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

Projet de fin module : Création d'un Simulateur Éducatif pour Identifier et Gérer les Cybermenaces

Laamache Akram
Siad Aya

2ème année Ingénierie Informatique et Réseaux
(4IIR)

2024 - 2025

Tuteur(s) EMSI :
Yousra Moh Ousellam

Membres du jury :

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

Résumé

Ce rapport décrit la conception et le développement d'une application éducative interactive appelée "CyberEscape Room". L'objectif principal de cette application est de renforcer les compétences en cybersécurité à travers des scénarios immersifs et ludiques, permettant aux utilisateurs de comprendre et de répondre à diverses cybermenaces. En progressant à travers des défis de plus en plus complexes, les utilisateurs acquièrent des connaissances pratiques tout en améliorant leur capacité à résoudre des problèmes de sécurité. L'application inclut des outils de suivi et de reporting pour les administrateurs, permettant de mesurer l'engagement et la performance des utilisateurs. Cette solution vise à sensibiliser et former de manière efficace les professionnels aux enjeux de la cybersécurité.

Abstract

This report outlines the design and development of an interactive educational application called "CyberEscape Room". The main goal of this application is to enhance cybersecurity skills through immersive and engaging scenarios, allowing users to understand and address various cyber threats. By progressing through increasingly complex challenges, users gain practical knowledge while improving their ability to solve security-related problems. The application includes tracking and reporting tools for administrators to monitor user engagement and performance. This solution aims to effectively raise awareness and train professionals on the critical issues of cybersecurity.

Remerciements

Nous souhaitons exprimer nos sincères remerciements à l'Ecole Marocaine des Sciences de l'Ingénieur (EMSI) pour son soutien continu et son engagement envers l'excellence académique. L'EMSI nous a offert un environnement d'apprentissage stimulant et des ressources précieuses qui ont grandement contribué à notre développement personnel et professionnel.

Nous tenons également à remercier chaleureusement notre professeur et encadrant, Mme.Yousra Moh Ousellam, pour ses conseils éclairés, son mentorat attentif et son soutien constant tout au long de ce projet. Ses précieuses contributions ont été essentielles à notre succès.

Table des matières

Table des figures

Introduction Générale

La transformation numérique a profondément changé les modes de fonctionnement des entreprises, des institutions et des individus, apportant une interconnexion sans précédent. Cependant, cette avancée s'accompagne de nouvelles menaces sous la forme de cyberattaques de plus en plus sophistiquées. Ces menaces nécessitent une sensibilisation accrue et une formation efficace pour garantir la sécurité des systèmes d'information.

Le projet "CyberEscape Room" s'inscrit dans ce contexte, en proposant une plateforme éducative et ludique qui simule des cyberattaques pour former les utilisateurs à réagir face à ces situations critiques. Inspiré du concept des escape rooms physiques, ce simulateur virtuel combine apprentissage théorique et pratique pour offrir une expérience immersive. Chaque scénario représente un type d'attaque spécifique, tel que le phishing, que les participants doivent résoudre pour "s'échapper".

L'objectif principal de ce projet est d'accroître la compréhension des enjeux de cybersécurité tout en développant les compétences nécessaires pour identifier les vulnérabilités et appliquer des solutions adaptées. Grâce à une interface intuitive et des retours personnalisés, CyberEscape Room vise à transformer une formation complexe en une activité interactive, engageante et accessible.

Le présent rapport détaille les différentes étapes de réalisation du projet, en abordant la conception technique, les fonctionnalités implémentées, ainsi que les défis rencontrés. En adoptant une approche créative et innovante, ce projet se positionne comme un outil pédagogique pertinent pour préparer les utilisateurs aux menaces numériques actuelles et futures.

Chapitre 1

Problematique

Dans un monde de plus en plus dépendant des technologies numériques, la cybersécurité est devenue une priorité pour protéger les systèmes d'information contre les cyberattaques en constante évolution. Cependant, une grande partie des entreprises et des individus manque de sensibilisation et de formation pratique face à ces menaces.

Les méthodes traditionnelles d'apprentissage, telles que les formations théoriques ou les manuels, ne suffisent souvent pas à préparer les utilisateurs aux situations réelles. Elles manquent d'interactivité et d'engagement, ce qui limite leur efficacité dans le développement des compétences nécessaires pour identifier, comprendre et gérer les cybermenaces.

