Varighed: 1 dag
Deltagerpris: 6.800,00 dkr
Kursusnummer: LB1954

Cyber Security for Application Developers

Kort om undervisningen

Briefly about the teaching: This course is aimed at software developers and tech teams, focusing on fundamental cybersecurity concepts essential for protecting sensitive information and ensuring robust security in software systems. This course integrates theoretical knowledge with practical exercises, providing hands-on experience in implementing security measures to your infrastructure, application, and organization. The purpose of the course is to raise security awareness and introduce a coherent framework for addressing security concerns.

Indhold

The course is structured around the CIA triad: Confidentiality, Integrity, and Availability.

Confidentiality - how do we keep our secrets

- **Encrypt & Decrypt Files (Symmetric & Asymmetric)**: Learn the principles of basic file encryption using symmetric and asymmetric algorithms. Practical exercises include file, encryption and decryption. This is a simple and often overlooked tool to mitigate data leaks
- **What is sensitive information?** Categorization of data
- **Basic Access Control**: Implement and test file system permissions and database roles to understand how access controls safeguard data. Get familiar with authentication and authorization. Apply the Principle of Least Privilege
- **Encrypting Sensitive Data**: Explore techniques for encrypting sensitive data on a database using Transparent Data Encryption (TDE) or column-level encryption

Integrity - prevent and discover tampering of data and code

- **Logs Management**: Understand the importance of application, audit, access, and error logs. The importance of fine-grained logging. Learn about the principle of write-once-read-many (WORM) and centralized logging
- **Version Control & Code Reviews**: Emphasize the necessity of version control and code reviews in maintaining code integrity
- **Continuous Deployment. Your build and deploy pipeline matters**. Learn why build, release, and run should be strictly separated stages
- **Redundancy and Fault Tolerance**: Engage in exercises to horizontally scale applications

Availability - make sure users can access your systems

- **Securing APIs from DoS Attacks**: Identify potential DoS (Denial of Service) attack vectors
- **Caching**: Integrate a caching system to mitigate overload, ensure resilience, and lower latency

- **Message Queuing**: Improve system availability by adding message queuing mechanisms to ensure reliability, scalability, and resilience
- **Request limiter**: Practical implementation of request limiting by applying a request limiter for a vulnerable public endpoint
- **Web Application Firewall (WAF) and Content Delivery Network (CDN)**: Conduct vulnerability scans and enhance security with a WAF proxy. Enable a Content Delivery Network to mitigate most DDoS attacks

Forudsætninger

In the course, an API is the centerpiece in many of the exercises. The infrastructure is often containerized using docker and docker-compose. The examples can have application code in Java, Python, Ruby, C# and use miscellaneous libraries. It is not a prerequisite to have specific programming experience in all those languages. The examples have been chosen to illustrate principles. The course can be held in Danish or English, the courseware is in English.

Målgruppe

This course is ideal for software developers, system administrators, devops, and tech teams who develop or manage applications.

Efter kurset kan deltageren

After the course, the participant will have a solid understanding of the key principles of cybersecurity—confidentiality, integrity, and availability. They will have seen practical examples on how to implement security measures, ensuring their systems and applications are more secure, resilient, and reliable.

Kommende afholdelsesdatoer

Klik på nedenstående links for tilmelding til en af vores planlagte afholdelser

25/11 2024 - Storkøbenhavn
03/02 2025 - Storkøbenhavn
05/05 2025 - Storkøbenhavn

Oplysning om yderligere afholdelser findes på vores hjemmeside. Andre spørgsmål besvares meget gerne ved brug af vores kontaktformular eller på telefon (+45) 33 861 861