ECOLE MAROCAINE DES SCIENCES DE L'INGENIEUR
Membre de HONORIS UNITED UNIVERSITIES

EMSI

Ecole Reconnue par l'Etat

RAPPORT DE PROJET

SCAM WARNING

Conception et développement d'une application mobile collaborative de signalement d'arnaques au Maroc

Rédigé par :

SIHADI Aya
JOUICHAT Khadija
RADOUANI Mohammed Reda
NORRI Yahya

Encadré par :

Mme. RACHIK Zineb

Filière :
Ingénierie Informatique et Réseaux

Année scolaire :
2025-2026

Jancier 2026

Remerciements

La finalisation du projet "Scam Warning", fruit d'une intense collaboration, n'aurait pu aboutir sans le soutien de précieux acteurs.

Nous exprimons notre profonde gratitude envers Madame RACHIK Zineb, notre encadrante, dont la guidance experte et la disponibilité ont structuré notre travail.

En tant qu'équipe, SIHADI Aya, RADOUANI Mohammed Reda, JOUICHAT Khadija et NORRI Yahya, nous soulignons notre synergie et notre engagement mutuel, piliers de cette réalisation.

Enfin, notre gratitude s'adresse à l'EMSI pour le cadre académique stimulant et les ressources mises à disposition.

Résumé

Ce projet, intitulé "Scam Warning", consiste en la conception et le développement d'une application mobile collaborative destinée à la prévention des arnaques au Maroc. L'objectif principal est de fournir une plateforme accessible où les citoyens peuvent signaler des tentatives de fraude, consulter les alertes publiées par d'autres utilisateurs et ainsi s'informer pour mieux se protéger. L'application cible un large public, des jeunes aux personnes âgées, souvent vulnérables à ces pratiques malveillantes. Développée avec les technologies React Native et Expo pour le frontend mobile, et une API .NET 9 pour le backend, la solution intègre des fonctionnalités telles que la création de signalements classés par catégorie, un système de commentaires, et un panel d'administration pour la modération du contenu. Ce rapport détaille la démarche complète du projet, depuis l'analyse du besoin et la conception, jusqu'à la réalisation technique et les perspectives d'évolution, en mettant l'accent sur la valeur ajoutée sociale d'un tel outil de vigilance collective.

Abstract

This project, titled "Scam Warning" involves the design and development of a collaborative mobile application aimed at preventing scams in Morocco. The main objective is to provide an accessible platform where citizens can report fraud attempts, consult alerts published by other users, and thus stay informed to better protect themselves. The application targets a wide audience, from young people to the elderly, who are often vulnerable to these malicious practices. Developed with React Native and Expo technologies for the mobile frontend, and a .NET 9 API for the backend, the solution integrates features such as creating reports categorized by scam type, a comment system, and an administration panel for content moderation. This report details the complete project process, from needs analysis and design to technical implementation and prospects, emphasizing the social added value of such a collective vigilance tool.

Table des matières

Table des figures

Liste des tableaux

Chapitre 1

Introduction Générale

Le paysage numérique marocain connaît une expansion rapide, avec une adoption croissante des services bancaires en ligne, du e-commerce et des réseaux sociaux. Cette transformation, bien que bénéfique, s'accompagne d'une recrudescence des activités frauduleuses. Les arnaques sous toutes leurs formes – phishing, appels téléphoniques usurpant l'identité d'opérateurs ou d'institutions, fausses offres d'investissement, chantages sentimentaux – ciblent une population parfois peu informée des mécanismes de protection numérique. Les victimes, souvent désemparées, subissent non seulement des pertes financières mais également une détresse psychologique.

Face à cette réalité, il devient crucial de développer des mécanismes de défense collective. L'information et la prévention sont les premières armes contre la cybercriminalité. C'est dans ce contexte que s'inscrit notre projet « Scam Warning ». L'idée centrale est de créer un réseau de vigilance citoyenne, matérialisé par une application mobile. Cette dernière a pour vocation de rompre l'isolement des victimes potentielles en permettant le partage rapide d'alertes sur des tentatives d'arnaque.

Notre travail, réalisé dans le cadre du Projet de Fin d'Année, s'est articulé autour de la conception et du développement d'un prototype fonctionnel de cette application. Nous avons opté pour une approche centrée sur l'utilisateur, en privilégiant la simplicité d'utilisation pour toucher le plus large public possible. Le développement technique a été mené en suivant une méthodologie itérative, avec une phase d'analyse poussée, une modélisation rigoureuse du système, et une implémentation utilisant des technologies modernes et adaptées aux contraintes d'un projet académique.

Ce rapport retrace l'intégralité de ce parcours. Il est structuré en quatre chapitres :

Chapitre 1 : Présentation de l'école et du contexte

Ce chapitre présente l'EMSI et le contexte des arnaques au Maroc, ainsi qu'il définit la problématique, les objectifs et le cahier des charges du projet "Scam Warning".

Chapitre 2 : Présentation du projet

Ce chapitre est consacré à la présentation générale du projet, en exposant son contexte, ses objectifs, ainsi que les principales fonctionnalités attendues de la plateforme.

Chapitre 3 : Analyse et conception

Ce chapitre détaille l'analyse des besoins, les choix techniques et la conception du système (diagrammes UML).

Chapitre 4 : Réalisation et développement

Ce chapitre décrit la mise en œuvre du projet, les outils utilisés, les étapes de réalisation et les technologies adoptés.

Chapitre 2

Présentation de l'école et du contexte

2.1 Introduction à l'école

2.1.1 Présentation de l'École et de son Environnement

FIGURE 2.1 – Un des sites de l'EMSI

L'EMSI (École Marocaine des Sciences de l'Ingénieur) se distingue comme l'une des institutions privées pionnières et de référence dans l'enseignement supérieur d'ingénierie au Maroc. Fondée sur une vision d'excellence et d'innovation, l'école s'efforce d'offrir un environnement d'apprentissage stimulant et complet, propice

au développement académique et personnel de ses étudiants. Ses campus modernes, stratégiquement implantés dans les grandes villes dynamiques du Maroc telles que Casablanca, Rabat, Marrakech et Tanger, sont dotés d'infrastructures de pointe : laboratoires spécialisés, salles informatiques équipées, bibliothèques fournies et espaces de vie étudiante. Cet écosystème favorise non seulement l'acquisition de compétences techniques de haut niveau, mais aussi l'épanouissement des étudiants dans un cadre qui reflète le dynamisme du monde professionnel et encourage l'interaction et la collaboration.

2.1.2 Historique de l'EMSI

Fondée en 1986, l'École Marocaine des Sciences de l'Ingénieur (EMSI) s'est imposée comme l'un des établissements privés d'enseignement supérieur les plus reconnus au Maroc dans le domaine de l'ingénierie. Depuis sa création, l'EMSI a pour mission de former des ingénieurs compétents, innovants et adaptés aux besoins du marché national et international. L'école a su évoluer au fil des années en diversifiant ses filières, en renforçant ses partenariats avec le monde industriel et en s'investissant activement dans la recherche appliquée et l'innovation technologique.

