Web Application Security

Duration: 2 days **Price: € 1399**

Open Schedule

Audience Course Web Application Security

The course Web Application Security is intended for web developers who want to learn how to protect web applications against the many security risks.

Prerequisites Course Web Application Security

Experience in developing web applications is required to participate in this course. Experience with PHP or JavaScript is beneficial for understanding but not required.

Realization Training Web Application Security

The course Web Application Security has a hands-on character. The theory is treated on the basis of presentation slides and is interchanged with practical exercises. The course material is in English. Course times are from 9.30 up and to 16.30.

Certification Course Web Application Security

After successful completion of the training the participants receive an official certificate Web Application Security.

Content Course Web Application Security

The Web Application Security course discusses the most common security risks in web applications and how they can be tackled. At a time when attacks on applications seem to be on the rise, it is vital for developers to be aware of the types of threats and how the applications can be armed against them.

Security Issues

The course starts with a discussion of the most common security issues as identified in the Open Web Application Security Project (OWASP). This includes the risks of vulnerabilities in libraries, the importance of minimizing the attack surface of an application and vulnerabilities in authentication control.

Cross Site Scripting

In Cross-Site Scripting (XSS) attacks, malicious scripts are injected into a web site. Typically, this happens because the attacker makes JavaScript code run in the browser. XSS attacks are common and can occur anywhere in the application where user input is not validated.

SQL Injection

Attention is also paid to SQL Injection, where an attacker places malicious code in SQL statements. SQL Injection is usually due to unchecked user input being used to create SQL statements. The consequences of SQL Injection can be serious such as data corruption, data theft or data destruction.

Cross Site Request Forgery

Next up in the course is the discussion of CSRF. Attention is paid to how CSRF executes malicious commands on behalf of a user trusted by the web application. Specially designed image tags or hidden forms are often used for this.

Session Hijacking

And Session Hijacking is on the program of the course as well. With Session Hijacking the attacker manages to obtain a session ID via sniffing techniques or XSS and then maliciously exploit it.

SSL Certificates

Finally the course Web Application Security discusses securing web applications by means of SSL or TLS. An encrypted communication channel then ensures that data can be transported securely and digital certificates provide authentication.

Modules Course 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

SpiralTrain BV
Standerdmolen 10, 2e verdieping
3995 AA Houten

info@spiraltrain.nl
www.spiraltrain.nl
Tel.: +31 (0) 30 – 737 0661

Locations
Houten, Amsterdam, Rotterdam, Eindhoven, Zwolle, Online