

Ecyware GreenBlue Inspector

Guía de usuario
Versión 1.0

Tabla de contenido

| | |
|---|-----------|
| TABLA DE CONTENIDO | 2 |
| INTRODUCCIÓN | 4 |
| CARACTERÍSTICAS | 5 |
| ECYWARE GREENBLUE INSPECTOR INICIO | 7 |
| NAVEGANDO HACIA UN RECURSO WEB | 9 |
| ANALIZANDO LOS RESULTADOS DE LLAMADA (REQUEST) | 9 |
| Usando los paneles | 9 |
| Usando el Editor de Formularios (Forms Editor) | 11 |
| Usando el Editor de Consultas HTML (Html Query Editor) | 13 |
| APLICANDO PRUEBAS A UN RECURSO WEB | 14 |
| Usando el panel de Pruebas Rápidas (Quick Tests) | 14 |
| Usando el Panel de Galletas (Cookies) | 14 |
| Usando el HTTP Request Header | 15 |
| Usando el Editor de Formularios (Forms Editor) | 15 |
| USANDO UNA SESIÓN PARA PROBAR UNA APLICACIÓN WEB | 16 |
| Grabando una sesión | 16 |
| Guardando una sesión | 16 |
| Abriendo una sesión | 17 |
| Vista de información general de sesión | 17 |
| Vista general de información de Session Request | 19 |
| Diseñador de formulario posteado | 20 |
| Diseñador de Post Data | 21 |
| Editor de galletas | 22 |
| Administrador de Pruebas de Unidad Web (Web Unit Tests Manager) | 23 |
| Eliminar un session request | 24 |

| | |
|---|-----------|
| Corriendo una sesión | 25 |
| REPORTES | 26 |
| Usando el dialogo de Vista previa de Reporte | 26 |
| Análisis del reporte | 27 |
| Reporte Básico | 27 |
| Reporte Avanzado | 27 |
| Guardar un reporte | 29 |
| Abrir un reporte | 29 |
| Imprimir un reporte | 29 |
| Plantillas de reporte | 29 |
| GREENBLUE INSPECTOR CONFIGURATION FILE | 30 |

Introducción

Ecyware GreenBlue Inspector es un ambiente integrado de analizador web que ofrece diferentes opciones de probar sus aplicaciones web. Uno puede probar los siguientes puntos usando Ecyware GreenBlue Inspector, tal como se define en la lista de pruebas de penetración para aplicaciones web de OWASP:

- Denegación de servicios de aplicaciones
- Controles de acceso
- Autenticación
 - Usuario
 - Administración de sesiones
- Administración de configuración*
 - Infraestructura*
 - Aplicación*
- Manejo de errores
- Protección de datos
 - Transporte*
- Validación de entrada
 - Inyección de SQL
 - Sistema Operativo*
 - LDAP*
 - XSS (Cross Site Scripting)
- Limpieza de salida
- Sobrecarga de datos (Buffer Overflow)

* Prueba que no esta disponible o no ha sido probada aun.

Características

Ecyware GreenBlue Inspector incluye algunas características únicas:

Control de navegador (browser) integrado

Use el control de browser para navegar como si estuviera usando su navegador favorito. Esto permite navegar fácilmente su aplicación y de este modo, tener una mejor experiencia visual.

Navegador HTML de texto enriquecido

El navegador de texto enriquecido de HTML le permite investigar e inspeccionar el código HTML de una página.

Manipulación de encabezados de request (Request Header)

Los encabezados de request pueden ser manipulados usando el panel de "HTTP Request Header". Usted también puede definir los valores predefinidos de los encabezados en el archivo de configuración de la aplicación.

Dialogo de editor de galletas (Cookies)

Las galletas pueden ser manipuladas en el panel de "Cookies". Solo haga doble clic y el Dialogo de Editor de Galletas se mostrara, donde podrá editar las galletas de un llamada (request).

Sitios recientes

Despliega una lista de sitios navegados.

Panel de pruebas rápidas

Contiene tres tipos de pruebas que pueden ser ejecutadas al enviar dentro del control de browser o usando el Editor de Formularios.

Editor de Formularios

Despliega los formularios contenidos dentro de una página web. Usted puede manipular cada valor del formulario y probar por medio un envío GET o POST.

Editor de consulta HTML

Una herramienta avanzada que permite hacer consultas XPath al código HTML, permitiendo al usuario analizar detalladamente una página web.

Autenticación básica

Un dialogo donde ingresa el nombre de usuario y contraseña para sitios web que usen seguridad de autenticación básica.

Grabación de sesión

Ecyware GreenBlue Inspector tiene la habilidad de grabar una sesión. Al terminar, un diseñador de sesión es abierto, donde usted puede cambiar la mayoría de propiedades de cada "Session Request". Estas propiedades incluyen pruebas de unidad web, manipulación de datos, manipulación de galletas y manipulación de encabezados.

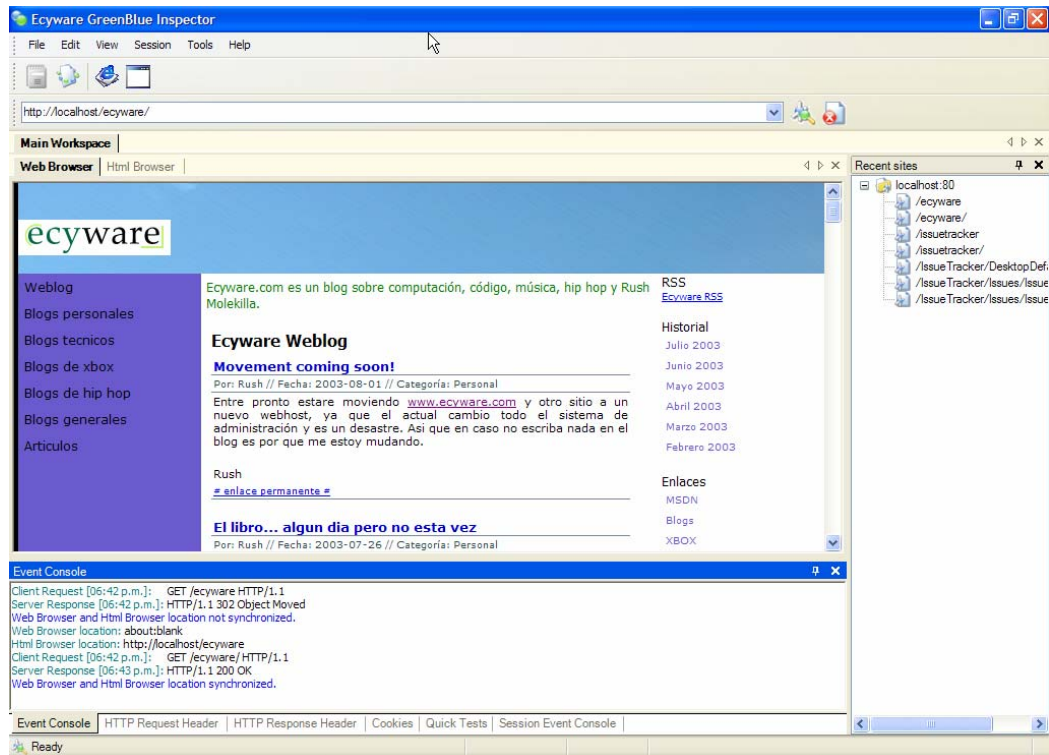
Reportes

Hay dos tipos de reportes, Reporte básico y avanzado. También existe un reporte XML para los que necesiten integrar esto a sus sistemas informáticos internos.

Error de aplicación

Los errores de aplicación son reportados por medio de la bitácora de Windows, la Consola de Eventos (Event Console) de la aplicación o por medio de ventanas de mensajes.

Ecyware GreenBlue Inspector Inicio



Menú

El menú consta de las siguientes opciones: File, Edit, View, Session, Tools y Help.

