

# **IIS Secure Parameter Filter (SPF)**



# Secure Parameter Filter (SPF)

- What is SPF?
  - Embedded application “Security Filter”
  - Analyses incoming requests and outgoing responses
  - Every URL and input value requires a security token
    - Generated on-the-fly as pages are rendered
    - Exceptions can be defined for certain pages/inputs
  - Deployed at the application level
    - No involvement from server administrator required



# Secure Parameter Filter (SPF)

- Designed to protect against:
  - **Input Tampering & Injection**  
Query String, Cookies, Form Inputs
  - **URI Tampering**  
Forced Browsing
  - **Forgery, Hijacking / Cross-Site Attacks**  
Session-Based Tokenization



# How it Works

- Output Filter
  - Analyzes HTTP output to determine what is presented
  - Only URLs and inputs presented to the user are permitted on subsequent requests
    - Append Cryptographic Token on each URL
      - Link HREF, Form ACTION, Frame SRC
    - Insert unique GUID on each form and record form input profile (name, type, disabled/read-only)
    - Encrypt eligible embedded Form input values
      - ASP.NET Machine Key

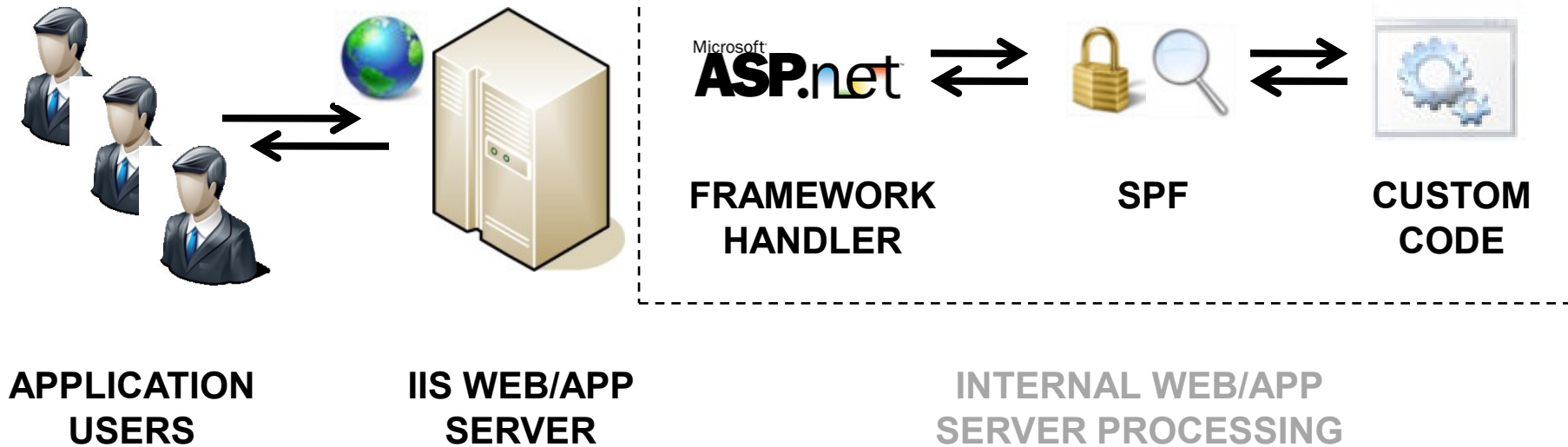


# How it Works

- Input Filter
  - Analyzes HTTP request to ensure it is for only authorized URLs and inputs
  - By default, only pre-determined “entry points” are permitted without a proper request token
  - Inspect free-form text inputs against specified regular expressions (optional)



# How it Works





# Applied Cryptography in SPF

- Encrypted Inputs
  - 16 Random Bytes Pre-Pended to Each Value
    - Produces Unique Cipher Text (similar to IV)
  - Uses ASP.NET Machine Key to Encrypt
  - Appends Time Stamp & SHA1 HMAC of:
    - Cipher Text
    - Time Stamp
    - Source IP Address
    - Source GUID (SPF Cookie)



# Applied Cryptography in SPF

- Tokenized Elements
  - Appends Time Stamp & SHA1 HMAC of:
    - Plain-Text (URL, Query String)
    - Time Stamp
    - Source IP Address
    - Source GUID (SPF Cookie)



# Configuration Requirements

- Default Protection Settings (Required)
  - Protection Scope (URI, QueryString, Forms, Cookies)
  - Main Application Entry Point (URL)
- Exceptions to Default Settings (Optional)
  - Global Exceptions (Form Inputs, Cookies)
  - URI Exceptions (URI, Query String, Form Inputs)



# Configuration Options

- Automatic Run-time Configuration Updates
  - Ineligible inputs are automatically granted exceptions
    - INPUT TYPE=TEXT, TEXAREA, etc
- “Black List” Regular Expression Filter
  - Used to optionally block malicious input strings
- Two Modes of Operation
  - Passive: Silent logging of all failed requests
  - Active: Failed requests are rejected



# Supported Content Types

- HTML Analyzer
  - Uses HTML Agility Pack
- JavaScript Analyzer
  - Custom functions with arguments that include URLs and request parameters
    - `__doPostBack(eventTarget, eventArgument)`
  - Native properties that contain URLs
    - `location.href`, `window.location`, etc



# Questions

- GDS Website:
  - <http://www.gdssecurity.com>
- GDS Blog:
  - <http://www.gdssecurity.com/l/b>
- SPF Website:
  - <http://www.gdssecurity.com/l/spf.php>