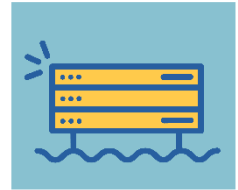


**HUGO CEREZO BAELO**

<https://hugo-cerezo.students-laplateforme.io/>

06 65 12 46 89



**La Plateforme\_**

**DOSSIER PROFESSIONNEL**

**REFONTE DU SITE « AVOTREGOUT.COM »**

**PROJET DE FIN D'ETUDE**

**DEVELOPPEUR WEB/MOBILE**

## Table des matières

1. Présentation de l'entreprise : .....	3
2. Présentation de l'équipe : .....	4
3. Liste des compétences du référentiel qui sont couvertes par le projet.....	5
3.1. partie front-end : .....	5
3.2. partie back-end : .....	5
4. Résumé du projet .....	5
5. Le Cahier des chargesdu projet .....	6
6. Les demandes .....	7
7. Les caractéristiques techniques à aborder.....	7
7.1. – LA MISE EN PLACE DU PROJET .....	7
7.2. – LA MÉTHODE DE TRAVAIL .....	8
7.3. – LE PROTOTYPAGE ET LA MAQUETTE DU SITE .....	9
7.4. – LES SPECIFICATIONS TECHNIQUES DU PROJET .....	9
7.5. – LA BASE DE DONNÉES .....	10
7.6. – LA GESTION DES UTILISATEURS.....	10
7.7. – PAGE ADMINISTRATEUR .....	11
8. Les Réalisations les plus significatives .....	12
8.1. – PARTIE UTILISATEUR .....	12
8.2. – LA PARTIE ADMINISTRATEUR .....	15
9. La Présentation du jeu d'essai élaboré par le candidat de la fonctionnalité la plus représentative (données en entrée, données attendues, données obtenues) ..	15
9.1. DEVIS EN LIGNE.....	15
10. La veille, effectuée sur les vulnérabilités de sécurité .....	21
10.1. utiliser htmlspecialchars.....	21
10.2. PDO :: prepare et PDOStatement::execute() .....	22
10.3. CERTIFICAT SSL/ TLS.....	22
11. La description d'une situation de travail ayant nécessité une recherche effectuée à partir de sites anglophones .....	22
12. Extrait du site anglophone, utilisé dans le cadre de la recherche décrite précédemment, accompagné de la traduction en français effectuée par le candidat sans traducteur automatique .....	23
13. Les annexes .....	23

## **Remerciements :**

2020 a été une année singulière pour tous.

Avec la crise du covid 19 et le confinement, nous avons dû nous adapter à un environnement peu propice aux suivis de notre formation et à la réalisation de notre projet professionnel.

Etudiants, formateurs et entreprises ont travaillé de concert afin que les conditions soient réunies pour que nous allions le plus loin possible dans notre projet.

Ces remerciements s'adressent donc à tous ceux qui ont su œuvré pour soutenir le lancement et l'avancement de ce projet malgré les contraintes :

- Mes formateurs d'abord qui nous ont livré les bases de lancement du projet
- L'entreprise qui nous a accueilli et dont le responsable s'est montré à la fois présent et à l'écoute de nos besoins à chaque étape du projet
- Enzo mon sparing partner avec lequel nous avons je crois, formé une équipe efficace et créative

# 1.Présentation de l'entreprise :

« **A VOTRE GOUT** » est une entreprise de « restauration nomade » qui a été créée en 2016 ; Elle propose des formules de restauration locavores et « clé en main » pour lesquelles la demande est de plus en plus croissante.

Le crédo de l'entreprise : une cuisine simple mais de saison, des fournisseurs locaux passionnés par leur métier et leurs produits, un engagement anti-gaspi et une démarche eco-responsable pour l'organisation des événements.

Pendant 3 ans, son créateur a régulièrement développé son activité auprès d'entreprises, d'organismes d'événements culturels et sportifs, d'institutionnels divers, de particuliers mais aussi d'associations. Ainsi, il a par exemple pu assurer la restauration de certaines organisations et entreprises qui recherchaient une alimentation plus durable chez leurs prestataires.

Aujourd'hui le concept est de développer davantage la prestation « sur mesure » pour répondre aux cahiers des charges des clients de plus en plus attentifs à ces questions de circuits courts et de cuisine de saison.

Concernant la composition des repas, « Avotre Gout » s'est associé à un réseau de fournisseurs locaux permettant de répondre aux besoins de variété, de qualité et de prise en compte des personnes à besoins spécifiques comme il est arrivé de le proposer par exemple aux coureurs de l'équipe DELKO lors de la course La Marseillaise en 2019, ou encore aux organisateurs du Concours Hippique de Pau en octobre 2019.

Les références clients :

**des festivals** : Cinéhorizontes, Espagne des 3 cultures...

des équipements culturels : Mucem, Théâtre Toursky, Cinéma Le Prado, Cinéma le Variété Marseille...

**des Associations** : La Cigale Puylobier, Cinépage Marseille, Regard 13 Arles, Les Amis d'Agape Droit Humain Aix en Provence, Loge Convivialité GDOF Marseille  
des événements sportifs : les Etoiles de Pau (concours hippique), Course Cycliste La Marseillaise...

**Des Centres de Formation** : Ecole Doctorale en Mathématiques et Informatiques St Jérôme, CROUS Aix en Provence, Ecole ALBERIC LAURENT Aix en Provence...

**Des événements privés** au domaine de Puyfond Aix en Provence

**Des événements d'entreprises** : KIA (circuit Sambuc), GOODHOTEL Marseille Aubagne, France Fermeture Rousset...

La demande de l'entreprise était de refondre son site web afin de :

- L'adapter et de le rendre visible pour les nombreuses cibles de clients
- Déployer ses fonctionnalités pour permettre de gagner du temps dans le suivi des clients, la réalisation de devis, l'organisation d'évènements et la gestion de sa comptabilité
- De numériser tous les documents et donc de pouvoir garder numériquement une trace de ses activités sur son serveur.

## 2. Présentation de l'équipe :

### HUGO CEREZO BAELO

Après un Baccalauréat STI2D SIN Systèmes d'Informations Numériques, je me suis orienté vers le DUT génie électrique puis en 1<sup>ere</sup> année de Math/info avant d'intégrer La Plateforme.IO pour me former spécifiquement au développement web full stack. J'y ai créé l'Association des élèves, dont j'ai pris la présidence pour participer aux choix proposés par les dirigeants de la formation.