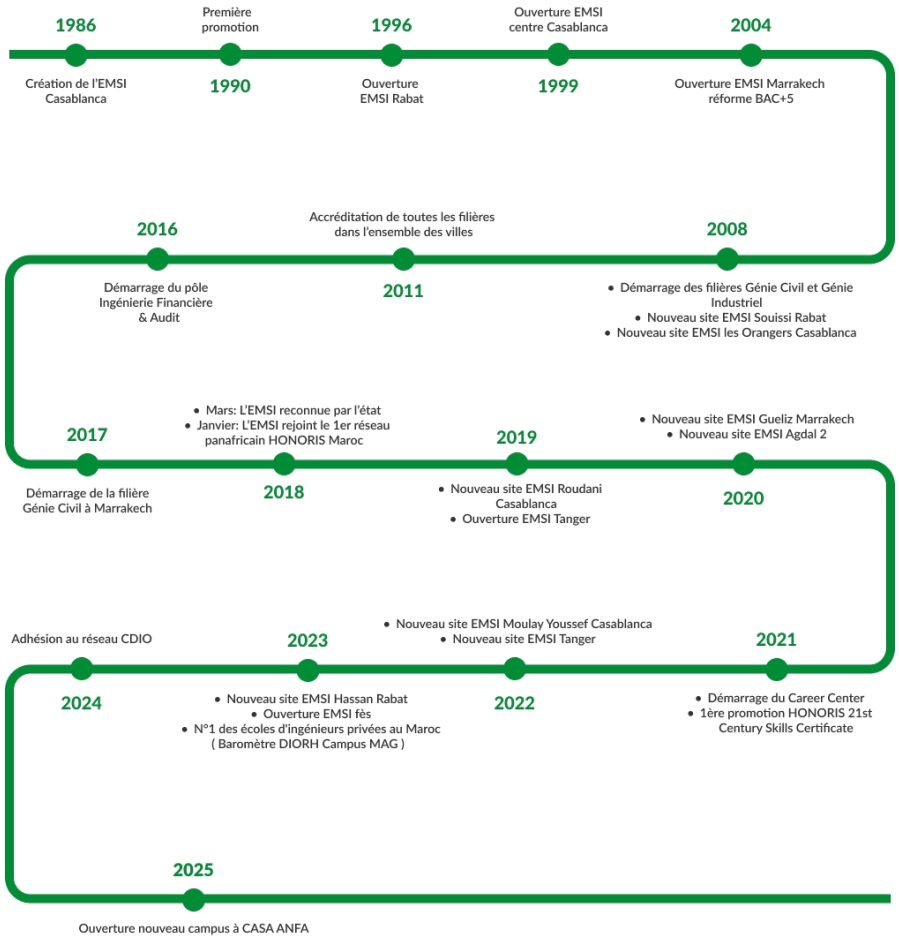


FIGURE 2.2 – Historique de l'EMSI

2.1.3 Missions et Secteurs d'Activité de l'EMSI

La mission principale de l'EMSI est de former des ingénieurs hautement qualifiés, polyvalents et dotés d'une forte capacité d'adaptation aux défis du monde moderne. L'école s'attache à développer chez ses étudiants non seulement des compétences techniques pointues, mais aussi des aptitudes managériales, entrepreneuriales et humaines essentielles à leur réussite professionnelle et personnelle.

Chapitre 3

Présentation du projet

3.1 Introduction

La lutte contre les arnaques numériques et téléphoniques ne peut être uniquement l'affaire des autorités. Elle nécessite l'implication et la collaboration des citoyens eux-mêmes. Notre projet "Scam Warning" propose une réponse concrète à ce défi en créant un canal numérique direct et participatif. Il s'agit de transformer chaque utilisateur en un acteur de sa propre sécurité et de celle de sa communauté.

3.2 Problématique

Les Marocains sont quotidiennement exposés à des tentatives d'arnaque sophistiquées. Les méthodes évoluent constamment, rendant la méfiance traditionnelle parfois insuffisante. Les principales difficultés identifiées sont :

- La décentralisation de l'information : Les alertes circulent de manière fragmentée sur les réseaux sociaux ou par bouche-à-oreille, sans vérification ni organisation.
- L'isolement des victimes : Une personne touchée peut hésiter à en parler, par honte ou par méconnaissance des recours, ce qui empêche les autres d'être prévenues.
- Le manque de contextualisation : Les applications internationales de signalement existent, mais elles ne couvrent pas spécifiquement les méthodes, les numéros ou les institutions ciblées au Maroc.

La question centrale qui a guidé notre travail est donc la suivante : Comment concevoir une application mobile simple, efficace et spécifiquement adaptée

au contexte marocain, qui permette de centraliser, de vérifier et de diffuser largement les informations sur les arnaques, afin de créer une barrière de protection collective ?

3.3 Motivation du projet

Notre motivation découle directement de la problématique. Nous avons constaté autour de nous, dans nos familles et nos cercles d'amis, que personne n'était à l'abri. L'idée de développer un outil utile, qui pourrait concrètement aider à prévenir des pertes d'argent et des traumatismes, a été un moteur fort. Sur le plan académique, ce projet représentait également une excellente opportunité de mettre en pratique nos compétences en développement full-stack, en gestion de projet et en conception d'interfaces utilisateur, sur un sujet à fort impact social.

3.4 Objectifs et engagements du projet

L'objectif principal était de livrer un prototype fonctionnel et testable d'une application mobile collaborative de signalement d'arnaques. Cet objectif se déclinait en plusieurs engagements :

- Concevoir une interface intuitive : Accessible aux personnes de tous âges et niveaux de technicité.
- Développer un système de publication modéré : Permettre à tout utilisateur inscrit de soumettre une alerte, avec contrôle a posteriori par un administrateur.
- Implémenter les rôles utilisateurs : Différencier les fonctionnalités d'un utilisateur lambda de celles d'un administrateur.
- Structurer l'information : Classer les signalements par catégories prédéfinies.
- Assurer une communication efficace : Développer une API RESTful robuste.
- Respecter les contraintes du projet académique : Utiliser des technologies gratuites et documenter intégralement le processus.

3.5 Solution proposée

Notre solution est une application mobile hybride, disponible à terme sur Android et iOS, structurée autour de plusieurs modules clés :

- Module d'authentification : Inscription et connexion simplifiées par email et mot de passe.

- Module de consultation : Page d'accueil présentant les alertes récentes validées.
- Module de signalement : Formulaire guidé pour décrire l'arnaque.
- Module de discussion : Espace de commentaires sous chaque alerte.
- Module d'administration : Écran sécurisé pour la modération du contenu.

3.6 Analyse de l'existant

Avant de nous lancer dans le développement, nous avons examiné les solutions similaires disponibles. Nous avons constaté que plusieurs applications internationales de signalement de spam ou d'arnaque existent (comme « Truecaller » pour les appels, ou des modules intégrés à certains antivirus). Cependant, elles présentent des limites pour notre contexte :

- Manque de focalisation locale
- Modération peu adaptée
- Complexité ou coût
- Absence de dimension communautaire explicite

3.7 Planification du projet

3.7.1 Diagramme de Gantt

Le diagramme de Gantt visualise ces différentes tâches sur une période de trois mois. Chaque barre horizontale représente une tâche, sa longueur indiquant sa durée et sa position sur l'axe horizontal, ses dates de début et de fin. Il permet de suivre l'avancement du projet et d'identifier les dépendances entre les tâches.

Ce projet vise à développer une application mobile sécurisée et conviviale pour une meilleure prévention des arnaques, en tirant parti des technologies modernes pour offrir une solution efficace et innovante.

3.7.2 Phases du projet et technologies utilisées

Le projet se déroule en plusieurs phases clés, chacune avec des objectifs spécifiques :

- **Analyse des besoins et rédaction du cahier des charges** : Cette phase initiale est cruciale pour comprendre les attentes des utilisateurs et définir les fonctionnalités de l'application.

- **Conception de l'architecture logicielle et de la base de données** : Il s'agit de structurer l'application, de choisir les technologies et de modéliser la base de données.
- **Développement du backend (API, logique métier)** : Cette étape concerne la création des fonctionnalités côté serveur avec .NET 9.
- **Développement du frontend (interface utilisateur)** : Construction de l'interface mobile avec React Native et Expo.
- **Intégration backend/frontend** : Assure la communication fluide entre le serveur et l'interface utilisateur.
- **Tests fonctionnels et corrections** : Tests rigoureux pour identifier et corriger les bugs.
- **Déploiement et documentation** : Mise en ligne de l'application et rédaction de la documentation.

3.8 Conclusion

L'amélioration de la prévention des arnaques au Maroc est un enjeu majeur de sécurité numérique. Grâce à une solution numérique innovante et adaptée aux besoins des citoyens, ce projet ambitionne d'optimiser la vigilance collective, de réduire les victimes d'arnaques et d'améliorer la sécurité numérique des citoyens. L'intégration d'une approche communautaire et la centralisation des alertes permettent une gestion plus efficace et proactive, contribuant ainsi à une société mieux protégée contre les fraudes.

Chapitre 4

Analyse et conception

4.1 Introduction

La phase d'analyse et de conception est cruciale pour transformer une idée en un projet structuré et réalisable. Elle permet de formaliser les besoins, d'identifier les acteurs, de définir les règles de gestion et de créer des modèles qui serviront de blueprint au développement. Pour « Scam Warning », nous avons combiné des méthodes formelles (spécification des besoins, modélisation UML pour la dynamique du système) et conceptuelles (modèle entité-association pour les données).

