

Spécifications techniques

Projet	[nom du projet + nom du client]
---------------	---------------------------------

Version	Auteur	Date	Approbation
1.0	Soufiane	23/09/23	John

Le but de ce document est de définir et justifier les spécifications techniques de [nom du projet].

I. Choix technologiques

- État des lieux des besoins fonctionnels et de leurs solutions techniques :

Besoin	Contraintes	Solution	Description de la solution	Justification (2 arguments)
<i>Landing non connectée : Fournir une page d'accueil informative pour les utilisateurs non connectés. Page login : Offrir une interface de connexion sécurisée pour les utilisateurs enregistrés.</i>	<i>Respecter les normes de conception UX/UI pour une expérience utilisateur conviviale. Utiliser des modèles de conception éprouvés pour la landing page. Implémenter une interface de connexion avec des mesures de sécurité robustes.</i>	<i>Landing non connectée : HTML, CSS, JavaScript, Bootstrap (optionnel). Page login : React.js, JWT pour l'authentification.</i>	La landing non connectée présentera les avantages de l'outil "Menu Maker" et des appels à l'action pour inciter les utilisateurs à s'inscrire ou à se connecter. La page de connexion comprendra des champs de saisie sécurisés pour les informations d'identification et des mécanismes de validation.	<i>La landing page convaincante augmente le taux de conversion des visiteurs en utilisateurs inscrits. La sécurité est cruciale pour protéger les données sensibles des utilisateurs.</i>

Exportation PDF : Permettre la génération de menus au format PDF. Commander l'impression d'un menu : Faciliter l'impression des menus physiques. Exportation Deliveroo : Intégrer la redirection vers Deliveroo. Partage sur Instagram : Fournir une option de partage sur Instagram	Assurer une exportation fluide et un partage facile. Utiliser une bibliothèque de traitement d'images pour le PDF (JS-PDF) et Instagram. Intégrer un lien hypertexte vers Deliveroo. Ajouter des boutons de partage social pour Instagram.	Exportation PDF : Génération de PDF à partir des données de menu. Commander l'impression d'un menu : Lien hypertexte vers un service d'impression. Partage sur Instagram : Boutons de partage. JS PDF	La génération de PDF et le partage sur Instagram sont des fonctionnalités attractives pour les restaurateurs. L'intégration de liens hypertexte simplifie la redirection vers d'autres plateformes	
Déconnexion : Permettre aux utilisateurs de se déconnecter en toute sécurité. Infos utilisateur : Afficher les informations du compte de l'utilisateur. Dashboard : Offrir un tableau de bord pour une gestion facile du compte.	Assurer la sécurité des données de compte et une gestion conviviale. Implémenter une fonction de déconnexion sécurisée. Créer une page d'informations utilisateur et un tableau de bord	Nous allons mettre en place un système d'authentification basé sur JWT (JSON Web Tokens) pour sécuriser les connexions. Pour la gestion du compte utilisateur, nous utiliserons une interface intuitive dans le tableau	Authentification sécurisée : Nous utiliserons JWT pour générer des tokens sécurisés lors de l'authentification. Ces tokens seront envoyés avec chaque requête et vérifiés côté serveur pour s'assurer de l'identité de l'utilisateur. Gestion du compte utilisateur : Le tableau de bord de l'interface utilisateur permettra aux utilisateurs de voir et de	L'utilisation de JWT offre une méthode d'authentification robuste, largement adoptée et sécurisée qui convient particulièrement bien à une application comme "Menu Maker". Cela permettra de garantir la sécurité des comptes utilisateurs.

			modifier leurs informations de compte, y compris les détails personnels, les préférences, et les informations de paiement si nécessaire.	
Fournir des informations légales essentielles pour le respect des réglementations.	La solution doit inclure les mentions légales, les conditions d'utilisation et la politique de confidentialité.	Nous allons créer une section dédiée dans l'application qui affichera les mentions légales, les conditions d'utilisation et la politique de confidentialité.	<p>Mentions légales : Cette section fournira les informations légales sur l'entreprise ou l'entité propriétaire de l'application, y compris les coordonnées, le numéro d'enregistrement, etc.</p> <p>Conditions d'utilisation : Les conditions d'utilisation énonceront les règles et les obligations que les utilisateurs doivent respecter lors de l'utilisation de l'application.</p> <p>Politique de confidentialité : Cette politique expliquera comment les données des</p>	inclure des informations légales est essentiel pour la conformité réglementaire et la protection juridique de l'entreprise. Offrir une transparence totale sur les pratiques de collecte et de traitement des données renforce la confiance des utilisateurs.

