



**DOSSIER DE PROJET POUR  
LE TITRE PROFESSIONNEL DE  
DÉVELOPPEUR WEB & WEB MOBILE**

**Aicheche Chaima  
Juin 2022**

## **Table des matières**

Compétences du référentiel couvertes par le projet	3
Introduction	4
Résumé	5
Spécifications fonctionnelles	6
Description de l'existant	6
Périmètre du projet	6
Cible adressée par le site internet	6
Arborescence du site	6/7
Description des fonctionnalités	7
1. Authentification	7
2. Articles	7
3. Une page contact	7
4. Fonctionnalité de recherche	8
5. Espace parents	8
6. Back-office	8
7. Responsive	9
Spécifications techniques	10
- Choix techniques et environnement de travail	
- Technologies utilisées pour la partie front-end	
- Environnement de développement	
Réalisations	11
1. Charte graphique	11
2. Maquette	11
3. Conception de la base de données	12
Extraits de code	13
Veille sur les vulnérabilités de sécurité.	17
1. Exposition des données sensibles	
2. Injection SQL	
Jeu d'essai	20
Recherche effectuées à partir d'un site anglophone	22
ANNEXES	25
Site existant	
Maquette	25
Modèle conceptuel des données	26
Modèle logique des données	27
Trello	

### ***Compétences du référentiel couvertes par le projet***

Le projet couvre les compétences énoncées ci-dessous.

Pour l'activité 1, ***‘Développer la partie front-end d'une application web et web mobile en intégrant les recommandations de sécurité’***:

- Maquetter une application
- Réaliser une interface utilisateur web ou mobile statique et adaptable
- Développer une interface utilisateur web dynamique
- Réaliser une interface utilisateur avec une solution de gestion de contenu ou e-commerce

Pour l'activité 2, ***‘Développer la partie back-end d'une application web ou web mobile en intégrant les recommandations de sécurité.’***:

- Créer une base de données
- Développer les composants d'accès aux données
- Développer la partie back-end d'une application web ou web mobile
- Élaborer et mettre en œuvre des composants dans une application de gestion de contenu ou e-commerce.

## Introduction

J'ai intégré ma première année dans cette formation dans le but de préparer mon passage au titre professionnel (RNCP de niveau 5) de développeuse web et web mobile, à LaPlateforme\_ Marseille.

Ayant pour objectif de me présenter à ce titre professionnel, de proposer un support de lecture complet et d'acquérir les compétences professionnelles requises pour, j'ai travaillé sur le développement d'un site permettant l'ajout d'articles avec des images et un module de connexion inscription.

Le projet que je vous présente dans ce dossier a été une première expérience dans le monde professionnel dans le développement web et web mobile. En effet, devoir élaborer un site web complet en commençant par le maquettage, la rédaction du cahier des charges, ensuite passer à la conception de la base de données et au développement. Tout en ayant un lien direct avec un client, devoir l'informer des avancées, mettre en place des réunions pour faire valider les modifications.

## Résumé

Kalliste La Graniere est un centre social à but non lucratif, il favorise la participation des habitants à la vie sociale notamment en organisant des comités d'usagers regroupant tous les secteurs d'activités de la structure et les partenaires institutionnels et associatifs...

Le centre social met en place de nombreuses actions à caractère social et/ou éducatif et visant des publics différents.

Les contenus de ces actions sont élaborés avec les partenaires du quartier.

Actuellement le site internet permet de contacter le centre, de voir quelques activités proposées et les différents secteurs.

Le logiciel wordpress est utilisé pour la mise en forme du site.

Des locaux associatifs sont affiliés au centre, sans site internet. (voir annexe)

Après avoir échangé avec le directeur sur leurs difficultés à gérer le site internet, nous avons convenu de le rendre plus dynamique et à leur image. Le manque de moyens financiers ne leur permet pas de créer un nouveau site web pour les locaux associatifs.

Mon projet consiste donc à relier le site déjà existant au nouveau, que je vais réaliser.

Le site va permettre de recenser toutes les activités et autres proposées par les locaux associatifs. Je vais réaliser un module d'inscription et de connexion pour que les membres puissent s'inscrire et se connecter sur le site. Les parents ayant des enfants qui font partie de l'association auront accès à une page avec des images et vidéos des activités.

## ***Spécifications fonctionnelles***

### ***Description de l'existant***

Le centre social ne possède pas les compétences pour améliorer le site internet déjà existant, ni d'en créer un nouveau pour les locaux associatifs.

Lors de nos différents entretiens nous avons convenu :

- quels étaient les besoins du centre,
- les fonctionnalités du site internet
- l'aspect graphique du site internet.
- la création d'un site internet pour les locaux associatifs reliait au site déjà existant.

### **Périmètre du projet**

Le site sera réalisé en français et ce dernier devra être accessible sur différents

supports, à savoir mobile, tablette et ordinateur.

### **Cible adressée par le site internet**

Le site s'adresse aux habitants du quartier, aux partenaires et aux associations.

### **Arborescence du site**

L'arborescence du site se décline comme suit :

- Page d'accueil
- Page connexion
- Page inscription
- Page activités

- Page produit
- Page associatives et sociales
- Page pour l'emploi
- Page contact
- Page A propos

La partie back-office est également prévue, elle permet la gestion du site, grâce à l'administrateur.

