GOTHAM DIGITAL SCIENCE

Protecting Vulnerable Applications with IIS7

Brian Holyfield

Source Boston 2009

Agenda

- Overview
- IIS7 Integrated Mode
- IIS7 Modules
  - Request Filtering Module
  - Add-on Modules (from Microsoft)
  - Custom Modules
  - Case Study: SPF

What's new in IIS7

- Totally New Design
  - File-Based Configuration
  - Completely Modular
  - Integrated Pipeline Mode
  - Support for non-HTTP Services (WCF)

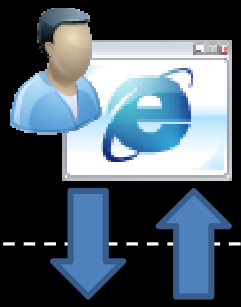
- Built-In Security Features
  - Request Filtering
  - Minimal Default Attack Surface

IIS7 Integrated Mode

- Unified Request Processing Pipeline
  - Both native and managed components (modules)
  - Modules can be applied to all requests, regardless of handler
  - ASP.NET HttpModules now comparable to ISAPI (can hook into one or more IIS7 pipeline events)

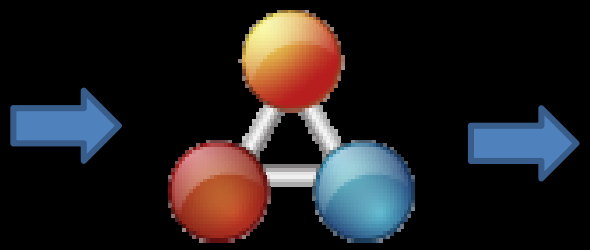
Integrated Pipeline + Modular Design = Major Extensibility!!

IIS Pipeline Events



Pre-Execution Events

- BeginRequest
- AuthenticateRequest
- PostAuthenticateRequest
- AuthorizeRequest
- PostAuthorizeRequest
- ResolveRequestCache
- PostResolveRequestCache
- MapRequestHandler
- PostMapRequestHandler
- AcquireRequestState
- PostAcquireRequestState
- PreRequestHandlerExecute



ProcessRequest
(Handler Execution)

Post-Execution Events

- PostRequestHandlerExecute
- ReleaseRequestState
- PostReleaseRequestState
- UpdateRequestCache
- PostUpdateRequestCache
- LogRequest
- PostLogRequest
- EndRequest
- PreSendRequestHeaders
- PreSendRequestContent

Case Study: Sample Application

- Battle Blog Application
  - Free Open Source Blogging Software
  - Written in Classic ASP
  - Vulnerable to numerous common security issues
    - Failure to Restrict Admin URLs
    - Cross-Site Request Forgery
    - SQL Injection
    - Information Disclosure

IIS7 Request Filtering

- Native Module (C++)
  - URLScan functionality built in to IIS7
  - Called on **BeginRequest** Event
- Effective for providing generic protection mechanism against certain attacks
  - Configurable for each application
  - Lacks granularity at the page/parameter level
  - No support for Regular Expressions

appcmd list config -section:requestFiltering

IIS7 Request Filtering

Request Filtering Directive	Description & Options
allowDoubleEscaping	Prevents Double-encoded Requests
allowHighBitCharacters	Allows or rejects all requests with non-ASCII characters
fileExtensions	Controls permitted file extensions • Uses **allowUnlisted** option to define default behavior • Exclusions can be added with allowed=true/false
requestLimits	Combines three features: • maxAllowedContentLength • maxUrl • maxQueryString
verbs	Controls request methods • Uses **allowUnlisted** option to define default behavior • Exclusions can be added with allowed=true/false
denyUrlSequences	**Does not** support Regular Expressions
hiddenSegments	Segments are folders that cannot be requested

IIS7 Add-On Modules

- The Microsoft IIS team is continually releasing new add-on modules for IIS7

- Some have potential security uses
  - Dynamic IP Restrictions
  - URL Rewrite
  - Application Request Routing