Mes expériences :

Un stage chez ELYPSIA GROUPE SCALA MARSEILLE dans la gestion des bases de données clients et le codage

Un Service Civique à la LIGUE REGIONALE D'ENSEIGNEMENT en tant que chargé de cours et d'accompagnement de projets et animation d'ateliers numériques dans les collèges de Marseille

La création de site pour des associations ou des entreprises (exemple la [piizzaduvillageauriol.fr](http://piizzaduvillageauriol.fr))

### ENZO MANDINE

Il est également étudiant à la plateforme.IO. Nous nous sommes associé pour 2 raisons :

- Des travaux et des projets précédents nous ont permis de nous connaître et d'apprendre à travailler correctement ensemble
- Notre complémentarité : dans le design et le développement backend

### 3. Liste des compétences du référentiel qui sont couvertes par le projet

#### 3.1. Partie front-end :

- Développer la partie front-end d'une application web ou web mobile en intégrant les recommandations de sécurité
- Maquetter une application.
- Réaliser une interface utilisateur web statique et adaptable.
- Développer une interface utilisateur web dynamique.

#### 3.2. Partie back-end :

- Développer la partie back-end d'une application web ou web mobile en intégrant les recommandations de sécurité
- Créer une base de données.
- Développer les composants d'accès aux données.
- Elaborer et mettre en œuvre des composants dans une application de gestion de contenu ou e-commerce.

### 4. Résumé du projet

Ce dossier présente une partie de mon travail effectué lors de ma formation à l'école « LaPlateforme.IO » à savoir le projet « À Votre Goût ».

Lors de la réalisation de ce projet, j'ai travaillé avec Enzo MANDINE, un camarade de formation avec lequel j'avais déjà réalisé différents projets. Le responsable de l'entreprise a été très disponible. Cela nous a permis d'avoir un contact permanent avec celui-ci malgré la période de confinement lié au COVID-19.

Ce projet avait pour but de moderniser le site existant de ce chef traiteur « nomade » afin de lui permettre la prise de devis en ligne, l'analyse du comportement client sur le site ainsi que la modification des articles qui seront proposés sur le site. Il lui servira de vitrine pour ses prestations passées ainsi que de catalogue. Les services proposés proposent une identité hispanique, aussi le site devra s'inspirer de la culture espagnole dans son design tout en restant sobre et professionnel.

**L'objectif pour le client est d'augmenter son nombre de client, lui offrir de la visibilité, simplifier sa comptabilité et sa gestion de devis.**

Concernant la répartition des tâches, nous avons fait le choix de nous répartir le travail équitablement et pris la décision que nous ferons tous les deux du back et du front dans ce projet. Une fois la maquette réalisée ensemble, nous avons mis en place un Trello qui est un outil de gestion de projet en ligne. Sur ce site nous avons la possibilité de mettre en place des tableaux sur lesquels les participants au projet peuvent intervenir. Un tableau « A faire » rassemblait toutes les tâches à faire, un tableau nominatif pour Enzo et moi dans lesquels nous déplaçons les tâches que nous allions réaliser, un tableau « bug fix » dans lequel nous déplaçons les tâches sur lesquelles nous rencontrons des difficultés et un tableau « fini » dans lequel nous déplaçons les parties terminées du projet. Cette organisation nous a permis d'avoir une représentation graphique de l'avancement du projet ainsi que de pouvoir établir un suivi du projet qui s'est déroulé sur plusieurs semaines.

Ce projet m'a permis de mettre en pratique mes acquis théoriques et ouvert de nouvelles compétences. J'en garderais une très bonne expérience.

## 5. Le Cahier des charges du projet

Pour établir le cahier des charges du projet, nous avons procédé par étapes :  
Inspection en profondeur du site web du client déjà mis en place : nous en avons conclu les 5 grands chapitres :

- une page d'accueil reprenant les liens vers toutes les autres pages,
- une partie vitrine destinée aux particuliers
- une partie services destinées aux professionnels,
- une partie valorisant les prestations pour l'organisation des événements
- une galerie photos.

Nous avons ensuite discuté avec le client pour savoir quelle amélioration ou module il souhaitait que l'on développe : fallait-il tout reprendre de zéro ou bien updater la version actuelle avec de nouvelles fonctionnalités ?

La décision fut de refondre entièrement le site en développant un certain nombre de fonctionnalités. Etant tous deux développeurs full-stack nous avons décidé de nous partager la tâche de travail sous la forme de modules à développer. Nous avons ensuite créé le cahier des charges avec toutes les tâches à effectuer.

## 6. Les demandes

- refonte graphique du site
- ajout de BDD articles
- ajout d'une page de gestion administrateur
- ajout de pré-devis en ligne
- ajout de la fonctionnalité « mail automatique »
- formulaire de contact
- google analytics mis en place sur le site

## 7. Les caractéristiques techniques à aborder

- Mailto
- Réseau sociaux
- Map google
- Agenda
- Devis pour particuliers
- Devis pour les pros
- BDD Produits
- BDD Users
- BDD Formules
- BDD Code promo
- Responsive
- module de promotion
- article gérable depuis la BDD
- cohérence graphique en rapport avec l'Espagne/les tapas
- hébergement et certificat de sécurité SSL
- Module Admin (Gestion d'article, insertion modification suppression)
- compte client
- gestion événements
- secteur d'intervention
- google api
- affichage Facebook plat du jour restaurant

### 7.1. – LA MISE EN PLACE DU PROJET

En ce qui concerne la mise en place du projet nous avons le champ libre que ce soit en termes de technologies à utiliser. Nous avons fait le choix de découper notre projet en divers modules, chacun d'entre eux abordant un aspect bien précis de ce que nous devons réaliser. Nous avons donc mis en place un trello afin de pouvoir visualiser l'avancement respectif des différents modules que nous nous sommes partagé.



Pour faciliter notre travail, nous avons également créé un git pour héberger notre projet, le git se composait de 3 branches : une branche principale comprenant l'état actuel global du projet, et 2 branches de tests comprenant les modules développés par mon partenaire ou moi-même.

