).

ISO/IEC 27001 : Apport méthodologique complémentaire, notamment pour la définition du périmètre et la gestion des risques.
→ Utilisé pour cadrer la logique globale de l'audit.

OWASP Top 10 (2021) : Employé pour l'évaluation des vulnérabilités applicatives.
→ Sert à identifier les failles les plus répandues affectant les applications web.

3.3.2 Type d'audit

Le présent audit de sécurité est à la fois**technique** et **organisationnel (hybride)**. Sur le plan technique, l'audit couvre l'ensemble de la pile technologique, incluant le système d'exploitation, le réseau, l'application web et la base de données. Il comprend des tests de vulnérabilités (injection SQL, XSS, etc.). Sur le plan organisationnel, l'audit s'appuie sur le **Référentiel National de Sécurité des Systèmes d'Information (RNSI)** algérien, afin d'évaluer la conformité des pratiques en matière de sécurité et la mise en œuvre des politiques internes de protection des données.

3.3.3 Type de test

Le type de test réalisé dans le cadre de cet audit est un **test de type Gray Box**, dans la mesure où un certain niveau d'information sur l'environnement cible (infrastructure, application, base de données) était disponible. Cette approche permet de simuler une attaque émanant d'un utilisateur authentifié ou d'un acteur interne disposant d'un accès partiel au système. Le choix de cette méthode vise à conjuguer les avantages des approches Black Box (réalisme des attaques externes) et White Box (profondeur et précision de l'analyse technique).

3.4 Plan d'audit et organisation des étapes

L'audit de sécurité s'est déroulé sur une période de deux mois, selon une approche structurée en quatre phases principales. Cette planification a permis de garantir une couverture exhaustive de l'infrastructure auditée, en mobilisant des outils adaptés à chaque étape et en respectant les bonnes pratiques recommandées par les référentiels RNSI, ISO/IEC 27001 et OWASP.

3.4.1 Phases principales de l'audit

Reconnaissance : collecte d'informations sur l'environnement, identification des services exposés, scan de ports, inventaire des technologies.

Analyse : examen des configurations réseau, système et application ; détection des vulnérabilités potentielles.

Exploitation : validation expérimentale de certaines vulnérabilités dans un environnement contrôlé.

Validation : vérification des résultats, mesure d'impact, détection des faux positifs et élaboration des recommandations.

3.4.2 Tableau récapitulatif des étapes de l'audit

Table 3.3 – Résumé des étapes de l'audit de sécurité

Phase	Objectif principal	Outils mobilisés	Durée estimée
Reconnaissance	Identifier les services accessibles, les IP actives, les technologies déployées	`nmap`, `masscan`, `whatweb`, `netstat`, `ss`, `whois`, `dig`, `nslookup`	Semaine 1 à 2
Analyse	Analyser les configurations système, réseau et applicative ; détecter les vulnérabilités	`nikto`, `OWASP ZAP`, `sslscan`, `sslyze`, `rkhunter`, `chkrootkit`, `grep`, `find`, `clamav`	Semaine 3 à 6
Exploitation	Valider les vulnérabilités détectées de manière contrôlée	`Metasploit`, `SQLmap`, `Gobuster`, `dirb`, `curl`	Semaine 6 à 7
Validation	érification des résultats, mesure d'impact, détection des faux positifs et élaboration des recommandations.s	`journalctl`, `auth.log`, vérification manuelle, re-scan ciblé	Semaine 8

3.5 Outils et technologies mobilisés

3.5.1 Présentation des outils d'audit utilisés

Dans le cadre de cet audit de sécurité, un ensemble d'outils open-source et de commandes Linux ont été mobilisés pour couvrir l'analyse du système, du réseau, des services exposés, ainsi que la sécurité applicative et des bases de données. Ces outils ont été sélectionnés pour leur efficacité, leur compatibilité avec les environnements Linux, et leur reconnaissance dans la communauté de la cybersécurité.

Les outils utilisés peuvent être regroupés selon les catégories suivantes :

Cartographie et analyse réseau :

- **Nmap** : Identification des hôtes actifs, ports ouverts, versions de services, scripts d'audit de vulnérabilités.
- **Masscan** : Scan rapide de grandes plages IP.

Tests de sécurité des applications web :

- **OWASP ZAP** : Détection automatique des vulnérabilités Web (XSS, injections...).
- **Nikto** : Scanner Web pour détecter des failles connues sur les serveurs HTTP.
- **WhatWeb** : Identification des technologies utilisées par un site Web.

Analyse du trafic et inspection des paquets :

- **Wireshark** : Capture et analyse détaillée des paquets réseau.
- **Tcpdump** : Capture de trafic en ligne de commande pour inspection rapide.

Outils système et réseau :

- **ss**, **netstat**, **iptables**, **nc**, **telnet** : Inspection des connexions réseau, écoute de ports, tests d'accessibilité.
- **find**, **grep**, **awk**, **cut** : Analyse des fichiers sensibles, utilisateurs système, permissions suspectes.
- **curl**, **wget** : Requêtes HTTP, test de connectivité et d'API.

Évaluation des vulnérabilités et exploitation :

- **Metasploit Framework** : Tests de pénétration avancés et exploitation de vulnérabilités.
- **SQLmap** : Détection et exploitation d'injections SQL.
- **Gobuster**, **Dirb** : Brute-force de répertoires et fichiers cachés.

Outils de détection de malwares ou rootkits :

- **rkhunter**, **chkrootkit**, **ClamAV** : Détection de rootkits et malwares sur le système.

3.5.1.1 Outils utilisés dans un audit EXTERNE

Phase 1 — Reconnaissance et cartographie

Outil	Fonction principale	Objectif dans l'audit
Nmap	Scan de ports, détection d'hôtes/-services	Cartographier les systèmes exposés
Masscan	Scan rapide de ports TCP	Identifier rapidement les services accessibles
WhatWeb	Détection des technologies web	Identifier les frameworks/applications en place
Wappalyzer	Fingerprinting d'applications Web	Obtenir une signature technologique

TABLE 3.4 – Outils utilisés et leur rôle dans l'audit de sécurité

Phase 2 — Analyse de vulnérabilités

Outil	Fonction principale	Objectif dans l'audit
Nikto	Analyse de sécurité HTTP	Identifier les vulnérabilités web basiques
OWASP ZAP	Scanning Web (actif/passif)	Repérer XSS, injections, mauvaises configurations
SSLyze / sslscan	Audit de certificats et protocoles SSL/TLS	Vérifier la robustesse du chiffrement

TABLE 3.5 – Outils d'analyse de la sécurité Web

Phase 3 — Exploitation ciblée

Outil	Fonction principale	Objectif dans l'audit
SQLmap	Injection SQL automatisée	Tester la sécurité des bases de données
Gobuster / Dirb	Bruteforce de chemins/dossiers Web	Trouver des ressources non protégées
Metasploit	Framework d'exploitation	Valider la faisabilité d'une compromission

TABLE 3.6 – Outils d'exploitation et de tests automatisés

3.5.1.2 Outils utilisés dans un audit INTERNE

Phase 1 — Reconnaissance locale

Outil	Fonction principale	Objectif dans l'audit
netstat / ss	Affichage des connexions réseau actives	Identifier les services en écoute
ps / systemctl	Liste des processus/services	Détecter des programmes non légitimes

TABLE 3.7 – Outils système pour l'analyse locale

Phase 2 —Analyse système et intégrité

Outil	Fonction principale	Objectif dans l'audit
find / grep / awk / getent	Recherches de comptes, permissions, fichiers	Identifier des failles locales ou élévations de privilège
journalctl / auth.log	Analyse des logs système	Détecter des intrusions ou comportements anormaux
rkhunter / chkrootkit	Détection de rootkits et malwares	Vérifier l'intégrité du système local

TABLE 3.8 – Outils d'analyse locale et de sécurité système

Phase 3 —Post-exploitation et élévation

Outil	Fonction principale	Objectif dans l'audit
Metasploit	Modules d'élévation de privilèges	Tester les failles locales connues

TABLE 3.9 – Utilisation de Metasploit pour les élévations de privilèges

3.5.1.3 Outils hybrides (interne / externe selon le contexte)

Certains outils sont polyvalents et utilisés dans les deux types d'audit.

