

# ECF STUDI

---

## Documentation technique du site



# Table des matières

<b>Documentation technique .....</b>	<b>1</b>
Table des matières .....	2
Spécifications techniques .....	3
Diagramme de Cas d'utilisation.....	4
Diagrammes de séquence .....	5
US1 – Se connecter.....	5
US6 – Réserver une table .....	6
US7 – Mentionner des allergies.....	7
Diagramme de classe.....	8
Modèle conceptuel des données .....	8
Modèle logique des données .....	9
Modèle physique des données.....	10
Pratiques de sécurité mises en place .....	11

# Spécifications techniques

---

Voici les différentes technologies que j'ai décidé d'utiliser pour ce projet :

## **Serveur Local :**

- Xampp version 3.3.0
  - MariaDB (version 10.4.28)
  - Apache (version 2.4.56)
  - PHP (version 8.2.4)

## **Serveur Production :**

- Déploiement sur O2Switch (sous Linux) :
  - MariaDB (version 10.6.12)
  - Apache
  - PHP (version 8.2.5)
  - cpanel (version 110.0.5) sous Linux

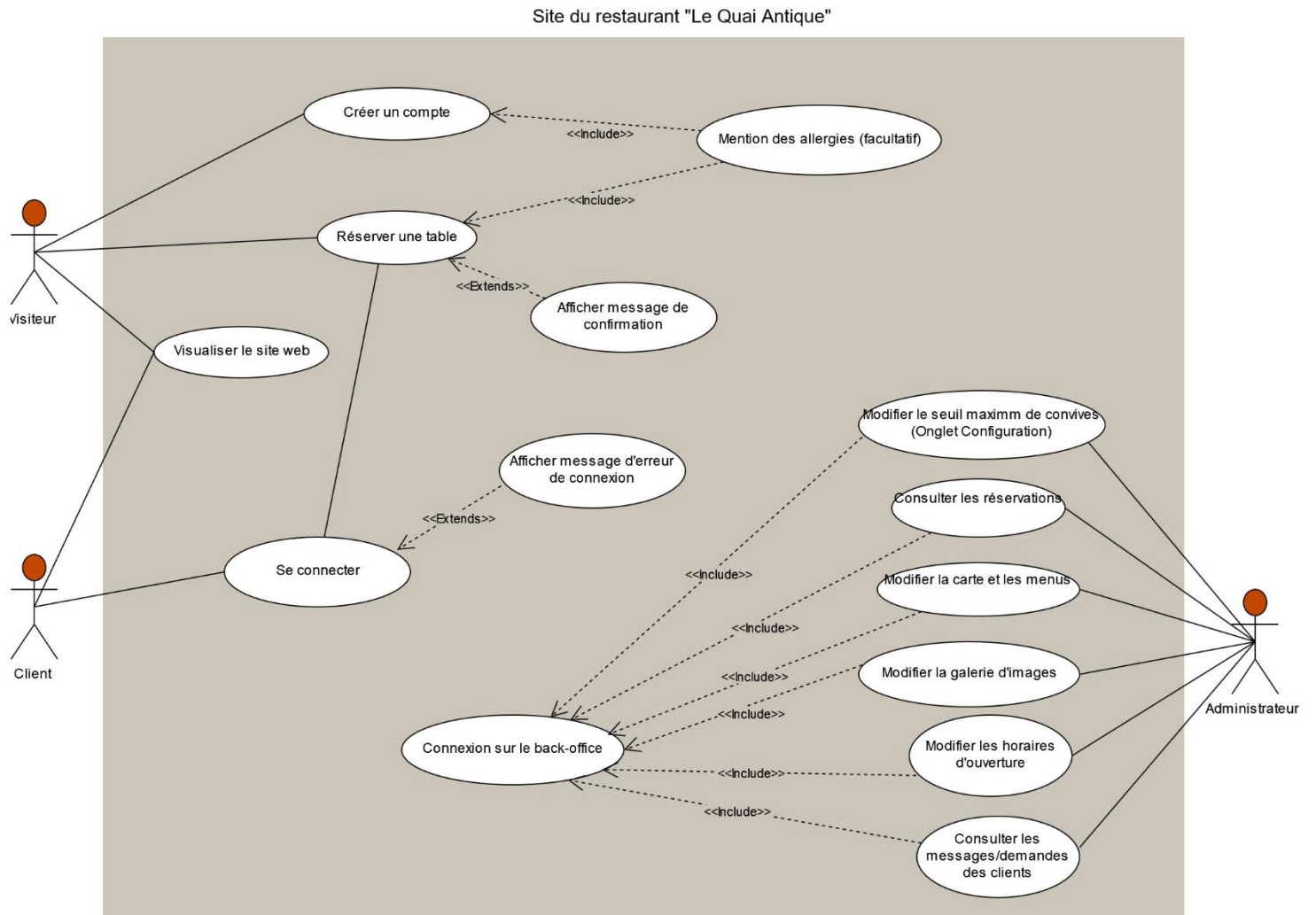
## **Pour le front-end :**

- HTML 5
- CSS 3
- React JS :
  - React Router
  - React Redux
  - Axios

## **Pour le back-end :**

- Symfony (version 6.2.8) :
  - Gestionnaire de dépendances Composer
  - Bundles :
    - Maker-bundle
    - ORM Doctrine
    - EasyAdminBundle
    - Security-bundle
    - Nelmio/Cors-bundle

