

# Dossier Projet

## My Cave

Septembre 2021

Réalisation par : Granier G rald





## **Le dossier de projet respecte ce plan type :**

- Liste des compétences du référentiel qui sont couvertes par le projet.
- Résumé du projet en français d'une longueur d'environ 20 lignes.
- Cahier des charges, expression des besoins, spécifications fonctionnelles du projet.
- Spécifications techniques du projet.
- Réalisation et extrait de code significatif avec argumentation.
- Présentation du jeu d'essai, fonctionnalité la plus représentative.
- Description de la veille durant le projet, sur les vulnérabilités de sécurité.
- Description d'une situation de travail ayant nécessité une recherche à partir d'un site anglophone. Extrait du site anglophone, utilisé dans le cadre de la recherche décrite précédemment et sans traducteur automatique.

## Table des matières

1. Liste des compétences du référentiel qui sont couvertes par le projet.	p 5
1.1 Développer la partie front-end d'une application web ou web mobile en intégrant les recommandations de sécurité.	p 5
1.1.1 Maquetter une application.	p 5
1.1.2 Développer une interface utilisateur web dynamique.	p 6
1.1.3 Réaliser une interface utilisateur web et web mobile.	p 7
1.2 Développer la partie back-end d'une application web ou web mobile en intégrant les recommandations de sécurité.	p 8
1.2.1 Créer une base de données.	p 8
1.2.2 Développer des composants d'accès aux données.	p 9
1.2.3 Développer la partie back-end d'une application.	p 10
2. Résumé du projet.	p 12
3. Cahier des charges, spécifications fonctionnelles du projet.	p 12
4. Spécifications techniques du projet.	p 15
5. Réalisation et extrait de code.	p 17
6. Présentation du jeu d'essai, fonctionnalité la plus représentative.	p 20
7. Description de la veille durant le projet, sur les vulnérabilités de sécurité.	p 25
8. Description d'une situation de travail ayant nécessité une recherche à partir d'un site anglophone.	p 26
9. Conclusion	p 29

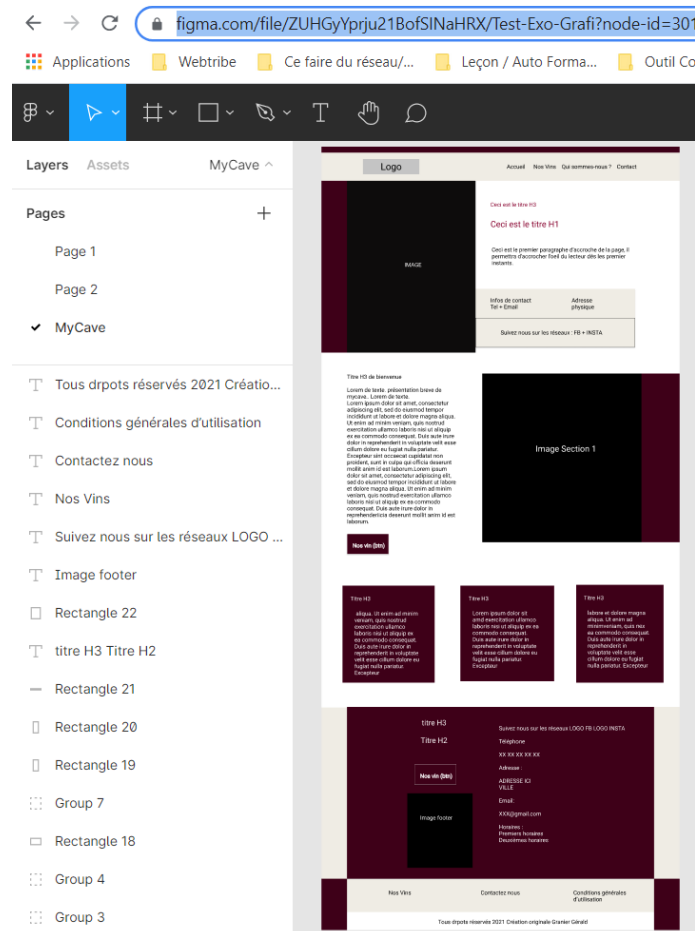
# 1. Liste des compétences du référentiel qui sont couvertes par le projet

## 1.1 Développer la partie front-end d'une application web ou web mobile en intégrant les recommandations de sécurité

### 1.1.1. Maquetter une application

Afin de maquetter mon application j'ai utilisé le logiciel gratuit Figma. Figma est un outil collaboratif de création d'interface disponible à la fois en version web ou desktop.

Son interface rappelle beaucoup celle de Adobe XD, la majeure partie du travail consiste à superposer des calques afin de déposer chaque élément à l'endroit où l'on souhaite le mettre. La courbe de progression sur ce logiciel est très rapide et permet de vite obtenir des résultats satisfaisants d'un point de vu visuel (voir ci-dessous).






### 1.1.2. Développer une interface utilisateur web dynamique

Une interface web dynamique présente de nombreux avantages, le principal étant qu'elle permet à l'utilisateur une expérience de navigation accrue.

Le langage PHP permet de manipuler des données, des tableaux pour pouvoir ensuite les afficher suivant ce que l'utilisateur insert via les formulaires.

Dans mon cas, cela permettra d'afficher les bouteilles de vins que le gérant vend dans sa boutique physique.

Pour ce projet, j'ai utilisé du PHP, du Javascript, et du CSS (explication page 15).

DOMAINE DU BOUSCAT	LAN RIOJA CRIANZA	CHATEAU LE DOYENNE
Année : 2009	Année : 2006	Année : 2005
Sépage : Merlot	Sépage : Tempranillo	Sépage : Merlot
Pays : France	Pays : Spain	Pays : France
Région : Bordeaux	Région : Rioja	Région : Bordeaux
Description : La couleur dorée claire de ce vin dément la saveur vive qu'il détient. Véritable vin d'été, il invite à un pique-nique dans un vignoble ensoleillé.	Description : A resurgence of interest in boutique vineyards has opened the door for this excellent foray into the dessert wine market. Light and bouncy, with a hint of black truffle, this wine will not fail to tickle the taste buds.	Description : Though dense and chewy, this wine does not overpower with its finely balanced depth and structure. It is a truly luxurious experience for the senses.
		

Le gérant de MyCave peut se connecter grâce à une interface de connexion pour rajouter des bouteilles :

**Se connecter :**

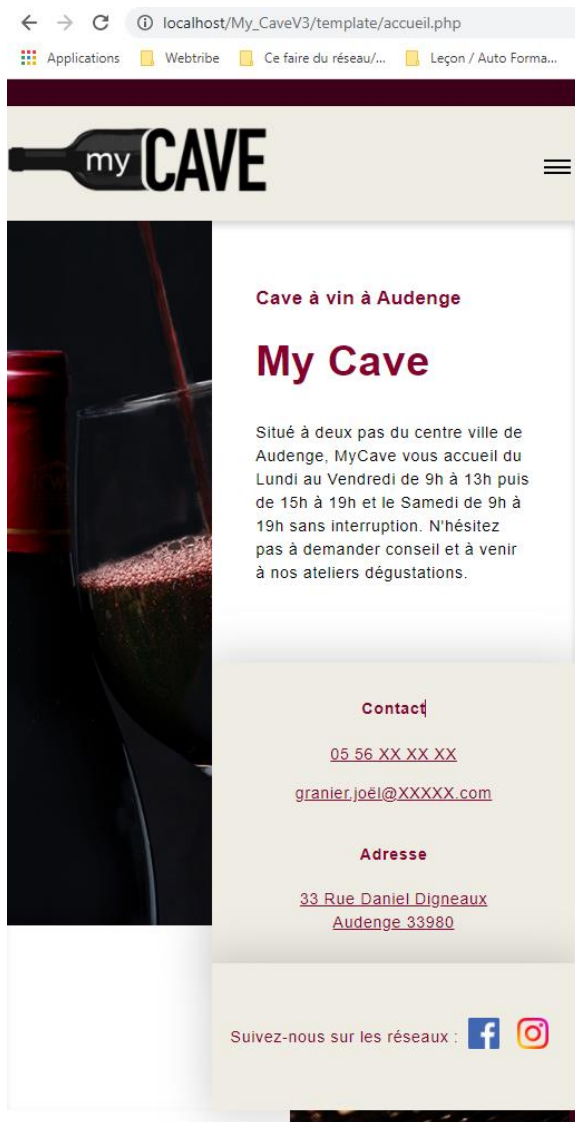
Pseudo

Email

Mot de passe

Se connecter

### 1.1.3. Réaliser une interface utilisateur web mobile et adaptable



De nos jours, ne pas faire d'interface responsive n'est pas envisageable. Voici quelques chiffres qui prouvent l'importance de réaliser des interfaces adaptables :

- L'année dernière, le trafic Internet mondial via ordinateur a représenté moins de 43 %, contre 55,35 % pour les appareils mobiles (+11 % par rapport à 2020).
- D'ici 2022, les mobiles devraient atteindre 59 % du trafic Internet mondial.
- En 2021, les appareils connectés sont au nombre de 11,7 milliards dans le monde.

