Application : Réaliser une application web

Table des matières

I. Application : réaliser une application web

Conseil

Cette application permet de valider vos connaissances et acquisitions de la compétence, en lien avec le référentiel du parcours visé. Elle ne participe pas à l'obtention de votre parcours, mais vous permet de vous entraîner à l'appropriation de la pratique professionnelle attendue.

Veillez à la qualité de votre syntaxe.

Durée indicative : 1 heure(s)

Documents autorisés : tous les documents sont autorisés.

Matériel autorisé : tous les matériels sont autorisés.

II. Exercice : Partie 1 : API d'authentification

Vous travaillez pour une entreprise de taille moyenne. Suite une attaque récente, votre responsable vous demande de trouver une solution afin de sécuriser les comptes utilisateurs.

Question 1

[solution n°1 p.5]

1.1. Qu'est-ce qu'une API ?

Question 2

[solution n°2 p.5]

1.2. Qu'est-ce qu'une API d'authentification ?

Question 3

[solution n°3 p.5]

1.3. Proposez une API d'authentification.

III. Exercice : Partie 2 : paiement en ligne

Vous venez de créer un site e-commerce spécialisé dans la vente d'accessoires de fitness. Vous devez faire la partie sécurisation du paiement.

Question 1

[solution n°4 p.6]

2.1. Qu'est-ce qu'une API de paiement ?

Question 2

[solution n°5 p.6]

2.2. Pourquoi choisir un module de paiement par API ?

Question 3

[solution n°6 p.7]

2.3. Quelle solution proposez-vous ?

Solutions des exercices

p. 3 Solution n°1

Une API ou Application Programming Interface est une couche applicative permettant de connecter 2 services ensemble. Dans la majorité des cas, l'API ne tient pas compte d'un langage en particulier et fonctionne avec l'ensemble des projets. Par exemple, une API peut relier un service Python avec une requête provenant de code JavaScript sans problème.

Il y a deux grands types d'API : les API publiques, également appelées API ouvertes, et les API privées, appelées API d'entreprise. Les API sécurisées possèdent une clé d'identification, communiquée par un service d'authentification et d'autorisation.

En raison de la grande variété des applications clientes, les API s'appuient sur des protocoles de communication, SOAP (Simple Object Access Protocol) ou REST (Representational State Transfer), afin d'être compatibles avec les différentes plateformes, qu'il s'agisse d'applications Windows, Apple ou Android. La plus utilisée aujourd'hui est l'API Rest (ou Restful), car elle offre plus de flexibilité.

p. 3 Solution n°2

L'authentification est le moment où une entité prouve son identité. En d'autres termes, l'authentification prouve que vous êtes bien celui que vous prétendez être. C'est comme avoir un permis de conduire délivré par une autorité de confiance que le demandeur, comme un officier de police, peut utiliser comme preuve que vous êtes bien celui que vous dites être.

L'authentification des API est le processus qui consiste à vérifier l'identité de la personne qui accède à votre système. Il s'agit d'un processus qui utilise des protocoles logiciels pour assurer que les clients du réseau sont effectivement ceux qu'ils prétendent être avant que l'accès ne soit accordé.

Elle permet de bénéficier des avantages suivants :

- Sécurité renforcée :l'authentification de l'utilisateur complique toujours la tâche des cybercriminels qui cherchent à pirater des mots de passe ou des comptes, puisqu'ils sont obligés de passer par plusieurs mesures de sécurité plus poussées pour y accéder.
- Réduction du coût d'exploitation : pour les propriétaires de sites web, l'utilisation de l'authentification API peut vous éviter des coûts supplémentaires lorsque les données de vos clients sont en danger. En effet, certains utilisateurs n'hésiteront pas à engager une action en justice lorsqu'ils découvriront que des données ont été exposées ou compromises.
- Accroître la confiance des utilisateurs : les sites Web dotés d'une authentification API procurent un sentiment de sécurité aux utilisateurs et inspirent leur confiance. Les utilisateurs apprécient de savoir que leurs informations personnelles sont en sécurité, même lorsqu'ils sont obligés de passer par une étape de vérification supplémentaire.

p. 3 Solution n°3

L'Open Authorization ou OAuth est une méthode d'authentification énormément utilisée dans des projets Open Source comme le service Cloud auto- hébergé NextCloud et OwnCloud et dans des services propriétaires comme GitHub. Sa notoriété vient de plusieurs avantages pouvant lui être attribués comme la sécurité d'authentification qu'elle offre, la facilité de mise en place et d'utilisation ou même le fait que cette méthode soit Open Source. L'OAuth existe actuellement sous 2 formes, sa version 1 appelée le plus souvent OAuth et sa version 2 nommée OAuth2 dans la majorité des cas. Cependant malgré leur nom en commun les 2 versions sont totalement différentes et ne partagent que leurs visions de l'authentification, une réécriture de zéro ayant été réalisée.

OAuth 2.0 fournit plusieurs flux populaires adaptés à différents types de clients d'API, les flux sont des scénarios qu'un client d'API exécute pour obtenir un jeton d'accès du serveur d'autorisation.

