scademy
secure coding academy

OWASP Top 10, C# Secure Coding Follow Up

CL-ONA | Virtual classroom | 1 day

Audience: C# Web developers
Preparedness: General C# and Web application development
Exercises: Hands-on

This course is the next step for our participants, who completed our OWASP Top 10, C# Secure Coding Fundamentals course. This is a follow up training, meaning that in order to attend this, everyone must already have the knowledge that is covered in the Fundamentals.

This course enables our participants to gain a deeper knowledge in the field, because here we emphasize the C#-specific aspects of secure coding instead of the general vulnerabilities.

At the end of the training everyone has the possibility to take an exam, where they are able to measure their level of the gained knowledge.

Outline:

Client-side security
.NET security architecture and services
Practical cryptography

Participants attending this course will:

Learn client-side vulnerabilities and secure coding practices
Learn to use various security features of the .NET development environment
Have a practical understanding of cryptography

Related courses:

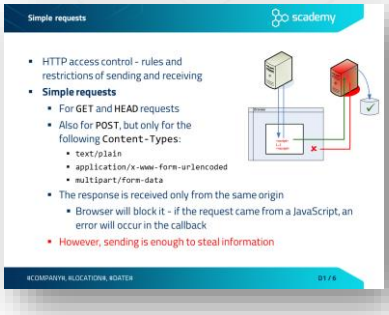
- CL-ANS - Secure desktop application development in C# (Onsite / Virtual classroom, 3 days)
- CL-NSM - C# and Web application security master course (Onsite / Virtual classroom, 5 days)
- CL-WSC - Web application security (Onsite / Virtual classroom, 3 days)
- CL-WTS - Web application security testing (Onsite / Virtual classroom, 3 days)
- CL-NSM - C# and Web application security master course (Onsite / Virtual classroom, 5 days)

scademy
secure coding academy

Detailed table of contents

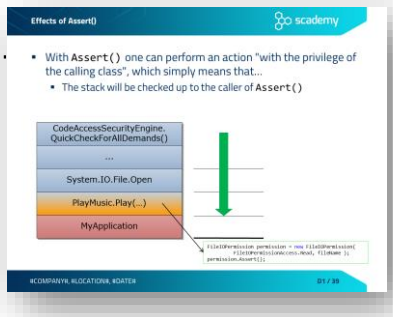
Client-side security

- JavaScript security
- Same Origin Policy
- Simple requests .....
- Preflight requests
- Clickjacking
  - Exercise – IFrame, Where is My Car?
  - Protection against Clickjacking
  - Anti frame-busting – dismissing protection scripts
  - Protection against busting frame busting
- AJAX security
  - XSS in AJAX
  - Script injection attack in AJAX
  - Exercise – XSS in AJAX
  - XSS protection in AJAX
  - Exercise CSRF in AJAX – JavaScript hijacking
  - CSRF protection in AJAX



.NET security architecture and services

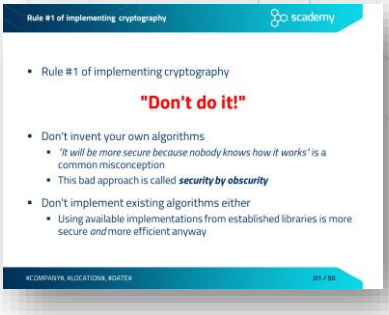
- .NET architecture
- Code Access Security
  - Full and partial trust
  - Evidence classes
  - Permissions
  - Code access permission classes
  - Deriving permissions from evidence
  - Defining custom permissions
  - .NET runtime permission checking
  - The Stack Walk
  - Effects of Assert().....
  - Class and method-level declarative permission
  - Imperative (programmatic) permission checking
  - Exercise – sandboxing .NET code
  - Using transparency attributes
  - Allow partially trusted callers
  - Exercise – using transparency attributes



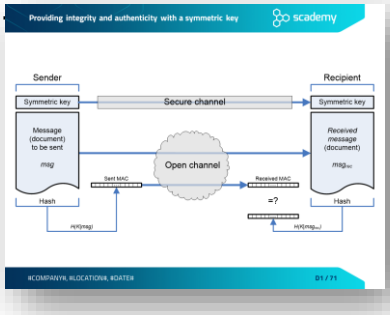
scademy
secure coding academy

Practical cryptography

- Rule #1 of implementing cryptography.....



- Cryptosystems
  - Elements of a cryptosystem
  - .NET cryptographic architecture
- Symmetric-key cryptography
  - Providing confidentiality with symmetric cryptography
  - Symmetric encryption algorithms
  - Modes of operation
  - Encrypting and decrypting (symmetric)
- Other cryptographic algorithms
  - Hash or message digest
  - Hash algorithms
  - SHAttered
  - Hashing
  - Message Authentication Code (MAC)
  - Providing integrity and authenticity with a symmetric key.....



  - Random number generation
    - Random numbers and cryptography
    - Cryptographically-strong PRNGs
    - Weak PRNGs in .NET
    - Strong PRNGS in .NET
    - Hardware-based TRNGs
- Asymmetric (public-key) cryptography
  - Providing confidentiality with public-key encryption
  - Rule of thumb – possession of private key
  - The RSA algorithm
    - Introduction to RSA algorithm
    - Encrypting with RSA
    - Combining symmetric and asymmetric algorithms
    - Digital signing with RSA
    - Asymmetric algorithms in .NET
    - Exercise Sign
    - Exercise – using .NET cryptographic classes
- Public Key Infrastructure (PKI)
  - Man-in-the-Middle (MitM) attack
  - Digital certificates against MitM attack
  - Certificate Authorities in Public Key Infrastructure
  - X.509 digital certificate