Dynamic IP Restrictions

- Dynamic IP Restrictions Extension
  - Dynamically blocking of requests from IP address based on
    - Number of concurrent requests
    - Number of requests over a period of time
  - Configurable at the Site or Server Level
  - Support for permanent static allow or deny list
    - Domain Name
    - IP Address

URL Rewriter for IIS7

- IIS7 version of mod_rewrite
  - Called on **BeginRequest** event
  - Regular expression pattern matching
  - Access to server variables and HTTP headers
  - Rule actions include redirect and request abort
- Not specifically designed for security, but can be used to block or validate certain requests

http://learn.iis.net/page.aspx/465/url-rewrite-module-configuration-reference/

Case Study: Demo

- Demo: White List URLs with Rewrite Rules
  - Only allow requests to authorized files
  - Only allow valid query string values

Request Filter vs. URL Rewrite

Request Entity	Request Filtering	URL Rewrite
Scan requested URL path	Yes (Substring)	Yes (Regex)
Check URL length	Yes	**No**
Scan query string	**No**	Yes (Regex)
Check query string length	Yes	**No**
Check HTTP verbs	Yes	Yes
Check request content length	Yes	**No**
Scan HTTP headers	**No**	Yes (Regex)
Check HTTP headers length	Yes	**No**
Scan server variables	**No**	Yes
Check IP address or host name	**No***	Yes

** The IP Restriction module in IIS 7.0 can be used for blocking requests by IP or host name*

Application Request Routing

- Similar to mod_proxy
  - Can perform HTTP based routing decisions based on HTTP request data
  - Load balancing algorithms
  - Client and hostname affinity

Custom IIS7 Modules

- With IIS7 modules, it is easy to monitor, change or add every request
- ASP.NET modules can now be used to protect any application running on IIS
  - .NET class that implements the ASP.NET **System.Web.IHttpModule** interface

Extensibility Examples

- "Enhancing Applications with the IIS7 Integrated Pipeline" -- *Mike Volodarsky - MSDN 2007*
- Used IIS7 Managed Module to enhance QDig (PHP)
  - Authentication
    - FormsAuthenticationModule
  - Search Engine Friendly URLs
    - Inbound: Server.TransferRequest
    - Outbound: Response.Filter
  - Output Caching
    - ASP.NET OutputCache

Application Security Module

- Custom module to secure outbound data and validate inbound requests
  - Request/Response Parsing
  - Data Validation
  - Input tracking & Parameter Encryption

- Defend Against Application Attacks
  - Known Bad Signatures
  - Intelligent Authorization Defense

Leveraging Response Events

- Goal
  - Only allow the user do what the application expects them to be able to do

- How
  - Analyze what is presented to the users (response)
  - If an option is not presented, don't let them use it
  - If we don't ask the user for input, don't accept it!

Secure Parameter Filter (SPF)

- **IIS Secure Parameter Filter (SPF)**
  - Protects Non-Editable Data from Manipulation
    - ASP.NET HttpModule (C#)
    - Does not require any changes to underling application
  - Response & Request Filter
    - Output Tracking
    - Request Validation
  - Free and available for download
    - http://www.gdssecurity.com/l/spf/

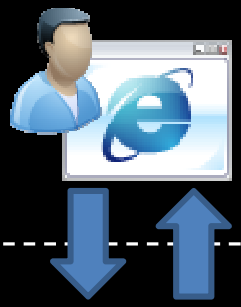
How it Works

- Response Filter
  - Analyzes HTML (HTML Agility Pack)
    - Embedded URLs
    - HTML Form Data
    - Cookies
    - JavaScript Functions
  - Tracks Form “State”
    - Editable vs. non-editable input
  - Correlates Forms & Links to each session