## **Description des fonctionnalités**

### **1.Authentification**

L'utilisateur pourra s'inscrire et se connecter grâce à un formulaire. Ensuite l'administrateur pourra lui attribuer un droit.

### **2.Articles**

Cette page va permettre d'afficher un article, son titre, sa description et une image.

Les articles seront triés par catégories chacun sur un onglet approprié. Un filtre doit être implémenté afin de trier les articles en fonction de leur catégorie.

### **3. Une page contact**

Cette page sera reliée au site déjà existant. Elle va permettre aux utilisateurs de contacter le centre grâce à un formulaire.

### **4. Fonctionnalité de recherche**

Le client devra être en mesure d'effectuer une recherche d'articles dans un champ prévu à cet effet. Afin de faciliter la recherche, un système de recherche doit être mis en place.

## 5.Espace parents

L'espace parents permet aux parents ayant inscrit leurs enfants à des activités ou ayant eux mêmes participer à des activités avec le centre, de consulter des photos ou vidéos prises lors des activités.

## 6.Back office

Le gérant du site devra avoir accès à un espace sécurisé lui permettant d'administrer le site.

### 6.1 Ajout des catégories

L'administrateur sera en mesure de gérer les catégories c'est-à-dire créer des catégories et les supprimer.

### 6.2 Gestion des articles

L'administrateur aura également la capacité de créer des articles et de les supprimer.

Lors de la création d'article, ce dernier sera en mesure de:

- Donner un titre à l'article
- L'article
- Uploader une ou plusieurs images



## 7. Responsive design

Afin de faciliter l'**adaptation de l'application web aux tablettes et mobiles**, j'ai utilisé des **display flex** pour composer les pages et l'ensemble des ses éléments. Je définis également la taille des éléments en pourcentage pour que celle-ci s'adapte le plus possible.

J'ai utilisé l'inspecteur de Chrome afin de pouvoir visualiser l'application sur les différents formats d'écran. En fonction de la taille de l'écran j'ai modifié les dimensions et la disposition des différents éléments de chaque page avec les **Media Queries**.

J'ai changé le type de **mise en page en fonction de la taille de l'écran**. Au lieu d'avoir une seule mise en page pour toutes les tailles d'écran, la mise en page est modifiée. Les éléments sont repositionnés, les typographies réduites, les images redimensionnées pour les écrans plus petits.

## Spécifications techniques

Choix techniques et environnement de travail

Technologies utilisées pour la partie back-end :

- Le projet sera réalisé avec le langage PHP
- Base de données SQL

Technologies utilisées pour la partie front-end:

- Le projet sera réalisé avec du HTML et CSS.
- Et enfin Javascript afin de dynamiser le site et d'améliorer l'expérience utilisateur.

L'environnement de développement est le suivant:

- Editeur de code: Visual Code
- Outil de versioning: GIT, Github.
- Maquettage: Figma
- MCD MLD MPD : Lucidchart

Afin d'optimiser mon organisation, j'ai utilisé Trello afin de découper le projet en plusieurs tâches à réaliser et de définir leur ordre de priorité. (voir annexe)

Trello m'a permis de montrer mon avancée à mon client, et de me mettre à la place d'un utilisateur afin de créer les pages nécessaires et une navigation fluide.

## Réalisations

### 1. Charte graphique

En ce qui concerne la charte graphique je devais respecter celle déjà existante.



La couleur dominante est la suivante :

- #E2001A
- #454545
- #666666

### 2. Maquette

La maquette a été réalisée avec le logiciel gratuit Figma.

Devant respecter la charte graphique du site existant je devais réaliser le même header, respecter les couleurs ainsi que la disposition des éléments. Il fallait rendre les pages plus attrayantes et plus faciles à visiter.

Je me suis donc inspirée du site existant pour réaliser la maquette du futur site internet.

Vous trouverez la maquette dans les annexes du dossier.

### 3. Conception de la base de données

Les données du premier site n'étaient stocker nul part, j'ai développé donc une base de données :

