

### **Capítulo 3.**

## **Análisis de una Herramienta de Apoyo para Asegurar las Aplicaciones Web del CENTIA.**

### **3.1. ¿Por qué es tan importante contar con una herramienta de apoyo para asegurar las aplicaciones Web?**

Hoy en día los piratas informáticos o los llamados “hackers” llegan a ser cada vez más sofisticados, haciendo cada vez más difícil proteger la integridad de las aplicaciones y la información que estas guardan. Proteger estas aplicaciones poniendo parches manualmente es una estrategia que tarde o temprano fallara. La seguridad Web, en la actualidad, debe ser construida de abajo hacia arriba, desde el desarrollo de la aplicación, pruebas de calidad, el despliegue y el mantenimiento.

Por estas razones es muy importante que las Aplicaciones Web del CENTIA cuenten con una Herramienta de Apoyo, para mantener su seguridad, confiabilidad y calidad que estas aplicaciones requieren; de esta manera, obtener y mantener una buena imagen de los servicios que brinda el CENTIA.

Una Herramienta de Apoyo permite construir la seguridad de la aplicación, esto es muy importante, porque el costo relativo de arreglar los errores y defectos que tiene una aplicación después del despliegue, es casi 15 veces más grande que hacerlo en el desarrollo.

### **3.2. AppScan DE: Una Herramienta de Apoyo como solución para asegurar las Aplicaciones Web del CENTIA.**

#### **3.2.1. ¿Qué es AppScan DE?**

**AppScan DE** es una poderosa herramienta de pruebas que permite el rápido desarrollo de la seguridad. Esta herramienta ayuda a hacer que la lógica de la aplicación sea resistente a ataques sin tocar su presentación o eficacia. **AppScan DE** detecta los defectos de la seguridad automáticamente; como un componente integrado al desarrollo

de la empresa, esta herramienta, automatiza las pruebas de creación de escritura, modificación y proceso de mantenimiento, asegurando confiabilidad y pruebas que son repetibles.

**AppScan DE** es una herramienta que ayuda a las empresas a reducir costos y a crear aplicaciones confiables y resistentes contra hackers, en el ambiente de desarrollo. Esta herramienta escanea las aplicaciones Web desde el punto de vista del usuario. **AppScan DE** explora la aplicación y aprende la lógica del negocio.

**AppScan DE** crea “Vulnerabilidades Potenciales” que son los defectos potenciales de la seguridad en el código y entonces los prueba para verificar que ellos existen. Las “Vulnerabilidades Potenciales” son las Aplicaciones Específicas relacionadas directamente a nuestra aplicación.

**AppScan DE** reporta los errores o defectos de la aplicación, luego se los proporciona al usuario para empezar a arreglar estos errores.

### **3.2.2. Proceso del AppScan DE.**

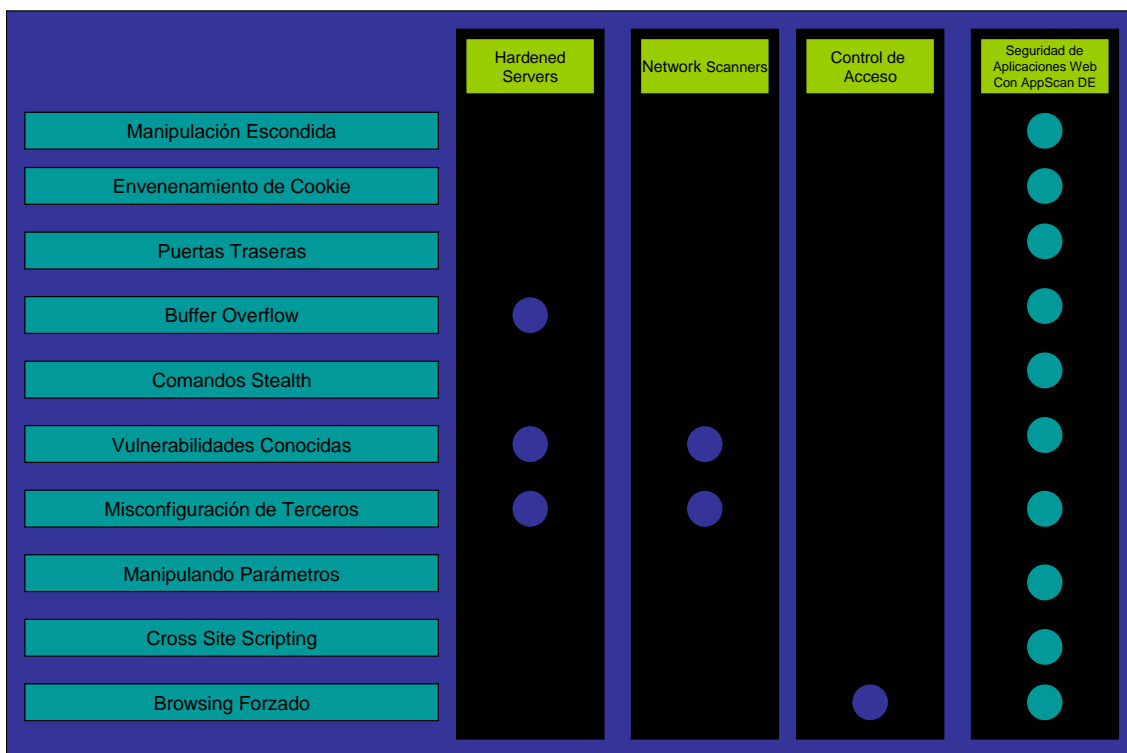
**AppScan DE** encuentra y prueba las vulnerabilidades desconocidas (ASVs):

- Vulnerabilidades Desconocidas: también llamadas Vulnerabilidades Específicas de la Aplicación (ASVs). Estas vulnerabilidades son el producto de las aplicaciones que se configuran impropriadamente o cuyas reglas para el uso válido no son impuestas apropiadamente por la lógica de las aplicaciones.
- Una vez que **AppScan DE** ha identificado las vulnerabilidades potenciales dentro de una aplicación Web, prueba cada vulnerabilidad potencial para determinar su severidad y la mejor manera de arreglarlo.

### 3.2.3. AppScan DE asegura las Aplicaciones Web en contra de las Persiones del Web.

Una Perversion del Web es una manera en el que un pirata informático o un hacker modifica o destruye una aplicación Web, sin el debido permiso del dueño de la aplicación y todo lo que necesita es un pequeño agujero en el código, un examinador del Web y una pequeña determinación.

A continuación la figura 3.1 muestra cuales son las perversiones del Web que asegura **AppScan DE**:



**Figura 3.1.** Persiones del Web [Sanctum, 2004].

Ahora mostraremos ejemplos y casos de algunas de estas perversiones del Web, de como estos tipos de perversiones del Web pueden ser fácilmente ejecutados para robar dinero, transferencia ilegales de dinero, obtener información de clientes o consumidores y destruir el sitio Web.

### a) Manipulación Escondida.

#### Situación:

Hay una aplicación Web en una tienda en línea, el objeto más vendido de la semana es una cámara para PC, el precio es de \$129 US, ver figura 3.2.

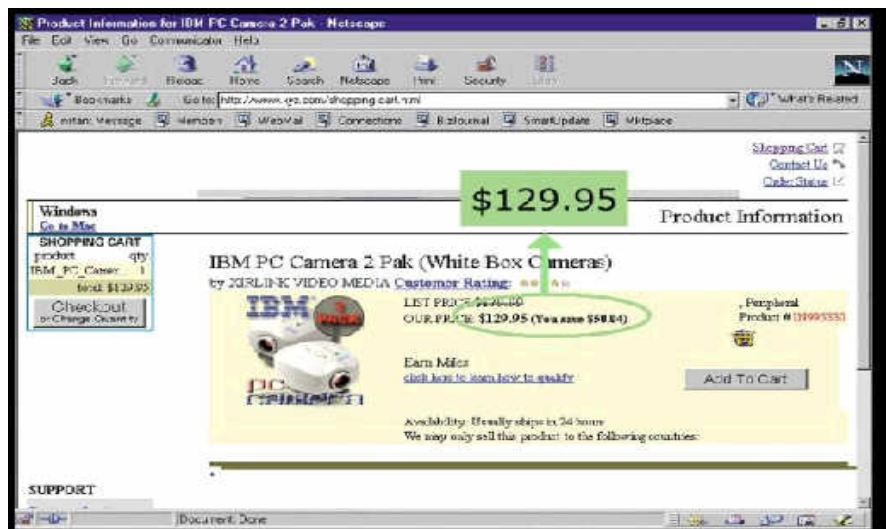
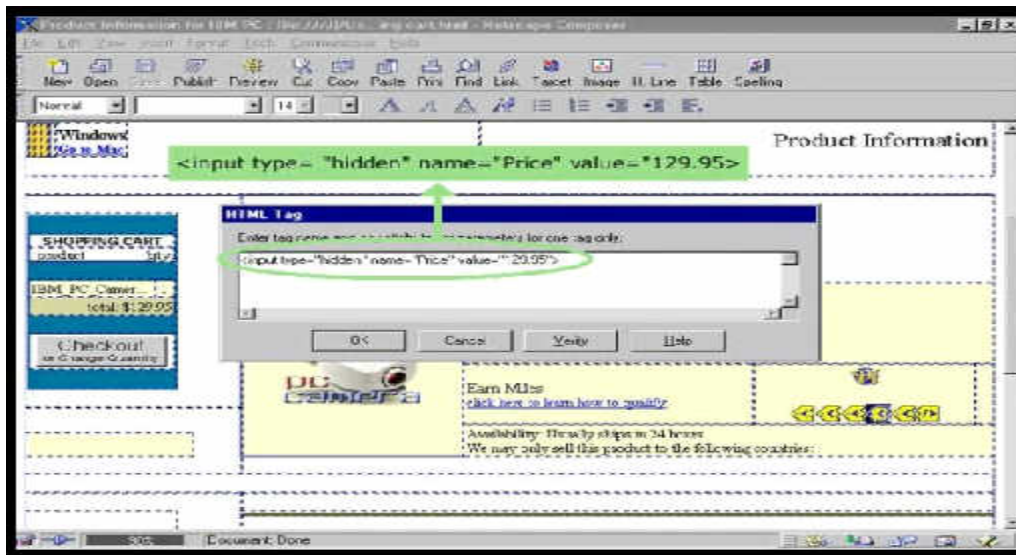


Figura 3.2. Manipulación Escondida [Sanctum, 2004].

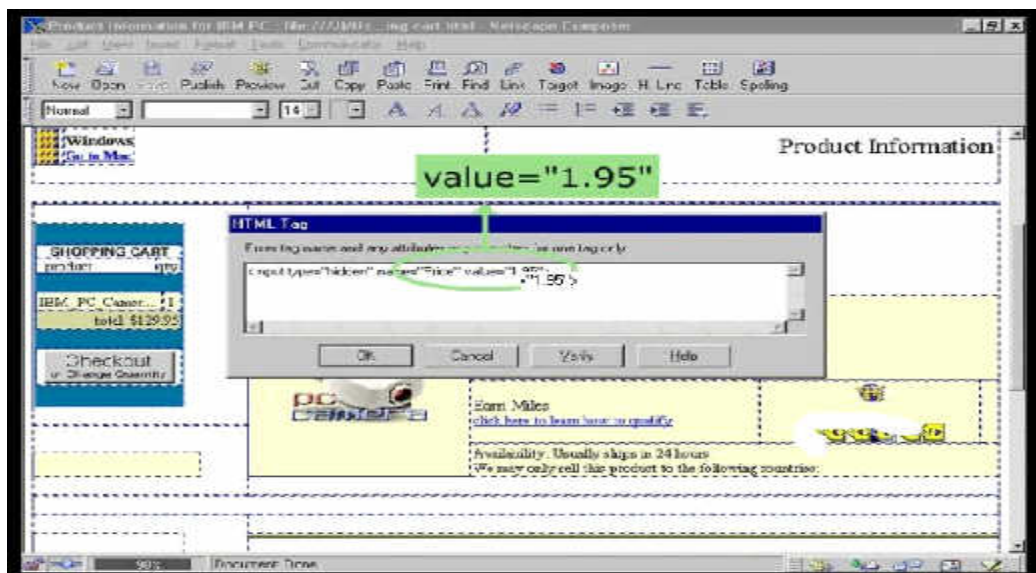
#### Punto de Ataque:

Para facilitar un desarrollo rápido de esta aplicación de comercio electrónico fue diseñada con campos escondidos (hidden fields). La información del precio se puso en un campo escondido, con la asignación de \$129 US, ver figura 3.3.



**Figura 3.3.** Manipulación Escondida, punto de ataque [Sanctum, 2004].

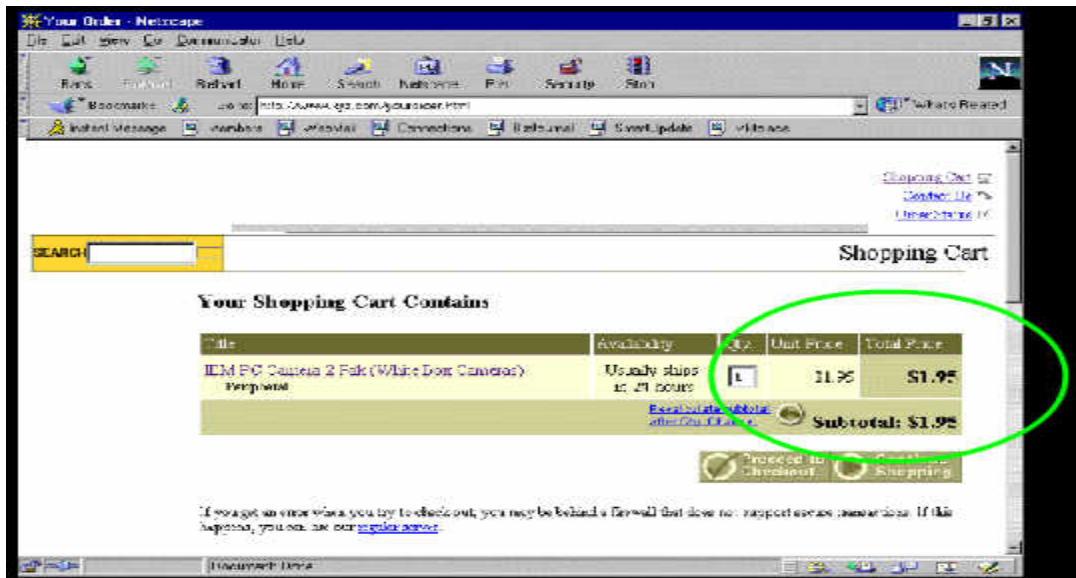
El desarrollador de la aplicación asume que la información del precio seguirá intacta. Pero si se usa un estándar *Netscape HTML Editor* un hacker puede cambiar el valor del campo escondido y cambiarlo a \$1.95 US, ver figura 3.4.



