

Mon P'tit truc en bois

LA MANU - AMIENS

Formation Développeur Web et Web Mobile Crée
par : Loïc FERRARIO

Remerciements

Merci à toute l'équipe de La MANU Amiens pour leur aide durant ces mois de formation

Merci M. Thierry LACHAT pour son temps, sa patience et sa formation de qualité

Merci à M. Gérard VUE pour m'avoir fait confiance pour réaliser ce projet

Merci à Mme Aurore FERRARIO pour son soutien et ses bonnes remarques

Merci à mes enfants pour leur soutien

Compétences couvertes

Le projet couvre les compétences suivantes :

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

- Maquetter une application
- Réaliser une interface utilisateur web statique et adaptable
- Développer une interface web dynamique

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

Résumé de projet

Mon projet est la refonte complète et la remise en conformité avec les standards du web du site actuel de Mon P'tit Truc En Bois, site de M. Gérard VUE.

Le site actuel est la vitrine de l'activité de M. Gérard VUE et présente l'ensemble des produits qu'il fabrique. Malheureusement, le site ne comporte à l'heure actuelle aucune gestion des utilisateurs ou des commandes.

Le but va être d'intégrer une partie "utilisateurs" au site afin de leur permettre de voir les produits mais également de les commander, de suivre sa commande...

Le nouveau site se sépare donc en trois parties distinctes :

- La partie "Visiteurs"
- La partie "Utilisateurs"
- La partie "Administrateur"

La partie "visiteurs" :

La partie « Visiteurs » sera accessible à tous, sans besoin de s'inscrire ni de se connecter.

Elle correspondra à la version actuelle du site, mais avec un code web conforme aux standards actuels et une sécurité renforcée.

Elle permettra d'explorer l'ensemble des produits ainsi que leurs caractéristiques techniques et commerciales. Il sera possible de connaître le type de bois utilisé, le poids, le prix...

Le site aura aussi une page « foire aux questions » afin de répondre aux questions que peuvent se poser les visiteurs. Elle intégrera également la possibilité de poser des questions et les réponses à ces questions.

Les visiteurs pourront envoyer un message via un formulaire pour demander des informations, poser des questions qui ne sont pas dans la foire aux questions

La partie "utilisateurs" :

La partie « Utilisateurs » ne sera accessible qu'après une inscription ou une connexion.

Elle permettra de placer des produits dans son panier et de les commander.

Une page utilisateur permettra de faire un suivi de ses commandes, consulter leur avancement, afficher les anciennes, modifier ses informations de profil, ajouter des adresses

de livraison...

Un utilisateur connecté pourra laisser des commentaires sur les produits et les noter. Ces notes seront utilisées pour créer une liste des produits préférés des utilisateurs et ainsi permettront de créer un petit encart sur la page d'accueil, avec la liste des produits favoris et les mieux notés.

Les utilisateurs seront suivis afin de connaître leur visite sur le site et ainsi désactiver les comptes inactifs.

La partie “administrateur” :

L'administrateur du site aura une page dédiée lui permettant de gérer l'intégralité du site ainsi que ses données. L'administrateur pourra grâce à elle ajouter des produits, les modifier, les supprimer...

La page permettra de suivre la réception des commandes leur paiement, la livraison...

Les commentaires seront également affichés permettant de les contrôler

Il sera possible de créer une liste des « produits du moment » et d'afficher les offres spéciales, les réductions...

L'intégralité des options et données du site pourra être ajoutée, modifiée ou supprimée depuis la page de gestion de l'administrateur.

Cahier des charges

Le site est basé sur le site actuel qui n'est que la vitrine des produits.

Le projet consiste à reprendre l'intégralité des données du site actuel et de les intégrer dans un nouveau site, plus en adéquation avec les attentes en matière de codage et de sécurité des sites web.

Le nouveau site devra conserver un rappel de l'ancien afin que les clients ne soient pas complètement perdus et ainsi éviter la perte de clients anciens tout en facilitant le gain de nouveaux clients.

Il devra intégrer les fonctions de gestions des utilisateurs, les commandes, les notes des produits, les commentaires...

LES VISITEURS :

Le visiteur devra pouvoir voir les produits, les commentaires, les notes, le prix et les caractéristiques techniques des produits.

Il ne pourra ni commander, ni laisser de commentaires, ni noter. Il devra s'inscrire ou se connecter pour le faire, ce qui le fera ainsi devenir un utilisateur.

Lors de l'inscription, il sera demandé uniquement l'adresse mail et un mot de passe.

Un mail sera envoyé afin de confirmer l'adresse mail et redirigera vers la page profil qui invitera à compléter le profil :

- Type de compte (particulier, professionnel)
- Nom,
- Prénom,
- Téléphone,
- Adresse postale,
- Complément d'adresse
- Code postal,
- Ville,
- Contact via... (email, téléphone, courrier postal)

Le remplissage du profil n'est pas obligatoire lors de la première connexion, mais en cas de commande, si une donnée du profil n'est pas complétée, la commande ne pourra pas être validée.

LES UTILISATEURS :

L'utilisateur pourra voir les produits et les commander, les noter, les commenter...

Il pourra les mettre dans son panier en choisissant la quantité souhaitée.

Il aura aussi la possibilité de mettre des produits en favoris afin de les retrouver rapidement dans son profil en cas de besoin de les recommander.

Lors de la mise en commande, un délai de fabrication sera calculé et indiquera une date estimée de livraison.

Le calcul du temps de fabrication se fera avec les informations du produit et se calculera en fonction du type de produit en commande et leur quantité.

Le panier avec la quantité de produits sera accessible via une icône dans la barre de navigation mais également depuis sa page de profil.

La page de profil utilisateur comportera les options suivantes :

- Gestion des adresses de livraison (ajout, par défaut, suppression)
- Modification des informations personnelles
- Affichage des commentaires effectués et des notes données
- Liste des commandes en cours et passées
- Résumé des commandes (nombre de commandes, nombre de produits, montant total des commandes)
- Pouvoir commenter une commande terminée
- Possibilité de demander la suppression de son compte

L'ADMINISTRATEUR :

L'administrateur aura la possibilité de gérer l'intégralité du site depuis une page dédiée

Cette page regroupera les fonctions suivantes :

- Utilisateurs :

Afficher la liste des nouveaux utilisateurs

Afficher la liste des utilisateurs (nouveaux et anciens)

Bloquer ou supprimer des utilisateurs

- Commandes :

Afficher la liste des nouvelles commandes

Afficher les commandes en cours (attente de paiement, de traitement, de livraison)

Afficher la liste des anciennes commandes et voir les commentaires associés

- Événements :

Créer un événement (manifestation, découverte, promotions...)