Par conséquent, à travers ce projet fait en CSS, je privilégie un maximum les propriétés Flexbox car cela permet facilement de faire des interfaces adaptables. Je factorise et ré-utilise le plus possible mes classes pour avoir un code plus léger. Je fais bien attention sur chaque unité de mesure, j'utilise si possible des unités relatives qui s'adapte à la taille de l'écran. Il y a aussi un menu burger pour un

gain de place et une meilleure expérience utilisateur. (Screenshot avec dézoom de 80%).

```
/*=====VARIABLE=====*/
:root {
  --primary-color: #3e0018;
  --secondary-color: #88002d;
  --third-color: #885c7e;
  --bckg-color: white;
  --txt-color: black;

  --dark-color: black;
  --light-color: white;
  --lightSecond-color: rgb(239, 236, 228);

  --GapPageRightLeft: 8%;
}

@media screen and (max-width: 1095px) {
  :root {
    --GapPageRightLeft: 6%;
  }
  body {
    font-size: 17px;
  }
}
```

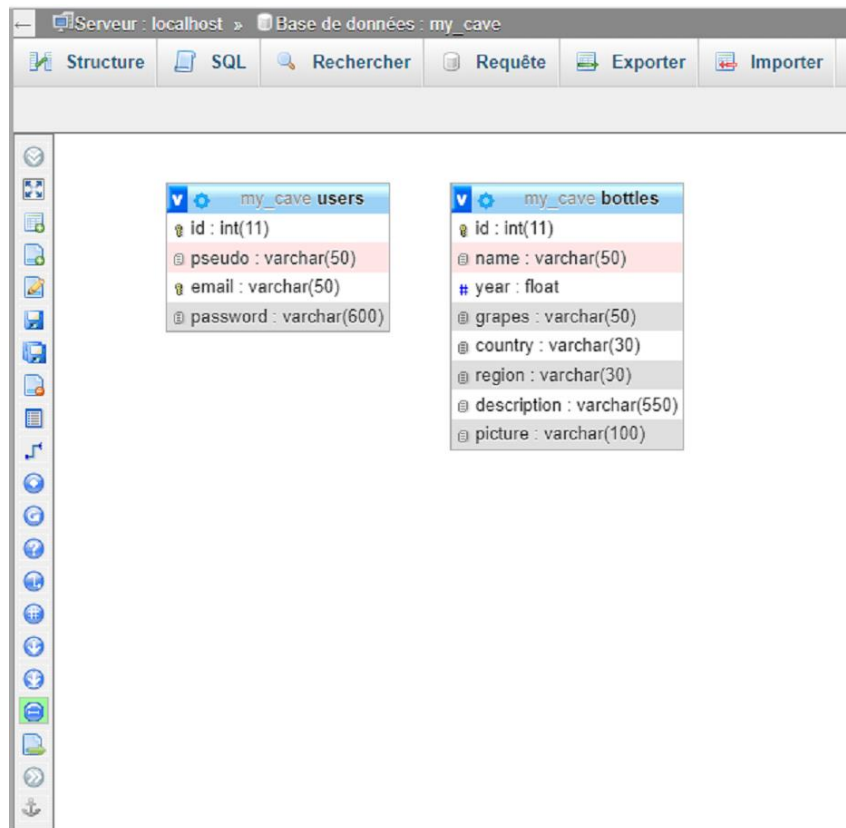
Mon fichier CSS contient une variable GapPageRightLeft qui correspond à la marge du site. Il est effectué en pourcentage pour être adaptable et j'effectue des media Queries pour baisser ce pourcentage suivant la résolution.

```
header {
  padding-left: var(--GapPageRightLeft);
  padding-right: var(--GapPageRightLeft);
}
```

## 1.2. Développer la partie back-end d'une application web ou web mobile en intégrant les recommandations de sécurité

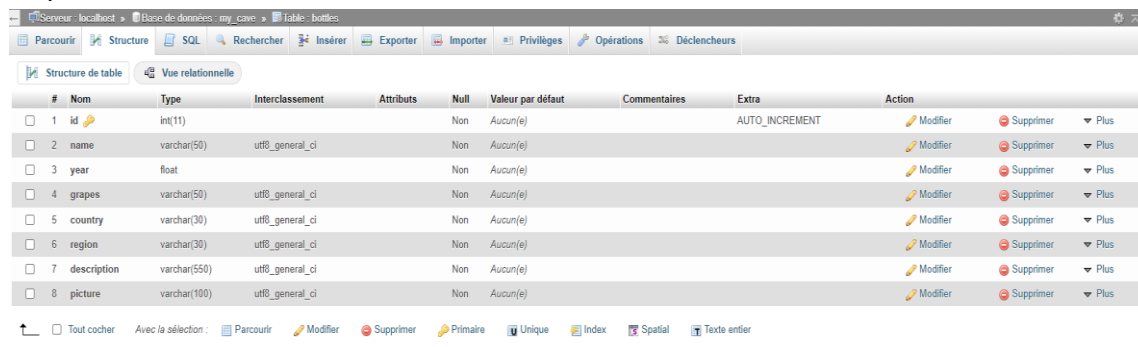
### 1.2.1. Créer une base de données

Création d'une base de données avec 2 tables.



Il s'agit des 2 tables utilisées pour le projet My\_Cave : une table contenant les utilisateurs, et une autre contenant les bouteilles du site. Les données sont modifiables grâce au CRUD en Php.

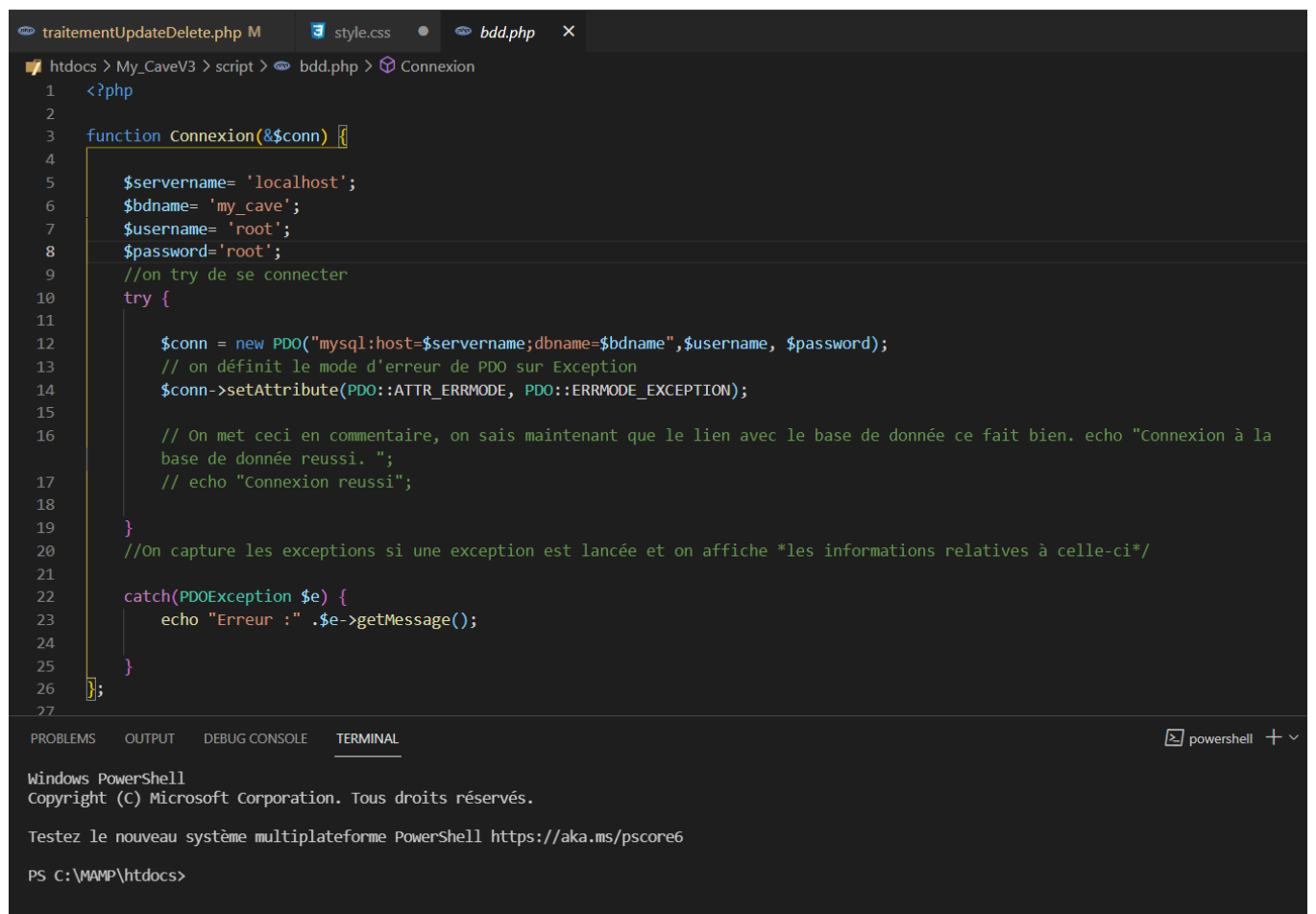
La base de données est créée sur PhpMyAdmin. Il est possible de créer des tables avec des requêtes SQL ou via les formulaires de cette interface.





