GOTHAM
DIGITAL • SCIENCE

Protecting Vulnerable Applications with IIS7

IIS7 Overview

- Modular Design
- Two Modes of Operation
  - Integrated Mode (new)
  - Compatibility (legacy)
- Supports .NET server extensions written in C#
  - Alternative to ISAPI
  - Managed Code

Leveraging Integrated Mode

- ASP.NET Runtime Integrated with the core web server
- Unified Request Processing Pipeline
  - Exposed to both native and managed components (known as modules)
  - Native and managed modules to apply to all requests, regardless of handler

Protecting Applications on IIS7

- ASP.NET modules can be used to protect any application running on IIS
- A module participates in the processing of every request in order to monitor, change or add to it
  - .NET class that implements the ASP.NET System.Web.IHttpModule interface

IIS7 Protection Module

- Inspects and validates HTTP request data
  - onBeginRequest pipeline event
  - Cookies, URI, Query String, Post Data
- Protects HTP response data
  - OnPreSendRequestContent pipeline event
  - Cookies, Location Headers, HTML Links, HTML Form Data
  - HttpResponse.Filter

Protection Mechanisms

- URL and cookie protection
  - SHA1 HMAC of URI, Query String, Source IP, Session ID, Timestamp
- HTML form protection
  - AES Encryption
  - Includes Source IP, Session ID, Timestamp
- Custom Regular Expression Matching
- JavaScript Argument Protection

Configuration

- Minimal configuration required
  - Default Protection settings (Required)
  - Exceptions to Default (Optional)
    - Global Exceptions (Post, Cookie)
    - URI Exceptions (URI, Query String, Post, Cookie)
  - JavaScript argument protections (Optional)
  - Custom Regular Expressions (Optional)

Live Demonstration

DEMO