Comment alors concevoir un outil pédagogique qui non seulement informe, mais aussi simule des scénarios réalistes, engage les utilisateurs et les prépare à réagir face à des attaques cybernétiques ? De plus, comment rendre cet apprentissage attractif et accessible, tout en restant fidèle aux enjeux de la cybersécurité moderne ?

Le projet "CyberEscape Room" cherche à répondre à cette problématique en combinant éducation et gamification pour transformer la formation en cybersécurité en une expérience immersive et interactive.

Chapitre 2

Méthodologies

1 Introduction

Dans ce chapitre, nous présentons la méthodologie adoptée pour la réalisation du projet simulateur d'attaques *CyberEscape Room*. Ce projet combine éducation et gamification pour offrir une expérience immersive permettant aux utilisateurs de s'entraîner à réagir face à des cyberattaques. Pour garantir une exécution structurée et efficace, notre méthodologie repose sur trois axes principaux : la conception du contenu (scénarios et énigmes), l'architecture technique, et l'intégration des outils et technologies. Chaque étape vise à assurer une interface conviviale, des scénarios réalistes et des retours utiles pour les utilisateurs. Cette méthodologie favorise à la fois la qualité du produit final et son conformisme avec les standards actuels en matière de cybersécurité.

2 Approches Méthodologiques et Outils Prévus

2.1 Méthodologie Prévue

Conception des scénarios d'attaque

- **Identification des thèmes et menaces** : Nous avons identifié les cybermenaces les plus courantes comme le phishing, pour créer des scénarios réalistes et pertinents.
- **Conception des énigmes** : Chaque scénario inclura des énigmes interactives et adaptées au type d'attaque simulé. Les énigmes guideront l'utilisateur vers la découverte de solutions.
- **Validation des scénarios** : Des experts en cybersécurité testeront et valideront les scénarios pour s'assurer de leur pertinence pédagogique et technique.

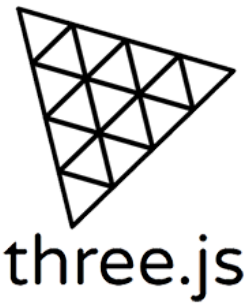
Architecture et design technique

— **Modélisation des données** : Nous utiliserons Django pour développer une base de données relationnelle permettant de gérer les scénarios, les performances des utilisateurs et les états des jeux.

— **Conception modulaire** : Chaque fonctionnalité sera implémentée comme un module indépendant, facilitant la maintenance et l'extensibilité de l'application.

Développement et intégration

— **Frontend interactif** : Le frontend sera conçu en Three.js pour créer une interface utilisateur immersive en 3D.

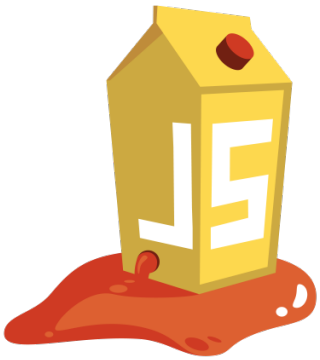


— **Backend robuste** : Le backend, basé sur Django, fournira les API REST pour gérer les scénarios, les scores et les retours personnalisés.
— **Tests unitaires et fonctionnels** : Chaque fonctionnalité sera testée pour vérifier son fonctionnement dans différents scénarios d'utilisation.

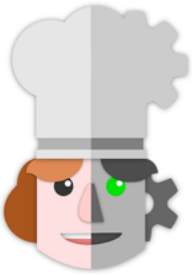
2.2 Outils Prévus

Conception des scénarios

— **OWASP Juice Shop** : Fournira des exemples d'attaques courantes pouvant être simulées dans les scénarios.

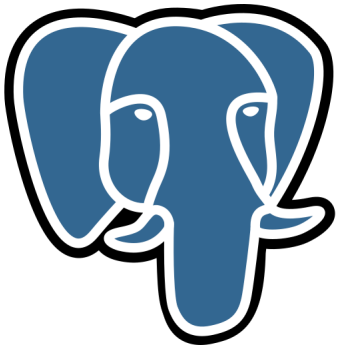


— **CyberChef** : Utilisé pour créer des énigmes liées au chiffrement et à la détection de patterns dans les données.