Outil	Cas d'usage externe	Cas d'usage interne
Nmap	Scan d'IP publiques	Scan du réseau local interne
Wireshark / Tcpdump	Surveillance réseau passif	Capture de trafic en interne (sniffing)
OWASP ZAP	Scan d'applications web publiques	Analyse des applications internes
Metasploit	Exploitation à distance	Post-exploitation locale

TABLE 3.10 – Comparaison des cas d'usage des outils en audit externe et interne

3.6 Topologie de l'infrastructure auditée

L'application web auditée est déployée dans une infrastructure structurée autour d'un pare-feu avancé, d'un WAF (Web Application Firewall), et de plusieurs services répartis sur des segments réseau distincts.

3.6.1 Schéma de topologie

Le schéma suivant (Figure 3.1) représente l'architecture technique de l'application auditée. Il met en évidence les différents éléments de sécurité déployés, les flux réseau et les composants critiques.

- **Pare-feu (Firewall)** : placé en frontal, il filtre le trafic réseau entrant et sortant. Il est équipé de :
  - **IDS/IPS** : pour la détection et la prévention des intrusions,
  - **Module GeoIP** : pour bloquer ou filtrer les adresses IP en fonction de leur origine géographique,
  - **Module de réputation IP** : pour rejeter automatiquement les connexions suspectes connues.
- **Adresse IP publique (IP externe)** : permet l'accès depuis Internet via les ports HTTP.
- **Réseau virtuel (V-IP)** : assure une séparation logique des flux internes et expose uniquement les services nécessaires.
- **WAF (Web Application Firewall)** : filtre les requêtes HTTP en profondeur, détecte les tentatives d'injection, de XSS, de fuzzing, etc. Il redirige le trafic légitime vers le serveur applicatif.
- **Serveur applicatif (Laravel)** : hébergé sur une machine Ubuntu 22.04.2 LTS avec une IP interne sécurisée. Il traite les requêtes, accède à la base de données et génère dynamiquement les réponses.
- **Base de données MySQL** : non exposée publiquement. Elle est accessible uniquement depuis le serveur Laravel via le réseau interne.

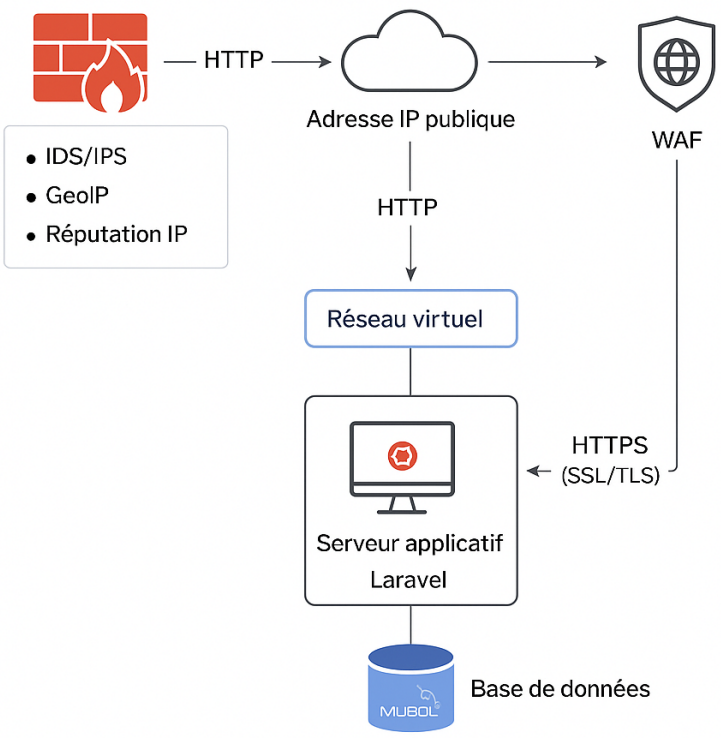

FIGURE 3.1 – Topologie du système audité

3.7 Contexte de l'application web auditée

L'application web auditée est une plateforme sécurisée, exclusivement destinée à un usage interne par les employés du groupe **Agrodive**. Elle ne comporte qu'un point d'accès via une interface d'authentification, et son utilisation est strictement soumise à une procédure de demande et de validation auprès de la direction.

3.8 Points d'entrée et structure applicative

L'audit a identifié plusieurs points d'entrée potentiels pour un attaquant :

Interface web (HTTP) : point d'accès principal à l'application.

Port SSH : accessible pour la gestion distante du serveur, nécessite un durcissement particulier.

Services réseau supplémentaires : tels que MySQL (en écoute locale), susceptibles d'être ciblés en cas de mauvaise configuration.

Structure applicative : l'application suit une architecture MVC typique de Laravel, avec des contrôleurs exposant certaines routes vulnérables si non sécurisées.

3.9 Critères d'évaluation des vulnérabilités

Afin d'évaluer de manière objective les vulnérabilités identifiées au cours de l'audit, nous nous sommes appuyés sur le système de notation standardisé CVSS v3.1 (Common Vulnerability Scoring System), largement reconnu dans l'industrie de la cybersécurité [5].

Ce système fournit un cadre méthodologique pour mesurer la gravité des vulnérabilités en se basant sur plusieurs facteurs, tels que :

— Le vecteur d'attaque (réseau, local, physique).
— La complexité d'exploitation.
— Le niveau de privilège requis.
— L'interaction nécessaire avec l'utilisateur.
— L'impact potentiel sur la confidentialité, l'intégrité et la disponibilité.

Dans le cadre de cet audit, seul le score de base (Base Score) a été utilisé. Ce score représente la gravité intrinsèque de la vulnérabilité, indépendamment du contexte organisationnel ou temporel. Il permet d'estimer rapidement le niveau de risque et de prioriser les actions correctives à entreprendre.

Les vulnérabilités identifiées ont été classées selon les intervalles de gravité suivants [5] :

— **0.0 – 3.9 : Faible** → Vulnérabilités à impact limité ou difficilement exploitables.
— **4.0 – 6.9 : Moyen** → Vulnérabilités présentant un risque modéré nécessitant une attention particulière.
— **7.0 – 8.9 : Élevé** → Vulnérabilités critiques nécessitant une correction prioritaire.
— **9.0 – 10.0 : Critique** → Vulnérabilités permettant une compromission complète du système.