**Figura 3.4.** Manipulación Escondida, punto de ataque (cont) [Sanctum, 2004].

## **Daño:**

El hacker somete el pequeño cambio en la página HTML, entonces el puede comprar la misma cámara por el precio de \$1.95 US, ver figura 3.5.



**Figura 3.5.** Manipulación Escondida, daño [Sanctum, 2004].

## **b) Envenenamiento de Cookies.**

### **Situación:**

Supongamos que hay una típica página Web de pagos de cuentas en línea, ya que este tipo de servicios se ha vuelto muy popular. En este ejemplo un cliente o un hacker llamado “Abacarius” ingresa al sitio y descubre las cantidades que debe pagar, ver figura 3.6.

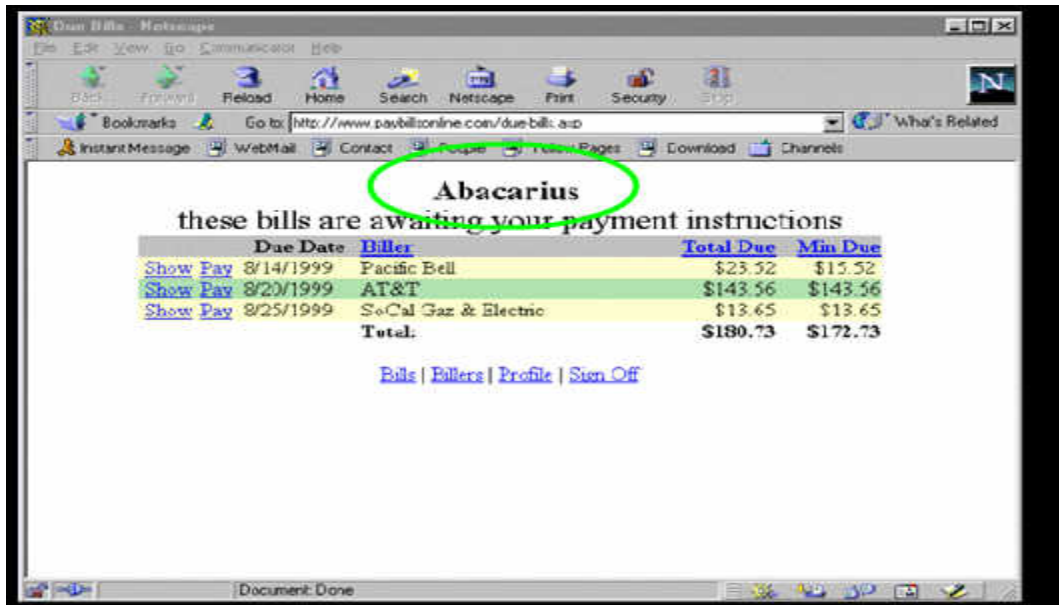


Figura 3.6. Envenenamiento de Cookies [Sanctum, 2004].

#### Punto de Ataque:

El área vulnerable en este ejemplo es el “cookie”, es una pequeña pieza de información que el sitio pone en la computadora de cualquier cliente que ingresa. El “cookie” pone información que identifica al cliente para el sitio y es incluido con cualquier petición enviada al sitio, ver figura 3.7.

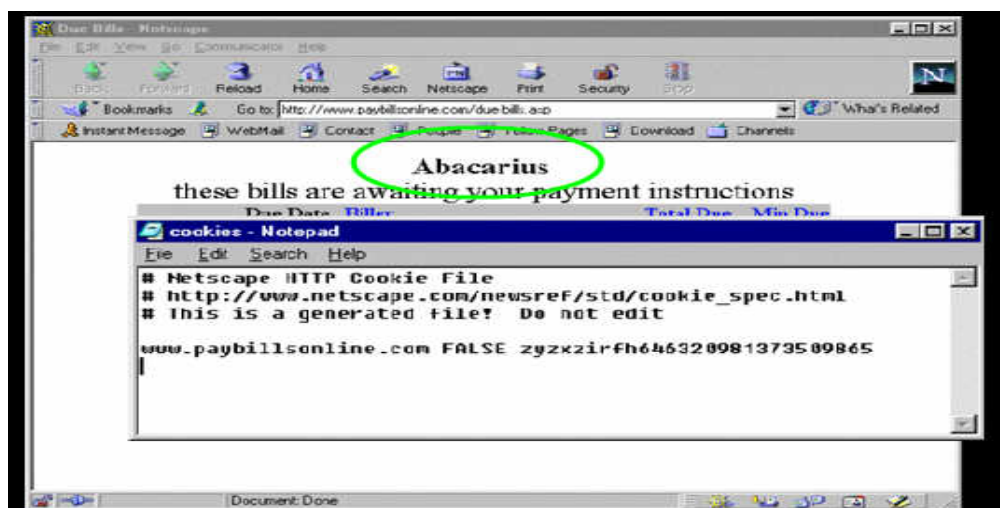


Figura 3.7. Envenenamiento de Cookies, punto de ataque [Sanctum, 2004].

Si nos fijamos en el archivo de cookies, nos encontraremos con una extraña combinación de letras y números. Nos estaremos enterando de la conexión entre el nombre del consumidor, Abacarius, y el *cookie* encriptado, zyzxrir. En esta encriptación, la “a” se vuelve “z” y “b” se vuelve “y”, ver figura 3.8.

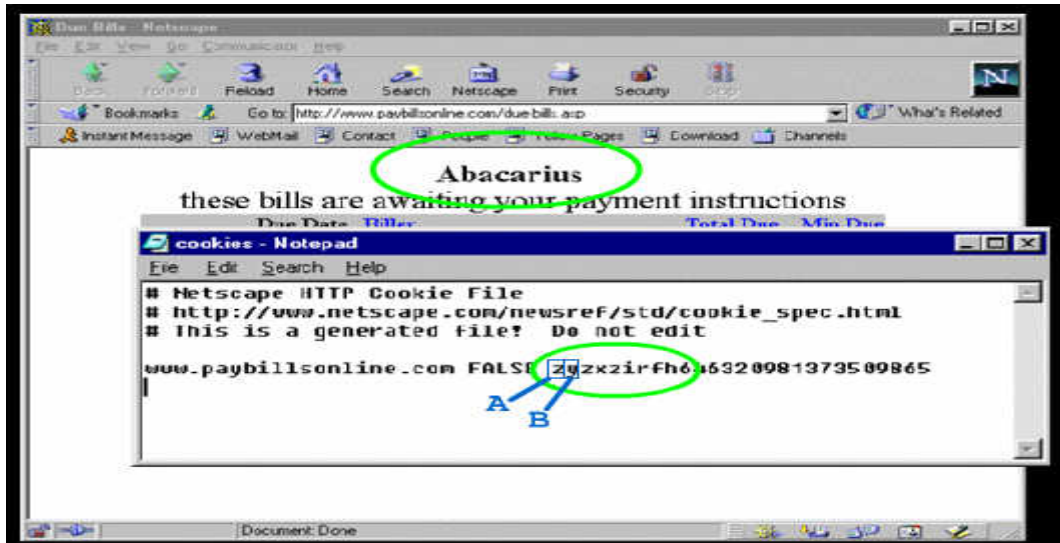


Figura 3.8. Envenenamiento de *Cookies*, punto de ataque (cont) [Sanctum, 2004].

*Cookies* es un alimento para los hackers listos. En este caso el hacker toma el *cookie* original y la convierte, para hacer que este sitio lo reconozca como “Johnson”. “J” se vuelve “q” y “o” se vuelve “i”. Una vez que el *cookie* es re-encriptada, el hacker esta listo para hacer uso de “Jonson”, ver figura 3.9.

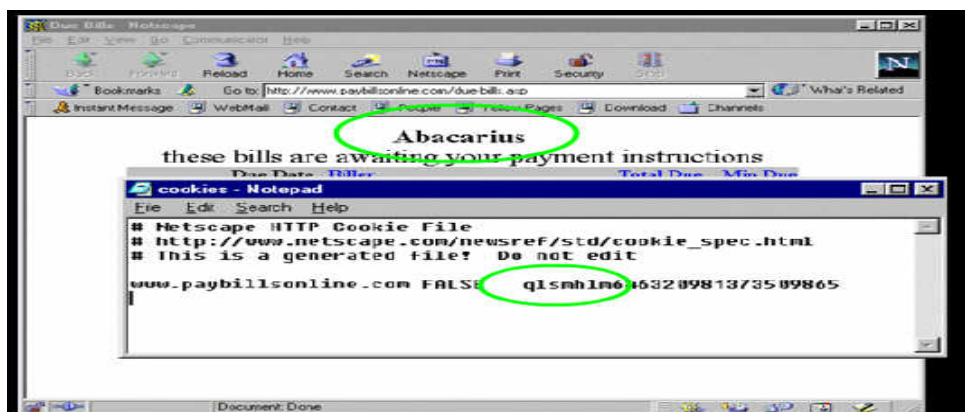
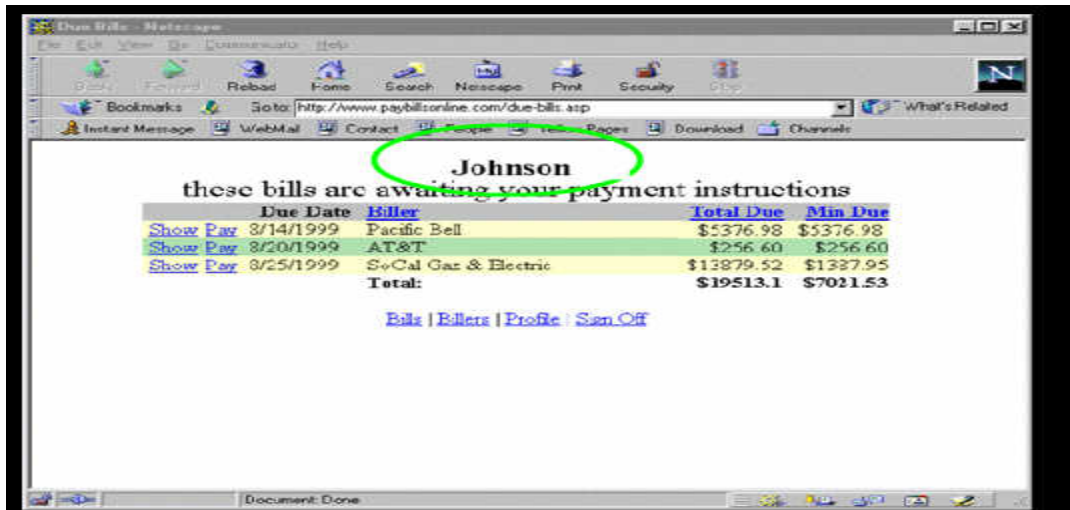


Figura 3.9. Envenenamiento de *Cookies*, punto de ataque (cont) [Sanctum, 2004].



### **Daño:**

Ahora este sitio reconoce Abacarius como Johnson, y deja que el vea la cuenta de Johnson, puede borrarlo, o ser especialmente generoso y actualizar el pago de algunas cuentas solo con la manipulación de números, ver figura 3.10.



**Figura 3.10.** Envenenamiento de *Cookies*, daño [Sanctum, 2004].

### **c) Puertas Traseras.**

#### **Situación:**

El chequeo de cuentas en el sitio de un banco es muy popular por los clientes. Con la nueva gama de servicios financieros en línea, los clientes del banco pueden fácilmente acceder a su record financiero y hacer transacciones financieras sofisticadas, incluyendo transferencias de dinero, ver figura 3.11.

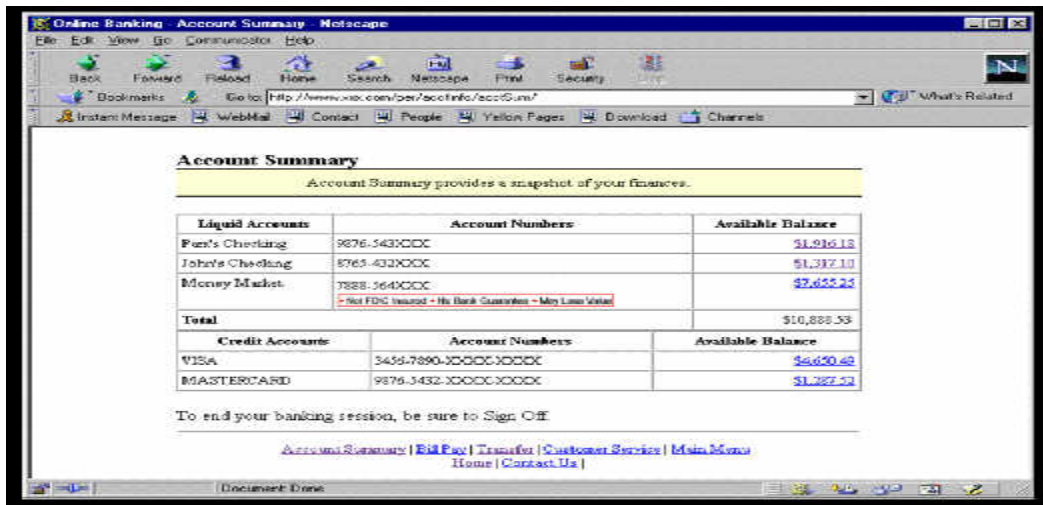


Figura 3.11. Puertas Traseras [Sanctum, 2004].

### Punto de Ataque:

La administración del banco, cree tener sus aplicaciones de transferencias de dinero en un lugar tranquilo. En la prisa de tener estas aplicaciones en línea, la opción de depuración utilizada para probar durante el desarrollo se dejó con errores. ¿Puedes imaginar lo que un hacker puede hacer en esta situación?, ver figura 3.12.