Barra de herramienta

La barra de herramientas contiene los siguientes botones:

- **Report Preview (Vista previa de reporte):** Genera una vista previa del reporte.
- **Record Session (Grabar sesión):** Inicia o detiene una grabación de sesión.
- **Allow Browser Navigate First (Permite al browser navegar primero):** Este botón es útil en sitios donde la página de login solo permite una llamada concurrente a la vez.
- **Block popups (Bloqueador de popups):** Bloquea cualquier nueva ventana de browser.
- **Address bar (Barra de dirección):** Entrada para el url a navegar.
- **Go button (Ir):** Ejecuta la navegación.
- **Stop (Alto):** Detiene la navegación.

Espacio de trabajos (Workspaces)

Solo hay un espacio de trabajo: Main Workspace. Versiones subsiguientes podrían tener más espacios de trabajo.

Espacio de trabajo principal (Main workspace)

Contiene una de estas ventanas:

- Web Browser (Navegador Web)
- Html Browser (Navegador HTML)
- Query Editor (Editor de consultas)
- Forms Editor (Editor de formularios)
- Session Designer (Diseñador de sesión)
- Report Preview (Vista previa de reporte)

Paneles (Panels)

Contiene los siguientes paneles:

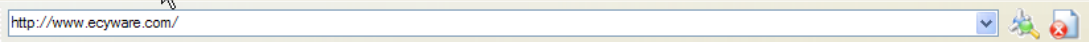
- **Event Console:** Despliega los eventos de la aplicación.
- **HTTP Request Header:** Este panel contiene una malla (grid) editable para los encabezados de request.
- **HTTP Response Header:** Este panel contiene un listado que despliega los headers de response.
- **Cookies:** Los cookies de request.
- **Quick Tests:** La consola de pruebas rápidas.
- **Session Event Console:** Despliega los eventos para una corrida de sesión.

Sitios recientes

Contiene los sitios navegados.

Navegando hacia un recurso web

1. Ingrese el web a llamar.
2. Haga clic en el botón de Go.
3. Espere hasta que la barra de progreso haya terminado. Es importante dejar que la aplicación termine de bajar todos los recursos.
4. Para detener la navegación actual, puede hacer clic en el botón de Stop.



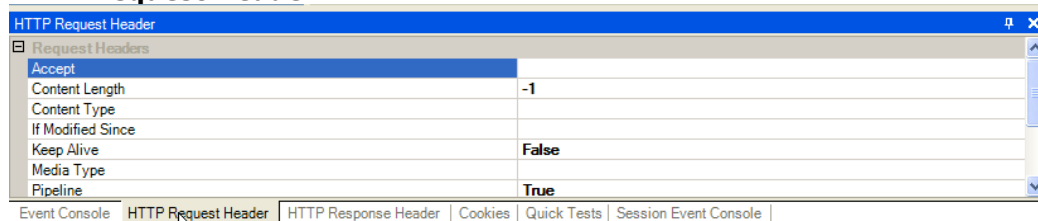
Analizando los resultados de llamada (Request)

Cuando una llamada a un recurso web es completada, uno puede continuar haciendo más llamadas o simplemente analizar los resultados.

Usando los paneles

En los paneles, uno puede analizar por medio de los paneles de Event Console, HTTP Request Header, HTTP Response Header y Cookies.

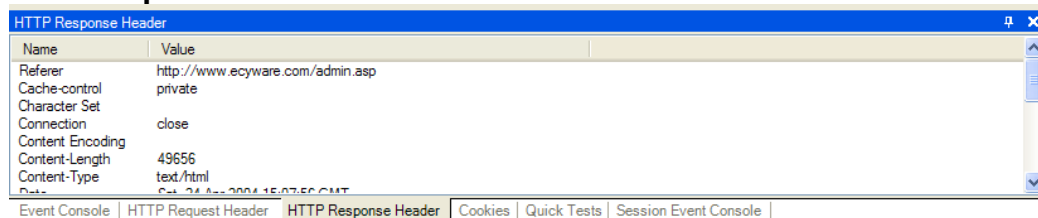
HTTP Request Header



El panel de HTTP Request Header es usado tanto en la acción de llamada (request) como la de respuesta (response). Antes de cada llamada sea hecha, la aplicación carga la configuración predeterminada en el panel de HTTP Request Header. Esta configuración puede ser cambiada y será aplicada en la próxima llamada.

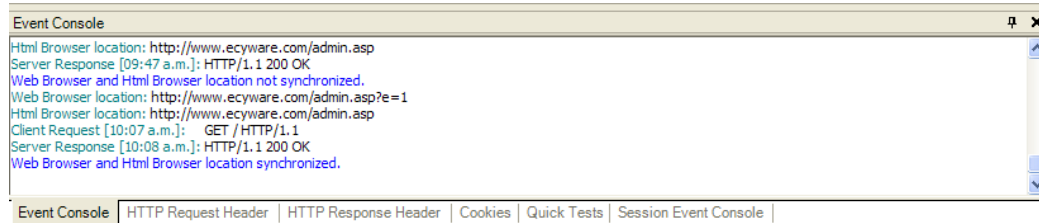
Cuando la llamada es hecha, el resultado de la llamada contiene ciertos headers (no todos) que actualizan el panel. La mayoría del tiempo, el campo actualizado será el valor del Referer.

HTTP Response Header



El panel de HTTP Response Header es usado cuando la llamada es completada. Despliega los headers retornados por el servidor.

Event Console



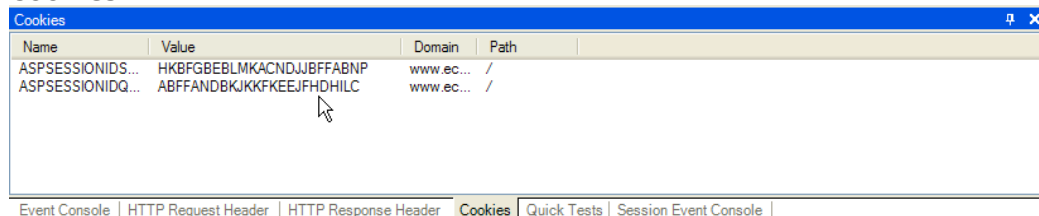
El panel de Event Console despliega las llamadas de la aplicación, respuestas del servidor, errores de la aplicación, errores de parseo (parsing) y advertencias de sincronización.

Los errores de aplicación son esos que ocurren cuando una conexión es cancelada, cuando no hay conexión de red u otras causas. También muestra errores relacionados al Diseñador de Sesión (Session Designer), apertura de archivos y otros.

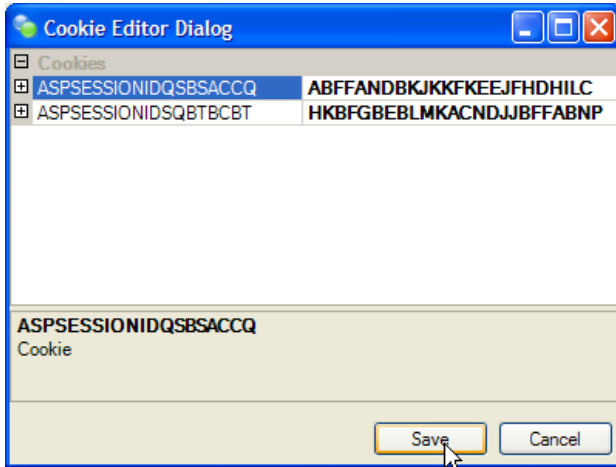
Los errores de parseo son esos relacionados al Editor de Consultas (HTML Query Editor) o el Editor de Formularios (Forms Editor).

Una advertencia de sincronización muestra cuando el Web Browser y el HTML Browser están sincronizados o no. Esto es importante, porque hay situaciones cuando el navegador ha sido reenviado, mientras que el navegador de HTML todavía se encuentra en la página anterior. La mayoría de las veces, la aplicación es capaz de detectar y navegar a la página correcta. Para corregir una advertencia de sincronización, vaya al Event Console, copie el url de localización del Web Browser en la barra de dirección (si es aplicable, por ejemplo <http://www.ecyware.com> en vez de about:blank) y haga clic en el botón de Go.