Les serveurs du site nous ont été fournis dès le début du projet. Ils nous ont permis d'uploader les versions en cours et de faire du bug test en condition réelle au fur et à mesure de l'avancement du projet.

En ce qui concerne les technologies utilisées, nous avons pris le parti de tout stocker depuis la base de données ce qui nous permettait :

- de faire appel à chacun de nos éléments dès que nous en avons besoin
- de modifier nos éléments quand nous le désirions via des requêtes sql

Concernant les utilisateurs, nous avons décidé d'utiliser de la programmation orientée « objet » pour simplifier l'utilisation des données.

Concernant les langages utilisés nous travaillons sur :

- html
- css
- php
- js /jquery/ajax
- sql

## 7.2. – LA MÉTHODE DE TRAVAIL

Nous avons opté pour 2 méthodes différentes durant la totalité du projet:

Au début du projet, nous étions en période de confinement ce qui nous permettait de travailler sur de plus longue durée d'affilée sans être mobilisés sur d'autres travaux. Nous avons mis à profit ce temps pour développer les principales fonctionnalités du site. Pendant ce confinement notre méthode de travail était singulière : nous ne pouvions pas nous voir. Nous avons donc choisi de travailler sur le logiciel (discord) qui nous permettait de communiquer vocalement mais aussi de nous partager deux écrans pour pouvoir voir ce que l'autre faisait mais également de s'entraider en cas de bug ou de problème technique.

A la sortie du confinement nous avons moins de temps à consacrer à ce projet. Nous avons donc mis en place un agenda spécifique : 1 à 2 jours par semaine étaient consacrés en quasi exclusivité au projet. Nous avons ainsi pu finaliser les derniers détails et développer de plus petites fonctionnalités. Nous travaillions sur le même bureau afin de pouvoir constamment avoir un œil sur ce que l'autre réalisait et pouvoir s'entraider en cas de problème technique.

Nous avons également mis en place un rendez-vous toutes les deux semaines avec le client afin de partager avec lui l'avancée du projet.

## 7.3. – LE PROTOTYPAGE ET LA MAQUETTE DU SITE

Pour ce qui est du prototypage et de la maquette du site, nous avons tout d'abord longuement discuté avec le client pour identifier ses besoins précisément et savoir ce qu'il attendait exactement. Nous avons alors effectué des prototypes en papier que nous lui avons soumis et une fois ces prototypes finis nous avons réalisé la maquette basique du site comprenant toutes les fonctionnalités attendues sur un logiciel qui s'appelle adobe XD(annexe 1)

## 7.4. – LES SPECIFICATIONS TECHNIQUES DU PROJET

Comme nous l'avons précisé plus haut, nous avons partagé les tâches en modules afin de pouvoir respectivement travailler sur du front ainsi que sur du back.

Pour ma part les éléments dont je devais m'occuper sont :

- Une Base de données
- Un système de devis dynamique
  - Les formules
  - Les produits à l'unité
  - Un champ pour insérer des demandes de plat particulier
  - nombre de convives
  - les prestations proposées par le client
    - système de checkbox pour la validation des prestations
  - date de livraison
- Système de compte comprenant
  - Module d'inscription
    - formulaire d'inscription au format bootstrap
    - connexion et requête pour insertion des données en sql
  - Module de connexion
    - vérification identité client
    - vérification rang utilisateurs
    - connexion à son profil personnalisé
  - Page Profil
    - affichage de toutes les commandes passées
    - affichage de toutes les commandes à venir
  - Page administrateur
  - Gestion de validation de devis
  - Extraction des données du devis en format csv
  - Upload de fichier au format pdf
  - mailto automatique des utilisateurs avec leurs devis au format pdf
  - champs permettant a l'administrateur d'upload des news sur sa page d'accueil
  - champs permettant a l'administrateur de créer des codes promotionnels
  - gestion des rôles

## 7.5. - LA BASE DE DONNÉES



Pour la base de données, nous avons tout à faire car la structure même de l'ancien site étant remodelé il fallait imaginer une BDD qui permettrait de stocker tous les articles, la mise en place des codes promos ainsi que tout le système de devis. Pour cela, il a fallu que l'on imagine au préalable comment nous allons afficher tous nos articles ainsi que la façon de gérer les produits et la gestion du devis. Cette phase de conception a été longue, le site devant être fait en « onepage ». Nous avons donc construit cette structure.

Pour créer notre modèle de base de données, nous nous sommes servis d'un logiciel appelé « Genmymodel » afin que l'export graphique de notre modèle de base de données soit nomenclaturée selon les normes des développeurs. Notre base de données se divise en 7 tables, chacune de ces tables stocke des données bien précises. Pour ce qui est du lien entre chaque élément de notre base de données nous l'avons imaginé au préalable lors de la création de celle-ci afin que les liens puissent ressortir lors de la visualisation du modèle.

## 7.6. - LA GESTION DES UTILISATEURS

Pour ce qui est de la gestion des utilisateurs nous avons repris tous les éléments que nous avons dans notre table users qui sont les suivants : id , login , password , mail , adress , phone ,rank. Nous avons décidé de créer une class user en PHP : hypertext processor (\*PHP) afin de gérer les données des utilisateurs via la programmation orientée objet (\*POO) dans notre fichier user.php.

Nous créons donc des fonctions globales qui ont pour but de manipuler plus aisément toutes les données des utilisateurs sur la totalité du site. A la suite de cela, nous avons mis en place les formulaires de connexion et d'inscription a notre site.

Pour ce qui est de l'inscription, il s'agit d'un formulaire au format Bootstrap(\*bibliothèque d'élément graphique). Nous avons ensuite vérifié que les données rentrées dans ses champs ne sont pas déjà dans notre base de données pour éviter les doublons en termes d'adresses mail, login...Nous avons également vérifié que le mot de passe choisi par l'utilisateur est bon en lui demandant de le taper deux fois et en vérifiant si les deux champs sont identiques. Une fois toutes les vérifications effectuées nous insérons les données de l'utilisateurs via une requête structured query language(\*SQL) dans notre table users de notre base de données

Pour la connexion des utilisateurs cela se passe également grâce a un formulaire au format bootstrap, puis une fois que les utilisateurs ont entré ces information, nous interrogeons notre serveur via des requêtes sql pour lui demander si effectivement le mot de passe ainsi que le nom d'utilisateur entré par l'utilisateur correspondent. Si c'est bien le cas, alors nous démarrons un class user avec les informations de l'utilisateur pour pouvoir s'en resservir jusqu'à sa déconnexion lors de la navigation sur le site. Dans le cas contraire, nous affichons un message d'erreur d'information saisie incorrecte. L'utilisateur devra retenter une connexion.