Gestion des événements en cours (modification, suppression)

Lister les événements anciens avec leurs commentaires

- Produits :

Créer un nouveau produit

Gérer les produits actuels (modification, suppression)

- Commentaires :

Afficher les commentaires laissés par les utilisateurs et les contrôler

Il sera possible d'y répondre, de "remercier" à l'aide d'un petit bouton, ou de les supprimer

- Informations :

Ajouter, modifier ou supprimer l'intégralité des données nécessaires au fonctionnement du site (type de bois utilisé, les transporteurs utilisés, les catégories de produits...)

Spécifications techniques du projet

Charte graphique

Couleurs

Pour la réalisation de mon projet, il m'a fallu respecter les demandes spécifiques de mon client :

- Permettre aux clients anciens de se retrouver dans le nouveau site
 - o Les noms ont été gardés tel que le client les avait nommés
 - o Toutes les photos utilisées proviennent du précédent site mais ont été mises à jour en respectant la nouvelle charte graphique
- Rajeunir l'esthétique du site créé il y a plus de 10 ans
 - o Passage en responsive
 - o Couleurs plus actuelles
 - o Mise en conformité de l'identité du site avec le métier
- Faire un site à l'esprit joyeux
 - o Récupération des couleurs rose et gris et intégration au nouveau site
 - o Respect de la demande du client de conserver l'esprit du site précédent

Police

Afin de conserver une continuité avec le site précédent, j'ai conservé la police d'écriture d'origine : Roboto

Ancien site :

```
Roboto:300,400,500,700
```

Nouveau site :

```
family=Roboto:ital,wght@0,100;0,300;0,400;0,500;0,700;0,900;
```

Outils utilisés

Gestion du projet :

- Trello
Gestion du planning de réalisation du projet, suivi de son évolution...

Carte mentale :

- Mindmeister
Conceptualisation du projet, visualisation de la navigation des utilisateurs

Maquettage :

- Adobe XD
Création de la maquette visuelle du site

MCD (Modèles Conceptuels de Données) :

- Looping
Modélisation de la base de données

Base de données :

- MySQL
Création / gestion de la base de données

Développement :

- VS Code (Visual Studio Code)
Codage du site web

Environnement de test :

- Laragon
Serveur local

Sauvegarde du projet :

- Git
Logiciel de versionning
- GitHub
Sauvegarde du projet

Framework :

- Bootstrap

Langages utilisés

Front-end

HTML5

Le langage HTML5 (de l'anglais *HyperText Markup Language*), utilisé en complément du PHP permet de créer une structure des fichiers grâce aux nouvelles balises intégrées dans cette dernière version (<header>, <main>, <nav>, <footer>...)

CSS3

La mise en forme du site (polices, couleurs, espacement, etc.) a été ajouté en utilisant le langage CSS3 (*Cascading Style Sheets*)

Ce langage permet de créer des espaces, de déterminer la taille des polices d'écrire ainsi toute la mise en forme des pages HTML et XHTML

JavaScript

JavaScript est un langage de programmation qui permet d'implémenter des mécanismes complexes sur une page web. En d'autres termes, cela permet d'afficher du contenu mis à jour à des temps déterminés, des cartes interactives, des animations 2D/3D, des menus vidéo défilants...

Cela augmente l'interactivité d'un site avec l'utilisateur.

Bootstrap

Bootstrap est un Framework utilisant les langages HTML, CSS et JavaScript qui fournit aux développeurs des outils pensés pour développer des sites avec un design responsive, qui s'adapte à tout type d'écran, et en priorité pour les smartphones.

Il fournit des outils avec des styles déjà en place pour des typographies, des boutons, des interfaces de navigation et bien d'autres encore.

Bootstrap fait partie de la catégorie des Framework dit "Front-End Framework".

Back-end

PHP

Le PHP (*HyperText Preprocessor*), désigne un langage informatique utilisé principalement pour la conception de sites web dynamiques. Sur un plan technique, le PHP s'utilise la

plupart du temps côté serveur. Il génère du code HTML (ou encore XHTML), CSS, des données (en PNG, JPG, etc.) ou encore des fichiers PDF.

MySQL

MySQL est un serveur de bases de données qui stocke les données dans des tables séparées plutôt que de tout rassembler dans une seule table. Les tables peuvent être reliées par des relations définies, qui rendent possible la combinaison de données entre plusieurs tables durant une requête. SQL dans "MySQL" signifie "*Structured Query Language*" : le langage standard pour les traitements de bases de données.

Bonnes pratiques

Code propre :

Utiliser un code propre consiste à commenter et indenter le code afin de faciliter la compréhension par soi-même ou d'autres personnes participant au projet. Cela est aussi utile dans le cas où le code sera repris dans le futur, lors de la reprise du projet

```
<!-- TOTAL WEIGHT / PRICE -->
<?php endforeach ?>
<div class="col-12 border-top border-1 py-3">
    <div class="row p-2 px-md-5">
        <div class="col-6">Poids total : <?= $order_weight ?? '' ?> grammes</div>
        <div class="col-6">Coût total de la commande : <?= $order_price_total ?? '' ?> €</div>
    </div>
</div>

<!-- LIST CHOICE CARRIER -->
<div class="col-12 pb-3">
    <div class="row">
        <div class="col-4 text-center">Choix du transporteur :</div>
        <div class="col-4">
            <select class='form-select' name='id_carrier'>
```

Utilisation d'une notation :

Utilisation d'une notation choisie, du “Camel case” ou du “Snake case”, dans les noms de variables, les id, les classes...

L'homogénéisation de la notation permet de créer une cohérence dans le code et d'augmenter la lisibilité

```
="postal_code" value="<?= $user_info->addresses_postal_code ?? '' ?>"
```

Internationalisation du code :

Utilisation de l'anglais pour les noms de variables, les id, les classes...

Redirection à l'accès du site :

Utilisation d'un fichier “index.php” à la racine du projet.
Cela permet d'augmenter la sécurité d'un site web

```
index.php
1 <?php
2
3 //----- REDIRECT TO HOMEPAGE -----
4 header('location: /accueil.html');
5 exit;
6
7 ?>
```

Sémantiques :

Respect de la hiérarchisation de la sémantique dans les titres

Utilisation des balises dans un ordre chronologique (*<h1>* puis *<h2>* puis *<h3>*...)