Développement technique

- **Django et DRF (Django Rest Framework)** : Backend pour gérer les scénarios, les utilisateurs et les performances.
- **Three.js** : Bibliothèque 3D pour le frontend, permettant de créer une expérience immersive.
- **PostgreSQL** : Base de données relationnelle pour stocker les informations sur les utilisateurs, scénarios et scores.



Suivi et évaluation des performances

- **Chart.js** : Pour visualiser les performances des utilisateurs sous forme de graphiques interactifs.

2.3 Phases du projet

Le projet sera réalisé en plusieurs phases :

- **Phase de conception** : Définition des scénarios et architecture du projet.
- **Phase de développement** : Implémentation des fonctionnalités backend et frontend.
- **Phase de tests** : Validation des scénarios et correction des bugs.
- **Phase de déploiement** : Mise en ligne de l'application sur une plateforme cloud (Heroku ou AWS).

Cette méthodologie assure une progression structurée et garantit une qualité optimale pour un produit final performant et pertinent.

Chapitre 3

Étude bibliographique

1 Introduction Générale

L'objectif de notre étude bibliographique est de poser les bases théoriques indispensables à la conception et au développement de notre simulateur éducatif "CyberEscape Room". Cette étude est cruciale, car elle nous permet d'acquérir une compréhension approfondie des concepts fondamentaux liés à la cybersécurité, aux attaques simulées, et aux approches pédagogiques innovantes. En explorant les méthodologies de formation actuelles et les outils de sensibilisation aux cybermenaces, nous identifions les bonnes pratiques et les limites des solutions existantes.

Cela nous permettra de concevoir un simulateur immersif qui combine éducation et gamification de manière efficace. De plus, cette analyse nous aide à anticiper les défis techniques et pédagogiques, tout en garantissant la pertinence des scénarios d'attaques simulés, comme le phishing, pour répondre aux besoins des utilisateurs. En nous appuyant sur les avancées technologiques récentes, notamment dans le domaine de la simulation 3D et de l'interactivité, nous visons à proposer une solution à la fois innovante et adaptée aux enjeux modernes de la cybersécurité.

En résumé, l'étude bibliographique constitue une étape essentielle pour assurer la qualité, la fiabilité et l'impact pédagogique de notre projet "CyberEscape Room".

2 Gamification et Cybersécurité

La gamification, définie comme l'application de mécanismes de jeu dans des contextes non ludiques, émerge comme un outil puissant pour l'éducation et la sensibilisation en cybersécurité. Cette approche transforme des concepts techniques complexes en expériences engageantes et interactives, facilitant ainsi leur compréhension et leur adoption. La gamification en cybersécurité vise à motiver les utilisateurs à apprendre les meilleures pratiques, à reconnaître les menaces potentielles et à développer des réflexes de protection face aux cyberattaques.

2.1 Avantages de la Gamification en Cybersécurité

L'utilisation de la gamification dans ce domaine présente plusieurs avantages clés :

1. **Engagement accru**
   L'une des principales forces de la gamification est sa capacité à maintenir l'engagement des apprenants. Les personnes formées en cybersécurité sont souvent confrontées à des informations techniques complexes et abstraites. La gamification transforme cette formation en une expérience interactive et divertissante, ce qui incite les participants à s'investir davantage dans leur apprentissage.
2. **Apprentissage pratique**
   La gamification permet aux apprenants de mettre en pratique leurs compétences en temps réel. Plutôt que de simplement lire des manuels ou d'assister à des conférences, les participants peuvent résoudre des problèmes réels et prendre des décisions qui auront un impact sur le scénario du jeu. Cela renforce leur compréhension pratique de la cybersécurité.
3. **Rétention améliorée**
   Les jeux et les défis posent des problèmes auxquels les apprenants doivent trouver des solutions. Cette approche active favorise la rétention des connaissances. Les participants se souviennent mieux des informations apprises lorsqu'elles sont associées à des expériences vécues.
4. **Motivation intrinsèque**
   La gamification offre la possibilité de gagner des récompenses, de monter dans les classements ou d'atteindre des objectifs spécifiques. Cette motivation intrinsèque pousse les apprenants à s'efforcer davantage, à s'améliorer constamment et à rester engagés sur le long terme.
5. **Évaluation des compétences**
   Les jeux de cybersécurité permettent de mesurer les compétences des participants de manière transparente. Les gestionnaires de formation peuvent évaluer rapidement les performances individuelles et identifier les domaines nécessitant une amélioration.
6. **Créativité et résolution de problèmes**
   La gamification encourage la créativité et la résolution de problèmes. Les participants doivent souvent trouver des solutions innovantes pour surmonter les défis du jeu, ce qui renforce leur capacité à anticiper et à contrer les menaces réelles.
7. **Collaboration**
   Certains jeux de cybersécurité encouragent la collaboration entre les participants, simulant ainsi des scénarios d'attaque où la coopération est essentielle. Cela prépare les équipes à travailler ensemble efficacement en cas de cybercrise [1] .