Après ceci, je n'oublie pas d'exporter les données et de les sauvegarder dans mon dossier du projet. Je crée un dossier et j'insère mes 2 fichiers users.sql et bottles.sql. Si un crash ou un problème de base de données intervient cela me permet d'avoir une sauvegarde et de pouvoir la recréer à l'identique.

### 1.2.2. Développer des composants d'accès aux données



```
traitementsUpdateDelete.php M style.css bdd.php X
htdocs > My_CaveV3 > script > bdd.php > Connexion
1 <?php
2
3 function Connexion(&$conn) {
4
5     $servername= 'localhost';
6     $dbname= 'my_cave';
7     $username= 'root';
8     $password='root';
9     //on try de se connecter
10    try {
11
12        $conn = new PDO("mysql:host=$servername;dbname=$dbname",$username, $password);
13        // on définit le mode d'erreur de PDO sur Exception
14        $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
15
16        // On met ceci en commentaire, on sais maintenant que le lien avec le base de donnée ce fait bien. echo "Connexion à la
17        base de donnée reussi. ";
18        // echo "Connexion reussi";
19    }
20    //On capture les exceptions si une exception est lancée et on affiche *les informations relatives à celle-ci*/
21
22    catch(PDOException $e) {
23        echo "Erreur :". $e->getMessage();
24    }
25
26 };
27
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL powershell + v

Windows PowerShell  
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell <https://aka.ms/pscore6>

PS C:\MAMP\htdocs>

Se connecter à sa base de données est la première étape pour ensuite créer le CRUD (Create, Read, Update, Delete).

A travers une fonction, on se connecte, dans ce cas au localhost (simulation d'hébergement de serveur en local). Nous rentrons le nom du serveur, le nom de la base de données, l'identifiant et le mot de passe pour y accéder.

Comme annoncé dans les commentaires, on définit l'affichage des erreurs puis on commente la phrase qui confirme que nous sommes connectés. Ce fichier Php doit être appelé à travers un « Include » ou « Require » sur les pages dont nous avons besoin. Pour finir, une fois en ligne, il ne faut pas oublier de changer le nom du serveur, de la base de données, l'identifiant et le mot de passe.

Il s'agit ci-dessus de la première étape. Je montre ci-dessous, la fonction permettant d'aller chercher les données.

Il s'agit de la fonction permettant de chercher les données de la BDD, elle renvoie les résultats sous forme de tableaux.

```
function readAllBottlesBDD()
{
    $dbco;

    Connexion($dbco);

    try {
        //on prépare la requête
        $req = $dbco->prepare('SELECT * FROM bottles ORDER BY id desc');
        $req->execute();

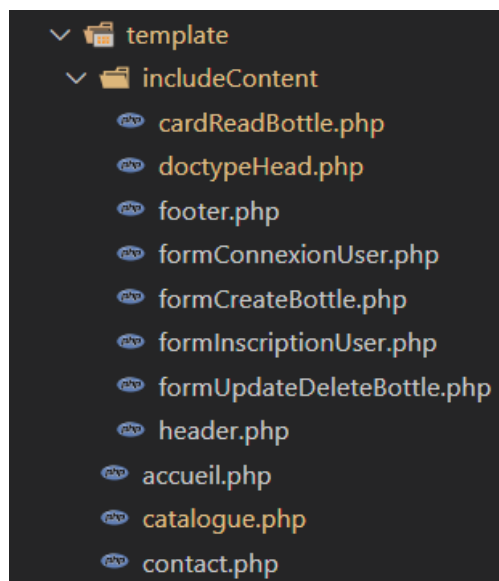
        $dataReadAllBottles = $req->fetchAll(PDO::FETCH_ASSOC);

        return $dataReadAllBottles;

        $req->closeCursor();
    }
    catch (PDOException $e){
        echo "Erreur : " . $e->getMessage();
    }
}
```

### 1.2.3. Développer la partie back-end d'une application

Voici l'architecture de mes composants dans Visual Studio code.



Le dossier template contient tout ce qui est visuel. A la racine de ce dossier, se situent les pages du site (accueil.php, catalogue.php, contact.php).

Dans includeContent il y a des éléments de page : le footer, le header et les formulaires qui servent pour le CRUD.

Voici ci-dessous le code de mon formulaire de création d'une bouteille dans le catalogue.

Je mets sur la page suivante, la partie visuelle du formulaire qui permet la création des bouteilles, sa mise à jour et sa suppression.

