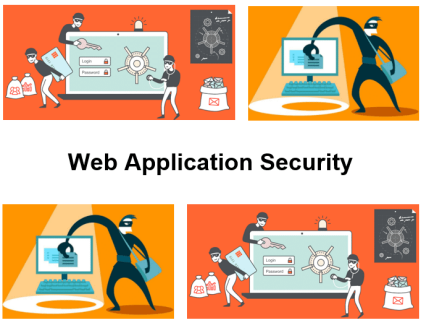
Web Application Security

Duur: 2 dagen **Prijs: € 1399**

Open Rooster



Doelgroep Cursus Web Application Security

De cursus Web Application Security is bedoeld voor web developers die willen leren hoe je web applicaties beschermt tegen de vele veiligheidsrisico's.

Voorkennis Cursus Web Application Security

Om aan deze cursus te kunnen deelnemen is ervaring met het ontwikkelen van web applicaties vereist. Ervaring met PHP of JavaScript is bevorderlijk voor de begripsvorming maar niet vereist.

Uitvoering Training Web Applicatie Security

De cursus Web Applicatie Security heeft een hands-on karakter. De theorie wordt behandeld aan de hand van presentatie slides en wordt afgewisseld met praktische oefeningen. Het cursusmateriaal is Engelstalig. De cursustijden zijn van 9.30 tot 16.30.

Certificering cursus Web Applicatie Security

De deelnemers krijgen na het goed doorlopen van de training een officieel certificaat Web Applicatie Security.

Inhoud Cursus Web Application Security

De cursus Web Application Security gaat in op de meest voorkomende security risico's bij web applicaties en hoe deze kunnen worden aangepakt. In een tijd waarin aanvallen op applicaties alleen maar toe lijken te nemen, is voor developers van groot belang zich bewust te zijn van de soorten bedreigingen en hoe applicaties daartegen kunnen worden gewapend.

Security Issues

De cursus gaat van start met een bespreking de meest voorkomende security issues zoals die zijn benoemd in het Open Web Application Security Project (OWASP). Hierbij wordt onder andere ingegaan op de risico's van kwetsbaarheden in libraries, het belang van het minimaliseren van het attack surface van een applicatie en kwetsbaarheden in authenticatie controle.

Cross Site Scripting

Bij Cross-Site Scripting (XSS) aanvallen worden kwaadaardige scripts geïnjecteerd in een web site. Typisch gebeurt dit doordat de aanvaller JavaScript code laat uitvoeren in de browser. XSS aanvallen komen veel voor en kunnen overal in de applicatie optreden waarbij user input niet wordt gevalideerd.

SQL Injection

Ook wordt aandacht besteed aan SQL Injection waarbij een aanvaller kwaadaardige code in SQL statements plaatst. SQL Injection heeft meestal als oorzaak dat ongecontroleerde user input wordt gebruikt voor de aanmaak van SQL statements. De gevolgen van SQL Injection kunnen ernstig zijn zoals data corruptie, data diefstal of de vernietiging van data.

Cross Site Request Forgery

Vervolgens is het de beurt aan de bespreking van CSRF. Aan de orde komt hoe bij CSRF kwaadaardige commando's in naam van een door de web applicatie vertrouwde gebruiker worden uitgevoerd. Vaak wordt hierbij gebruikt gemaakt van speciaal ontworpen image tags of hidden forms.

Session Hijacking

En ook Session Hijacking staat op het programma van de cursus. Bij Session Hijacking weet de aanvaller via sniffing technieken of XSS een session ID te bemachtigen en die vervolgens kwaadaardig te exploiteren.

SSL Certificates

Tenslotte wordt in de cursus Web Application Security ingegaan op het beveiligen van web applicaties door middel van SSL of TLS. Een encrypted communicatie kanaal zorgt er dan voor dat data veilig getransporteerd kan worden en digital certificates zorgen voor de authenticatie.

Modules Cursus Web Application Security

Module 1 : Intro Security	Module 2 : Cross Site Scripting	Module 3 : SQL Injection
Security Risks Top 1O OWASP Risks Sensitive Data Exposure Broken Authentication Social Engineering Library Vulnerabilities Sensitive Data Exposure Attack Surface Security Patches Under Protected API's Coding for Security	Malicious Code Cookie Theft HTML Entity Encoding XSS Prevention Rules Prevent Untrusted Data Attribute Encoding JavaScript Encoding HTML Encode JSON CSS Encoding URL Encoding Sanitize HTML Markup	SQL Injection Exploits Preventing SQL Injection Avoiding Dynamic Queries Prepared Statements Stored Procedures Allow-List Input Validation Escaping User Input Enforcing Least Privilege Union Injections Database Differences Blind SQL Injection
Module 4 : Cross-Site Request Forgery	**Module 5 : Session Hijacking**	**Module 6 : SSL Certificates**
CSRF Attacks Malicious Requests Stored CSRF Flaws IMG or IFRAME Tags Secret Cookies Only Accept POST Form Tokens URL Rewriting Same Origin Policy Check Referrer Header	Authentication Handshake Session Cookies Cookie Theft Session Sidejacking Session Fixation Man in the Middle Packet Sniffing Hijack TCP-IP Session Checking IP Session Encryption	SSL and TLS Public and Private Keys Encryption Methods Asymmetric Encryption Symmetric Encryption Hash Encryption SSL Certificates Root Certificates Wildcard Certificates PKI Infrastructure