Security Misconfiguration

Troy Hunt

troyhunt.com

pluralsight
hardcore developer training

Outline

- How OWASP views the risk
- Performing an attack
- Configuring custom errors and tracing
- Keeping packages current with NuGet
- Encrypting sensitive data in the web.config
- Using config transforms to keep the web.config secure
- Enabling retail mode on the server

OWASP overview and risk rating

Threat Agents
—
Consider anonymous external attackers as well as users with their own accounts that may attempt to compromise the system. Also consider insiders wanting to disguise their actions.

Summary

- **Simple configuration changes can introduce serious security risks**
  - Get custom errors and tracing under control
- **Make sure you have a strategy for keep frameworks current**
  - NuGet makes package management easy
- **Protect sensitive data in the web.config**
- **Automate the security configuration of the web.config settings**
  - Use config transforms to correctly configure it during deployment
- **Consider retail mode on the server as a safety net**