```
1 <form class="InsertBottle" id="InsertBottle" method="post" enctype="multipart/form-data" action="...script/
2 TraitementInsert.php">
3 <legend> <h2>Rajouter une bouteille de vin </h2></legend>
4 <p>
5 <label for="CreateNameBottle">Nom du vin</label>
6 <input type="text" name="CreateNameBottle" id="CreateNameBottle" maxlength="100" size="20" required>
7 </p>
8 <p>
9 <label for="CreateYearBottle">Année</label>
10 <input type="number" name="CreateYearBottle" id="CreateYearBottle" maxlength="100" size="20" required>
11 </p>
12 <p>
13 <label for="CreateGrapesBottle">Sépage</label>
14 <input type="text" name="CreateGrapesBottle" id="CreateGrapesBottle" maxlength="50" size="20" required>
15 </p>
16 <p>
17 <label for="CreateCountryBottle">Pays</label>
18 <input type="text" name="CreateCountryBottle" id="CreateCountryBottle" maxlength="20" size="20" required>
19 </p>
20 <p>
21 <label for="CreateRegionBottle">Région</label>
22 <input type="text" name="CreateRegionBottle" id="CreateRegionBottle" maxlength="20" size="20" required>
23 </p>
24 </form>
```

### Rajouter une bouteille de vin :

Nom du vin

Année

Sépage

Pays

Région

Description

500 caractères maximum

Image

Aucun fichier choisi

### Selectionner une bouteille à modifier:

Please choose a bottle to update ▾

### Mettre à jour / Supprimer une bouteille de vin :

L'id du vin est le numéro 12

Nom du vin

DOMAINE DU BOUSCAT

Année

2009

Sépage

Merlot

Pays

France

Région

Bordeaux

Description

La couleur dorée claire de ce vin dément la sav

Le formulaire « Mettre à jour / Supprimer une bouteille de vin » n'est au début pas visible. Il est nécessaire de sélectionner une bouteille pour l'afficher et faire des modifications.

## 2. Résumé du projet

C'est l'histoire d'une cave à vin physique (My Cave) née le 1<sup>er</sup> juillet 2015 dans la commune d'Audenge, créée par Joël. Son amour du vin l'a poussé dans cette voie, à ouvrir sa cave pour partager sa passion et vendre ses bouteilles qu'il s'approvisionne à travers différents châteaux. Vous trouverez une large gamme de vin dans la boutique.

Le site a un but promotionnel et montre les différentes bouteilles présentes en boutique physique. Il est dynamique et le catalogue peut être modifié par le gérant de la boutique. L'interface est intuitive et ne demande aucun codage pour le client.

Le client ne souhaite pas gérer et afficher ses stocks, il souhaite afficher : l'année du vin, le cépage, le château, une description et l'image de la bouteille de vin.

Une charte graphique est donnée et doit être respectée.

Le client n'est pas fermé à l'idée de l'a compléter par de nouveaux éléments qui seront ajoutés avec approbation du client par le développeur.

Agréable visite sur notre site internet et à bientôt.

## 3. Cahier des charges, spécifications fonctionnelles du projet

### Cahier des charges :

Monsieur Granier Joël possède une Cave à Vin depuis le 1<sup>er</sup> juillet 2015. Sa communication se faisait uniquement sur LinkedIn. Il décide de faire appel à un site pour la promotion de ses bouteilles.

Objectif de son site :

- Donner plus de visibilité à sa Cave à Vin.
- Consulter le catalogue des vins présent en boutique physique.
- Permettre au gérant d'ajouter, de mettre à jour ou supprimer des bouteilles.
- Pouvoir être contacter via un formulaire de contact.

L'objectif de Joël est d'avoir davantage de client.

### Spécifications fonctionnelles du projet :

L'utilisateur peut :

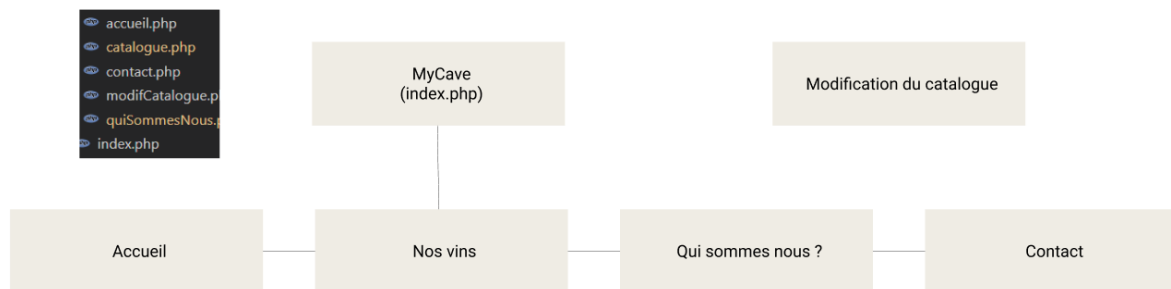
- Visiter le site et consulter la carte des vins sans être connecté.
- Ecrire via un formulaire de contact si besoin.

Les employés/le gérant de MyCave peuvent :

- Se connecter pour ajouter, modifier ou supprimer une bouteille du catalogue des vins
- Savoir si un utilisateur leur a écrit via le formulaire de contact en se connectant à l'adresse email [granier.joël@XXXXX.com](mailto:granier.joël@XXXXX.com).

Le site doit être responsiv.

Arborescence du site :



Charte graphique :

Le client possède une charte graphique que voici ci-dessous.



Le client ne veut pas payer un photographe pour inclure des photos de son enseigne.

N'ayant que ces éléments en termes graphiques, j'ai demandé au client de choisir des photos sur les sites suivant afin de personnaliser les photos du site du client à sa guise.

<https://www.pexels.com/fr-fr/chercher/wine/>

<https://pixabay.com/fr/images/search/wine/>

<https://unsplash.com/s/photos/wine>

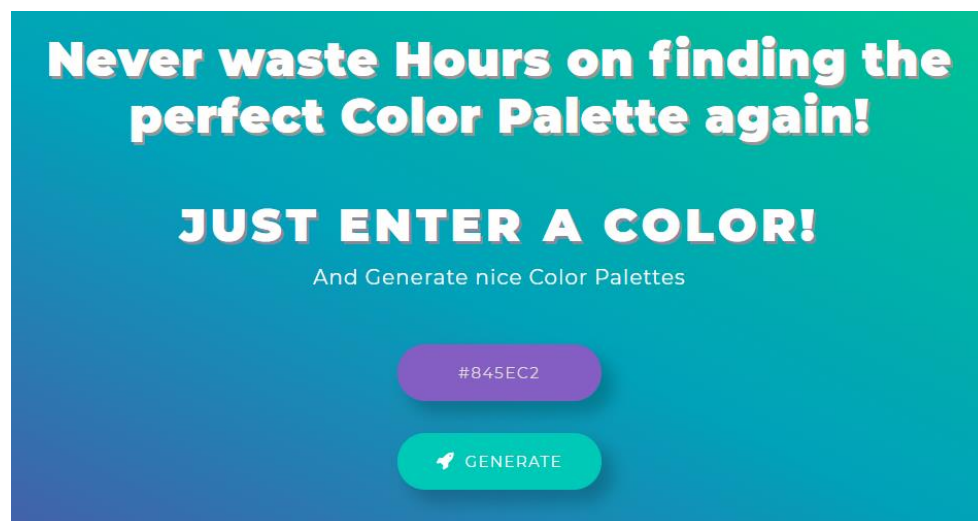
Ces sites permettent d'avoir des photos de bonne qualité gratuitement tout en respectant les droits à l'image.

Manquant de couleur dans la charte graphique, je me suis permis d'utiliser quelques outils et d'en suggérer à mon client.

Outil pour des inspirations graphiques concernant les couleurs :  
<https://www.designwizard.com/blog/design-trends/colour-combination>



<https://mycolor.space/>

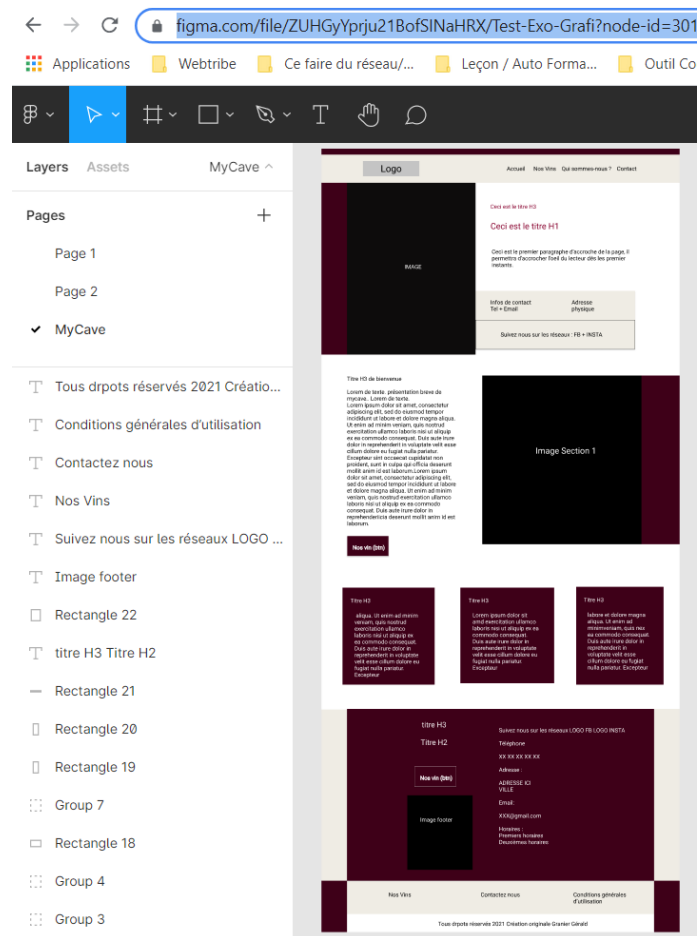


Une couleur rajoutée à la charte graphique est : rgb(239, 236, 228) :



Cette couleur sert de background color pour certaines sections et pour charter le hover de chaque bouton présent sur le site.

## Maquette :



## 4. Spécifications techniques du projet

Outil développement Front :

**HTML** : « HyperText Markup Language » qu'on peut traduire par « langage de balises pour l'hypertexte ». Il est utilisé afin de créer et de représenter le contenu d'une page web et sa structure.

**CSS** : « Cascading Style Sheets » utilisé pour mettre en forme une page web. Il permet de styliser, de mettre des éléments esthétiques sur une page.

Depuis décembre 2015, il est possible d'utiliser des variables. Il est très utile et important d'en utiliser pour charter des couleurs, des marges etc...

```

:root {
  --primary-color: #3e0018;
  --secondary-color: #88002d;
  --third-color: #885c7e;
  --bckg-color: white;
  --txt-color: black;

  --dark-color: black;
  --light-color: white;
  --lightSecond-color: rgb(239, 236, 228);