Optimisation des images :

Redimensionnement des images

Utilisation des formats JPG et/ou PNG

Lors de la connexion à un site depuis un accès réseau limité, le temps de chargement des ressources est amélioré

Accessibilité :

Utilisation des attributs “alt” et “title” sur les images

Utilisation de l’attribut “title” sur les liens

L’accès par les logiciels d’aides à l’accessibilité est amélioré car ces balises sont lues et améliorent la lisibilité du site

```
alt='<?= $productInfo->products_name; ?>' title='<?= $productInfo->products_name; ?>'>
```

Placement des styles et Javascript :

Enregistrement des styles dans un fichier à part, inclus dans la balise *<head>*

Cela permet de ne charger que la feuille de style nécessaire lors de la connexion d’un terminal, et ainsi réduire la quantité de ressources chargées et donc le temps de chargement de la page

```
<link href='https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/css/bootstrap.min.css' rel='stylesheet'>
<link rel='stylesheet' href='./public/assets/css/style.css'>
<link rel='stylesheet' href='./public/assets/css/sm.css' media="screen and (max-width:576px)">
<link rel='stylesheet' href='./public/assets/css/md.css' media="screen and (min-width:576px)">
<script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.8/jquery.min.js"></script>
<title>Mon P'tit Truc En Bois - <?= $pageTitle; ?></title>
</head>
```

Enregistrement du javascript dans un fichier à part, avant la balise fermante </body>

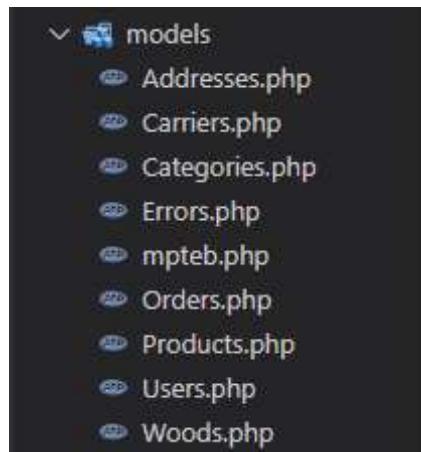
```
<!--- BOOTSTRAP SCRIPT --->
<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/js/bootstrap.bundle.min.js"
integrity="sha384-ka7Sk0Gln4gmtz2MlQnikT1wXgYsOg+OMhU P+IlRH9sENBO0LRn5q+8nbTov4+1p" crossorigin="anonymous"></script>
<!--- PERSONAL SCRIPT --->
<script src='../public/assets/js/script.js'></script>
</body>
```

Utilisation des “quotes” :

Utilisation de “quotes” simples (‘’), doubles (“ ”) ou magiques (` `) selon leur utilisation

Les “classes” :

Création d'un fichier par classe, avec un nom explicite, commençant par une majuscule



Balise fermante PHP :

Pas de balise fermante “?>” dans les fichiers ne contenant que du PHP

La sécurité des fichiers est ainsi augmentée par cette pratique.

Architecture MVC :

Utilisation de l'architecture MVC

L'utilisation de cette architecture permet de séparer les pages web en de multiples fichiers et ainsi augmenter la sécurité et la possibilité de travailler à plusieurs en même temps sur un projet

Responsivité ou Mobile First :

Création du contenu pour un maximum de terminaux (mobile, tablette, ordinateur fixe ou mobile) et créations de feuilles de style séparées selon le terminal



```
<link rel='stylesheet' href='../public/assets/css/style.css'>
<link rel='stylesheet' href='../public/assets/css/sm.css' media="screen and (max-width:576px)">
<link rel='stylesheet' href='../public/assets/css/md.css' media="screen and (min-width:576px)">
```

Compatibilité des navigateurs :

Utilisation d'un Framework afin d'être compatible avec le plus grand nombre de navigateur

