Rapport Patisport

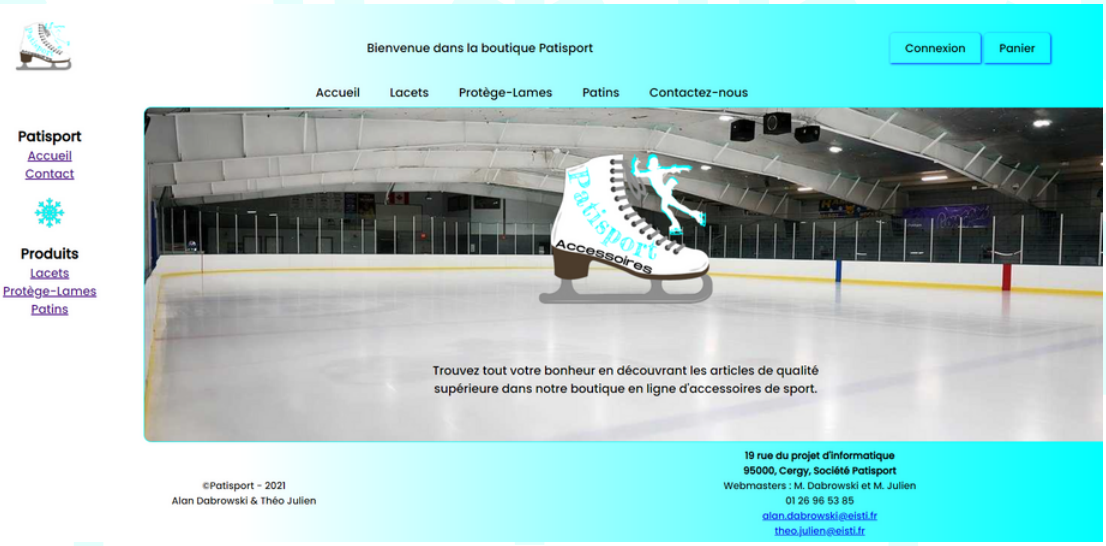
DABROWSKI ALAN - JULIEN THÉO

MODULE DÉVELOPPEMENT WEB
ING1 GI1 - 2021

Sommaire

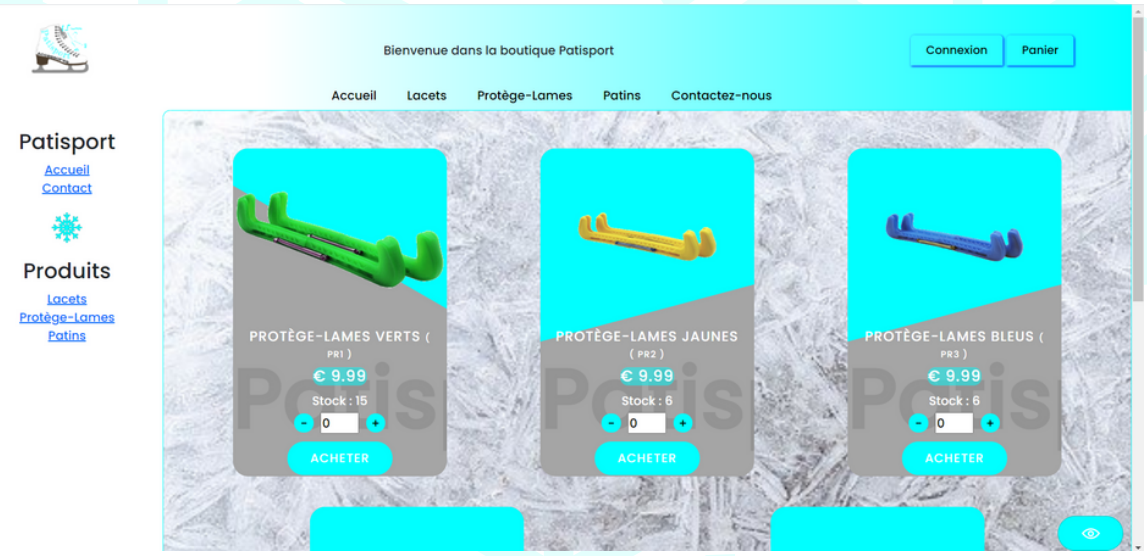
Présentation

Le projet **Patisport** est né de notre intérêt envers le patinage artistique. Ainsi nous avons souhaité réaliser une boutique d'accessoires de patinage artistique comme projet du module développement Web.