4.2 Analyse et Spécification du Projet

4.2.1 Identification des besoins fonctionnels et non fonctionnels

Exigences fonctionnelles

Ce sont les services que l'application doit fournir à ses utilisateurs. Nous les avons classifiés et priorisés.

mainblue!20 **ID**	**Besoins fonctionnels**	**Priorité**
F1	Authentification - Permettre la création de compte et la connexion	Élevée
F2	Consultation alertes - Afficher une liste et le détail des alertes publiques	Élevée
F3	Création alerte - Formulaire pour soumettre un nouveau signalement	Élevée
F4	Commentaires - Ajouter un commentaire à une alerte	Moyenne
F5	Modération (Admin) - Valider, modifier, supprimer alertes et commentaires	Élevée
F6	Navigation par catégorie - Filtrer la liste des alertes	Moyenne

TABLE 4.1 – Besoins fonctionnels principaux

Exigences non fonctionnelles

Ces exigences définissent la « qualité » du système, ses performances et ses contraintes d'exploitation.

accentred!20 **ID**	**Exigences non fonctionnelles**
NF1	Performance - Temps de réponse API $<$ 500ms pour les requêtes principales
NF2	Utilisabilité - Test utilisateur positif avec 5 personnes novices
NF3	Sécurité - Mot de passe hashé dans la base. Accès admin par flag
NF4	Compatibilité - L'application s'exécute sans crash sur Expo Go
NF5	Disponibilité - L'API est accessible en local pendant les phases de dev/test

TABLE 4.2 – Besoins non fonctionnels principaux

4.3 Contraintes

4.3.1 Contraintes Techniques et Stratégiques du Projet

Le développement s'est fait dans le cadre précis d'un projet académique, ce qui a imposé plusieurs contraintes :

- **Contrainte budgétaire** : Aucun budget n'était alloué. Tous les outils et services utilisés devaient être gratuits.
- **Contrainte temporelle** : Le projet devait être mené à bien en un semestre.
- **Contrainte technique (base de données)** : Choix de SQLite pour simplifier le déploiement et les tests.
- **Contrainte de sécurité (niveau démo)** : Authentification par session simple pour les besoins de la démonstration.
- **Contrainte d'hébergement** : L'API backend exécutée en local lors du développement.

4.4 Choix techniques

Les technologies ont été sélectionnées pour leur adéquation avec les contraintes, leur modernité et leur courbe d'apprentissage compatible avec le calendrier.

mainblue!20 **Couche**	**Technologie**	**Justification**
Frontend	React Native avec Expo	Cross-platform, hot reload, test via Expo Go
Backend	.NET 9 (Web API)	Performance, Entity Framework, Swagger
Base de données	SQLite	Légère, sans serveur, parfaite pour prototype
Communication	Axios	Simple, gère bien les promesses
Navigation	React Navigation	Standard, expérience native fluide
Stockage local	AsyncStorage	Stockage clé-valeur asynchrone

TABLE 4.3 – Choix techniques du projet

4.5 Modélisation

4.5.1 Modélisation UML

Dans le cadre de la modélisation du système « Scam Warning », plusieurs types de diagrammes UML (Unified Modeling Language) sont utilisés afin de représenter de manière structurée les différentes facettes du système.

Diagramme de cas d'utilisation

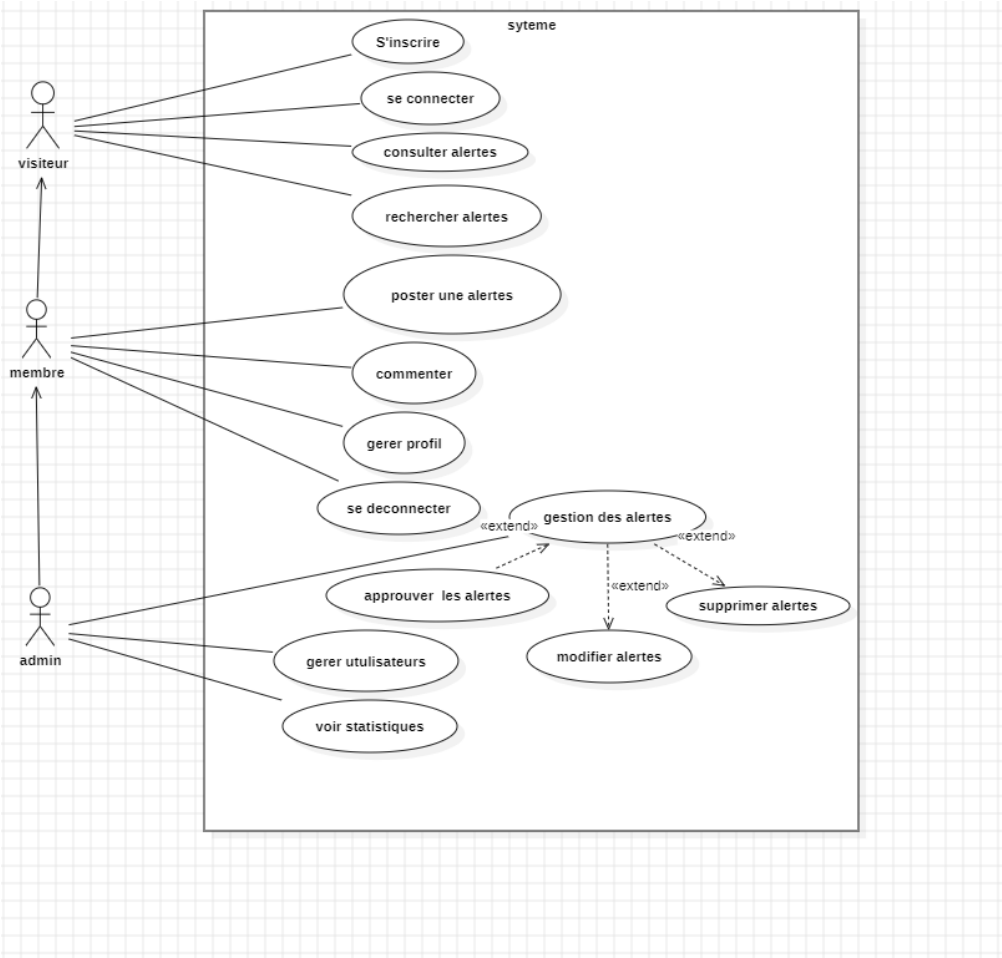


FIGURE 4.1 – Diagramme de cas d'utilisation

Ce diagramme de cas d'utilisation UML illustre les interactions possibles entre les acteurs du système et les fonctionnalités offertes par l'application. Il met en évidence les différents rôles impliqués (Utilisateur, Administrateur) et leurs actions sur le système via des cas d'utilisation.

Acteurs :

- **Utilisateur** : Représente tout type d'utilisateur standard
- **Administrateur** : Gère la modération du contenu

Cas d'utilisation clés :

- Se connecter / S'inscrire

- Consulter les alertes
- Créer une alerte
- Commenter une alerte
- Modérer le contenu (Admin)
- Gérer les catégories (Admin)

Diagramme de séquence

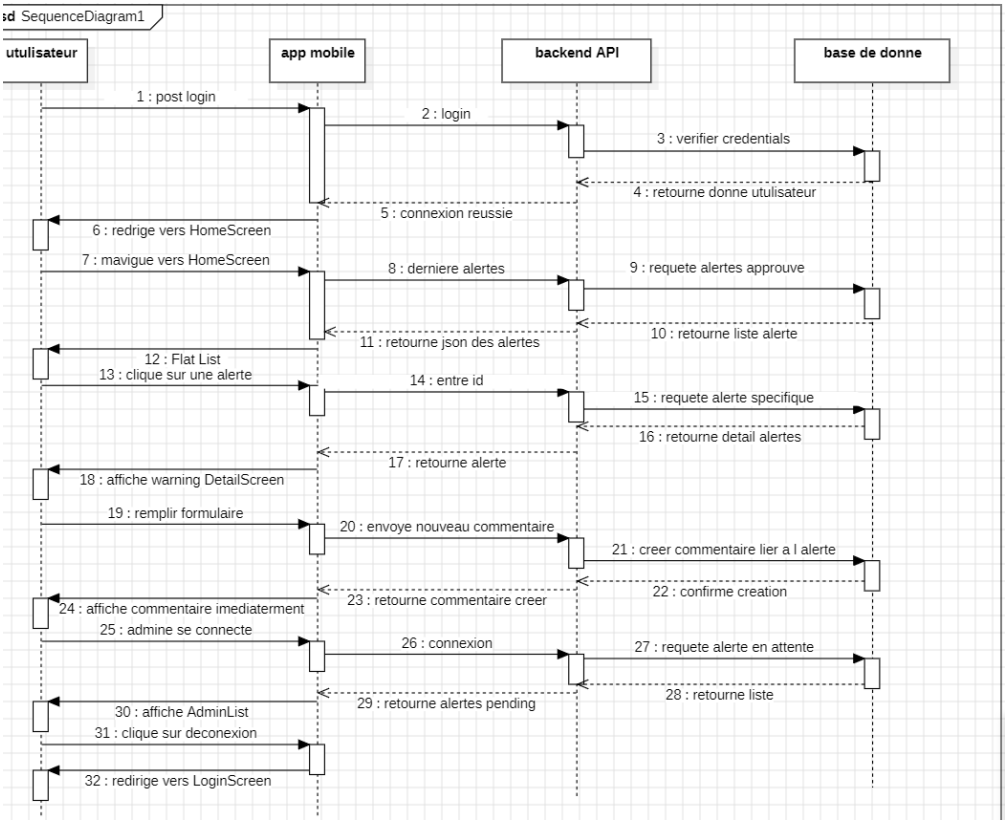


FIGURE 4.2 – Diagramme de séquence de création d'alerte

Le diagramme de séquence illustre les interactions dynamiques entre les différents acteurs du système (Utilisateur, Administrateur) et les composants fonctionnels du système logiciel. Il modélise de façon linéaire et chronologique la suite d'actions et de messages échangés pour réaliser des cas d'utilisation essentiels.