2.2 Cybermenaces Traitées dans la Gamification

Dans le cadre de notre étude sur la gamification appliquée à la cybersécurité, nous avons identifié plusieurs cybermenaces clés qui seront traitées à travers des scénarios interactifs. Ces menaces, courantes dans les environnements numériques actuels, permettent aux participants de se confronter à des situations réalistes tout en renforçant leurs compétences pratiques.

— **Phishing**
Le phishing est un type de menace de cybersécurité qui cible les utilisateurs directement par e-mail, SMS ou messages directs. Lors de l'une de ces escroqueries, l'assaillant se fera passer pour un contact de confiance pour voler des données telles que des identifiants, des numéros de compte et des informations de carte de crédit. Le phishing est un type d'attaque d'ingénierie sociale dans laquelle un cybercriminel utilise des e-mails ou d'autres messages textuels pour voler des informations sensibles. En utilisant une adresse e-mail crédible, un attaquant vise à inciter la cible à lui faire suffisamment confiance pour divulguer des données personnelles, telles que des identifiants deconnexion, des numéros de carte de crédit ou des informations de compte financier[2].
Résolution : Identifier les signes de phishing et signaler le faux email afin de prévenir d'éventuelles compromissions.

— **Ransomware**
Un rançongiciel ou *ransomware* en anglais est un code malveillant qui bloque l'accès à votre appareil ou à des fichiers en les chiffrant et qui vous réclame le paiement d'une rançon pour obtenir le déchiffrement de vos données. L'appareil peut être infecté de différentes façons :
  — après l'ouverture d'une pièce-jointe frauduleuse ou d'un lien malveillant reçu par email ;
  — lors d'une navigation sur des sites compromis ;
  — suite à une intrusion informatique sur le système de la victime.

  Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.
Résolution : Isoler la machine infectée pour limiter la propagation et restaurer les fichiers depuis une sauvegarde sécurisée.

— **Attaque par déni de service distribué (DDoS)**
Une attaque en déni de service ou en déni de service distribué (DDoS pour Distributed Denial of Service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service. Ce type d'attaque peut être d'une grande gravité pour l'organisation qui en est victime. Durant l'attaque, le site ou service n'est plus utilisable, au moins temporairement, ou difficilement, ce qui peut entraîner

des pertes directes de revenus pour les sites marchands et des pertes de productivité. L'attaque est souvent visible publiquement, voire médiatiquement, et laisse à penser que l'attaquant aurait pu prendre le contrôle du serveur, donc potentiellement accéder à toutes ses données, y compris les plus sensibles (données personnelles, bancaires, commerciales...) : ce qui porte directement atteinte à l'image et donc la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires[3].
Résolution : Identifier les sources du trafic malveillant et mettre en place des règles de filtrage appropriées.

— **Injection SQL**
Les participants interagissent avec un formulaire web vulnérable à une Une injection SQL (SQLi) est un type d'attaque dans laquelle les cybercriminels tentent d'exploiter les vulnérabilités du code d'une application en insérant une requête SQL dans des champs de saisie ou de formulaire réguliers, tels qu'un nom d'utilisateur ou un mot de passe. L'instruction SQL est ensuite transmise à la base de données SQL sous-jacente de l'application.

Les attaques par injection SQL réussissent lorsque le formulaire d'entrée Web permet aux instructions SQL générées par l'utilisateur d'interroger directement la base de données. Ces attaques ont également proliféré avec l'utilisation de bases de code partagées, telles que les plug-ins WordPress, qui contiennent une vulnérabilité dans le modèle de code sous-jacent. Cette vulnérabilité est transmise à l'ensemble de l'application et peut affecter des centaines de milliers de sites Web qui utilisent tous ce code partagé.