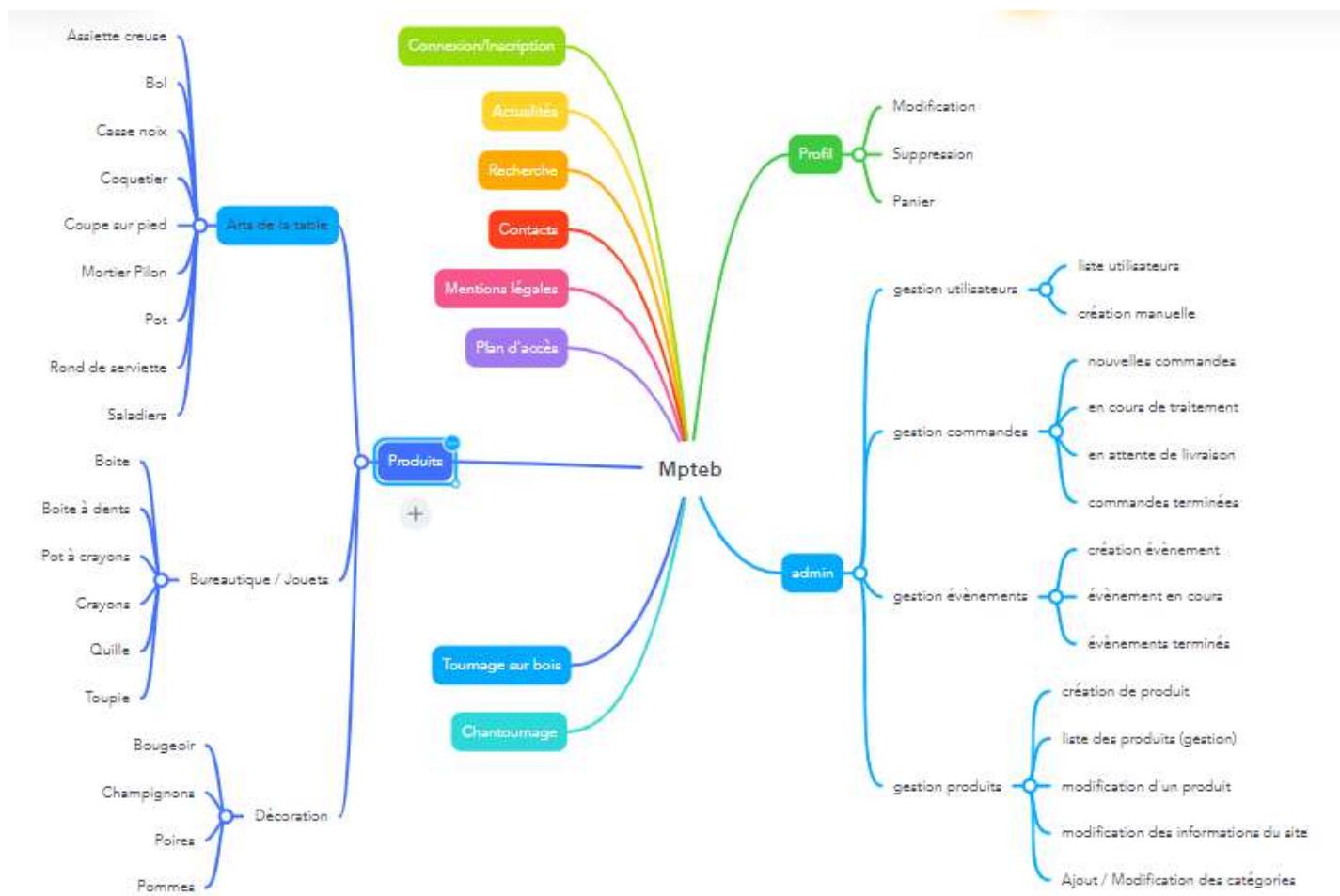
Réalisations du candidat

Carte mentale

Pour la réalisation de mon projet, j'ai tout d'abord eu à étudier la navigation des utilisateurs actuels au travers d'une carte mentale. J'ai étudié la manière dont le site avait été conçu afin de respecter la navigation naturelle actuelle mais en réfléchissant à pouvoir la réorienter vers un usage plus efficace et plus agréable.

Pour faire cela, j'ai utilisé le logiciel Mindmeister en le classant en deux parties :

- La partie visiteur, accessible sans inscription (partie gauche)
- La partie utilisateurs, accessible uniquement une fois connecté (en haut à droite)
- La partie administrateur, visible uniquement par le compte administrateur



Maquettage

J'ai ensuite réalisé la maquette avec le logiciel Adobe XD

Etant donné que mon projet est la refonte complète d'un site existant, je devais tout d'abord présenter mon idée du changement visuel du site au client afin d'obtenir son approbation.

J'ai donc passé en revue l'intégralité du site afin de me faire une idée de l'identité visuelle actuelle afin de déterminer les éléments que je pourrais garder de la charte graphique pour les réintégrer au nouveau site ou les transformer.

Pour une première ébauche, je me suis basé sur le site actuel que j'ai remis légèrement au gout du jour afin de proposer une première vue à mon client en ne modifiant que la partie visuelle du site, mais tout en reprenant ses textes et images

The image displays three wireframe prototypes of a website for "Mon P'tit Truc En Bois".

Landing Page: Features a header with the logo and navigation. Below is a section titled "Bienvenue sur le site" with text about original ideas for wooden gifts. A "Chantournage et Pyrogravure" section lists products like wooden boxes, bracelets, and photo puzzles. A "Tournage sur bois" section lists items like wooden cars and planes.

Contact Page: Titled "Besoin de renseignement?", it asks users to complete a form. Fields include "Vous êtes..." (Particulier or Professionnel), "Civilité" (Madame or Monsieur), "Nom", "Prénom", "Adresse Email", "Téléphone", and "Date de naissance".

Product Page: Titled "Boite à dents", it shows a wooden tooth box. Text: "Réalisée en Bois de Hêtre 10€ pièce Personnalisable". It says "Existe en deux versions" and shows "Modèle Ionique" and "Modèle Dorique". Below are images of the box in three states: closed, open, and interior view. A "Commander" button is at the bottom.

Suite à l'acceptation du changement de mise en forme, j'ai entamé la modification complète du site afin de le rendre actuel et compréhensible pour le plus grand nombre.

J'ai donc fait une étude de marché des sites équivalents afin de me faire une idée des tendances actuelles et ainsi le rendre accessible et moderne.

J'ai donc orienté mes changements de couleurs vers une charte graphique qui ne laisserait aucun doute au nouveau visiteur sur la nature du site. J'ai pour cela utilisé des couleurs qui évoquent les différentes essences de bois, du clair au foncé.

J'ai aussi cherché un moyen de conserver la couleur rose à laquelle tenait mon client, que j'ai fait le choix d'intégrer en titre des pages.

