



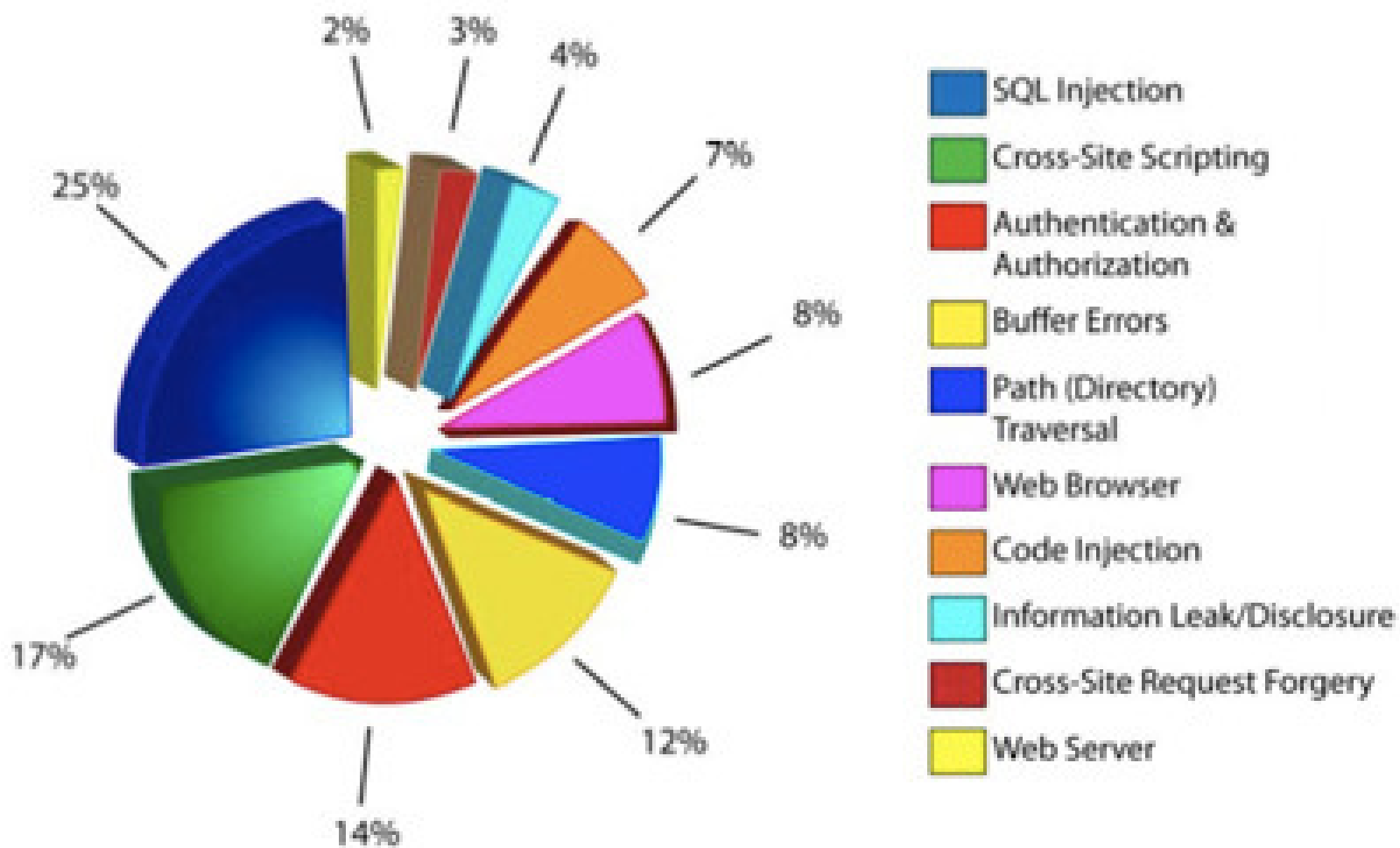
# Introduction to Web Protection Library (WPL)