How it Works

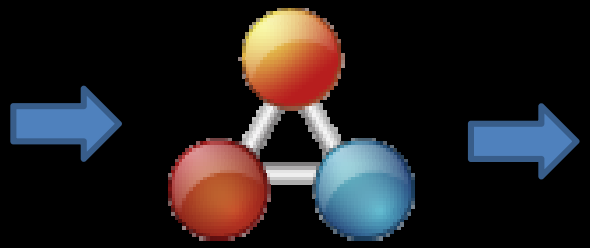
- Request Filter
  - Analyzes HTTP requests to ensure only "authorized" URLs and inputs are accepted
    - User sessions are tracked with a unique ID
  - Only configured "entry points" are permitted without authorization
  - Inspect editable-data against configurable Regular Expressions (Black List)

SPF Pipeline Events



Pre-Execution Events

- **BeginRequest**
- AuthenticateRequest
- PostAuthenticateRequest
- AuthorizeRequest
- PostAuthorizeRequest
- ResolveRequestCache
- PostResolveRequestCache
- MapRequestHandler
- PostMapRequestHandler
- AcquireRequestState
- PostAcquireRequestState
- PreRequestHandlerExecute



ProcessRequest
(Handler Execution)

Post-Execution Events

- PostRequestHandlerExecute
- **ReleaseRequestState**
- PostReleaseRequestState
- UpdateRequestCache
- PostUpdateRequestCache
- LogRequest
- PostLogRequest
- **EndRequest**
- PreSendRequestHeaders
- PreSendRequestContent

Installing a Module

- IIS7 modules can be installed in of two ways
  - Configuration file (web.config)
  - IIS7 Management Console
    - Module must be registered globally
- Custom Configuration Settings
  - Minimal Configuration
  - Configure default behavior & define exceptions to the default

Case Study: Demo

- Demo: Failure to Restrict URL Access
  - Application fails to restrict access to some administrator URLs
  - These URLs are not linked from un-authenticated pages
    - "Security through Obscurity"

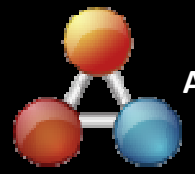
URL Access Protection

- Cryptographic “token” appended to every protected URL rendered to the user
  - Verifies integrity of Query String values
  - Verifies authorization to access page
    - Required for protected URL access

/ShowArticle.aspx?ArticleId=123

URL Access Protection

- Cryptographic “token” appended to every protected URL rendered to the user
  - Verifies integrity of Query String values
  - Verifies authorization to access page
    - Required for protected URL access



/ShowArticle.aspx?ArticleId=123&UrlToken=182734:A7A9369D50B2E185F54A

Time Stamp

URL Access Protection

- Cryptographic “token” appended to every protected URL rendered to the user
  - Verifies integrity of Query String values
  - Verifies authorization to access page
    - Required for protected URL access

/ShowArticle.aspx?ArticleId=123&UrlToken=182734:A7A9369D50B2E185F54A

**SHA1HMAC (URL + Query String +
Time Stamp + Session Cookie + Source IP)**

HMAC key derived from ASP.NET Machine Key

Case Study: Demo

- Demo: Cross-Site Request Forgery (CSRF)
  - Administrative user-management requests are vulnerable to CSRF
    - Add Users
    - Change Password
    - Elevate Privileges

CSRF Protection

- The same cryptographic “token” automatically protects against CSRF exploits
  - Tied to session cookie & source IP

/ShowArticle.aspx?ArticleId=123&UrlToken=182734:A7A9369D50B2E185F54A

SHA1HMAC (URL + Query String + Time Stamp + Session Cookie + Source IP)