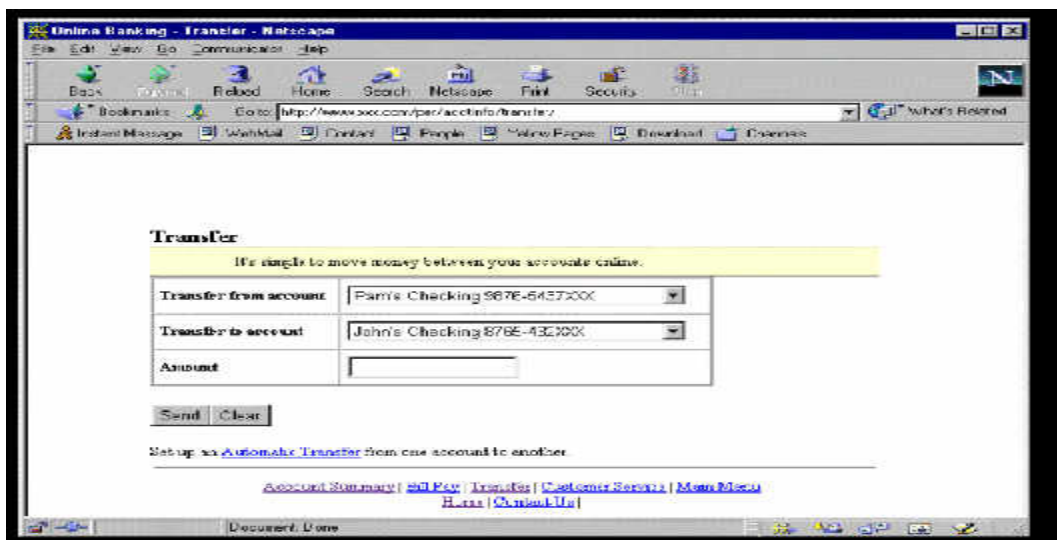
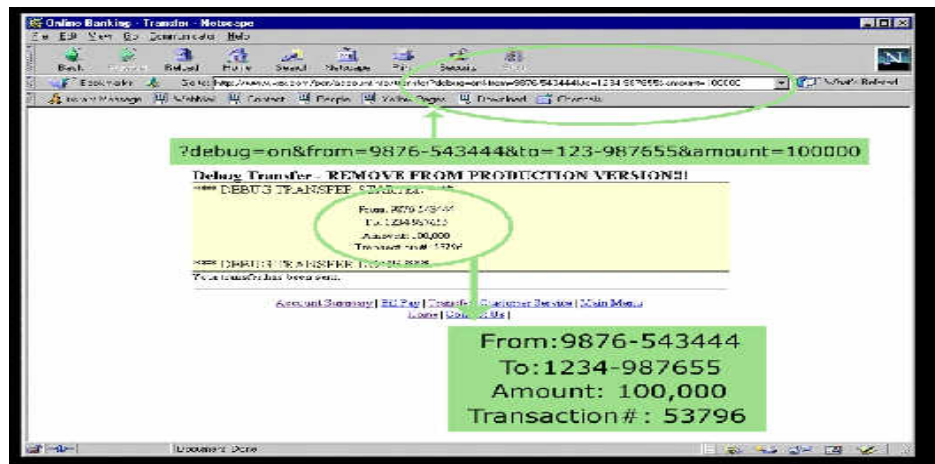


Figura 3.12. Puertas Traseras, punto de ataque [Sanctum, 2004].

## **Daño:**

Transmitiendo una petición a la transferencia CGI con un parámetro debug “=on”, el hacker activa el *debug o atajo* y comienza a manipular una característica que fue erróneamente dejada en la versión final de la aplicación. Usando una opción común del *debug*, el hacker descubre que puede fácilmente transferir cualquier cantidad de dinero de cualquier cuenta a cualquier otra cuenta, ver figura 3.13.



**Figura 3.13.** Puertas Traseras, daño [Sanctum, 2004].

## **d) Vulnerabilidades Conocidas.**

### **Situación:**

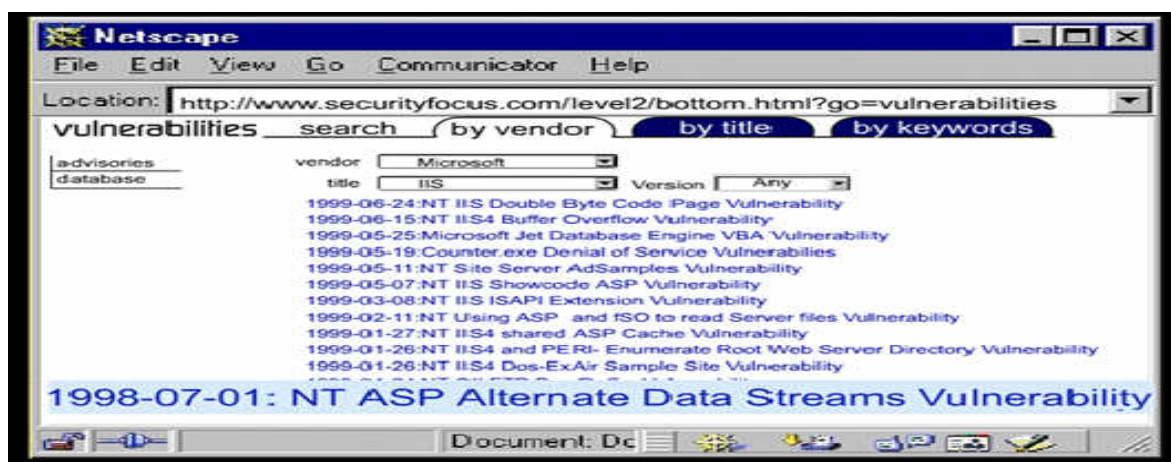
En este sitio de comercio electrónico, los administradores manejan varias tareas usando una interfaz Web. Un procedimiento de la entrada protege esta área de la administración de usuarios no invitados, ver figura 3.14.



**Figura 3.14.** Vulnerabilidades Conocidas [Sanctum, 2004].

### Punto de Ataque:

Te has dado cuenta en el URL, que este sitio se relaciona con la tecnología de *Microsoft Active Server Page* (ASP). Usado en millones de sitios, la tecnología ASP infortunadamente ha obtenido debilidades que hackers listos y persistentes pueden explotar. Una rápida búsqueda de seguridad relacionada con un sitio Web, [www.securityfocus.com](http://www.securityfocus.com), revela un número de de potenciales y peligrosos problemas con ASPs. Una debilidad, *NT ASP Alternate Data Streams Vulnerability*, deja a cualquiera ver el código fuente de cualquier ASP, ver figura 3.15.



**Figura 3.15.** Vulnerabilidades Conocidas, punto de ataque [Sanctum, 2004].

El problema es uno de muchos encontrados en software de terceros. Con demasiados “bugs” por arreglar y parches para aplicar, los programadores simplemente no pueden mantener el ritmo. La mayoría de los sitios Web son vulnerables de una o otra manera, incluso teniendo parches recientemente aplicados.

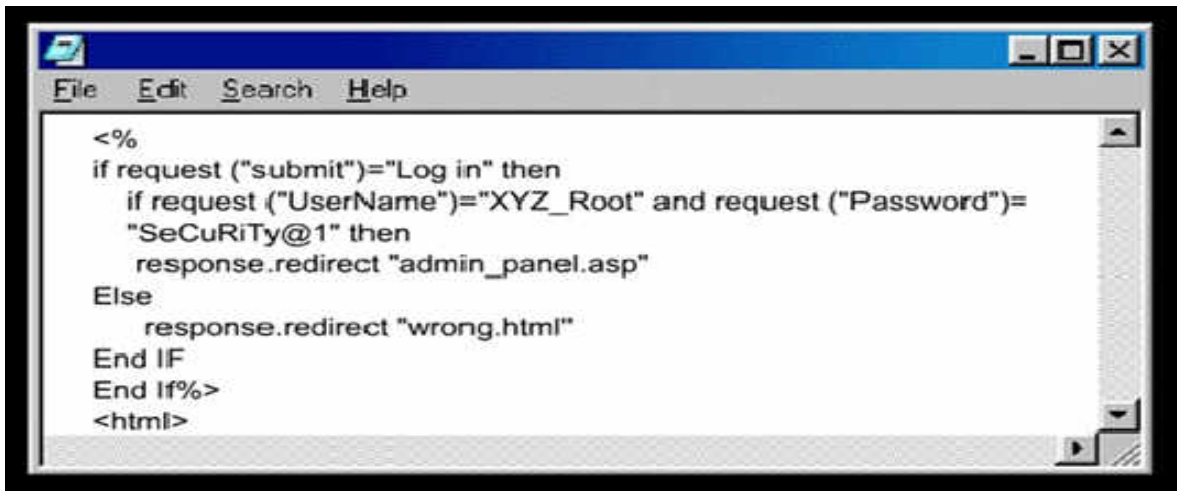
### **Daño:**

En este ejemplo, el último parche no fue aplicado, es una puerta abierta para un hacker. Añadiendo al URL “::\$DATA” al nombre del ASP y refrescando la página, un hacker puede instruir al servidor Web que le mande el código fuente completo para el “admin.\_login” ASP, ver figura 3.16.



**Figura 3.16.** Vulnerabilidades Conocidas, daño [Sanctum, 2004].

Si miramos el código fuente ASP, observamos que tenemos el nombre del administrador (XYZ\_Root) y también la contraseña (SeCuRiT@1). Ahora el hacker tiene el completo control del sitio Web, ver figura 3.17.

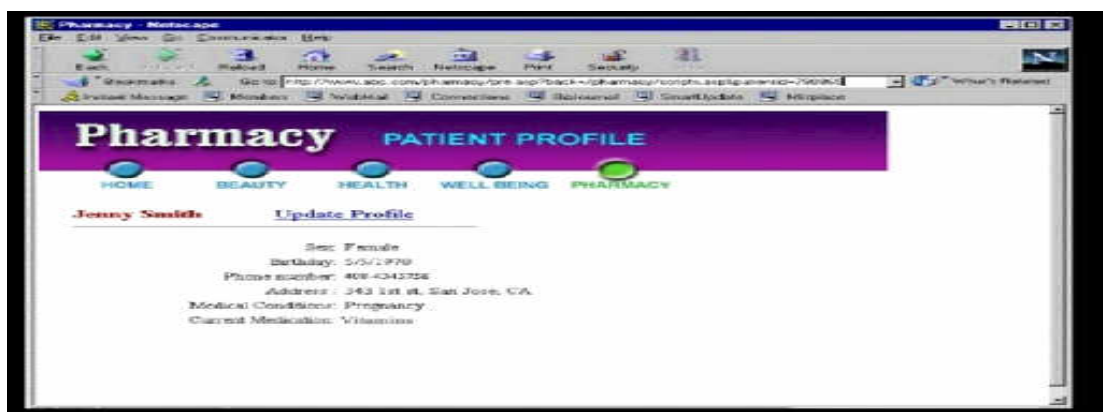


**Figura 3.17.** Vulnerabilidades Conocidas, daño (cont) [Sanctum, 2004].

#### e) Manipulando Parámetros.

##### Situación:

Para un hacker, información personal es como dinero en el banco. Una vez que mete sus manos en información confidencial, tales como, record médicos, el hacker puede rápidamente volver esa información en dinero. En este ejemplo, los clientes de una farmacia en línea, tienen sus perfiles de salud en un sitio Web. Asumiendo que esta información será bien protegida. El cliente Jenny Smith incluyó información de alta confidencialidad en su perfil, ver figura 3.18.



**Figura 3.18.** Manipulando Parámetros [Sanctum, 2004].

## Punto de Ataque:

Miren cerca del URL que da acceso al perfil de Jenny. Se darán cuenta que contiene el ID del paciente, un parámetro que identifica solamente a ella. Quedarán asombrados cuando vean que pasa cuando un hacker cambia el ID del paciente a “\*” y refresca la página del perfil, ver figura 3.19.



Figura 3.19. Manipulando Parámetros, punto de ataque [Sanctum, 2004].

## Daño:

Con este simple comando, el hacker ahora tiene acceso a la entera base de datos de los pacientes, incluyendo las condiciones médicas de todos los pacientes y medicamentos. La aplicación trata de usar el símbolo “\*” para encontrar un paciente específico, este símbolo significa “*matchall*”, la aplicación recupera toda la base de datos y la manda al hacker. El resultado no es solo una gran invasión de privacidad, sino también quebranta una serie de leyes en contra de la farmacia.



### **3.3. Situación en el CENTIA y sus Necesidades.**

Existe una preocupación que es constante por parte de los investigadores que realizan sus proyectos desarrollando aplicaciones Web en el CENTIA. Esto es referente a la seguridad, confiabilidad y calidad de las Aplicaciones Web resultado de sus proyectos de investigación. Muchas veces estas Aplicaciones Web son propensas a ataques, de los cuales muchas veces, no nos damos cuentas, ni sabemos cuales son las vulnerabilidades que estas tienen.

La necesidad principal del CENTIA es que sus aplicaciones Web sean seguras, a que se refiere esto, tanto a la modificación, robo o destrucción total de información valiosa que contienen estas Aplicaciones. Otra necesidad que es muy importante en una organización es que los servicios que brinda sean confiables y de calidad, esto se logra a través de seguimientos de pasos o lineamientos.

De acuerdo con la investigación que se ha realizado en este trabajo de tesis, la mejor manera de solucionar este problema es utilizando una herramienta de apoyo que nos ayude a disminuir este problema. Con la investigación que se llevó a cabo la mejor manera de asegurar las Aplicaciones Web, es saber cuales son sus vulnerabilidades en la etapa de desarrollo. De esta manera, sabiendo cuales son sus vulnerabilidades se arreglan sus errores y se pueden publicar en la red, con menos posibilidad o menos propensas a un ataque informático.

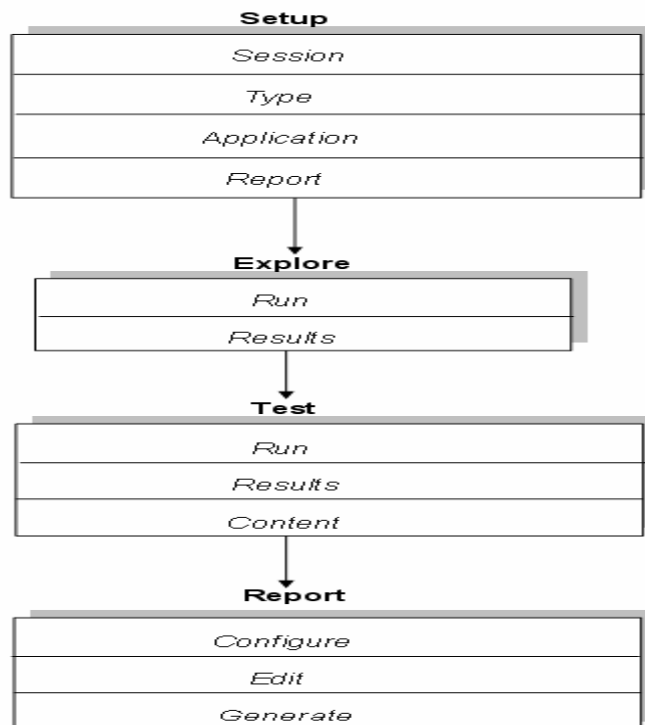
### **3.4. Beneficios de la Herramienta para el CENTIA.**

Como todos sabemos no se puede asegurar un sistema al 100 por ciento, siempre existen vulnerabilidades. En tiempo real, existen Aplicaciones Web del CENTIA que muchas de estas no son seguras, que tienen vulnerabilidades. Esta herramienta ayudará a encontrar cuales son las vulnerabilidades existentes que tienen estas Aplicaciones, hacer un reporte y proponer cual es la mejor manera de arreglar estas vulnerabilidades. De esta manera, ahorrar costos significativos en pérdidas si se llegará a realizar algún ataque a estas Aplicaciones.