Scénarios couverts :

1. Connexion au système

2. Consultation des alertes
3. Création d'une nouvelle alerte
4. Modération d'alerte par l'administrateur
5. Ajout de commentaires

Diagramme de classes

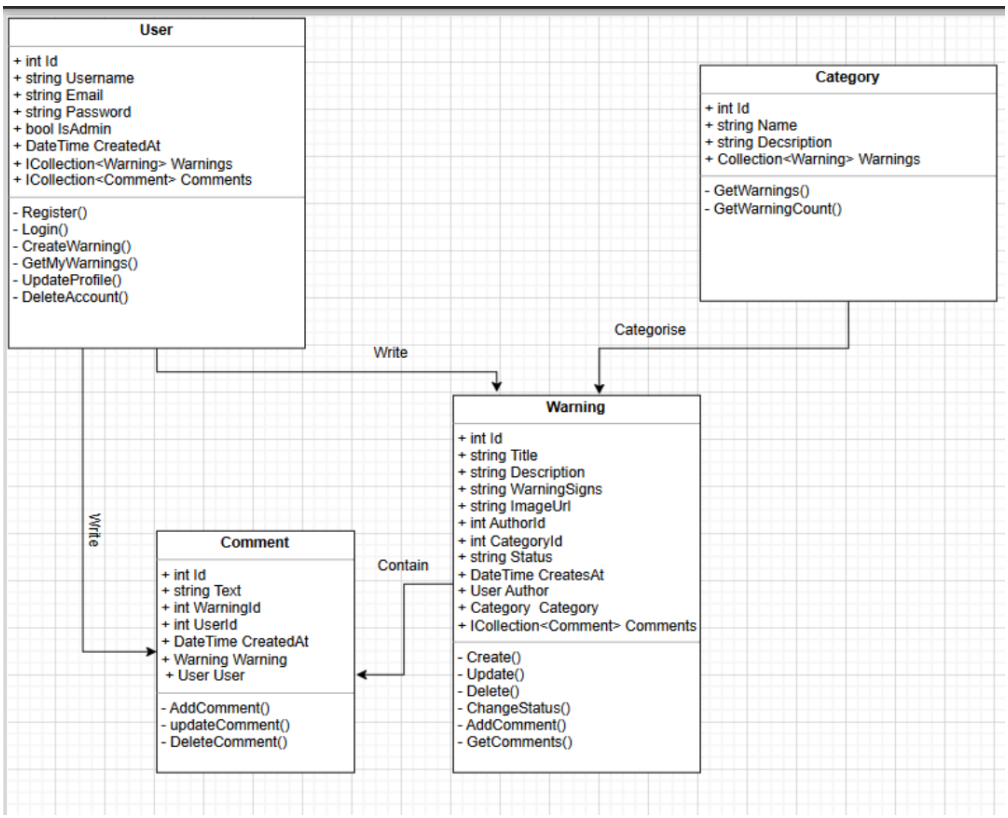


FIGURE 4.3 – Diagramme de classes

Le diagramme de classes représente les principales entités et leurs relations dans le système « Scam Warning ».

Classes principales :

- **Utilisateur** : Classe abstraite avec attributs communs
- **UtilisateurStandard** : Hérite d'Utilisateur, peut créer des alertes et commentaires
- **Administrateur** : Hérite d'Utilisateur, peut modérer le contenu

- **Alerte** : Représente un signalement d'arnaque
- **Commentaire** : Commentaire associé à une alerte
- **Catégorie** : Catégorie d'arnaque (Phishing, Téléphonique, etc.)

4.5.2 Modélisation conceptuelle

Diagramme d'entité/associations

Le Modèle Conceptuel de Données (MCD) constitue une étape cruciale dans la phase de conception du système « Scam Warning ». Il permet de représenter de manière abstraite et rigoureuse l'ensemble des données manipulées par le système.

mainblue!20 **Entité**	**Attributs principaux**
Utilisateur	id, nom, email, mot_de_passe, rôle, date_inscription
Alerte	id, titre, description, catégorie, date, statut, utilisateur_id
Commentaire	id, contenu, date, alerte_id, utilisateur_id
Catégorie	id, nom, description
Notification	id, message, date_envoi, utilisateur_id

TABLE 4.4 – Les entités principales

Associations clés :

- Un Utilisateur peut créer plusieurs Alertes
- Une Alerte appartient à une Catégorie
- Une Alerte peut avoir plusieurs Commentaires
- Un Commentaire appartient à un Utilisateur et une Alerte
- Un Utilisateur peut recevoir plusieurs Notifications

4.6 Conclusion

Ce chapitre a présenté une analyse approfondie et une conception détaillée du système « Scam Warning ». À travers l'élaboration des diagrammes UML et du modèle conceptuel, nous avons pu identifier et définir les principales entités, leurs attributs et leurs relations. Cela a permis de clarifier les rôles et les responsabilités de chaque acteur au sein du système. En conclusion, cette phase d'analyse et de conception a jeté les bases d'un développement réussi de l'application, en assurant que toutes les parties prenantes sont prises en compte et que les processus sont optimisés pour offrir une expérience utilisateur fluide et efficace.

Chapitre 5

Réalisation et développement

5.1 Introduction

Dans cette partie, nous abordons les différentes étapes techniques qui ont permis de concrétiser le projet, depuis la mise en place de l'environnement de développement jusqu'à l'implémentation des fonctionnalités principales. Nous présentons l'architecture choisie, les technologies utilisées, ainsi que la structure générale du système. Chaque module du projet est détaillé, en mettant en évidence les choix de conception, les modèles de données, les interfaces et les interactions entre les composants.

5.2 Technologies et environnement de développement

La réussite de notre projet « Scam Warning » repose sur une sélection rigoureuse de technologies modernes et éprouvées, garantissant robustesse, sécurité, évolutivité et une expérience utilisateur optimale.

5.2.1 Technologies Utilisées : Un Aperçu Technique du Projet

Frontend : L'Interface Utilisateur (React Native, Expo, JavaScript)

La partie visible de notre application, celle avec laquelle les utilisateurs interagiront directement, est construite avec des technologies mobile modernes.

React Native : Framework JavaScript pour développer des applications mobiles natives pour iOS et Android avec un seul codebase.

Expo : Ensemble d'outils et de services construits autour de React Native qui facilitent le développement, la construction, le déploiement et l'itération rapide.

JavaScript/TypeScript : Langage de programmation principal pour le développement du frontend.

React Navigation : Bibliothèque de routage et de navigation pour React Native.

Backend : Le Cœur Intelligent de l'Application (.NET 9, C#)

Le backend est la partie non visible de l'application, responsable de la logique métier, de la gestion des données et de la communication avec la base de données.

.NET 9 : Plateforme de développement moderne et performante pour la création d'API web.

C# : Langage de programmation orienté objet, robuste et sécurisé.

Entity Framework Core : ORM (Object-Relational Mapper) pour .NET qui simplifie l'accès aux données.

Swagger/OpenAPI : Outil pour la documentation et la testabilité des API.

Base de Données : Le Stockage des Données (SQLite)

La gestion des données est fondamentale pour une application de signalement.

SQLite : Base de données relationnelle légère, sans serveur, parfaite pour le développement mobile et les prototypes.