Afin de visualiser la gravité des vulnérabilités détectées dans le périmètre audité, le graphique suivant présente leur répartition selon les catégories CVSS :

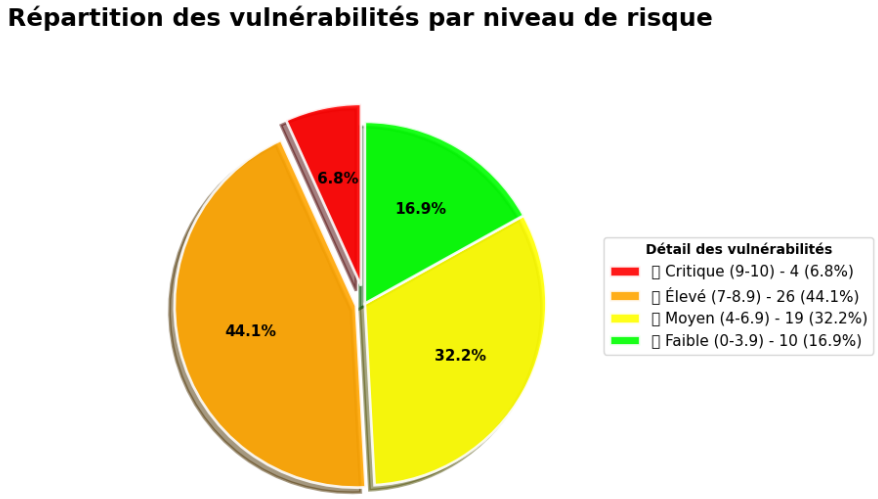

FIGURE 3.2 – Répartition des vulnérabilités par niveau de criticité (CVSSv3)

Ce graphique illustre la distribution des vulnérabilités identifiées, selon leur score *CVSSv3* de base. On observe une concentration significative de failles classées **élevées** (55,6 %) et **moyennes** (23,8 %), représentant ensemble environ **79,4 %** du total. Les vulnérabilités **faibles** (15,9 %) sont moins préoccupantes, mais doivent tout de même être surveillées. Les failles **critiques**, bien que représentant seulement 4,8 %, nécessitent une attention immédiate en raison de leur potentiel d'impact majeur sur la sécurité du système.

Exemple de calcul d'un score CVSS de base

Considérons la vulnérabilité suivante, identifiée dans le périmètre audité :

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`

Ce vecteur correspond aux valeurs suivantes :

- **AV (Attack Vector)** = Network = 0.85
- **AC (Attack Complexity)** = Low = 0.77
- **PR (Privileges Required)** = None = 0.85
- **UI (User Interaction)** = None = 0.85
- **S (Scope)** = Unchanged
- **C (Confidentiality)** = High = 0.56
- **I (Integrity)** = High = 0.56
- **A (Availability)** = High = 0.56

Impact (si `Scope = Unchanged`) :

$$\text{Impact} = 1 - (1 - C)(1 - I)(1 - A) = 1 - (0.44)^3 = 1 - 0.085 = 0.915$$
$$\text{Impact Score} = 6.42 \times 0.915 = 5.8773$$

Exploitabilité :

$$\text{Exploitability} = 8.22 \times AV \times AC \times PR \times UI = 8.22 \times 0.85 \times 0.77 \times 0.85 \times 0.85 \approx 3.85$$

Score de base final :

$$\text{Base Score} = \text{Impact Score} + \text{Exploitability} = 5.88 + 3.85 = 9.73 \Rightarrow \boxed{9.8}$$

Ce score est classé comme **critique**.

Calcul réalisé sur la base des spécifications officielles du CVSS v3.1 [5].

3.10 Limitations ou périmètre hors scope

Certaines limites techniques et organisationnelles ont restreint le périmètre de l'audit. Ces éléments, volontairement exclus ou inaccessibles durant l'évaluation, sont précisés ci-dessous :

Accès limité à l'interface utilisateur de l'application web : L'accès authentifié à l'interface web (frontend) n'a pas été possible durant l'audit.

Absence de visibilité sur les dispositifs de protection réseau : Aucun accès n'a été fourni concernant la configuration ou les règles en place du pare-feu applicatif (WAF) ou du pare-feu réseau (firewall).

Chapitre 4

Résultats de l'audit et recommandations

4.1 Introduction

Ce chapitre présente les résultats obtenus à l'issue de l'audit de sécurité mené sur l'application web du groupe agrodiv. Les constatations techniques sont détaillées selon différents axes d'analyse, incluant les services réseau, la configuration des composants serveur, la sécurité des échanges web et l'intégrité de la base de données. Chaque vulnérabilité identifiée est accompagnée d'une évaluation des risques associés, ainsi que de recommandations concrètes alignées sur les exigences du Référentiel National de Sécurité des Systèmes d'Information (RNSI 2020).

4.2 Constatations techniques détaillées

4.2.1 Vulnérabilités critiques identifiées

1. Configuration dangereuse de SSH (PermitRootLogin activé, authentification par mot de passe).
2. Exposition du service PHP-FPM sur l'interface réseau.
3. Absence de chiffrement TLS entre frontend et backend.
4. Service VPN obsolète accessible publiquement.
5. Fichier SQL critique présent sur le serveur.

4.2.2 Risques associés

— Compromission complète du serveur via SSH.
— Interception des données sensibles.
— Prise de contrôle de comptes utilisateurs.
— Accès non autorisé à la base de données.
— Attaques par force brute.

4.2.3 Recommandations principales

1. Correction immédiate des vulnérabilités critiques (SSH, PHP-FPM...).
2. Mise en œuvre du chiffrement TLS.
3. Renforcement des mécanismes d'authentification.
4. Mise à jour ou suppression du VPN obsolète.
5. Application des bonnes pratiques de sécurisation HTTP.

4.3 Constatations techniques détaillées

4.3.1 Services en écoute réseau

TABLE 4.1 – Ports ouverts et services associés

Port	Protocole	Service présumé	Justification
22	TCP	SSH	Accès distant pour l'administration système.
80	TCP	HTTP	Serveur web hébergeant l'application.

4.3.2 Configuration et sécurité du service SSH

TABLE 4.2 – Évaluation des paramètres SSH

Paramètre SSH	Valeur actuelle	Risque	Commentaire
PermitRootLogin	oui (autorisé)	● Critique	Permet aux attaquants de viser directement root et compromettre l'ensemble du système
PasswordAuthentication	oui	● Élevé	Favorise les attaques par force brute si le mot de passe est faible
UsePAM	no (désactivé)	● Moyen	Réduit les possibilités de sécurité fine en désactivant certains mécanismes d'authentification
MaxAuthTries	valeur par défaut	● Moyen	Facilite les attaques par force brute si le nombre d'essais n'est pas limité
AllowUsers	non défini	● Moyen	Aucun filtrage spécifique par utilisateur,tous les comptes valides peuvent tenter une connexion
X11Forwarding	non configuré	● Faible	Désactivé par défaut, limite les risques liés aux interfaces graphiques distantes

Recommandations SSH

— Interdire `PermitRootLogin`.
— Forcer l'authentification par clé SSH (`PasswordAuthentication no`).

— Réduire `MaxAuthTries` à 3 ou moins.
— Définir `AllowUsers` pour restreindre les accès autorisés.
— Installer `fail2ban` pour bloquer automatiquement les IP après échecs répétés.