Cookies



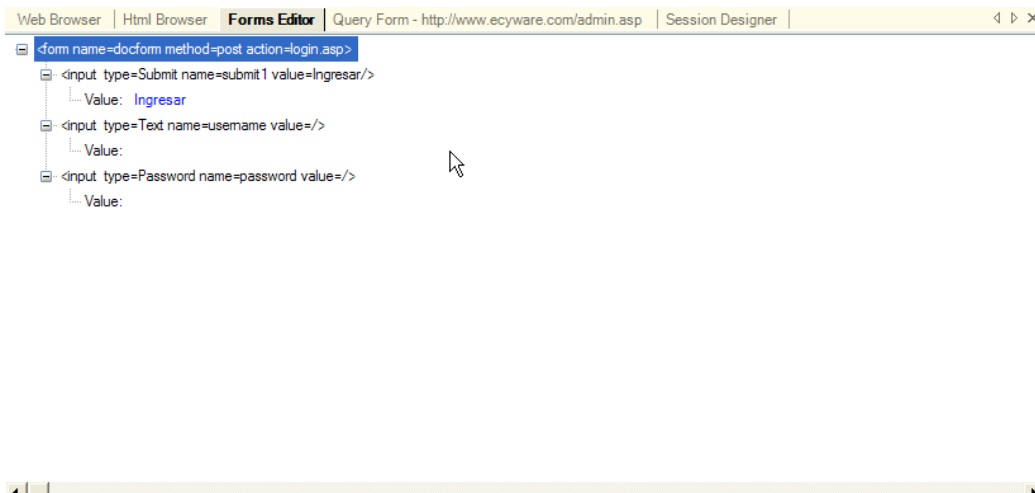
Este panel contiene las galletas encontradas en la llamada. Haga doble clic en el panel para desplegar el dialogo de Editor de Galletas (Cookie Editor Dialog).



| | |
|-----------|---|
| Comment | |
| Discard | False |
| Domain | localhost |
| Expired | False |
| Expires | |
| Path | / |
| Port | |
| Secure | False |
| Timestamp | 4/22/2004 07:35 p.m. |
| Value | 5371A0AED676DE8FACDAF8D27DF4A69EBE5453EF |
| Version | 0 |

Los valores pueden ser editados tal como están y serán actualizados en la próxima llamada.

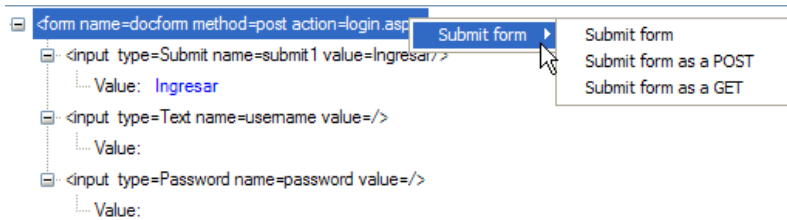
Usando el Editor de Formularios (Forms Editor)



Otra forma de análisis disponible es usando el Editor de Formularios. Este editor es generado automáticamente para cada página que contenga formularios.

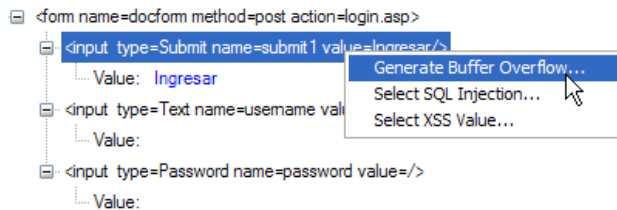
En el Editor de Formularios, los valores pueden ser cambiados y editados. Las opciones son desplegadas por medio del botón derecho del ratón.

Si hace clic derecho en el padre de un formulario, uno tiene la opción de enviar un formulario. Uno puede ya sea enviar el formulario predeterminadamente o forzar a enviar el formulario como un método HTTP GET o POST.



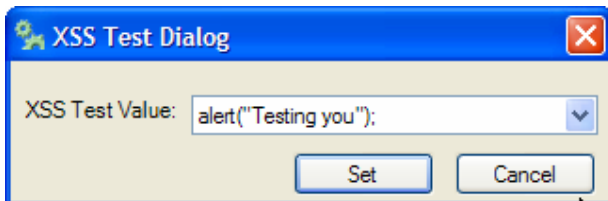
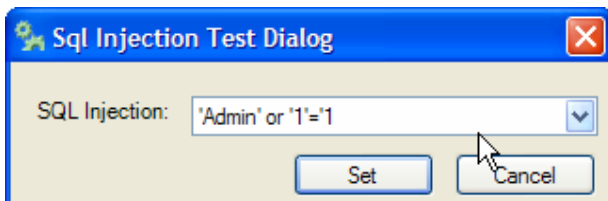
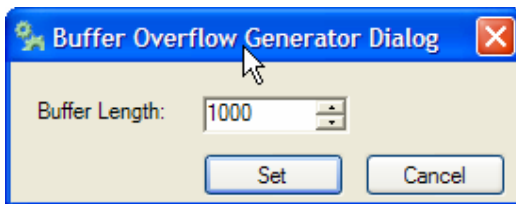
Un elemento de formulario puede ser editado manualmente o usando el botón derecho del ratón para mostrar las opciones de generar pruebas.

Para generar una prueba rápida para un elemento de formulario, seleccione el nodo de elemento de formulario (no el nodo de Value) y haga clic derecho.



Las pruebas rápidas disponibles son:

- Generar Buffer Overflow (Generate Buffer Overflow)
- Seleccionar inyección SQL (Select SQL Injection)
- Seleccionar valor XSS (Select XSS Value)



El Editor de Formularios puede ser usado para con la opción de grabar sesión por grabar enviado de formularios. Esto puede ser útil para los formularios GET, los cuales no son automáticamente guardados en la grabación de sesión.

Usando el Editor de Consultas HTML (Html Query Editor)



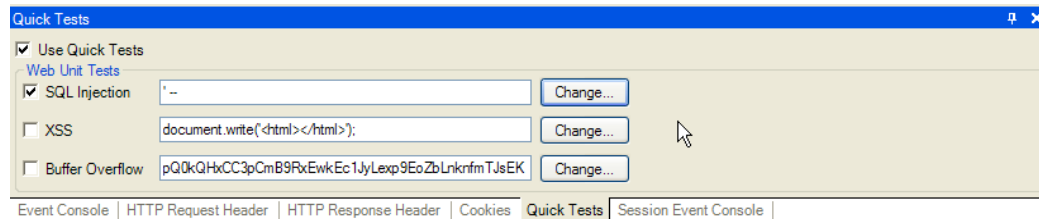
El Editor de Consultas HTML es para usuarios avanzados que tiene conocimientos de XPath. Las consultas más básicas son incluidas y son útiles para parsear código fuente HTML.

Como usar

1. Vaya el menú de Tools y seleccione Html Query Editor.
2. Seleccione cualquier consulta o ingrese una consulta nueva. Entonces haga clic en Filter.
3. El editor de texto mostrara los resultados parseados.