La page profil se compose d'un tableau affichant les commandes effectuées par l'utilisateur, l'affichage se compose de la manière suivante :  
Numéro de commande/date de la commande/date de livraison/adresse de livraison

Cette page n'est à l'heure actuelle, pas très étoffée mais pourrait par la suite recevoir diverses améliorations telles que la modification du profil, un système de messagerie, la visualisation des commentaires laissés sur le site avec les notations attribuées par exemple.

## 7.7. - PAGE ADMINISTRATEUR

La page administrateur doit être l'affichage principal de la gestion de devis. Celle-ci se présente de la manière suivante : un tableau récapitulatif des commandes : commande de : /effectue le :/pour le :/bouton pour télécharger le devis/bouton pour envoyé le devis au client via mail.

//suite pas encore codée

## 8. Les Réalisations les plus significatives

### 8.1. - PARTIE UTILISATEUR

-class user

Afin de réaliser ce projet, certaines fonctionnalités devront être utilisées à de multiples reprises. Dans le but de simplifier la tâche et de centraliser ces fonctionnalités, une classe « user » a été mise en place. Elle représente nos utilisateurs, et contient les fonctionnalités que nos différents types d'utilisateur ont à leur disposition.

```
<?php
class user
{
    public $id = '';
    public $login = '';
    public $email = '';
    public $phone = '';
    public $adress = '';
    public $rank = '';
    // Bool check if user is connected
    public $connectState = false;
```

Dans l'extrait ci-dessus je déclare une classe et définit les attributs qui lui seront associés. Ces attributs ont le type public afin que les fonctions soient utilisables en dehors de la portée de la classe. Ils seront renseignés à la connexion de l'utilisateur et sont par défaut renseignés vides.

```
public function connectBdd()
{
    $conn = new PDO("mysql:host=****;dbname=****;charset=utf8", "****", "****");
    return $conn;
}
```

Dans le but de ne pas avoir à réécrire la connexion à la base de données à chaque requête je me servirais de cette fonction. Elle déclare une variable « \$conn » qui contient une instance de la classe PHP « PDO ». Celle-ci représente une connexion entre notre code PHP et un serveur de base de données.

```
public function getUserData()
{
    if ($this->connectState == true) {
        return [$this->id, $this->login, $this->email, $this->phone, $this->adress, $this->rank];
    }
}
```

La fonction « getUserData() » nous permettra de récupérer les informations de l'utilisateur connecté sur l'instance de la classe. Elle ne retournera ces informations qu'à condition que l'utilisateur se soit connecté sur le site.

```
public function isConnected()  
{  
    return $this->connectState;  
}
```

La fonction « isConnected() » nous permettra de vérifier le statut de la connexion de l'utilisateur.

```
public function getRank()  
{  
    if ($this->connectState == true) {  
        return $this->rank;  
    }  
}  
public function getId()  
{  
    if ($this->connectState == true) {  
        return $this->id;  
    }  
}
```

Les deux fonctions ci-dessus, « getRank » & « getId » sont des versions tronquées de la fonction « getUserData » présenté plus haut.

```
public function getNews()  
{  
    $sql = "SELECT * FROM articles WHERE cat = 'news' AND start <= NOW() AND end >=  
NOW()";  
    $result = $this->connectBdd()->query($sql)->fetchAll(PDO::FETCH_ASSOC);  
    return $result;  
}
```

La fonction « getNews() » servira à alimenter le fil d'actualité de la page d'accueil.

```
public function disconnect()  
{  
    $this->id = '';  
    $this->login = '';  
    $this->email = '';  
    $this->phone = '';  
    $this->adress = '';  
    $this->rank = '';  
    $this->connectState = false;  
    header('location:index.php');  
}
```

La fonction « disconnect() » servira à déconnecter l'utilisateur du site.

```
public function getConnected()
{
    $sql = "SELECT * FROM users WHERE mail = '$_POST[mail]'";
    $result = $this->connectBdd()->query($sql)->fetch(PDO::FETCH_ASSOC);
    if ($result != NULL) {
        if (password_verify($_POST['mdp'], $result['password'])) {
            $this->id = $result['id'];
            $this->login = $result['login'];
            $this->email = $result['email'];
            $this->phone = $result['phone'];
            $this->address = $result['address'];
            $this->rank = $result['rank'];
            $this->connectState = true;
            header("location:index.php");
        } else {
            echo '<p class="text-center my-5">Mauvais Mot De Passe</p>';
        }
    } else {
        echo '<p class="text-center my-5">Adresse inconnu</p>';
    }
}
```

La fonction « getConnected() » servira à se connecter sur le site. Elle comprend une requête SQL servant à vérifier l'identité de l'utilisateur, qu'il est bien enregistré en base de données. Cette requête vérifie si le login de l'utilisateur existe et si c'est le cas elle récupère les informations liées à ce login afin d'effectuer une vérification de mot de passe avec l'instruction « password\_verify() ». Chaque vérification effectuée dans cette fonction possède son message d'erreur afin d'indiquer à l'utilisateur s'il s'est trompé de mot de passe ou de login.

```
public function getRegistered()
{
    $pass = htmlspecialchars(password_hash($_POST['mdp'], PASSWORD_DEFAULT));
    $sql = "SELECT * FROM users WHERE mail = '$_POST[email]'";
    $result = $this->connectBdd()->query($sql)->fetch();
    $login = htmlspecialchars($_POST['login']);
    $email = htmlspecialchars($_POST['email']);
    $address = htmlspecialchars($_POST['address']);
    $phone = htmlspecialchars($_POST['phone']);
    if ($result == 0) {
        $sql = "INSERT INTO `users`(`id`,`login`,`password`,`mail`,`address`,`phone`,`rank`) VALUES (NULL,'$login','$pass','$email','$address','$phone',0)";
        $this->connectBdd()->query($sql);
        header('location:connexion.php');
    }
}
```

```

    } else {
        echo '<p class="text-center my-5">Adresse déjà prise</p>';
    }
}

```

La fonction « `getRegistered()` » servira à un utilisateur pour s'inscrire sur le site. Elle récupère les informations que l'utilisateur a renseigné dans les champs du formulaire d'inscription et les insère dans la base de données. Afin de s'assurer que l'identité de l'utilisateur soit unique, j'effectue une requête « `SELECT` » dans la base de données pour vérifier que l'email de l'utilisateur n'existe pas. Si cette requête ne retourne rien, je peux insérer les informations dans la base de données en prenant soin de sécuriser l'insertion des données avec l'instruction « `htmlspecialchars()` ».