Anil Chintala  
Information Security Tools  
Microsoft Corporation  
[anil.chintala@microsoft.com](mailto:anil.chintala@microsoft.com)

# OWASP Top 10 - 2007

- A1. Cross Site Scripting (XSS)
- A2. Injection Flaws
- A3. Insecure Remote File Include (NEW)
- A4. Insecure Direct Object Reference
- A5. Cross Site Request Forgery (CSRF) (NEW)
- A6. Information Leakage and Improper Error Handling
- A7. Broken Authentication and Session Management
- A8. Insecure Cryptographic Storage
- A9. Insecure Communications (NEW)
- A10. Failure to Restrict URL Access

# Top Vulnerabilities



Picture courtesy of <http://www.net-security.org/secworld.php?id=8489>.

# Comprehensive Web Application Protection

# Agenda

- **Anti-XSS Library**
- **Introduction to WPL**
  - Encoding Library
  - Security Runtime Engine
  - Configuration Engine
  - Extensibility
- **Demo**
- **Questions?**

# What is Anti-XSS Library?

- Anti-XSS is an encoding library designed to help developers protect their ASP.NET applications from XSS attacks.
- It differs from most encoding libraries in that it uses the white-listing technique to provide protection against XSS attacks.
- Anti-XSS 3.1 introduced Security Runtime Engine (SRE)

# Introduction

- Comprehensive web application protection
  - Security Runtime Engine
  - Encoding Library
- Does not require any code change
- Extensible framework for plug-ins
- Minimal Performance Impact