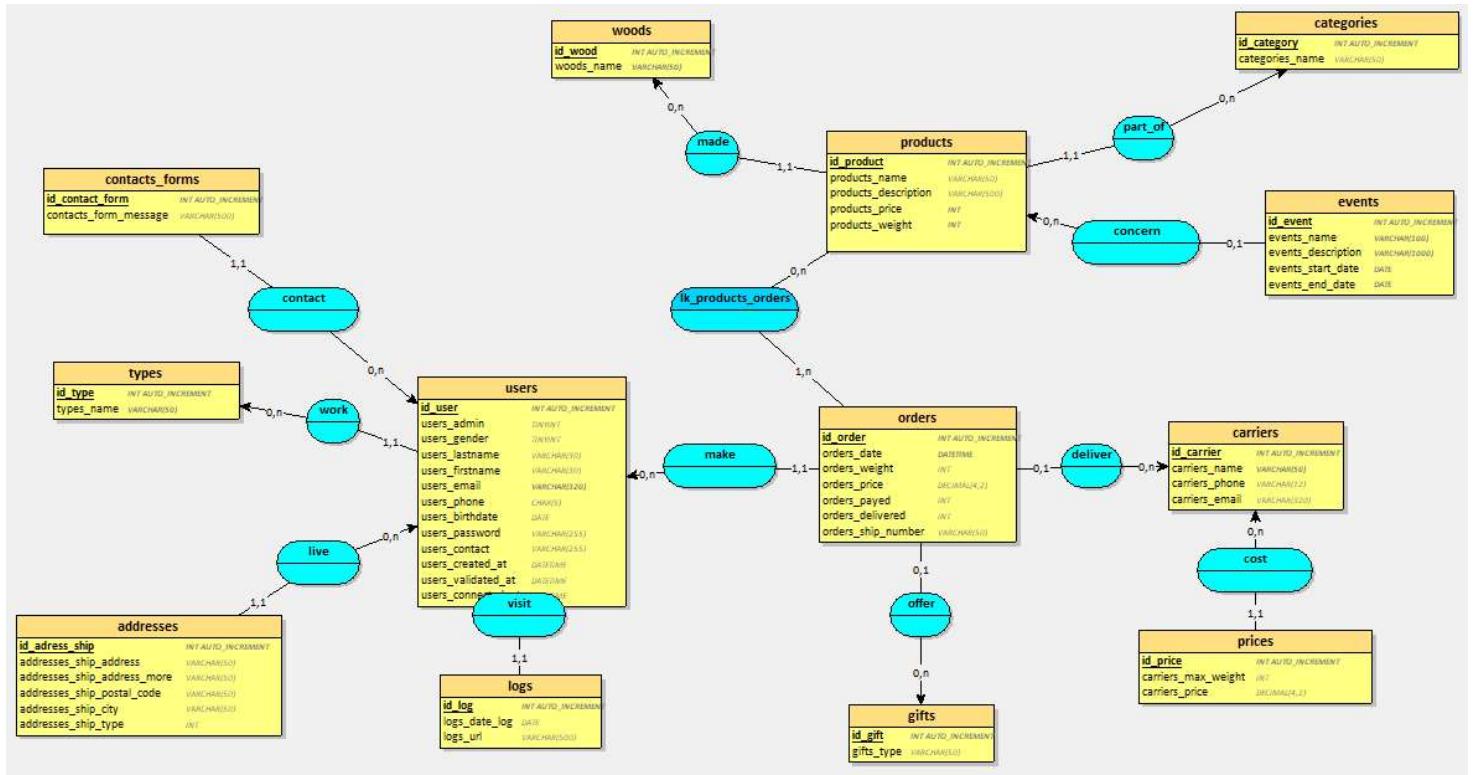
Conception de la base de données

À l'aide de la carte mentale, j'ai listé l'ensemble de tous les éléments qui devraient être présents dans la base de données.

J'ai identifié les besoins réels actuels ainsi que les probables évolutions afin de créer un MCD (Modèle Conceptuel de Données) le plus efficace possible et évolutif si besoin.

Cette étape est très importante car des relations peuvent exister entre les différentes tables. Toutes les relations doivent être soigneusement réfléchies car une fois la base de données créée, si des modifications doivent être apportées, cela peut entraîner des soucis pouvant mener à la refonte complète de la base de données.

Suite à cette réflexion, j'ai déterminé que la base de données serait composée de deux parties distinctes, les utilisateurs et leur gestion, les produits et leur gestion.



MCD (Modèle Conceptuel de Données)

J'ai donc travaillé sur ces deux parties, afin que chacune soit la plus optimisée possible.

Le MCD est donc constitué de 13 tables :

- 5 tables utilisateur
- 8 tables produits

Les 5 tables utilisateur sont :

- “`contacs_form`” : permet aux visiteurs et/ou utilisateurs d’envoyer un message.
 - o S'il s'agit d'un visiteur, un compte lui sera pré-enregistré
 - o S'il s'agit d'un utilisateur, ses informations de profil seront utilisées pour préremplir le formulaire
- “`types`” : permet de connaître le type d'utilisateur (particulier, professionnel, association...)
- “`addresses`” : liste des adresses utilisées par les utilisateurs, que ce soit leur adresse principale ou une adresse de livraison
- “`logs`” : table de suivi des pages visitées par les visiteurs / utilisateurs afin de connaitre les pages les plus visitées, le nombre de vues...

- “users” : informations du profil d’un utilisateur :
 - Statut administrateur
 - Genre
 - Nom
 - Prénom
 - Adresse mail
 - Date de naissance
 - Mot de passe (hashed – pour la sécurisation)
 - Contact (téléphone, mail...)
 - Date de création
 - Date de validation
 - Date de dernière connexion

Les 8 tables produits sont les suivantes :

- “woods” : liste des essences de bois utilisées
- “categories” : liste des catégories de produit :
 - Arts de la table
 - Bureautique
 - Décoration
 - Jouets
- “products” : contenant les informations d’un produit :
 - Nom du produit
 - Description du produit
 - Prix
 - Poids
 - Temps de fabrication
- “events” : informations en cas d’un évènement :
 - nouveau produit,
 - réduction,
 - présence à des festivités extérieures (salon de l’artisanat, exposition...),
 - journées portes ouvertes...
- “carriers” : liste des transporteurs avec leurs informations :
 - Nom
 - Numéro de téléphone
 - Adresse mail

- “prices” : liste des prix des transporteurs en fonction du poids du colis
- “gifts” : si la commande est un cadeau, sélection du type de cadeau
 - Anniversaire
 - Mariage
 - Retraite
 - Fête
- “orders” : liste des commandes avec les informations :
 - Date de la commande du produit
 - Poids du produit
 - La commande est-elle payée
 - La commande est-elle livrée
 - Bordereau de livraison

Les liaisons entre les tables sont les suivantes :

- “users” est liée à :
 - “contacts_form” pour récupérer les informations d'un utilisateur qui enverrait un message
 - “types” pour savoir si l'utilisateur est un particulier, un professionnel...
 - “addresses” pour lier les adresses d'un utilisateur (adresse principale ou de livraison)
 - “logs” pour permettre un suivi des utilisateurs
 - “orders” pour lier une commande à un utilisateur
- “products” est liée à :
 - “woods” pour connaitre l'essence de bois utilisée pour le produit
 - “categories” pour savoir de quelle catégorie est le produit
 - “events” pour lier des produits à des évènements
- “carriers” est liée à :
 - “prices” pour connaitre le prix de la livraison en fonction du poids de la commande
- “orders” est liée à :
 - “products” pour savoir quel produit est commandé et connaitre ses caractéristiques (prix, poids...)
 - “gifts” pour connaitre le type de cadeau (si besoin)
 - “carriers” pour connaitre le transporteur choisi

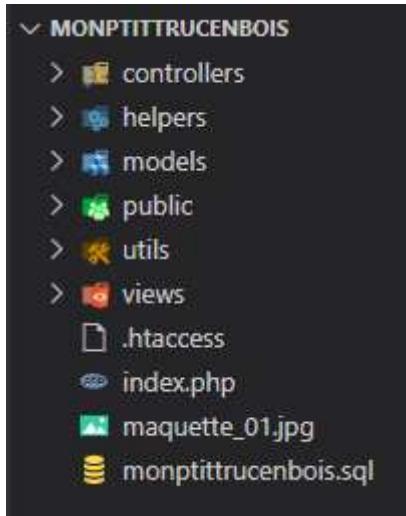
Architecture MVC

L'architecture MVC (Model-View-Controller), est l'une des architectures logicielles les plus utilisées pour les applications Web. Elle permet la structuration d'un projet en trois parties.

