.NET Web Application Security

Course ID #: 7000-009-ZZ-Z

Hours: 21

Course Content

Course Description:

Our .NET Web Application Security training course teaches students the fundamentals of web application security by allowing them to play the role of a malicious user. As this user, they perform a variety of tasks involving application profiling and penetration testing. After that, students learn about the countermeasures and best practices necessary for building secure .NET web applications.

At Course Completion:

After competing this course, student will be able to:

- Gain a familiarity with the tools and techniques used to exploit web application vulnerabilities
- Perform profiling tasks and penetration testing against a sample web application
- Learn about various forms of input injection and their associated countermeasures
- Acquire hands-on experience with configuring IIS to host secure ASP.NET web applications
- Use the cryptography classes in the .NET Framework to explore various forms of encryption and signing
- Learn about several different forms of authentication and study their advantages and drawbacks

Prerequisites:

Target Student:

Topics:

Introduction

- Business Impacts of a Cyberattack
- Industry Statistics
- Popularity Factors
- Web Application Weak Spots

Review of HTTP

- Headers
- Verbs
- State
- Requests
- Web Debugging Proxies
- Protocol Analyzers

OWASP Top Ten

- Current Top Ten List

Profiling

- Organizational Profiling
- Infrastructure Profiling
- Footprinting, Scanning, and Fingerprinting
- Application Profiling
- Anonymity
- Countermeasures

.NET Web Application Security

Course ID #: 7000-009-ZZ-Z

Hours: 21

Cryptography

- Symmetric Encryption
- Asymmetric Encryption
- Cryptographic Hash Functions
- Keyed-Hash Message Authentication Codes (HMAC)
- Digital Signatures
- Digital Certificates
- SSL, TLS, and HTTPS

Injection

- SQL Injection
- ASP.NET ViewState
- Over Posting
- Countermeasures

Authentication Fundamentals

- Credential Types
- Two Factor Authentication
- IIS Identities
- IIS Anonymous Authentication

Authentication Protocols

- HTTP Basic Authentication
- HTTP Digest Authentication
- Windows Authentication
- Client Certificate Authentication
- Forms Authentication
- Pre-Shared Key Authentication
- Token-Based Authentication

OAuth 2.0

- Roles
- Client Types
- Grant Types
- Access Token
- OpenID Connect
- IdentityServer

ASP.NET Identity

- OWIN
- Visual Studio Templates

Authorization

- NTFS Authorization
- URL-Based Authorization
- Application-Level Authorization

Application Vulnerabilities

- Session Management
- Cross-Site Scripting (XSS)
- Direct Object References
- Sensitive Data Exposure
- Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Platform Vulnerabilities
- Validating Redirects and Forwards

IIS Hardening

- Reducing Attack Surface Area
- Configuring for Least Privilege
- Handler Mappings
- ISAPI and CGI
- MIME Types
- IP Address and Domain Restrictions