Les dommages peuvent être considérables. Un attaquant ayant une bonne connaissance de SQL saisit des requêtes sur une application Web sans paramètres de validation d'entrée en place, puis accède facilement aux fichiers clients d'une entreprise ou aux informations financières sensibles[4].
Résolution : Mettre en œuvre des pratiques de codage sécurisées, telles que l'utilisation de requêtes paramétrées, pour empêcher l'exploitation de la vulnérabilité.

3 Conclusion

L'étude bibliographique présentée met en lumière l'importance de la gamification dans l'éducation à la cybersécurité, un domaine où les enjeux sont en constante évolution. En explorant les concepts clés de la cybersécurité et en analysant les menaces actuelles comme le phishing, le ransomware, les attaques DDoS et les injections SQL, cette étude nous a permis de mieux comprendre les défis auxquels les utilisateurs et les organisations sont confrontés dans un environnement numérique de plus en plus complexe.

La gamification, en transformant l'apprentissage traditionnel en une expérience interactive et engageante, s'avère être un outil puissant pour améliorer l'efficacité de la formation en cybersécurité. Elle offre une approche innovante pour renforcer l'engagement, la rétention des connaissances et la résolution de problèmes, tout en permettant une évaluation pratique des compétences. De plus, l'intégration de scénarios réalistes dans un environnement immersif, tel que celui proposé par notre simulateur "CyberEscape Room", permet aux apprenants de se confronter à des situations concrètes et d'améliorer leur capacité à réagir face aux cybermenaces.

Ainsi, cette étude bibliographique constitue une étape fondamentale pour le développement de notre simulateur éducatif, en nous offrant une base solide de connaissances et de bonnes pratiques qui guideront la conception de notre projet. La combinaison de la pédagogie moderne et des technologies de simulation avancées permettra de proposer une solution efficace, immersive et pertinente pour sensibiliser les utilisateurs aux défis contemporains de la cybersécurité.

Chapitre 4

Spécification des besoins

1 Introduction

Dans ce chapitre, nous détaillerons les spécifications des besoins pour l'application éducative que nous avons développée dans le cadre de ce projet de fin de module. Cette application vise à offrir une plateforme permettant aux employés de passer des tests après leur formation. L'objectif est de renforcer les connaissances acquises et d'évaluer l'efficacité des formations dispensées. Nous commencerons par analyser les besoins du client cible et les fonctionnalités attendues pour garantir une application utile et fonctionnelle.

2 Analyse du besoin

L'analyse des besoins est une étape fondamentale pour identifier les attentes des utilisateurs et garantir que notre solution y répond adéquatement. Bien que nous n'ayons pas mené d'entretiens directs avec des utilisateurs, nous avons basé notre analyse sur les objectifs généraux d'une application éducative dans le cadre d'une formation professionnelle.

2.1 Identification des besoins

L'identification des besoins repose sur l'objectif de permettre aux employés de tester et de valider leurs connaissances après une formation. Nous avons formulé les besoins à partir des exigences suivantes :

— **Suivi des progrès :** L'application doit permettre de suivre les progrès des employés en temps réel, y compris les résultats des tests et les domaines nécessitant des améliorations.

— **Facilité d'accès aux tests :** Les tests doivent être facilement accessibles après chaque module de formation, avec une interface utilisateur claire et intuitive.

— **Personnalisation des tests :** Les tests doivent pouvoir être adaptés en fonction des objectifs spécifiques de la formation, en permettant d'inclure des questions variées.