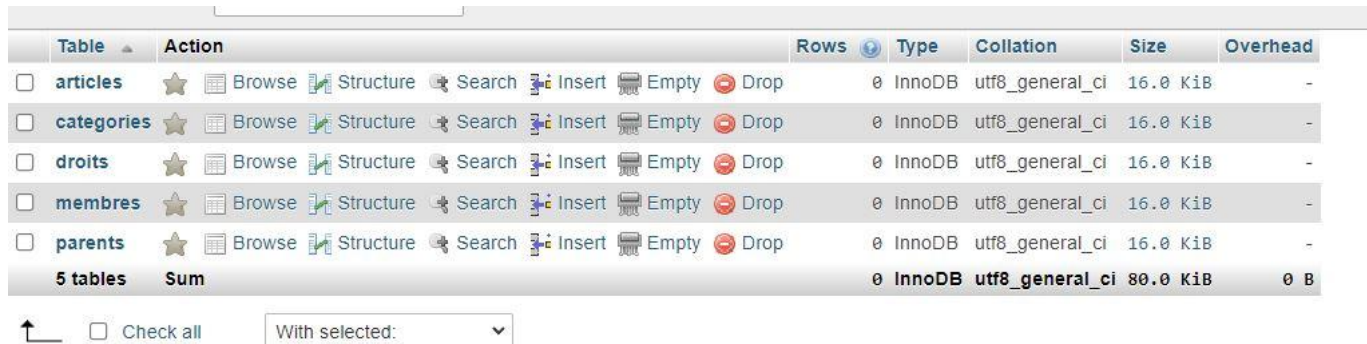


Table	Action	Rows	Type	Collation	Size	Overhead
<input type="checkbox"/> articles	★ Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_general_ci	16.0 KiB	-
<input type="checkbox"/> categories	★ Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_general_ci	16.0 KiB	-
<input type="checkbox"/> droits	★ Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_general_ci	16.0 KiB	-
<input checked="" type="checkbox"/> membres	★ Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_general_ci	16.0 KiB	-
<input type="checkbox"/> parents	★ Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_general_ci	16.0 KiB	-
5 tables	Sum	0	InnoDB	utf8_general_ci	80.0 KiB	0 B

↑ ☐ Check all With selected: ▼

Comme illustré ci dessus, on peut voir que la base de données s'articule autour de 4

tables. Dans un premier temps, la table membres qui permet d'identifier les utilisateurs inscrits. Cette table est liée à la table droits, qui va permettre de donner un droit spécifique à chaque membre lors de son inscription.

Il y a ensuite la table article qui va regrouper toutes les informations sur chaque article publié. Elle va être reliée à la table catégories. Cette dernière table va permettre à l'administrateur de choisir dans quelle catégorie publier chaque article.

Vous trouverez également dans les annexes le modèle conceptuel de données ainsi que le modèle logique de données.

Modèle conceptuel de données : Il s'agit d'une représentation des données, facilement compréhensible, permettant de décrire le système d'information à l'aide d'entités.

Modèle logique de données : Il s'agit donc de préciser le type de données utilisées lors des traitements. Ainsi, le modèle logique est dépendant du type de base de données utilisé.

## Extrait de code

### PDO et gestion des requêtes en BDD

Toutes les requêtes en base de données sont gérées par la class `Config`. Cette classe permet d'exécuter des requêtes préparées. L'utilisation de requêtes préparées, rendues possibles grâce à l'extension PDO, présentent un double avantage par rapport à l'exécution directe de requêtes SQL. Premièrement, peu importe le nombre d'exécution des requêtes, je n'ai besoin de les préparer qu'une seule fois pour qu'elles soient réutilisables à volonté avec des paramètres identiques ou différents. Deuxièmement et non des moindres, elles présentent un avantage majeur en termes de sécurité notamment pour prévenir des injections SQL. Les requêtes étant pré-formatées, elles empêchent le passage de code malicieux en paramètre, je n'ai donc pas besoin de protéger les paramètres ou valeurs manuellement.

```
<?php
class Config
{
```

Concernant la connexion à la base de données j'ai procédé de la manière suivante. J'ai utilisé un “**try and catch**” la fonction php qui gère les erreurs. La gestion d'une erreur via une exception se fait en deux temps.

J'ai utilisé un bloc try dans lequel le code qui peut potentiellement retourner une **erreur** va être exécuté. On crée à l'intérieur une nouvelle connexion grâce à l'objet **new PDO**.

Je créer un bloc catch dont le but va être d'attraper l'exception si celle-ci a été lancée et de définir la façon dont doit être gérée l'erreur. La fonction est appelée dans les autres classes afin de réaliser différentes requêtes.

```
<?php
```

```

class Config
{
    protected $bdd;
    public function __construct()
    {

        try {
            $this->bdd = new PDO(
                'mysql:host=localhost;dbname=kalliste',
                'root', 'root');
        } catch (Exception $e) {
            // En cas d'erreur, on affiche un message et
            on arrête tout
            die('Erreur : ' . $e->getMessage());
        }
        return $this->bdd;
    }
}

```

Grâce au principe d'héritage de la programmation orientée objet de PHP, je fais hériter cette class Bdd à toutes mes autres classes qui ont besoin d'une connexion à la base de données pour ne pas répéter mon code, et pouvoir réaliser différentes requêtes.

```

class Droits extends Config
{
    public function alerts()

```

### Espace administrateur

Afin de pouvoir se connecter et accéder à son espace, l'administrateur devra s'inscrire. Pour cela il devra choisir un **login** et un **mot de passe**, si le login choisi est déjà pris l'inscription sera impossible. J'ai également utilisé une expression

régulière **REGEX** pour qu'il soit obligé de choisir un mot de passe de minimum 8 caractères contenant une majuscule, une minuscule, un chiffre et un caractère spécial.

```
if ($email != htmlspecialchars('admin@gmail.com')) &&
$password == $passwordverify) {
    if
(preg_match('#^(?=.*[A-Z])(?=.*[a-z])(?=.*\d)(?=.*[-+!*$@%_]) ([-+!*$@%_
\w]{8,35})$#', $password)) {
        $password = hash('sha512', $password);
```

## Faible upload

La faille upload est une faille permettant d'uploader des fichiers avec une extension non autorisée, cette faille est due à la mauvaise configuration du script d'upload ou à l'absence complète de sécurité. Celle-ci est généralement présente dans les scripts d'upload d'images.