5.2.2 Outils, Langages et Bibliothèques Utilisés dans le Projet

mainblue!20 **Catégorie**	**Outils / Technologies**	**Description**
Langages	C#	Langage principal pour le backend .NET
	JavaScript/TypeScript	Langage principal pour le frontend React Native
	SQL	Pour les requêtes de base de données
Framework	.NET 9	Framework backend pour l'API
	React Native	Framework frontend pour applications mobiles
	Entity Framework Core	ORM pour .NET
Outils	Visual Studio / VS Code	Environnements de développement
	SQLite	Base de données pour développement
	Git / GitHub	Contrôle de version et collaboration
	Postman	Test des API
	Expo Go	Test de l'application sur mobile
Bibliothèques	Axios	Client HTTP pour les requêtes API
	AsyncStorage	Stockage local sur device
	React Navigation	Navigation entre écrans

TABLE 5.1 – Outils et technologies utilisés

5.3 Architecture logicielle du système

L'architecture logicielle du système « Scam Warning » suit une approche client-serveur moderne :

Composants principaux :

1. **Client Mobile (React Native)** : Interface utilisateur exécutée sur les appareils mobiles

2. **API REST (.NET 9)** : Serveur backend exposant des endpoints pour les opérations CRUD
3. **Base de Données (SQLite)** : Stockage persistant des données
4. **Services d'Authentification** : Gestion des utilisateurs et des sessions
5. **Services de Notification** : Envoi de notifications push (perspective)

5.4 Étapes de Réalisation du Projet

La réalisation du projet « Scam Warning » s'est déroulée en plusieurs étapes clés :

1. **Phase 1 : Analyse et Conception** (2 semaines)
   - Définition des besoins fonctionnels et non fonctionnels
   - Modélisation UML et conception de la base de données
   - Choix des technologies et planification
2. **Phase 2 : Développement Backend** (3 semaines)
   - Configuration du projet .NET 9
   - Implémentation des modèles de données
   - Développement des contrôleurs API
   - Mise en place de l'authentification
3. **Phase 3 : Développement Frontend** (3 semaines)
   - Configuration du projet React Native avec Expo
   - Création des écrans principaux
   - Implémentation de la navigation
   - Intégration avec l'API backend
4. **Phase 4 : Intégration et Tests** (1 semaine)
   - Tests d'intégration entre frontend et backend
   - Tests utilisateur
   - Correction des bugs
   - Optimisation des performances
5. **Phase 5 : Finalisation** (1 semaine)
   - Documentation du code
   - Préparation de la démonstration
   - Rédaction du rapport final

5.5 Exemple d'Exécution de Processus dans l'Application

5.5.1 Scénario de Signalement d'Arnaque

Contexte : Un utilisateur souhaite signaler une tentative d'arnaque via l'application « Scam Warning ».

Étapes du Scénario :

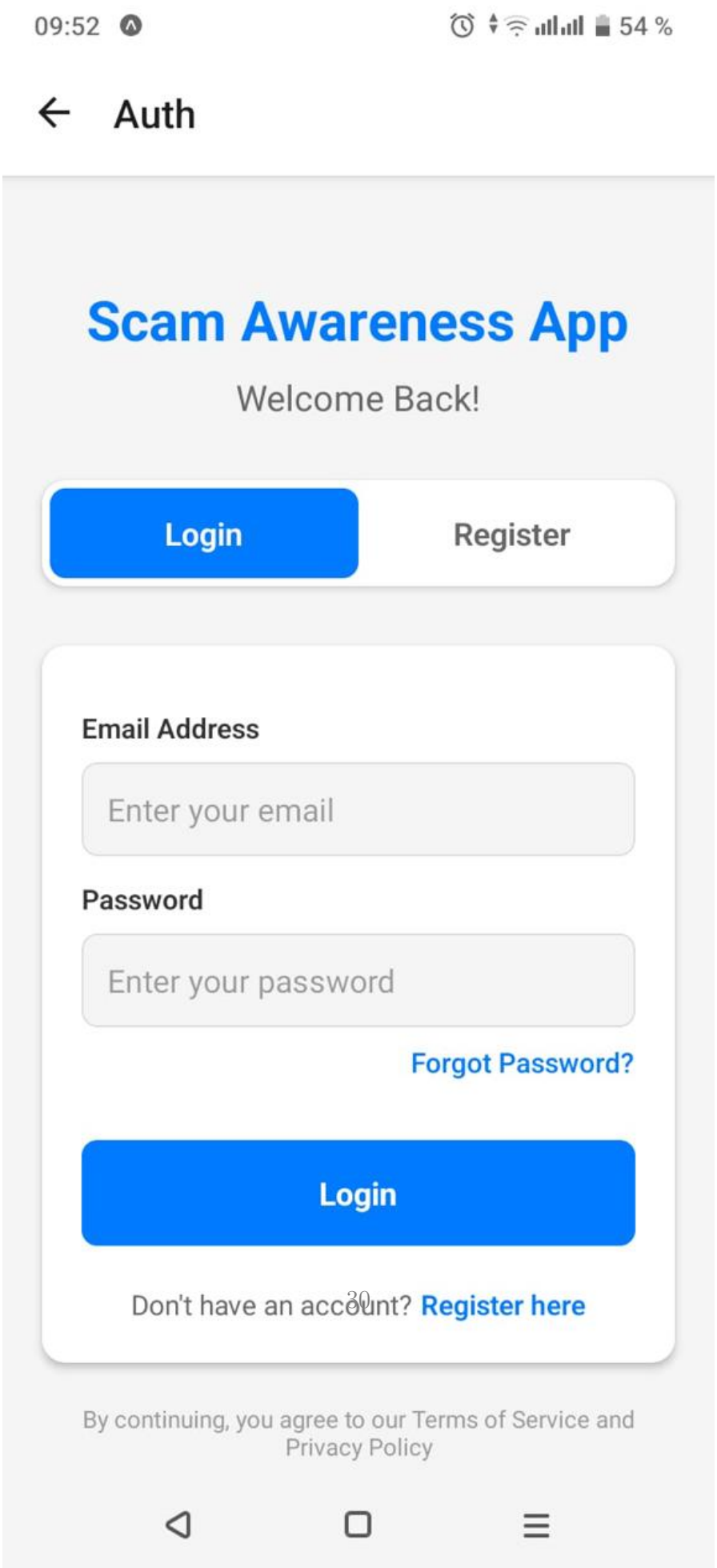
1. **Connexion à l'Application :**
   - L'utilisateur ouvre l'application
   - Il se connecte avec ses identifiants (ou s'inscrit si c'est sa première utilisation)
   - Le système valide les credentials et ouvre la session
2. **Accès au Formulaire de Signalement :**
   - Depuis l'écran d'accueil, l'utilisateur clique sur le bouton « Signaler une arnaque »
   - Le formulaire de signalement s'ouvre avec les champs nécessaires
3. **Remplissage du Formulaire :**
   - L'utilisateur sélectionne la catégorie d'arnaque (Phishing, Téléphonique, etc.)
   - Il entre un titre descriptif
   - Il décrit l'arnaque en détail
   - Il peut optionnellement ajouter des informations supplémentaires (numéro, URL, etc.)
   - Il soumet le formulaire
4. **Traitement par le Système :**
   - L'application envoie les données à l'API backend
   - L'API enregistre l'alerte avec le statut « En attente »
   - Une notification est envoyée aux administrateurs pour modération
5. **Modération par l'Administrateur :**
   - L'administrateur consulte la liste des alertes en attente
   - Il examine le signalement
   - Il approuve ou rejette l'alerte
   - Si approuvée, l'alerte devient visible par tous les utilisateurs
6. **Notification à l'Utilisateur :**
   - L'utilisateur reçoit une notification concernant le statut de son signalement
   - Il peut consulter les commentaires ajoutés par d'autres utilisateurs

5.6 Présentation des Captures d'Écran

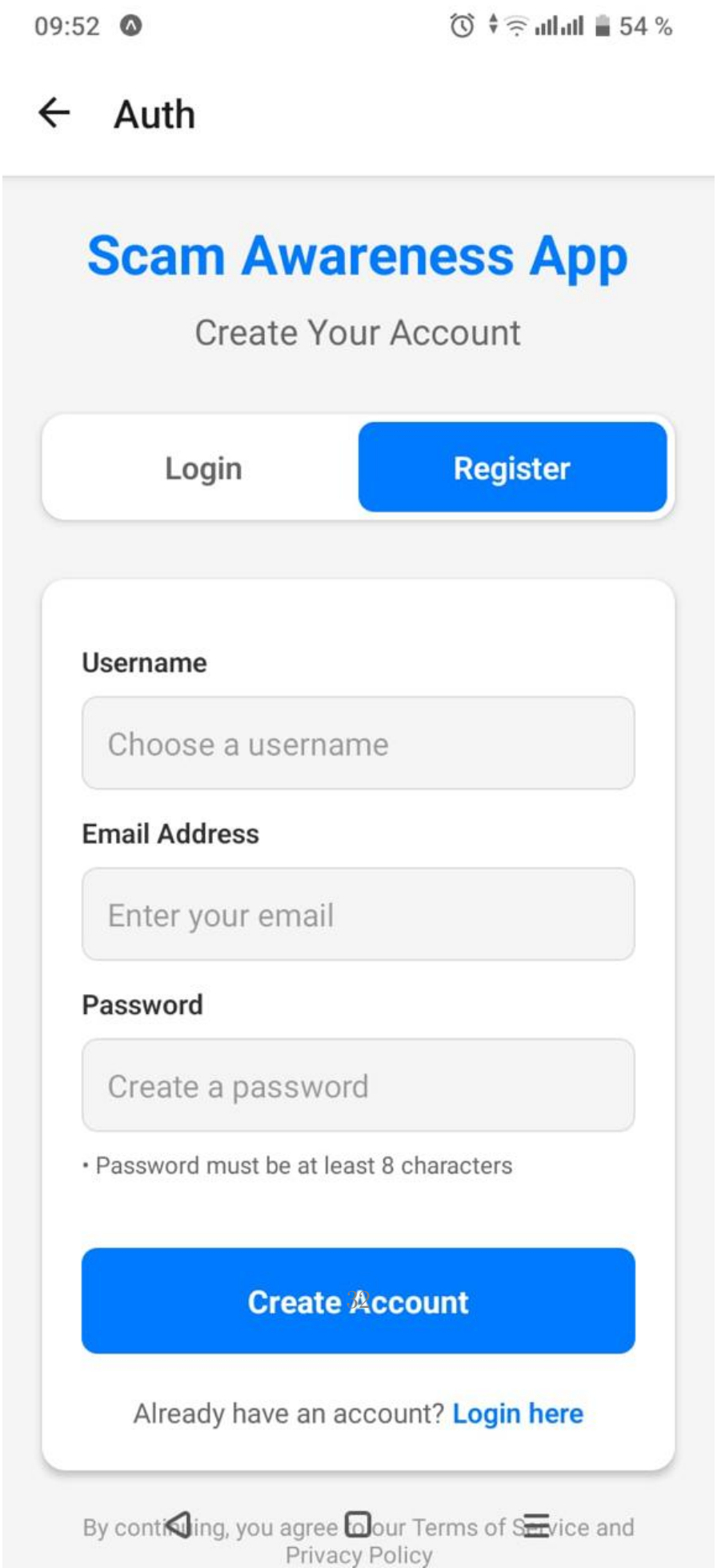
Dans cette section, nous examinons une série de captures d'écran qui illustrent les fonctionnalités clés et l'interface de notre application « Scam Warning ». Ces images fournissent un aperçu visuel de l'expérience utilisateur, mettant en avant la navigation et les outils disponibles.