  --GapPageRightLeft: 8%;
}

@media screen and (max-width: 1095px) {
  :root {
    --GapPageRightLeft: 6%;
  }
}

```

Le :root permet de stocker mes éléments suivants :

- Charte graphique (couleurs)
- Les marges à droites et à gauche du site (GapRightLeft)

Je peux également modifier les marges dans des media queries qui me permettent de mieux m'adapter sur des résolutions d'écrans plus petits.

JavaScript : (souvent abrégé en « JS ») est un langage de script léger, orienté objet, principalement connu comme le langage de script des pages web, important notamment pour le menu burger (responsiv).

### Outil développement Back :

PHP : ce sigle est un acronyme récursif pour PHP. Il s'agit d'un langage de scripts généraliste et Open Source, spécialement conçu pour le développement d'applications web. Il peut être intégré facilement au HTML. Le code est exécuté côté serveur, et renvoie la page HTML côté client ainsi traduite.

MySQL : est un serveur de bases de données relationnelles Open Source. Un serveur de bases de données stocke les données dans des tables séparées plutôt que de tout rassembler dans une seule table. Cela améliore la rapidité et la souplesse de l'ensemble.

phpMyAdmin : (PMA) est une application Web de gestion pour les systèmes de gestion de base de données MySQL et MariaDB, réalisée principalement en PHP.

### Autre outil pour le développement :

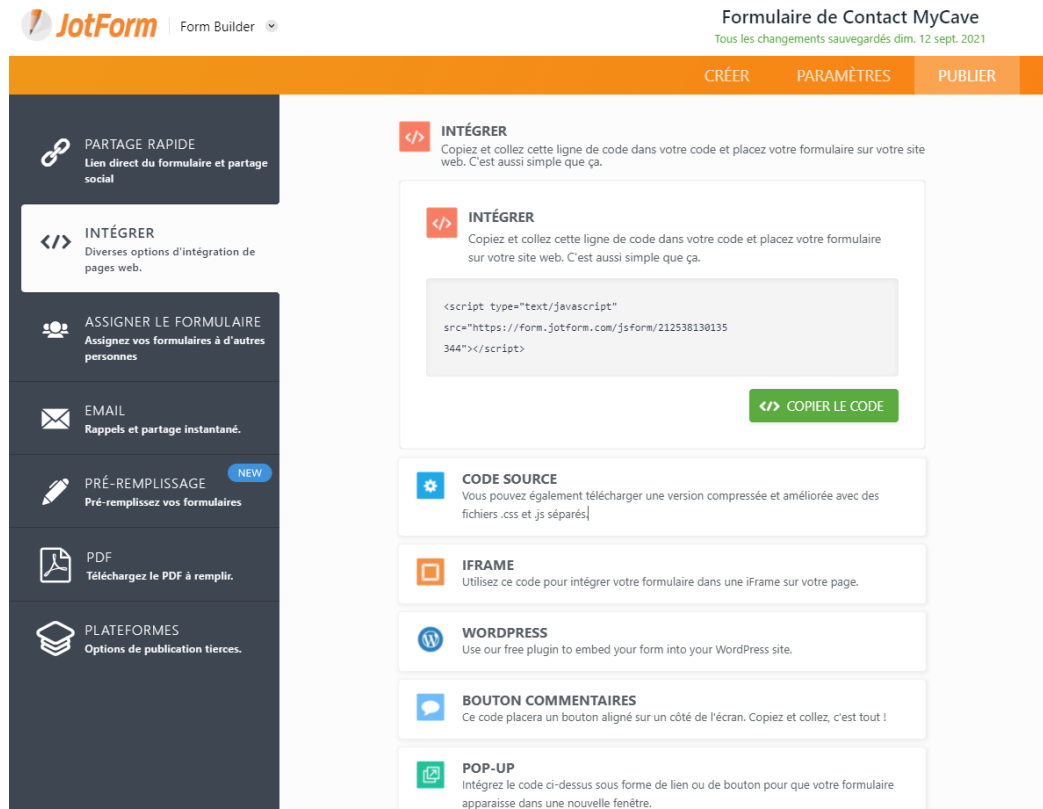
Visual Studio Code : integrated development environment ou IDE. Editeur de texte pour le développement, associé à des extensions, il facilite le travail et augmente la productivité.

Git et Github : Git est un logiciel de versions décentralisé, c'est-à-dire qu'il crée des versions de fichiers qui seront dans notre cas stockées sur l'hébergeur Github. Ce dernier est spécialisé en gestion de développement de logiciel.

Il permet de revenir à différentes étapes du développement en cas de problème. Aussi, il est possible de travailler seul, ou avec une équipe, chacun travaillant sur une partie différente du projet, ou la même. Dans ce cas, une version des deux peut être utilisée ou une fusion des codes.



Jotform : cet outil permet la création de formulaire de contact en ligne. Il est possible de le personnaliser comme le souhaite le développeur pour ensuite pouvoir l'intégrer sur son site internet. Pour ceci il y a encore plusieurs manières de faire, soit intégré directement le code source dans son VS code ou alors utiliser un script.

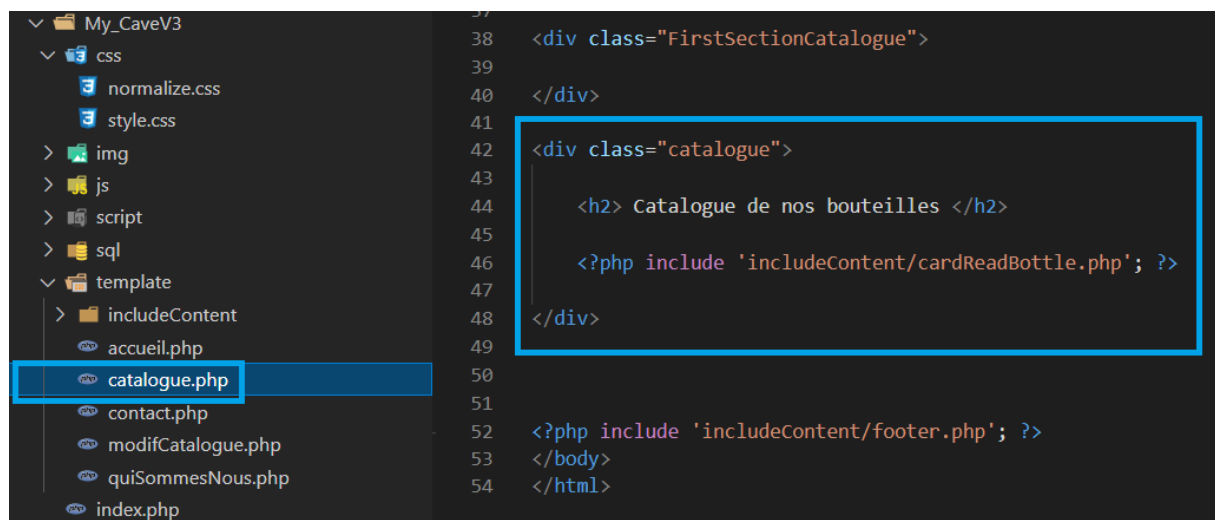


## 5. Réalisation et extrait de code

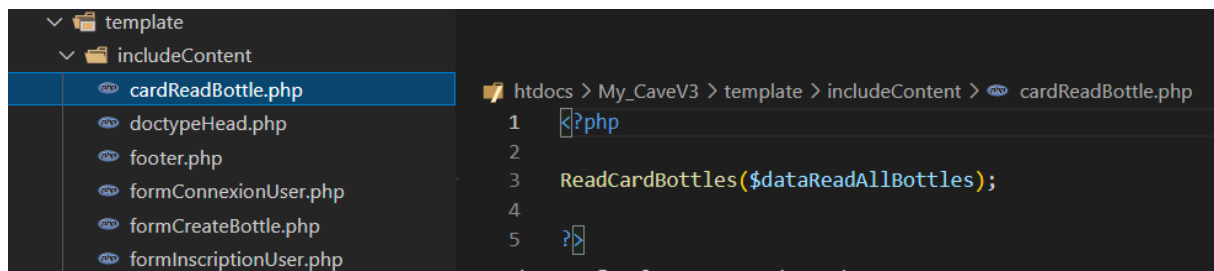
Affichage des bouteilles de vins du catalogue :

L'intérêt de cette section est d'afficher les bouteilles de vins du catalogue.

Regardons de plus près l'architecture employée dans VS Code :

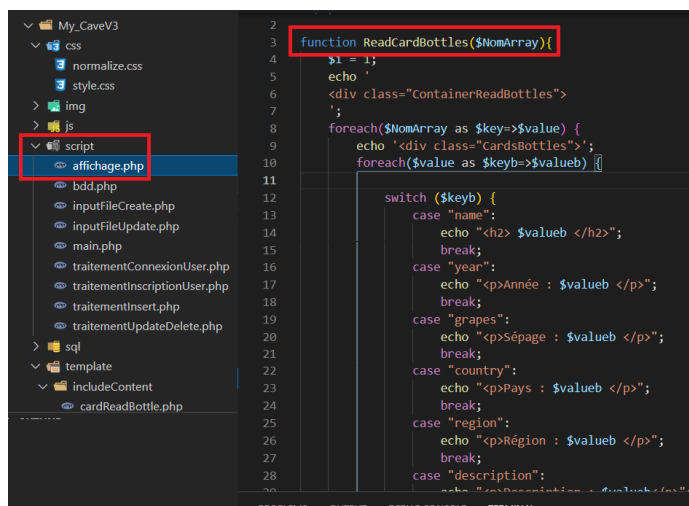


Sur le côté visuel (dossier template), j'inclus une Div puis une section qui figure dans le dossier includeContent qui a pour but d'intégrer cette partie-là.



Dans le cardReadBottle.php je mets uniquement une fonction. L'objectif est de définir ce fichier php comme une section qui puisse être intégrée dans n'importe quelle page.

Cette fonction appelle un fichier php qui est dans le dossier script (les fonctions php sont uniquement dans le dossier script).

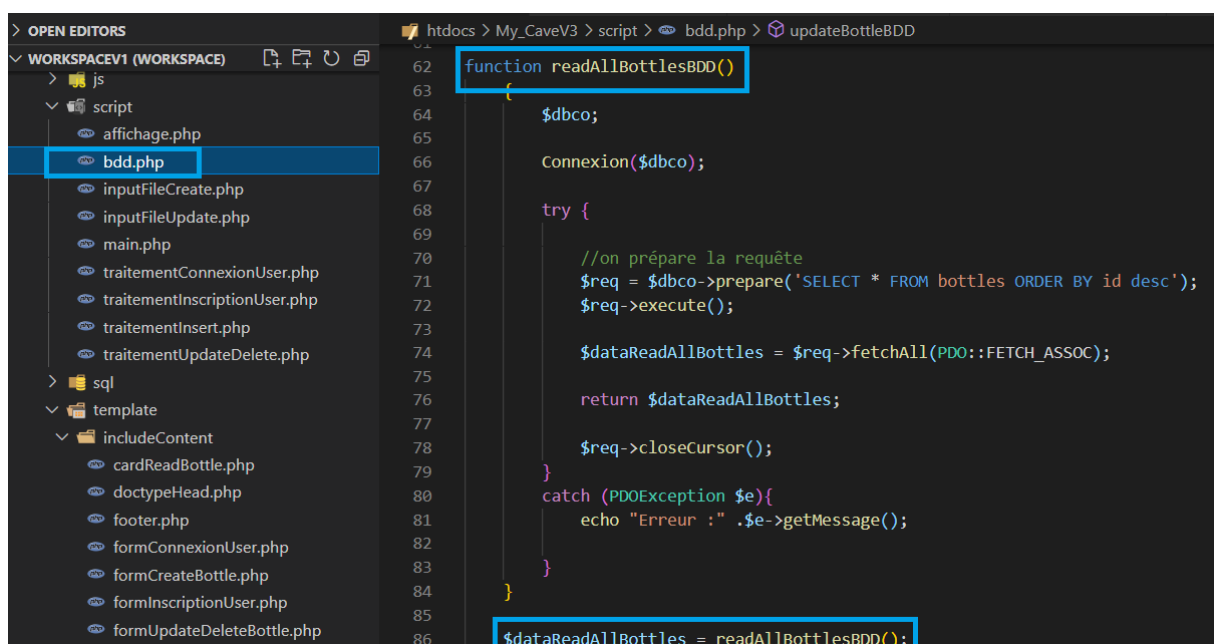


Voici la fonction php figurant dans affichage.php.

La fonction permet à partir d'un tableau de bouclé (foreach) sur chaque élément.

Grâce à un switch/case, j'énumère chaque nom de colonne et demande à les afficher dans (\$valueb).

Ce tableau, lu par la fonction ReadCarBottles est obtenu grâce à une requête SQL (ci-dessous).



Toutes mes requêtes SQL se font dans le dossier bdd.php.

J'utilise la fonction readAllBottleBDD pour effectuer la requête. Connexion(\$dbco) permet la connexion à la base de données.

try{ et catch{ permettent de définir « l'essai » et l'erreur en cas d'erreur de requête. Après la requête (\$req) je l'exécute, et je fais un fetchAll pour récupérer les données sous forme de tableaux. La dernière étape est de retourner la valeur dans la variable \$dataReadAllBottles.

Pour finir (page 18), grâce aux classes définies dans la fonction ReadCarBottles, je peux appliquer du CSS pour choisir l'affichage.

