Data Security voor Developers

Duur: 5 dagen **Prijs: € 3299**

Open Rooster

Data Security for Developers


Doelgroep Cursus Data Security voor Developers

De cursus Data Security voor Developers is bedoeld voor developers die willen leren welke data beveiligingsrisico's er zijn en hoe je je daar tegen kunt wapenen.

Voorkennis Cursus Data Security voor Developers

Om aan deze cursus te kunnen deelnemen is development ervaring vereist. Ervaring met object georiënteerd programmeren in C#, Python of Java is bevorderlijk voor de begripsvorming.

Uitvoering Training Data Security voor Developers

De cursus Data Security voor Developers heeft een hands-on karakter. De theorie wordt behandeld aan de hand van presentatie slides en wordt afgewisseld met praktische oefeningen.

Certificering cursus Data Security voor Developers

De deelnemers krijgen na het goed doorlopen van de training een certificaat van deelname aan de cursus Data Security voor Developers.

Inhoud Cursus Data Security voor Developers

De cursus Data Security voor Developers behandelt de meest voorkomende risico’s bij het beveiligen van data en hoe je je daar tegen kunt wapenen. Aandacht wordt besteed aan data protectie, het beveiligen van communicatie, het configureren van access control en het gebruik van authenticatie methoden. Ook standaarden zoals de General Data Protection Regulation (GDPR) worden besproken.

Intro Data Security

De cursus gaat van start met een bespreking en verklaring van de voornaamste concepten die een rol spelen bij Data Security zoals onder andere authenticatie, access control, encryptie, confidentiality, integrity en ook backup en recovery.

Secure Communication

Vervolgens wordt ingegaan op het opzetten van beveiligde verbindingen over Secure Sockets Layers (SSL). Hierbij komt de creatie van client en server certificates aan de orde en wordt de rol van certificate authorities besproken.

Encryption

Dan komen de verschillende types encryption aan bod zoals symmetrische, asymmetrische en hash encryption. En er wordt ingegaan op diverse encryption algorithms zoals RSA en ECC.

Web App Risks

Vervolgens wordt aandacht besteed aan typische security risks die bij web applicaties een rol spelen. Ingegaan wordt op het voorkomen van cross site scripting, SQL injection, cross site request forgery en session hijacking.

Access Control

Ook het veilig regelen van access control middels key management systems, secure password storage en two factor authentication staat op het programma van de cursus. Dan wordt eveneens het belang van role based en permission based authorization besproken.

Updates, Monitoring and Logging

Vervolgens wordt ingegaan op het belang van het veilig houden van systemen en applicaties door updates toe te passen. Het belang van monitoring, logging en incident responding komt eveneens aan de orde.

Securing Apps en API's

Tenslotte wordt aandacht besteed aan het veilig houden van Apps en API's door het testen van endpoints op data leakage en security flaws. Ook komen dan nog verschillende standaarden voor data regulatie zoals GDPR, CCPA, PCI DSS en HIPAA aan bod.

Modules Cursus Data Security voor 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		