Otro beneficio que traerá esta herramienta al CENTIA, es que a partir de que esta herramienta este trabajando, su objetivo principal es encontrar cuales son las vulnerabilidades de las Aplicaciones en la etapa de desarrollo. Esto es, con el fin de que una vez publicada en la red sean menos propensas a ataque de hackers. También brinda una solución para automatizar los análisis de vulnerabilidades y pruebas de penetración de sus aplicaciones y plataformas Web. Elimina los exámenes manuales que eran necesarios antes de implementar una aplicación, genera reportes que determinan la mejor manera de cumplir con estas auditorías para asegurar sus aplicaciones, antes de su implementación. Como vemos, esta herramienta traerá muchos beneficios al CENTIA, se le dará un proceso a las aplicaciones descubriendo sus vulnerabilidades y llegando a ese 100 por ciento de seguridad que queremos alcanzar.

### 3.5. Arquitectura de la Herramienta AppScan DE.



**Figura 3.20.** Arquitectura de AppScan DE [Sanctum, 2004].

**Etapla Setup.** Se selecciona que tipo de Scan quieres correr de la lista de tipos de Scan. Hay dos tipos de Scan: uno que es completamente automático y uno que es “Scan Interactivo”. También se puede hacer cambios y salvar uno nuevo, personalizar los tipos de Scan, exactamente a la medida de las necesidades del usuario. Una vez que esta etapa está completa, comienza el proceso de evaluación que consiste en tres partes:

**Etapla de Exploración.** Durante la etapa de Exploración, se explora el sitio Web, visitando los links que tiene, como lo hace un usuario normal. Esta exploración del sitio puede ser manual, automática, o interactiva (una combinación de las dos), dependiendo del tipo de Scan que se escogió/definió durante la etapa de *Setup*. La exploración se puede realizar completa de la aplicación o se puede dividir en procesos pertinentes de la aplicación. Cuando se explora el sitio Web, se reúne información del sitio, tales como, los links y las respuestas a las peticiones. Esta información se almacena en la base de datos de la etapa de Exploración y se utiliza para crear una lista de “vulnerabilidades potenciales”; las peticiones del URL que se diseñan para probar la elasticidad del sitio Web y revelar sus debilidades.

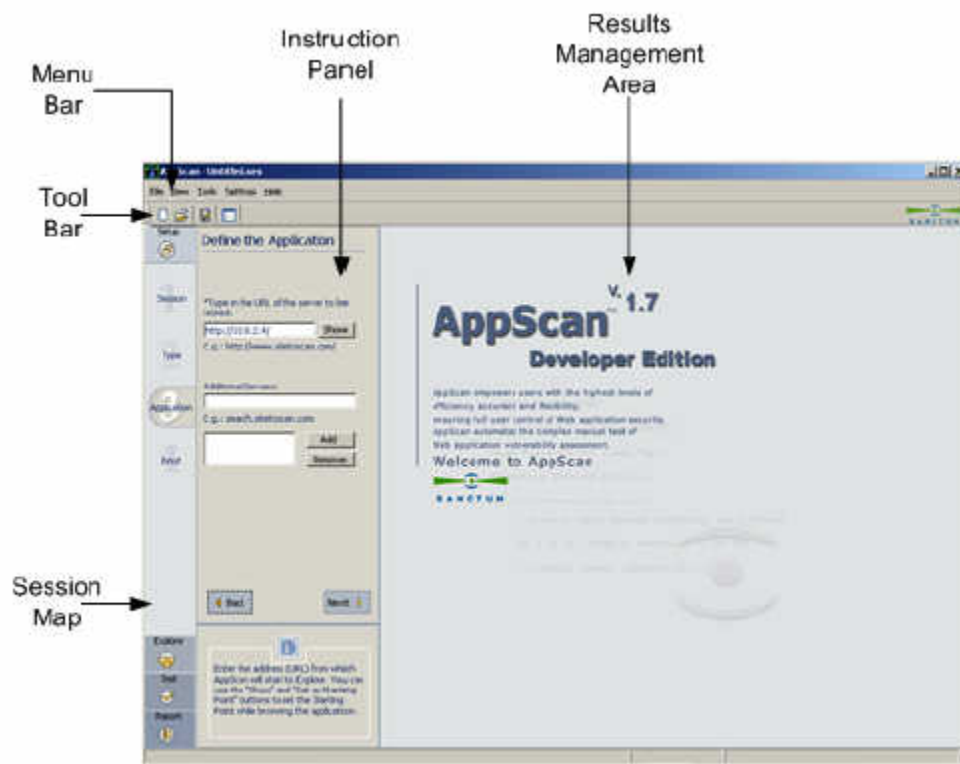
**Etapla de Prueba.** Durante la etapa de Prueba, las vulnerabilidades potenciales que se encontraron en la etapa de Exploración son probadas. Estas pruebas utilizan técnicas avanzadas de hackers informáticos para escoger las vulnerabilidades verdaderas (de las muchas vulnerabilidades probadas) y valoran su severidad. Como en la etapa de Exploración, en esta etapa el proceso se puede realizar automáticamente o con muchas intervención del usuario. Una vez, que las pruebas están completas el sistema permite que el usuario verifique los resultados reexaminando manualmente alguna vulnerabilidad potencial. Si el usuario tiene sospecha de cualquiera de los resultados de la prueba, se puede modificar el reporte de la sesión e incluir cualquier paso siguiente para una investigación adicional. Los piratas informáticos pueden obtener información sensible de ciertos archivos de sitio Web viendo su código fuente. La exposición de este código fuente es una vulnerabilidad potencial, así que la revisión del código fuente es altamente recomendada. Artículos de interés pueden ser añadidos al reporte de la Sesión.

**Etapla del Reporte.** Esta etapa final procesa la evaluación de las vulnerabilidades y permite personalizar el reporte. La información del reporte incluye las listas de vulnerabilidades potenciales, así como la severidad de vulnerabilidades y recomendaciones verdaderas para así arreglarlas. Además de poder personalizar los reportes, usted puede exportar también los datos crudos del reporte en el formato de CSV, para un análisis adicional.

### 3.6. Funcionamiento del Sistema.

#### Consola de Administración de AppScan DE.

La Consola de Administración de **AppScan DE**, se divide en cinco secciones principales, que se muestran en la figura 3.21:



**Figura 3.21.** Consola de Administración [Sanctum, 2004].

**Sección del Mapa.** Se utiliza la sección de Mapa, para ver y navegar entre las etapas diferentes de AppScan (*Setup, Explore, Test, Results*), haciendo clic en el icono a la que pertenece cada etapa.

**Barra de Herramientas (Toolbar).** Una barra de herramientas uniforme para tareas comúnmente utilizadas, tales como Salva, Abre la sesión, Crea la sesión nueva, etc.

**Menú Bar.** La barra de Menú de **AppScan DE** tiene cinco menús, que consiste en los siguientes: *File, View, Tools, Settings and Help*.

**Panel de Instrucciones (Instruction Panel).** El Panel de Instrucciones se divide en tres áreas: El área **Entrada**, aquí es donde se proporciona a AppScan la entrada de datos necesaria para completar el paso. Área de **Navegación**, incluye los botones de *Next* y *Back* para navegar entre los pasos diferentes. Área de **Información**, proporciona una descripción corta acerca del paso y las acciones que se requirió para completarlo. En la figura 3.22 se muestra estas tres áreas:

The image shows a 'Define User Input' dialog box with the following components:

- User Name:** A text input field containing 'john', with an example 'E.g.: (Smith)' below it.
- Password:** A password input field with masked characters '\*\*\*\*', with an example 'E.g.: pass1234' below it.
- Re-enter password:** A second password input field with masked characters '\*\*\*\*', with an example 'E.g.: pass1234' below it.
- Form Properties:** A button located below the password fields.
- Navigation:** Two buttons at the bottom: 'Back' and 'Next'.
- Information:** A section at the bottom containing an information icon and a text block: 'Enter the user name and password, and use the "Form Properties" button to supply more user input (e.g., address, credit card number). This data will be used by AppScan as it explores the application.'

Arrows point from the labels 'Input', 'Navigation', and 'Information' to their respective sections in the dialog box.

**Figura 3.22.** Panel de Instrucciones [Sanctum, 2004].

**Área de Administración de Resultados (*Results Management Area*).** El Área del Administración de Resultados se utiliza para ver, manejar y procesar la producción de cada una de las etapas y pasos de **AppScan DE**.

### **3.6.1. Etapa *Setup*.**

Para realizar esta etapa, lo primero que se debe hacer es proporcionar a AppScan con información preliminar acerca del sitio y escoger el tipo de Scan que se desea realizar. Durante el proceso de *Setup*, se escoge uno de los tipos de Scan y se suministra los escenarios que determinan cómo el específico tipo de Scan se realizará. Es importante notar que las definiciones en *Setup* se salvan y se pueden volver a utilizar en sesiones futuras. El proceso de *Setup* tiene cuatro partes, para visualizar el contenido de cada parte se hace un clic a cualquiera de ellas:

#### **a) Sesión.**



***Session:*** escoger entre crear una nueva sesión y la locación donde se desea salvarla, o seguir trabajando en una sesión ya existente.

#### **b) Tipo.**



***Type:*** se escoge el tipo de Scan que se desea realizar, se puede escoger entre los dos tipos de Scan que están predefinidos o se puede crear un nuevo tipo de Scan. **AppScan DE** provee los siguientes Scans predefinidos:

**Scan Automático.** Es el tipo de Scan más completo, no requiere la intervención del usuario durante (y entre) las etapas de Exploración y Prueba, pero permite definir y configurar los parámetros de la etapa de Exploración y Prueba.

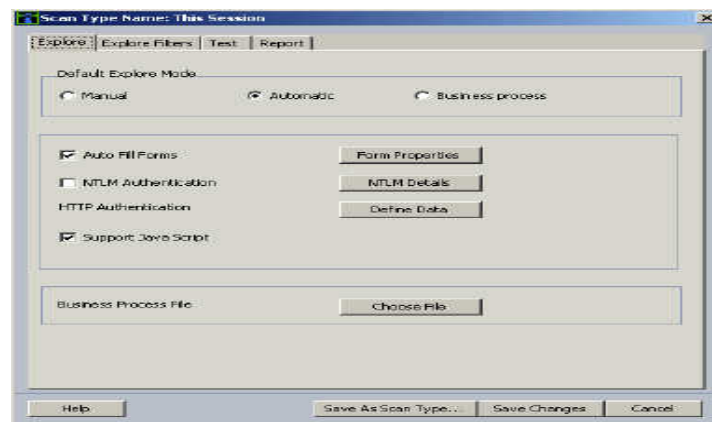
**Scan Interactivo.** Permite al usuario intervenir en el proceso de la etapa de Prueba. También permite al usuario que manualmente se exploren y prueben páginas específicas utilizando el examinador de **AppScan DE**. En la etapa de Prueba se puede volver al modo automático haciendo clic en el botón que dice “Run”.

El usuario puede modificar las propiedades de un Scan predefinido que convengan a las necesidades del usuario. Una vez que el usuario hizo esto, se puede escánear utilizando la nueva configuración (sin salvar).

**Usuario Define Tipo.** Permite seleccionar una propiedad del Scan que será salvado en el sistema. (Se activa solamente si al menos una propiedad ha sido salvada).

**Propiedades del tipo de Scan, “This Session scan type properties”.** Corre un Scan con las propiedades actuales configuradas por el usuario. (Está opción solo se activa una vez que se hicieron cambios en una predefinida (o que el usuario defina) configuración.

Cada tipo de Scan tiene una única configuración. La configuración del tipo de Scan puede ser vista y modificada en la caja de diálogo de las Propiedades del Tipo del Scan (*Scan Type Properties*), que se mostrará en la figura 3.23. Para ver o editar las propiedades del Scan se hace clic en el botón de “*Scan Type Properties*”.



**Figura 3.23.** Propiedades del tipo de Scan [Sanctum, 2004].

La caja de diálogo de las Propiedades del Tipo de Scan, contiene cuatro etiquetas. Las dos primeras contienen las propiedades del Scan para la etapa de Exploración, la tercera para la etapa de Prueba y la cuarta para la etapa de Reporte. Las secciones siguientes describen los campos y propiedades de cada una de estas etiquetas.

### **Etiqueta *Explore*.**

Hay dos etiquetas de *Explore*, la general, que aparece en la figura anterior, y que se explicara en esta parte. Y la etiqueta de “*Explore Filters*” que se explicará más adelante. Las etiquetas de *Explore* se usan para definir el Scan para la etapa de Exploración. La siguiente tabla explica cada una de las partes del contenido de la etiqueta de Exploración:

Tabla 1: Explore Tab Options

Artículo	Descripción
Default Explore Mode.	Define el modo en que se va utilizar durante la etapa de Explore, ya sea (Manual, Automatico o Business Process).
Auto Fill Forms.	Una vez seleccionado, automáticamente llenará formas necesarias para el sitio que se explora.
Form Properties button.	Abre un diálogo donde se definen los valores para utilizarlas cuando llene las formas automáticamente.
NTML Authentication.	(NT LAN Manager), se usa cuando se necesita una autenticacion NTML.
NTML Details button.	Abre una diálogo donde se pide el nombre del dominio, el usuario y password necesarios para la autenticación NTML.
HTTP Authentication define Data button.	Abre un diálogo donde se pide el usuario y password necesarios para http autenticación.
Support Jav a Script.	Cuando se selecciona se incluirá links creados de Jav a Script en la exploracion automática.
Businnes Procces File button.	Abre un diálogo que permite escoger un proceso que ha sido salvado previamente.

**Forma de Propiedades (*Form Properties*).** Cuando la caja de diálogo de “*Auto Fill Form*” es seleccionada, se llenan automáticamente formas encontradas en la etapa de Exploración. En orden para llenar las formas, se usan los valores de las formas que están definidas en la caja de diálogo de “*Form Properties*”. Esta caja de diálogo se puede ver en vista simple o avanzada. En vista simple se despliegan el grupo del nombre y los valores. En vista avanzada se despliegan dos columnas extras, para cambiar de una vista a la otra, con el segundo botón se hace clic en la caja de diálogo y aparecen las dos opciones. La figura 3.24 muestra esta caja de diálogo en vista avanzada:

Form Properties

Doubleclick on any field to type in a new value for the parameter.

Group Name	Value
Address	753 Main Street
Age	25
Area code	555
City	Mystery
Company	Acme Corp.
Country	USA
Day	01
Email	jsmith@acme.com
Month	01
Number	98765 432 18
Passport	98765 432 18
Phone	555-555-5555
Social Security	987 65 432 1
State	AK
Year	01
Zip Code	99901

User name

Username: Smith

User password

Password: Password Password Password

Help Advanced View OK Cancel

**Figura 3.24.** Forma de propiedades [Sanctum, 2004].



La Tabla siguiente explica los campos que aparecen en esta caja de diálogo:

Tabla 2: Form Properties Fields

Campo	Descripción
Group Name.	El nombre que describe el contenido.
Parameters.	Los parametros de http que se buscaran para indentificar el grupo. (Solo en Advance View).
Value.	Los valores que se asignarán con este parametro.
Match Type.	Define que tipo de match quieres usar, si el match completo o un match parcial. Por ejemplo si seleccionas match completo para el parametro Address y el parametro definido es Add, se someterá la dirección definida solo si se detecta el exacto "string" (Add) que aparece en el campo del parametro Country. Si se escoge el match parcial se agregará el valor definido cuando encuentre cualquier "string" en la forma que incluya estos "string" (Add, Addr, y Address).