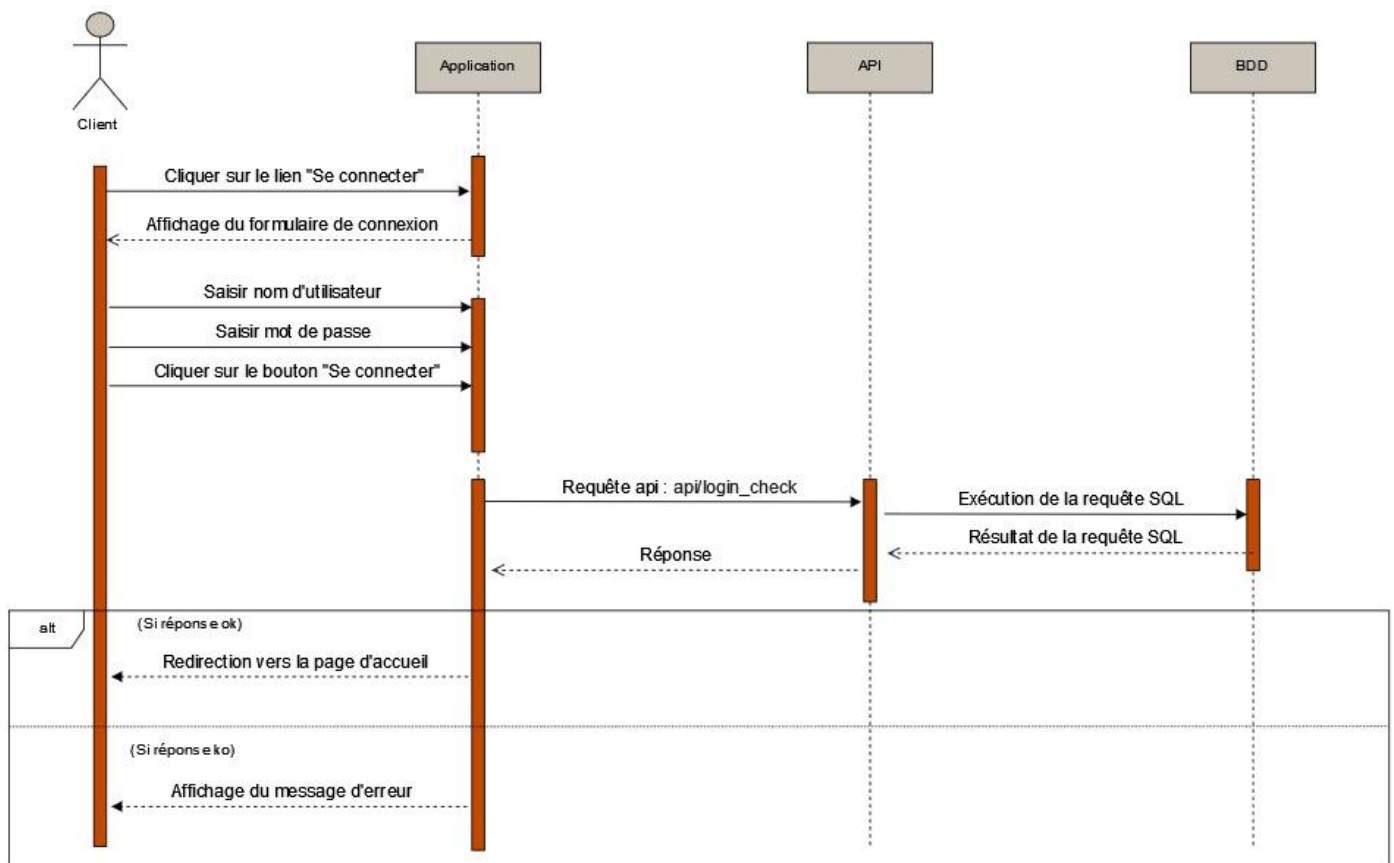
## Diagramme de cas d'utilisation



# Diagrammes de séquence

