

## In-Depth Web Application Security Outline: Day One

### Outline:

The following outline provides a high-level overview of the topics covered during the Web Application Security day of training.

### The Big Picture:

- Information Security Concept Overview
- Key Fundamental Principles of Security
- Network/Host/Application Security
- “General IT” Security vs. Application Security
- Understanding Separation of Security Layers (Defense/Attack)

### Introduction To Web Application Security

- Modern Web Application Architecture
- A New Model to Manage, New Risks to Manage
- Status of Web Application Security
- Types of Web Application Vulnerabilities/Attacks (General)
- Web Application Functional Layers
- Attacking Each Functional Layer of a Web Application
- Preying on Assumptions, Un-enforced Restrictions

### Web Application Vulnerabilities

- Overview: Vulnerabilities named, Observations
- Exploring Vulnerabilities/Attacks:
  - Discuss, Explain
  - SQL Insertion
  - HTML Insertion
  - XML Insertion
  - Cross Site Scripting
  - System Command Insertion
  - Parameter Insertion
  - Parameter Manipulation and "Hidden Manipulation"
  - Cookie Manipulation and Cookie Information Disclosure
  - "Session Theft" and "Point Blank Sessions"
  - Unicode Vulnerabilities



## In-Depth Web Application Security Outline: Day One Continued

- Forced URL exploration
- Reconnaissance Attacks
- Error Handling
- Specific Known Vulnerabilities
- Categorize Design Vulnerabilities, Demonstrate:
  - Insertion Attacks, Multi-Layer
  - Information Disclosure
  - Parameter Manipulations
  - Session Attacks
- Demonstrate Testing/Attack Tools
- Discussion of Issues
  - “Gratuitous Assumptions” - Unfounded Trust of the Client
  - Parameter “Scrubbing”/Validation
  - The Challenge of Sessions, User/Entity Authentication
  - Client-side State Weakness
  - Information Disclosure, Common Mistakes
  - Other Specific Points and Discussion

## Mitigating Risk at Design and Development

- Lessons Learned
- Revisiting Attack of the Layers
- The Need for Design/Development Standards
- Discussion of the Role of Security Frameworks
- Creating Security API/Libraries
- Revisiting Security Safeguards/Standards
- The Role Web Application Security Assessments

## Final Notes

- Importance of Application Environment Security
- Understanding Web Application Security Assessments
- Resources