- partie profil
- affichage des devis :

## 8.2. – LA PARTIE ADMINISTRATEUR

Cette partie est dédiée à l'administrateur et lui permet de tout gérer sur le site, elle se compose de 3 parties :

- Gestion des devis
- Gestion des produits
- Gestion des news

A l'heure actuelle ces parties ne sont pas encore faites mais elles ont pour vocation d'être développées pendant le mois d'août 2020.

# 9. La Présentation du jeu d'essai élaboré par le candidat de la fonctionnalité la plus représentative (données en entrée, données attendues, données obtenues)

## 9.1. DEVIS EN LIGNE

Je vais ici vous présenter comment je réalise toute la partie de création de devis, comment se déroule la navigation de l'utilisateur sur cette page ainsi que les points bloquant ou qui ont été compliqués à résoudre. La partie devis est l'une des plus importantes dans ce projet car en effet, c'est elle qui permettra à notre donneur d'ordre de simplifier la réalisation des devis pour ses clients. L'objectif est de dynamiser le site et inviter la clientèle potentielle à se projeter dans le contrat.



Pour commencer nous avons réalisé la structure de la page

```
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/css/
bootstrap.min.css" integrity="sha384-
Vkoo8x4CGsO3+Hhvx8T/Q5PaXtkKtu6ug5TOeNV6gBiFeWPGFN9MuhOf23Q9Ifjh" cross
origin="anonymous">
<!-- <script src="https://code.jquery.com/jquery-3.4.1.slim.min.js" integrity="sha384-
J6qa4849bIE2+poT4WnyKhv5vZF5SrPo0iEjwBvKU7imGFAV0wwj1yYfoRSJoZ+n" crossorig
in="anonymous"></script> -->
<script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js" in
tegrity="sha384-
Q6E9RHvblyZFJoft+2mJbHaEWldlvI9IOYy5n3zV9zzTml3UksdQVRVvoxMfooAo" crossorig
in="anonymous"></script>
<script src="https://ajax.aspnetcdn.com/ajax/jquery/jquery-3.4.1.min.js"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/js/bootstrap.min.js"
integrity="sha384-
wfSDF2E50Y2D1uUdj0O3uMBJnjuUD4lH7YwaYd1iqfktj0Uod8GCExl3Og8ifwB6" crossori
gin="anonymous"></script>
<script src="https://code.jquery.com/jquery-3.5.1.js" integrity="sha256-
QWo7LDvxbWT2tbbQ97B53yJnYU3WhH/C8ycbRAKjPDc=" crossorigin="anonymous"><
/script>
<script async src="devis.js"></script>
<?php
$sql = 'SELECT * FROM products ';
$sql2 = 'SELECT * FROM formules';
$conn = new PDO("mysql:host=localhost;dbname=avotregout;charset=utf8", "root", ""
);
$requestProduct = $conn->query($sql)->fetchAll(PDO::FETCH_ASSOC);
$requestFormules = $conn->query($sql2)->fetchAll(PDO::FETCH_ASSOC);
?>
<div id="containerDevisActuel" class="row justify-content-around m-2 p-
2" style='display:flex;'>
  <div class='col-5 border border-dark'>
    <div class="dropdown">
      <button class="btn btn-secondary dropdown-
toggle" type="button" id="dropdownMenuButton" data-toggle="dropdown" aria-
haspopup="true" aria-expanded="false">
        choix cat
      </button>
      <div class="dropdown-menu" aria-labelledby="dropdownMenuButton">
        <?php
          foreach ($requestFormules as $formules) {
            echo "<a id='$formules[title]' value='".nl2br($formules['description'])."' clas
s='dropdown-item' href='#'$formules[title]</a>";
```

```

    }
    ?>
  </div>
</div>
<?php
foreach ($requestProduct as $products) {
    echo "<div class='d-flex justify-content-
between' id='$products[name]'><p>" . $products['name'] . "</p><p class='navLink' id
='description$products[name]'>description</p><input class='justify-content-
end' type='number' id='qtt$products[name]' value='1'><p class='justify-content-
end'>$products[qtt]</p><input class='justify-content-
end addProductBtn' type='button' id='$products[name]' value='add'><p id='textdes
cription$products[name]' style='display:none;'>$products[description]</p></div>";
    }
    ?>
  </div>
  <div class="col-5 border border-dark" id="devisActuel">
  </div>
</div>
<div id="containerDevisFinal" class="row justify-content-md-center m-auto p-
2" style='display:none;'>
  <div id="devisFinal" class="justify-content-md-center col-8 h-100 border border-
dark">
  </div>
</div>

```

Sur la structure de cette page nous pouvons voir quelle se compose de 3 div dont une qui est en display none qui nous servira par la suite.

Dans la première div c'est là que nous allons afficher nos divers éléments qui sont :

- les formules
- les produits à l'unité
- les produits sur mesure

Pour afficher tous ces produits nous les récupérons donc de la base de données via des requêtes sql. Nous effectuons 2 requêtes distinctes : une pour les formules et une pour les produits à l'unité et sur mesure. Enfin, nous effectuons deux foreach afin d'afficher nos éléments mais pas seulement, chaque élément se compose du nom du produit d'un bouton description, un input type number pour choisir la quantité et une description en display none.

