# Cahier des charges

**E5 - Jeux Olympiques**



**Fait par Anatoli Mikoyan**

Cahier des charges techniques

Sommaire

[1. Contexte du projet](#_heading=h.1d6mma2ci7xl)

[1.1. Présentation du projet](#_heading=h.wek20lqal41w)

[1.2. Date de rendu du projet](#_heading=h.hsbf2s9v0gpe)

[2. Besoins fonctionnels](#_heading=h.72adhlswac0n)

[3. Ressources nécessaires à la réalisation du projet](#_heading=h.lr47i5krzqwp)

[3.1. Ressources matérielles](#_heading=h.moe5ly27tmhr)

[3.2. Ressources logicielles](#_heading=h.cvyk6p742phf)

[4. Gestion du projet](#_heading=h.wj6e27o1xw4s)

[5. Conception du projet](#_heading=h.4jjvlmxvhcof)

[5.1. Le front-end](#_heading=h.b3pf1ig00kap)

[5.1.1. Wireframes](#_heading=h.xbdoysf41ddh)

[5.1.2. Maquettes](#_heading=h.taj1xh3jo3sr)

[5.1.3. Arborescences](#_heading=h.7cpah6l43vkf)

[5.2. Le back-end](#_heading=h.ri4n2nlk4x5y)

[5.2.1. Diagramme de cas d’utilisation](#_heading=h.4hfnlk8rv9if)

[5.2.2. Diagramme d’activités](#_heading=h.d1ay6n1m7wn9)

[5.2.3. Modèles Conceptuel de Données (MCD)](#_heading=h.mhbyfyrbmn9)

[5.2.4. Modèle Logique de Données (MLD)](#_heading=h.rr2kq3n12ss)

[5.2.5. Modèle Physique de Données (MPD)](#_heading=h.5jowy0y259aj)

[6. Technologies utilisées](#_heading=h.6j2nbpnxpppw)

[6.1. Langages de développement Web](#_heading=h.uhwlwqptkq2s)

[6.2. Base de données](#_heading=h.q8i476rr9oys)

[7. Sécurité](#_heading=h.15p9a6rgigad)

[7.1. Login et protection des pages administrateurs](#_heading=h.q04sq9cnrw82)

[7.2. Cryptage des mots de passe avec Bcrypt](#_heading=h.ct1wz6q0jyd1)

[7.3. Protection contre les attaques XSS (Cross-Site Scripting)](#_heading=h.cimahn54kest)

[7.4. Protection contre les injections SQL](#_heading=h.cg22ajiezi4v)

# 

# Contexte du projet

## 1.1. Présentation du projet

Votre agence web a été sélectionnée par le comité d’organisation des jeux olympiques de Paris 2024 pour développer une application web permettant aux organisateurs, aux médias et aux spectateurs de consulter des informations sur les sports, les calendriers des épreuves et les résultats des JO 2024.

Votre équipe et vous-même avez pour mission de proposer une solution qui répondra à la demande du client.

## 1.2. Date de rendu du projet

Le projet doit être rendu au plus tard le 7 novembres 2024.

# Besoins fonctionnels

Le site web devra avoir une partie accessible au public et une partie privée permettant de gérer les données.

Les données seront stockées dans une base de données relationnelle pour faciliter la gestion et la mise à jour des informations. Ces données peuvent être gérées directement via le site web à travers un espace administrateur.

# Ressources nécessaires à la réalisation du projet

## 3.1. Ressources matérielles

Pour assurer la mise en œuvre efficace du projet, les ressources matérielles indispensables comprennent :

* **Ordinateur :** C’est un équipement informatique indispensable pour faire fonctionner les logiciels et réaliser les tâches de développement, de conception et de gestion du projet.
* **Moniteur :** Un écran d'ordinateur nécessaire pour visualiser et interagir avec les données, les applications et les interfaces utilisateur lors du processus de travail.
* **Périphériques :**
  + **Clavier :** Utilisé pour saisir des commandes, du texte et des données, facilitant ainsi la communication avec l'ordinateur et l'exécution des tâches.
  + **Souris :** Un dispositif d'entrée permettant de contrôler le curseur à l'écran, de cliquer sur des éléments et d'interagir avec les applications de manière intuitive.