Aplicando pruebas a un recurso web

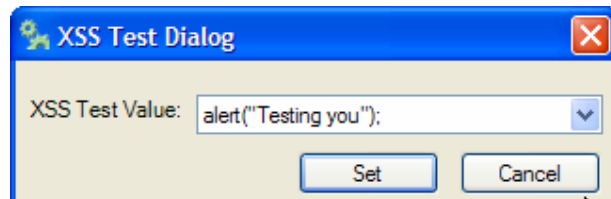
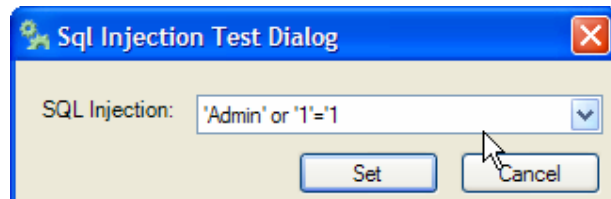
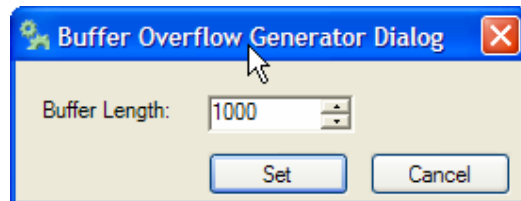
Usando el panel de Pruebas Rápidas (Quick Tests)



Las pruebas rápidas son aplicadas cuando uno envía una página ya sea desde el Web Browser o desde el Editor de Formularios.

Para usarlas, haga clic en el checkbox de **Use Quick Tests** y al menos un check en una de las pruebas.

Para cambiar el valor predeterminado, haga clic en el botón de Change. Un dialogo muestra donde uno puede seleccionar o generar los valores para usar.



Los resultados de las pruebas rápidas pueden ser accedidos desde el botón de Report Preview.

Usando el Panel de Galletas (Cookies)

Para mayor información sobre el Panel de Galletas, vaya a la página 10.

Usando el HTTP Request Header

Para mayor información sobre el Panel de HTTP Request Header, vaya a la página 9.

Usando el Editor de Formularios (Forms Editor)

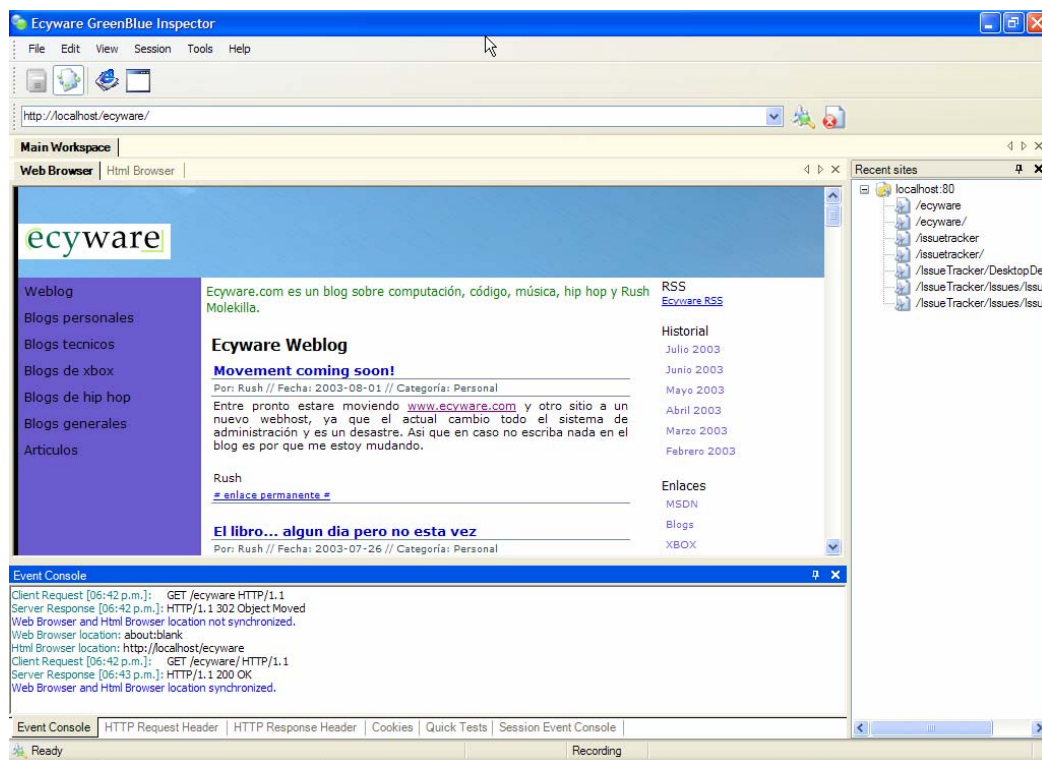
Para mayor información sobre el Panel de Editor de Formularios, vaya a la página 11.

Usando una sesión para probar una aplicación web

Una sesión de GreenBlue Inspector contiene la grabación de un flujo de trabajo de "session requests". Esta sesión puede ser usada para automatizar pruebas de unidad de web (web unit tests) y facilitan el trabajo de pruebas de aplicaciones web.

Grabando una sesión

Para iniciar una grabación, haga clic en el botón de Record Session (Grabar Sesión). La barra de estatus mostrara el mensaje de "Recording" cuando este disponible. Para detener la grabación, haga clic nuevamente en el botón de Record Session.

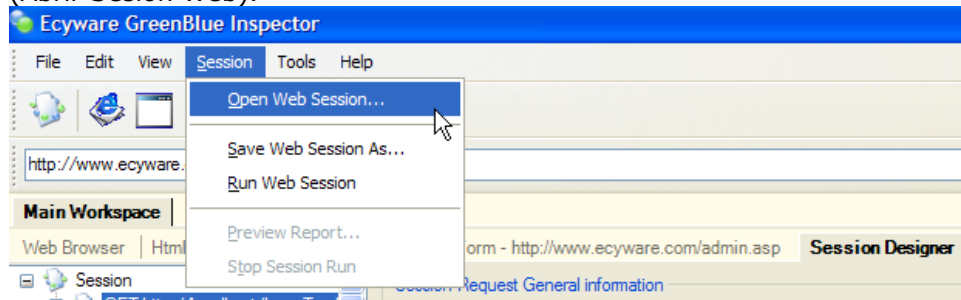


Guardando una sesión

Después de hacer clic en detener, si hay alguna llamada grabada, el Diseñador de Sesión (Session Designer) es desplegado. Para guardar la sesión, vaya al menú de Session y seleccione Save Web Session (Guardar Sesión Web).

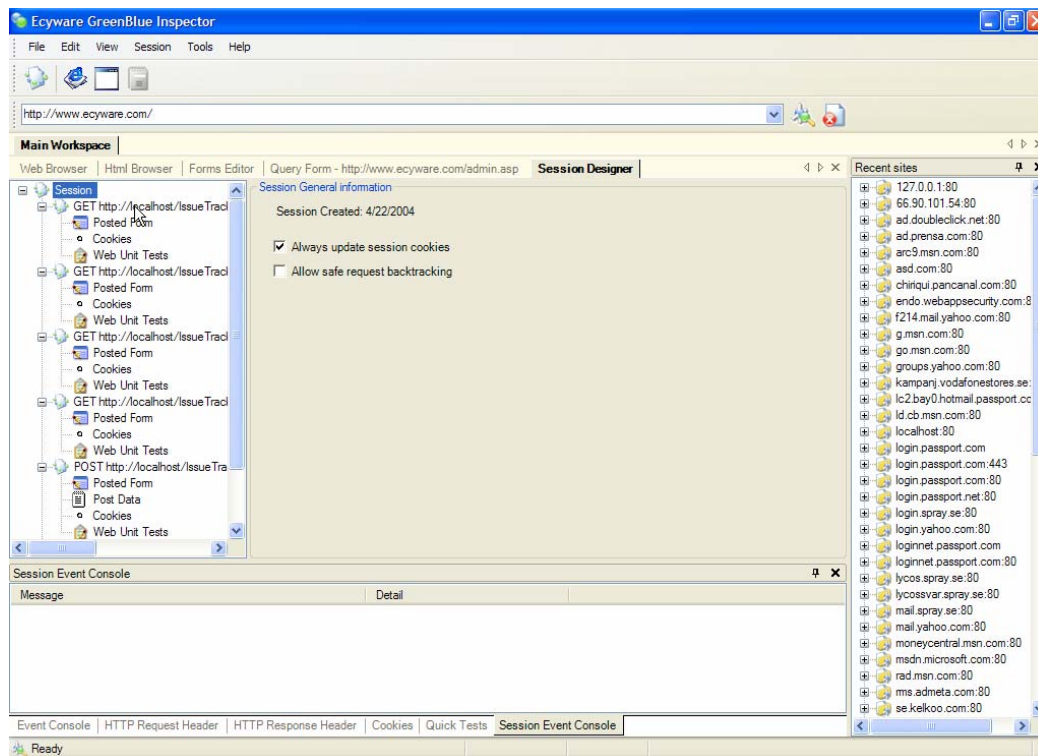
Abriendo una sesión

Para abrir una sesión, vaya al menú de Session y seleccione Open Web Session (Abrir Sesión Web).