Cada celda en la tabla de la caja de diálogo de “*Form Properties*” puede ser modificada o borrada, incluso se puede añadir un nuevo campo; este nuevo campo se pondrá al final de la tabla.

**Nombre del usuario y contraseña.** Este es el campo más común e importante. Notar que el nombre del usuario y contraseña son parte del paso 4 en la etapa de *Setup*.

**Definiendo los detalles de NTML.** Para definir los detalles de NTML se deben de seguir los siguientes pasos:

1. En la etiqueta *Explore* (de la caja de diálogo de “*Scan Type Properties*”), hacer clic en “*NTML Details*”. La caja de diálogo de la autenticación de NTML aparece como se muestra en la figura 3.25:



**Figura 3.25.** Autenticación de NTML [Sanctum, 2004].

2. Teclear un nombre de usuario, una contraseña y el dominio.
3. Hacer clic en OK.
4. Seleccionar la caja de diálogo de la autenticación de NTML.

#### **Etiqueta *Explore Filters*.**

En esta etiqueta se definen los filtros para una mayor rapidez y eficiencia. La siguiente Tabla explica los campos y propiedades que se presenta en esta etiqueta:

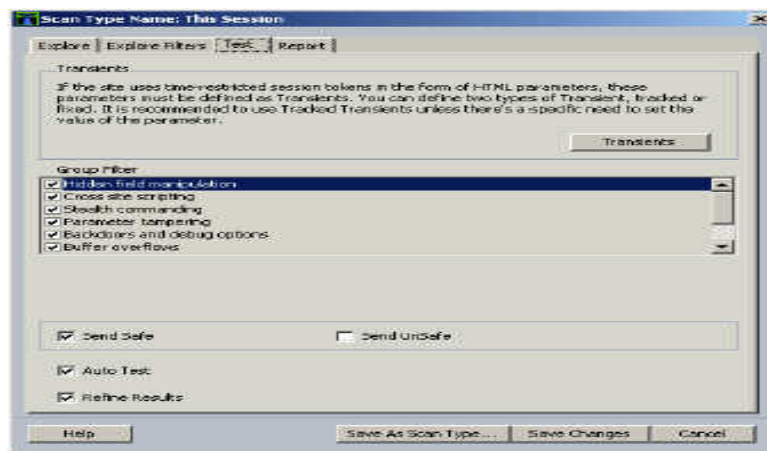
**Tabla 3: The Explore - Filter Parameter Tab Properties**

Artículo	Descripción
Limit Path.	Al seleccionarlo no se tendrá acceso al path más que el número de v es especificados.
Limit Depth.	Al seleccionarlo no se explorará links que se anidan "profundos" que el limte espicificado.
Limit Number of Links.	Al seleccionarlo la etapa de Site-Exploring esta siendo limitada por el número de links que se especifica.
Restrict Exploring to these paths.	Se restringe para explorar los paths indicados, esto es útil para el desarrollador del "scan" para definir que parte de la aplicación será escaneada.
Exclude these paths (Regular Expressions).	No se escaneará paths que emparejan las expresiones regulares entradas aquí.

**Tabla de archivos de extensión (*The File Extensión Table*).** Esta tabla contiene una lista de los tipos de archivos que no serán tomados en cuenta durante la etapa de Explore, no serán incluidos los tipos de archivos seleccionados en el Scan. La lista contiene un número de tipos de archivos defectuosos y archivos de extensiones. También se puede escoger de remover un tipo de archivo y añadir uno nuevo.

### Etiqueta *Test*.

Esta etiqueta es usada para configuraciones asociadas con la etapa de Prueba, como se muestra en la figura 3.26:

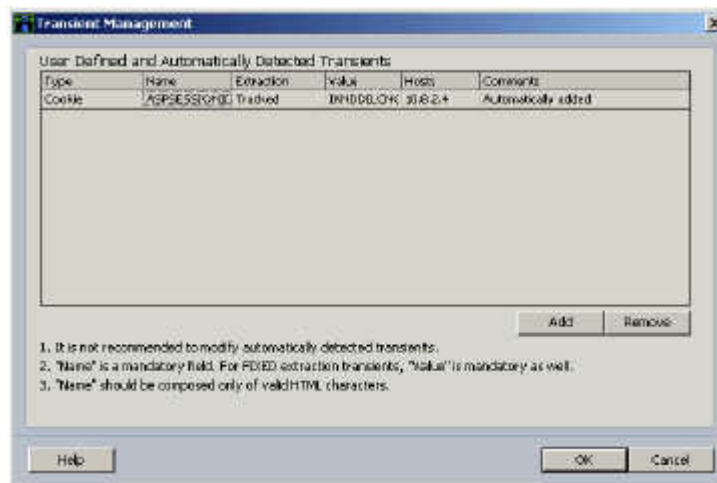


**Figura 3.26.** Etiqueta Test [Sanctum, 2004].

**Transeúntes (*Transients*).** Después que se explora un sitio, se puede escoger realizar las pruebas en un tiempo posterior. Consecuentemente, una cantidad significativa de tiempo puede pasar entre la etapa de Exploración y la etapa de Pruebas, y entre diferentes sesiones de escaneo. **AppScan DE** utiliza información almacenada en su base de datos durante la etapa de Prueba. Si el sitio utiliza muestras de identificación de sesiones con tiempo restringido (en la forma de parámetros de *cookies* o HTML), el sitio rechazará los pedidos que contienen muestras expiradas, así causará que las pruebas del sitio fallen. Por lo tanto todas muestras de sesiones con tiempo restringido en la forma de parámetros de HTML o *cookies*, se deben definir como Transeúntes.

Cuándo una muestra de sesión se define como un **AppScan DE** transitorio siempre lo asignará el valor más reciente disponible. Esto prevendrá la sesión “time out”. Durante la Exploración **AppScan DE** automáticamente detecta los parámetros de *cookies* y HTML que son probables de ser muestras de sesión, y las agregan a la lista de transeúntes. Transeúntes innecesarios se pueden borrar de esta lista antes de la etapa de la Prueba. Se pueden definir dos tipos de transeúntes, rastreado o fijo. Transeúntes fijos retienen un valor fijo. Para transeúntes rastreados, **AppScan DE** utiliza el valor más reciente encontrado dentro de la base de datos (al realizar una prueba). Se recomienda utilizar transeúntes rastreados a menos que hay una necesidad específica de poner el valor del parámetro o un *cookie*. Notar que si se utiliza transeúntes rastreados, (cuando se sospecha que la muestra de la sesión del sitio se contuvo en la base de datos, puede haber expirado,) actualice la base de datos con un valor más reciente antes de probar el sitio.

Para actualizar la base de datos, visita simplemente la página en el sitio Web donde una muestra de sesión se manda (por ejemplo, una página de la entrada). Un clic en el botón de los Transeúntes abrirá la tabla Transitoria de administración, como se muestra en la figura 3.27:



**Figura 3.27.** Tabla Transitoria [Sanctum, 2004].

La siguiente Tabla describe las propiedades de la tabla Transitoria de Administración:

Tabla 4: Transient Management

Campo	Descripción
Type.	Los tipos de Transient son: Cookie y HTML parametros.
Parameter Name.	Nombre del parametro o cookie.
Extraction.	Los tipos de extracciones de la Transient son: Traked: el valor del traked es actualizado por el más reciente valor que se encontró para este parametro o el cookie.
Value.	Valor del parametro o del cookie (para extracciones tipo fixed).
Host.	Se puede dejar vacío, si se deja vacío se utilizará los transients para todos los hots relevantes. Cuando un host específico es definido se utilizará los transients solo para el host definido.
Comments	Para comentarios del usuario.

Para añadir un Transeúnte se siguen los pasos siguientes:

1. En la pantalla de Propiedades de Tipo de Scan, hacer clic en la etiqueta de Prueba después hacer clic en Transeúntes. Se abre la tabla Transitoria de Administración como se ve en la figura anterior.
2. Hacer clic en *Add*. Una fila nueva se añade a los Transeúntes.
3. Llenar los campos para el Transeúnte nuevo, como se refiere en la tabla anterior.
4. Hacer clic en *OK*. El Transeúnte nuevo se agrega.

Para modificar un Transeúnte se siguen los pasos siguientes:

1. Editar los campos en la tabla de Transeúntes.

Para borrar un Transeúnte se siguen los pasos siguientes:

1. De la tabla Transitoria de Administración, hacer clic en el record o registro transitorio que se quiere remover.
2. Hacer clic en *Remove*. El Transeúnte se borra de la lista.

**Lista del Grupo de Filtros (*Group Filter List*).** Durante la etapa de Prueba se corren una serie de pruebas para checar y analizar la seguridad del sitio. En el grupo hay nueve categorías, cuando se selecciona una de estas categorías está será incluida en la etapa de Prueba. El Área del grupo de filtros se muestra en la figura anterior y los filtros son explicados en la siguiente tabla, al igual que estas categorías son explicadas y mejor detalladas en el capítulo 4.

Tabla 5: Group Filter Checkboxes.

Nombe del Ckeckbox.	Descripción.
Hidden field manipulation	Modificación de las campos de formas, estos permiten el daño de datos que alcanza la aplicación web.
Cross site scripting	Inserta lenguajes encriptados en campos de textos para así mostrar información a otros usuarios.
Stealth commanding	Plantear Caballos de Trojan en un campo de texto, haciendo que la aplicación web realicé ordenes que no debe hacer.
Parameter tampering	Modificación de parametros que son parte del URL.
Backdoor and debug options.	Explotación de vulnerabilidades que se dejaron abiertas durante la etapa de desarrollo del código del sitio web.
Buffer overflows	Sobrecargar el sitio web con una simple petición.
Cookie Poisoning	Modificación de archivos de cookies para tener acceso a información sensible o realizar actividades a fav or un usuario diferente.
Suspicious Content	Durante la etapa de Test, se puede también buscar contenido sospechoso.

**Filtros Adicionales.** Cada una de estas categorías de pruebas incluye un rango de prueba que puede ser mostrado en el sitio. En el área de filtros adicionales se define que tipo de prueba en cada categoría será mandado. El área de filtros adicionales se muestra en la figura anterior y la siguiente tabla explica sus funciones:

Tabla 6: Additional Filter Checkboxes

Campo	Descripción
Send Safe Test requests.	Al seleccionarlo se mandará solo las peticiones seguras de la prueba, las que no pueden causar daño al sitio web.
Send Unsafe Test requests.	Al seleccionarlo mandará las peticiones inseguras, las que pueden causar daño al sitio web.
Auto Test	Al seleccionarlo se avanzará automáticamente a la siguiente etapa.
Refine Results	Al seleccionarlo se realizará procesos internos del refinamiento de resultados para aumentar la certeza del resultado.

### Etiqueta Report.

Esta etiqueta es usada para filtrar el contenido que aparecerá en el Reporte del Resultado del Scan.

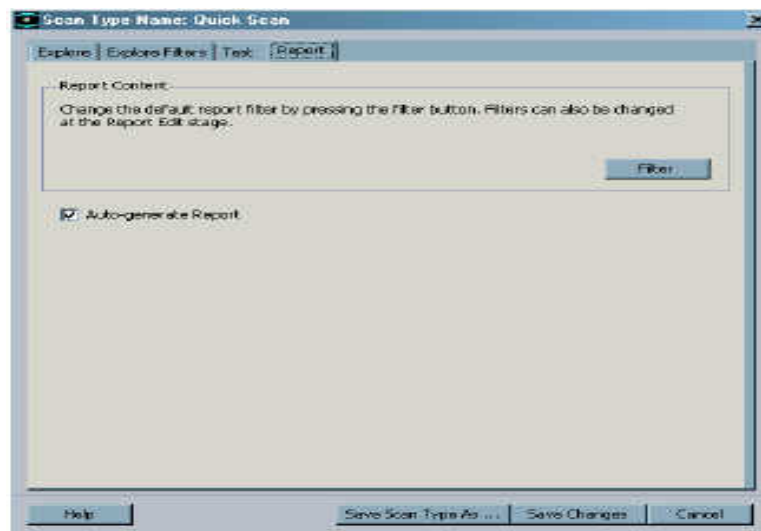
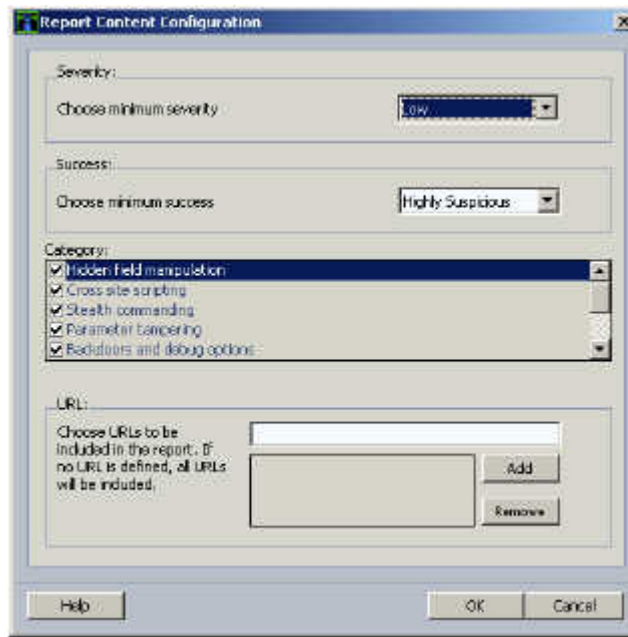


Figura 3.28. Etiqueta Report [Sanctum, 2004].

Cuando se selecciona la opción de generar el reporte automáticamente, **AppScan DE** genera de manera automática un reporte del Scan después que la etapa de Prueba esta completa.

Para filtra el contenido del Reporte:

1. En la etiqueta Reporte, hacer clic en “*Filter*”. Aparece una caja de diálogo con la configuración del contenido del Reporte:



**Figura 3.29.** Configuración del contenido del reporte [Sanctum, 2004].

2. Del Área de “*Severity*”, seleccionar el nivel de severidad que se quiere obtener (*High/ Medium/Low*).
3. Del Área de “*Success*”, seleccionar el nivel de los sucesos que se quiere obtener (*Vulnerable/ Highly Suspicious/ Not Vulnerable*).
4. Del Área de las categorías, limpiar alguna categoría que se quiere excluir del reporte.
5. Si se quiere que en el reporte se incluya solo los resultados de un URL específico, entonces especificar el URL en la caja de texto y hacer clic en “*Add*”.



**Salvar los cambios en el tipo de Scan.** Después de definir la configuración en el tipo de Scan, se puede salvar los cambios de la sesión en uso; esto se hace, haciendo clic en el botón de “*Save Changes*”. También se puede salvar la configuración permanentemente bajo un nuevo nombre haciendo clic en el botón de “*Save Scan Type As*”.