3 Description des besoins fonctionnels et non fonctionnels

3.1 Besoins fonctionnels

Les besoins fonctionnels déterminent les principales fonctionnalités que l'application doit offrir. Voici les besoins identifiés pour notre projet :

— **Création et gestion des tests :**
  — **Génération automatique des tests :** L'application doit pouvoir générer des tests basés sur les modules de formation suivis.
  — **Personnalisation des questions :** Il doit être possible de personnaliser les questions en fonction des sujets de la formation.
— **Suivi des résultats :**
  — **Visualisation des scores :** L'application doit afficher les résultats des tests de manière claire, avec des graphiques ou des tableaux pour un suivi facile.
  — **Historique des performances :** Les utilisateurs doivent pouvoir consulter l'historique de leurs tests passés pour suivre leur évolution.
— **Interface utilisateur :**
  — **Interface simple et intuitive :** L'application doit être facile à utiliser pour les employés, sans nécessiter de compétences techniques.
  — **Accessibilité multi-device :** Les utilisateurs doivent pouvoir accéder à l'application depuis différents appareils (PC, tablettes, smartphones).
— **Notifications et rappels :**
  — **Rappels de tests :** Les utilisateurs doivent recevoir des rappels pour passer les tests après avoir terminé un module.
— **Administration des utilisateurs :**
  — **Gestion des comptes utilisateurs :** L'application doit permettre l'administration des utilisateurs, notamment la création de comptes et la gestion des profils des employés.

3.2 Besoins non fonctionnels

Les besoins non fonctionnels définissent les critères de qualité de l'application. Voici ceux que nous avons identifiés :

— **Performance :**
  — **Réactivité :** L'application doit offrir une réactivité optimale, avec des temps de réponse rapides lors des tests et de l'affichage des résultats.

- **Sécurité :**
  - **Protection des données :** Les informations des utilisateurs et les résultats des tests doivent être stockés de manière sécurisée et protégées par des mécanismes de sécurité robustes (cryptage, authentification).
- **Scalabilité :**
  - **Extensibilité :** L'application doit être conçue pour s'adapter à un nombre croissant d'utilisateurs sans dégradation des performances.
- **Accessibilité :**
  - **Multiplateforme :** L'application doit être accessible sur différents systèmes d'exploitation (Windows, macOS, Android, iOS).
- **Facilité d'utilisation :**
  - **Interface simple et intuitive :** L'interface utilisateur doit être claire et intuitive, permettant une prise en main rapide.

4 Client cible

Les clients cibles de notre application sont principalement les responsables de formation et les employés dans un cadre professionnel. L'application est destinée à faciliter le suivi des progrès après chaque module de formation, en permettant aux employés de passer des tests qui valident leurs connaissances. Voici les profils des utilisateurs :

4.1 Responsables de formation

Les responsables de formation peuvent utiliser l'application pour suivre les résultats des employés, générer des tests personnalisés et analyser les progrès réalisés. Ils auront également accès à des rapports détaillés pour évaluer l'efficacité des formations.

4.2 Employés

Les employés sont les utilisateurs finaux de l'application, qui passeront des tests après avoir terminé des modules de formation. L'application doit leur offrir une expérience simple, avec des rappels pour passer les tests et un suivi clair de leurs résultats.

5 Méthode utilisée

Pour répondre aux besoins fonctionnels et non fonctionnels identifiés, nous avons adopté une méthodologie agile qui permet une flexibilité et une réactivité maximales tout au long du projet. Nous avons choisi une architecture technique modulaire et

bien structurée, associée à une sélection d'outils et de technologies adaptées aux spécifications du projet.

5.1 Conception des Scénarios et Tests

Dans un premier temps, nous avons élaboré les scénarios d'utilisation de l'application en définissant les principaux flux de tests et les critères de succès pour chaque utilisateur (responsables de formation et employés). Cette phase de conception a été validée par un processus itératif avec les besoins définis pour chaque fonction :

- **Création et gestion des tests :** L'application doit permettre aux responsables de formation de créer des tests personnalisés. Nous avons utilisé **Node.js et Express** pour la gestion des API qui génèrent des tests basés sur les formations.
- **Suivi des résultats :** Pour assurer une visualisation claire et dynamique des résultats, nous avons intégré **Chart.js** pour afficher les performances des utilisateurs sous forme de graphiques interactifs.

5.2 Développement Backend

Le développement du backend repose sur une architecture solide et scalable, permettant de gérer de manière sécurisée les utilisateurs et les résultats des tests. Nous avons choisi les outils suivants pour garantir une gestion optimale des données :

- **Django et Django Rest Framework (DRF) :** Pour la création d'une base de données relationnelle, nous avons utilisé **Django**, un framework robuste et bien adapté au développement rapide d'applications. **DRF** nous a permis de créer des API RESTful pour l'interaction avec le frontend.
- **PostgreSQL :** Comme base de données relationnelle, nous avons utilisé **PostgreSQL**, qui permet une gestion efficace des données structurées, telles que les utilisateurs, tests et scores.