Vista de información general de sesión

La vista inicial del Diseñador de Sesión es la vista de información general de sesión. Esta contiene la fecha que la sesión fue creada y dos opciones que son usadas cuando la sesión es ejecutada.



Las opciones son:

Always update session cookies (Siempre actualiza las galletas de sesión): Esto es usado para actualizar las galletas por cada "session request". Algunos sitios pueden requerir esta opción, mientras que otros no.

Allow safe request backtracking (Permite llamada segura hacia atrás): Esta opción es usada para el "safe session request". Una "safe session request" es una llamada que originalmente fue grabada, sin ningún cambio aplicado en el

Diseñador de Sesión. Este tipo de "session request" es usado para ejecución de la sesión. Una llamada segura hacia atrás es cuando una "session request" de prueba termina de enviar pruebas, regresa hacia atrás, al inicio de una sesión y recursivamente hasta la siguiente llamada pendiente.

Ejemplo:

Sin llamada segura hacia atrás

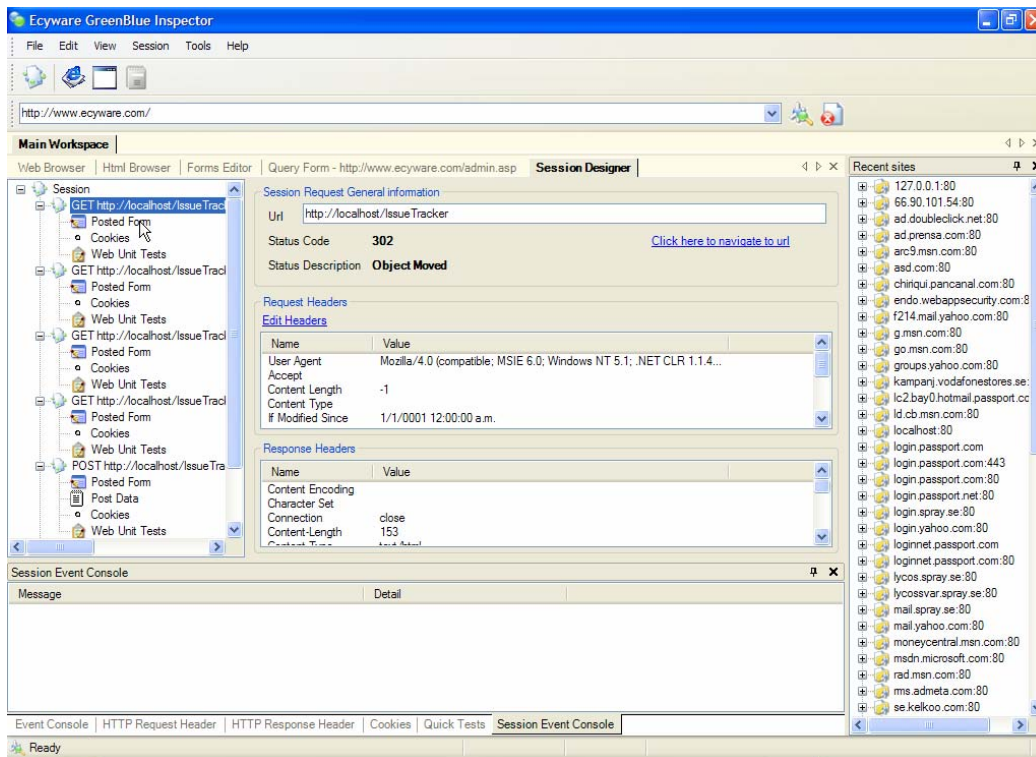
1. GET /default.asp
 - a. Submit SQL Test 1
 - b. Submit SQL Test 2
 - c. Submit Buffer Overflow Test 1
2. POST /login.asp
 - a. Submit SQL Test 1
 - b. Submit SQL Test 2
 - c. Submit Buffer Overflow Test 1
3. GET /mywelcomepage.asp

Con llamada segura hacia atrás

1. GET /default.asp
 - a. Submit SQL Test 1
 - b. Submit SQL Test 2
 - c. Submit Buffer Overflow Test 1
4. GET /default.asp
2. POST /login.asp
 - a. Submit SQL Test 1
 - b. Submit SQL Test 2
 - c. Submit Buffer Overflow Test 1
5. GET /default.asp
6. POST /login.asp
3. GET /mywelcomepage.asp

Las secciones sobre marcadas muestran las llamadas seguras aplicadas. Básicamente, una llamada segura hacia atrás es usada para los casos en que la aplicación detecta ataques y reseteo de galletas y sesiones. Con la llamada segura hacia atrás, una llamada segura es hecha hasta que la llamada de prueba en la cola ejecute.

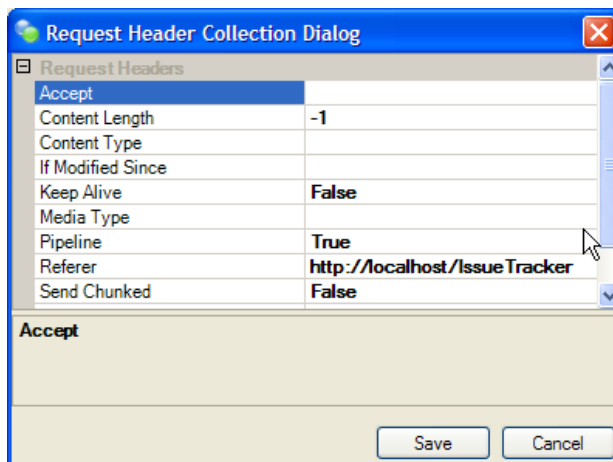
Vista general de información de Session Request



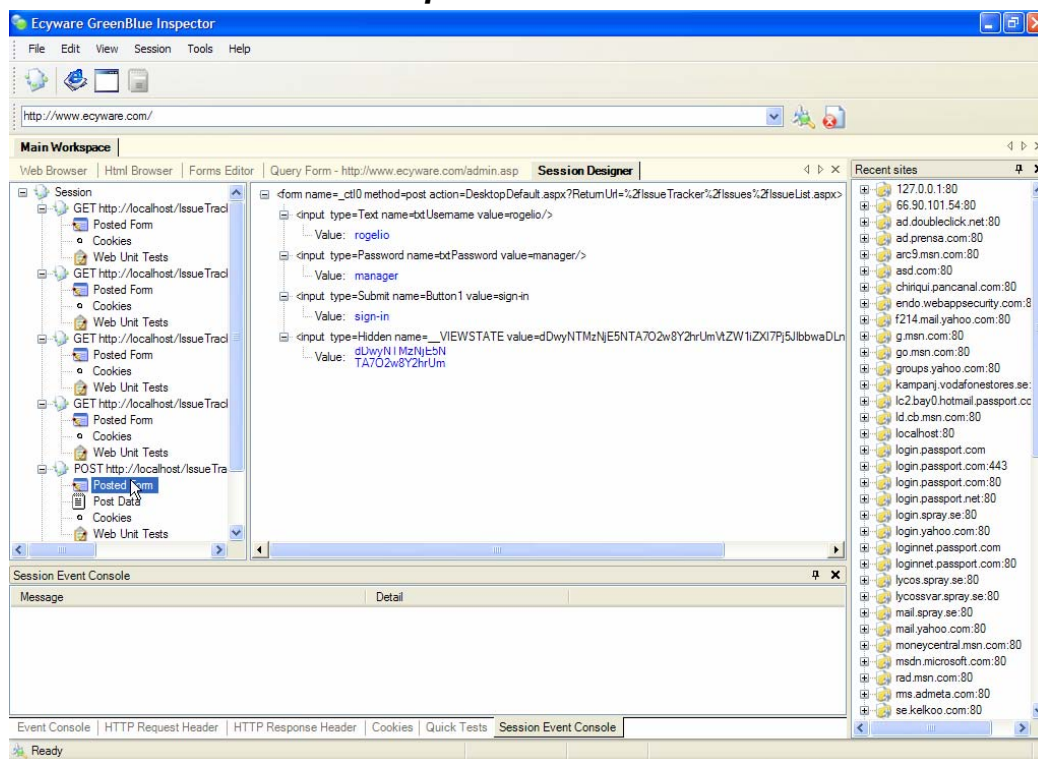
La vista general de información de Session Request contiene el url, el código de estatus y la descripción del estatus para un llamado. También contiene los encabezados de Request y los encabezados de Response.