5.6.1 Présentation des interfaces utilisateur

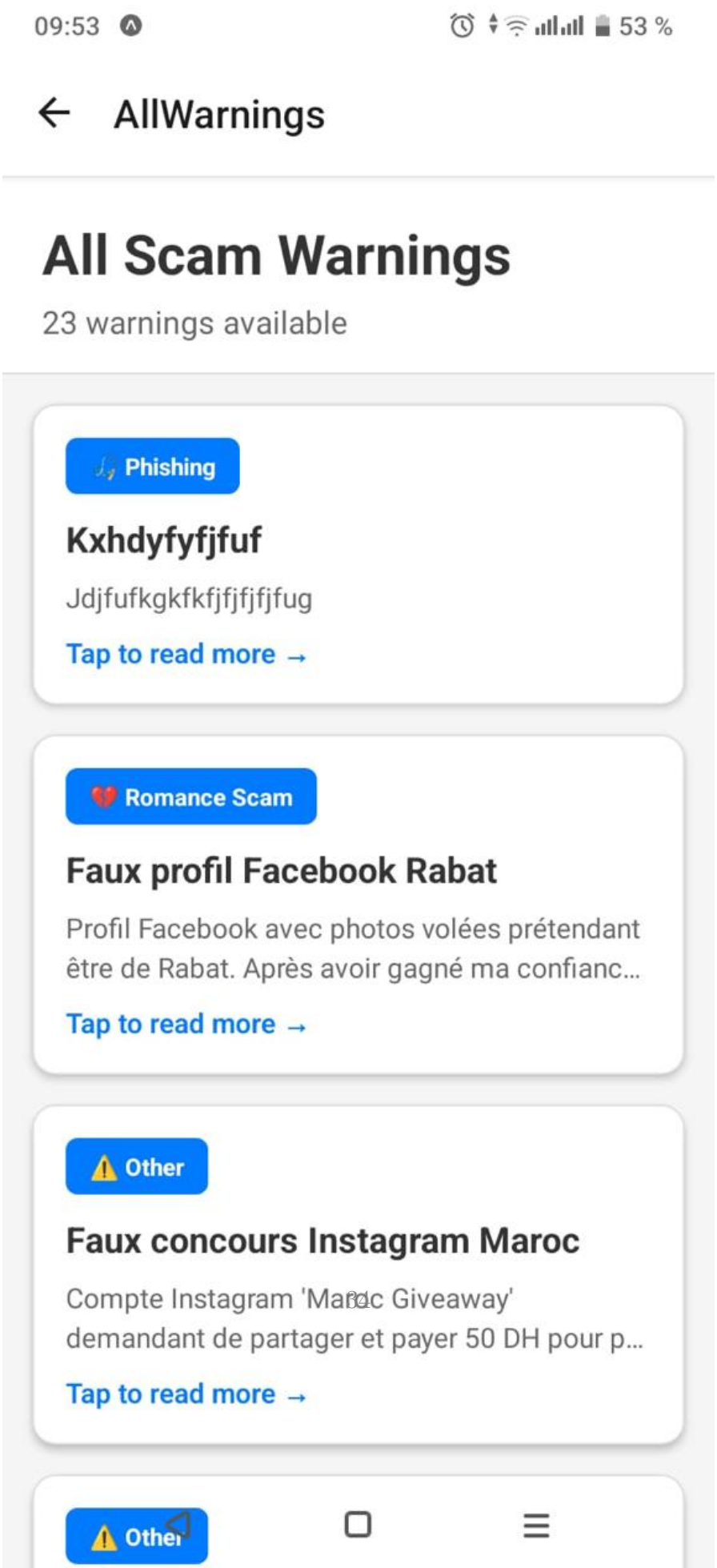
Les captures d'écran suivantes illustrent les principales interfaces de l'application "Scam Warning". Chaque écran est présenté individuellement pour une meilleure lisibilité.


09:52
54 %
Auth
Scam Awareness App
Welcome Back!
Login
Register
Email Address
Enter your email
Password
Enter your password
Forgot Password?
Login
Don't have an account? Register here
By continuing, you agree to our Terms of Service and Privacy Policy

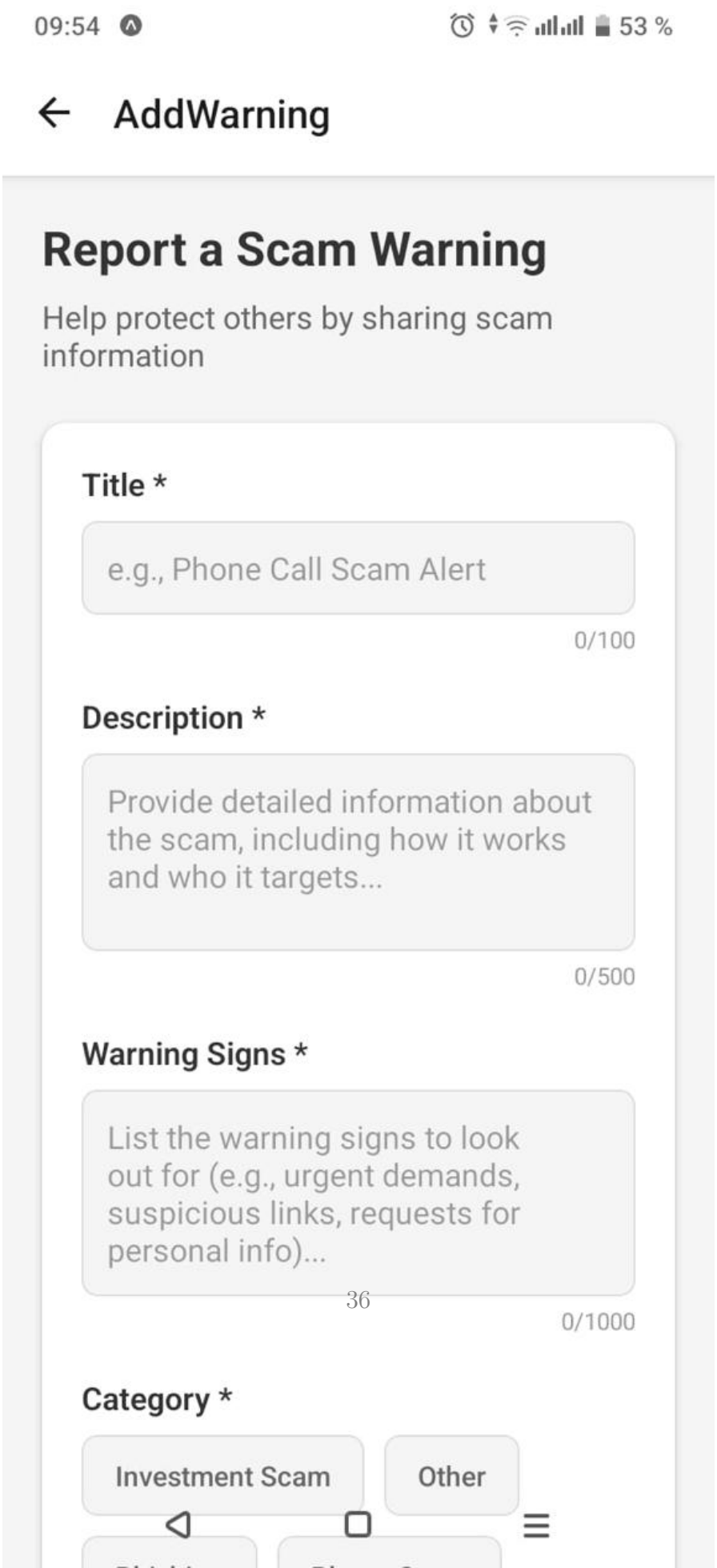
Description : L'écran de connexion permet aux utilisateurs de s'authentifier avec leur email et mot de passe. Interface épurée avec validation en temps réel.