			utilisateurs sont collectées, utilisées, et protégées.	
Afficher de manière claire et transparente les coûts associés à l'utilisation de l'outil "Menu Maker" afin d'informer les utilisateurs sur les différents plans d'abonnement et leurs fonctionnalités.	Les informations tarifaires doivent être facilement accessibles depuis l'interface utilisateur et présentées de manière compréhensible.	Nous allons créer une page dédiée aux tarifs et aux plans d'abonnement. Cette page fournira des détails sur les plans d'abonnement disponibles, les fonctionnalités incluses et les tarifs mensuels.	Page des tarifs : Nous créerons une page spécifique dans l'interface utilisateur où les utilisateurs pourront consulter les différents plans d'abonnement. Cette page présentera de manière claire les options disponibles et les avantages associés à chaque plan.	La transparence des tarifs favorise la confiance des utilisateurs envers l'application. En affichant clairement les coûts associés, nous éliminons toute confusion et permettons aux utilisateurs de prendre des décisions éclairées. Une page de tarifs bien conçue aide les restaurateurs à choisir le plan qui correspond le mieux à leurs besoins et à leur budget, ce qui contribue à une expérience utilisateur positive.
Choisir un nom de domaine approprié et sélectionner un hébergement fiable qui répondent aux besoins de l'application "Menu Maker".	Le nom de domaine doit être pertinent et lié au service offert. L'hébergement doit être fiable et offrir des performances constantes.	Nom de domaine : Nous choisirons un nom de domaine pertinent lié au service, par exemple "MenuMakerByQwent a.com". Hébergement : Opter	Choix du nom de domaine : Nous sélectionnerons un nom de domaine qui reflète clairement le service proposé, renforçant ainsi la reconnaissance de la marque.	Un nom de domaine approprié est essentiel pour la reconnaissance de la marque et facilite la mémorisation pour les utilisateurs. Un hébergement fiable garantit une disponibilité constante de l'application, ce qui est crucial pour offrir une expérience

		pour un service d'hébergement de confiance, tel qu'AWS (Amazon Web Services) ou Google Cloud. Ces plateformes offrent une infrastructure fiable et hautement évolutive.	Sélection de l'hébergement : Nous opterons pour un service d'hébergement reconnu pour sa fiabilité et ses performances constantes, assurant ainsi une disponibilité optimale de l'application.	utilisateur optimal
Assurer une accessibilité maximale du site web, garantissant ainsi que celui-ci soit utilisable depuis différents navigateurs et appareils.	Le site doit être compatible avec les navigateurs majeurs tels que Google Chrome, Mozilla Firefox, Microsoft Edge et Safari. Il doit également être convivial sur les PC.	Compatibilité navigateur : Nous veillerons à ce que le site soit entièrement fonctionnel et optimisé pour les navigateurs tels que Google Chrome, Mozilla Firefox, Microsoft Edge et Safari. Types d'appareils : Le site sera conçu pour offrir une expérience	Nous effectuerons des tests de compatibilité pour chaque navigateur majeur afin de garantir que toutes les fonctionnalités du site soient opérationnelles. L'interface utilisateur sera conçue pour offrir une expérience optimale sur les	Une compatibilité multi-navigateurs élargit la portée de l'application à un public plus large, garantissant que les utilisateurs puissent accéder au site depuis leur navigateur préféré. L'optimisation pour les PC est essentielle car de nombreux utilisateurs accéderont au site à partir de ces appareils. Une expérience utilisateur fluide et conviviale est donc primordiale

		utilisateur optimale sur les PC.	ordinateurs personnels.	
--	--	----------------------------------	-------------------------	--