Les trois parties sont : Modèle (Model), Vue (View), Contrôleur (Controller)

Composition de l'architecture MVC

- **Modèle** : un noyau de l'application qui gère les données, permet de récupérer les informations dans la base de données, de les organiser pour qu'elles puissent ensuite être traitées par le contrôleur.
- **Vue** : composant graphique de l'interface qui permet de présenter les données du modèle à l'utilisateur.
- **Contrôleur** : composant responsable des prises de décision, gère la logique du code qui prend des décisions, il est l'intermédiaire entre le modèle et la vue.



Sécurisation

Front-end

Sécurisation des balises <input> à l'aide des “pattern”, “required” et “min / max”

- **Pattern :**

Mise en place de pattern sur les champs de formulaire afin de filtrer les données entrées

- **Required:**

Oblige la saisie de données dans le champ renseigné afin d'éviter l'envoi d'un formulaire avec des données vides

- **Min / Max:**

Mise en place d'attributs “min” et “max” afin de limiter le nombre de caractères autorisés à la saisie dans une balise de type input

Back-end

Sécurisation des données à l'aide de fonctions PHP

- **Intval :**

Retourne la valeur numérique entière équivalente d'une variable

- **Filter_input :**

Récupère une variable externe et la filtre

- **Filter_var :**

Filtre une variable avec un filtre spécifique

Inscription

L'inscription au site a été sécurisée à l'aide d'un mail de confirmation envoyé lors de la validation du formulaire d'inscription à l'adresse renseignée. Ce mail comprend un lien de redirection vers la page de validation comprenant un token.

Lors de l'envoi du mail, le token est généré en intégrant l'adresse mail de l'utilisateur ainsi qu'une durée de validité d'une heure et est ajouté au lien de validation du compte.

```
if($isUserRegistered){
    //envoi d'un mail avec lien contenant un jwt
    $subject = "Validez votre inscription";
    $payload = array('email'=> $email, 'exp'=>(time() + 3600));
    $token = JWT::generate($payload);
    $message = 'Merci de valider votre compte en cliquant sur ce lien: <a href="'. $_SERVER['HTTP_ORIGIN']. '/controllers/signup_validate_Controller.php?token='.$token.'">Cliquez ici</a>';
    mail($email, $subject, $message);
    header('location: /connexion.html');
    exit;
} else {
    $errors['email'] = 'Un problème est survenu';
}
```

Ainsi, lors de l'accès à la page de validation, le token est décodé et contrôlé afin de vérifier qu'il s'agisse du lien envoyé et que l'adresse mail dans le token corresponde bien à l'adresse mail à laquelle a été envoyée le lien.

```
//----- IF SEND = GET -----//
if($signature_url_encoded === $signature_provided){
    return json_decode($payload);
} else {
    return false;
}
```

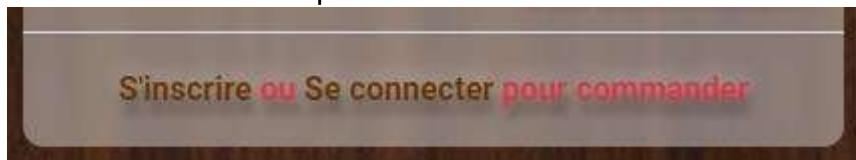
Jeu d'essai

Réalisation de la gestion des commandes

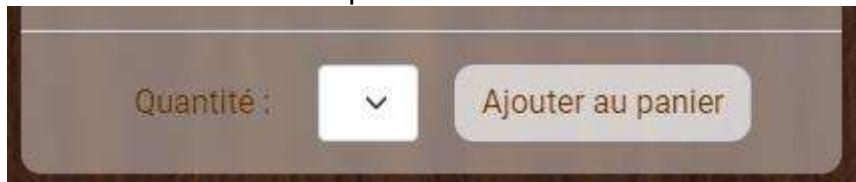
Les commandes sont gérées depuis l'interface d'utilisateur mais intègrent un critère important, un visiteur ne peut pas avoir accès à la partie "commande de produits" car celle-ci est liée à un profil utilisateur.

Il a donc fallu que je paramètre l'affichage des informations de produit selon que la personne soit un visiteur ou un utilisateur.

Vue d'une personne non connectée :



Vue d'une personne connectée :



De plus, lors de la commande d'un produit, ce dernier est ajouté à la liste des produits de la commande en cours.

Si aucune commande n'existe, elle est automatiquement créée et consultable dans le profil, dans l'encart nommé "Ma commande en cours".

Cette partie regroupe la liste de tous les produits mis en commande avec leurs informations respectives :

- Le nom du produit,
- La quantité souhaitée,
- Le prix unitaire du produit,
- Le prix total par produit
-

Il est possible, en cas d'erreur ou de changement d'avis, de modifier la quantité souhaitée d'un produit ou de le supprimer de la commande.

Produit	Quantité	Prix unitaire	Prix total		
Assiette creuse	6	30	180	Modifier	X
Bol (grand)	1	20	20	Modifier	X

Sont indiqués en dessous de la liste, le nombre total d'articles et le poids total de la commande.

Nombre total d'articles : 12	Poids total de la commande : 4.9 kilos
------------------------------	--

Il est également demandé à l'utilisateur de choisir avec quel transporteur il souhaite que son colis lui parvienne.

Choix du transporteur :	Chronopost	Enregistrer
-------------------------	------------	-------------

Ce choix ajoute au prix total de la commande le prix du transport selon le transporteur choisi et le poids de la commande

Prix du transport : 13.90	Montant total de la commande : 353.9 €
---------------------------	--

En cas de modification des quantités, le choix du transporteur est supprimé afin de permettre à l'utilisateur de calculer le prix de transport selon le transporteur

Une fois toutes les informations remplies, l'utilisateur clique sur le bouton "Confirmer la commande" qui le redirige alors vers le mode de paiement

Description de la veille

Les vulnérabilités d'un site web et leur sécurité

La sécurité des sites web est un enjeu majeur pour les entreprises. Etant exposés au public, tous ces systèmes sont des cibles de choix pour des personnes mal intentionnées, qui profitent de nombreuses vulnérabilités au niveau des fonctionnalités et autres composantes des sites web : serveurs, données, authentification, gestion des sessions ou contrôle d'accès. Cette sécurité passe par le fait de se protéger contre les intrusions malveillantes mais à aussi un but commercial afin de rassurer nos clients et de tout mettre en œuvre pour les protéger même si le risque zéro n'existe pas.

