

Documentation technique pour l'application web de visualisation des données pour GoldenLine

Introduction :

Ce document présente l'application web de visualisation des données pour GoldenLine. L'application permet aux membres de l'équipe marketing de visualiser les dépenses des clients en fonction de leur catégorie socioprofessionnelle et de la catégorie des produits achetés.

Architecture :

L'application est basée sur le modèle de publication web de Power BI. Le modèle de publication web est un ensemble de rapports et de tableaux de bord Power BI qui peuvent être publiés sur un serveur web.

La base de données est une base de données relationnelle PostgreSQL. Elle contient plusieurs tables :

Exemples :

- anonymisées_clients : cette table stocke les données anonymisées des clients, telles que le nombre d'enfants, la catégorie socioprofessionnelle, le prix du panier client sur le jour du passage en caisse, le suivi d'un identifiant collecte.
- collecte : cette table détaillera le prix du panier client en fonction des catégories.

Sécurité :

La sécurité des données et de l'application est une priorité absolue. Les mesures de sécurité suivantes sont mises en œuvre pour protéger les données et l'application :

- Chiffrement des données sensibles

Les données sensibles, telles que les numéros de carte de crédit, sont chiffrées avant d'être stockées dans la base de données. Cela les rend illisibles pour les personnes non autorisées.

- Autorisation d'accès

L'accès à la base de données est limité aux utilisateurs autorisés. Cela permet de garantir que seuls les utilisateurs autorisés peuvent accéder aux données.

- Sauvegardes régulières

Les données sont sauvegardées régulièrement pour éviter leur perte en cas de sinistre. Cela permet de restaurer les données en cas de perte ou de corruption.

- Utilisation de bonnes pratiques de codage

Le modèle de publication web est codé en suivant les bonnes pratiques de sécurité. Cela permet de réduire le risque d'attaques.

- Tests de sécurité

Le modèle de publication web est testé par un auditeur de sécurité pour identifier et corriger les vulnérabilités. Cela permet de garantir que l'application est sécurisée.

- Mises à jour régulières

Le modèle de publication web est mis à jour régulièrement pour corriger les vulnérabilités connues. Cela permet de garantir que l'application est toujours sécurisée.

Évolutions futures :

L'application est conçue pour être évolutive. Elle pourra être facilement adaptée aux besoins futurs de GoldenLine. Voici quelques exemples d'évolutions possibles :

- Ajout de nouvelles fonctionnalités

L'application pourrait être enrichie de nouvelles fonctionnalités, telles que la possibilité de visualiser les données sous forme de tableaux ou de graphiques, ou la possibilité de créer des rapports personnalisés.

- Amélioration des performances

L'application pourrait être optimisée pour améliorer ses performances, par exemple en utilisant un cache ou en optimisant les requêtes SQL.

- Extension de la base de données

La base de données pourrait être étendue pour ajouter de nouvelles informations, telles que les préférences des clients ou leurs habitudes d'achat.

Conclusion :

La documentation technique de l'application a été rédigée en français et est disponible en ligne. Elle sera mise à jour régulièrement pour refléter les modifications apportées à l'application.

Sécurité :

En plus des mesures de sécurité décrites ci-dessus, il est important de prendre les mesures suivantes pour protéger l'application :

- Utiliser un certificat SSL

Un certificat SSL permet de crypter les communications entre le navigateur web et le serveur web. Cela protège les données sensibles, telles que les numéros de carte de crédit, des interceptions.

Power BI possède sur son plateforme Microsoft en ligne (Learn/Power Platform /Power BI/ **créer un certificat SSL**)

- Mettre à jour le logiciel régulièrement

Les logiciels, tels que le serveur web, le navigateur web et le modèle de publication web, sont régulièrement mis à jour pour corriger les vulnérabilités. Il est important de mettre à jour le logiciel régulièrement pour maintenir la sécurité de l'application.

- Former les utilisateurs

Il est important de former les utilisateurs à la sécurité des données. Cela permettra aux utilisateurs de comprendre les risques et de prendre des mesures pour protéger les données.