
Documentation technique du projet LabXpert - Angular

Réalisé par

GUELSA Mouna

2023-2024

TABLE DES MATIÈRES

Documentation	2
1 Introduction	2
2 Etude technique et technologique	2
3 Démonstration	3
4 Conclusion	3

1 Introduction

Dans tout projet reposant sur Angular, la sécurisation des données et des utilisateurs est une priorité cruciale. Intégrer des mesures de sécurité solides dès les premières étapes du développement est essentiel pour prévenir les vulnérabilités et établir la confiance des utilisateurs. À cet égard, l'utilisation des fonctionnalités de sécurité d'Angular se révèle être une approche efficace et intégrée pour gérer l'authentification, l'autorisation, ainsi que d'autres aspects de la sécurité dans votre application. Cette introduction explorera les principaux points à considérer lors de l'implémentation de la sécurité dans votre projet Angular, soulignant l'importance de cette démarche et les avantages de l'utilisation des fonctionnalités de sécurité fournies par Angular.

2 Etude technique et technologique

* Guards (Gardes) :

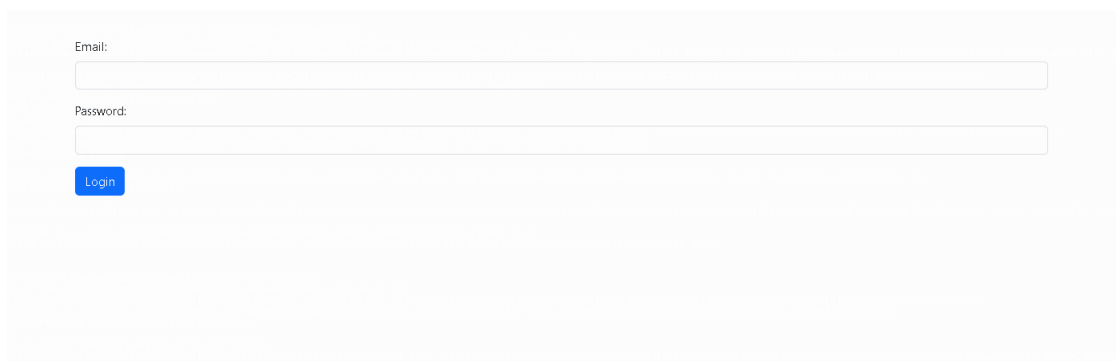
Les guards (ou gardes) sont des éléments essentiels dans la stratégie de sécurité d'une application Angular. Ils agissent comme des gardiens, contrôlant l'accès aux différentes parties de l'application en fonction des règles prédéfinies. En vérifiant l'authentification de l'utilisateur, en autorisant ou en refusant l'accès en fonction des permissions accordées, les guards permettent de sécuriser efficacement les routes et fonctionnalités sensibles. Par exemple, un guard 'CanActivate' peut empêcher un utilisateur non authentifié d'accéder à certaines pages de l'application, tandis qu'un guard 'CanActivateChild' peut restreindre l'accès à des sous-routes spécifiques à certains utilisateurs ou rôles. Grâce à leur flexibilité et à leur intégration transparente avec le système de routage d'Angular, les guards offrent un moyen puissant de renforcer la sécurité tout en assurant une expérience utilisateur fluide et sécurisée. En les utilisant de manière appropriée, les développeurs peuvent créer des applications Angular robustes et sécurisées, capables de protéger efficacement les données et les ressources sensibles contre les accès non autorisés.

* Les intercepteurs

Les interceptors jouent un rôle crucial dans le renforcement de la sécurité et de la fiabilité des communications HTTP au sein des applications Angular. Agissant comme des points d'entrée et de sortie pour chaque requête HTTP, les interceptors offrent un moyen centralisé de gérer les en-têtes, de traiter les erreurs et d'ajouter des fonctionnalités de sécurité supplémentaires. Par exemple, un interceptor peut être utilisé pour intercepter chaque requête sortante et y ajouter automatiquement un jeton d'authentification, garantissant ainsi que seules les demandes provenant d'utilisateurs authentifiés sont acceptées par le serveur. De même, ils peuvent être utilisés pour gérer les réponses entrantes, vérifier les codes d'état, et prendre des mesures appropriées en cas d'erreur ou de besoin de rafraîchissement du jeton d'authentification. En centralisant la logique de traitement des requêtes HTTP, les interceptors favorisent une meilleure maintenabilité du code et une cohérence dans la gestion des communications réseau au sein de l'application. Leur flexibilité permet également d'implémenter des stratégies de sécurité avancées, telles que la prévention des attaques CSRF en ajoutant des en-têtes anti-forgery à chaque requête sortante. Ainsi, en utilisant judicieusement les interceptors, les développeurs peuvent renforcer la sécurité de leurs applications Angular tout en améliorant la fiabilité et la cohérence des communications réseau.

3 Démonstration

* Login :



A login form with a light gray background. It contains two input fields: 'Email:' and 'Password:'. Below the 'Password:' field is a blue 'Login' button.

4 Conclusion

Intégrer la sécurité à un projet Angular est une étape essentielle pour garantir la protection des données et instaurer la confiance des utilisateurs. En adoptant une approche proactive dès les phases initiales de développement, Angular propose une solution complète et flexible pour répondre aux exigences de sécurité modernes. Elle simplifie la gestion de l'authentification, de l'autorisation et d'autres aspects de la sécurité.