Publicatiedatum : 12/02/2024

Opleiding : PHP, je applicaties beveiligen

Voor versies 8, 7 en 5

Praktijkcursus - 3d - 21u00 - Ref. PSE

Prijs : 1830 € V.B.

5 / 5

Door zijn aard opent een dynamische webpagina veel deuren naar de buitenwereld. Voor ontwikkelaars is het van vitaal belang om zich bewust te zijn van de typen aanvallen waaraan hun code mogelijk wordt blootgesteld en om te weten hoe ze hiermee om moeten gaan, wat het tweeledige doel is van deze cursus.

Pedagogische doelstellingen

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

- Wees je bewust van de typen aanvallen waaraan je code kan worden blootgesteld
- Veiligheid al in de ontwerpfase in de ontwikkeling integreren
- Identificeer potentiële ontwikkelingsfouten
- Veiligere applicaties ontwikkelen

Doelgroep

Ontwikkelaars die veiligere PHP-toepassingen willen ontwikkelen.

Voorafgaande vereisten

Goede kennis van PHP en SQL. Basiskennis van JavaScript.

Praktische modaliteiten

Praktisch werk

Windows-werkstations uitgerust met Apache2-servers met PHP, MySql, Oracle, LDAP, FTP en mail worden beschikbaar gesteld aan de deelnemers.

Leer methodes

Actief onderwijs op basis van voorbeelden, demonstraties, het delen van ervaringen, praktische casestudy's en beoordeling van het leerproces gedurende de hele cursus.

Opleidingsprogramma

DEELNEMERS

Ontwikkelaars die veiligere PHP-toepassingen willen ontwikkelen.

VOORAFGAANDE VEREISTEN

Goede kennis van PHP en SQL. Basiskennis van JavaScript.

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 Inleiding

- Presentatie van risico's.
- Vernietiging van gegevens.
- Site kapen.
- Publicatie van vertrouwelijke gegevens.
- Misbruik van middelen.
- Identiteitsdiefstal.
- Veiligheidsplan: ontwerp, ontwikkeling en onderhoud.

2 Webpagina's

- XSS-principes en beschermingsmethoden. Zoekmachine.
- CSRF: principe en tegenmaatregelen. Databasevirussen.

3 Formulieren: de grote deur

- Kwetsbaarheden. Validatie en beperkingen van de JavaScript-benadering. Chaining, HTTP en Ajax aanvallen. Tegenmaatregelen.
- Validatie van invoer. Tests en het principe van lijsten. Reguliere expressies, standaarden en filters.
- Uploaden. Kwetsbaarheden en tegenmaatregelen.

4 Cookies en sessies

- Cookies. Principes en risico's. JavaScript-behandeling. Cookietabellen.
- Sessies. Cookie versus headermodus. Principe van sessiediefstal.

5 PHP beveiligen: de juiste instellingen

- PHP.ini. Gevoelige directives, sessies en fouten.
- Scripts beschermen. Fysieke bescherming. Scripts op afstand of on-the-fly uitvoeren.

6 Databases

- Mogelijke kwetsbaarheden. Beheer. Opslag.
- SQL-injecties. Principe en tegenmaatregelen. Opgeslagen procedures en geparametriseerde queries. Beperkingen.
- Toegangsbestanden. Organisatie en standaardwaarden. Anonieme toegang en protocollen.

7 Het gebruik van uitbreidingen beveiligen

- E-mail. Spam via een contactformulier: injecties en tegenmaatregelen.
- Netwerktoegang met PHP. Sequentiële en recursieve aanroepen. Stealth aanvallen.

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.

8 Algemene overwegingen

- BFA. Principe. Identificatie en tegenmaatregelen.
- Phishing. Principe- en gebruikerstraining.
- DoS. Quota en belastingsbeheer.
- Wachtwoorden. Versterking en opslag .
- Encryptie en handtekening. Encryptie/decryptie: PHP en MySQL implementatie.
- Trucs. Honeypot, verduistering en omgekeerde Turing.
- Frameworks en softwarebouwstenen. Beveiligingsbeheer in samengestelde ontwikkelingen.
- Beveiligingsaudits. Basismethodologie, kruisproeven en auditrapport.

Data en plaats

KLAS OP AFSTAND
2026 : 8 juni, 21 okt.

PARIS LA DÉFENSE
2026 : 8 juni, 21 okt.