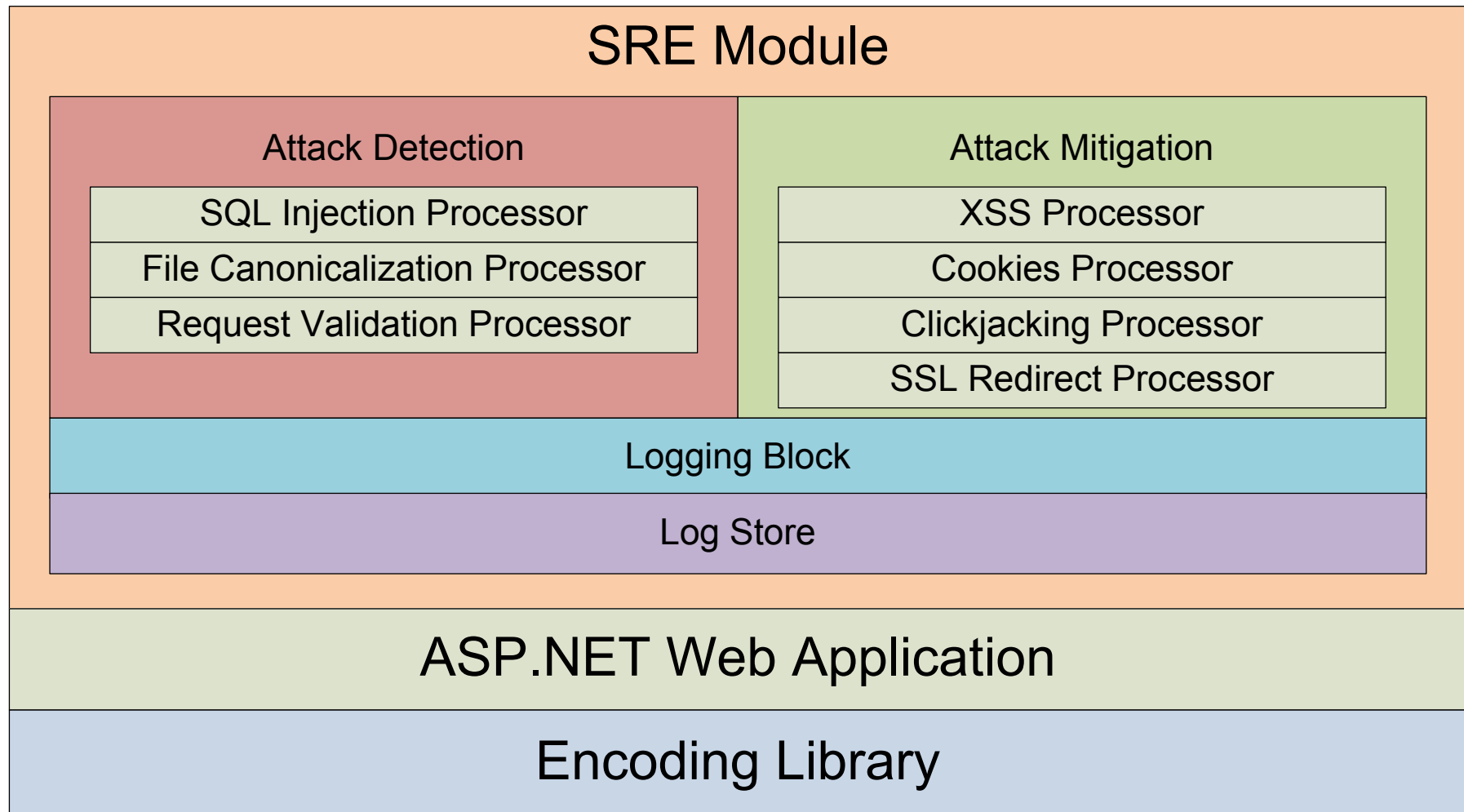
# Features

- **Encoding Library**
  - HTML Encoding
  - HTML Sanitization
  - LDAP Encoding
  - Cascading Style Sheets Encoding
- **Security Runtime Engine**
  - Centralized Logging
  - Extensive Configurable Options
  - Comprehensive Attack Protection

# Comprehensive Attack Protection

Attack Detections	Attack Mitigations
SQL Injection	Cross Site Scripting
File Canonicalization	Cookie Theft
Script Injections	Clickjacking
	Information Disclosure

# Architecture



# Demo

# Extensibility

- Abstract Classes for new processors
- Extensible Configuration Base Classes
- Configuration UI Attributes
- Asynchronous Log Writer
- Included Samples in Final Release

# Release Timeline

- **November 1<sup>st</sup> week**
  - Encoding Library Updates
  - Extensible Framework for Processors
  - XSS and SQL Injection Protection
- **February 1<sup>st</sup> Week**
  - Cookies, SSL, Clickjacking, Request Validation Processors
- **March 1<sup>st</sup> Week**
  - Help
  - Sample Code
  - File Canonicalization Processor

# Call to Action

- You can register for our program at Connect and can download the tool directly
- <https://connect.microsoft.com/Downloads/DownloadDetails.aspx?SiteID=734&DownloadID=23329> - WPL 1.0 CTP

# Other Security Tools

## ■ CAT.NET 2.0 CTP

- Ported to the Phoenix compiler infrastructure
- Shiny new configuration rules engine that look in the \*.config for common security mis-configurations
- This CTP is a command line only single-pass data flow engine and configuration rules engine.
- Will fully integrate the tool into the Code Analysis menu of Visual Studio 2010.

- <https://connect.microsoft.com/Downloads/DownloadDetails.aspx?SiteID=734&DownloadID=23328>

# Other Security Tools

## ■ WACA 1.0 CTP

- Web Application Configuration Analyzer.
- Over 100 security rules in total (many more in the final release)
- IIS / .NET / SQL Server Security Configuration
- Windows Permissions
- Generate HTML based report, export results to Excel and export findings as work items to TFS
- Scan a machine remotely (Requires WMI and Remote Registry)

- <https://connect.microsoft.com/Downloads/DownloadDetails.aspx?SiteID=734&DownloadID=23>

# Questions?