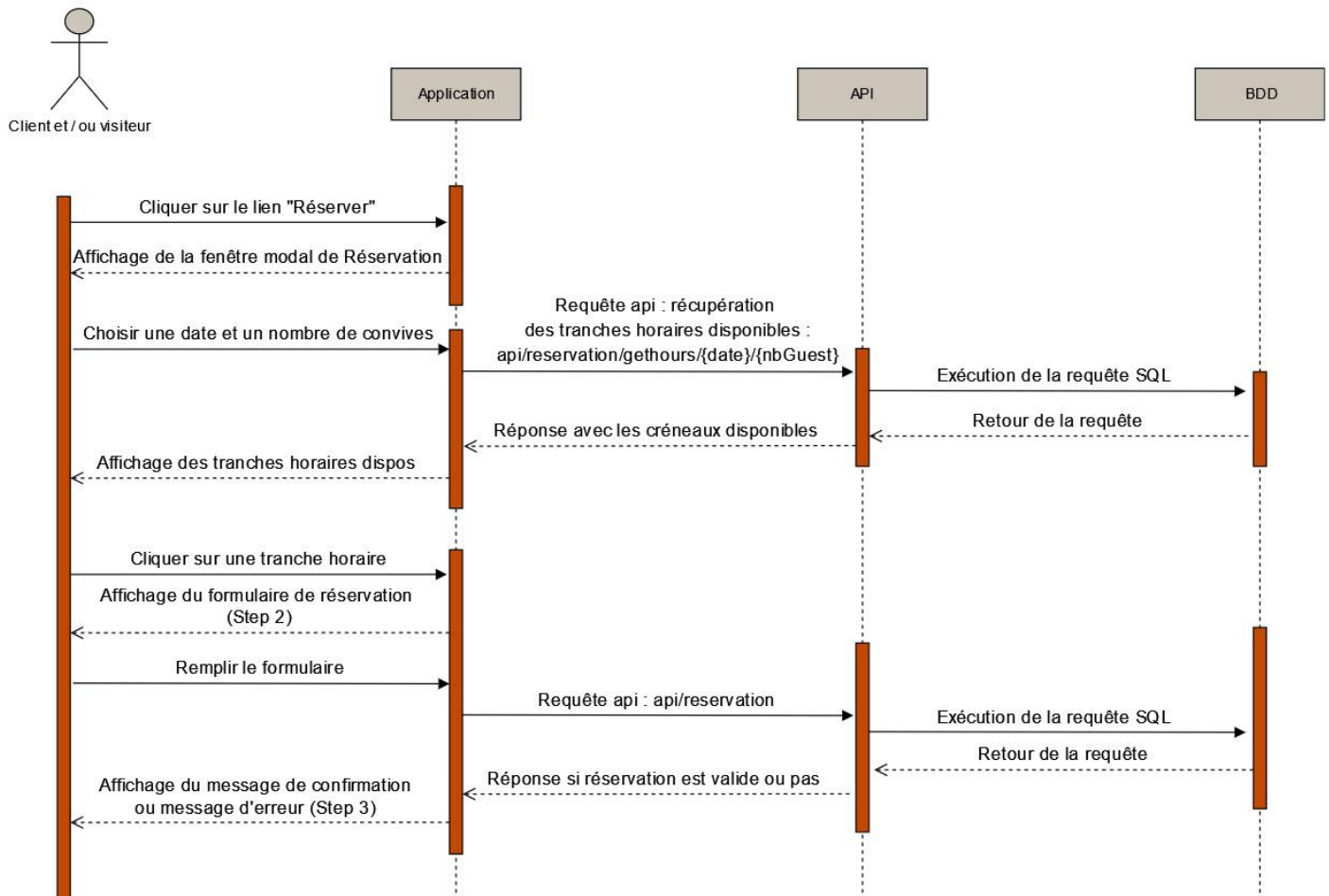
## US1 – Se connecter

### AUTHENTIFICATION



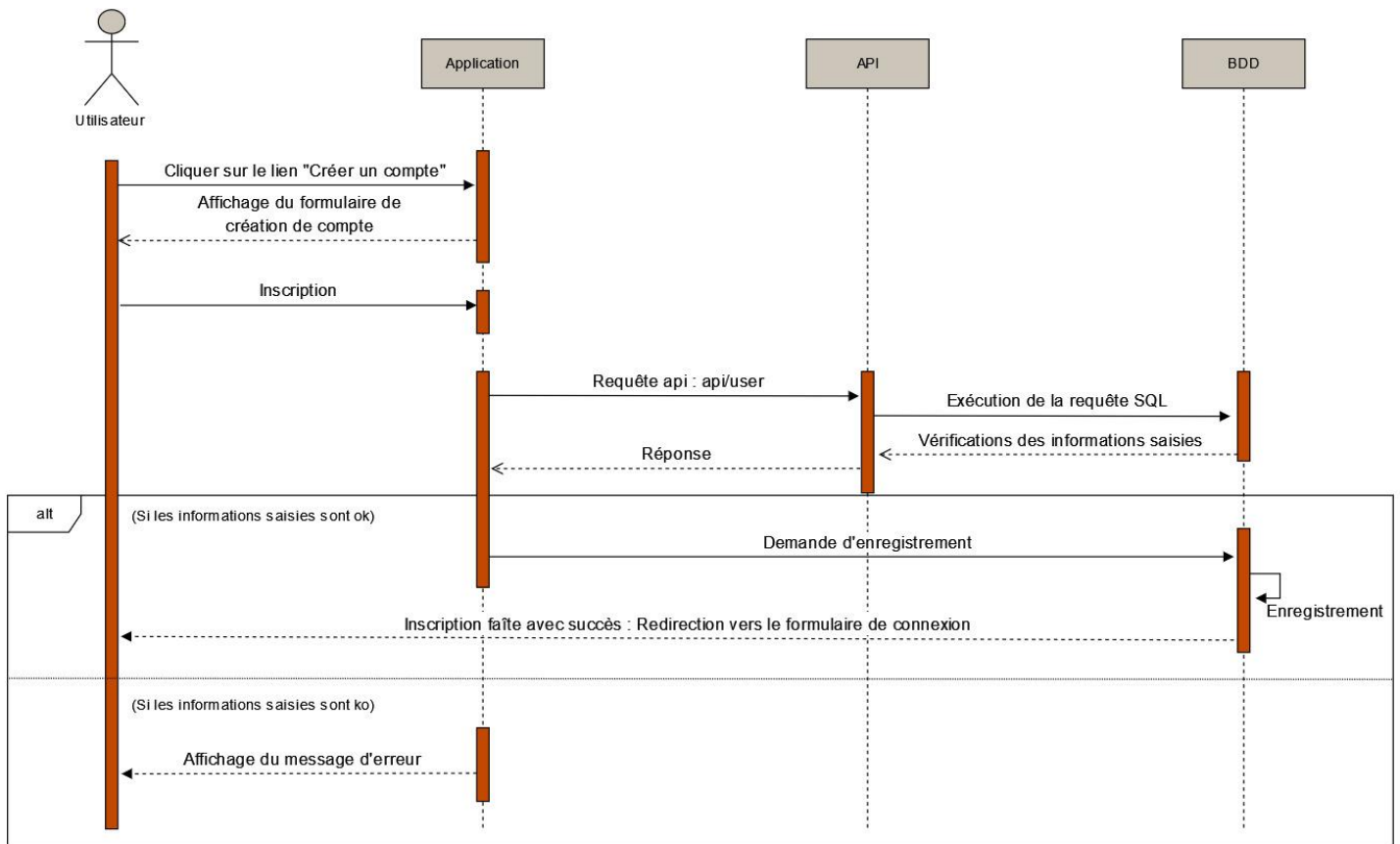
