Publicatiedatum : 29/02/2024

Opleiding : Beveiliging van webtoepassingen, geavanceerd

Praktijkcursus - 3d - 21u00 - Ref. SEI
Prijs : 2100 € V.B.

4,6 / 5

Deze geavanceerde cursus geeft je de vaardigheden die je nodig hebt om jezelf te beschermen en effectiever te reageren op de vele bedreigingen van het web. Je leert hoe je de beveiliging van je applicaties controleert, ze test en de meest geschikte tegenmaatregelen implementeert.

Pedagogische doelstellingen

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

- Het proces begrijpen en een audit van een webapplicatie opzetten
- Een webserver opzetten met kwetsbaarheden om het gedrag ervan te observeren
- Beveiligingsmaatregelen implementeren voor webapplicaties
- Een private certificeringsinstantie met certificaatintegratie implementeren in een toepassing
- Gebruik een webspider om gebroken links en pagina's met of zonder verificatie op te sporen

Doelgroep

Netwerk- en systeembeheerders, webmasters.

Voorafgaande vereisten

Goede kennis van systemen en netwerken, basiskennis van ontwikkeling of kennis die gelijkwaardig is aan die van de cursus "Web Application Security" ref. SER.

DEELNEMERS

Netwerk- en systeembeheerders, webmasters.

VOORAFGAANDE VEREISTEN

Goede kennis van systemen en netwerken, basiskennis van ontwikkeling of kennis die gelijkwaardig is aan die van de cursus "Web Application Security" ref. SER.

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

Oefening

Gedurende de hele cursus worden talloze oefeningen en casestudy's aangeboden.

Leer methodes

Theoretische fundamenten geïllustreerd met praktische oefeningen.

Opleidingsprogramma

1 Herinnering aan de belangrijkste beveiligingsproblemen

- Cross-Site Scripting (XSS)-aanval.
- Opdrachtinjectie en SQL-injectie.
- Denial of Service (DoS)-aanvallen.
- Distributed Denial of Service (DDoS).
- Bufferoverloop.
- Het Open Web Application Security Project (OWASP).

Praktisch werk

Een webserver opzetten met kwetsbaarheden om het gedrag ervan te observeren. Aantonen hoe een bufferoverloop kan worden misbruikt.

2 Toepassingsbeveiliging

- Basisconcept en belang.
- De accounts die zijn aangemaakt om de tests uit te voeren.
- Kunnen we zonder fictieve bestanden?
- Zijn de test- en afstemreeksen nog steeds aanwezig in de productie?

3 Een webapplicatie auditen en beveiligen

- Een audit uitvoeren en implementeren. Interactie met de database beheren.
- Veilige authenticatie instellen. Een authenticatiefout misbruiken.
- Fout-, uitzonderings- en logboekbeheer.
- Weten hoe je logboekinformatie moet analyseren en correleren.
- Best practices voor veilige formulieren. Voorbeeld van een slecht ontwikkeld formulier.

Praktisch werk

Implementatie van een drielaags infrastructuur: client, webserver en databases. Simulatie van een aanvalspoging. Analyse en oplossing.

4 Encryptie

- Een herinnering aan de basisprincipes.
- Encryptie implementeren in een applicatie. Mogelijk gebruik.
- Test of een applicatie goed beveiligd is met encryptie.
- Encryptietoepassingen op de markt.

Praktisch werk

Implementatie van een private certificeringsinstantie met integratie van certificaten in een applicatie.

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.

5 Toepassingen testen

- Hoe te testen voordat je live gaat.
- Fingerprinting: het identificeren van de kenmerken van de server (web engine, framework, applicaties).
- Gebruik een webspider om gebroken links en pagina's met of zonder verificatie en codering op te sporen.
- Hoe de beschikbaarheid van een applicatie meten met behulp van simulatie.

Praktisch werk
Voorbeeld van pogingen tot aanvallen en fingerprinting. Hoe een webspin schrijven om gebroken links te detecteren. Authenticatie op pagina's controleren.

Data en plaats

KLAS OP AFSTAND
2026 : 25 maa., 27 mei, 5 okt., 7 dec.

PARIS LA DÉFENSE
2026 : 25 maa., 27 mei, 5 okt., 7 dec.