### c) Aplicación.



**Application:** se define la aplicación que se quiere scanear y el punto de partida que el proceso de Scan realizará.

**Definir el servidor o servidores que serán escaneados.** Sobre el título de “*type the server to be scanner*”. Por ejemplo: <http://www.sanctuminc.com/>.

Para añadir servidores a la lista se siguen los pasos siguientes:

1. Seleccionar “*Additional Server*”.
2. En la caja de texto de “*Additional Server*”, poner el servidor adicional que se quiere agregar.
3. Hacer clic en “*Add*”.

Para remover servidores de la lista se hace lo siguiente:

1. De la lista de servidores, seleccionar el servidor que se quiere remover.
2. Hacer clic en “*Remove*”.

**Definir el punto de partida del Scan.** Hay dos maneras para definir el punto partida:


- La primera es muy simple, teclear la dirección en la caja de texto de “*server to be scanned*”.
- La segunda opción es manual, esto se hace de la siguiente manera:

1. En el panel de instrucciones hacer clic en “Show”.

La página de punto de partida aparece en el área de administración de **AppScan DE**, como se muestra en la figura 3.30:



**Figura 3.30.** Página del punto de partida [Sanctum, 2004].

2. Usar la barra de navegación del área de administración para examinar el sitio y localizar el punto de partida del Scan.
3. Hacer clic en  para mandar la página en uso como el punto de partida.

#### d) Entrada.



**Input:** provee a **AppScan DE** con la información del usuario, tales como, nombre del usuario y contraseña o acceder a la caja de diálogo de “*Form Properties*”, antes de proceder a la etapa de Pruebas. Esto puede ser requerido para ciertas áreas en la etapa de pruebas.

Hay una opción avanzada que permite seleccionar una sesión de ingreso manualmente para casos donde la sesión de ingreso automática puede no ser suficiente, esto lo veremos más adelante. En la figura 3.31 se muestra la sesión de ingreso:



**Figura 3.31.** Datos de ingreso [Sanctum, 2004].


**Opciones de la Sesión de Ingreso.** Durante la etapa de Exploración **AppScan DE** identifica el proceso de ingreso. El botón de “*Session Login button*”, aparece en la barra de herramientas del examinador durante la sesión de ingreso o “*Input*”.

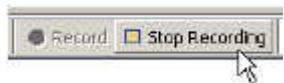
Esta opción permite cambiar el ingreso de datos de Automático a Manual o No ingresar datos. La figura 3.32 muestra estas opciones, al cual se accede haciendo clic en el botón de “*Session Log*”:



**Figura 3.32.** Opciones de la sesión de ingreso [Sanctum, 2004].

**Ingresar Manualmente.** Se selecciona ingresar manualmente si se quiere hacer peticiones de ingreso para grabaciones manuales, que **AppScan DE** usará para ingresar al sitio instantáneamente a la petición de la grabación automáticamente durante la etapa de Exploración. Para grabar una petición de ingreso manual se siguen los siguientes pasos:

1. Seleccionar “*Manual Login*” de la lista del botón de “*Session Log*”, el examinador se abre y va al punto de partida.
2. Examinar manualmente hasta llegar a la página de ingreso.
3. Apretar  .
4. Llenar los campos de ingreso como sea necesario. Si el ingreso envuelve mas de una forma, ir a cada forma (usando el examinador) y llenar los datos (manualmente) antes de para la grabación.
5. Una vez que se han llenado todas las formas requeridas, apretar



Los datos de ingresos grabados serán usados (automáticamente) para ingresar dentro del sitio para la etapa de Prueba.

### 3.6.2. Etapa de Exploración.

La primera parte en el proceso de **AppScan DE** es la Exploración. **AppScan DE** explora el sitio y construye un modelo de las aplicaciones que se corrieron en él. También crea una lista de las vulnerabilidades potenciales, basándose en las vulnerabilidades potenciales identificadas, **AppScan DE** crea Pruebas para verificar las vulnerabilidades actuales del sitio. La etapa de Exploración esta subdividida en dos partes:

### a) Correr.



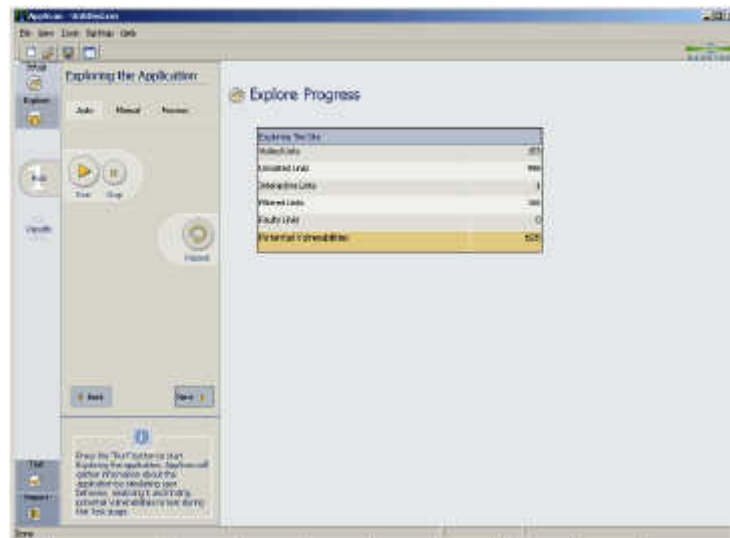
**Run:** manda peticiones a la aplicación (“*Explore the Site*”) y colecciona las respuestas de esas peticiones. Esto se puede hacer automáticamente, o manualmente, incluso se puede escoger una de las aplicaciones del proceso. Basado en las respuestas que recibe de la aplicación, se prepara una lista de peticiones de Pruebas, las cuales serán mandadas durante la etapa de Prueba. Cuando se “corre” el proceso de Exploración, **AppScan DE** inicia el Scan de la “Página inicial” que se escogió durante la etapa de *Setup*. De ahí, se explora el sitio metódicamente visitando cada liga o “*link*” con la aplicación hasta que haya visitado cada liga con la aplicación. La exploración automática es mucho más rápida que la exploración manual, ya que así, se pueden visitar miles de ligas en segundos. Es importante notar que el criterio que se dio en la etapa de *Setup* define los límites del proceso de Exploración. Por ejemplo, si el límite que se dio fue de 5 ligas, no se visitarán más que 5 ligas iniciando del punto de partida.

**Peticiones de Exploración que abren una pantalla.** El panel de instrucciones de la petición inicial abre una pantalla con botones de inicio, parar y repetir el proceso de Exploración. Incluso muestra la configuración del punto de partida de la Exploración. La información desplegada en el área de administración de resultados depende del tipo de Scan que se selecciono en la etapa de *Setup*.

La Exploración puede darse en Automático, Manual o en el modo de proceso. Una vez que la Exploración dio inicio, para cambiar a un modo diferente de exploración, primero se necesita para la exploración en curso, y luego seleccionar el nuevo modo de exploración.

**Exploración Automática.** Una vez que el Scan fue propiamente configurado e iniciado a correr en el modo Automático, todo lo que se tiene que hacer es iniciar el Scan y dejar que **AppScan DE** haga el resto.

Como la etapa de Exploración progresa, el contador en la tabla del progreso de la Exploración indica que tanto ha progresado. Como se muestra en la figura 3.33:



**Figura 3.33.** Exploración automática [Sanctum, 2004].

Para iniciar la Exploración Automática se deben seguir los siguientes pasos:

1. Para proceder en la etapa de Exploración (habiendo completado la etapa de *Setup*) presionar **Next**.
2. Presionar **Run**.

Exploring The Site	
Visited Links	153
Unvisited Links	998
Interactive Links	1
Filtered Links	106
Faulty Links	0
Potential Vulnerabilities	625

**Figura 3.34.** Tabla de progreso [Sanctum, 2004].

El contador en la tabla del progreso de la Exploración crece cuando las peticiones iniciales son mandadas.

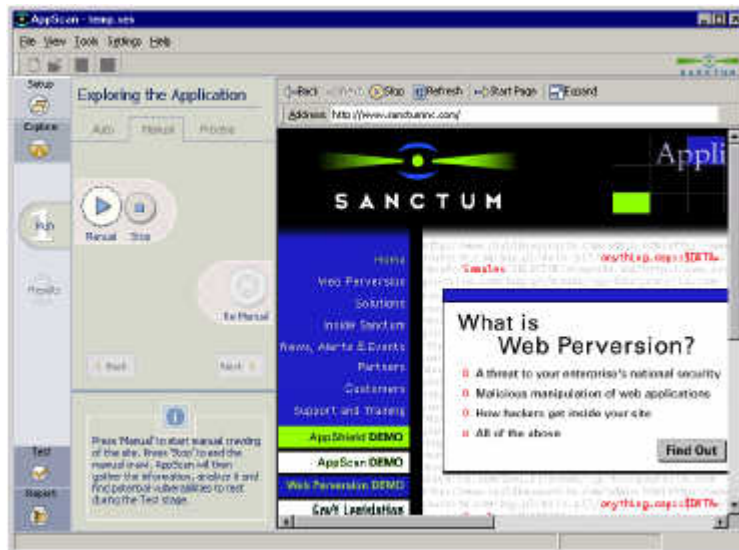
3. Espera hasta que el contador deja de crecer y el botón de *Next* se vuelve activo, esto indica que el proceso de Exploración esta completo, o para parar la Exploración antes de que este completo presionar *Stop*.
4. Para proceder con los resultados iniciales, presionar *Next* en el panel de instrucciones. Una vez que Exploración esta completa se inicia automáticamente con la etapa de Pruebas.

**La tabla del progreso de la Exploración.** Cuando la Exploración esta completa, la tabla de progreso de la Exploración resume las exploraciones que se hicieron. La figura anterior muestra esta tabla, y la siguiente tabla muestra como se explica cada campo de la tabla de progreso de la Exploración.

Tabla 7: Explore Progress table summary

Artículo	Descripción
Visited links.	Número de links que se han visitado hasta ahora.
Unvisited links.	Número de links que se tienen que visitar durante el proceso de Exploring.
Interactive links	Número de links que requieren alguna entrada que no se puede llenar automáticamente.
Filtered links	Número de links que no se exploraron porque ellos fueron filtrados fuera de la línea de la etapa de Explore, o por un defecto del filtro.
Faulty links	Número de links totales que no respondieron a la petición inicial.
Potential vulnerabilities	Peticiones que fueron indentificadas como vulnerabilidades potenciales durante el proceso de Explore y que serán probadas durante la etapa de Test.

**Exploración Manual.** Si se desea escánear el sitio manualmente, hacer clic en “*Manual*” para abrir el examinador de **AppScan DE** en la ventana de administración. Como se muestra en la figura 3.35:



**Figura 3.35.** Exploración Manual [Sanctum, 2004].

La siguiente Tabla explica los botones del examinador:

**Tabla 8:** AppScan Browser buttons

Botón.	Descripción
Back	Página anterior.
Next	Página Siguiente.
Expand / Collapse (toggle)	Muestra el Browser como una ventana separada (muestra el progreso de la tabla de la etapa de Explore en el área de la Administración/ Muestra el Browser en el área de la Administración en vez del progreso de la tabla de la etapa de Explore).
Stop	Para de mandar la petición actual.
Refresh	Refresca la página.
Start Page	Regresa al punto de inicio de la página.
Auto Scan	Cierra el Browser e inicia automáticamente la etapa de Explore.
Finish	Cierra el Browser.



Para la Exploración Manual, se deben de seguir los pasos siguientes:

1. Usar el examinador de **AppScan DE** para hacer clic en las ligas que se quieren visitar. Por cada petición mandada, automáticamente se clasifican las respuestas y se generan peticiones de Prueba. Notar que una vez que el la exploración ha iniciado, para cambiar a un modo diferente primero se debe parar la exploración, y luego seleccionar un nuevo modo de exploración.
2. Para cerrar el examinador, hacer clic en **Finas** en la barra de herramientas del examinador.
3. Para proceder con los resultados iniciales, hacer clic en **Next** en el panel de instrucciones.

**Proceso del Negocio (*Business Proccess*).** Una tercera opción para escánear tu sitio, es escánear una específica transacción o proceso dentro de la aplicación.

Para crear un archivo “.bps” para una porción deseada de la aplicación, se siguen el paso siguiente:

1. En la etapa de Exploración, seleccionar la etiqueta de **Proccess** (en el panel de instrucciones).



2. Si se desea conjuntar un punto de partida diferente, hacer clic en “*browser*” en la etiqueta de proceso. El examinador aparece mostrando la aplicación seleccionada. (Opcional).
3. Manualmente explora el sitio para el punto de partida deseada. (Opcional).



4. En la etiqueta de proceso hacer clic en .
5. Manualmente explora todas las secciones relevantes del sitio.



6. En la etiqueta de proceso hacer clic en para parar la fase de grabación.

Una lista de las peticiones grabadas es presentada, como se muestra en la figura 3.36:




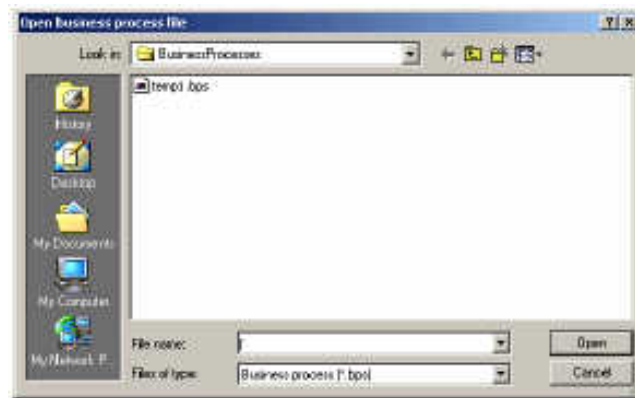
**Figura 3.36.** Lista de peticiones grabadas [Sanctum, 2004].

7. Hacer clic en *Save* para salvar la exploración grabada. Clic en *Continue* para continuar grabando, o *Discard* para cancelar cualquier cambio o reiniciar la sesión de los resultados de la exploración.
8. En la caja de diálogo de “*Save recorded data*”, teclear el nombre del archivo para el proceso grabado (.bps) y dar salvar.


La exploración grabada esta ahora salvada como archivo de proceso en el fólder de *Business Proccess*. Notar que las ligas visitadas durante este proceso de exploración son añadidos como ligas visitadas manualmente de la sesión en uso.

Para Explorar un proceso se deben seguir los pasos siguientes:

1. Cuando se esta en la etapa de Exploración, seleccionar la etiqueta de **Proccess** (localizada en el panel de instrucciones).
2. En la etiqueta de **Proccess**, hacer clic en . Cuando se abre la caja de diálogo del Proceso, aparece en la figura 3.37:



**Figura 3.37.** Abrir un proceso [Sanctum, 2004].

3. Seleccionar el proceso que se desea bajar.
4. Hacer clic en **Open**, el proceso seleccionado ha sido bajado.
5. En la etiqueta de **Proccess**, clic en . **AppScan DE** explora el proceso seleccionado.