09:52
54 %
Auth
Scam Awareness App
Create Your Account
Login
Register
Username
Choose a username
Email Address
Enter your email
Password
Create a password
• Password must be at least 8 characters
Create Account
Already have an account? Login here
By continuing, you agree to our Terms of Service and
Privacy Policy

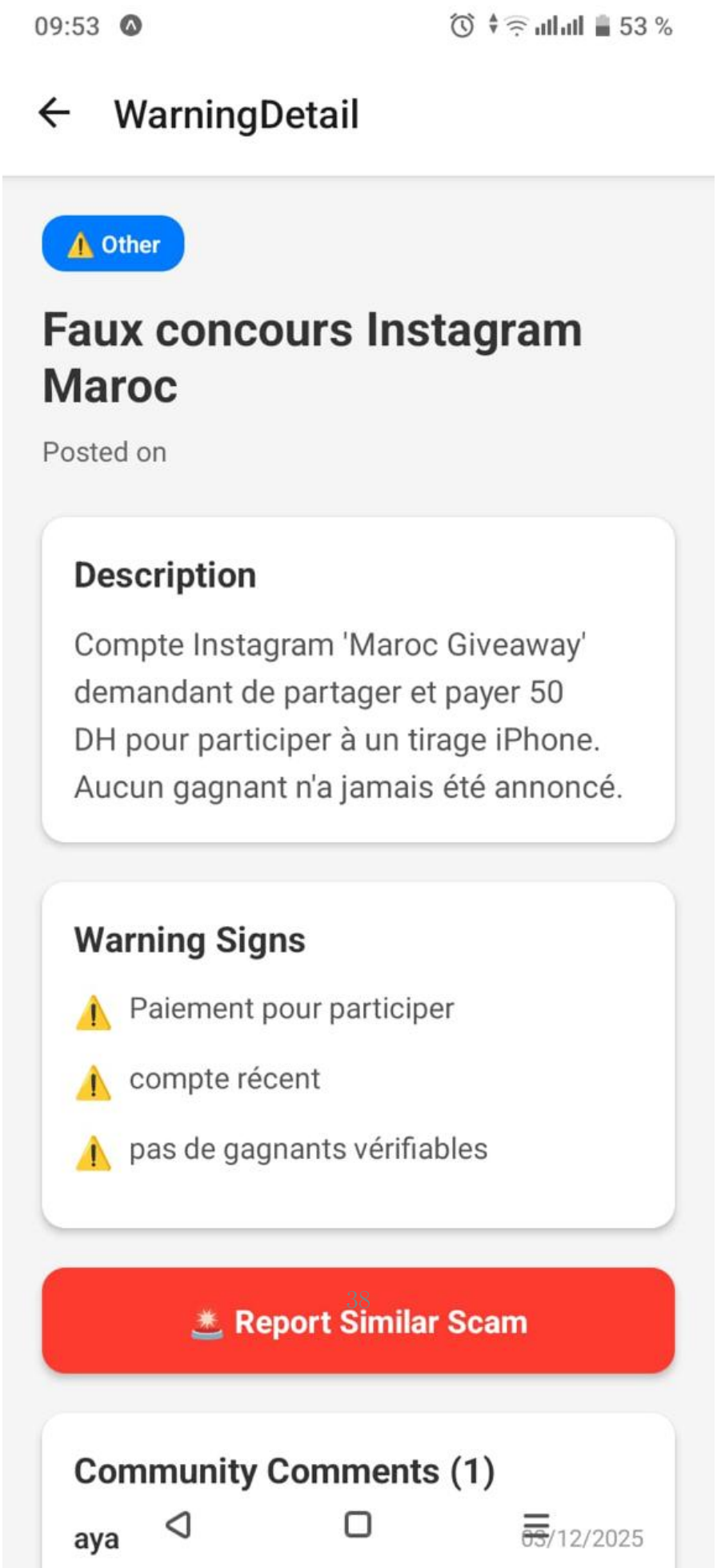
Description : Formulaire d'inscription pour les nouveaux utilisateurs avec validation des champs et indicateur de force du mot de passe.


09:53
53 %
AllWarnings
All Scam Warnings
23 warnings available
Phishing
Kxhdyfyfjfuf
Jdjfufkgkfkfjfjfjfjfug
Tap to read more →
Romance Scam
Faux profil Facebook Rabat
Profil Facebook avec photos volées prétendant être de Rabat. Après avoir gagné ma confianc...
Tap to read more →
Other
Faux concours Instagram Maroc
Compte Instagram 'Maroc Giveaway' demandant de partager et payer 50 DH pour p...
Tap to read more →
Other

Description : L'écran d'accueil présente les alertes récentes sous forme de cartes interactives avec navigation par catégories.


09:54
53 %
AddWarning
Report a Scam Warning
Help protect others by sharing scam information
Title *
e.g., Phone Call Scam Alert
0/100
Description *
Provide detailed information about the scam, including how it works and who it targets...
0/500
Warning Signs *
List the warning signs to look out for (e.g., urgent demands, suspicious links, requests for personal info)...
0/1000
Category *
Investment Scam
Other

Description : Interface guidée pour signaler une nouvelle arnaque avec sélection de catégorie et champs détaillés.


09:53
53 %
WarningDetail
Other
Faux concours Instagram Maroc
Posted on
Description
Compte Instagram 'Maroc Giveaway' demandant de partager et payer 50 DH pour participer à un tirage iPhone. Aucun gagnant n'a jamais été annoncé.
Warning Signs
Paiement pour participer
compte récent
pas de gagnants vérifiables
Report Similar Scam
Community Comments (1)
aya
05/12/2025

Description : Affichage complet d'une alerte spécifique avec toutes les informations et section de discussion communautaire.