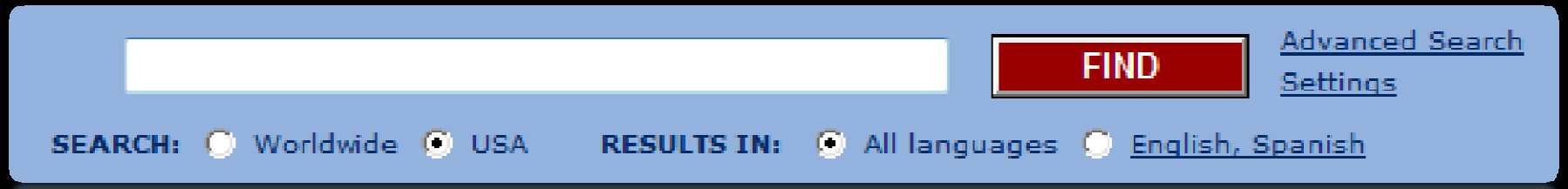
Case Study: Demo

- Demo: SQL Injection
  - Website search filter is vulnerable to SQL Injection
    - Anonymously Accessible
    - Supports POST and GET

HTML Form Protection

- Two Types of Protection
  - Form State Protection
    - Ensures each form submission includes only the correct input name & value combinations
  - Input Value Protection
    - Protects Inputs from being viewed by users
- Non-editable Form inputs cannot be altered
  - TYPE=HIDDEN | RADIO | CHECKBOX, SELECT
  - Read-Only Text Inputs

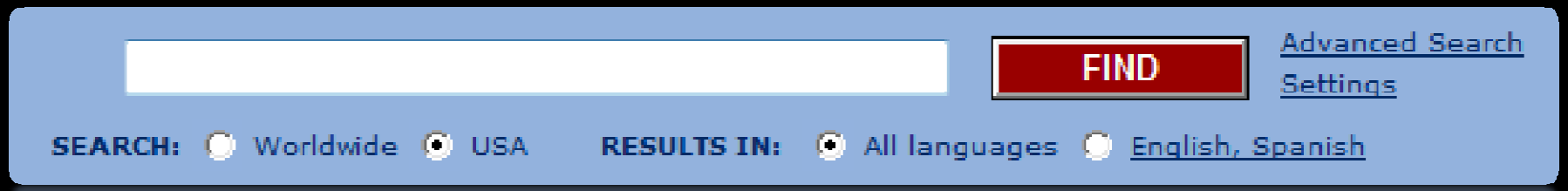
HTML Form Protection




```
<form action= "/search.aspx">
 <input type=“text" name="query">
 <input type ="submit" name="find" value="FIND">
 <input type ="hidden" name="src" value="web">
 <input type ="radio" name="scope" value="world">
 <input type ="radio" name="scope" value="us">
 <input type ="radio" name="lang" value="all">
 <input type ="radio" name="lang" value="en-sp">
</form>
```

Form State Information

HTML Form Protection

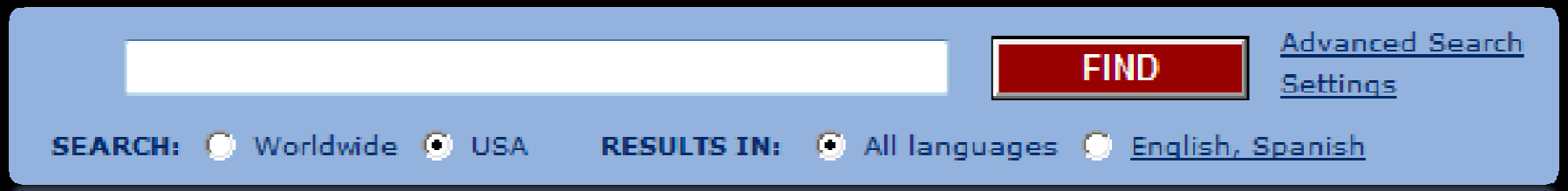



```
<form action= "/search.aspx">
 <input type="text" name="query">
 <input type ="submit" name="find" value="FIND">
 <input type ="hidden" name="src" value="web">
 <input type ="radio" name="scope" value="world">
 <input type ="radio" name="scope" value="us">
 <input type ="radio" name="lang" value="all">
 <input type ="radio" name="lang" value="en-sp">
</form>
```