Suite à cela nous commençons notre script devis.js qui va traiter toutes les interactions de l'utilisateur

- `$('.dropdown-item').click(function() )`

```

$('.dropdown-item').click(function() {

```

```

    test = $(this).attr('id')
    test2 = $(this).attr('value')
/*    console.log(test) */
    test3 = test2.split(',')
    console.log(test3)
    test3.forEach(element => {
        devis.push("'" + element + "1")
    });
    ajaxFunction()
})

```

Cette fonction a pour but de gérer les évènements du menu déroulant qui nous sert à choisir les formules dans le devis. Elle permet de récupérer tous les éléments de la formule choisie par l'utilisateur de les parse dans un array en y ajoutant la quantité de l'élément de la formule. Cela permettra par la suite d'afficher la formule modifiable à volonté pour l'utilisateur, puis nous envoyons dans notre array devis tous ces éléments, ensuite je fais appel à ma fonction ajaxFunction() que je détaillerai plus tard pour traiter ces données.

- \$(''.desc).click(function() )

```

$('').desc).click(function () {
    var desc = $(this).attr("id")
    if (document.getElementById('text' + desc).style.display == 'none') {
        document.getElementById('text' + desc).style.display = "block";
    } else {
        document.getElementById('text' + desc).style.display = "none";
    }
})

```

Cette fonction me permet de gérer l'interaction entre de l'utilisateurs pour afficher la description des produits, elle affiche ou désaffiche la div contenant la description du produit ciblé, nous avons mis cela en place pour rendre la lecture de la page plus agréable pour l'utilisateurs et plus fluide

- \$(''.addproductBtn').click(function() )

```

$('').addProductBtn').click(function () {
    var product = $(this).attr("id")
    qtt = document.getElementById('qtt' + product).value
    document.getElementById('qtt' + product).value = "1"
    console.log(qtt)
    devis.push(product + ':' + qtt)
    console.log(devis)
}

```

```

    ajaxFunction()
    console.log(devis);

})

```

Cette fonction a pour but de gérer les produits à l'unité dans la sélection des produits. Cette fonction n'a pas le même fonctionnement que celle pour les formules car nous ajoutons le fait que le client puisse choisir lui-même la quantité de produit qu'il désire. Du coup nous récupérons la valeur du champ servant à définir la quantité de produit désiré puis nous la stockons dans une variable et nous envoyons dans notre array devis tous ces éléments. Une fois cela effectué on fait appel à notre ajaxfunction ()

- function ajaxFunction ()

```

function ajaxFunction() {
    $.ajax({
        url: "cookiesDevis.php",
        method: "post",
        data: "cookie=" + devis,
        success: function (res) {

            console.log(res)
            $('#devisActuel').empty();
            $('#devisActuel').append(res);
            $('.close').click(function () {
                console.log(devis)
                var delta = ($(this).parent().attr("id"))
                console.log(delta)
                devis.splice(delta,1)
                $(this).parent().remove()
            })
            $('#validationDevis').click(function () {
                document.getElementById('containerDevisFinal').style.display = "block";
                document.getElementById('containerDevisActuel').style.display = "none";
                $.ajax({
                    url: "validationDevis.php",
                    method: "post",
                    data: "cookie=" + devis,
                    success: function (res) {
                        $('#devisFinal').empty();
                        $('#devisFinal').append(res);
                        $('#devisFinal').append("<input class='test' type='button' id='bddDevis' value='valider mon devis'>")
                        $('#bddDevis').click(function () {

```



chaque choix effectué par l'utilisateur afin que s'il désire supprimer des choix de sa sélection, il puisse le faire sans soucis. J'effectue cette opération grâce à une boucle dans ma page php. Une fois tout cela effectué, je réaffiche tous les produits sélectionnés sur la deuxième div qui se situe sur la droite de l'écran avec comme dit précédemment, un bouton supprimer pour l'utilisateur. Suite à cela il y a trois possibilités :

- soit l'utilisateur rajoute un article supplémentaire : dans ce cas, on réeffectue la même opération que précédemment.
- Soit l'utilisateur souhaite supprimer un de ses choix dans la liste des devis dans ce cas j'effectue la fonction splice sur ma variable devis puis je supprime grâce à : `$(this).parent().remove()`
- Soit l'utilisateur valide son devis et dans ce cas on fait appel

## 10. La veille, effectuée sur les vulnérabilités de sécurité

La veille de sécurité a été un point très complexe à aborder car nous avons dû effectuer toutes les recherches relatives à ce thème. Nous en avons conclu qu'il y avait trois grands axes à aborder pour sécuriser un site web :

### 10.1. utiliser htmlspecialchars

Certains caractères ont des significations spéciales en HTML, et doivent être remplacés par des entités HTML pour être affichés. **htmlspecialchars()** remplace tous ces caractères par leur équivalent dans la chaîne *string*. Cette conversion est très pratique pour la programmation web. Lorsque tous les caractères doivent être remplacés, il convient d'utiliser plutôt htmlentities(). **htmlspecialchars()** est pratique pour éviter que des données fournies par les utilisateurs contiennent des balises HTML, comme pour un forum ou un chat.

Cette fonction nous permet d'éviter une partie des injections de code et donc de rendre notre site plus sûr pour nos utilisateurs

Les 5 caractères qui seront remplacés sont :

- "&" (et commercial) devient "&amp;"
- "\"" (guillemets doubles) devient "&quot;" lorsque **ENT\_NOQUOTES** n'est pas utilisée.
- "'" (guillemet simple) devient "&#039;" uniquement lorsque **ENT\_QUOTES** est utilisée.
- "<" (inférieur à) devient "&lt;"
- ">" (supérieur à) devient "&gt;"

## 10.2. PDO :: prépare et PDOStatement::execute()

PDO::prepare() et PDOStatement::execute() aident à prévenir les attaques par injection SQL en éliminant le besoin de protéger les paramètres manuellement. Cela nous permet de sécuriser nos requêtes SQL.

## 10.3. CERTIFICAT SSL/ TLS

SSL (Secure Sockets Layer) est un protocole non commercial et avant tout l'une des méthodes plus utilisées de transfert sécurisé de données entre le serveur et le navigateur (utilisateur). TLS 1.2 (Transport Layer Security) est actuellement la version la plus utilisée du protocole. Il s'agit d'un protocole standardisé avec son propre RFC. Les différences entre TLS 1.2 et TLS 1.3 sont petites, alors on parle le plus souvent de la connexion SSL/TLS.