La vulnérabilité est due au mauvais contrôle des entrées de l'utilisateur, alors qu'il suffit de vérifier si le type/Mime du fichier uploadé correspond bien à une image JPEG ou PNG en utilisant le code suivant par exemple:

```
if(preg_match("#jpeg|png#",$_FILES["image"]["type"]))
    // Accépter l'upload
else
    echo "Format du fichier invalide.";
```

Il faut également penser à isoler les fichiers chargés dans un dossier à part pour minimiser les risques de rebond au cas où il s'agit d'un fichier malveillant. Renommer les fichiers chargés sera aussi d'une grande utilité car le pirate aura du mal à appeler son fichier s'il ne connaît pas son chemin et son nom.





## Veille sur les vulnérabilités de sécurité

La veille en vulnérabilités est la méthode la plus efficace. Elle consiste à suivre quotidiennement la découverte de nouvelles failles de sécurité, mais surtout elle s'inscrit dans un processus global : détection, alerte, remédiation et suivi.

Lorsqu'on est sur internet il faut éviter d'exposer les données sensibles en transit pour cela il faut dans un premier temps utiliser le HTTPS, même sans données sensibles. HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable.

Ensuite il faut utiliser les requêtes GET pour récupérer les informations et POST pour modifier les informations.

```
align="center" >  
    <form class="forms" method="POST">  
        <?php if (isset($_POST['connexion'])) {  
  
1 <form action="contact.php" method="GET">
```

Afin que les cookies soient transmis par l'en-tête et via HTTPS il faut les sécuriser. En ajoutant une date d'expiration, en sécurisant l'ID et en ne mettant pas l'ID dans l'URL, les sessions sont sécurisées.

Lors d'une inscription, l'utilisateur entre un mot de passe qui est par la suite stocké dans la base de données. Il faut le protéger pour cela on utilise le hachage de mot de passe.

Le hachage de mot de passe permet de chiffrer de manière irréversible les mots de passe via une fonction de hachage cryptographique.

```
$hash = password_hash($password, PASSWORD_DEFAULT);
```

La faille SQL est un groupe de méthodes d'exploitation de failles de sécurité d'une application interagissant avec une base de données. Elle permet d'injecter dans la requête SQL en cours un morceau de requête non prévu par le système et pouvant compromettre la sécurité.

Ce type d'attaque s'effectue généralement grâce aux champs présents dans les formulaires.

Dans le cas d'une attaque par injection SQL, au lieu de mettre un nom d'utilisateur et un mot de passe sur une page de connexion, un utilisateur malveillant entrera des données directement interprétées par le moteur SQL, ce qui lui permettra de modifier le comportement de votre application.

#### Exemple : accès grâce à une saisie utilisateur insuffisamment masquée.

Afin d'accéder à une base de données, un utilisateur doit tout d'abord s'authentifier. A cette fin, des scripts existent qui présentent par exemple un formulaire login avec nom d'utilisateur et mot de passe. L'utilisateur remplit le formulaire et le script vérifie si une entrée correspondante existe dans la base de données. En règle générale, les bases de données se présentent sous forme de tableau avec les colonnes « utilisateur » ainsi que « nom d'utilisateur » et « mot de passe ». Pour importer l'application Web, les lignes de script (pseudo-code) pour l'accès au serveur Web peuvent être les suivantes :

```
nom = request.POST['username']
passwd = request.POST['password']

sql = "SELECT id FROM utilisateur WHERE username='" + nom + "' AND password='" + passwd + "'"
database.execute(sql)
```

Un attaquant a maintenant la possibilité de manipuler le champ relatif au mot de passe grâce à une injection SQL, en entrant par exemple password' OR 1='1, ce qui mène à la requête SQL suivante :

```
sql = "SELECT id FROM utilisateur WHERE username='' AND password='password' OR 1='1'
```

En agissant ainsi, il peut accéder à l'ensemble des tables utilisateurs de la base de données, le mot de passe étant toujours valide (1='1'). S'il se connecte en tant qu'administrateur, il peut procéder à toutes les modifications qu'il désire. Autrement, c'est le champ « nom d'utilisateur » qui peut être également manipulé de cette manière.

Pour s'en protéger, il faut limiter ce que l'utilisateur peut mettre dans la zone de texte. Cela n'empêchera pas l'injection, mais c'est une mesure que vous pouvez mettre en place pour limiter des attaques de base. En effet, les caractères spéciaux spécifiques à certains langages ne pourront pas être utilisés.

Par exemple, la contrainte password s'assure que la valeur est bien un password valide.

```
<input class="input-field" type="password" name="password" placeholder="Mot de passe" required>
</div>
```

Pour prévenir les injections SQL, il faut faire appel aux requêtes préparées. Ce sont des requêtes dans lesquelles les paramètres sont interprétés indépendamment de la requête elle-même. De cette manière, il est impossible d'effectuer des injections.