II. Liens avec le back-end

- *Quel langage pour le serveur ? NodeJS*
- *Node.js est un choix populaire pour le développement de serveurs web en raison de sa rapidité, de sa scalabilité, et de sa facilité de développement. Il est bien adapté aux applications en temps réel et aux applications web interactives.*
- A-t-on besoin d'une API ? Si oui laquelle ? Oui
- La création d'une API (Interface de Programmation Applicative) est essentielle pour permettre la communication entre le front-end de votre application (côté client) et le backend (côté serveur). L'API facilite l'échange de données et de fonctionnalités, ce qui est nécessaire pour un outil tel que "Menu Maker."



- Base de données choisie : SQL :
- *Les bases de données SQL présentent plusieurs avantages, notamment la structuration des données, la possibilité de réaliser des requêtes complexes (y compris les jointures), la cohérence des données grâce à la transaction ACID (Atomicité, Cohérence, Isolation, Durabilité), et la capacité à gérer de grands ensembles de données. Ce choix est particulièrement approprié si vous avez besoin d'une gestion structurée des menus et des catégories.*

En résumé, avec Node.js côté serveur, une API pour la communication frontend/back-end, et une base de données SQL, vous avez fait des choix solides pour développer l'outil "Menu Maker" de manière performante, évolutive, et structurée. Cela devrait vous permettre de mettre en place une application robuste et efficace pour vos utilisateurs.

1. Préconisations concernant le domaine et l'hébergement

- Nom du domaine : Menu Maker by Qwenta
- Nom de l'hébergement.

Voici une liste intéressante :



1. **AWS (Amazon Web Services)** : AWS est l'un des plus grands fournisseurs de services cloud au monde, offrant une gamme complète de services d'hébergement web. Il est hautement évolutif et offre une grande flexibilité, mais il peut nécessiter une certaine expertise technique.
2. **Google Cloud** : Similaire à AWS, Google Cloud offre des services cloud puissants et une infrastructure fiable. Il est connu pour son écosystème de services et d'outils.
3. **Heroku** : Heroku est une plateforme d'hébergement cloud qui simplifie le déploiement et la gestion d'applications. Il est apprécié pour sa facilité d'utilisation.
4. **DigitalOcean** : DigitalOcean propose des serveurs virtuels privés (VPS) avec des tarifs compétitifs. C'est un choix populaire pour les développeurs et les petites entreprises.
5. **HostGator** : HostGator offre une variété de plans d'hébergement partagé, VPS et dédiés. Il est reconnu pour ses tarifs compétitifs.
6. **A2 Hosting** : A2 Hosting est apprécié pour ses performances élevées et sa rapidité. Il propose également des options d'hébergement optimisé pour les applications spécifiques.

- Adresses électroniques :

Lorsque vous choisissez des adresses électroniques pour votre domaine "Menu Maker by Qwenta", il est important de les rendre professionnelles et faciles à comprendre. Voici quelques suggestions pour la création



d'adresses électroniques professionnelles liées à votre domaine :

1. **contact@menumakerbyqwenta.com** : Cette adresse électronique est générique et peut être utilisée pour la communication générale avec vos utilisateurs, partenaires et clients.
2. **support@menumakerbyqwenta.com** : Cette adresse électronique peut être utilisée pour les demandes de support technique, les questions et les problèmes que les utilisateurs rencontrent avec votre application.
3. **info@menumakerbyqwenta.com** : Vous pouvez utiliser cette adresse électronique pour diffuser des informations générales, des actualités ou des mises à jour sur votre application "Menu Maker."
4. **admin@menumakerbyqwenta.com** : Cette adresse électronique peut être réservée à l'administration du site web et à la gestion des comptes utilisateurs.
5. **sales@menumakerbyqwenta.com** : Si vous envisagez de proposer des offres premium ou des services associés, cette adresse électronique peut être utilisée pour les demandes de vente et les questions commerciales.
6. **yourname@menumakerbyqwenta.com** : Si vous êtes le fondateur ou le responsable du projet, vous pouvez utiliser votre propre nom dans l'adresse électronique pour une communication personnelle. Par exemple, john@menumakerbyqwenta.com.
7. **billing@menumakerbyqwenta.com** : Cette adresse électronique peut être utilisée pour les questions de facturation, de paiement et de gestion des comptes.
8. **team@menumakerbyqwenta.com** : Si vous travaillez en équipe, vous pouvez avoir une adresse électronique dédiée à l'équipe pour les communications internes et externes.
9. **partners@menumakerbyqwenta.com** : Si vous avez des partenaires ou collaborateurs, cette adresse