Para llamadas GET, uno puede navegar haciendo clic en el enlace de "Click Here To Navigate Url".

Para editar los encabezados de Request, haga clic en el enlace de "Edit Headers". El diálogo de Colección de Encabezados de Request (Request Header Collection) aparece.

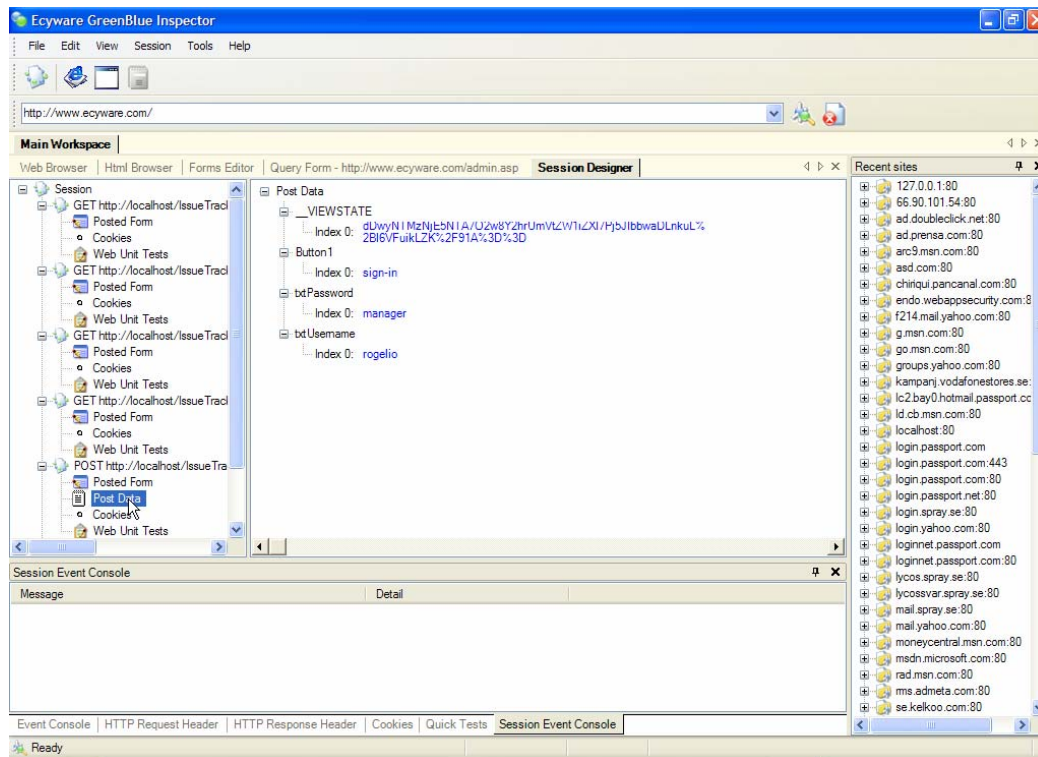


Diseñador de formulario posteadado



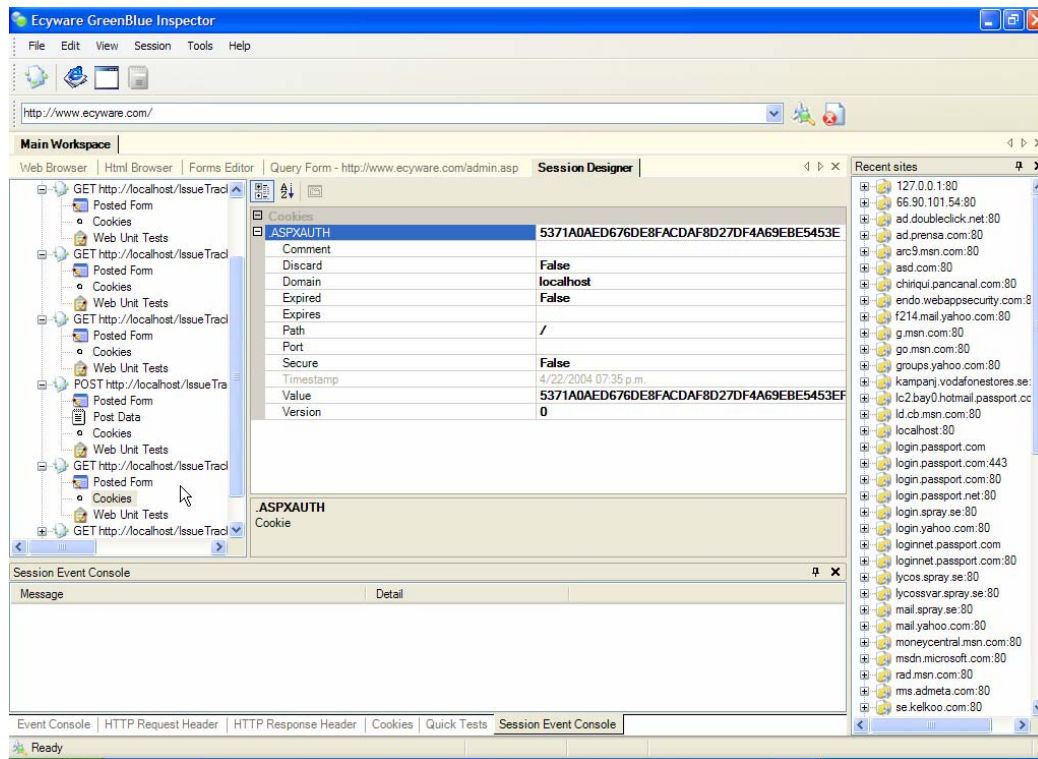
El diseñador de formulario posteadado es igual al del Editor de Formularios, pero uno solo puede cambiar los valores manualmente. Los cambios serán guardados en la próxima llamada (de un Session Request) y puede ser usado por el Administrador de Pruebas de Unidad Web (Web Unit Tests Manager), seleccionando el tipo de datos Form.

