Data Security for Developers

Duration: 5 days **Price: € 3299**

Open Schedule

Data Security for Developers


Audience Course Data Security for Developers

The course Data Security for Developers is intended for developers who want to learn what data security risks there are and how you can arm yourself against them.

Prerequisites Course Data Security for Developers

To participate in the course Data Security for Developers, experience with software development is required. Experience with object-oriented programming in C#, Python or Java is beneficial for understanding.

Realization Training Data Security for Developers

The course Data Security for Developers has a hands-on character. The theory is treated on the basis of presentation slides and is interchanged with practical exercises.

Certification Course Data Security for Developers

After successfully completing the training, the attendants receive a certificate of participation in the course Data Security for Developers.

Content Course Data Security for Developers

The course Data Security for Developers covers the most common risks in securing data and how you can arm yourself against them. Attention is paid to data protection, securing communication, configuring access control and using authentication methods. Standards such as the General Data Protection Regulation (GDPR) are discussed as well.

Intro Data Security

The course starts with a discussion and explanation of the main concepts that play a role in Data Security such as authentication, access control, encryption, confidentiality, integrity, as well as backup and recovery.

Secure Communication

Subsequently setting up secure connections over Secure Sockets Layers (SSL) is treated. The creation of client and server certificates and the role of certificate authorities is covered.

Encryption

Then the different types of encryption are explained such as symmetric, asymmetric and hash encryption. And various encryption algorithms such as RSA and ECC are considered.

Web App Risks

Next attention is paid to typical security risks that play a role in web applications. The prevention of cross site scripting, SQL injection, cross site request forgery and session hijacking are debated then.

Access Control

The safe regulation of access control by means of key management systems, secure password storage and two factor authentication are also on the program of the course. The importance of role-based and permission-based authorization is treated as well.

Updates, Monitoring and Logging

Next the importance of keeping systems and applications secure by applying updates is covered. And the importance of monitoring, logging and incident responding is discussed also.

Securing Apps and APIs

Finally attention is paid to keeping Apps and APIs secure by testing endpoints for data leakage and security flaws. Various standards for data regulation such as GDPR, CCPA, PCI DSS and HIPAA are also treated then.

Modules Course Data Security for Developers

Module 1 : Intro Data Security	Module 2 : Secure Communication	Module 3 : Secure Data at Rest
Access Controls Authentication Backups and Recovery Data Erasure Data Masking Data Resiliency Encryption Confidentiality Integrity Availability Cookie Theft	Secure Sockets Layer (SSL) Private and Public Key SSL Certificates Creating Certificates CSR's Client and Server Certificates Chain of Trust Trusted certificate authorities (CAs) Transport Layer Security Verify network connections Verify metadata in HTTP headers	Asymmetric Encryption Symmetric Encryption Hash Encryption Encryption Algorithms RSA algorithm ECC algorithm Using standard encryption Encoding and obfuscation Digital Signing Salt Function Protect against Malware
Module 4 : Web App Risks	**Module 5 : Keys and Passwords**	**Module 6 : Access Controls**
Cross Site Scripting Prevent Untrusted Data Social Engineering SQL Injection Escaping User Input Prepared Statements URL Rewriting Cross-Site Request Forgery Session Hijacking Session Fixation	Key management systems Assigning Keys Revoking Keys Rotating Keys Deleting Keys Secure passwords storage Avoid embedding in code Two factor Authentication Provide Two Factor option Remove vendor-supplied defaults	Role Base Security Lattice Based Access Control Separate Roles and Functions Role Assignment Role Authorization Permission Authorization Role Hierarchies Mandatory Access Control Discretionary Access Control Removing access and privileges
Module 7 : Updates and Patches	**Module 8 : Monitor and Log**	**Module 9 : Securing Apps and API's**
Addressing Security Vulnerabilities Applying Patches Keeping Systems Updated Checking Distributions Use Trusted Network Locations Emails and Attachments Manual Updates Automatic Updates Updating Core libraries	Event Recording Log Monitoring Tracing Sending Data Tracing Storing Data Monitoring Transfers Ensure system stability Incident Responding Improving Compliance Identify security breaches	Basic app security practices Assessing permissions and data needs Aligning data access to purpose of use Testing APIs for data leakage Testing endpoints for data leakage Testing transmissions third parties Scanning app and code Searching security flaws Regularly test security systems
Module 10 : Data Security Regulations		
GDPR, CCPA, PCI DSS and HIPAA General Data Protection Regulation California Consumer Protection Health Insurance Accountability Act Sarbanes-Oxley (SOX) PCI Data Security Standard ISO 27001		