Form State Information

Action: /search.aspx

HTML Form Protection

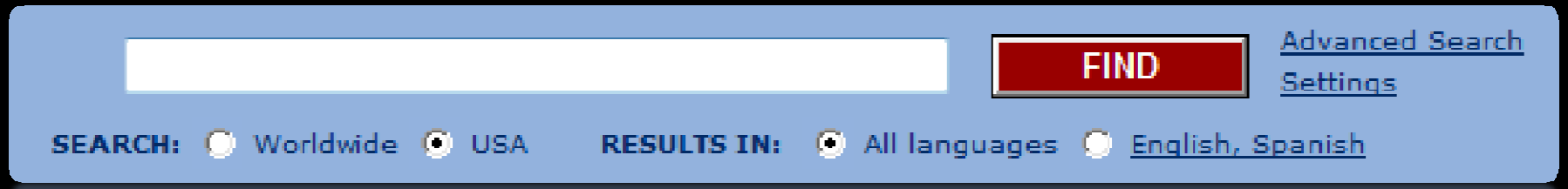



```
<form action= "/search.aspx">
 <input type="text" name="query">
 <input type ="submit" name="find" value="FIND">
 <input type ="hidden" name="src" value="web">
 <input type ="radio" name="scope" value="world">
 <input type ="radio" name="scope" value="us">
 <input type ="radio" name="lang" value="all">
 <input type ="radio" name="lang" value="en-sp">
</form>
```

Form State Information

Action: /search.aspx
Owner: 25574bb9-792d-4c4b-9873-c9fae1631485
(Session Cookie)

HTML Form Protection

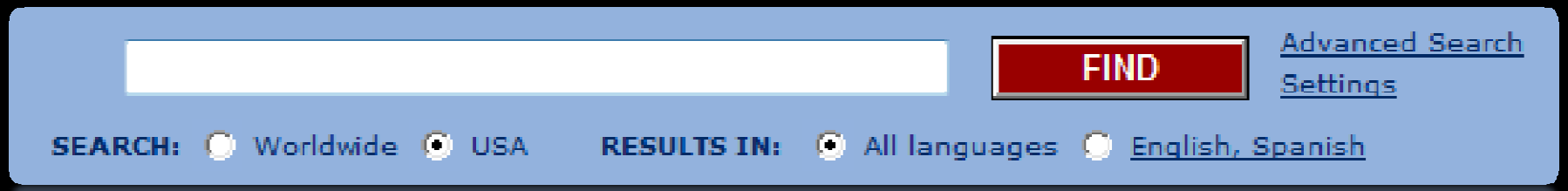



```
<form action= "/search.aspx">
 <input type ="hidden" name="FormToken"  value=
 "3F2504E0-4F89-11D3-9A0C-0305E82C3301">
 <input type=“text" name="query">
 <input type ="submit" name="find" value="FIND">
 <input type ="hidden" name="src" value="web">
 <input type ="radio" name="scope" value="world">
 <input type ="radio" name="scope" value="us">
 <input type ="radio" name="lang" value="all">
 <input type ="radio" name="lang" value="en-sp">
</form>
```

Form State Information

Action: /search.aspx
Owner: 25574bb9-792d-4c4b-9873-c9fae1631485
Form-Id: 3F2504E0-4F89-11D3-9A0C-0305E82C3301 (New GUID)