Pour contrer ces intrusions, il faut bien sur les connaître.

Faille XSS

La faille XSS est un type de faille de sécurité des sites web que l'on trouve dans les applications web mal sécurisées.

Le principe de cette faille est d'injecter du code malveillant en langage javascript dans un site web vulnérable. Par exemple en déposant un message dans un forum qui redirige l'internaute vers un faux site (phishing) ou qui vole ses informations (cookies)

- Comment s'en protéger

En sécurisant toutes les entrées et envois de donnée faite par l'utilisateur.

Elles se font particulièrement dans les champs de formulaires. Lors de la récupération de ces données, il est indispensable de les contrôler et de les nettoyer afin d'éviter tout risque.

Les fonctions PHP permettent d'assainir les données telles que trim(), filter_input(FILTER_SANITIZE...), filter_var(FILTER_VALIDATE...)

Injection SQL

Les attaques par injection de commandes SQL exploitent les failles de sécurité d'une application qui interagit avec des bases de données.

L'attaque SQL consiste à modifier une requête SQL en cours par l'injection d'un morceau de requête non prévu, souvent par le biais d'un formulaire.

La personne malveillante peut ainsi accéder à la base de données, mais aussi modifier le contenu et donc compromettre la sécurité du système

- Comment s'en protéger

En sécurisant les requêtes le plus possible. L'utilisation des marqueurs nominatifs et la

fonction “bindValue” sont indispensables

Il faut également utiliser des requêtes préparées. Une requête préparée est un modèle de requête SQL dans lequel vous spécifiez des paramètres à un stade ultérieur pour l'exécuter

Faille CSRF

Il s'agit d'effectuer une action visant un site ou une page précise en utilisant l'utilisateur comme déclencheur, sans qu'il en ait conscience. L'utilisateur malveillant va deviner un lien qu'un utilisateur utilise habituellement et faire en sorte qu'il clique lui-même sur ce lien

- **Comment s'en protéger**

Pour se protéger contre cette faille, on utilise généralement l'authentification par jeton.

Un jeton (appelé “token” en anglais) est un nombre ou une chaîne de caractère aléatoire qui va être testé avant toute modification ou édition d'un article.

Attaque par Brute Force

Les attaques par Brute Force consistent à trouver un mot de passe ou une clé en testant successivement toutes les combinaisons possibles. L'attaque peut se faire soit par ordre alphabétique, soit par les mots les plus utilisés connus. Cependant, l'ordre du test peut être optimisé par la consultation de mot de passe les plus souvent utilisé, par exemple

- **Comment s'en protéger**

En demandant aux utilisateurs des mots de passe complexes, mettre en place des captchas ou mettre en place des compteurs d'essai

Situation de travail

Lors de la réalisation de mon projet, j'ai été confronté à un souci de persistance de données. En effet, lors de l'affichage de pages ou de mise à jour de l'affichage, j'utilise des variables auxquelles j'attribue des valeurs afin de confirmer la bonne exécution de la requête ou provisoirement lors de traitement de données.

Mon souci était que ces variables conservaient leurs valeurs, ce qui provoquait des problèmes de persistances de valeurs qui généraient des erreurs lors d'envoi de formulaire ou de nouvelle actualisation d'une même page.

J'ai donc fait des recherches sur la possibilité de "détruire" une variable ou d'effacer leur valeur.

Lors de mes recherches, j'ai découvert la fonction PHP `unset()` qui, comme la documentation l'explique, de "détruire" une variable.

unset

(PHP 4, PHP 5, PHP 7, PHP 8)

`unset` — Détruit une variable

La documentation indique également la façon de la mettre en place et les détails de fonctionnement

Description

```
unset(mixed $var, mixed ...$vars): void
```

`unset()` détruit la ou les variables dont le nom a été passé en argument `var`.

Le comportement de `unset()` à l'intérieur d'une fonction peut varier suivant le type de variable que vous voulez détruire.

Si une variable globale est détruite avec `unset()` depuis une fonction, seule la variable locale sera détruite. La variable globale gardera la valeur acquise avant l'appel à `unset()`.

Dans différentes pages, j'ai créé des variables (`$ResultWood`, `$ResultCategory...`) qui me permettent d'afficher la réussite ou l'échec de modification des informations, de suppression, de commandes, qui sont temporaires.

Le souci que j'avais était que je ne pouvais pas vider ou réécrire la valeur de la variable car elle était contrôlée afin de modifier l'affichage en fonction de sa valeur. Il fallait donc que la

variable n'existe qu'une fois afin que le code de test ne la retrouve pas lors d'une mise à jour de l'affichage.

```
if ($resultCarrier == 0) { ?>
    <div class="col-12 my-2 text-center align-self-center errorBox d-flex justify-content-center justify-self-center">
        <span class="align-self-center errorForm">Erreur, le transporteur n'a pas été enregistré</span>
    </div>
<?php } elseif ($resultCarrier == 1) { ?>
    <div class="col-12 my-2 text-center align-self-center validBox d-flex justify-content-center justify-self-center">
        <span class="align-self-center validForm">Le transporteur a bien été enregistré</span>
    </div>
<?php } elseif ($resultCarrier == 2) { ?>
    <div class="col-12 my-2 text-center align-self-center validBox d-flex justify-content-center justify-self-center">
        <span class="align-self-center validForm">Le transporteur a bien été mis à jour</span>
    </div>
<?php } elseif ($resultCarrier == 3) { ?>
    <div class="col-12 my-2 text-center align-self-center validBox d-flex justify-content-center justify-self-center">
        <span class="align-self-center validForm">Le transporteur a bien été supprimé</span>
    </div>
<?php }
unset($resultCarrier);
```

La fonction “*unset()*” me permet donc de détruire la variable une fois affichée afin que lors d'une mise à jour de l'affichage, elle n'existe plus.

