

Rapport Projet Web : Bakaraoke

Cecconi Quentin

Chatelet Leo
Sadler Alec

Goyard Louis

May 2020

Contents

1	introduction	2
2	sécurité	2
3	utilisateurs	3
3.1	personnaliser son compte	3
3.2	les playlists	3
3.3	droits des utilisateurs	4
4	conclusion	4

1 Introduction

Lors de conventions basées sur la culture japonaise(japanExpo, bakanim), il n'est pas rare d'y trouver des séances de Karaoké, ou tout un public se regroupe et chante au rythme des plus grands chefs d'oeuvre nippons.

Cependant, si les visiteurs viennent à ces séances, c'est qu'ils s'attendent à chanter des musiques qu'ils connaissent et aiment. Pourtant les playlists sont souvent préfaites, et les "chanteurs" n'ont pas la possibilité de choisir sur quel hymne ils vont épuiser leurs cordes vocales.

Voici donc le site Bakaraoké : un gestionnaire de playlist où les utilisateurs peuvent rajouter à leur guise les musiques qu'ils veulent chanter.

Nous étions 4 pour ce projet, la répartition des tâches fut:

- Châtelet Leo: implémentation des playlists
- Cecconi Quentin: style css et pages html
- Goyard Louis: implémentation de la queue et interface lektor
- Sadler Alec: système d'utilisateurs et formulaires

2 Sécurité

Un minimum de sécurité a été implanté pour éviter des attaques récurrentes comme un ddos ou des injections SQL :

Chaque variable obtenue d'un formulaire via la méthode POST sera d'abord filtré avec la commande htmlspecialchars() pour éviter que des caractères spéciaux apparaissent. Ensuite, ces variables seront rentrées en paramètres dans les commandes SQL via la méthode bindParam du PDO.

Lors d'une création, d'une connexion ou de la modification d'un compte, on vérifie bien que les champs remplis sont bien valides (email au bon format, pas d'espace dans le username), ainsi nous n'aurons pas de risque concernant l'utilisateur qui rentre une commande de type 'DROP TABLE'.

Chaque formulaire aura avant tout une validation `JavaScript` pour ne pas surcharger le serveur par de mauvaises requêtes.

Pour éviter que l'utilisateur ne "spam" les listes de lectures, on utilise le fichier "`ddosPreventer.php`" qui limite à 6 le nombre de requêtes toutes les 30 secondes. On utilise aussi ce fichier au moment du login ou de l'inscription.

3 Lektor

4 La queue

5 Utilisateurs

Lorsque qu'un client arrive pour la première fois sur le site, il n'aura pas accès aux différents services du site. Il devra d'abord se créer un compte sur la page `registration.php`, ici il entrera ses identifiants comme son adresse email, son nom d'utilisateur, et son mot de passe.

Il est à noter qu'un utilisateur ne peut pas avoir d'espace dans son nom, ce qui permet d'avoir une sécurité supplémentaire contre les injections SQL.

Après vérification `javascript` d'un formulaire, on récupère et envoie ces informations à la page `addUser.php` qui va les insérer dans la table "user", le mot de passe sera hashé pour éviter toute tentative de vol de mot de passe. Tout transfert d'information se fera via la méthode POST, afin de transférer les données de manière sécurisée.

Ces informations peuvent être ultérieurement modifiées sur la page `modifyUser.php`, qui enverra les modifications à `modifyUserAccount.php`.

Une fois qu'un utilisateur s'est créé un compte, il peut se connecter via `login.php`. Si il le fait, on démarre une session et on initialise les attributs de la variable de session, c'est avec ces attributs qu'on déterminera si la session est ouverte, et qu'on affichera les cosmétiques de l'utilisateur.

5.1 Personnaliser son compte

Aussi, après ajout d'un utilisateur dans "user", on insère une nouvelle ligne dans la table "UserCosmetics", cette table permet de savoir quel sont les cosmétiques choisis par l'utilisateur. Chaque utilisateur aura accès à une liste d'images de profil et de titres qu'il pourra sélectionner pour customiser son profil. Ces cosmétiques sont contenus dans les tables "Image" et "Titles".

Ces images ne sont pas toutes disponibles dès le départ. En effet chaque utilisateur possède des points d'expérience, initialisés à 0 à la création du compte, qui peuvent être gagnés lorsqu'un kara est rajouté à une playlist. Les images se

débloquent au fur et à mesure que l'utilisateur passe du temps sur le site. Sur ChangePP.php seules les images et titres dont `xpNeeded;SESSION['xp']` sont affichés.

Pour pouvoir modifier son compte, l'utilisateur doit se rendre sur `changePP.php`, pour modifier son image de profil et/ou son titre. Un formulaire envoie les informations à `modifyUserCosmetics.php`. L'utilisateur a le choix entre les différentes images contenues dans la table "Images" et les différents titres dans "Titles".

5.2 Les playlists

Un utilisateur peut créer ses propres playlists de karas disponibles dans la table "Karas". D'ici il pourra ajouter cette playlist dans la Queue du lecteur, ou simplement retrouver les karas qu'il préfère afin de les ajouter. Toutes ces informations sont contenues dans la table Playlist, et les utilisateurs peuvent regarder les playlists des autres utilisateurs si elles sont paramétrées comme étant publique.

Une playlist ne peut cependant être éditée que par son créateur.

5.3 Droits des utilisateurs

Lorsqu'un utilisateur se register dans la base de donnée, on lui attribut un droit 0. Les différents droits sont définis par des entiers:

- 0 pour un utilisateur lambda
- 1 pour un administrateur
- 2 pour un super-administrateur

Un utilisateur a la possibilité de révoquer ou d'augmenter les droits d'un utilisateur ayant un droit inférieur. Ceci se fait sur la page `admin.php`, page seulement accessible par les admins. C'est en vérifiant les attributs de la session actuelle (SESSION) qu'on détermine si l'utilisateur est bien un admin.

6 Conclusion

Notre site Bakaraoké a donc rempli les objectifs fixés par le projet, que ce soit la gestion d'utilisateurs avec en plus un ajout de personnalisation, l'utilisation de scripts pour protéger le site ou encore la gestion de tables permettant de gérer les karaokés de la base de donnée et la création de playlists.

Nous pensons que l'amélioration du site se fera à partir de maintenant sur l'approfondissement de la personnalisation des comptes et des playlists, en permettant de créer des playlists collaboratives par la modification de la table pour rajouter un champ collaborateur, ou l'ajout d'une fonctionnalité de lecture directe sur le site en ajoutant le lecteur de vidéos sur le site.