- Code d'autorisation :utilisé principalement pour les applications web côté serveur et mobiles. Ce flux est similaire à la façon dont les utilisateurs s'inscrivent à une application web en utilisant leur compte Facebook ou Google.
- Implicite : le client doit récupérer directement un jeton d'accès. Il est utile dans les cas où les informations d'identification de l'utilisateur ne peuvent pas être stockées dans le code client parce qu'elles peuvent être facilement accessibles par un tiers. Elle convient aux applications Web, de bureau et mobiles qui n'incluent aucun composant serveur.
- Mot de passe du propriétaire de la ressource - Nécessite de se connecter avec un nom d'utilisateur et un mot de passe. Comme dans ce cas, les informations d'identification feront partie de la demande, cette méthode ne convient qu'aux clients de confiance (par exemple, les applications officielles publiées par le fournisseur d'API).
- Informations d'identification du client - Destiné à l'authentification de serveur à serveur, il décrit une approche dans laquelle l'application client agit en son propre nom plutôt qu'au nom d'un utilisateur individuel. Dans la plupart des scénarios, il fournit les moyens de permettre aux utilisateurs de spécifier leurs informations d'identification dans l'application client, afin que celle-ci puisse accéder aux ressources sous le contrôle du client.

OAuth 2.0 est le meilleur choix pour identifier les comptes utilisateurs personnels et accorder les autorisations appropriées. Dans cette méthode, l'utilisateur se connecte à un système. Ce système demande alors une authentification, généralement sous la forme d'un jeton. L'utilisateur transmet ensuite cette demande à un serveur d'authentification, qui rejette ou autorise cette authentification. De là, le jeton est fourni à l'utilisateur, puis au demandeur. Ce jeton peut ensuite être vérifié à tout moment indépendamment de l'utilisateur par le demandeur pour validation et peut être utilisé dans le temps avec une portée et une durée de validité strictement limitées.

p. 3 Solution n°4

Une API de paiement est une API conçue spécifiquement pour échanger des informations avec la banque afin de permettre d'effectuer des paiements sécurisés directement sur votre site web marchand ou votre interface de paiement.

Une bonne API de paiement se caractérise par une intégration facile sur votre site web et la protection des données.

p. 3 Solution n°5

Grâce à l'API, l'utilisateur effectue la transaction, puis votre site Web vérifie directement auprès de la banque que les informations sont correctes et que le paiement est effectué. La transaction est synchronisée et l'utilisateur voit immédiatement si le paiement a réussi.

Lorsque l'utilisateur effectue un paiement sur la page de la banque, le site vérifie toujours la transaction lorsqu'il revient sur le site. Il s'agit d'un traitement asynchrone qui peut être source de frustration pour l'utilisateur. Si le serveur de la banque revient trop tard, ou s'il n'y a pas de transaction à associer à l'achat, le site web indiquera que le paiement a échoué.

Ce système de paiement présente plusieurs avantages :

- Expérience utilisateur fluide : le parcours de l'utilisateur reste ainsi fluide. Ils ne quitteront pas votre site et passeront d'une étape à l'autre sans réfléchir.
- Meilleures performances : Lors de la mise en place d'un module de paiement, le site web ou l'application échangera des informations avec la banque. Lorsqu'il y a un fonctionnement par API, cette communication est synchronisée, ce qui permet d'éviter certaines erreurs ou risques.

- Tracking E-commerce : il y a souvent un écart entre le chiffre d'affaires réel généré et les chiffres figurant dans votre outil de suivi statistique (par exemple, Google Analytics). Un facteur qui revient souvent dans cet écart est la sortie du site au milieu du cheminement de l'utilisateur. Lorsque vous n'utilisez pas tous les points d'API ou que les utilisateurs quittent le site au moment du paiement, l'outil de suivi risque de perdre la trace de la transaction s'ils choisissent de ne pas revenir sur le site au moment du paiement.

p. 3

Solution n°6

Pour le paiement sur un site e-commerce, il est possible d'utiliser Payline, Lemonway ou Stripe. Les trois services proposent un paiement via CB, Visa, Mastercard et de nombreux autres moyens de paiement.

Stripe est une solution de paiement en ligne spécialement conçue pour les e-commerçants. Il les aide à développer et à faciliter leurs processus et leurs stratégies de conversion des clients. Il prend en compte :

- Les systèmes d'abonnement
- Le paiement sur la boutique
- Les dons / investissements dans des projets de financement

Stripe est une solution idéale pour les développeurs, car elle permet une grande flexibilité et une adaptation à votre boutique en ligne. Le fait que l'entreprise ait annoncé son soutien à la communauté des développeurs l'a amenée à imaginer une solution modulaire, puissante et évolutive.

En outre, la solution est constamment améliorée. L'objectif est de fournir aux utilisateurs une plateforme toujours à la pointe de la technologie. De nouvelles fonctionnalités sont ajoutées en permanence. Cela est dû aux différentes équipes au sein de l'entreprise.