5.3 Développement Frontend

Le frontend de l'application a été conçu pour offrir une interface réactive et simple d'utilisation, essentielle pour une adoption rapide par les employés et les responsables de formation :

- **React.js :** Utilisé pour créer une interface dynamique et réactive, offrant une expérience fluide aux utilisateurs lors de la consultation des tests, résultats et historiques.
- **Bootstrap :** Le framework **Bootstrap** a été intégré pour créer une mise en page réactive, permettant à l'application de s'adapter à divers types d'appareils (PC, tablettes, smartphones).

5.4 Sécurité et Protection des Données

La sécurité des données a été une priorité dans le développement de l'application, notamment en ce qui concerne les informations sensibles des utilisateurs et les résultats des tests. Nous avons choisi les solutions suivantes pour garantir la protection des données :

- **JWT (JSON Web Tokens) :** Nous avons utilisé **JWT** pour l'authentification et l'autorisation des utilisateurs, permettant une gestion sécurisée des sessions.
- **SSL/TLS :** Les communications entre le client et le serveur sont sécurisées grâce à **SSL/TLS**, assurant le chiffrement des données sensibles échangées.

5.5 Tests et Validation

Nous avons mis en place une série de tests unitaires et fonctionnels tout au long du développement pour valider chaque fonctionnalité de l'application. Ces tests ont permis de vérifier la conformité des fonctionnalités avec les besoins définis, notamment en termes de génération de tests, suivi des résultats et gestion des utilisateurs. Les outils comme **Postman** ont été utilisés pour tester les API, et des tests manuels ont été effectués pour garantir une expérience utilisateur optimale.

6 Résumé

Ce chapitre a permis de définir les besoins fonctionnels et non fonctionnels de l'application, ainsi que d'identifier les outils et technologies nécessaires à sa mise en œuvre. L'application éducative vise à améliorer l'efficacité des formations en permettant un suivi des progrès des employés à travers des tests après chaque module. La prochaine étape consistera à transformer ces spécifications en un plan de développement détaillé et à commencer la phase de codage.

Chapitre 5

Réalisation

1 Introduction

Ce chapitre décrit la mise en œuvre pratique de l'application éducative développée pour le suivi des formations et l'évaluation des connaissances des employés. Nous commencerons par présenter les diagrammes utilisés dans le processus de conception, tels que les diagrammes de cas d'utilisation, de séquence et de classes, qui illustrent le fonctionnement et les interactions de l'application. Ensuite, nous détaillerons l'architecture technique et les technologies sous-jacentes choisies pour garantir la robustesse et la scalabilité de l'application. Enfin, nous exposerons les principales fonctionnalités implémentées, ainsi que les interfaces utilisateurs clés, permettant d'assurer une expérience fluide et intuitive pour les employés et les responsables de formation.

1.1 Description des acteurs :

Un acteur représente une abstraction d'un rôle joué par des entités externes au système qui interagissent directement avec lui.

- **Utilisateur :** Une personne qui interagit avec le simulateur CyberEscape Room pour résoudre des énigmes, proposer des solutions et passer à différents niveaux.
- **Administrateur :** Une personne responsable de la gestion du système, notamment en visualisant les rapports de performances des utilisateurs.

2 Diagramme de cas d'utilisation :

Le diagramme de la figure 5.1 illustre les interactions principales entre les utilisateurs, l'administrateur, et le système.