4.3.3 Analyse de la configuration du serveur

TABLE 4.3 – Analyse de la configuration du serveur

Vulnérabilité	Détail technique	Risque	Commentaire
Protocoles TLS obsolètes activés	TLS 1.0, TLS 1.1	• Élevé	Vulnérable à POODLE et autres attaques
Cipher suites par défaut	Pas de `ssl_ciphers` personnalisé	• Élevé	Inclusion possible de ciphers faibles
HTTPS non forcé	Accès HTTP non redirigé vers HTTPS	• Élevé	Expose les échanges en clair
PHP-FPM écoute sur `interface publique`	Interface publique au lieu de localhost	• Élevé	Exposition inutile d'un backend critique
Mauvais `server_name`	Syntaxe incorrecte	• Moyen	Peut provoquer des conflits de résolution
Version serveur exposée	En-tête HTTP indique la version du serveur	• Faible	Facilite le fingerprinting des versions

Recommandations Serveur :

— Corriger la directive `server_name`.
— Désactiver TLS 1.0 / 1.1 : `ssl_protocols TLSv1.2 TLSv1.3`.
— Définir explicitement des `ssl_ciphers` modernes.
— Supprimer ou masquer l'en-tête `Server` (`server_tokens off`).
— Rediriger tout le trafic HTTP vers HTTPS (redirection 301).
— Restreindre PHP-FPM à `localhost` uniquement.

4.3.3.1 Évaluation de la sécurité de l'application Laravel (Backend)

TABLE 4.4 – Évaluation de sécurité Laravel (backend)

Vulnérabilité	Détail technique	Risque	Commentaire
CSRF manquant	Sur les routes API (`api.php`)	● Élevé	Possibilité de requêtes non autorisées
IDOR potentiel	`update_user`, `delete_user` sans contrôle d'accès	● Élevé	Accès possible à des comptes tiers
Absence de `auth:sanctum`	Sur routes sensibles	● Élevé	Accès non authentifié possible
Pas de validation stricte	Dans le `ClientController`	● Moyen	XSS possible si rendu HTML
Erreurs verbeuses	Stacktrace exposée publiquement	● Moyen	Révèle la structure de l'application
Faibles exigences de mot de passe	6 caractères seulement requis	● Moyen	Non conforme aux recommandations NIST

Recommandations Laravel :

— Appliquer `auth:sanctum` et CSRF sur toutes les routes sensibles
— Supprimer ou cacher les messages d'erreur détaillés côté API
— Valider systématiquement les entrées et encoder les sorties (ex : `htmlspecialchars`)
— Appliquer des règles de mot de passe robustes (longueur minimale, complexité, blacklist)

4.3.3.2 Sécurisation des entêtes HTTP et des sessions

TABLE 4.5 – Évaluation des entêtes HTTP et de la gestion de session

Élément	Problème détecté	Risque	Recommandation
Cookies `Secure` et `SameSite` absents	Accès aux cookies via MITM	● Élevé	Configurer ces attributs côté serveur
Headers manquants	Absence de `CSP`, `X-Frame-Options`, `HSTS`	● Élevé	Ajouter les Headers manquants
`SESSION_SECURE_COOKIE` à `false`	Cookies transmis en HTTP non sécurisé	● Élevé	Activer dans config/session.php

4.3.3.3 Analyse des privilèges et des outils système

TABLE 4.6 – Analyse des privilèges et outils de surveillance

Élément analysé	Détail technique	Risque
Contrôle de rootkits	Aucun outil installé (`chkrootkit`, `rkhunter`)	● Moyen
Fichiers SUID sensibles	Présence de fichiers standards avec droits SUID	● Faible

Commentaires :

— L'absence d'outils de détection de rootkits rend le système vulnérable à des compromissions furtives.

— Les fichiers SUID détectés sont classiques, mais une surveillance régulière est recommandée pour éviter les abus d'élévation de privilèges.

4.4 Analyse de l'exposition Réseau

4.4.0.1 Cartographie des ports internes (IP privée)

TABLE 4.7 – Ports internes détectés sur l'interface privée

Port	Protocole	Service	Risque
22	TCP	SSH	● Élevé
80	TCP	HTTP	● Élevé
port non standard 1	TCP	PHP-FPM (Laravel)	● Élevé
port non standard 2	TCP	Audit SPA HTTP	● Élevé
port non standard 3	TCP	Cisco SCCP (VoIP)	● Moyen
port non standard 4	TCP	SIP (VoIP)	● Faible

Analyse :

— Plusieurs services internes critiques sont accessibles en clair sur toutes les interfaces.

— `PHP-FPM` ne devrait être exposé que sur `localhost`.

— port non standard 2 expose des services non chiffrés (audit SPA HTTP).

— Les services VoIP (SIP/SCCP) semblent inutilisés et doivent être désactivés si non nécessaires.

4.4.0.2 Cartographie des ports exposés (IP publique)

TABLE 4.8 – Ports détectés sur l'interface publique

Port	Protocole	Service	Risque
port non standard 5	UDP	ISAKMP	● Critique
port non standard 6	TCP	SSL VPN	● Critique
443	TCP	HTTPS	● Élevé

Analyse :

— Le port non standard 6 expose un SSL VPN vulnérable à des attaques distantes connues.

— Aucune restriction d'IP ne protège ce service critique, augmentant fortement le risque.

— Le service ISAKMP (`port non standard 5/UDP`) est également exposé sans filtrage.

Recommandations :

— Fermer tous les services inutilisés (VoIP, Audit SPA) si non requis.

— Restreindre `PHP-FPM` et **port non standard 2** à `127.0.0.1`.

— Appliquer une politique de filtrage IP et firewall strict.

4.4.1 Évaluation du frontend web

4.4.1.1 Absence de chiffrement TLS entre frontend et backend

TABLE 4.9 – Absence de chiffrement entre frontend et backend

Élément	Description technique	Risque
Absence de chiffrement TLS	Les communications HTTP transitent en clair entre Vite/React et Laravel	● Élevé

4.4.1.2 Sécurité des cookies et des sessions

TABLE 4.10 – Évaluation des cookies et des sessions

Élément	Problème détecté	Risque
Cookies non sécurisés	Attributs `Secure` et `SameSite` absents	**Élevé**
`SESSION_SECURE_COOKIE`	Désactivé dans `session.php`	**Élevé**

4.4.1.3 En-têtes HTTP manquants

TABLE 4.11 – En-têtes HTTP manquants

Header	Problème	Risque
Strict-Transport-Security	Absent (pas de forçage HTTPS)	● Élevé
Content-Security-Policy	Absent ou mal configuré (`unsafe-inline`)	● Élevé
X-Frame-Options	Absent (protection contre clickjacking)	● Élevé
X-Content-Type-Options	Absent (protection contre MIME sniffing)	● Moyen

4.4.1.4 Code exposé côté client

TABLE 4.12 – Éléments sensibles exposés côté client

Élément	Description	Risque
JavaScript exposé dans le HTML	Fonctions internes visibles	● Moyen
Champs cachés sensibles	Présents dans le code source (`redir`, `grpid`)	● Moyen
Commentaires HTML révélateurs	`<!-sslvpnerrmsg=Too many bad login attempts->`	● Moyen

4.4.2 Analyse de la base de données

4.4.2.1 Système de gestion et structure

Système de gestion : MySQL
Nombre de tables : 22
Moteurs de stockage :

- **InnoDB** pour la majorité.
- **MyISAM pour certaines logs**

4.4.3 4.4.2 Cartographie des données sensibles

TABLE 4.13 – Tables contenant des données sensibles

Table	Description	Données sensibles détectées
`users`	Utilisateurs	email, username, password (bcrypt), phone
`clients`	Clients	NIF, téléphone, email
`password_reset_tokens`	Tokens de récupération	email, token (6 chiffres)
`personal_access_tokens`	Jetons API	token, abilities, tokenable_id
`mouvements`	Historique de mouvements clients	nif_client
`emplacements`, `entites`, `dairas`, etc.	Métadonnées géographiques ou métiers	Aucune donnée critique directe

