DOCUMENTATION TECHNIQUE

JO FICTIF 2024

Table des matières

Présentation du projet

Pour les Jeux Olympiques 2024, la sécurité est renforcée concernant la fraude des tickets physiques. De ce fait l'administration souhaite mettre en place des e-tickets. Cela implique la création d'un site web permettant l'achat de ticket électronique en ligne.

Spécifications fonctionnelles

Fonctionnalités utilisateurs

Une page d'accueil présente les Jeux Olympiques ainsi que les épreuves.

Une page présente les offres disponibles (1, 2 ou 4 personnes). Nous avons choisi de rendre les offres propres à chaque épreuve. Cela permet d'avoir une page par épreuves présentant toutes les offres de celle-ci. Cela permet également de définir un prix propre à chaque épreuve et non à chaque offre.

Un utilisateur peut sélectionner l'offre qui l'intéresse afin de la mettre dans son panier. Cela crée un ticket provisoire qui n'est pas affilier à un utilisateur connecté car il n'est pas nécessaire de l'être pour glisser des offres dans son panier. Nous utilisons le système de session utilisateur.

Lorsque l'utilisateur veut finaliser son achat, s'il n'est pas connecté, il est alors redirigé vers page de connexion / inscription afin de s'authentifier.

L'inscription d'un utilisateur génère une clé sécrète non divulguée, visible uniquement par le staff.

Lorsque le paiement est finalisé avec succès, une autre clé est générée. Pour ce faire, nous avons choisi de créer la seconde clé sécrète lors de la création du ticket provisoire. Cependant la combinaison des deux clés permettant de sécuriser le billet se fait bien après l'achat et sera stockée dans le ticket électronique passant alors en statut « payé ».

Cette nouvelle clé sert à créer un QR code stocké également dans le ticket électronique.

Fonctionnalités staff

Un espace administrateur doit permettre l'ajout, la modification et la suppression d'offres. Ceci est disponible pour les administrateurs, leur permettant également de créer des comptes employés.

Les employés ont quant à eux la possibilité d'accéder à cet espace d'administrateur uniquement pour la vérification des tickets électroniques.

La sécurité du compte utilisateur doit permettre de s'assurer que l'utilisateur connecté est bien le bon, en ce sens une validation des comptes par email est mise en place.

Enfin l'administrateur doit pouvoir visualiser le nombre de vente par offres.

Spécifications techniques

Le site web sera hébergé avec Heroku.

Back-end

Le back-end est réalisé avec le langage PHP en version 8.2 et le framework Symfony en version 7.1.

MySQL : SGBDR utilisant le langage SQL avec l'addon JawsDB de Heroku.

Front-end

Le front-end est réalisé avec HTML5 avec Twig, le moteur de template de Symfony, CSS3 et JavaScript.

Le framework Bootstrap est également utilisé en version 5.3.

Sécurité

Concernant la sécurité de l'application web, les mots de passe utilisateurs sont « hasher » en « BCRYPT » avant d'être stockés en base de données. De plus la possibilité de se connecter avec Gmail offre la sécurité oAuth2 de Google. A l'inscription, les utilisateurs reçoivent un email de vérification avec un lien permettant de s'assurer qu'il s'agit bien de leur adresse email. Les utilisateurs utilisant le service oAuth2 ne sont pas concerné par cette mesure.

Une mesure de restriction des mots de passes est présente afin que ces derniers contiennent minimum 8 caractères avec une majuscule, une minuscule et un caractère spécial.

Doctrine permet de sécuriser le site web contre les injections SQL tant que nous n'utilisons pas de requête manuelle, si tel est le cas, il est nécessaire d'utiliser des requêtes préparées.

Le composant Symfony Form permet de se protéger contre les attaques CSRF.

Twig échappe les entrées formulaire permettant d'éviter les failles XSS, de plus les entrées utilisateurs sont vérifiées par des contraintes.

Enfin, les annotations fournies avec Symfony permettent de sécuriser les routes en fonction de rôle de l'utilisateur (user, admin ou employee).

Evolution

Les évolutions permettant d'améliorer le site web seront les suivantes :

- Possibilité de télécharger le billet électronique,
- Plusieurs possibilités de création de compte via oAuth2 comme Github, Microsoft, Facebook...
- Plusieurs possibilités de paiement comme PayPal.