Opleiding : Campus Atlas - Applicatiebeveiliging

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

NEW

À l'issue de la formation, le participant sera capable de développer des applications web et mobiles sécurisées. Tous les points fondamentaux de la sécurité des applications seront abordés, des modèles de maturité aux bonnes pratiques en Java incluant un tour d'horizon des vulnérabilités courantes et spécifiques pour mieux les gérer. Ce programme de formation est destiné aux salariés des branches professionnelles relevant de l'OPCO Atlas.

Pedagogische doelstellingen

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

- Problemen met applicatiebeveiliging begrijpen
- De belangrijkste bedreigingen en kwetsbaarheden voor web- en mobiele applicaties identificeren
- Goede beveiligingspraktijken toepassen bij de ontwikkeling van applicaties
- Tools en technieken gebruiken om kwetsbaarheden in de beveiliging op te sporen en te verhelpen
- Ontdek de basisprincipes van cyberbeveiliging en hun invloed op de beveiliging van applicaties

Doelgroep

Leden van OPCO Atlas: architecten, ontwikkelaars, analisten, projectmanagers, enz.

Voorafgaande vereisten

Posséder une bonne connaissance de la programmation objet et de la programmation
d'applications web.

DEELNEMERS

Leden van OPCO Atlas: architecten, ontwikkelaars, analisten, projectmanagers, enz.

VOORAFGAANDE VEREISTEN

Posséder une bonne connaissance de la programmation objet et de la programmation
d'applications web.

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.

Praktische modaliteiten

Praktisch werk

Praktische oefeningen en/of casestudies.

Leer methodes

60% pratique – 40% théorie. Pour optimiser le parcours d'apprentissage, des modules e-learning peuvent être fournis avant et après la session présentielle ou la classe virtuelle, sur simple demande du participant.

Opleidingsprogramma

1 OWASP Top 10 - Kwetsbaarheden in webtoepassingen deel 1 - Vooropleiding digitale leerinhoud

- Inleiding.
- Gebrek aan toegangscontrole.
- Onjuiste beveiligingsconfiguratie.
- Cross-site scripting (XSS).
- Onveilige deserialisatie.
- Gebruik van componenten met bekende kwetsbaarheden.
- Gebrek aan logging en monitoring.

Digitale activiteiten

In deze online cursus leert u meer over de laatste 6 kwetsbaarheden in de OWASP top 10, de beveiligingsprincipes die u moet kennen om ze te voorkomen, de technieken die hackers gebruiken om ze te misbruiken en de best practices en tegenmaatregelen die u kunt nemen om uw webapplicaties te beschermen.

2 IT-beveiliging, essentiële concepten en beschermingstechnieken voor gebruikers - Inhoud voor digitale vooropleiding

- Veiligheidsconcepten.
- Kwaadaardige software.
- Netwerkbeveiliging.
- Veilig gebruik van het web.
- Veilig gebruik van e-mail.
- Beheer van gegevensbeveiliging.

Digitale activiteiten

In deze e-learningcursus leer je over de belangrijkste IT-beveiligingsrisico's, hun oorzaken en gevolgen, en de best practices om ze te voorkomen. Na een inleiding tot de fundamentele concepten, verkent u de bedreigingen die samenhangen met malware, netwerken, surfen op internet, messaging en de bescherming van opgeslagen gegevens, zodat u uw computer met het volste vertrouwen kunt gebruiken.

3 Inleiding tot applicatiebeveiliging

- Belangrijkste definities: kwetsbaarheid, dreiging, risico, aanval.
- Beveiligingsspelers: CERT, OWASP, BSIMM.
- Risico's die gepaard gaan met het ontwikkelen van een applicatie.
- Sporen achtergelaten door ontwikkelaars: geheugen, logs, enz.

Demonstratie

Analyse van een kwetsbare applicatie om de sporen te identificeren die de ontwikkelaars hebben achtergelaten.

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.

4 Volwassenheidsmodellen voor beveiliging

- Presentatie van het OpenSAMM-model.
- De 4 niveaus van volwassenheid.
- Inleiding tot het BSIMM (Building Security In Maturity Model).