Page accueil

La première page du site est bien évidemment une page d'accueil contenant notre logo et une ligne de présentation de la boutique. La structure du site sera la même pour la plupart des pages (excepté la page de connexion et le panier). Cette structure correspond à une barre de navigation en haut du site qui restera fixe si l'utilisateur décide de faire défiler les pages vers le bas. Dans cette barre de navigation nous avons deux boutons sur la droite : un pour se connecter/déconnecter et un pour accéder au panier qui sera obligatoirement vide si l'utilisateur n'est pas authentifié. Nous avons ensuite accès à deux boutons renvoyant sur la page d'accueil ou sur la page de contact. En complément de ces deux boutons nous avons autant de boutons en plus qu'il y'a de catégories dans le site (initialement trois). Nous disposons d'un menu vertical à gauche permettant lui aussi de naviguer à travers le site en cliquant sur la page à visiter. La majeure partie de l'écran est associée au contenu (qui change selon la page), c'est ici la photo d'une patinoire qui représente la taille du contenu de la page. Un pied de page est aussi présent dans la structure du site dans lequel les coordonnées et les détenteurs du site sont indiqués.



Page produits

La page des produits est dynamique c'est-à-dire qu'elle est similaire quels que soient les produits affichés. Nous constatons sur la capture d'écran que le premier article (protège-lames verts) est plus gros que les autres ; cela correspond à l'animation au passage de la souris sur l'article (un zoom sur le produit et un changement d'orientation de la séparation des deux couleurs sur le fond). Pour chaque produit nous pouvons ajouter la quantité nécessaire au panier en incrémentant ou décrémentant le nombre entre les deux boutons. Pour ajouter au panier le produit, il suffit de cliquer sur le bouton "Acheter".

Page contact

Cette page est consacrée à contacter le support en cas de problème. Nous pouvons estimer que dans un site en condition réelle, une catégorie destinée à la raison du contact pourrait être ajoutée afin de rediriger automatiquement le mail envoyé. Actuellement cette page envoie un mail au webmaster (à condition d'avoir configuré un serveur de mail préalablement). Toutes les données sont vérifiées du côté client et du côté serveur afin de garantir une bonne expérience d'utilisation du site et d'éviter l'utilisation malveillante de cette page indirectement liée au mail des webmasters.

Page connexion

La page de connexion du site est réservée à la connexion des membres et de l'administrateur du site. La connexion via ses identifiants est obligatoire afin de pouvoir ajouter des articles au panier et commander. Voici quelques combinaisons d'identifiant/mot de passe pour se connecter au site car la page d'enregistrement n'étant pas demandée, des identifiants ont été préalablement créés.

Nom d'utilisateur :	root	theo	theo2	alan
Mot de passe :	root	julien	julien2	dabrowski
Rôle :	administrateur	membre	membre	membre

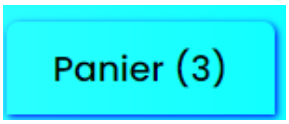
Page panier

La page panier est en réalité divisée en trois parties. Dans un premier temps nous avons la panier tel quel avec la possibilité de supprimer des articles achetés par erreur, le prix total est calculé en incluant les frais. Une fois notre panier validé, une page de saisie d'informations est à remplir afin de transmettre les coordonnées du client. Une fois les deux précédentes pages complétées, un récapitulatif est affiché. Le client peut alors valider la commande et par conséquent acheter les articles dont le stock sera mis à jour dans la base de donnée.

Détails techniques

Barre de navigation

- Le bouton de connexion change en fonction de la connexion de l'utilisateur, le bouton deviendra "[pseudo] - Déconnexion" s'il est connecté. Appuyer sur le bouton permettra de se déconnecter et donc de vider le panier si l'utilisateur était connecté puis de rediriger vers la page de connexion. Sinon, l'utilisateur sera uniquement redirigé vers la page de connexion.
- Le bouton panier contient le nombre d'articles dans le panier si l'utilisateur est connecté. Il redirige vers la page du panier même si l'utilisateur n'est pas connecté.
- Les boutons qui correspondent aux catégories évoluent en fonction du nombre de catégorie. S'il y'a 4 catégories alors il y aura 4 boutons de redirection.




```php
foreach($categories as $value){
    echo "<a href='produits.php?categorie=".$value["id"]."'>".$value["label"]."</a>";
}
```

index.php

- Lorsque le paramètre "reset" contenant la valeur "true" est passé en argument dans l'URL, le panier est remis à zéro. Nous utilisons cette fonctionnalité une fois qu'un commande a été réalisée entièrement afin de ne pas avoir à vider son panier pour de nouveaux achats.

