.NET Threats & Countermeasures

Hands-on Training (2 Days)

Course description

Secure programming is the best defense against hackers. This multilayered Hands on course will demonstrate live real time hacking methods , analyze the code deficiency that enabled the attack and most importantly teach how to prevent such vulnerabilities by adopting secure coding best practices in order to bullet-proof your .NET application. The methodology of the Cycle of knowledge is as follows: Understand, Identify, Prevent. This methodology presents the student with analytical tools to keep a deeper understanding of coding vulnerabilities and implement security countermeasures in different areas of the software development lifecycle. The hands on labs will enable the student to get a firsthand experience of the Hackers world and what could be done to stop him. Using sound programming techniques and best practices shown in this course, you will be able to produce high-quality code that stands up to attack. The course covers major security principles in the .NET framework, programming vulnerabilities, and specific security issues in ASP.NET web applications and Winform applications.

Trainer

Erez Metula (CISSP), Founder
Erez Metula is a world renowned application security expert, spending most of his time finding software vulnerabilities and teaching developers how they should avoid them. Erez has an extensive hands-on experience performing security assessments, code reviews and secure development trainings for worldwide organizations. He is a constant speaker at international security conferences, and the author of the book "Managed Code Rootkits".

Target audience

Members of the software development team:

- .Net Developers in ASP.NET / Windows based application
- Designers & Architects

Prequisites

Before attending this course, students should be familiar with:

- Basic Knowledge of the .NET Framework
- IIS, Databases (SQL Server) & SQL language

Each student will receive a personal DVD equipped with a LAB VM, code samples, slides, etc. **Students should bring their own laptop**, equipped with VMWare Player / Workstation equipped with 2GB of RAM and about 15GB of Disk Space for Software Installation.

Course topics

Day 1

Securing Authentication & Authorization mechanisms

Blocking Brute force attacks
Account lockout
Securing passwords
Implementing Captcha
Asp.net authentication
Client side authorization
Failure to Restrict URL Access
Insecure Direct Object Reference
Using ASP.NET File authorization
Using ASP.NET URL authorization

Performing Input Validation

Injection Flaws
OS Command Injection
Preventing SQL Injection
Using Parameterized queries to prevent SQL Injection
Stored procedures
Preventing XPATH Injection
Mitigating LDAP Injection
Using Strong typing
Blacklist VS. Whitelist validation
Regular expressions (Regex)

LAB 1

Output Encoding

Preventing HTML Injection
Understanding Cross Site Scripting (XSS) attacks
Html encode
The Anti-XSS Library
ASP.NET Request Validator

Unit: Browser Manipulation

Cross Site Request Forgery (CSRF)
Anti CSRF token
The dangers of open redirect mechanisms
Index based redirection

Exception Management

Information disclosures via errors
.NET error settings in web.config
Custom error pages
Page level error handling
Application level error handling
Error Handling strategy

LAB 2

Day 2

File Handling

Path traversal attacks
Canonicalization
Virtual path mapping using MapPath
Sanitizing file names using GetFullPath
Uploaded files backdoors
File extension handling
Directory listing

Session & Cookie Management

Client side state management
Session hijacking
Restricting cookies to SSL
Reducing cookies exposure
Reducing session lifetime
The HttpOnly option
Avoiding session fixation
ViewState integrity validation
Preventing ViewState reply attacks

LAB 3

Data Confidentiality & Integrity

Insecure communication
Secure traffic enforcement
Insecure storage
Symmetric encryption
A-Symmetric encryption
Hash functions

Digital signatures

Availability Problems

Denial of Service (DoS)
Client side DOS
Server Side DOS
Resource starvation
Quotas

Security Logging

.NET logging technologies
Events you should log
Events you should **not** log
Integration with exception management

LAB 4