Bases de données

Éric BERTHOMIER
berthomiereric70@gmail.com

4 janvier 2026

Version 1.0 - Version Stagiaire

Exemple pratique

Exemple de base de données

Une entreprise souhaite gérer ses clients et leurs commandes. Pour cela, elle souhaite stocker les informations suivantes :

- Clients : Chaque client possède un identifiant unique, un nom, un prénom, une adresse, un numéro de téléphone et une adresse e-mail.
- Commandes : Chaque commande est identifiée par un numéro unique, a une date de commande, un montant total et est liée à un client.
- Produits : Chaque produit a un identifiant unique, un nom, une description et un prix unitaire.
- Détail des commandes : Chaque commande peut contenir plusieurs produits. Pour chaque produit d'une commande, on stocke la quantité commandée et le prix unitaire au moment de la commande.

Analyse

A quoi sert l'identifiant unique ?

Donner un exemple dans le monde réel

Dans la pratique

Cette notion d'identifiant unique est présente sur tous les sites web marchands mais encore faut-il savoir le voir ...

Manipulations

1. Connectez-vous à un site marchand à l'aide du navigateur Firefox
2. Une fois connecté, utilisez la touche F12 pour activer l'inspecteur
3. Rechercher votre identifiant unique de connexion, compararer avec votre voisin

SSI - Vol de session - session hijacking

- Le vol de session consiste pour un pirate à obtenir ton session-id et l'utiliser à ta place.

SSI - Vol de session - session hijacking

- Le vol de session consiste pour un pirate à obtenir ton session-id et l'utiliser à ta place.
- Exemples de vol de session

SSI - Vol de session - session hijacking

- Le vol de session consiste pour un pirate à obtenir ton session-id et l'utiliser à ta place.
- Exemples de vol de session
  - Wi-Fi public non sécurisé : un pirate peut "sniffer" les codes qui circulent et récupérer le session-id.

SSI - Vol de session - session hijacking

- Le vol de session consiste pour un pirate à obtenir ton session-id et l'utiliser à ta place.
- Exemples de vol de session
  - Wi-Fi public non sécurisé : un pirate peut "sniffer" les codes qui circulent et récupérer le session-id.
  - XSS (Cross-Site Scripting) : un site malveillant injecte du code pour voler ton session-id depuis ton navigateur.

SSI - Vol de session - session hijacking

- Le vol de session consiste pour un pirate à obtenir ton session-id et l'utiliser à ta place.
- Exemples de vol de session
  - Wi-Fi public non sécurisé : un pirate peut "sniffer" les codes qui circulent et récupérer le session-id.
  - XSS (Cross-Site Scripting) : un site malveillant injecte du code pour voler ton session-id depuis ton navigateur.
  - Session non chiffrée : si le site n'utilise pas HTTPS, le session-id peut être intercepté pendant sa transmission.

SSI - Vol de session - session hijacking

- Le vol de session consiste pour un pirate à obtenir ton session-id et l'utiliser à ta place.
- Exemples de vol de session
  - Wi-Fi public non sécurisé : un pirate peut "sniffer" les codes qui circulent et récupérer le session-id.
  - XSS (Cross-Site Scripting) : un site malveillant injecte du code pour voler ton session-id depuis ton navigateur.
  - Session non chiffrée : si le site n'utilise pas HTTPS, le session-id peut être intercepté pendant sa transmission.
- Protection

SSI - Vol de session - session hijacking

- Le vol de session consiste pour un pirate à obtenir ton session-id et l'utiliser à ta place.
- Exemples de vol de session
  - Wi-Fi public non sécurisé : un pirate peut "sniffer" les codes qui circulent et récupérer le session-id.
  - XSS (Cross-Site Scripting) : un site malveillant injecte du code pour voler ton session-id depuis ton navigateur.
  - Session non chiffrée : si le site n'utilise pas HTTPS, le session-id peut être intercepté pendant sa transmission.
- Protection
  - Sites qui utilisent HTTPs (la connexion est chiffrée).

SSI - Vol de session - session hijacking

- Le vol de session consiste pour un pirate à obtenir ton session-id et l'utiliser à ta place.
- Exemples de vol de session
  - Wi-Fi public non sécurisé : un pirate peut "sniffer" les codes qui circulent et récupérer le session-id.
  - XSS (Cross-Site Scripting) : un site malveillant injecte du code pour voler ton session-id depuis ton navigateur.
  - Session non chiffrée : si le site n'utilise pas HTTPS, le session-id peut être intercepté pendant sa transmission.
- Protection
  - Sites qui utilisent HTTPs (la connexion est chiffrée).
  - Expiration rapide des session-id.

SSI - Vol de session - session hijacking

- Le vol de session consiste pour un pirate à obtenir ton session-id et l'utiliser à ta place.
- Exemples de vol de session
  - Wi-Fi public non sécurisé : un pirate peut "sniffer" les codes qui circulent et récupérer le session-id.
  - XSS (Cross-Site Scripting) : un site malveillant injecte du code pour voler ton session-id depuis ton navigateur.
  - Session non chiffrée : si le site n'utilise pas HTTPS, le session-id peut être intercepté pendant sa transmission.
- Protection
  - Sites qui utilisent HTTPs (la connexion est chiffrée).
  - Expiration rapide des session-id.
  - Ne jamais partager les liens ou informations de connexion.