HTML Form Protection



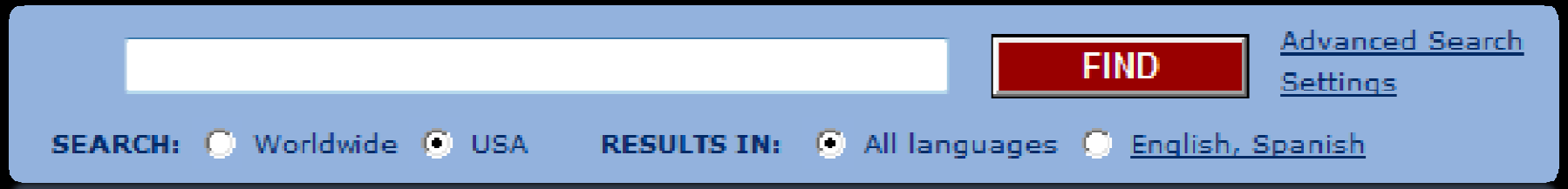

```
<form action= "/search.aspx">
 <input type ="hidden" name="FormToken"  value=
 "3F2504E0-4F89-11D3-9A0C-0305E82C3301">
 <input type=“text" name="query">
 <input type ="submit" name="find" value="FIND">
 <input type ="hidden" name="src" value="web">
 <input type ="radio" name="scope" value="world">
 <input type ="radio" name="scope" value="us">
 <input type ="radio" name="lang" value="all">
 <input type ="radio" name="lang" value="en-sp">
</form>
```

Form State Information

Action: /search.aspx
Owner: 25574bb9-792d-4c4b-9873-c9fae1631485
Form-Id: 3F2504E0-4F89-11D3-9A0C-0305E82C3301

Input Name	Editable	Value
query	Y	-
find	N	{ FIND }
src	N	{ web }
scope	N	{ world , us }
lang	N	{ all , en-sp }

HTML Form Protection




```
<form action= "/search.aspx">
 <input type ="hidden" name="FormToken"  value=
 "3F2504E0-4F89-11D3-9A0C-0305E82C3301">
 <input type="text" name="query">
 <input type ="submit" name="find" value="1">
 <input type ="hidden" name="src" value=" 1">
 <input type ="radio" name="scope" value=" 1">
 <input type ="radio" name="scope" value="2">
 <input type ="radio" name="lang" value="1">
 <input type ="radio" name="lang" value="2">
</form>
```

Form State Information

Action: /search.aspx
Owner: 25574bb9-792d-4c4b-9873-c9fae1631485
Form-Id: 3F2504E0-4F89-11D3-9A0C-0305E82C3301

Input Name	Editable	Value
query	Y	-
find	N	{ FIND }
src	N	{ web }
scope	N	{ world , us }
lang	N	{ all , en-sp }

Case Study: Demo

- Demo: Information Disclosure
  - The comment submission CAPTCHA value is disclosed within a hidden HTML form field

JavaScript Protection

- Quoted string assignment to common JavaScript property values are treated as URLs (UrlToken)
  - window.location
  - location.href
- JS Functions can also be defined for protection
  - Function Name & Arguments
    - Protect (Y/N)
    - URL / Form Input
      - INPUT NAME
      - TARGET URL

JavaScript Protection

- Example JavaScript Function

```
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
```

JavaScript Protection

- Example JavaScript Function

```
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
```

JavaScript Protection

- Example JavaScript Function

```
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
```

JavaScript Protection

- Example JavaScript Function

```
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
```

JavaScript Protection

- Protecting this function with SPF

```
<scriptProtection functionName="__doPostBack">
  <functionArguments>
    <add argumentName="eventTarget" protect="true"
     targetName="__EVENTTARGET" />
    <add argumentName="eventArgument" protect="true"
     targetName="__EVENTARGUMENT" />
  </functionArguments>
</scriptProtection>
```

JavaScript Protection

```
<a href="javascript:__doPostBack('ctl00$MainContent$gvwThreads'
,'Sort$LastPostDate')">
```

```
<a href="javascript:__doPostBack('b/xEVUeEDOCnhiKu0jS5USUs6N
4Qu1VH5OqHOwF146wSPlA87g==:1829384:61D26FD0849FF93D67B8489CF
A76','b/xEVUeEDOBfdZR3UM0Ds212HDDwHY3KoYyc/+/JULiDcjQ=:1829384:
83BF9D18B5C34CE2FC0541F954C093B43F0C3EA5')">
```

