Curso CSDS300 - Escrever Código Seguro para a Web

Duração: 21h

Introdução

A cibersegurança é um tema cada vez mais importante para as organizações. A quantidade e a importância dos dados confiados a aplicações web não param de crescer, e quem defende precisa de saber protegê-las. Imagine a sua organização nas notícias — não por causa de um produto revolucionário, mas por causa de uma fuga com os dados de todos os clientes, incluindo informação pessoal e dados de cartão de crédito. Como programador web moderno, dominar cibersegurança é indispensável: simplesmente não se pode dar ao luxo de não o fazer.

Este curso percorre as várias ameaças e defesas de cibersegurança e ensina, na prática, a aplicá-las em ASP.NET Core. Entre outras coisas, vai aprender a autenticar com OpenID Connect e Entra ID, a proteger a sua API com OAuth2 e a proteger os dados da empresa com técnicas de cifra adequadas. Começando por sites simples renderizados no servidor e progredindo para APIs, JavaScript moderno e aplicações web completas — incluindo a integração de chatbots com IA —, este curso dá experiência prática e aprofundada na proteção de aplicações web, na perspetiva de quem as desenvolve.

Público-alvo

Este curso destina-se a programadores com experiência de ASP.NET Core que queiram tornar o mundo mais seguro através da aplicação de boas práticas de cibersegurança.

No final do curso

Após a conclusão deste curso, os formandos deverão ser capazes de:
- Aplicar threat modeling e o OWASP Top 10 ao desenvolvimento web.
- Utilizar corretamente cifra, hashing e assinatura.
- Proteger cookies, autenticação, autorização e formulários contra CSRF e overposting.
- Prevenir SQL injection, XSS e ameaças cross-origin, com CORS e Content Security Policy.
- Proteger APIs com OAuth2 e access tokens JWT, e proteger Single Page Applications.
- Avaliar as novas superfícies de ataque criadas por bots e pela IA.

Pré-requisitos

Experiência de desenvolvimento com ASP.NET Core.

Exames de certificação

(não existem exames)

Conteúdo programático em detalhe

Fundamentos e mentalidade de cibersegurança para a web
- Porque é que a segurança web importa
- Ameaças, vulnerabilidades e risco
- Princípios básicos de segurança

www.actualtraining.pt
Tel: +351 217 158 018

- Como funciona a Web do ponto de vista da segurança
- Autenticação e autorização

O OWASP Top 10 como mapa do curso

- Introdução ao OWASP Top 10
- Como vamos referir o OWASP ao longo do curso
- Técnicas gerais de mitigação

Cifra, hashing e assinatura

- Codificação, hashing, encriptação e assinatura digital
- Encriptação simétrica vs. assimétrica
- O que são as assinaturas digitais?
- Comunicação segura com HTTPS
- Algoritmos comuns: AES, RSA, SHA-2 e ECC
- Criptografia pós-quântica
- Encriptação em .NET
- Guardar palavras-passe corretamente com hashing e salts
- LAB: usar a DPAPI na sua aplicação web

Compreender e proteger cookies

- Compreender os cookies
- Proteger os seus cookies
- Cookies de terceiros e privacidade

Autenticação e autorização em aplicações web renderizadas no servidor

- Formas de autenticação: palavras-passe, MFA, passkeys, ...
- Os cookies como mecanismo de sessão (e porquê)
- Identidade baseada em claims no ASP.NET Core
- Políticas de autorização vs. papéis
- Falhas de autenticação
- Broken access control
- Fluxo de início de sessão OpenID Connect com o Entra ID
- Introdução aos tokens JWT
- LAB: proteger o seu sítio

Forms e estado: CSRF, overposting e validação

- Como funciona o CSRF
- Anti-forgery tokens e SameSite
- Riscos de overposting e mass assignment
- Validação de entrada, codificação de saída, sanitização e desserialização
- LAB: proteger contra CSRF e overposting

Acesso a dados em aplicações renderizadas no servidor: SQL injection e manuseamento seguro de dados

- Segurança das bases de dados
- Mecânica da SQL injection
- Parametrização (com EF Core)
- LAB: injetar SQL num sítio vulnerável

Proteger APIs com OAuth2 e access tokens JWT

- Porque é que os cookies não servem todos os clientes
- Panorâmica do OAuth2 (scopes, audiences e clients)

- Access tokens e refresh tokens
- Fundamentos da validação de JWT
- Scopes, papéis e claims em APIs
- OAuth2 com o Entra ID
- LAB: proteger e consumir a sua API

Pedidos a partir de JavaScript: CORS e ameaças cross-origin

- Same-origin policy
- O que o CORS faz mesmo (e o que não faz)
- Pedidos de preflight
- JavaScript e CSRF
- LAB: configurar o CORS

Injeção de scripts: XSS e Content Security Policy

- Tipos de XSS e vetores de ataque
- Codificação de saída em views renderizadas no servidor
- Tratamento seguro de HTML não fiável
- Fundamentos da content security policy
- LAB: proteger contra injeção de scripts

Proteger Single Page Applications

- Usar OAuth 2.0 com PKCE em clientes públicos, incluindo SPA e aplicações móveis
- Usar o padrão backend-for-frontend (BFF) para tratar tokens e lógica sensível no servidor
- Blazor: um caso de estudo
- LAB: proteger um projeto Blazor WASM com o padrão BFF

IA e cibersegurança: o bom, o mau e o vilão

- Bots tradicionais vs. bots com IA
- Abuso de automatização e deteção
- Mecanismos de verificação humana
- Prompt injection
- Excessive agency
- Tratamento inseguro da saída

Cibersegurança: o quadro geral

- Defesa em profundidade: controlos por camadas
- Registo, monitorização e deteção
- Segurança da cadeia de fornecimento de software em pipelines de CI/CD DevSecOps
- Segurança da infraestrutura: redes, configuração da nuvem, segredos e atualizações
- Identity and access management (IAM): privilégio mínimo, MFA e estratégia de sessões e tokens
- Frameworks e normas de segurança: OWASP ASVS, NIST, ISO 27001 e CIS Benchmarks
- Resposta a incidentes e recuperação: playbooks, cópias de segurança, exercícios de simulação e post-mortems
- Conformidade e privacidade: RGPD, classificação de dados, retenção, encriptação e controlos de acesso