Il est primordial pour nous d'avoir un certificat SSL afin de pouvoir passer en https et d'utiliser pleinement les fonctionnalités de l'API google

Le principe du fonctionnement des certificats SSL est basé sur un chiffrement asymétrique où chaque personne communiquant détient deux clés : publique et privée. La clé publique peut être rendue publique, et si elle est utilisée pour le chiffrement, le destinataire pourra la déchiffrer uniquement à l'aide de sa clé privée. Inversement, si la clé privée est utilisée pour chiffrer les données, seule la clé publique permettra de les déchiffrer. Mais cela n'a pas beaucoup de sens, puisque la clé publique est par définition connue de tous. Alors, si la clé publique contient une information disant qu'elle appartient à une entité concrète (société) et que cette information est confirmée par une autorité de confiance, nous sommes assurés d'avoir communiqué avec la bonne entité et pas avec un fraudeur.

A l'heure où l'on rédige ce dossier, la veille sur la sécurité mérite d'être approfondie. Elle sera mise en place dans les semaines à venir

# 11. La description d'une situation de travail ayant nécessité une recherche effectuée à partir de sites anglophones

Lors de ce projet il y a eu plein de moment où nous avons été confrontés à des situations nouvelles qui ont constitué des points de bloquants. Pour avancer, nous avons dû consulter une majorité de sites anglophones.

Ce sont des sources précieuses pour trouver des explications précises sur des fonctions, ou encore de la documentation utile. je vais prendre l'exemple de la recherche effectuée pour transformer un array php en fichier csv :

Ici on peut donc voir comment fonctionnent les fonctions nécessaires pour utiliser le csv qui nous sert à sortir un fichier traitable sur Excel pour le client afin de réaliser facilement des devis par la suite

## 12. Extrait du site anglophone, utilisé dans le cadre de la recherche décrite précédemment, accompagné de la traduction en français effectuée par le candidat sans traducteur automatique

(CF annexe)

## 13. Les annexes



logo		<div></div> <div></div> <div></div>
------	--	-------------------------------------

Nous contactez

tel : 06.50.84.30.01	email : fcbaelo@gmail.com
----------------------	---------------------------

logo		<div></div> <div></div> <div></div>
------	--	-------------------------------------

liste de toutes les prestation en termes de

nom du produit	qtt	add	description
si description est appuyé ouvre une div sous le produit avec ça description			
nom du produit	qtt	add	description
nom du produit	qtt	add	description
nom du produit	qtt	add	description
nom du produit	qtt	add	description
nom du produit	qtt	add	description
nom du produit	qtt	add	description
nom du produit	qtt	add	description

récapitulatif du devis

logo		<div><div></div><div></div><div></div></div>
------	--	----------------------------------------------

vous n'etes pas connectez

veuillez vous connectez

pas encore de compte ? crée en un !

logo		<div><div></div><div></div><div></div></div>
------	--	----------------------------------------------

adresse mail

mot de passe

connexion

pas encore de compte ? crée en un !

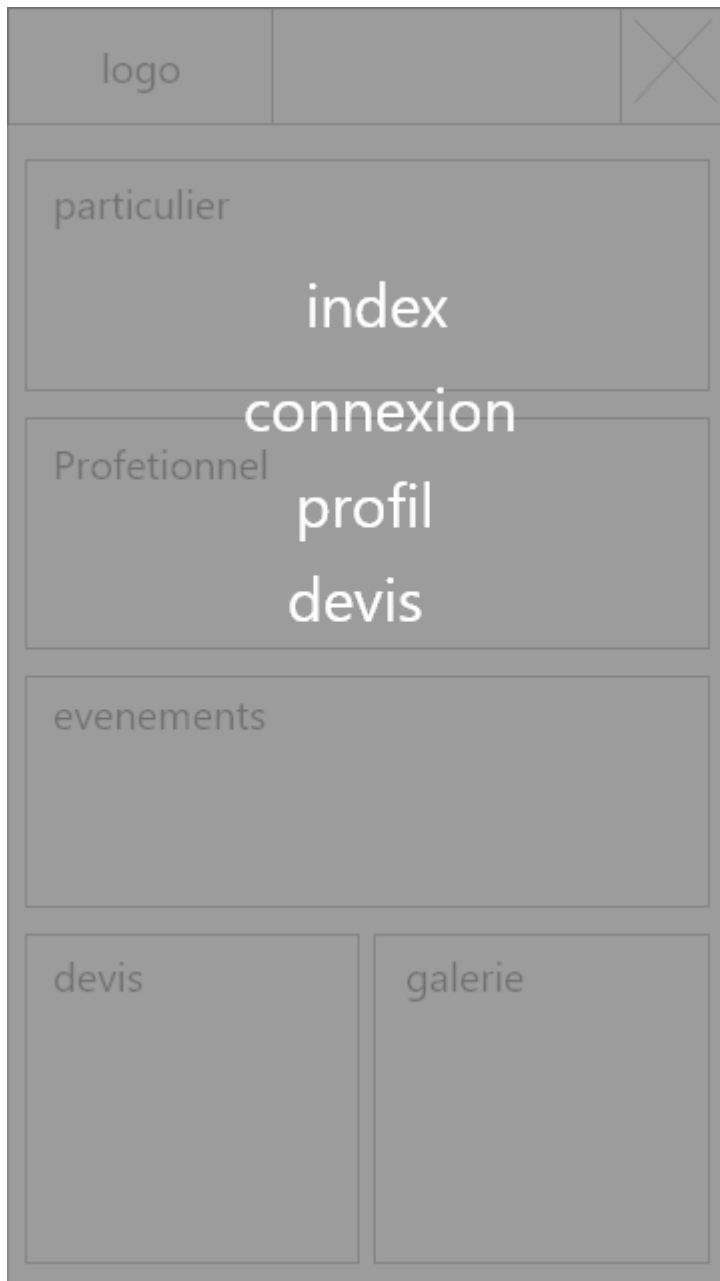
logo		<hr/> <hr/> <hr/>
------	--	-------------------

adresse mail

mot de passe

connexion

pas encore de compte ?  
inscrivez vous



logo		<div> <div></div> <div></div> <div></div> </div>
------	--	--------------------------------------------------