## 3.2. Ressources logicielles

Les outils logiciels essentiels pour mener à bien le projet sont :

* **MAMP** : Environnement de développement local utilisé pour gérer les bases de données MySQL et configurer des serveurs web Apache.
* **GitHub** : Plateforme collaborative permettant d'héberger le code source, de suivre les versions et de gérer les modifications apportées au projet.
* **Visual Studio Code (IDE)** : Outil utilisé pour la programmation du projet.
* **Trello** : Outil de gestion de projet en ligne, facilitant l'organisation des tâches, leur suivi et la collaboration au sein de l'équipe.
* **Figma** : Utilisé pour la création des wireframes et maquettes, afin de visualiser et concevoir l'interface utilisateur.
* **Moccodo** : Permet de simplifier la création du modèle conceptuel de données, facilitant ainsi la structuration et la compréhension des informations.
* **Visual Paradigm** : Employé pour modéliser et concevoir les processus, tout en établissant une arborescence structurée du projet.

# Gestion du projet

Pour réaliser le projet, nous utiliserons la méthode Agile Kanban. Nous utiliserons également l’outil de gestion de projet en ligne Trello.

**Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement**

Nous travaillons également sur GitHub, plateforme de développement collaboratif.

# Conception du projet

## 5.1. Le front-end

### 5.1.1. Wireframes

Une image contenant texte, capture d’écran, diagramme, ligne

Description générée automatiquementUne image contenant texte, diagramme, capture d’écran, ligne

Description générée automatiquement

Une image contenant diagramme, ligne, capture d’écran, Tracé

Description générée automatiquementUne image contenant capture d’écran, texte, diagramme, ligne

Description générée automatiquement

### 5.1.2. Maquettes

Une image contenant capture d’écran, texte, diagramme, conception

Description générée automatiquementUne image contenant texte, capture d’écran, conception

Description générée automatiquement

### Une image contenant capture d’écran, texte, conception, peigne Description générée automatiquement

### 5.1.3. Arborescences

Une image contenant texte, capture d’écran, Rectangle, Post-it

Description générée automatiquement

## 

## 5.2. Le back-end

### 5.2.1. Diagramme de cas d’utilisation

Une image contenant texte, diagramme, capture d’écran, ligne

Description générée automatiquement

### 5.2.2. Diagramme d’activités

Une image contenant texte, capture d’écran, diagramme, ligne

Description générée automatiquement

### 5.2.3. Modèles Conceptuel de Données (MCD)

Une image contenant texte, diagramme, capture d’écran, Parallèle

Description générée automatiquement

### 5.2.4. Modèle Logique de Données (MLD)

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

### 5.2.5. Modèle Physique de Données (MPD)

Une image contenant texte, Police, capture d’écran, diagramme

Description générée automatiquement

# Technologies utilisées

## 6.1. Langages de développement Web

Dans le cadre de la réalisation du projet, nous avons prévu d'utiliser les langages de développement web suivants, chacun jouant un rôle spécifique dans la création et l'interactivité des pages web :

- **HTML5** : Ce langage de balisage est essentiel pour structurer le contenu des pages web, en organisant les textes, images, liens et autres éléments de manière cohérente.

- **CSS3** : Il s'agit du langage des feuilles de style en cascade, utilisé pour définir la présentation visuelle des pages web, comme la mise en page, les styles et l'agencement des éléments, ce qui améliore l'expérience utilisateur et l'esthétique globale.

- **JavaScript** : Ce langage de programmation côté client est crucial pour ajouter des fonctionnalités dynamiques et interactives aux pages web, permettant de manipuler en temps réel le contenu et les éléments, ainsi que de gérer l'interaction utilisateur.

## 6.2. Base de données

Pour la gestion de la base de données, nous avons prévu d'utiliser les technologies suivantes, alliant un langage de programmation serveur à un langage de requête structuré :

- **PHP8**: Ce langage de programmation côté serveur sera utilisé pour dynamiser les interactions entre la base de données et l'interface de l'application web, facilitant ainsi le traitement des données et la génération de contenu dynamique.

