Publicatiedatum : 26/03/2025

Opleiding : Beveiliging van Java-toepassingen

Praktijkcursus - 3d - 21u00 - Ref. JAS
Prijs : 1650 € V.B.

4,7 / 5

Nouvelle édition

In deze cursus krijg je inzicht in de mechanismen voor beveiligingsbeheer die Java biedt, door middel van een theoretische studie van de concepten en hun geleidelijke implementatie binnen standalone applicaties en applicatieservers.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- Beveiliging implementeren in de virtuele machine van Java
- Gebruik moderne beveiligde infrastructuren om uw applicaties te beveiligen
- Webservices beveiligen met OAuth 2.0

Doelgroep

Ontwikkelaars en projectmanagers die betrokken zijn bij het beveiligen van Java-toepassingen.

Voorafgaande vereisten

Zeer goede kennis van de taal Java. Ervaring met programmeren in Java vereist.

Praktische modaliteiten

Praktisch werk

Beveiliging implementeren in de virtuele machine van Java.

Opleidingsprogramma

DEELNEMERS

Ontwikkelaars en projectmanagers die betrokken zijn bij het beveiligen van Java-toepassingen.

VOORAFGAANDE VEREISTEN

Zeer goede kennis van de taal Java. Ervaring met programmeren in Java vereist.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

1 Grondbeginselen van de beveiliging van Java-toepassingen

- Inleiding tot de JVM.
- Gebruik van recente versies van Java (Java 17+).
- Bytecode en verduistering.
- Afhankelijkheden beheren met Maven en kwetsbaarheden detecteren in bibliotheken.
- Implementatie van een veilig logsysteem (bijv. SLF4J, Logback of Log4J).

2 Authenticatiebeheer

- De verschillende authenticatiemethoden (wachtwoord, biometrisch, digitale sleutel, enz.).
- Gebruik van de OAuth 2.0 standaard voor modern toegangsbeheer.
- JWT (JSON Web Tokens) voor veilig sessiebeheer.
- Multi-factorauthenticatie (MFA).
- Integratie van een identiteitsprovider.

Praktisch werk

Mise en place d'un processus d'identification par mot de passe, d'une clé d'API et d'un token JWT avec Keycloak.

3 Toegangscontrole en autorisaties

- Principe van de minste privileges in toepassingen.
- Gebruik van RBAC (Role-Based Access Control).
- Toegangscontrole implementeren in applicaties. (Spring Beveiliging).

Praktisch werk

Implementatie van een beveiligde sectie gebaseerd op het principe van least privilege met Spring Security.

4 SSL/TLS gebruiken

- Gebruik van SSL/TLS om communicatie te beveiligen.
- Veilige configuratie van databaseverbindingen (gebruik van SSL/TLS om verbinding te maken met MySQL/PostgreSQL).
- Een zelfondertekend certificaat genereren met Java KeyStore.

Praktisch werk

Een zelfondertekend certificaat genereren met KeyStore en een toepassing hosten met SSL.

5 Gegevensbeveiliging

- SQL Injection : comment les éviter (utilisation des Prepared Statements, ORMs comme Hibernate).
- Encryptie van gevoelige gegevens in de database.
- Beheer van databasetoegang (scheiding van rollen en privileges).
- Veilig wachtwoordbeheer (opslag met algoritmen zoals MD5, SHA256 of bcrypt).

Praktisch werk

Création d'une base de données stockant des mots de passe chiffrés, connexions utilisateurs et utilisation de requêtes préparées.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

6 Moderne veilige infrastructuur

- De verschillende HTTPS-certificaten.
- Zero trust modellen.
- Java-beveiliging binnen containers.
- SIEMS.
- Het CORS-protocol.
- Veilige architecturen door ontwerp.

7 De verschillende soorten aanvallen

- Validatie van gebruikersinvoer (Vertrouw nooit op gebruikersinvoer).
- RESTful API's beveiligen met headers zoals Autorisatie en X-XSS-bescherming.
- SQL-injecties.
- XSS en opschonen van gebruikersinvoer.
- CSRF (Cross-Site Request Forgery): implementatie van anti-CSRF tokens.

Praktisch werk
Gebruikersgegevens opschonen met OWASP.

Data en plaats

KLAS OP AFSTAND
2026 : 3 juni, 14 sep.

PARIS LA DÉFENSE
2026 : 3 juni, 14 sep.