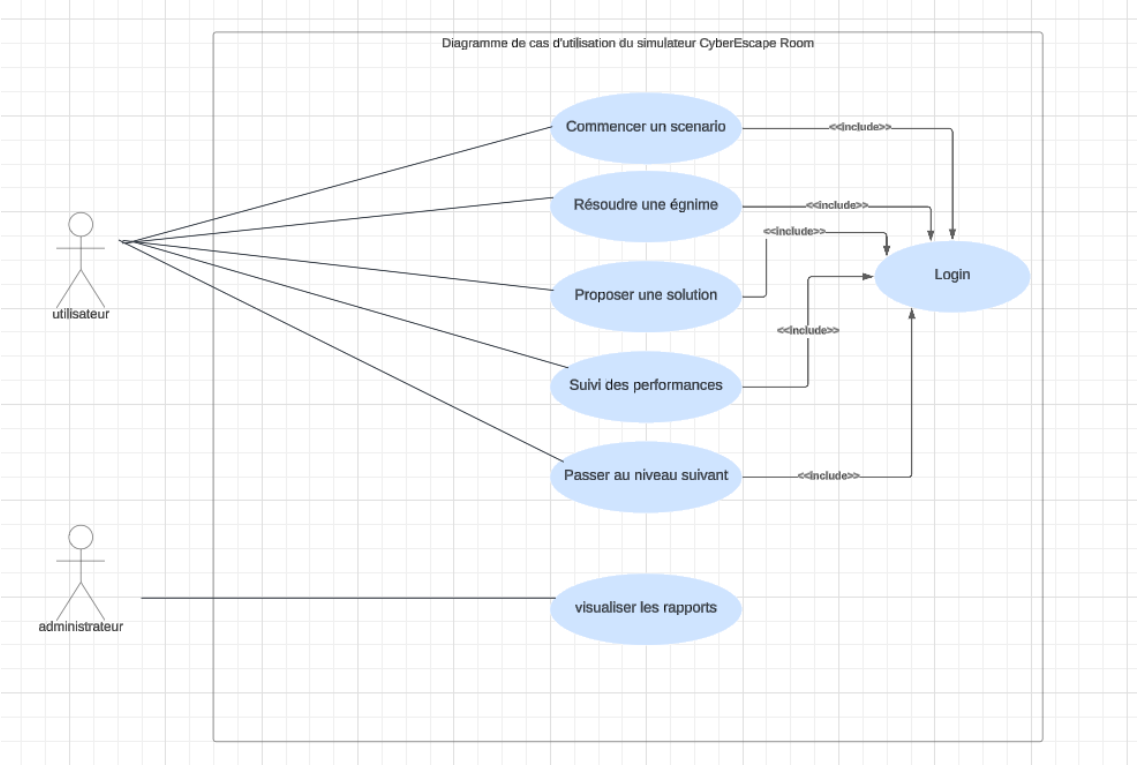


FIGURE 5.1 – Diagramme de cas d'utilisation du simulateur CyberEscape Room

2.1 Description détaillée des cas d'utilisation :

Titre	Interagir avec le simulateur
Description	Ce cas d'utilisation permet aux utilisateurs de résoudre des énigmes et suivre leur progression, et aux administrateurs de consulter les performances.
Acteurs	Utilisateur, Administrateur
Pré-conditions	— L'utilisateur doit être connecté pour accéder aux énigmes. — L'administrateur doit avoir des privilèges d'accès au tableau des rapports.
Scénario nominal	1. L'utilisateur ou l'administrateur se connecte via le système de login. 2. Pour un utilisateur : — Sélectionne un scénario à jouer. — Résout une énigme et propose une solution. — Suit sa progression et passe au niveau suivant. 3. Pour un administrateur : — Accède aux rapports détaillés des performances des utilisateurs. — Analyse les résultats pour identifier les points à améliorer dans le système.

TABLE 5.1 – Description détaillée des cas d'utilisation : Interagir avec le simulateur

2.2 Résumé

En conclusion, le diagramme de cas d'utilisation de l'application CyberEscape Room met en évidence les interactions principales entre les utilisateurs et les administrateurs avec les fonctionnalités du système. Les utilisateurs peuvent commencer des scénarios, résoudre des énigmes, proposer des solutions, suivre leurs performances et passer au niveau suivant, tandis que les administrateurs ont la possibilité de visualiser les rapports de performance. L'inclusion systématique du cas d'utilisation "Login" garantit une authentification sécurisée avant toute interaction avec le système. Ce diagramme offre une vue d'ensemble claire et structurée des capacités et des bénéfices offerts par l'application.

3 Diagramme de classe

4 diagramme de sequence

Bibliographie

[1] “Utiliser la Gamification pour Renforcer la Sécurité,” Mar. 2024.

[2] “Qu’est-ce que le phishing ? Types d’attaques par phishing.”

[3] “Attaque DDoS, que faire ?.”

[4] “Qu’est-ce que l’injection SQL ? Comment prévenir l’injection SQL ?.”