Tips and Tricks To Secure .Net Web Application

Walter Wong
Gain Secure
MVP – Developer Security
walterwws.wordpress.com
walter_wws@hotmail.com
Security Updates

Operation Malaysia

http://world.yes.my/?id=511&q=ytlc
Agenda

• Introduction to ASP.Net – Security Perspective
• Securing Layers Architecture
• Secure Deployment Environment
• .Net Obfuscation
Introduction to ASP.Net – Security Perspective

• Preventing XSS input by default
• Tools ensure security level of the application
• Prevent buffer overrun by default
• Application behavior configured via web.config
Demo

Introduction to ASP.Net (Security Perspective)
Securing Layers Architecture

• Standard practice, deploy into at least 3 layers – Web Application, Business Logic, Database
• How to ensure attackers do not bypass second layer?
• Identity should be transferred across different layers
Secure Web Services

- Most of the web services available internal or externally are accepting and allowing anonymous requests
- Security Token should be used to validate the request
- Recommend to use federation to secure the web services
- Microsoft way of implement Federation – Windows Identity Foundation (WIF)
Demo
Secure WCF Services using WIF
Secure Application

- Web Application Configuration Analyzer (WACA)
- Rules based driven scanner
- 3 main categories
  - General Application
  - IIS
  - SQL
Secure Server

• Microsoft Based Security Analyzer 2.2
• Advice based on best practice for
  – Windows
  – SQL Server
  – Desktop Application
• Explanation of
  – What was scanned
  – Results
  – Recommend correction step
Demo

Web Application Configuration Analyzer 2.0
Microsoft Baseline Security Analyzer
Obfuscation

- Microsoft.Net Framework is managed framework
- Assemblies able to "reverse engineer" by using tools
- Recommend to obfuscate before deploy
Conclusion

• Users are EVIL
• Obfuscate every deployment projects
• Developers seldom involve in IT administrative tasks which is not healthy
• Learn how to secure application today
• Learn how to secure server and IIS