## US6 – Réserver une table

### RESERVER UNE TABLE



## US7 – Mentionner des allergies

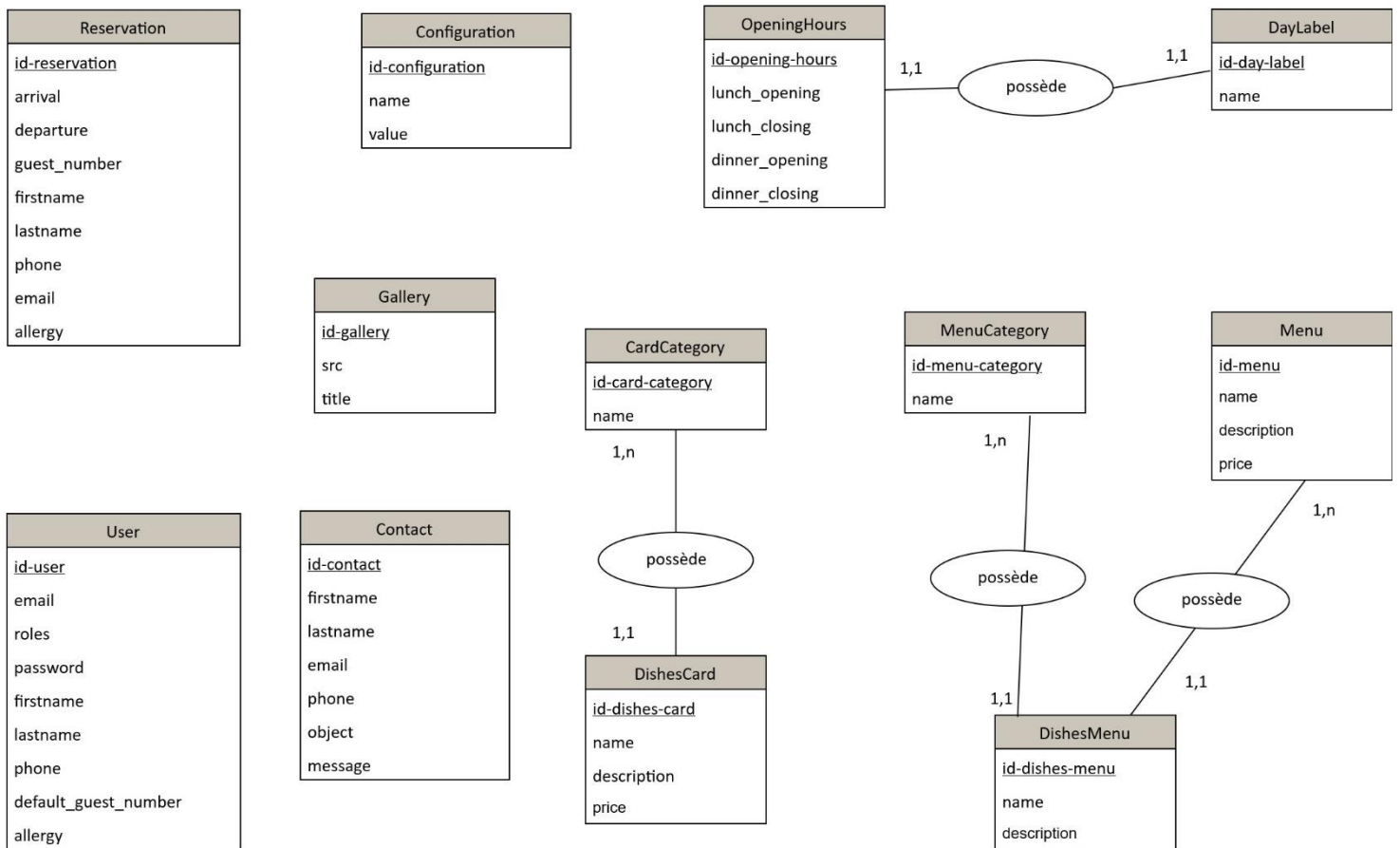
### INSCRIPTION



# Diagramme de classe

Modèle conceptuel des données :