Diseñador de Post Data



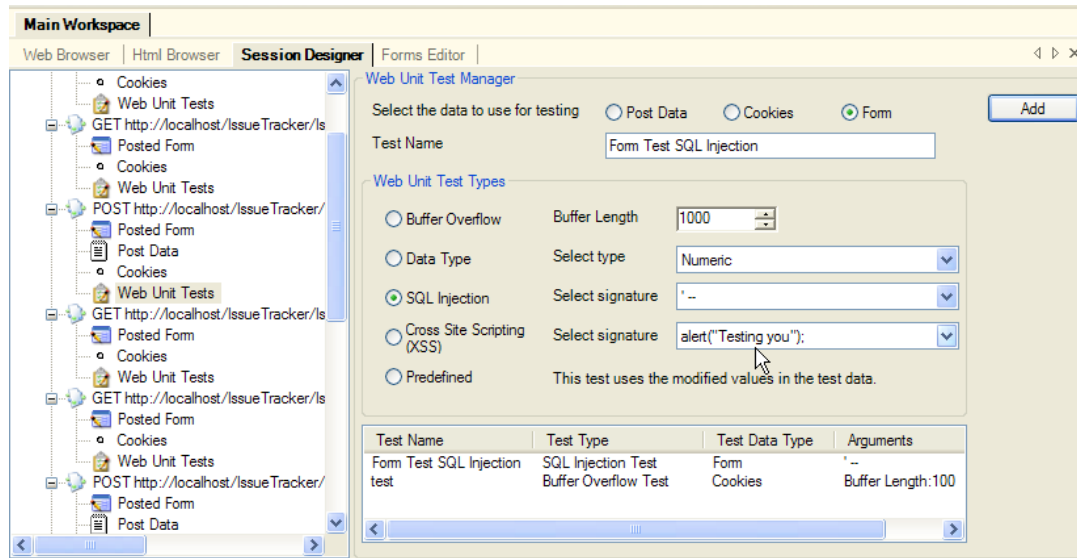
El diseñador de post data contiene una representación del Post Data, en este caso, un nivel más bajo que la representación de Formulario. Uno puede cambiar los valores manualmente. Los cambios serán guardados en la próxima llamada (de Session Request) y pueden ser usados y puede ser usado por el Administrador de Pruebas de Unidad Web (Web Unit Tests Manager), seleccionando el tipo de datos Post Data.

Editor de galletas



El editor de galletas es donde uno cambia los valores para una galleta (cookie). Los cambios serán guardados en la próxima llamada (de Session Request) y pueden ser usados y puede ser usado por el Administrador de Pruebas de Unidad Web (Web Unit Tests Manager), seleccionando el tipo de datos Cookies.

Administrador de Pruebas de Unidad Web (Web Unit Tests Manager)



El administrador de pruebas de unidad web es donde las pruebas son creadas. Estas pruebas son aplicadas a cada llamada cuando la sesión es ejecutada.

Para crear una prueba.

1. Seleccione el tipo de datos
 - a. Para llamadas GET, seleccione Url, Cookies o Form (si existe).
 - b. Para llamadas POST, seleccione Post Data, Cookies o Form.
2. Ingrese el nombre de la prueba.
3. Existen 5 diferentes tipos de pruebas:
 - a. **Buffer Overflow**: Seleccione el largo del búfer para generar.
 - b. **Data Type**: Selecciona de una lista de pruebas.
 - Numeric: Un búfer que representa valores numéricos.
 - Character: Un búfer que representa valores de caracteres.
 - Null: Un búfer que representa un string vacío.
 - c. **SQL Injection**: Selecciona una prueba de SQL injection de una lista de valores.
 - d. **Cross Site Scripting (XSS)**: Selecciona una prueba de XSS de una lista de valores.
 - e. **Predefined**: Utiliza el Post Data o Form modificado. Aplica solamente a llamadas POST.
4. Haga clic en el botón de Add.

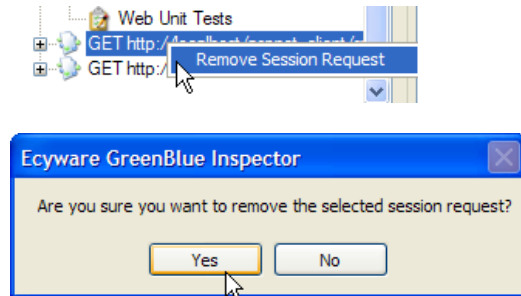
Una corrida de sesión ejecuta la prueba en orden. Por ejemplo:

1. GET /default.asp
 - Prueba Cookie Buffer Overflow.
 - Prueba Cookie Data Type.
2. POST /login.asp
 - Prueba Post Data SQL injection.
 - Prueba Cookie Data Type
3. GET /insiderPage.asp?id=123&module=M01
 - Prueba Url Buffer Overflow
 - Prueba Url XSS

La prueba de Url solo aplica a un query string normal. Tipos de query string adicionales serán agregados en versiones futuras.

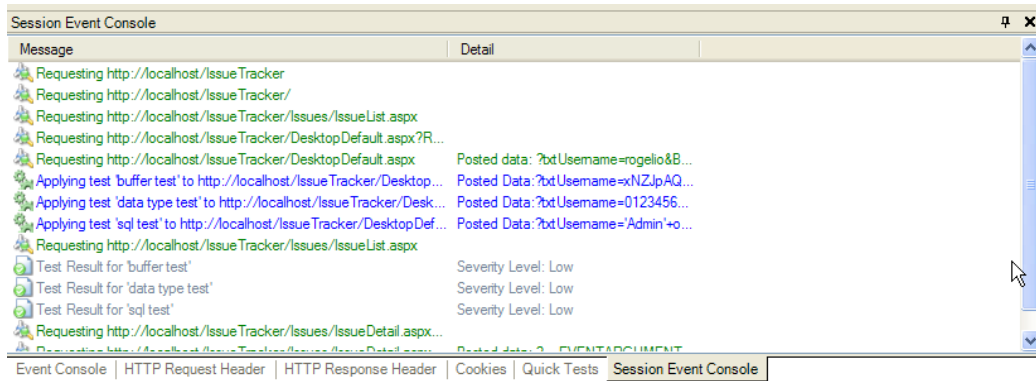
Eliminar un session request

Para eliminar un session request de una sesión, seleccione un session request y haga clic derecho. El menú de Remove Session Request (Remover Session Request) es desplegado. Seleccione esta opción y un mensaje aparecerá, preguntado si quiere eliminar el session request seleccionado. Haga clic en Yes (Si) para completar esta acción.



Corriendo una sesión

Para correr una sesión, seleccione el menú de Session, después seleccione Run Web Session (Correr una sesión web). Esto iniciara la ejecución de la sesión y la Consola de Eventos será activada.



- Las líneas verdes muestran las llamadas seguras realizadas.
- Las líneas azules muestran las llamadas de pruebas realizadas.
- Las líneas grises muestran el resultado de la prueba aplicada y el posible nivel de severidad para una llamada.
- Cualquier línea roja representa un error de ejecución de la sesión. Este error puede ser encontrado en la consola de eventos del sistema operativo.

Uno puede detener la sesión seleccionando Stop Session Run (Detener ejecución de sesión) desde el menú de Session.