```
/* **** CONTAINER + CARDS READ **** */

.ContainerReadBottles {
  display: flex;
  justify-content: center;
  flex-wrap: wrap;
  margin-top: 50px;
  margin-bottom: 50px;
}

.CardsBottles {
  display: flex;
  flex-direction: column;
  width: 25%;
  height: auto;
  margin: 15px;
  padding: 15px;
  border-radius: 20px;
  background-color: var(--lightSecond-color);
}

.DivCardImg {
  text-align: center;
}
```

Voici le résultat visuel à la fin du codage :



## 6. Présentation du jeu d'essai, fonctionnalité la plus représentative.

Essai réalisé pour la fonctionnalité « création d'une bouteille de vin » dans le catalogue.

On se retrouve sur la page `modifCatalogue.php` grâce à un lien ou en tapant l'adresse dans la barre d'adresse.

Cette page n'est pas référencée dans le menu, l'utilisateur n'y a pas accès, et dans le cas où l'utilisateur trouve le lien de cette page, il faut l'identifiant, l'email et le mot de passe.

Vous devez être connecté pour modifier le catalogue de vins.



Se connecter :

Identifiant

Email

Mot de passe

Monsieur Granier possède un compte, connectons-nous et faisons des tests.



Se connecter :

Identifiant

Email

Mot de passe

! Veuillez renseigner ce champ.

Si je ne rentre pas de mail, je ne peux pas me connecter. En trichant, j'enlève le champ « required » dans l'inspecteur d'élément et en cliquant sur me connecter, une page blanche s'affiche. Je fais un retour en arrière et je ne suis pas connecté. Le résultat est le même pour le champ « Identifiant ».

Explication à la prochaine page niveau code.

```

htdocs > My_CaveV3 > template > includeContent > formConnexionUser.php
1 <form class="ConnexionUser" id="ConnexionUser" method="post" action="../script/TraitementConnexionUser.php">
2 <legend> <h2>Se connecter :</h2></legend>

```

Le formulaire redirige vers cette page PHP qui aura pour but de collecter les éléments de celui-ci.

```

htdocs > My_CaveV3 > script > traitementConnexionUser.php
1 <?php
2 session_start();
3
4 require 'bdd.php';
5
6 if(isset($_POST['SelectUserNickname']) && isset($_POST['SelectUserEmail']) && isset($_POST['SelectUserPassword']) && !empty($_POST['SelectUserNickname']) && !empty($_POST['SelectUserEmail']) && !empty($_POST['SelectUserPassword']))
7
8 {
9
10 $SelectUserEmailClean = filter_var($_POST['SelectUserEmail'], FILTER_SANITIZE_SPECIAL_CHARS);
11 $SelectUserPasswordClean = filter_var($_POST['SelectUserPassword'], FILTER_SANITIZE_SPECIAL_CHARS);
12
13 $PasswordUserBDD = SelectUserBDD($SelectUserEmailClean);
14
15
16 //comparer mdp taper et hash.
17 if(password_verify($SelectUserPasswordClean, $PasswordUserBDD['password']))
18 {
19     echo "<script>";
20     echo "alert('Connexion Reussi');";
21     echo "location.href='../template/modifCatalogue.php'";
22     echo "</script>";
23
24     $_SESSION['NickNameUser'] = $_POST['SelectUserNickname'];
25 }
26

```

Titre : IMG TraitementConnexionUser

Le cadre bleu permet de bien vérifier que chaque éléments sont présents (!empty).

Pour se prémunir de tentative malveillante de hack et contre la faille XSS, j'effectue une la fonction native PHP, FILTER\_SANITIZE\_SPECIAL\_CHARS (cadre rouge).




Explication de ce filtre : <https://www.php.net/manual/fr/filter.filters.sanitize.php>.

Ce filtre permet de transformer en entité HTML les caractères "<>&" et les caractères ASCII de valeur inférieur à 32, et supprime ou encode les autres caractères spéciaux.

Cadre vert, j'effectue la requête. J'effectue la requête grâce à l'adresse email.

Titre : IMG\_Re-  
quête UserBDD