4.4.3.1 Comptes et politique d'accès

TABLE 4.14 – État des éléments liés à la gestion des comptes et des accès

Élément	État actuel	Risque
Aucune politique de rotation	`password_lifetime` absent : validité illimitée	• Élevé
Aucune expiration des comptes	Aucun mécanisme de contrôle de l'âge des comptes	• Élevé
Comptes MySQL	6 comptes détectés, tous avec mot de passe défini	• Faible
Authentification `auth_socket` pour root	Active, accès restreint au système local	• Faible

Points positifs :

— Tous les comptes ont un mot de passe
— Aucun compte anonyme
— Password policy STRONG active (`validate_password`)
— Hachage sécurisé via `bcrypt`

I - Vulnérabilités critiques identifiées

A) Failles liées à la gestion des jetons et au hachage des données sensibles

TABLE 4.15 – Présentation des failles liées à la gestion des jetons et au hachage des données sensibles

Élément	Description	Risque
Jetons API stockés en clair	Table `personal_access_tokens`, colonne `token` non hachée	• Élevé
Aucune rotation de mots de passe	Absence de politique d'expiration ou de renouvellement régulier	• Élevé

B) Présence de scripts SQL à haut risque sur le serveur

TABLE 4.16 – Présentation des failles liées aux scripts SQL

Fichier SQL	Détail technique	Impact de la vulnérabilité	Risque
`/chemin/vers/application`	Crée un utilisateur root sans mot de passe	Exploitable localement pour obtenir un accès complet sans authentification	• Critique
Autres scripts MySQL (`install_*.sql`)	Non sensibles	Aucun impact de sécurité détecté	• Faible

C) Absence de journalisation et de mécanismes d'audit

TABLE 4.17 – Présentation des failles liées à la journalisation et aux mécanismes d'audit

Élément	Description	Risque
`general_log` désactivé	Aucune trace des requêtes SQL exécutées	• Moyen
`slow_query_log` désactivé	Pas de détection des requêtes lentes ou inefficaces	• Moyen
`audit_log` absent	Aucun suivi détaillé des accès et des actions	• Moyen
Rotation des logs	Non confirmée par les fichiers de configuration	• Moyen

II- Paramètres critiques de configuration MySQL

TABLE 4.18 – Présentation des failles liées à configuration MySQL

Élément	État actuel	Risque
`skip_symbolic_links`	Valeur non définie (comportement dépendant du système)	• Moyen
`secure_file_priv`	Défini à `/chemin/vers/fichierMysql/` (restreint l'import/export)	• Faible
`local_infile`	Désactivé (bon paramétrage)	• Faible

4.5 Plan de Recommandations Aligné au RNSI 2020

I. Actions Immédiates (Criticité Critique)

1. Sécurisation des accès distants

RNSI : Domaine 3 – Gestion et contrôle des accès (14.3.1, 14.3.2)

— Désactiver l'accès root SSH (`PermitRootLogin no`)
— Imposer l'authentification par clés SSH uniquement
— Déployer `fail2ban` pour limiter les attaques par force brute

2. Nettoyage et durcissement système

RNSI : Domaine 6 – Sécurité des systèmes d'information (14.6.2, 14.7.1)

— Supprimer le fichier critique **/chemin/vers/debianCreateRootUser**
— Restreindre `php-fpm` à `127.0.0.1` ou à un socket Unix

3. Sécurité des services réseau exposés

RNSI : Domaine 5 – Sécurité des réseaux (14.5.1, 14.5.4)

— Mettre à jour le système d'exploitation de l'équipement de sécurité vers une version supportée.
— À défaut, désactiver temporairement l'accès VPN exposé à Internet

II. Actions à Court Terme (Criticité Élevée)

4. Sécurisation de l'application web

RNSI : Domaine 6 – Sécurité des applications (14.6.4, 14.18), Domaine 5 (14.5.4)

— Forcer l'usage de HTTPS par défaut
— Corriger les vulnérabilités de type CSRF et IDOR

5. Protection des données stockées

RNSI : Domaine 10 – Cryptographie (14.10.3, 14.10.6), Domaine 3 (14.3.3)

— Chiffrer les jetons d'authentification/API dans la base de données
— Mettre en œuvre une politique de rotation des mots de passe

6. Réduction de la surface d'attaque réseau

RNSI : Domaine 5 – Réseaux (14.5.1), Domaine 7 – Exploitation (14.7.1)

— Désactiver les services non utilisés (ex. : VoIP, SMTP)
— Restreindre l'accès aux ports sensibles via pare-feu (ACL, `iptables`)

III. Actions à Moyen Terme (Criticité Moyenne)

7. Mise en place de la supervision et détection

RNSI : Domaine 13 – Journalisation (14.13), Domaine 14 – Incidents (14.14)

— Activer les journaux MySQL : `general_log`, `slow_query_log`, `audit_log`

8. Sécurisation approfondie de l'application

RNSI : Domaine 6 – Applications (14.6.4), Domaine 18 – SSDLC

— Appliquer des en-têtes HTTP stricts : `HSTS`, `X-Frame-Options`, etc.
— Mettre en œuvre une **Content Security Policy (CSP)**
— Sécuriser les cookies : `Secure`, `HttpOnly`, `SameSite=Strict`

9. Maintien en condition de sécurité

RNSI : Domaine 7 – Exploitation (14.7.6), Domaine 15 – Continuité (14.15.3)

— Mettre en place un processus de mise à jour régulier (OS et applicatif)
— Déployer une solution de sauvegarde chiffrée, automatisée et testée

IV. Actions de Fond (Criticité Faible à Continue)

10. Sensibilisation et culture sécurité

RNSI : Domaine 16 – Ressources humaines (14.16.4), Domaine 18 – SSDLC

— Former les développeurs aux pratiques OWASP et au codage sécurisé
— Former les administrateurs système à la réponse aux incidents

11. Amélioration continue

RNSI : Domaine 14 – Incidents (14.14.7), Domaine 12 – Revue de sécurité (14.13)

— Réaliser des revues régulières de configuration et d'audit de conformité
— Programmer des tests de pénétration internes et externes périodiques

4.6 Conclusion

L'audit a permis de révéler plusieurs vulnérabilités critiques susceptibles de compromettre la sécurité de l'application, tant au niveau du backend que du frontend. Les constats exposés mettent en évidence des lacunes en matière de configuration, de gestion des accès et de protection des communications. Les recommandations formulées dans ce chapitre constituent une base solide pour corriger les failles identifiées, renforcer la posture de sécurité globale du système et assurer sa conformité aux bonnes pratiques nationales.

Conclusion générale

Dans un contexte où les systèmes d'information constituent la colonne vertébrale des organisations publiques et privées, leur sécurité revêt une importance stratégique. Les cyberattaques, toujours plus fréquentes et sophistiquées, ne se contentent plus de viser des cibles isolées : elles s'inscrivent désormais dans une logique globale de perturbation, de déstabilisation, voire d'espionnage économique ou politique. Face à cela, l'audit de sécurité informatique se positionne comme un outil fondamental de diagnostic, de prévention et de pilotage de la cybersécurité.