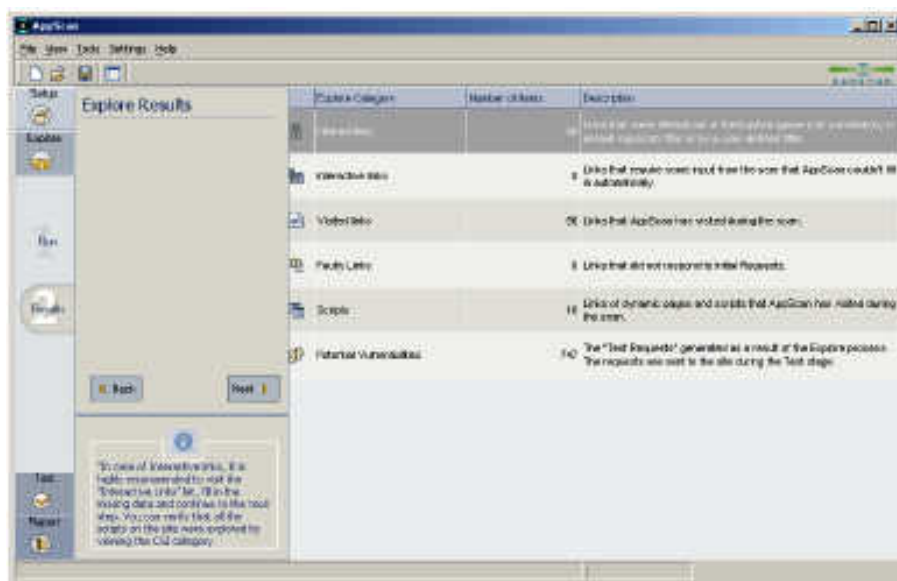
**Conflicto con el Host.** Si se encuentra en una situación de conflicto con el *Host*, se escoge bajar un proceso salvado en la etapa de Exploración, y el *Host* configurado no está definido en el proceso que se selecciono, se puede hacer:

1. Ignorar el *Host* salvado.
2. Añadir el *Host* grabado a la lista de servidores de la exploración.
3. Durante la exploración, reemplazar el *Host* salvado con el *Host* que está en uso.

## b) Resultados.



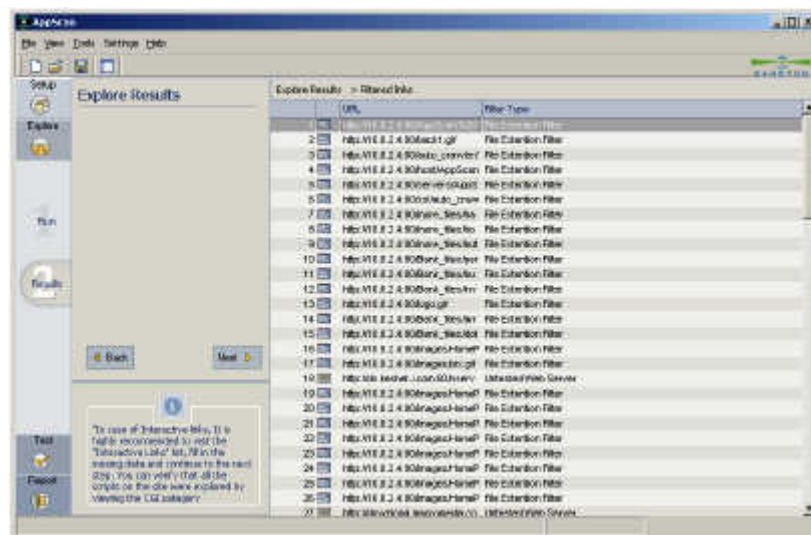
**Results:** los resultados de la etapa de Exploración son una manera de evaluar para determinar si el escáneo fue preciso y comprehensivo como se quiso. La página de los resultados de la Exploración es una versión interactiva de la tabla final del Progreso de la Exploración (con la excepción de las ligas no visitadas, lo cual no es relevante en los resultados). Da la oportunidad de examinar las peticiones que fueron mandadas, las peticiones que no fueron mandadas, y cualquier parámetro que fue mandado con la petición (u otras ligas interactivas). Si es necesario se puede mandar o volver a mandar peticiones antes de la etapa de Prueba. Una reexaminación de las vulnerabilidades potenciales encontradas durante los resultados en la etapa de Exploración es recomendada, porque estas serán probadas durante la etapa de Pruebas. Cuando se examina los resultados de la Exploración, se puede hacer clic en **Analysis Category** para más información sobre los artículos actuales en esa categoría. Para más información sobre cualquier artículo hacer clic en la lista, hacer clic en ese artículo. En la figura 3.38 se muestra la página de los resultados de la Exploración:



**Figura 3.38.** Resultados de la exploración [Sanctum, 2004].

**Ligas Filtradas.** La lista de ligas filtradas muestra las ligas que no fueron visitadas porque fueron filtradas fuera. Se puede examinar las ligas de esta lista y si se desea se puede hacer manualmente. Los valores de la tabla de los resultados en la Exploración serán actualizados acordeamente. Para explorar las ligas filtradas se siguen los siguientes pasos:

1. En la lista de los resultados de la Exploración, hacer clic en ***Filtered Links***. La lista completa de las ligas filtradas aparece así:



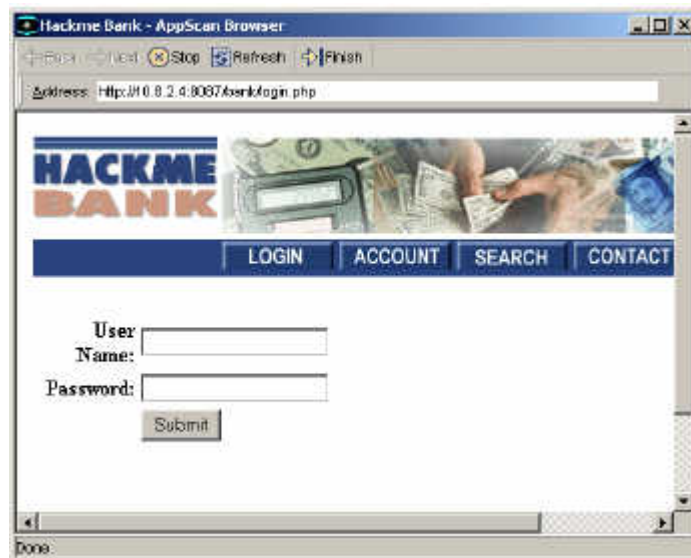
**Figura 3.39.** Ligas filtradas [Sanctum, 2004].

Hacer clic en la liga que se quiere visitar. El examinador se abre, y se manda la petición.

2. Para regresar a los resultados de la Exploración, clic en ***Explore Results*** en la barra de navegación. Los resultados de la Exploración están actualizados para ser incluidas las peticiones mandadas.

**Ligas Interactivas.** La lista de las ligas interactivas muestra las peticiones que no fueron mandadas, porque ellas requieren entradas del usuario que no se hicieron durante la etapa de *Setup*. Exactamente cuales ligas se clasifican como “Interactivas” depende del tipo de Scan que se selecciono durante la etapa de *Setup*. Se puede examinar las ligas interactivas, y si se quiere se puede requerir la información del usuario y mandarla manualmente. Los números de la tabla de resultados de la Exploración serán actualizados acordemente. Se recomienda que se examinen muy bien la lista de las ligas interactivas, llenar los datos requeridos y mandar esas peticiones. Entonces se incluirá esas ligas durante la fase de prueba. Después de visitar las ligas interactivas se puede continuar con el proceso de Exploración. Incluso si previamente se completo el proceso de Exploración, nuevas ligas serán añadidas y el botón de Exploración se vuelve activo otra vez. Para explorar una liga interactiva se siguen los pasos siguientes:

1. En la lista de Resultados de la Exploración, hacer clic en ***Interactive Links***. La página de la lista completa con las ligas interactivas aparece.
2. Hacer clic en el URL requerido. El examinador abre la página seleccionada, como se muestra en la figura 3.40:



**Figura 3.40.** Página de la lista completa con las ligas interactivas [Sanctum, 2004].

3. Para cerrar el examinador, hacer clic en ***Finish***.
4. Para regresar a los resultados de la Exploración, hacer clic en ***Explore Results*** en la barra de navegación, en la parte de arriba en el área de administración. Los resultados de la Exploración se actualizaron para incluir las formas mandadas. Notar que desde que la liga interactiva se mandó, puede haber abierto una nueva parte del sitio, es muy recomendable que se resuma y complete el proceso de la Exploración después de haber mandado una liga interactiva.

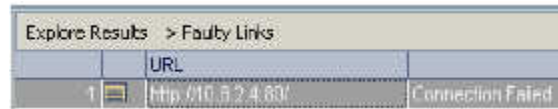
**Ligas Visitadas.** Las ligas visitadas son peticiones por las cuales **AppScan DE** recibe una respuesta inicial válida. Basada en esas respuestas se generan las peticiones de Prueba, peticiones diseñadas para revelar las debilidades en el sitio, que serán mandadas durante la etapa de Pruebas. Si un número pequeño de ligas o páginas fueron cambiadas en el sitio después del Scan, tal vez se quiera volver a mandar algunas peticiones manualmente, en vez de volver a correr todo el proceso de la Exploración de nuevo. Para explorar las ligas visitadas se debe seguir los pasos siguientes:

1. En la lista de resultados de la Exploración, clic en ***Visited Links***. La lista de ligas visitadas aparece, y se puede volver a mandar cualquier petición de nuevo haciendo clic en ella.
2. Para regresar a los resultados de la Exploración, clic en ***Explore Results*** en la barra de navegación en la parte de arriba en el área de administración.

**Ligas No Válidas.** Las ligas no válidas o ***Faulty Links*** son esas peticiones donde la petición fue mandada pero no hay una respuesta válida. Usualmente es un problema de comunicación, ya sea que el sitio este sin red, o cuando la liga se ha roto (ligas con una página no existente). Si una liga importante es listada como no válida, se puede volver a mandar la petición manualmente, en vez de repetir todo el proceso. Para volver a mandar una liga no válida se siguen estos pasos:

1. En la lista de resultados de la Exploración, clic en ***Faulty Links***.

La lista de ligas no válidas aparece. Luego para cada URL, **AppScan DE** los lista como no válidos, como se muestra en la figura 3.41:



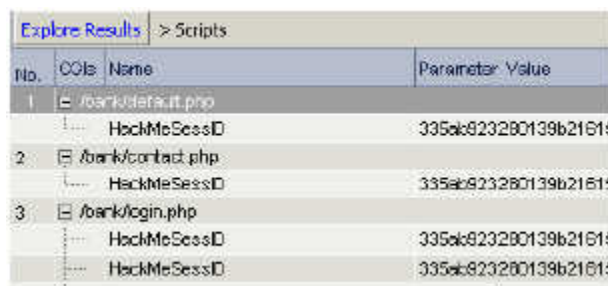
Explore Results > Faulty Links		
	URL	
1	http://10.0.2.4:80	Connection Failed

**Figura 3.41.** Lista de ligas no válidas [Sanctum, 2004].

2. Para volver a intentar con una liga, hacer clic en ella. El examinador de **AppScan DE** se abre y manda la petición seleccionada. Se puede continuar con la Exploración de esta manera como se desee, todas la peticiones mandadas son añadidas a los resultados de la Exploración.
3. Para regresar a los resultados de la Exploración, clic en **Explore Results**. Los resultados de la Exploración se actualizaron para incluir las peticiones mandadas.

**Scripts.** Se lista un *Scripts* todas las peticiones iniciales que incluye uno o más parámetros. Estos son las ligas más vulnerables para tener un ataque informático. Para cada petición se puede examinar los parámetros de nombre, valor (es) y tipo. Para examinar un *Script* se siguen estos pasos:

1. En la lista de resultados de la Exploración, clic en **Script**. La lista de ligas *Script* aparece, y con cada URL están los parámetros de nombre, valor (es) y tipo, como se muestra en la figura 3.42:



Explore Results > Scripts		
No.	CGIs Name	Parameter Value
1	/bank/default.php	HackMeSessID 335ab923280139b21615
2	/bank/contact.php	HackMeSessID 335ab923280139b21615
3	/bank/login.php	HackMeSessID 335ab923280139b21615

**Figura 3.42.** Lista de resultados de la exploración [Sanctum, 2004].

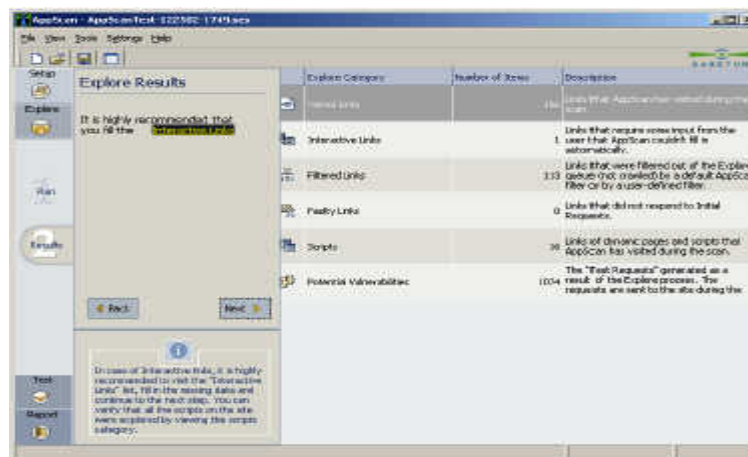


Notar que hay más de un parámetro para cada URL, los parámetros son listados uno seguido del otro. Donde hay más de un valor para un particular parámetro de nombre, los valores son separados por comas.

