

Spring Security et authentification

Apprenez à mettre en œuvre une authentification et un contrôle d'accès sécurisés dans vos applications Spring.

Catégorie: Programmation · Durée: 2 jours

POUR QUI ?

- Développeurs Java
- Ingénieurs sécurité et administrateurs système
- Équipes qui veulent pratiquer sur des cas réels

Dans cette formation, vous acquerrez une compréhension complète de Spring Security et apprendrez à exploiter ses fonctionnalités pour authentifier les utilisateurs et protéger vos applications contre les accès non autorisés. Vous explorerez différents mécanismes d'authentification, tels que identifiant/mot de passe, OAuth et JWT, et découvrirez comment mettre en œuvre un contrôle d'accès basé sur les rôles et sécuriser des API REST. À l'issue de cette formation, vous disposerez des connaissances et compétences nécessaires pour concevoir des applications Spring robustes et sécurisées.

Prérequis

Connaissances de base du framework Spring et du développement d'applications web.

Programme

- Introduction à Spring Security
- Authentification par identifiant et mot de passe
- Authentification avec OAuth
- Authentification avec les JSON Web Tokens (JWT)
- Autorisations et contrôle d'accès
- Mise en œuvre du contrôle d'accès basé sur les rôles
- Sécurisation des API REST
- Sécurisation des applications web
- Utilisation de Spring Security avec Spring Boot
- Bonnes pratiques d'authentification sécurisée
- Sécurisation des intégrations tierces
- Sécurisation des bases de données et du stockage

- Sécurisation des applications côté client
- Mise en place de l'authentification unique (SSO)
- Sécurisation d'une architecture microservices
- Supervision et journalisation à des fins de sécurité
- Tests et débogage des problèmes de sécurité
- Sécurisation des téléversements et téléchargements de fichiers
- Mise en place de l'authentification à deux facteurs (2FA)
- Prévention des vulnérabilités de sécurité courantes
- Sécurisation de la gestion des sessions