JavaScript Protection

```
<a href="javascript:__doPostBack('ctl00$MainContent$gvwThreads'
,'Sort$LastPostDate')">
```

```
<a href="javascript:__doPostBack('b/xEVUeEDOCnhiKu0jS5USUs6N
4Qu1VH5OqHOwF146wSPlA87g==:1829384:61D26FD0849FF93D67B8489CF
A76','b/xEVUeEDOBfdZR3UM0Ds212HDDwHY3KoYyc/+/JULiDcjQ=:1829384:
83BF9D18B5C34CE2FC0541F954C093B43F0C3EA5')">
```

BASE64(ENCRYPT(Random 8 Bytes + Argument Value))

- ASP.NET Machine Key
- AES by default in ASP.NET 2.0 (configurable)
- RNGCryptoServiceProvider for Random Bytes

JavaScript Protection

```
<a href="javascript:__doPostBack('ctl00$MainContent$gvwThreads'
,'Sort$LastPostDate')">
```

```
<a href="javascript:__doPostBack('b/xEVUeEDOCnhiKu0jS5USUs6N
4Qu1VH5OqHOwF146wSPlA87g==:1829384:61D26FD0849FF93D67B8489CF
A76','b/xEVUeEDOBfdZR3UM0Ds212HDDwHY3KoYyc/+/JULiDcjQ=:1829384:
83BF9D18B5C34CE2FC0541F954C093B43F0C3EA5')">
```

Time Stamp

JavaScript Protection

<a href="javascript:__doPostBack('ctl00$MainContent$gvwThreads'
,'Sort$LastPostDate')">

<a href="javascript:__doPostBack('b/xEVUeEDOCnhiKu0jS5USUs6N
4Qu1VH5OqHOwF146wSPlA87g==:1829384:61D26FD0849FF93D67B8489CF
A76','b/xEVUeEDOBfdZR3UM0Ds212HDDwHY3KoYyc/+/JULiDcjQ=:1829384:
83BF9D18B5C34CE2FC0541F954C093B43F0C3EA5')">

SHA1HMAC (CipherText + Time Stamp + GUID Cookie +
Source IP + [Input Name] + [Target URL])

Configuring SPF

- Minimal Configuration (Exception Based)
  - Default Protection Settings (Required)
    - Protection Scope (URI, QueryStrings, Forms, Cookies)
    - Main Application Entry Point (URL)
  - Exceptions to Default Settings (Optional)
    - Global Exceptions (Form Inputs, Cookies)
    - URI Exceptions (URI, Query String, Form Inputs)
  - Several alternate configuration options
    - Send state information to client (encrypted)
    - Active vs. Passive mode
    - BlackList Regexes

OWASP Top 10 Coverage

A1 - Cross Site Scripting (XSS)

- Request tokens should thwart reflected XSS exploits

A2 - Injection Flaws

A3 - Malicious File Execution

A4 - Insecure Direct Object Reference

A5 - Cross Site Request Forgery (CSRF)

- Request tokens provide CSRF protection

A6 - Information Leakage and Improper Error Handling

- Input protection can mitigate information leakage through application inputs (hidden fields, cookies, etc)

OWASP Top 10 Coverage

A7 - Broken Authentication & Session Management

- Cookie protection will mitigate weak/predictable session IDs

A8 - Insecure Cryptographic Storage

A9 - Insecure Communications

A10 - Failure to Restrict URL Access

- Request tokens prevent forced browsing

Conclusion

- IIS7 is now more extensible than ever
  - Modules in native or managed code

- Vulnerable legacy apps can be secured on IIS7 infrastructure
  - Built-in Features
  - Add-On Modules
  - Custom Modules

Questions?

- GDS Blog
  - **http://www.gdssecurity.com/l/b**
- SPF Download Page
  - **http://www.gdssecurity.com/l/spf**
- SPF Demo Site (.NET StockTrader)
  - **http://trade-spf.gdsdemo.com**
- Official Microsoft IIS Site
  - **http://www.iis.net**