SSI - Vol de session - session hijacking

- Le vol de session consiste pour un pirate à obtenir ton session-id et l'utiliser à ta place.
- Exemples de vol de session
  - Wi-Fi public non sécurisé : un pirate peut "sniffer" les codes qui circulent et récupérer le session-id.
  - XSS (Cross-Site Scripting) : un site malveillant injecte du code pour voler ton session-id depuis ton navigateur.
  - Session non chiffrée : si le site n'utilise pas HTTPS, le session-id peut être intercepté pendant sa transmission.
- Protection
  - Sites qui utilisent HTTPs (la connexion est chiffrée).
  - Expiration rapide des session-id.
  - Ne jamais partager les liens ou informations de connexion.
  - **Déconnexion** après usage.

Connexion à une base de données

À quoi sert la connexion à une base de données ?

C'est le pont entre une application (site, appli mobile) et l'endroit où sont stockées les données (utilisateurs, produits, commandes). La connexion permet d'envoyer des requêtes (lire, écrire, modifier) et de récupérer des réponses.

Connexion à une base de données

À quoi sert la connexion à une base de données ?

C'est le pont entre une application (site, appli mobile) et l'endroit où sont stockées les données (utilisateurs, produits, commandes). La connexion permet d'envoyer des requêtes (lire, écrire, modifier) et de récupérer des réponses.

Éléments nécessaires pour se connecter

- Adresse de la base : serveur (ex. db.example.com) et port (ex. 5432 pour PostgreSQL).
- Nom de la base : quelle base (ex. ma_boutique).
- Utilisateur & mot de passe : compte avec droits définis.

Dans la vie courante

Backend

1. On n'adresse pas directement une base de données (sauf le DBA (Database Administrator))

Dans la vie courante

Backend

1. On n'adresse pas directement une base de données (sauf le DBA (Database Administrator))
2. On passe par une interface nommée backend qui permet d'opérer des actions dans la base de données.

Dans la vie courante

Backend

1. On n'adresse pas directement une base de données (sauf le DBA (Database Administrator))
2. On passe par une interface nommée backend qui permet d'opérer des actions dans la base de données.

Dans la vie courante

Backend

1. On n'adresse pas directement une base de données (sauf le DBA (Database Administrator))
2. On passe par une interface nommée backend qui permet d'opérer des actions dans la base de données.

Métaphore avec un restaurant

- Frontend = salle / serveur : tu vois le menu, commandes ton plat, le serveur te rapporte la nourriture.

Dans la vie courante

Backend

1. On n'adresse pas directement une base de données (sauf le DBA (Database Administrator))
2. On passe par une interface nommée backend qui permet d'opérer des actions dans la base de données.

Métaphore avec un restaurant

- Frontend = salle / serveur : tu vois le menu, commandes ton plat, le serveur te rapporte la nourriture.
- Backend = cuisine / chef : reçoit ta commande, prépare le plat, suit les recettes, gère les stocks.

Dans la vie courante

Backend

1. On n'adresse pas directement une base de données (sauf le DBA (Database Administrator))
2. On passe par une interface nommée backend qui permet d'opérer des actions dans la base de données.

Métaphore avec un restaurant

- Frontend = salle / serveur : tu vois le menu, commandes ton plat, le serveur te rapporte la nourriture.
- Backend = cuisine / chef : reçoit ta commande, prépare le plat, suit les recettes, gère les stocks.
- Base de données = réserve / frigo : contient tous les ingrédients (données).

Métaphore avec un restaurant

- Imaginons que le serveur transmet le texte de la commande telle que au chef sans prendre en compte son contenu (exemple une assiette de soupe solide).

Métaphore avec un restaurant

- Imaginons que le serveur transmet le texte de la commande telle que au chef sans prendre en compte son contenu (exemple une assiette de soupe solide).
- Le client peut alors tenter de donner l'ordre au frigo de *"Passer en mode dégivrage"*

Métaphore avec un restaurant

- Imaginons que le serveur transmet le texte de la commande telle que au chef sans prendre en compte son contenu (exemple une assiette de soupe solide).
- Le client peut alors tenter de donner l'ordre au frigo de *"Passer en mode dégivrage"*

Métaphore avec un restaurant

- Imaginons que le serveur transmet le texte de la commande telle que au chef sans prendre en compte son contenu (exemple une assiette de soupe solide).
- Le client peut alors tenter de donner l'ordre au frigo de *"Passer en mode dégivrage"*

Dans la vie réelle

On va essayer de glisser des assertions de type : `' OR '1'='1`

Métaphore avec un restaurant

- Imaginons que le serveur transmet le texte de la commande telle que au chef sans prendre en compte son contenu (exemple une assiette de soupe solide).
- Le client peut alors tenter de donner l'ordre au frigo de *"Passer en mode dégivrage"*

Dans la vie réelle

On va essayer de glisser des assertions de type : `' OR '1'='1`

Que signifie dans un test `OR 1=1` ?

SSI - SQL Injection - Démonstration

`http://localhost/sqlinjection`