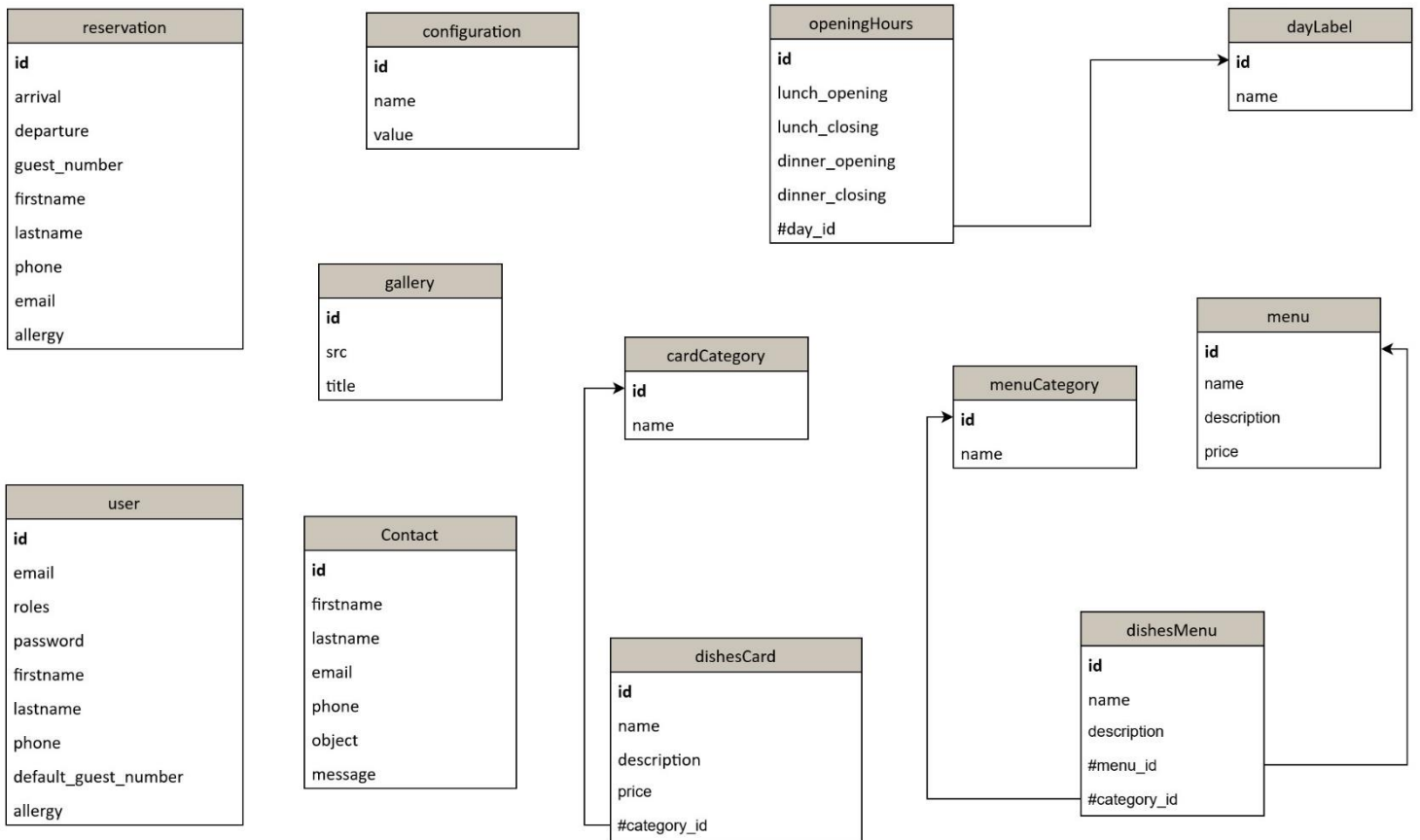
## MCD





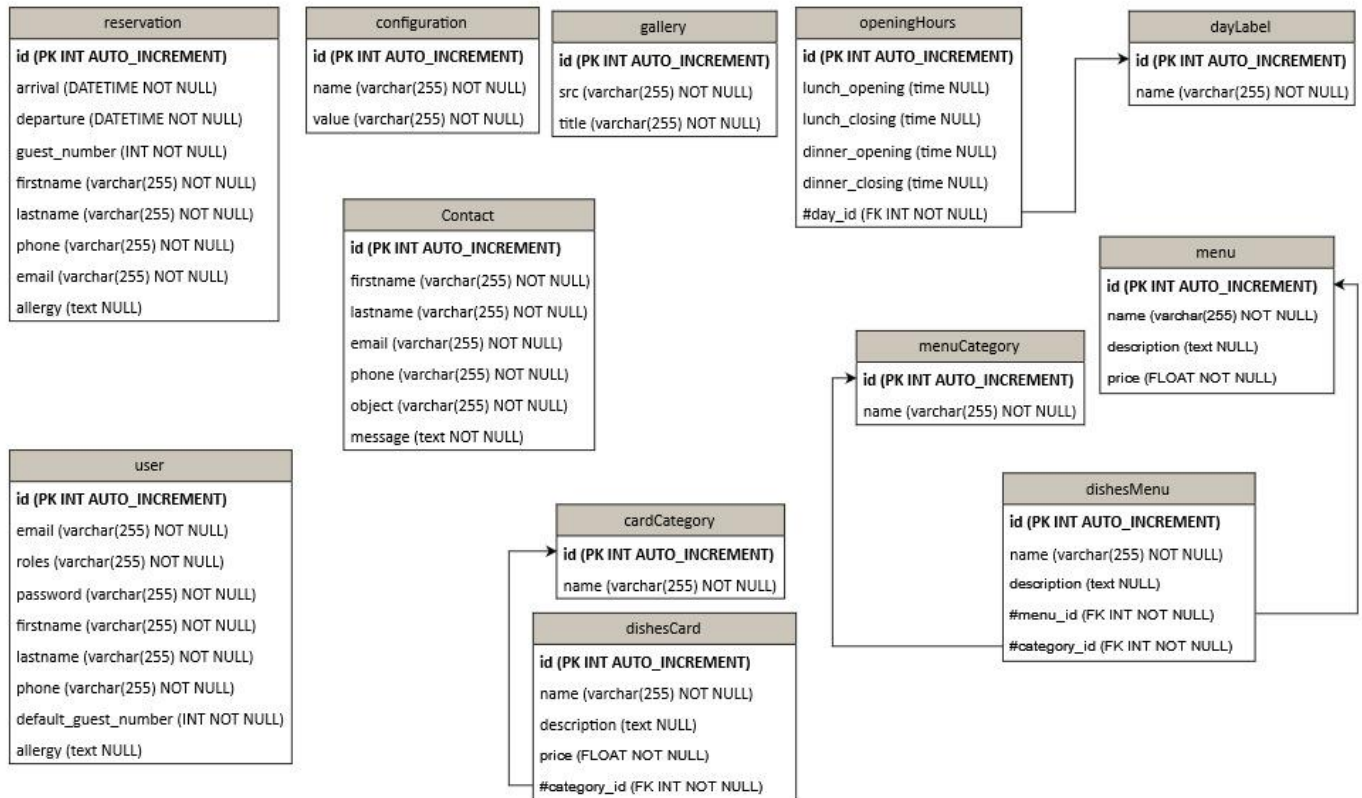
## Modèle logique des données :

### MLD



## Modèle physique des données :

### MPD



## Pratiques de sécurité mises en place

---

En faisant mon back-end avec le framework Symfony, j'ai pu installer le « Security bundle ». Ce dernier m'a permis de gérer les droits des utilisateurs en restreignant l'accès du panneau d'administration seulement à l'administrateur du site.

De plus, si nous regardons en base de données, nous pouvons constater que les mots de passe sont hashés.

L'utilisation du service https renforce également les relations entre le back et le front.

Certaines routes sont aussi protégées via Token JWT, grâce à « jwt-authentication-bundle ». Par exemple, pour récupérer les informations utilisateur, il faut que ce dernier se soit authentifié et que nous passions le token dans l'en-tête de la requête api.