Ce mémoire a permis de mettre en lumière les enjeux, méthodes et outils liés à l'audit de sécurité, à travers une approche combinant cadre théorique rigoureux et mise en œuvre concrète. Dans une première phase, nous avons posé les fondements conceptuels de l'audit en nous appuyant sur les normes internationales (*ISO/IEC 27001*) et les référentiels nationaux (*RNSI 2020*), tout en détaillant les typologies d'audits, les méthodes d'évaluation des risques, et les critères d'analyse pertinents. Cette base a permis de structurer une démarche claire, applicable dans des environnements réels.

La deuxième partie du travail a consisté en une étude de cas appliquée au sein du Ministère de l'Industrie, sur une application web sensible. À travers des phases méthodiques — reconnaissance, évaluation des vulnérabilités, tests d'intrusion, interprétation des résultats — nous avons identifié des failles techniques critiques, des erreurs de configuration, ainsi que des insuffisances organisationnelles. Les outils utilisés (*Nmap*, *Burp Suite*, *Metasploit*, etc.) ont permis de mettre en évidence la surface d'attaque effective et les vecteurs d'exploitation potentiels.

L'analyse a également intégré une évaluation rigoureuse de la gravité des vulnérabilités selon le système CVSS v3.1, offrant une priorisation rationnelle des correctifs à appliquer. Cette hiérarchisation constitue un levier clé pour la prise de décision en matière de cybersécurité.

Au-delà des constats techniques, ce travail met en exergue l'importance d'une culture de cybersécurité partagée à tous les niveaux de l'organisation, soutenue par une politique claire de gestion des risques, des audits périodiques, des formations continues, et une documentation à jour. Il apparaît également crucial de dépasser la vision purement technique de l'audit pour l'intégrer à une gouvernance globale de la sécurité des systèmes d'information.

En conclusion, l'audit ne doit pas être perçu comme une action isolée, mais comme un processus continu et dynamique, au service de la résilience organisationnelle. Il ouvre la voie à des améliorations concrètes, à condition d'être suivi d'un plan d'action, d'une évaluation régulière des progrès, et d'une veille technologique constante. Ce mémoire, à la croisée des dimensions techniques, normatives et opérationnelles, illustre l'apport stratégique de l'audit de sécurité pour la pérennité des infrastructures numériques.

Perspectives

Plusieurs pistes d'approfondissement peuvent être envisagées à la suite de ce travail :

— Automatisation des audits à l'aide de solutions d'analyse continue, basées sur l'intelligence artificielle ou l'apprentissage automatique, permettant une détection plus rapide et plus fine des vulnérabilités
— élargir le périmètre d'analyse à d'autres couches critiques du système d'information (postes de travail, cloud) pour une vision plus globale de la sécurité.
— À partir de cette expérience, un livret ou une méthode d'audit simplifiée à destination d'organisations ne disposant pas d'experts internes pourrait être élaboré, en vulgarisant les étapes et les outils essentiels.

Annexe

Annexes du rapport d'audit

Annexe A – Commandes d'audit et outils employés

Reconnaissance système

```
uname -af
lsb_release -a
hostnamectl
```

Analyse du service SSH

```
sudo cat /etc/ssh/sshd_config
grep "Failed password" /var/log/auth.log
grep -Ei "Ciphers|MACs|KexAlgorithms" /etc/ssh/sshd_config
grep -Ei "PermitRootLogin|PasswordAuthentication|UsePAM" /etc/ssh/
   sshd_config
```

Vérification du serveur web

```
server -T
grep -r "autoindex on" /etc/server/
grep -r "server_tokens" /etc/server/
sudo grep -r "server_tokens off" /etc/server/
```

Tests d'application web

```
ffuf -u http://target.com/FUZZ -w ~/wordlists/api_endpoints.txt -mc
    200 -H "X-API-Key: TEST"
gobuster dir -u http://target.com -w /usr/share/wordlists/dirbuster
   /directory-list-2.3-medium.txt -x php,html,txt -t 50
whatweb http://target.com
sudo tcpdump -i any -nn "port 80 or port 443" -w web.pcap
```

Détection des services & analyse réseau

```
sudo ss -tuln
sudo ss -tulnp | grep -Ev '127.0.0.1|::1'
nmap -sV <IP>
nmap -sA website.com -p-
nmap -sS -Pn -n --disable-arp-ping --min-rate 5000 -p- <IP>
sudo nmap -sV -sC -O --script vuln <IP> -p- -T4
sudo nmap -sUV -p- --script vuln <IP>
shodan host <IP>
censys search services.ip:<IP>
```

Analyse VPN / IKE / IPSec

```
ike-scan -A website.com
sudo ike-scan --aggressive -M --id=XXX <IP>
sudo ike-scan --aggressive --multiline --id=XXX <IP>
```

Annexe B – Captures techniques et extraits de preuves

Fuite d'information dans le code HTML

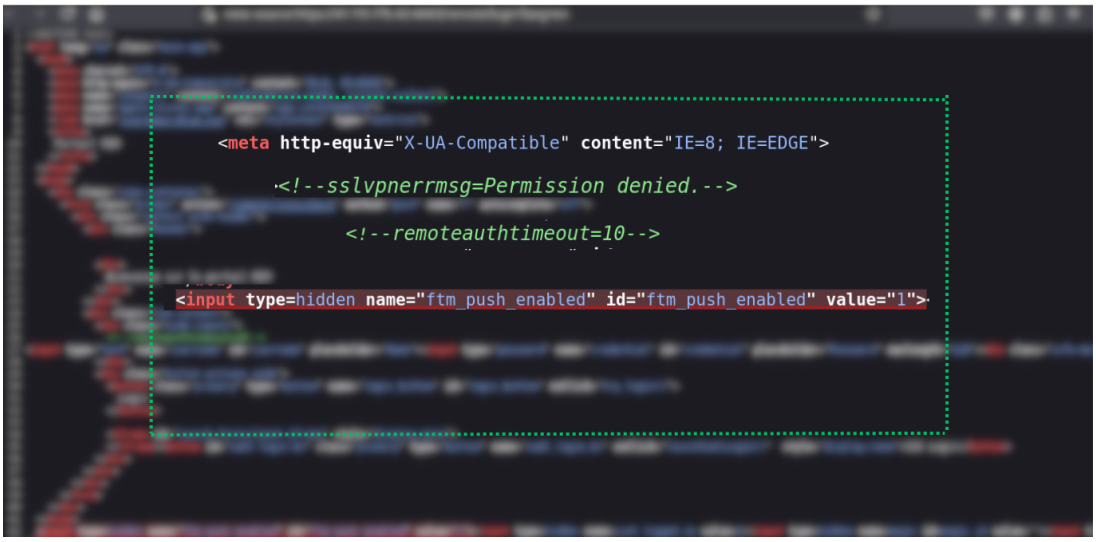

FIGURE 1 – Exemple de code source contenant des informations sensibles

la figure montre un code source HTML accessible publiquement incluant des fonctions internes JavaScript, des champs cachés sensibles et support de navigateur obsolètes, ainsi que des commentaires révélateurs. Ces éléments facilitent la reconnaissance pour un attaquant.