```
htdocs > My_CaveV3 > script > bdd.php > SelectUserBDD
195 function SelectUserBDD(string $EmailUser){
196
197     $dbco;
198
199     Connexion($dbco);
200
201     try {
202
203         //on prépare la requête
204         $req = $dbco->prepare("SELECT * FROM users WHERE email=:email");
205         $req->bindValue(':email', $EmailUser, PDO::PARAM_STR);
206         $req->execute();
207
208         $SelectUser = $req->fetch(PDO::FETCH_ASSOC);
209
210         return $SelectUser;
211
212     }
213
214     catch (PDOException $e){
215         echo "Erreur :" . $e->getMessage();
216
217     }
218
219 };
```



#	Nom	Type
<input type="checkbox"/> 1	id 	int(11)
<input type="checkbox"/> 2	pseudo	varchar(50)
<input type="checkbox"/> 3	email 	varchar(50)
<input type="checkbox"/> 4	password 	char(600)

L'email étant unique, je suis sûr de sélectionner une seule et unique personne.

La clé grise sur l'image correspond à une clé unique, cela permet une identification unique, pratique pour faire un SELECT en SQL.

Ensuite sur l'IMG TraitementConnexionUser (cadre violet), je vérifie le mot de passe tapé par l'utilisateur avec le mot de passe stocké dans la BDD (son hash) et j'utilise la fonction password\_verify (cela vérifie qu'un mot de passe correspond à un hachage).

Le hash permet de stocker dans la base de données un mot de passe crypté. Une mesure de sécurité qui évite que des hackers puissent obtenir toutes nos données permettant l'identification à notre place.

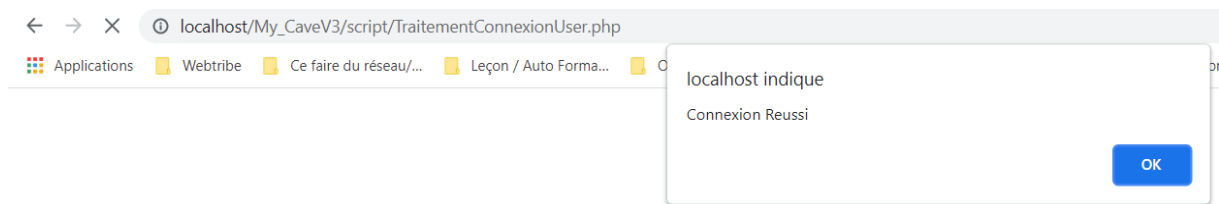
 Éditer  Copier  Supprimer 20 Granier Joël granierjoel@gmail.com \$2y\$10\$MSVElcmVdJAA384Ojh7XR.hb2xuDzc4T.D8/E1P0ekz...

(extrait de PhpMyAdmin pour montrer le hash).

Une petite contrainte à laquelle il faut penser (et je me suis déjà fait avoir), c'est d'autoriser à cette colonne de la table de stocker 255 caractères (recommandation de la doc Php.net). L'utilisation de l'algorithme BCRYPT est destiné à changer dans le temps et donc le nombre de caractère du hash aussi.

Info supplémentaire ici : <https://www.php.net/manual/fr/function.password-hash.php>.

Après l'ensemble de ces vérifications, si tout est bon, l'utilisateur est connecté.



J'ai maintenant accès au formulaire de création d'une bouteille de Vin.

Par soucis pratique et esthétique je trouvais bien d'afficher une `window.alert(message);` (Javascript).

A form titled 'Rajouter une bouteille de vin' in a bold, dark red font. Below the title is a colon ':'. The form contains several input fields: 'Nom du vin', 'Année', 'Sépage', 'Pays', 'Région', and 'Description'. Each of these fields is a simple white rectangle with a thin black border. The 'Description' field is larger and has a placeholder text '500 caractères maximum' in a smaller, grey font. The entire form is set against a light beige background.

Comme pour la connexion de l'utilisateur, mon fichier PHP contient `!empty` et j'effectue des `FILTER_SANITIZE_SPECIAL_CHARS` pour tout les champs sauf « Année » où j'effectue un `FILTER_SANITIZE_NUMBER_INT` (Supprime tous les caractères sauf les chiffres, et les signes plus et moins).

Remarque : une image est obligatoire pour créer une bouteille.

Visuel du code ci-dessous.

```
style.css  modifCatalogue.php M  bdd.php  traitementInsert.php x  formConnexionUser.php  accueil.php
htdocs > My_CaveV3 > script > traitementInsert.php
1  <?php
2
3  require "bdd.php";
4  require "inputFileCreate.php";
5
6
7  if(isset($_POST['CreateNameBottle']) && isset($_POST['CreateYearBottle']) && isset($_POST['CreateGrapesBottle']) && isset($_POST
['CreateCountryBottle']) && isset($_POST['CreateRegionBottle']) && isset($_POST['CreateDescriptionBottle']) && isset($_FILES
['CreatePictureBottle']) && !empty($_POST['CreateNameBottle']) && !empty($_POST['CreateYearBottle']) && !empty($_POST
['CreateGrapesBottle']) && !empty($_POST['CreateCountryBottle']) && !empty($_POST['CreateRegionBottle']) && !empty($_POST
['CreateDescriptionBottle']) && !empty($_FILES['CreatePictureBottle'])) {
8
9
10
11      $CreateNameBottleClean = filter_var($_POST['CreateNameBottle'], FILTER_SANITIZE_SPECIAL_CHARS);
12      $CreateYearBottleClean = filter_var($_POST['CreateYearBottle'], FILTER_SANITIZE_NUMBER_INT);
13      $CreateGrapesBottleClean = filter_var($_POST['CreateGrapesBottle'], FILTER_SANITIZE_SPECIAL_CHARS);
14      $CreateCountryBottleClean = filter_var($_POST['CreateCountryBottle'], FILTER_SANITIZE_SPECIAL_CHARS);
15      $CreateRegionBottleClean = filter_var($_POST['CreateRegionBottle'], FILTER_SANITIZE_SPECIAL_CHARS);
16      $CreateDescriptionBottleClean = filter_var($_POST['CreateDescriptionBottle'], FILTER_SANITIZE_SPECIAL_CHARS);
17      $CreatePictureBottleClean = filter_var($_FILES['CreatePictureBottle'], FILTER_SANITIZE_SPECIAL_CHARS);
18
19      checkPictureInsert();
20
21      createBottleBDD($CreateNameBottleClean, $CreateYearBottleClean, $CreateGrapesBottleClean, $CreateCountryBottleClean,
$CreateRegionBottleClean, $CreateDescriptionBottleClean, $PictureInsert);
22
23      echo "<script>:"
```

Titre :IMG\_Traitement\_Insert.

La fonction checkPictureInsert() permet de gérer les erreurs liés aux téléchargements des images.

#### UPLOAD\_ERR\_OK

Value: 0; There is no error, the file uploaded with success.

#### UPLOAD\_ERR\_INI\_SIZE

Value: 1; The uploaded file exceeds the [upload\\_max\\_filesize](#) directive in `php.ini`.

#### UPLOAD\_ERR\_FORM\_SIZE

Value: 2; The uploaded file exceeds the `MAX_FILE_SIZE` directive that was specified in the HTML form.

#### UPLOAD\_ERR\_PARTIAL

Value: 3; The uploaded file was only partially uploaded.

#### UPLOAD\_ERR\_NO\_FILE

Value: 4; No file was uploaded.

#### UPLOAD\_ERR\_NO\_TMP\_DIR

Value: 6; Missing a temporary folder.

#### UPLOAD\_ERR\_CANT\_WRITE

Value: 7; Failed to write file to disk.

#### UPLOAD\_ERR\_EXTENSION

Value: 8; A PHP extension stopped the file upload. PHP does not provide a way to ascertain which extension caused the file upload to stop; examining the list of loaded extensions with [phpinfo\(\)](#) may help.

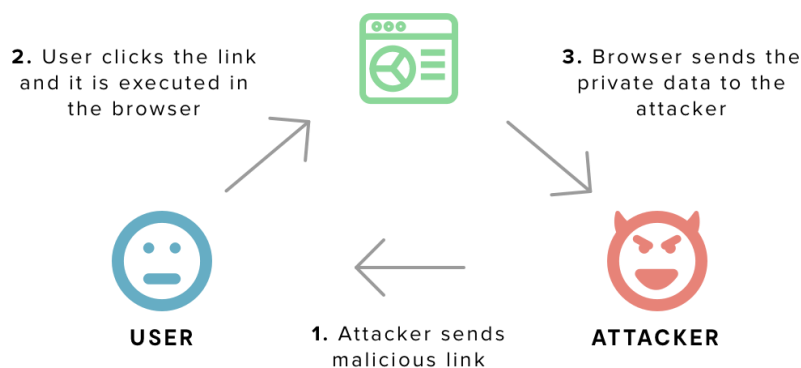


## 7. Description de la veille durant le projet, sur les vulnérabilités de sécurité.

Tout au long de ce projet, j'ai mis en place de nombreuses mesures de sécurité.

A l'heure où les données sont cruciales dans la vie de chacun, il va de soi que la protection de celles-ci ne soit pas négligée. Une simple connexion à un formulaire ou un achat en ligne avec numéro de carte bancaire, et se sont vos informations, extrêmement sensibles, qui circulent sur internet.

Une faille très importante à contrer est la faille XSS.



IMG FailleXSS

Explication IMG FailleXSS :

Un attaquant va utiliser des formulaires pour écrire du code à l'intérieur des inputs et ainsi faire ce qu'il souhaite de la base de données, récupérer des infos, en supprimer, s'il le souhaite etc. Cela met en danger les utilisateurs et le bon fonctionnement du site.

Pour se prémunir du danger j'ai utilisé une fonction native de PHP. `FILTER_SANITIZE`.

<https://www.php.net/manual/fr/filter.filters.sanitize.php>

<b>FILTER_SANITIZE_ENCODED</b>	"encoded"	<b>FILTER_FLAG_STRIP_LOW, FILTER_FLAG_STRIP_HIGH, FILTER_FLAG_STRIP_BACKTICK, FILTER_FLAG_ENCODE_LOW, FILTER_FLAG_ENCODE_HIGH</b>	Applique l'encodage URL, et supprime ou encode les caractères spéciaux.
<b>FILTER_SANITIZE_MAGIC_QUOTES</b>	"magic_quotes"		Applique <code>addslashes()</code> . (OBSOLÈTE à partir de PHP 7.3.0 et SUPPRIMÉE à partir de PHP 8.0.0, utiliser <b>FILTER_SANITIZE_ADD_SLASHES</b> à la place.)
<b>FILTER_SANITIZE_ADD_SLASHES</b>	"add_slashes"		Applique <code>addslashes()</code> . (Disponible à partir de PHP 7.3.0)
<b>FILTER_SANITIZE_NUMBER_FLOAT</b>	"number_float"	<b>FILTER_FLAG_ALLOW_FRACTION, FILTER_FLAG_ALLOW_THOUSAND, FILTER_FLAG_ALLOW_SCIENTIFIC</b>	Supprime tous les caractères, sauf les chiffres, +- et éventuellement ., eE.
<b>FILTER_SANITIZE_NUMBER_INT</b>	"number_int"		Supprime tous les caractères sauf les chiffres, et les signes plus et moins.
<b>FILTER_SANITIZE_SPECIAL_CHARS</b>	"special_chars"	<b>FILTER_FLAG_STRIP_LOW, FILTER_FLAG_STRIP_HIGH, FILTER_FLAG_STRIP_BACKTICK, FILTER_FLAG_ENCODE_HIGH</b>	Transforme en entité HTML les caractères ' ">& et les caractères ASCII de valeur inférieur à 32, et supprime ou encode les autres caractères spéciaux.

Voici en encadrement rouge les 2 filtres que j'ai utilisés. Enlever les caractères spéciaux empêche toute attaque possible venant d'un attaquant.

J'ai intégré ces filtres à chaque entrée de données (formulaire de connexion, formulaire de création de bouteilles, formulaire de mis à jour des bouteilles).

Un autre élément de sécurité très important est l'utilisation du PasswordHash.

<https://www.php.net/manual/fr/function.password-hash.php>

Le Password Hash permet de stocker le mot de passe crypter dans la base de données.

Une fonction `verify_password` est nécessaire lors de la connexion de l'utilisateur pour vérifier si le mot de passe tapé par l'utilisateur est le bon.

## 8. Recherche en anglais

In english :

For my example, i sometimes search Flexbox properties, i have a simple reminder when i hesitate or don't find what's the property i need.

I searched on google using « flexbox » keyword and the first website returned was <https://css-tricks.com/snippets/css/a-guide-to-flexbox/>.

[HOME](#) / [GUIDES](#) /

# A Complete Guide to Flexbox



Chris Coyier on Apr 8, 2013 (Updated on Sep 10, 2021)

Our comprehensive guide to CSS flexbox layout. This complete guide explains everything about flexbox, focusing on all the different possible properties for the parent element (the flex container) and the child elements (the flex items). It also includes history, demos, patterns, and a browser support chart.

Titre : IMG Guide Flexbox

Part 1: [Background](#)  
Part 2: [Basics and terminology](#)  
Part 3: [Flexbox properties](#)  
Part 4: [Prefixing Flexbox](#)  
Part 5: [Examples](#)  
Part 6: [Flexbox tricks](#)  
Part 7: [Browser support](#)  
Part 8: [Bugs](#)  
Part 9: [Related properties](#)  
Part 10: [More information](#)

This website explain very well with example and some picture.

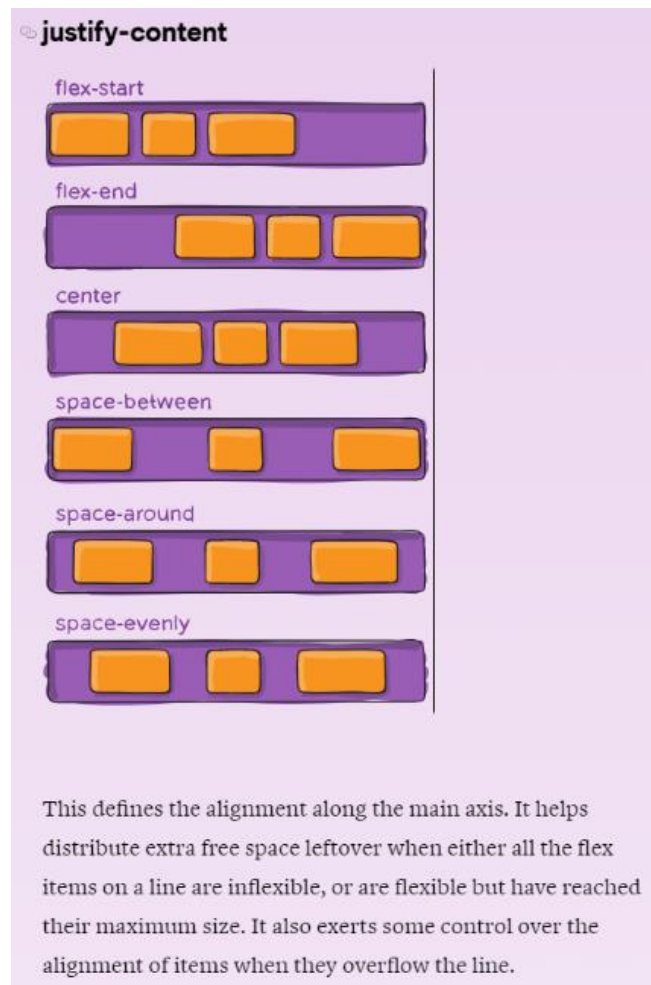
I don't always use flex-wrap, i don't know by heart how to write it, so i check and i have the property here when i need it :

By default, flex items will all try to fit onto one line. You can change that and allow the items to wrap as needed with this property.