Dans tous les systèmes de gestion de bases de données, deux méthodes sont utilisées : `prepare()` qui prépare la requête et `execute()` qui exécute la requête avec les paramètres.

```
public function getCategories()
{
    $check = $this->bdd->prepare("SELECT * FROM `categories`");
    $check->execute();
    $res = $check->fetchAll(PDO::FETCH_ASSOC);
}
```

d'autres failles existent tels que :

- Faille xss
- L'Upload

- Dépassement de mémoire tampon ou buffer overflow

Consiste en une corruption de la mémoire de la pile des appels. La plupart du temps, le programme va planter, mais ceci ouvre aussi une porte au hacker qui veut contrôler un processus à distance.

- Injection de commandes

Consiste à exécuter des commandes systèmes non autorisées sur le système d'exploitation d'une victime via une application vulnérable.

- Désérialisation non sécurisée (Insecure Deserialisation)

Permet à un utilisateur malveillant d'accéder et de modifier les fonctionnalités de l'application ciblée.

- Utiliser un logiciel ou des composants présentant des vulnérabilités

Lorsqu'une faille est découverte, les développeurs de l'application en question proposent généralement un patch qui permet de corriger le problème.

## Jeu d'essai

Par exemple, je vais utiliser mon formulaire d'inscription et vous montrer tout ce qui se passe au niveau du côté client et du côté serveur lorsqu'un utilisateur veut s'inscrire sur mon site.

Lors de l'inscription d'un membre, il doit remplir plusieurs informations dans le formulaire de la page inscription, toutes ces informations sont ensuite récupérées à travers `$_Post` et stockées dans des variables.

Dans le back, je vais dans un premier temps afin de me connecter à ma base de données faire un require de ma class config, ensuite j'étends ma class config à ma class utilisateur qui va hériter des fonctions de cette dernière.

J'affiche le formulaire, une fois rempli, il est traité.

L'utilisateur clique sur "S'inscrire", je demande donc si les champs sont définis avec "isset". Si par exemple le champ nom est vide, on arrête l'exécution du script et on affiche un message d'erreur.

Si le champ nom est renseigné mais ne convient pas au format qu'on souhaite qu'il soit, soit: que des lettres minuscule + des chiffres

Un message d'erreur s'affiche si le pseudo est trop long (dépassé 25 caractères), on vérifie que le nom n'est pas déjà utilisé par un autre membre.

```
public function Register($nom, $email, $password, $passwordverify)
{
    $req = $this->bdd->prepare("SELECT * FROM `utilisateurs` WHERE
nom= ?");
    $req->execute(array($email));
    $res = $req->fetchAll(PDO::FETCH_ASSOC);
```

Ce code me permet de récupérer toutes les informations dans la base de données et de vérifier avec l'email qu'il n'existe pas déjà.

Une fois toutes les vérifications faites, on passe à l'enregistrement dans la base de données.

Je crypte le mot de passe et une fois inscrit, le formulaire n'est plus affiché.

Les balises <form> sert à dire que c'est un formulaire ,je lui demande de faire fonctionner la page inscription.php une fois le bouton "S'inscrire" cliquer, je lui dit également que c'est un formulaire de type "POST"

Les balises <input> sont les champs de formulaire type="text" sera du texte type="password" sera des petits points noir (texte caché) type="submit" sera un bouton pour valider le formulaire name="nom de l'input" sert à le reconnaître une fois le bouton submit cliqué, pour le code PHP.

une fois qu'on a vérifié que le nom n'existe pas dans la base de données et respecte les conditions et que le mot de passe est bien crypté on peut les envoyer dans la base de données.

Pour les envoyer dans la base de données je fais une requête préparer

```
$req = $this->bdd->prepare("INSERT INTO
`utilisateurs`(`nom`,`prenom`,`mail`,`password`) values (:nom, :prenom,
:email, :password)");
    $i=$req->execute(array(
        ':nom' => $nom,
        ':email' => $email,
        ':password' => $password,
    ));
```

## Recherche effectuées à partir d'un site anglophone

En ce qui concerne ma recherche à partir d'un site anglophone, lors de la réalisation de mon header je devais mettre en place un button burger. Pour cela j'ai effectué une recherche sur google 'button burger in css & html'.

---

If you are looking for a more complete example of how a CSS hamburger menu can be useful, this CodePen renders an example website to showcase the use of the CSS hamburger menu.

It only uses pure HTML and CSS, so it is easy to learn from and understand what is happening. The menu icon is animated and transforms into a cross when the menu is open.

The menu itself slides out from the slide and overlays the main website. As this design is responsive, it will automatically hide the header menu and make the burger menu available once the screen width decreases.

### Traduction :

Le code présenté utilise uniquement du HTML et du CSS, l'icône du menu est animée et se transforme en croix lorsque le menu est ouvert.