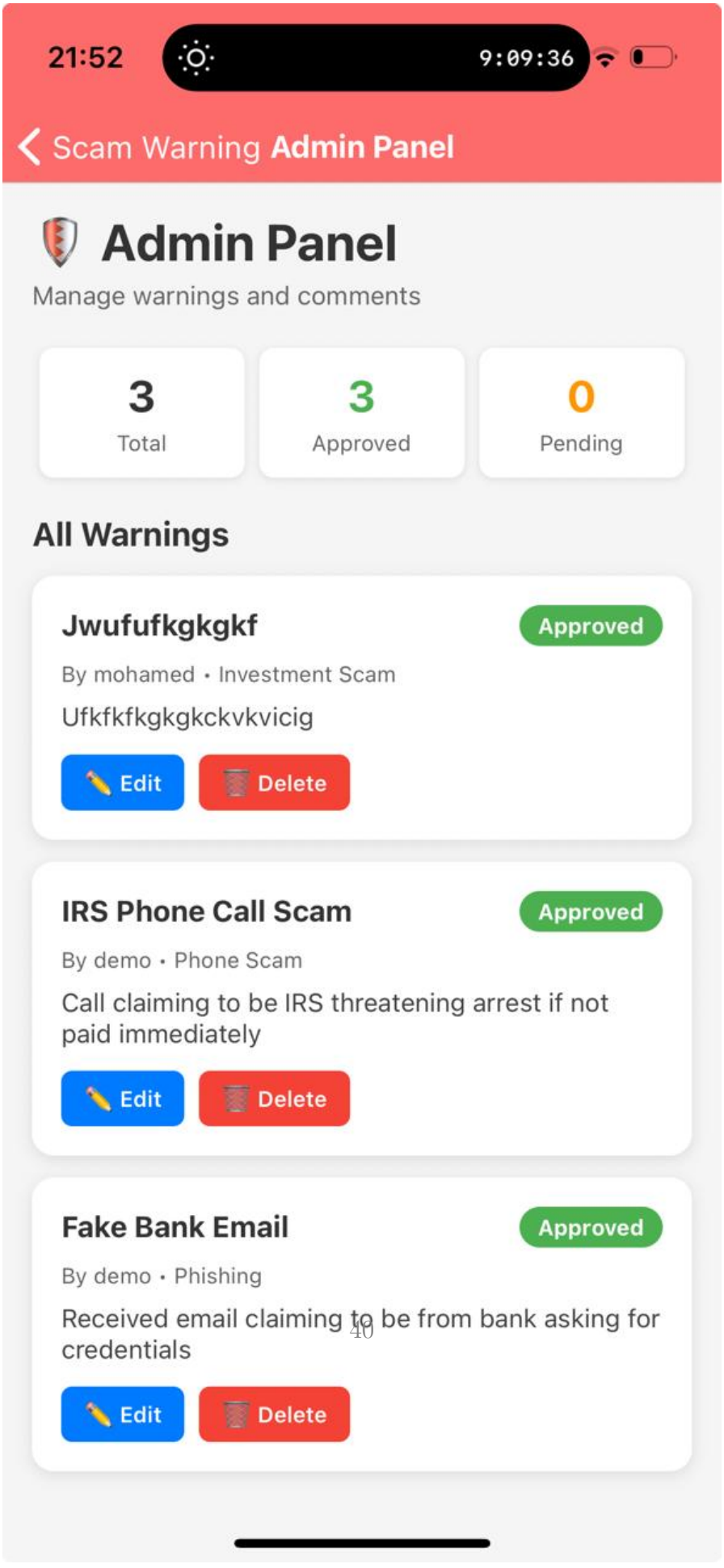


FIGURE 5.6 – Panel d'administration pour la modération

Description : Interface réservée aux administrateurs pour la modération des alertes et la gestion des utilisateurs.

5.6.2 Analyse des interfaces

L'analyse des différentes interfaces présentées ci-dessus révèle une application conçue avec une attention particulière à l'expérience utilisateur. Chaque écran répond à un besoin spécifique :

- **Authentification** : Processus simplifié pour l'accès à l'application
- **Consultation** : Accès rapide aux informations avec présentation claire
- **Signalement** : Formulaire guidé pour faciliter le partage d'informations
- **Discussion** : Espace d'échange pour renforcer la communauté
- **Modération** : Outils complets pour assurer la qualité du contenu

5.6.3 Description des Écrans

Écran de Connexion (Figure 5.1) :
Interface d'authentification permettant aux utilisateurs de se connecter avec leur email et mot de passe. Design épuré avec la palette de couleurs du projet.

Écran d'Inscription (Figure 5.2) :
Formulaire d'inscription pour les nouveaux utilisateurs. Capture les informations de base et valide les données avant création du compte.

Page d'Accueil (Figure 5.3) :
Affiche les alertes récentes validées sous forme de cartes. Navigation intuitive avec menu et bouton d'action principal pour signaler une arnaque.

Formulaire de Signalement (Figure 5.4) :
Interface guidée pour signaler une arnaque. Catégories prédéfinies, champs obligatoires et optionnels, validation en temps réel.

Détail d'Alerte (Figure 5.5) :
Affiche toutes les informations d'une alerte spécifique. Section des commentaires pour les discussions communautaires.

Panel d'Administration (Figure 5.6) :
Interface réservée aux administrateurs pour modérer le contenu. Liste des alertes en attente, outils d'approbation/rejet, gestion des utilisateurs.

5.7 Conclusion

Le développement technologique joue un rôle fondamental dans la création d'outils de prévention efficaces. À travers ce chapitre, nous avons exploré les prin-

cipales technologies utilisées dans le développement de « Scam Warning », notamment les Framework mobiles, les API backend, les bases de données, ainsi que les outils de développement et de collaboration.

Les captures d'écran insérées dans ce chapitre ont permis d'illustrer concrètement les interfaces de l'application, les étapes d'interaction, ainsi que le rendu visuel final. Elles facilitent la compréhension des concepts et des processus en offrant un aperçu visuel réel du travail effectué.

Ainsi, ce chapitre a mis en évidence :

- L'importance du choix technologique dans la réussite d'un projet mobile
- La complémentarité entre les outils de développement frontend et backend
- L'impact positif des technologies modernes sur la productivité et la qualité
- Le lien étroit entre conception UX/UI et développement technique

En résumé, la combinaison de React Native pour le frontend et .NET pour le backend constitue une base solide pour une application mobile performante, évolutive et adaptée aux besoins spécifiques de prévention des arnaques au Maroc.

Conclusion et Perspectives

Conclusion Générale

Le projet « Scam Warning » représente une réponse concrète et innovante à un problème sociétal majeur au Maroc : la prolifération des arnaques numériques qui touchent particulièrement les personnes vulnérables. Grâce à une approche collaborative et communautaire, l'application permet aux citoyens de signaler, partager et consulter des alertes sur des fraudes réelles, contribuant ainsi à une sensibilisation collective et à une protection mutuelle.

Développée dans un cadre académique avec des contraintes budgétaires et temporelles fortes, elle a su démontrer la faisabilité d'une solution mobile cross-platform (React Native et Expo) couplée à une API robuste (.NET 9 et SQLite), tout en respectant les besoins fonctionnels (authentification, gestion des alertes, modération) et non fonctionnels (ergonomie, performance, simplicité d'utilisation).

Les différentes phases du projet – analyse des besoins, modélisation UML, choix techniques justifiés, développement collaboratif et tests exhaustifs – ont permis de produire un prototype fonctionnel, intuitif et opérationnel sur Android et iOS. Les captures d'écran et les résultats obtenus confirment la qualité de l'interface et la fluidité des interactions, même si certaines limites inhérentes au statut de prototype (scalabilité de la base de données, sécurité avancée, notifications push) ont été identifiées et seront adressées dans les évolutions futures.

Ce travail a non seulement répondu aux exigences du cahier des charges académique, mais il a également renforcé nos compétences techniques en développement full-stack, gestion de projet agile, travail en équipe et prise en compte des besoins réels des utilisateurs. Au-delà de l'aspect technique, « Scam Warning » porte une vraie valeur sociale : en donnant la parole aux victimes et en créant une base de connaissances partagée, elle participe à la construction d'une société plus vigilante et mieux protégée face aux menaces numériques.

Perspectives d'Évolution

Bien que les objectifs principaux aient été atteints, certaines limitations subsistent et ouvrent la voie à des perspectives d'amélioration :

1. **Migration vers une base de données cloud** : Remplacer SQLite par PostgreSQL ou MySQL pour une meilleure scalabilité et gestion de la concurrence.
2. **Renforcement de la sécurité** :
   - Implémentation de l'authentification JWT
   - Chiffrement des données sensibles
   - Validation avancée des entrées utilisateur
3. **Notifications push** : Intégration d'un service de notifications pour alerter les utilisateurs en temps réel des nouvelles arnaques dans leur région.
4. **Géolocalisation** : Ajout de la localisation pour afficher les alertes par proximité géographique.
5. **Analyse de données** : Implémentation d'un dashboard analytique pour visualiser les tendances des arnaques.
6. **Application web complémentaire** : Développement d'une version web pour élargir l'accessibilité.
7. **Intégration avec les autorités** : Possibilité de transférer les signalements vers les autorités compétentes.
8. **Système de réputation** : Mise en place d'un système de crédibilité pour les utilisateurs les plus actifs et fiables.
9. **Multilinguisme** : Support de l'arabe et éventuellement d'autres langues.
10. **Application iOS native** : Publication sur l'App Store d'Apple pour une distribution officielle.

Impact Social et Potentiel

« Scam Warning » s'inscrit dans une dynamique d'innovation au service de la sécurité numérique des citoyens marocains. Son potentiel impact social est significatif :

- **Réduction des victimes d'arnaques** : En informant préventivement la population.
- **Création d'une communauté vigilante** : Favorisant l'entraide et le partage d'information.

- **Sensibilisation continue** : Sur les nouvelles techniques de fraude.
- **Données pour la recherche** : Collecte d'informations précieuses sur l'évolution des arnaques au Maroc.
- **Renforcement de la confiance numérique** : En donnant aux citoyens des outils pour se protéger.

En conclusion, ce projet constitue une base solide pour une plateforme de prévention des arnaques moderne et évolutive. Il s'inscrit dans une dynamique d'innovation au service de la sécurité numérique et ouvre la voie à de nombreux axes d'amélioration dans le cadre de futurs travaux. Nous sommes convaincus qu'avec les améliorations envisagées, cette application pourrait devenir un outil incontournable de prévention au Maroc et au-delà.

Bibliographie

1. React Native Documentation. Disponible sur : `https://reactnative.dev/`
2. .NET Documentation. Disponible sur : `https://learn.microsoft.com/dotnet/`
3. Expo Documentation. Disponible sur : `https://docs.expo.dev/`