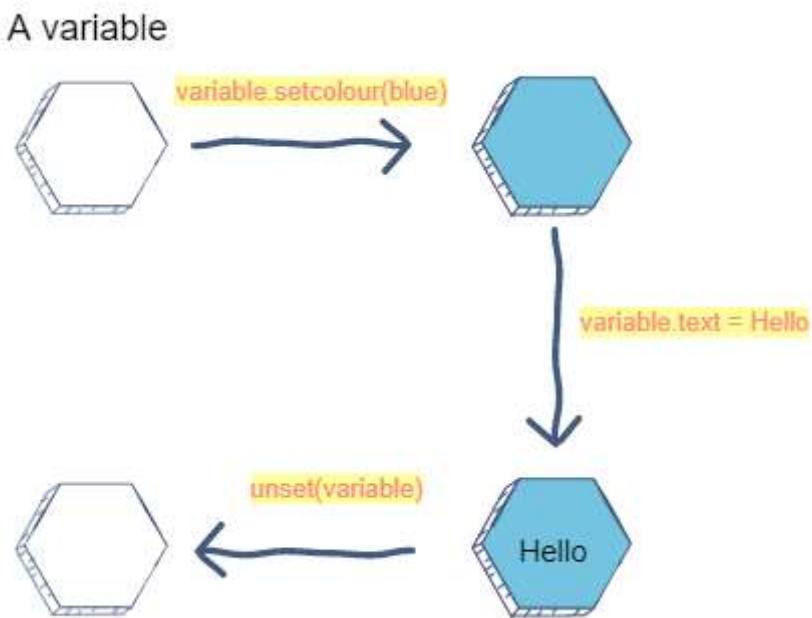
Extrait site anglophone

Version du site en anglais :

What is the PHP unset() function?

The **unset()** function in PHP resets any variable. If **unset()** is called inside a user-defined function, it unsets the local variables. If a user wants to unset the global variable inside the function, then he/she has to use **\$_GLOBALS** array to do so. The **unset()** function has no return value.

The illustration below explains how a variable is **unset()**:



Examples

Code 1

The coded example below unsets the local variable:

```
1 <?php
2 $my_var='Hello User';
3 echo " before unset : ".$my_var;
4 echo"\n";
5 unset($my_var);
6 echo "after unset : ".$my_var;
7 ?>
```

Run

Code 2

The coded example below unsets the global variable using `$_GLOBALS` array:

```
1 <?php
2 $my_var='Hello User';
3
4 function unset_var()
5 {
6     global $my_var;
7     echo "Before unset and inside function : ".$my_var."\n";
8     unset($_GLOBALS['my_var']);
9 }
10 echo "Outside function before using function : ".$my_var."\n";
11 unset_var();
12 echo "Outside function after using function : ".$my_var."\n";
13 ?>
```

Run

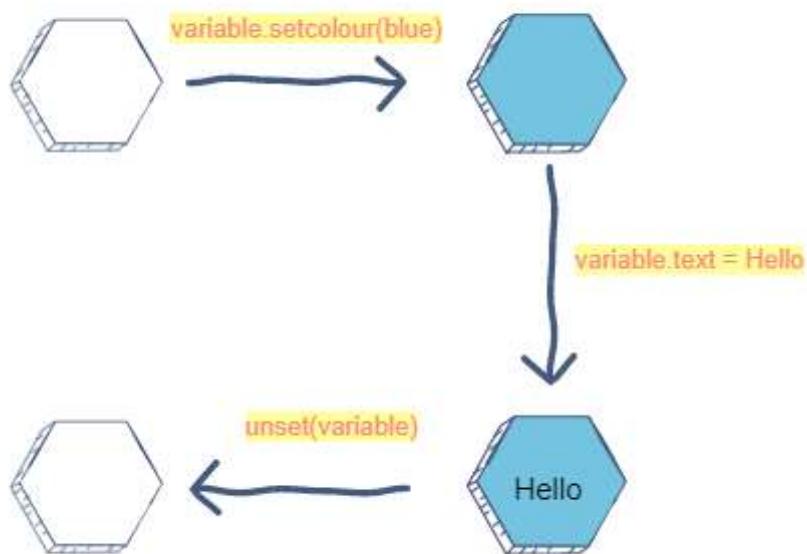
Traduction en français :

Qu'est-ce que la fonction PHP `unset()` ?

La fonction PHP `unset()` réinitialise n'importe quelle fonction. Si `unset()` est appelé à l'intérieur d'une fonction définie par l'utilisateur, cela réinitialise les variables locales. Si un utilisateur veut réinitialiser globalement la variable dans une fonction, alors il/elle doit pour cela utiliser le tableau `$_GLOBALS`. La fonction `unset()` n'a pas de valeur de retour.

L'illustration ci-dessous explique comment une variable est unset() :

A variable



Exemples

Code 1

L'exemple codé si dessous réinitialise une variable locale :

```
1 <?php
2 $my_var='Hello User';
3 echo " before unset : ".$my_var;
4 echo"\n";
5 unset($my_var);
6 echo "after unset : " . $my_var;
7 ?>
```

Code 2

L'exemple codé ci-dessous réinitialise la variable globale en utilisant le tableau `$_GLOBALS` :

```
1 <?php
2 $my_var='Hello User';
3
4 function unset_var()
5 {
6     global $my_var;
7     echo "Before unset and inside function : ".$my_var."\n";
8     unset($GLOBALS['my_var']);
9 }
10 echo "Outside function before using function : ".$my_var."\n";
11 unset_var();
12 echo "Outside function after using function : ".$my_var."\n";
13 ?>
```

Run



Conclusion

Nous voilà désormais au terme de ces six mois de formation très riches techniquement et humainement.

Avant d'intégrer la formation, je disposais d'une expérience de 7 ans dans le codage de site web (dont 5 professionnellement), que je considérai comme importante. Mais au cours de ses 6 mois, je me suis rendu compte que mes connaissances n'étaient que la base de la connaissance du développement web dont je n'avais pas suivi les évolutions, et que cela demandait de l'investissement personnel et le besoin de sans arrêt se demander si l'on ne peut pas améliorer le système, simplifier le code ou le rendre plus sécurisé.

Cette remise en question m'a permis de confirmer mon envie de faire partie des acteurs du web.

En effet, le monde du codage web est encore extrêmement ouvert et porteur d'avenir, beaucoup de langages existent et de nouveaux peuvent surgir et devenir des références. De plus, la sécurisation du web et des données est un secteur qui prend une place de plus en plus grande.

Je vais principalement porter mon attention sur la veille technologique et la mise en conformité du web, car mon projet m'a permis de réaliser que la mise à jour de sites web ou la création pour des particuliers ou des sociétés est très intéressante pour moi.