/index.php?reset=true

contact.php

- Le formulaire est vérifié dans la partie JavaScript donc coté client et dans la partie PHP donc coté serveur. Tous les champs sont vérifiés et affichés en rouge s'il ne sont pas conformes.
- Si le serveur est configuré pour envoyer des mails alors le mail sera envoyé à l'adresse "julientheo@eisti.eu".

```php
/* Vérification formulaire */
if(!empty($_POST)){
    include './php/functions.php';
    $res = verifContact();
    $wrong = $res[0];
    $valid = $res[1];
}
```

```php
mail($to, $subject, $message);
```

produits.php

- Les boutons "+" et "-" permettent d'ajuster la quantité du produit à ajouter au panier dans la limite des stocks disponibles. La quantité ne peut pas être négative.

```
<?php echo "onclick='del_stock(".($i+1).")'"; ?>
<?php echo "onclick='add_stock(".($i+1).")'"; ?>
```

- Si l'utilisateur n'est pas connecté alors nous affichons un modal pour l'avertir qu'il faut se connecter.

```
var myModal = new bootstrap.Modal(document.getElementById('myModal'));
myModal.show();
```

- Une vérification des stocks est réalisée lors de l'ajout d'un produit dans le panier. Il n'est pas non plus possible d'ajouter un produit dont la quantité est 0. Si le panier possède déjà le produit alors nous allons rajouter la quantité à l'ancienne quantité.

```
if(verifstock($tableau,$produits)>=0 && intval($_POST["nombre_produit"])>0){
    if(in_panier($tableau)){
        array_push($_SESSION["panier"],$tableau);
```

- Le stock peut être affiché/caché par l'administrateur. Le stock n'est pas visible pour les visiteurs ou les membres.

connexion.php

- Un utilisateur connecté et dont le paramètre "deconnexion=yes" est passé en argument dans l'URL permet de détruire la session et donc de pouvoir se reconnecter.
- Un utilisateur déjà connecté sera redirigé vers la page index.php.
- Les mots de passe sont hashés.
- L'utilisateur est notifié en cas d'erreur dans la combinaison d'identifiant.

```
session_destroy();
header("Location: connexion.php");
```

```
hash("sha256",$_POST["password"]);
```

Injections SQL

- Les fonctions permettant une interaction avec la base de données sont protégées contre les injections SQL.

```
$req = $GLOBALS['cnx'] -> prepare('SELECT * FROM produits WHERE ref = ? LIMIT 1;');
$req -> execute(array($ref));
```

Failles XSS

- Les failles XSS peuvent être exploitées uniquement lors du remplissage du formulaire de coordonnées lors des informations de livraison (informations affichées sur la page suivante). Nous avons donc protégé notre site contre les failles XSS à cet endroit.

Pays : <script>alert('Yo');</script>

```
<?php echo htmlspecialchars($_POST["prenom"]); ?>
```

panier.php

- La page du panier est découpée en trois parties.

```php
if(!empty($_POST["prenom"]) && isset($_SESSION["user"])){
    include "./php/confirmCommande.php";
}else{
    if(isset($_GET["page"]) && intval($_GET["page"]) == 2 && isset($_SESSION["user"]) && count($_SESSION["panier"])>0){
        include "./php/infoClient.php";
    }else{
        include "./php/recapPanier.php";
    }
}
```

- Le panier est accessible pour tout le monde. Pour accéder à la page de remplissage du formulaire, il faut cliquer sur valider dans le récapitulatif du panier. Pour ensuite accéder au récapitulatif de commande, il faut que l'utilisateur ait préalablement rempli correctement le formulaire de livraison.
- Toutes les données du formulaire sont vérifiées par du JavaScript afin de mettre les champs non conformes en surbrillance rouge.

```javascript
if(nom.value.trim() == ""){
    ok=false;
    nom.classList.add("wrong");
}else{
    nom.classList.remove("wrong");
```

- Toutes les données du formulaire envoyées sont vérifiées par du PHP et l'utilisateur est redirigé vers la première page du panier si le formulaire n'est pas conforme dans le récapitulatif de commande.

```php
|| !isset($_POST["mail"])
|| preg_match("/^\S+@\S+\.\S+$/", $_POST["mail"])==0
|| !isset($_POST["adresseLivr"])
|| trim($_POST["adresseLivr"]) == ""
```

- Avant de modifier la base de données avec les nouvelles valeurs des stocks en fonction de ce que le client a acheté, une vérification totale est effectuée sur les articles et les quantités du panier. Les stocks sont aussi comparés avec ceux de la base de données pour éviter de vendre plus de stock qu'il n'y en a. Cette vérification permet aussi d'éviter les fraudes telles que des quantités négatives, par exemple, qui permettraient d'avoir un montant à payer négatif.