Vulnérabilité Clickjacking

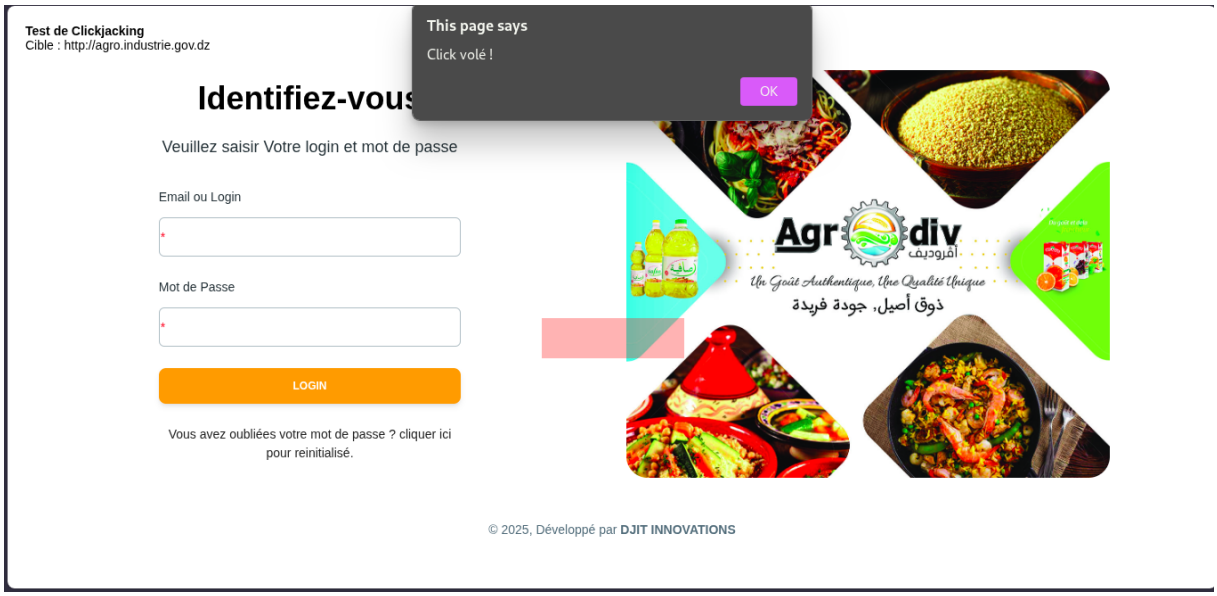

FIGURE 2 – Vulnérabilité clickjacking

Analyse du service IKEv1 sur le Port (UDP/port non standard 5)

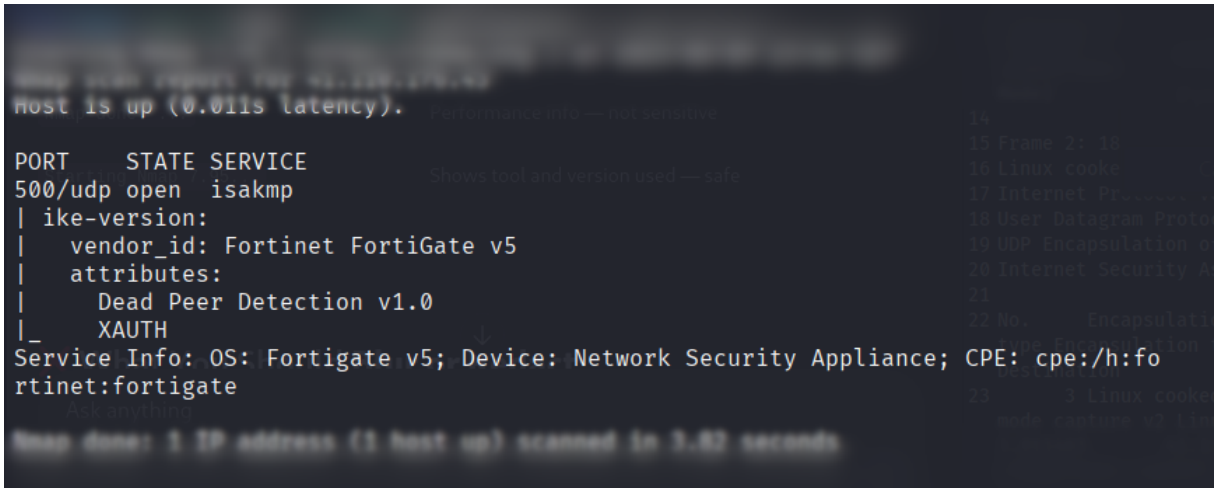

FIGURE 3 – Présence d'un service IKEv1 exposant un équipement de sécurité réseau utilisant une version obsolète de son système.

Le scan révèle que le port UDP port non standard 5 est ouvert et expose un service ISAKMP avec un équipement de sécurité réseau utilisant une version obsolète de son système, utilisant les extensions Dead Peer Detection v1.0 et XAUTH, ce qui pourrait potentiellement indiquer un point d'entrée intéressant pour une attaque ou une vérification de configuration.

Analyse de la configuration IKEv1

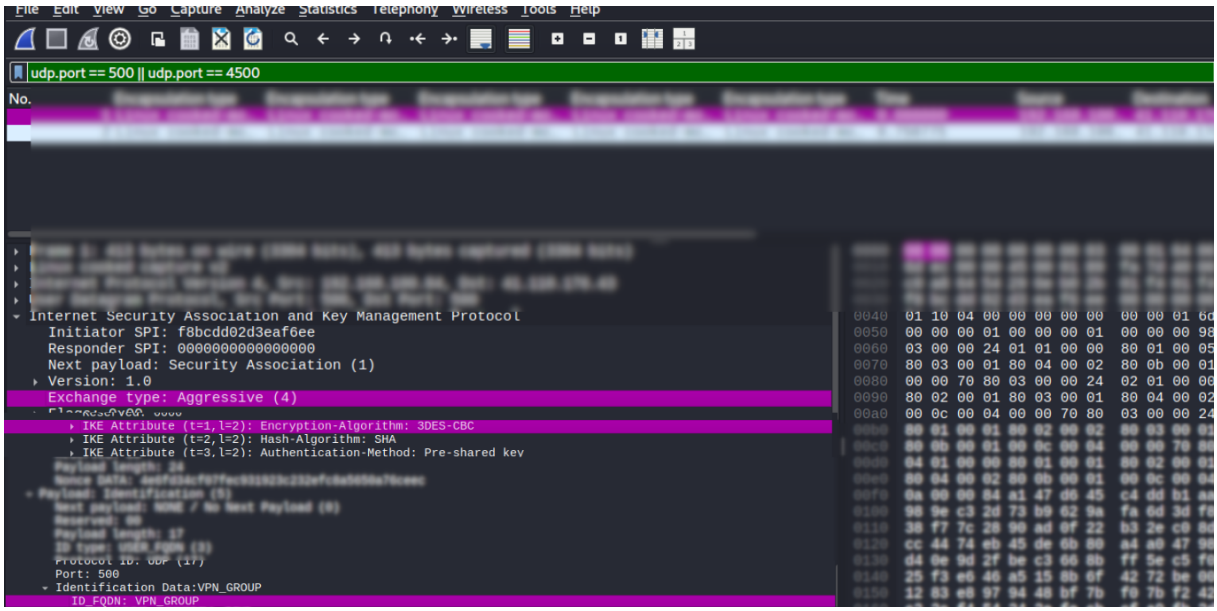

FIGURE 4 – Analyse Wireshark d'un échange IKEv1 en mode agressif

Le port UDP/port non standard 5 répond à une requête IKEv1 en mode Aggressive. L'identifiant utilisé est un FQDN, avec les algorithmes MD5 (hash) et 3DES-CBC (chiffrement). Cette combinaison est faible et vulnérable à des attaques passives et actives connues.