Praktisch werk
Het volwassenheidsniveau van een organisatie berekenen met OpenSAMM.

5 Veelvoorkomende kwetsbaarheden in webapplicaties

- De praktische gids Application Security Verification Standard (ASVS).
- Een ecosysteem van open source tools.
- OWASP Top 10: Gebroken toegangscontrole, cryptografische fouten, injectie (bijv. SQL-injectie)...

Praktisch werk
Eenvoudige uitbuiting van een SQL Injection of XSS-fout in een mini-Java-toepassing. Hoe had dit voorkomen kunnen worden?

6 Kwetsbaarheden die specifiek zijn voor mobiele toepassingen

- Onbeveiligde opslag.
- Zwakke verificatie.
- API-tentoonstelling.

Praktisch werk
Analyse van een mobiele applicatie om specifieke kwetsbaarheden te identificeren.

7 Veiligheid door ontwerp

- Principes van beveiliging door ontwerp.
- Beveiliging integreren in de ontwikkelcyclus (DevSecOps).

Demonstratie
Casestudy in het ontwerpen van veilige toepassingen.

8 Beste werkwijzen in Java

- Gebruikersinvoer valideren.
- Fout- en uitzonderingsafhandeling.
- REST API's beveiligen met Spring Security of Jakarta Security.

Praktisch werk
Spring Security of Jakarta Security gebruiken om een REST API te beveiligen.

9 Beveiliging van configuraties en afhankelijkheden

- Beheer van gevoelige configuraties.
- Afhankelijkheden bijwerken en bekende kwetsbaarheden beheren.

Demonstratie
Dependency-Check gebruiken om kwetsbaarheden in de afhankelijkheden van een Java-project te identificeren.

10 Mobiele toepassingen beveiligen

- Best practices voor veilige mobiele ontwikkeling.
- Specifieke tools en technieken voor mobiele platforms.

Praktisch werk
Goede beveiligingspraktijken toepassen op een bestaande mobiele applicatie.

11 Inleiding tot veiligheidstesten

- Doelstellingen van beveiligingstests: proactieve detectie.
- Statische codecontrole (SAST).
- Dynamische tests (DAST).
- Interactieve testen (IAST).

Demonstratie
Tool-gebaseerde analyse van een applicatie om kwetsbaarheden te identificeren.

12 Beheer van kwetsbaarheden

- Kwetsbaarheidsbeheerproces.
- Implementatie van corrigerende maatregelen en follow-up.

Praktisch werk
Het opstellen van een kwetsbaarheidsbeheerplan voor een bestaande applicatie.

13 Afsluitende workshop - De praktijk

- De verworven kennis toepassen op een volledig project.
- Kwetsbaarheden identificeren en verhelpen.
- Presentatie van de geïmplementeerde oplossingen.

Praktisch werk
Project om een web- of mobiele applicatie te beveiligen, van het identificeren van kwetsbaarheden tot het corrigeren ervan.

14 OWASP Top 10 - Kwetsbaarheden in webtoepassingen deel 2 - Post-training digitale leerinhoud

- Inleiding.
- Injecties.
- Schending van authenticatie en sessiebeheer.
- Blootstelling van gevoelige gegevens.
- De XXE (XML External Entity) aanval.

Digitale activiteiten
In deze online cursus leert u meer over de top 4 kwetsbaarheden in de OWASP Top 10, waaronder injecties (SQL, XPath, code), gebreken in authenticatie en sessiebeheer, blootstelling van gevoelige gegevens en XXE-aanvallen. U leert hoe hackers deze kwetsbaarheden misbruiken en welke best practices u kunt toepassen om uw webapplicaties te beveiligen.

Data en plaats

KLAS OP AFSTAND
2026 : 16 juni, 22 sep., 24 nov.

LILLE
2026 : 16 juni, 22 sep., 24 nov.

PARIS LA DÉFENSE
2026 : 9 juni, 15 sep., 17 nov.