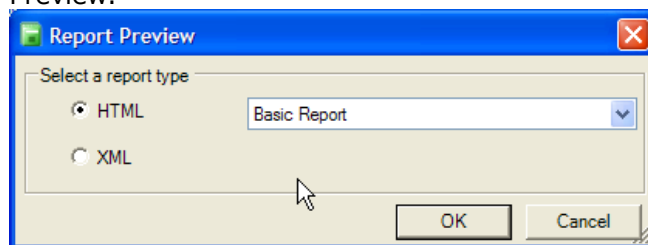
Reportes

Usando el dialogo de Vista previa de Reporte

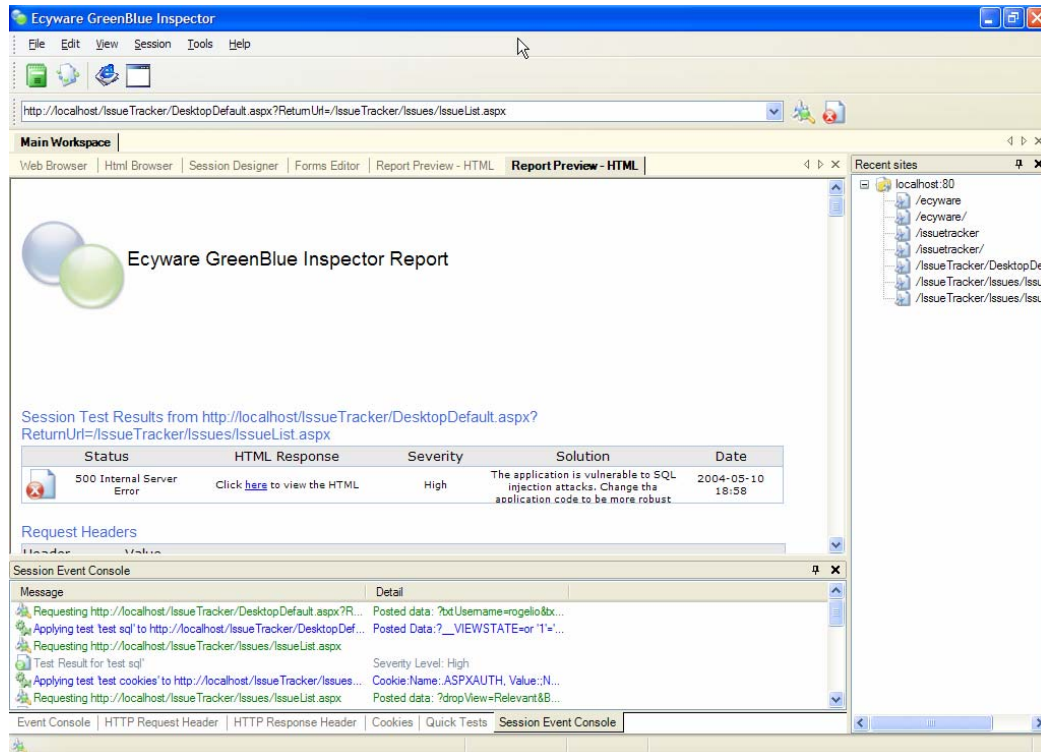
Después de que la ejecución de una sesión es completada, el Report Preview (Vista previa de Reporte) es habilitado. Para ver un reporte:



1. Haga clic en el botón de Report Preview o vaya al menú de File, Report Preview.



2. Seleccione HTML o XML. Si selecciono HTML, elija entre Basic Report (Reporte Básico) o Advanced Report (Reporte Avanzado).
3. Haga clic para mostrar el reporte.



Análisis del reporte

Reporte Básico

Para el reporte básico, los siguientes resultados están disponibles:

General Information

- **Test applied:** La prueba de unidad web.
- **Data:** El tipo de datos HTTP usado para la prueba.
- **HTML Source:** La respuesta HTML de la llamada.
- **Severity Level:** El nivel de severidad de la prueba.
- **HTTP Status:** El código de estatus y descripción HTTP.
- **Solution:** La solución para la vulnerabilidad encontrada.
- **References:** Muestra más información como ayuda de la solución.
- **Fecha y hora.**

General Information

Date: 2004-05-10 18:58

Test applied SQL Injection
Data Form
Html Source (Click [here](#) to view HTML Source)
Severity Level High
Http Status 500 Internal Server Error

Solution

The application is vulnerable to SQL injection attacks. Change the application code to be more robust against these types of attacks and apply known best practices for SQL injection prevention.

References

Validating user input, SQL Server 2000 SP3 Help, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/bldgapps/ba_highprog_11kk.asp
ASP Security Issues, Microsoft, <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/aspsecuritychecklist.asp>


Reporte Avanzado

Para el reporte avanzado, los siguientes resultados están disponibles:

Session Test Results

- **Status:** El código de estatus y descripción HTTP.
- **HTML Response:** La respuesta HTML de la llamada.
- **Severity Level:** El nivel de severidad de la prueba.
- **Solution:** La solución para la vulnerabilidad encontrada.
- **Fecha y hora.**

Session Test Results from [http://localhost/IssueTracker/Issues/IssueDetail.aspx?pid=document.write\("<html></html>"\);&](http://localhost/IssueTracker/Issues/IssueDetail.aspx?pid=document.write()

| Status | HTML Response | Severity | Solution | Date |
|---|---|----------|--|------------------|
|  500 Internal Server Error | Click here to view the HTML | High | The application is vulnerable to Cross Site Scripting (XSS) attacks. Change the application code so that each form field is check for invalid HTML, JavaScript or similar client side script code. | 2004-05-10 18:58 |

Request Headers

- **Header:** El nombre del encabezado.
- **Value:** El valor del encabezado.

Request Headers

| Header | Value |
|-------------------|---|
| Pipelined | True |
| If-Modified-Since | If-Modified-Since |
| Cookie | Cookie |
| Method | GET |
| Send Chunked | False |
| Referer | Referer |
| Request Uri | http://localhost/IssueTracker/Issues/IssueDetail.aspx?pid=document.write("<html></html>");& |
| Keep Alive | False |
| User Agent | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322) |

Response Headers

- **Header:** El nombre del encabezado.
- **Value:** El valor del encabezado.

Response Headers

| Header | Value |
|------------------|---|
| X-AspNet-Version | 1.1.4322 |
| Content-Type | text/html; charset=utf-8 |
| Last Modified | 5/10/2004 06:58:37 p.m. |
| Cache-Control | private |
| Server | Microsoft-IIS/5.1 |
| Response Uri | http://localhost/IssueTracker/Issues/IssueDetail.aspx?pid=document.write("<html></html>");& |
| Date | Tue, 11 May 2004 00:58:36 GMT |
| Protocol Version | 1.1 |
| Content-Length | 3776 |
| Method | GET |
| X-Powered-By | ASP.NET |
| Referer | http://localhost/IssueTracker/Issues/IssueList.aspx |

Web Unit Test

- **Name:** El nombre de la prueba de unidad web.
- **Test Data Container:** El tipo de datos HTTP utilizado.
- **Test Type:** El tipo de prueba de unidad web.
- **Post Data (opcional):** Muestra el post data enviado al servidor.
- **Test Value:** El valor seleccionado de la prueba.
- **Buffer length (opcional):** La longitud del bufer.

Web Unit Test

| Name | Test Data Container | Test Type | Post Data | Test Value |
|-------------------------|---------------------|---------------|-----------------------------|------------|
| Form Test SQL Injection | Form | SQL Injection | ?dropView='+--&Button1='+-- | '.. |

Web Unit Test

| Name | Test Data Container | Test Type | Post Data | Test Value |
|----------|---------------------|-----------|-----------|----------------------------------|
| test xss | Url | XSS | | document.write("<html></html>"); |

Guardar un reporte

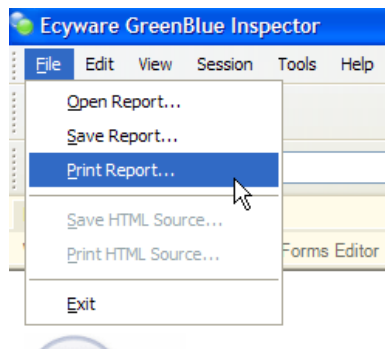
Para guardar un reporte, vaya al menú de File y haga clic en la opción de Save Report (Guardar Reporte).

Abrir un reporte

Para abrir un reporte, vaya al menú de File y haga clic en la opción de Open Report (Abrir Reporte).

Imprimir un reporte

Para imprimir un reporte, vaya al menú de File y haga clic en la opción de Print Report (Imprimir Reporte).



Plantillas de reporte

Las plantillas de los reportes están localizadas en el directorio de Common Folder. Las plantillas están en formato XSLT.

GreenBlue Inspector Configuration File

The following settings can be changed from the configuration file.

defaultBufferOverflowLength: Sets the default buffer overflow length for the quick tests panel.

defaultSqlTest: Sets the default SQL injection test for the quick tests panel.

defaultXssTest: Sets the default Cross Site Scripting test for the quick tests panel.

xssSignatures: Sets the name for the XSS signatures file.

sqlSignatures: Sets the name for the SQL injection signatures file.

basicReportTemplate: Sets the name for the basic report template file.

advancedReportTemplate: Sets the name for the advanced template file.

solutionDataFile: Sets the name for the solution data file.

referenceDataFile: Sets the name for the references data file.

userAgent: Sets the default user agent for the application.

keepAlive: Sets the default keep alive setting for the application.