électronique peut être utilisée pour les communications liées aux partenariats.

2. Accessibilité

- Compatibilité navigateur : Google Chrome, Mozilla Firefox, Microsoft Edge et Safari, pour garantir une compatibilité optimale.
- Types d'appareils : pc

3. Services tiers

- Noms et justification de ceux qui devront être implémentés pour le bon fonctionnement et le suivi du site (par exemple les plugins).

- Suivi et analyse des performances :

- Outil d'analyse : Exemple - Google Analytics.
- Justification : Pour surveiller le trafic du site, analyser le comportement des utilisateurs et évaluer les

performances.

- **Réseaux sociaux et partage :**

- Plugins de partage social : Exemple - AddThis, ShareThis.
- Justification : Pour faciliter le partage de contenu sur les réseaux sociaux et augmenter la visibilité.

-

4. Recommandations en termes de sécurité

- La sécurité est un aspect critique de tout site web, et il est essentiel de prendre des mesures pour protéger l'accès aux comptes des utilisateurs, les plugins et l'ensemble de votre application. Voici quelques recommandations en termes de sécurité :

1. Gestion des accès aux comptes :

- **Authentification sécurisée :** Utilisez des méthodes d'authentification sécurisées, telles que le hachage des mots de passe et l'utilisation de protocoles d'authentification robustes comme OAuth ou OpenID Connect.



- **Protection contre les attaques par force brute** : Mettez en place des mécanismes de protection contre les attaques par force brute en limitant le nombre de tentatives de connexion et en verrouillant les comptes après un certain nombre d'échecs.
- **Validation des entrées** : Assurez-vous de valider toutes les entrées utilisateur pour éviter les attaques d'injection, comme les injections SQL ou les scripts intersites (XSS).
- **Mots de passe forts** : Encouragez les utilisateurs à créer des mots de passe forts et assurez-vous que les mots de passe stockés sont correctement hachés.

2. Gestion des plugins :

- **Mises à jour régulières** : Veillez à ce que tous les plugins, bibliothèques et composants tiers utilisés dans votre application soient maintenus à jour régulièrement pour corriger les vulnérabilités connues.
- **Analyse de sécurité** : Effectuez des analyses de sécurité régulières pour identifier les vulnérabilités potentielles dans les plugins et les composants tiers. Vous pouvez utiliser des outils d'analyse de sécurité automatisés pour cela.
- **Limitation des privilèges** : Accordez uniquement les privilèges nécessaires aux plugins et aux composants

tiers. Évitez d'accorder un accès excessif aux ressources sensibles de votre site.

3. Gestion des sessions :

- **Expiration de session** : Configurez des sessions utilisateur avec une expiration automatique après une période d'inactivité pour éviter les sessions ouvertes non sécurisées.

4. Protection contre les attaques :

- **Protection DDoS** : Mettez en place une protection contre les attaques par déni de service distribué (DDoS) pour garantir la disponibilité de votre site web.
- **Protection contre les injections** : Utilisez des requêtes paramétrées pour éviter les injections SQL et assurez-vous que toutes les entrées utilisateur sont correctement filtrées et validées.
- **Firewall d'application Web (WAF)** : Considérez l'utilisation d'un WAF pour détecter et bloquer les attaques courantes, telles que les injections SQL et les attaques XSS.

5. Surveillance et journaux :

- **Surveillance en temps réel** : Mettez en place des mécanismes de surveillance en temps réel pour détecter les activités suspectes ou les tentatives d'intrusion.