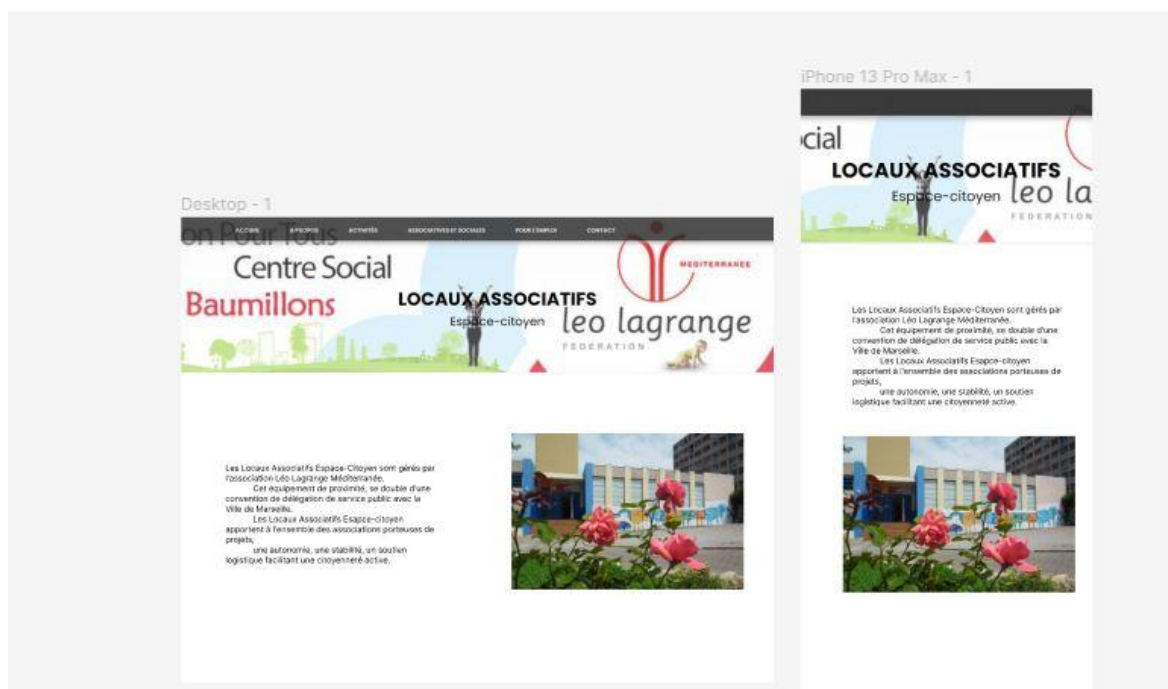
Le menu lui-même glisse hors de la diapositive et recouvre le site Web principal. Comme cette conception est réactive, elle masque automatiquement le menu d'en-tête et rend le menu burger disponible une fois que la largeur de l'écran diminue.

Ce site m'a permis de réaliser un burger button responsive avec des lignes alignées. ( voir annexe )

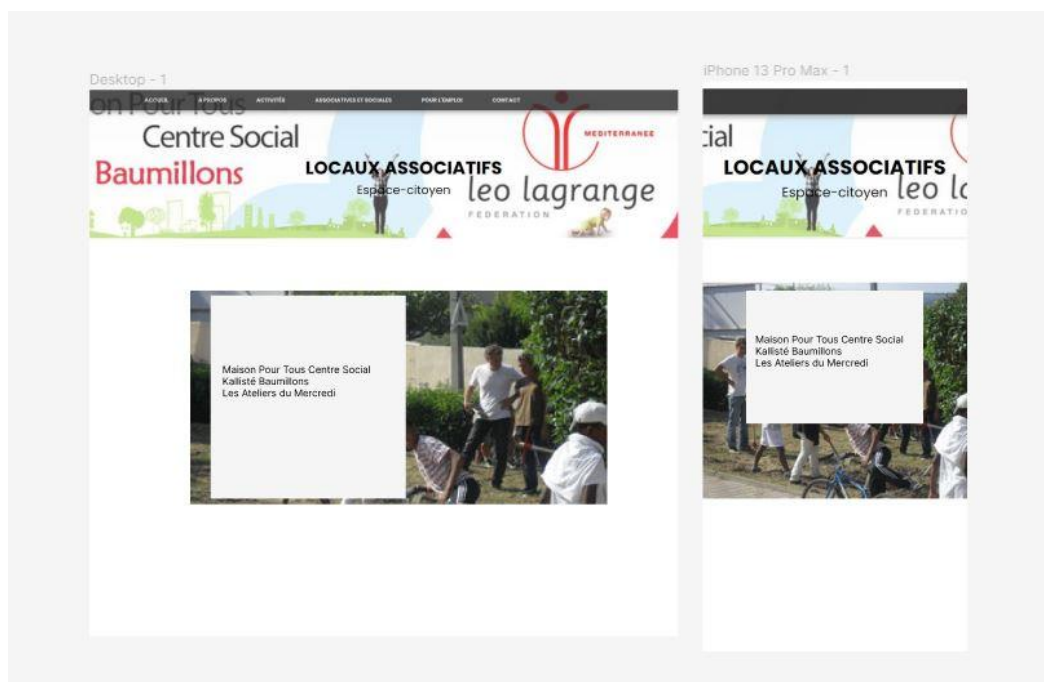
## ANNEXES

Maquette :