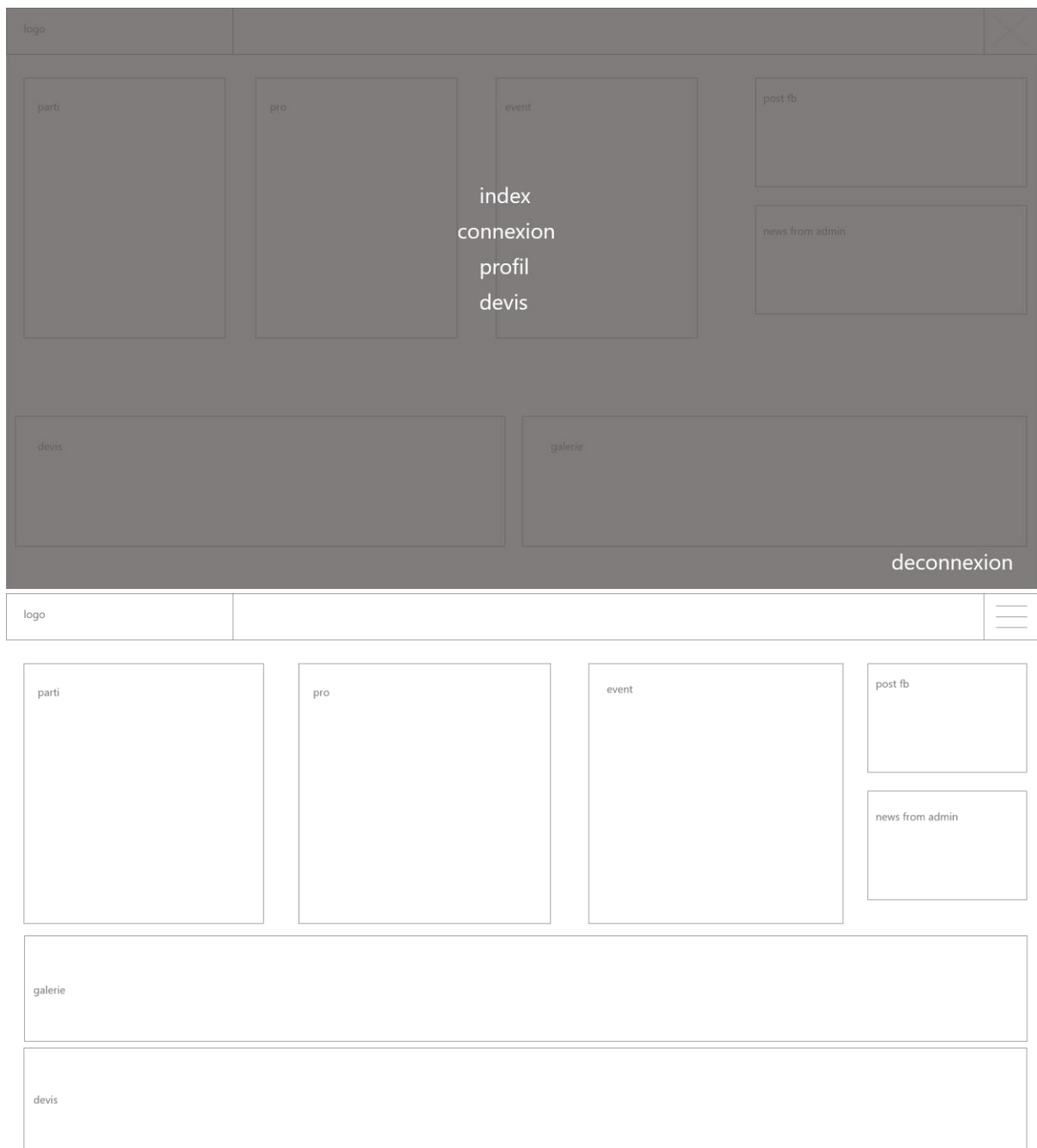
particulier

Profetionnel

evenements

devis

galerie





buffets

tapas

brunch

sous landing

sous landing

sous landing



buffets

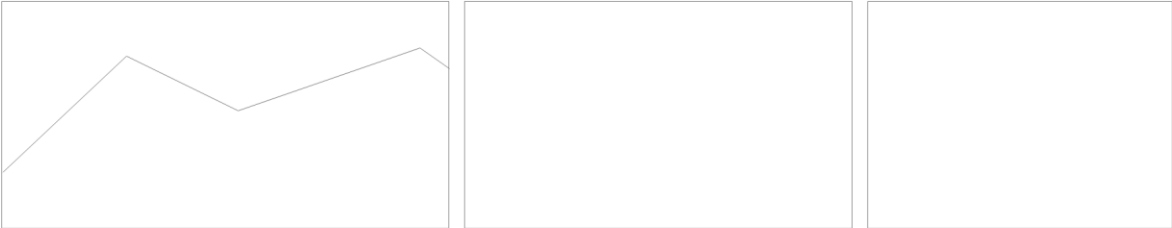
tapas

brunch

welcome NOM DE LA PERSONNE

mes dernières commandes

commandes en cours de validation



devis n°00X from NOM DE LA PERSONNE	POUR LE XX/XX/XXXX	A VALIDER AVANT LE XX/XX/XXXX	MODIFIER LE DEVIS	VALIDER LE DEVIS
devis n°00X from NOM DE LA PERSONNE	POUR LE XX/XX/XXXX	A VALIDER AVANT LE XX/XX/XXXX	MODIFIER LE DEVIS	VALIDER LE DEVIS
devis n°00X from NOM DE LA PERSONNE	POUR LE XX/XX/XXXX	A VALIDER AVANT LE XX/XX/XXXX	MODIFIER LE DEVIS	VALIDER LE DEVIS
devis n°00X from NOM DE LA PERSONNE	POUR LE XX/XX/XXXX	A VALIDER AVANT LE XX/XX/XXXX	MODIFIER LE DEVIS	VALIDER LE DEVIS
devis n°00X from NOM DE LA PERSONNE	POUR LE XX/XX/XXXX	A VALIDER AVANT LE XX/XX/XXXX	MODIFIER LE DEVIS	VALIDER LE DEVIS
devis n°00X from NOM DE LA PERSONNE	POUR LE XX/XX/XXXX	A VALIDER AVANT LE XX/XX/XXXX	MODIFIER LE DEVIS	VALIDER LE DEVIS



logo		<div></div> <div></div> <div></div>
------	--	-------------------------------------

# TITLE

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

demander un devis    contactez-moi