Attaque force brute via SSH

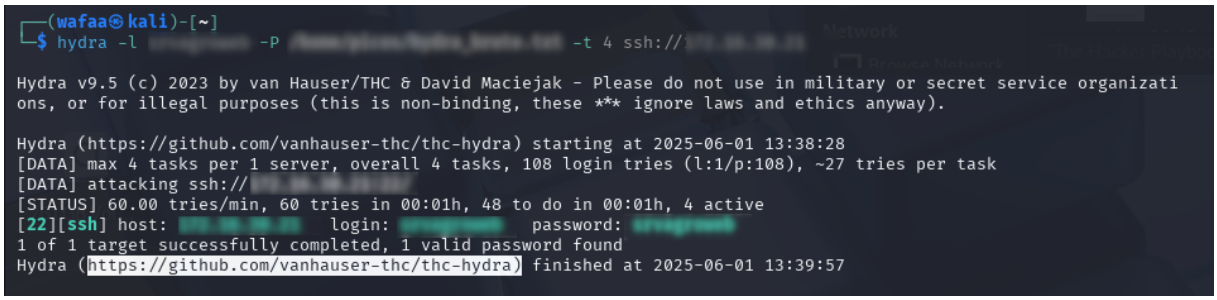

FIGURE 5 – Attaque Force Brute via SSH

Fuite d'information via une erreur de configuration serveur

```
curl -k -X GET -H "Authorization: Bearer invalid.jwt.token" \
     http://xxxx.xxxx.xxxx/api/logout

 <!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\Routing\Exception\RouteNotFoundException: Route [
   login] not defined. in file .
.
.
.
.
.
.
..
```

Bibliographie

[1] Agence nationale de la sécurité des systèmes d'information. Panorama de la cybermenace. Consulté le 9 juin 2025. 2021. URL : https://www.ssi.gouv.fr.

[2] C. Berriz. Cybersecurity and United States Policy Issues. Rapp. tech. 2014.

[3] Stephen Casper. "Black-Box Access is Insufficient for Rigorous AI Audits". In : arXiv preprint arXiv :2307.XXXX (2023). URL : https://arxiv.org/abs/2307.XXXX.

[4] S. Ebiesuwa et al. "Impact of Information Systems on Operational Efficiency : A Comprehensive Analysis". In : Indian Journal of Computer Science and Engineering 14.4 (2023), p. 661-673. DOI : 10.21817/indjcse/2023/v14i4/231404013.

[5] FIRST. Common Vulnerability Scoring System v3.1 : Specification Document. Consulté en juillet 2025. 2019. URL : https://www.first.org/cvss/specification-document (visité le 08/07/2025).

[6] A. Folorunso et al. "L'impact des normes de sécurité ISO sur l'amélioration de la cybersécurité des organisations". In : World Journal Of Advanced Research and Reviews 24.1 (2024), p. 2582-2595. DOI : 10.30574/wjarr.2024.24.1.3169.

[7] OWASP Foundation. Access Control Cheat Sheet. 2021. URL : https://cheatsheetseries.owasp.org/cheatsheets/Access_Control_Cheat_Sheet.html.

[8] OWASP Foundation. Cryptographic Storage Cheat Sheet. Accessed : 2025-06-10. 2021. URL : https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html.

[9] OWASP Foundation. Input Validation Cheat Sheet. 2021. URL : https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html.

[10] OWASP Foundation. Logging Cheat Sheet. 2021. URL : https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html.

[11] OWASP Foundation. Password Storage Cheat Sheet. 2021. URL : https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html.

[12] OWASP Foundation. Security Testing Cheat Sheet. 2021. URL : https://cheatsheetseries.owasp.org/cheatsheets/Security_Testing_Cheat_Sheet.html.

[13] Gouvernement Algérien. Décret exécutif n° 16-61 du 2 Joumada El Oula 1437 (11 février 2016). Modification du décret n° 09-410 du 10 décembre 2009. 2016.

[14] Gouvernement Algérien. Décret présidentiel n° 20-05 du 24 Joumada El Oula 1441 (20 janvier 2020). Dispositif national de sécurité du système d'information (DNSSI). 2020.

[15] Gouvernement Algérien.
Loi n° 09-04 du 5 août 2009 sur la cybersécurité et la lutte contre la cybercriminalité.
Texte officiel. 2009.

[16] Gouvernement Algérien.
Loi n° 18-04 du 24 Chaâbane 1439 (10 mai 2018) relative à la poste et communications électroniques.
Texte officiel. 2018.

[17] Gouvernement Algérien.
Loi n° 18-07 du 25 Ramadhan 1439 (10 juin 2018) relative à la protection des données personnelles.
Texte officiel. 2018.

[18] Guide d'audit des systèmes d'information : Audit de sécurité et contrôle interne. Extrait des sections V.A, VI et Annexes. Club informatique des grandes entreprises françaises (CIGREF), 2016.

[19] A. Kumar. "Cyber Security Issues and Challenges – A Review". In : IJSRCSEIT 8.3 (2022), p. 269-273. doi : 10.32628/CSEIT228379.

[20] C. Lozano-Lévano, B. Castillo-Santamaria et L. Chávez Ordinola.
"Information Management in Public Administration : A Systematic Review from a Technological Perspective". In : Nanotechnology Perceptions (2024). doi :
10.62441/nano-ntp.vi.1009.

[21] Ministère de la Poste, des Télécommunications, des Technologies et du Numérique (MPTTN), Algérie.
Référentiel National de Sécurité de l'Information (RNSI). Document officiel. 2020. url :
https://www.mpt.gov.dz/wp-content/uploads/2023/12/Referentiel-National-de-la-Securite-de-lInformation-2020-VERSION-FINALE-1-1.pdf.

[22] National Institute of Standards and Technology (NIST).
Technical Guide to Information Security Testing and Assessment. Rapp. tech. Special Publication 800-115. NIST, 2008. url :
https://csrc.nist.gov/publications/detail/sp/800-115/final.

[23] S. J. Nisrina et al. "The Role of Information Systems in Improving the Efficiency of Business Decision Making". In : Jurnal Bisnis Dan Komunikasi Digital 2.2 (2024), p. 10. doi : 10.47134/jbkd.v2i2.3470.

[24] S. R. Nistane et R. R. Sharma. "Cyber Security : Strategy to Security Challenges A Review". In : International Journal of Scientific Research in Science and Technology (2022), p. 316-319. doi : 10.32628/ijsrst229170.

[25] K. K. Olanrewaju. "Business Data Breaches—Impact on Brand Reputation and Employee Integrity : A Case Study of Desjardins in Canada". In :
Texila International Journal of Academic Research 12.2 (2025), p. 1-15. url :
https://www.texilajournal.com/thumbs/article/8_TJ3360.pdf.

[26] OWASP Foundation.
OWASP Top 10 – 2021 : The Ten Most Critical Web Application Security Risks.
https://owasp.org/Top10. 2021.

[27] OWASP Foundation. Session Management Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html. 2021.

[28] C. Radha et al. "Challenges and issues in cyber security". In :
International Journal for Research Trends and Innovation 8.12 (2023), p. 129-135. url :
https://www.ijrti.org.

[29] William Stallings. Cryptography and Network Security : Principles and Practice. 7e éd. Boston : Pearson Education, 2018.

[30] National Institute of Standards et Technology. Digital Identity Guidelines. Rapp. tech. SP 800-63-3. NIST, 2017. URL : https://pages.nist.gov/800-63-3/.

[31] R. Thakur et N. Manoj. "Cyber Security". In : International Journal of Science and Research 13.1 (2024), p. 440-444. DOI : 10.21275/mr231228122722. URL : https://doi.org/10.21275/mr231228122722.