Page accueil

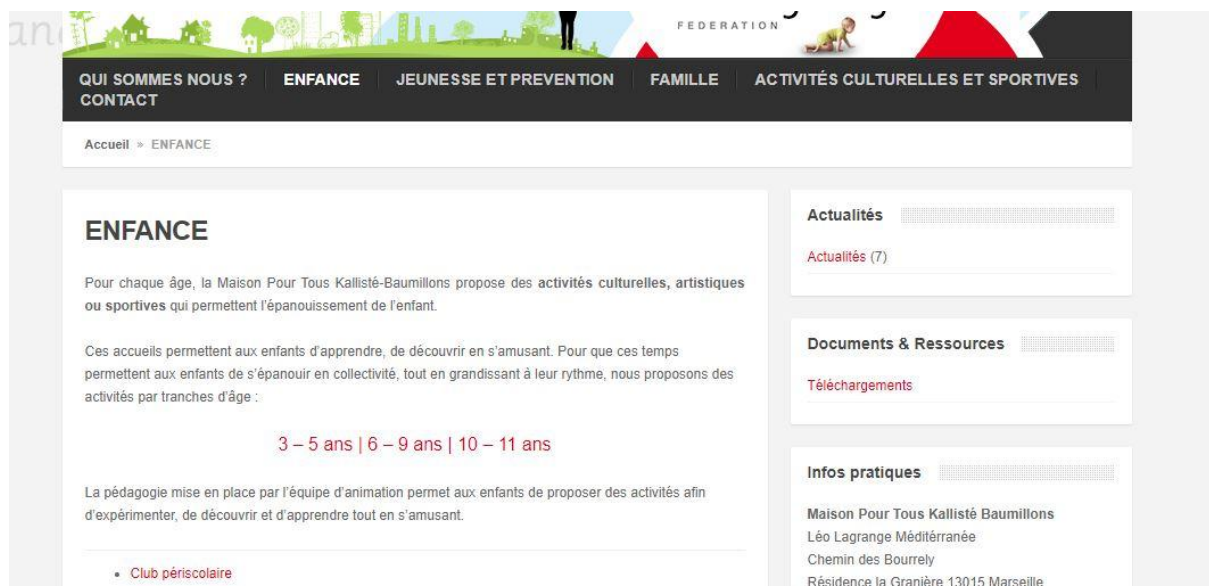


Page articles



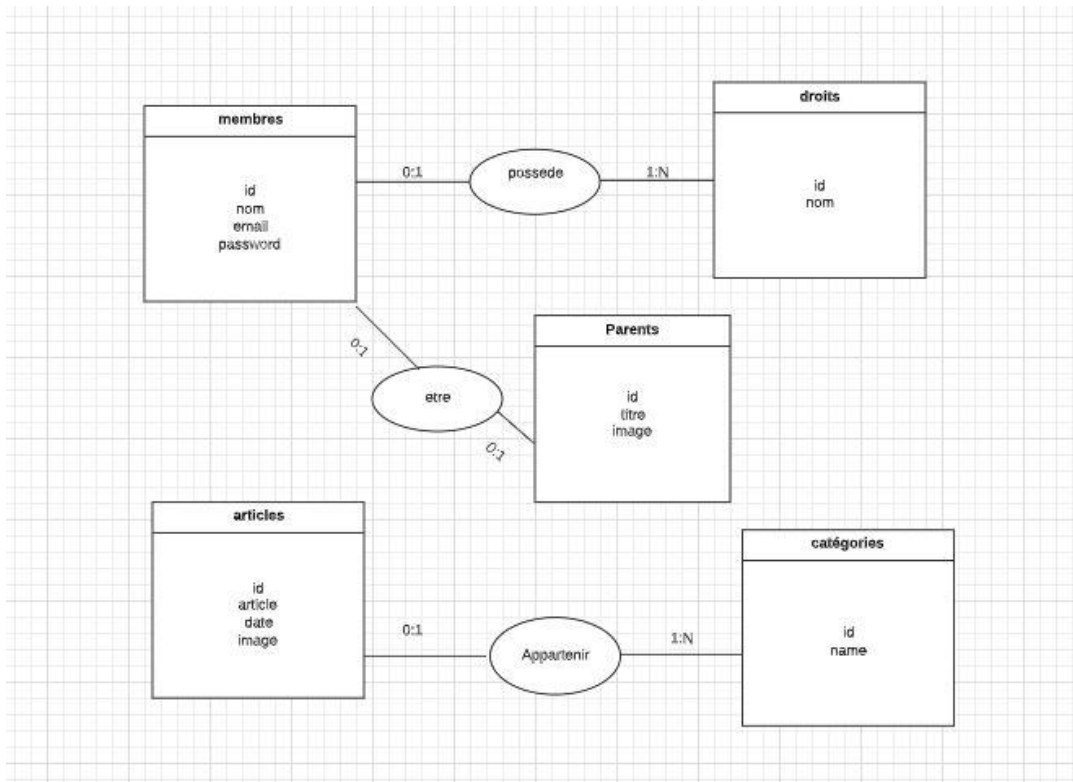


Site déjà existant :