- **SQL** : Langage de requête structuré indispensable pour la manipulation des données dans la base de données, SQL sera utilisé pour exécuter des requêtes, gérer les mises à jour et effectuer diverses opérations, garantissant la cohérence et l'intégrité des informations stockées.

- **MAMP** : Nous utiliserons MAMP, une plateforme de développement local, pour créer et gérer une base de données MySQL. Cette solution propose un environnement complet, intégrant un serveur Apache, MySQL et PHP, permettant un développement et des tests efficaces de notre application web.

# Sécurité

La sécurité des sites web a pour but principal de prévenir les attaques et les intrusions malveillantes. Elle englobe un ensemble de pratiques et de mécanismes conçus pour empêcher l'accès non autorisé, l'altération, l'exploitation ou la destruction des ressources en ligne. Ces mesures visent à protéger les données, à garantir le bon fonctionnement des services et à préserver l'accès continu au site. En assurant la confidentialité, l'intégrité et la disponibilité des informations, elles renforcent la fiabilité du site et protègent les utilisateurs contre les risques liés aux menaces en ligne.

## 7.1. Login et protection des pages administrateurs

Pour gérer l'authentification des utilisateurs, nous mettrons en place un système de connexion qui collectera les identifiants, tels que le nom d'utilisateur et le mot de passe. Ces informations seront vérifiées en les comparant à celles enregistrées dans la base de données, afin de confirmer l'existence d'un compte valide. Cette fonctionnalité sera principalement destinée à l'accès à l'interface administrateur, ce qui accentue la nécessité de sécuriser rigoureusement le processus d'authentification.

## 7.2. Cryptage des mots de passe avec Bcrypt

Bcrypt est un algorithme de hachage conçu pour sécuriser les mots de passe en résistant aux attaques par force brute et dictionnaire. Il ajoute un "sel" unique à chaque mot de passe, garantissant que même des mots de passe identiques auront des hachages différents. De plus, il permet d'ajuster la complexité du calcul, ralentissant le processus de hachage et augmentant la sécurité avec le temps. En PHP, Bcrypt est facile à utiliser via la fonction `password\_hash()` pour créer des hachages sécurisés et `password\_verify()` pour vérifier les mots de passe lors de la connexion. Il est également possible d’ajuster le coût pour renforcer encore la sécurité.

## 7.3. Protection contre les attaques XSS (Cross-Site Scripting)

Les attaques XSS (Cross-Site Scripting) se produisent lorsque des attaquants injectent du code malveillant, généralement en JavaScript, dans une page web vue par d'autres utilisateurs. Cela leur permet de voler des informations sensibles, comme des cookies de session.

Pour se protéger contre les attaques XSS en PHP, il est essentiel d'échapper toutes les données avant de les afficher. La fonction htmlspecialchars() est très utile pour transformer des caractères spéciaux comme <, >, et & en texte inoffensif, évitant ainsi qu'ils soient interprétés comme du code.

Il est également important de valider les entrées des utilisateurs pour s'assurer qu'elles contiennent les types de données attendus. Enfin, l'utilisation de frameworks ou de moteurs de templates qui gèrent l’échappement des sorties peut réduire les risques d'injection XSS. En appliquant ces bonnes pratiques, vous pouvez considérablement diminuer les risques de scripts malveillants sur votre site web.

## 7.4. Protection contre les injections SQL

Pour protéger nos applications contre les injections SQL, nous avons mis en place une stratégie qui inclut l'utilisation de la fonction `htmlspecialchars`. Cette fonction est essentielle, car elle convertit les caractères spéciaux des données utilisateur en entités HTML, réduisant ainsi le risque d'injection de code malveillant dans les requêtes SQL.

En remplaçant des caractères tels que les guillemets, les apostrophes et les signes inférieurs par leurs équivalents en entités HTML, nous empêchons le moteur SQL d'interpréter ces caractères de manière incorrecte. Ainsi, même si des données utilisateur contiennent des caractères potentiellement dangereux, ceux-ci seront considérés comme du texte ordinaire et non comme des éléments de syntaxe SQL.

Cette méthode constitue une mesure préventive efficace contre les attaques par injection SQL, renforçant ainsi la sécurité de nos applications et protégeant les données sensibles stockées dans nos bases de données contre les tentatives d'exploitation malveillante.