- **Journalisation** : Tenez des journaux d'activité pour enregistrer les actions des utilisateurs et les événements système, ce qui peut être utile pour l'audit et la détection d'anomalies.
- **Réponse aux incidents** : Élaborez un plan de réponse aux incidents pour savoir comment réagir en cas de violation de sécurité.

6. Formation et sensibilisation :

- **Formation du personnel** : Assurez-vous que votre équipe de développement est formée aux meilleures pratiques de sécurité et de développement sécurisé.
- **Sensibilisation des utilisateurs** : Éduquez vos utilisateurs sur les bonnes pratiques en matière de sécurité, telles que la création de mots de passe forts et la vigilance en matière de phishing.

En suivant ces recommandations en matière de sécurité, vous pouvez renforcer la sécurité de votre application web, protéger l'accès aux comptes des utilisateurs et garantir la sécurité de vos plugins et de votre site dans son ensemble. La sécurité doit être un aspect essentiel de la conception, du développement et de l'exploitation de votre site web.

5. Maintenance du site et futures mises à jour

- Grandes lignes du contrat de maintenance.

Un contrat de maintenance de site internet est un accord écrit entre un prestataire de services de maintenance et le propriétaire d'un site web. Il établit les termes et conditions pour la gestion continue, la mise à jour, la sécurité et le soutien technique du site web. Voici les grandes lignes d'un contrat de maintenance de site internet :

1. Parties concernées :

- Identification du prestataire de services de maintenance (nom de l'entreprise, adresse, numéro de téléphone, etc.).
- Identification du client (nom de l'entreprise ou du propriétaire du site, adresse, numéro de téléphone, etc.).

2. Objet du contrat :

- Décrire en détail les services de maintenance offerts, y compris les mises à jour, les correctifs de sécurité, la surveillance du site, etc.
- Préciser les éléments spécifiques du site web couverts par le contrat.

3. Durée du contrat :



- Indiquer la durée initiale du contrat (généralement en mois ou en années).
- Préciser les modalités de renouvellement, de résiliation ou de résiliation anticipée.

4. Fréquence des mises à jour :

- Définir à quelle fréquence les mises à jour du site web seront effectuées (quotidiennes, hebdomadaires, mensuelles, etc.).
- Préciser les délais de livraison des mises à jour.

5. Tarifs et modalités de paiement :

- Indiquer les tarifs mensuels ou annuels pour les services de maintenance.
- Préciser les modalités de paiement, les pénalités de retard et les frais supplémentaires éventuels.

6. Responsabilités du prestataire :

- Détail des tâches spécifiques incluses dans la maintenance.
- Engagement à assurer la sécurité du site web.

- Mesures de sauvegarde des données.

7. Responsabilités du client :

- Fournir un accès adéquat aux ressources nécessaires au prestataire.
- Signaler les problèmes ou les demandes de maintenance en temps opportun.

8. Support technique :

Spécifier les heures de disponibilité du support technique.

Détail des canaux de communication pour le support (courriel, téléphone, chat en ligne, etc.).

9. Confidentialité :

Clauses de confidentialité pour protéger les données sensibles du client.

10. Propriété intellectuelle :

Définir la propriété des travaux réalisés dans le cadre du contrat (par exemple, les mises à jour du site web).

11. Garanties et responsabilités :

Préciser les garanties fournies par le prestataire.



Limitier la responsabilité en cas de dommages ou de pertes.

12. Résiliation :

Conditions de résiliation du contrat par l'une ou l'autre des parties.

13. Loi applicable et juridiction compétente :

Indiquer la loi applicable au contrat et la juridiction compétente en cas de litige.

14. Dispositions diverses :

Clauses supplémentaires, le cas échéant.

15. Signatures :

Signature des représentants autorisés des deux parties pour valider le contrat.

Un contrat de maintenance de site internet est essentiel pour définir clairement les attentes, les responsabilités et les droits des deux parties. Il est recommandé de consulter un avocat spécialisé en droit des contrats pour la rédaction ou la révision d'un tel contrat afin de s'assurer qu'il est conforme à la législation en vigueur et qu'il protège adéquatement les intérêts des deux parties.