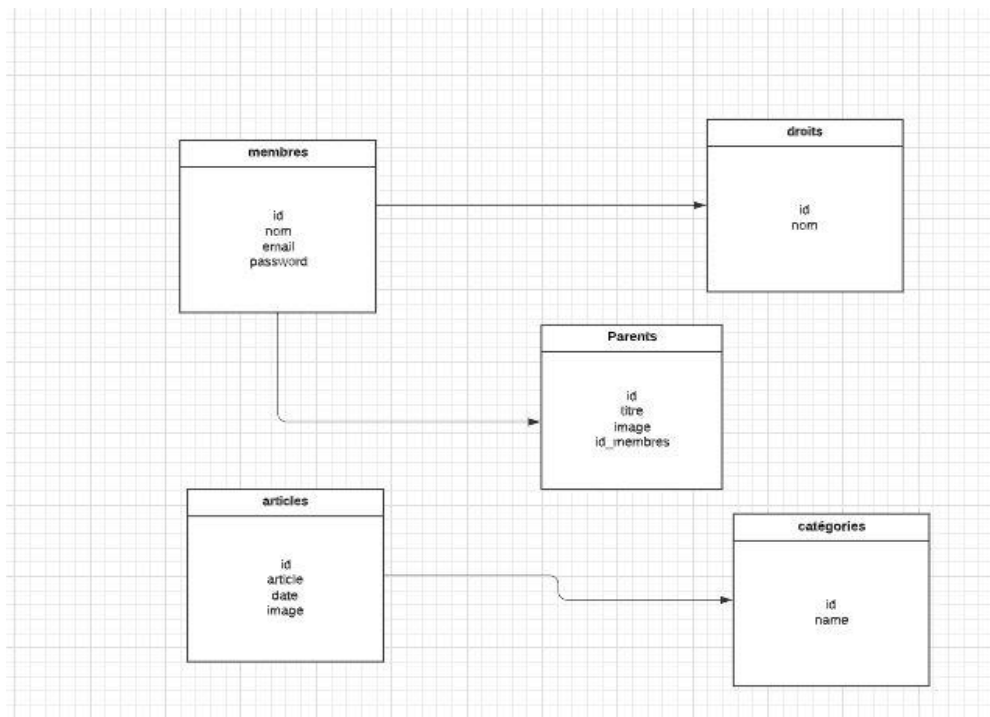


## Conception de la base de données

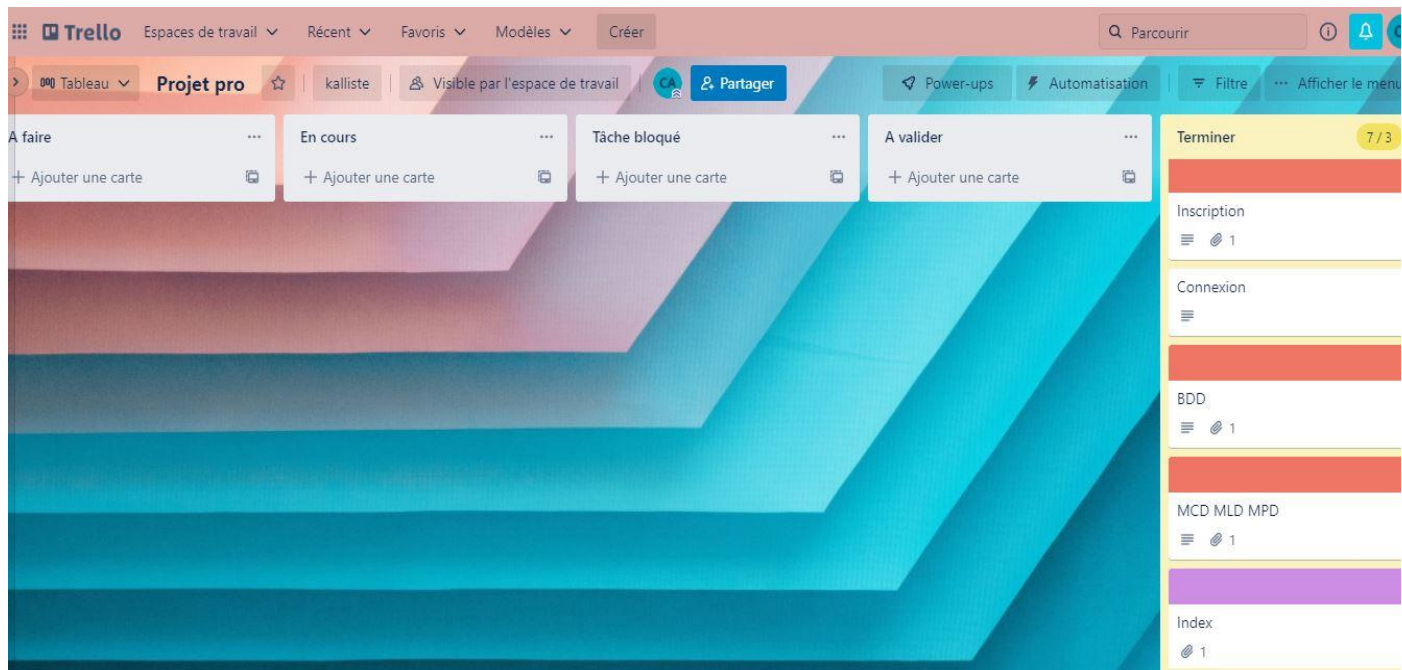
### Mcd



### Mld



Trello :



Button burger :