AJAX

- AJAX est utilisé pour l'ajustement des stocks une fois que la commande a été validée et donc que les produits doivent être déduit des stocks disponible. Ainsi nous adressons une requête HTTP à l'adresse "api/updateStock.php".

```javascript
$.post( "api/updateStock.php", {informations})
.done(function(data){
    if(data="ok"){
        document.getElementById("write_message").innerHTML = "Votre commande a été prise en compte.</br> Les stocks ont été ajustés.";
    }else{
        document.getElementById("write_message").innerHTML = "Un problème a été rencontré durant le processus d'ajustement des stocks.</br> Veui
    }
})
.fail(function() {
    document.getElementById("write_message").innerHTML = "Un problème a été rencontré durant le processus d'ajustement des stocks.</br> Veuillez
})
.always(function() {
    var myModal = new bootstrap.Modal(document.getElementById('staticBackdrop'),{backdrop:'static'});
    myModal.show();
});
```

- Le fichier updateStock.php s'occupe de vérifier les stocks disponibles et modifier la base de données avec les nouveaux stocks.

```php
if(!empty($_POST)){
    $panier = $_POST["informations"];
    if(verificationFinale($panier)){
        foreach ($panier as $value) {
```

```php
foreach ($panier as $value) {
    $stockTotal = getStock($value[0]);
    $nouveauStock = $stockTotal - $value[1];
    if(!updateStock($value[0],$nouveauStock)){
        echo "Erreur";
        return;
    };
```

Changements apportés

Changements techniques

- Les variables de session comprenant les catégories et les produits ont été remplacées par des fonctions liées à la base de données. Les variables de session sont uniquement utilisées pour la gestion du panier et pour la connexion.
- Une base de données à été mise en place. Dans le dossier "sql" nous pouvons retrouver deux script : un pour la structure de la base de donnée ("patisport.sql") et un pour les données initiales ("patisportdata.sql").
- Il est possible de remplir la base de donnée grâce aux données statiques du site via l'exécution du fichier "scriptSQL.php" dans le dossier "bdd".
- Une commande peut être validée jusqu'à la fin en remplissant le formulaire qui sera vérifié du coté client et du coté serveur.
- Ajout de la partie AJAX à la fin de la commande pour correspondre à l'énoncé du projet.
- Ajustement de certains détails tel que le nom d'utilisateur sur le bouton déconnexion ou le nombre d'article dans le panier sur le bouton panier de la barre de navigation.
- Réalisation de deux bonus : stock visible uniquement par l'administrateur (root) et gestion complète d'une commande de plusieurs articles.
- Utilisation des librairies Bootstrap (composants et mise en page), jQuery (AJAX) et Axios (requêtes HTTPS).

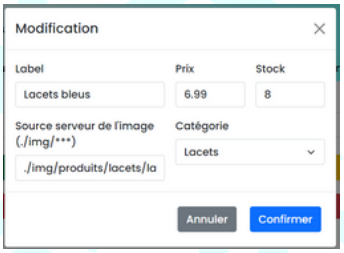
Changements graphiques

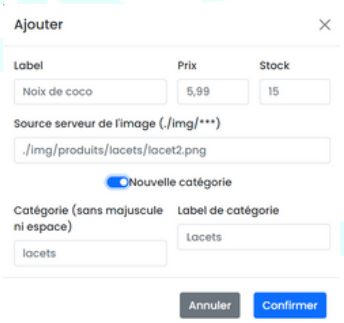
- Nouveau logo

- Harmonisation des éléments (boutons de même taille par exemple)

- Adaptation mobile et tablette du site avec prise de libertés en enlevant le menu vertical et en enlevant la position fixée de la barre de navigation sur mobile

Captures d'écran sur iPhone 5 via l'inspecteur d'élément





admin.php

Le panneau d'administration n'est accessible que par le compte administrateur (root). Il permet d'ajouter, modifier ou supprimer un produit ainsi qu'une catégorie en créant un nouvel article avec une nouvelle catégorie. Cette fonctionnalité vérifie constamment (coté serveur) les droits d'accès et valeurs écrites. Pour les images il faut d'abord mettre les images dans le dossier puis indiquer son lien lors de la création d'un nouvel article. Si le dernier article d'une catégorie est supprimé alors la catégorie est elle aussi supprimée.

Perspectives d'amélioration

Le projet Patisport étant actuellement un projet scolaire et prévu pour un certain nombre d'heures, nous nous sommes concentrés sur ce qui était demandé et nous n'avons pas eu le temps d'ajouter des fonctionnalités coûteuses en temps mais nous vous en faisons part :

- Facture PDF à imprimer lors de la validation complète d'une commande.
- Enregistrement d'utilisateurs.
- Modification d'un compte utilisateur (changement de mot de passe, de mail...).
- Suivi de commande pour l'utilisateur (avancement de la préparation et de l'envoi d'une commande).
- Suivi des commandes pour l'administrateur.
- Connexion plus sécurisée (elle se fait actuellement grâce à la variable $_SESSION).
- Rendre accessible le dossier GitLab à des développeurs de confiance afin d'être plusieurs à développer ce projet.
- Téléchargement des images plutôt que d'entrer le lien lors d'un ajout/modification d'un article dans le panneau d'administration.