## TARGET AUDIENCE:

* Web developer or web master.
* SQL developer or database administrator.
* Network administrator.
* Tester.

## BUSINESS NEEDS:

* Maintain the quality of customer health.
* Support customers and partners to deliver secure, strong, and high-availability products or services.
* By professional knowledge transferring, improve customer and partner’s reliability for Microsoft Support and Service.

## BENEFITS:

* Pre-defends threats and save costs to prevent the loss of application vulnerability for an Enterprise.
* Improves the knowledge and skills of developing secure web applications and maintain a high-level of awareness for potential threats.

## SESSION OUTLINE:

* Information Security Threats Situation and Trends.
* Security Engineering.
  + Security Essential & Modeling.
  + Microsoft Security Engineering.
    - Security Development Lifecycle (SDL) Briefing.
    - Threats Modeling.
      * Standard Threat Mitigations.
  + Security Principle.
* Frequency Security Threats.
* Threats Countermeasures Best Practice (Hands-on lab).

DELIVERABLES:

* Instructor-led classroom training.
* Hands-on labs.
* Student course material.

This workshop presents a practical and scenario-driven approach to designing and building secure ASP.NET applications. It focuses on the key elements of Threats and Security Modeling Analysis, and how to defend threats across the multi-tiers of distributed .NET Web applications. The course covers multiple aspects of improved application security, such as system design, network/hardware infrastructure, software development, application deployment, and management etc. After completion of this course, participants will be all to design secure ASP.NET web applications and implement security on the IT infrastructure and system architecture as well as improve the security of the source code.

Workshop

1 Day

Development

300

ASP.NET Web Development Security Practice