```
.container {  
  flex-wrap: nowrap | wrap | wrap-reverse;  
}
```

Titre : IMG .container

I check this page always as a reminder. If i hesitate, i always know where i can search.



Titre : IMG justify-content

When i didnt code some CSS since a long time, i check justify-content and align-items properties.

En Français :

Par exemple, de temps en temps, je cherche les propriétés Flexbox, j'ai un aide-mémoire simple quand j'hésite ou que je ne trouve pas la propriété que j'ai besoin. Je cherchais dans google les mots-clés utilisant « flexbox » et le premier site internet qui m'est retourné étais : <https://css-tricks.com/snippets/css/a-guide-to-flexbox/>.

Traduction de l'IMG Guide Flexbox :

Notre guide de compréhension de la disposition CSS Flexbox. Ce guide complet explique tout à propos de Flexbox, axé sur différentes propriétés de l'élément parent (le conteneur flex) et l'élément fils (flex item). Cela inclut également l'historique, des démonstrations, des modèles, et le support.

Ce site explique très bien, avec des exemples et plusieurs images.

Je n'utilise pas tout le temps flex-wrap et je ne connais pas par cœur comment l'écrire, donc je vérifie et j'ai la propriété ici quand j'en ai besoin : `IMG.container` traduction :

Par défaut, les articles flex vont toujours essayer de s'adapter sur une ligne. Vous pouvez changer ceci et autoriser les articles à wrap si besoin avec cette propriété.

Je vérifie cette page toujours comme aide-mémoire. Si j'hésite, je sais toujours où chercher.

Traduction de l'`IMG.justify-content` :

Ceci définit l'alignement le long de l'axe principal. Cela aide à distribuer de l'espace supplémentaire restant lorsque tous les éléments d'une ligne sont inflexibles ou qu'ils sont flexibles mais ont atteint leur taille maximum. Cela exerce aussi du contrôle sur l'alignement des items quand ils débordent de la ligne.

Quand je ne faisais pas de code CSS depuis un certain temps, je vérifie les propriétés align-items et justify-content.

## 9. Conclusion

Ce projet My\_Cave a été très formateur tout au long de sa conception. Par curiosité, j'ai comparé avec des anciens projets que j'ai faits et je suis de plus en plus satisfait de la qualité de travail que je fournis.

Le long de ma formation, je me suis équipé de plein d'outils que je réutilise (exemple outil charte graphique page 14) et j'en découvre encore et toujours de nouveau.

J'aime cette perpétuelle recherche de documentation, d'outils permettant de développer un site de plus en plus performant et qualitatif.

Je fais un point remerciement qui compte pour moi.

Je remercie :

- Mon père, qui a su être là pour discuter pendants mes moments de doutes et sur l'avancement de mon projet.
- Mon cher ami Thomas Bréard, pour la relecture de ce dossier, m'a aidé et conseillé sur la mise en forme que j'ai effectué.
- Les collègues de classe que j'apprécie beaucoup et avec qui il a été possible de beaucoup discuter, se motiver pour ce projet si long qui finalise notre formation.

- Madame Dominique Hélène Ruisseaux, grâce à elle, j'ai aujourd'hui davantage le goût de la persévérance qui m'a permis d'accomplir ce projet.

Je fini les remerciements par les personnes qui m'ont permis d'accéder à cette formation et ont permis l'encadrement de celle-ci.

Merci au Campus du Lac pour la formation.

Granier Gérald