2. Para regresar a los resultados de la Exploración, clic en **Explore Results**. Los resultados de la Exploración se actualizaron para incluir las peticiones mandadas

**Vulnerabilidades Potenciales.** El artículo final en la tabla de resultados de la Exploración es más que un conjunto de resultados, contiene las peticiones propuestas para la Prueba, que **AppScan DE** generó basado en los resultados de la Exploración. Se puede observar el número de las Vulnerabilidades Potenciales generadas en cada categoría, como mirar cada petición de Prueba como URL. Para examinar las vulnerabilidades potenciales se siguen estos pasos:

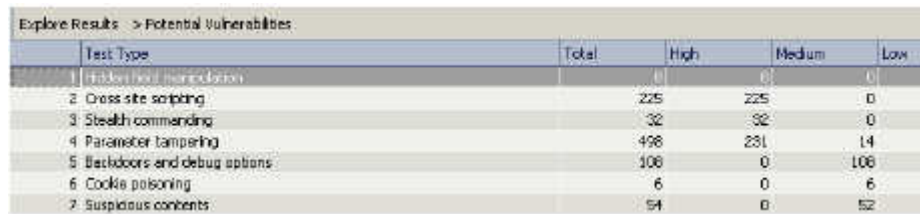
1. En la lista de resultados de la Exploración, clic en **Potential Vulnerabilities**. La lista de vulnerabilidades potenciales provee un resumen con las ligas para detallar sobre las vulnerabilidades potenciales detectadas como se mostrará en la figura siguiente. Luego para cada categoría que esta sobre la columna de *Test Type* es el número total de vulnerabilidades potenciales en esa categoría. A la derecha de los totales están los números de peticiones las cuales están en un nivel de *High (H)*, *Medium (M)* and *Low (L) Severity*. Como se ve en la figura 3.43:



Explain Category	Number of Items	Description
Invalid Links	14	Links that AppScan couldn't visit during the scan.
Interactive Links	1	Links that require some input from the user that AppScan couldn't fill in automatically.
Filtered Links	113	Links that were filtered out of the Explore phase not covered by a default AppScan filter or by a user-defined filter.
Fuzzily Links	0	Links that did not respond to initial requests.
Scripts	36	Links of dynamic pages and scripts that AppScan has visited during the scan.
Potential Vulnerabilities	1004	The "Test Requests" generated as a result of the Explore process. The requests are sent to the site during the

**Figura 3.43.** Vulnerabilidades potenciales [Sanctum, 2004].

2. Para examinar una vulnerabilidad potencial específica en una categoría, clic en la Categoría, como se muestra en la figura 3.44:



Test Type	Total	High	Medium	Low
1. Unauthenticated authentication	0	0	0	0
2. Cross site scripting	225	225	0	0
3. Stealth commanding	32	32	0	0
4. Parameter tampering	498	231	14	0
5. Backdoors and debug options	108	0	108	0
6. Cookie poisoning	6	0	6	0
7. Suspicious contents	54	0	52	0

**Figura 3.44.** Examinar una vulnerabilidad potencial [Sanctum, 2004].

3. Para regresar a la lista de categorías, clic en *Potential Vulnerabilities*.
4. Para regresar a la tabla principal de resultados de la Exploración, clic *Explore Results*.

### 3.6.3. Etapa de Prueba.

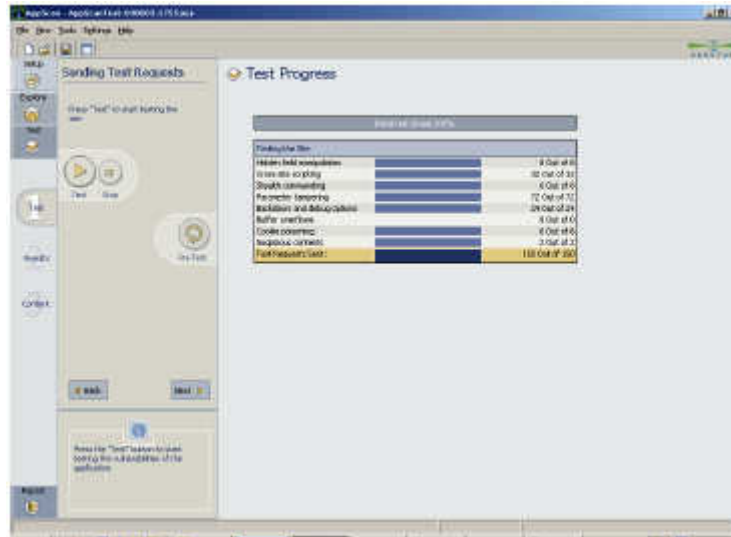
La segunda parte en el proceso de **AppScan DE** es la etapa de Prueba, en la cual se usa la información generada durante la etapa de Exploración para probar el sitio. La etapa de Prueba esta subdividida en tres partes:

#### a) Prueba.



**Test:** primero **AppScan DE** manda varias (Pre-Pruebas) peticiones al sitio (tales como, peticiones de ingreso), para mejorar la eficiencia de la Prueba. Luego da inicio a mandar peticiones de las Pruebas, las cuales están diseñadas a revelar los riesgos de seguridad en el sitio.

**Correr la Prueba.** La pantalla inicial de las peticiones de Prueba muestra una tabla de categorías. Luego para cada categoría se puede ver el número de las Pruebas propuestas en esa categoría, como se muestra en la figura 3.45:





**Figura 3.45.** Correr la prueba [Sanctum, 2004].

Cuando se presiona el botón de **Test**, AppScan DE hace lo siguiente:

- Ingresa a donde sea en la aplicación que requiera autenticación.
- Realiza varias pruebas preliminares en los URL's que ayuda a interpretar los resultados de la Prueba.
- Iniciar a probar URL's en el sitio mandando las peticiones de la Prueba "*Test Requests*" (peticiones diseñadas a revelar las vulnerabilidades actuales) y grabando las respuestas del sitio para cada petición. (Las peticiones de la Prueba fueron creadas durante la etapa de Exploración, basándose en las vulnerabilidades potenciales descubiertas).

Para iniciar a probar el sitio, se deben seguir los pasos siguientes:

1. Hacer clic en el botón de **Test** .
2. Para examinar los resultados hacer clic en .

La pantalla interactiva de resultados aparece, con un resumen de todas las pruebas, agrupadas por Resultados, como se muestra en la figura 3.46:

The screenshot shows the 'Test Results' window in AppScan. The table 'Tests Grouped By: Result\*' has the following data:

No.	Name	Test Requests	Vulnerable	Highly Suspicious	Suspicious
2	Not Vulnerable	170	0	0	0
3	Suspicious	27	0	0	27

**Figura 3.46.** Resultados de la prueba [Sanctum, 2004].

Usar la lista de las Pruebas Agrupadas para seleccionar un método de un grupo diferente, como se ve en la figura 3.47:

The screenshot shows the 'Test Results' window with a context menu open over the 'Tests Grouped By' table. The menu options are: Result\* (checked), Category, Safety, Severity, Link, Name, and Auto/Manual.

No.	Name	Test Requests	Vulnerable	Highly Suspicious	Suspicious	Not Vulnerable
1	Not tested	0	0	0	0	0
2	Not Vulnerable	0	0	0	0	166

**Figura 3.47.** Lista de las pruebas agrupadas [Sanctum, 2004].

3. Hacer clic en un artículo de la tabla para ver todas las Pruebas que pertenecen a ese grupo.

## b) Resultados.



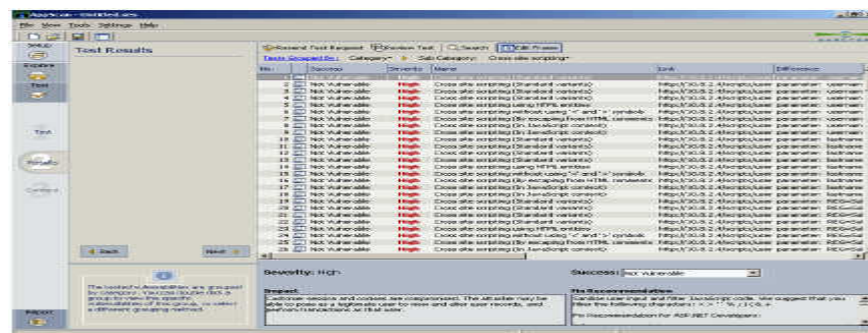
**Results:** después que las pruebas están completas se puede ver y analizar los resultados en varios grupos. Hay numerosas opciones disponibles en esta fase, por ejemplo, se puede observar pruebas individuales y consejos que explican el problema descubierto, los cuales se pueden editar para imprimir un Reporte. Incluso se puede comparar los resultados de la Prueba del sitio con los resultados recibidos durante la etapa de Exploración. Los resultados se pueden observar en tres niveles:

- Nivel 1: Un resumen de todos los resultados, agrupados de acuerdo con el método de agrupación que se seleccionó, es desplegado. Solo el número de resultados por grupo es mostrado, como se muestra en la figura 3.48, no los resultados actuales.

No.	Name	Test Requests	Vulnerable	Highly Suspicious	Suspicious	Not Vulnerable
1	Multiple (all vulnerabilities)	0	0	0	0	0
2	Cross site scripting	242	0	0	0	32
3	SQLi	37	0	0	0	9
4	Parameter tampering	602	0	0	0	69
5	Backdoors and debugging	132	0	0	0	68
6	Cookie poisoning	6	0	0	0	0
7	Suspicious contents	47	0	0	27	0

**Figura 3.48.** Resumen de resultados [Sanctum, 2004].

- Nivel 2: Todos los resultados con un grupo seleccionado es desplegado, como se muestra en la figura 3.49:



**Figura 3.49.** Resultados con un grupo seleccionado [Sanctum, 2004].

- Nivel 3: Resultados Detallados. La “tarjeta índice” para un resultado individual es desplegado, como se muestra en la figura 3.50:

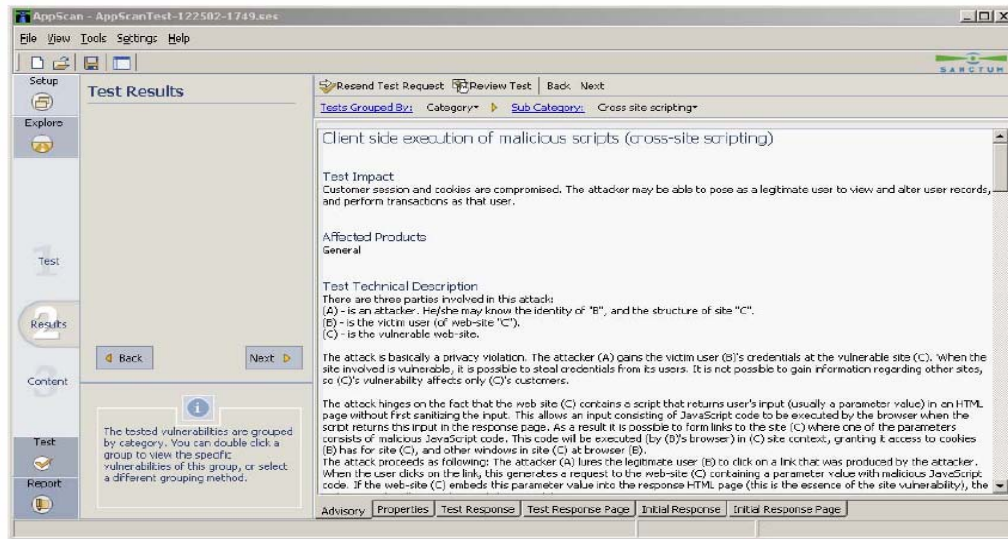


Figura 3.50. Resultados detallados [Sanctum, 2004].

**Métodos Agrupados.** La página de los resultados de la Prueba se abre por default con una lista de nivel 1 de los resultados de la prueba agrupados por Resultado. El menú de *Grouping Methods* deja seleccionar diferentes métodos agrupados para los resultados de la Prueba, como se muestra en la siguiente figura 3.51:

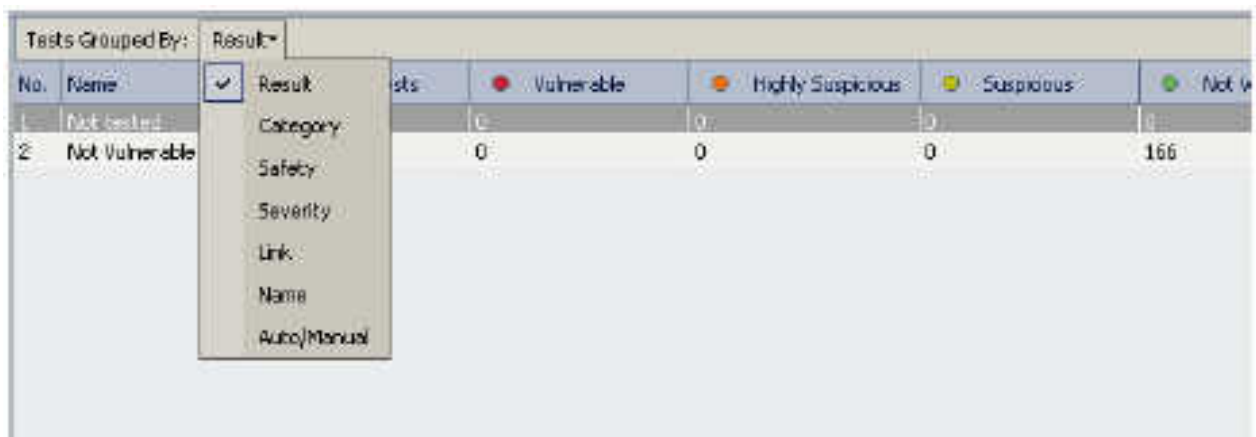


Figura 4

3.51. Menú de métodos agrupados [Sanctum, 2004].





Estos métodos de búsqueda están explicados en la Tabla que se muestra a continuación:

Tabla 9: Grouping methods summary

Agrupado por	Nombre del Grupo	Explicación
Result.	None.	Las Pruebas planeadas que no se mandaron.
	Not vulnerable	Las pruebas a que el sitio ciertamente casi no es vulnerable.
	Suspicious.	Pruebas a que el sitio puede ser vulnerable.
	Highly suspicious.	Pruebas a que el sitio es probablemente vulnerable
	Vulnerable	Pruebas a que el sitio es casi seguro vulnerable.
Category.	Son los mismos elementos explicados en la tabla 5.	
Safety.	Safe	Ningún peligro de dañar al sitio.
	Not safe	Puede probablemente dañar al sitio.
Severity.	High.	La calificación de la Severidad se relaciona con la Seguridad.
	Medium.	
	Low.	
Link	Artícluos que se dieron por el URL principal.	
Name	Articulos que se dieron por el nombre del consultor.	

**Resultado del Color del Código.** Cuando se selecciona un método para buscar información, **AppScan DE** crea una tabla en el cual cada grupo en un renglón. En cada renglón hay una columna que muestra el número total de Pruebas en el grupo, seguido por cuatro columnas de color de código. Estas columnas muestra el número de respuestas de la Prueba en el grupo en cual indica que una liga es: *Vulnerable*, *Highly suspicious*, *Suspicious*, or *Not vulnerable*.





Se debe notar que la columna de Peticiones de las Pruebas contiene la suma de las 4 columnas de color, porque incluye las peticiones de las pruebas que no fueron mandadas. Como se muestra en la figura 3.52:

No.	Name	Test Requests	 Vulnerable	 Highly Suspicious	 Suspicious	 Not Vulnerable
1	Unlabeled test requests	0	0	0	0	0
2	Cross site scripting	242	0	0	0	32
3	Stealthy commanding	37	0	0	0	9
4	Parameter tampering	602	0	0	0	69
5	Bedidators and debug	132	0	0	0	80
6	Cooke poisoning	6	0	0	0	0
7	Suspicious contents	47	0	0	27	0

**Figura 3.52.** Columna de peticiones de las pruebas [Sanctum, 2004].

**Examinando los Resultados con un Grupo.** Cuando se ha seleccionado un método de búsqueda, se puede examinar los artículos con un grupo (nivel 2). Por ejemplo, si se selecciono *Category* como el método de búsqueda, una lista de categorías se despliega. Luego para cada categoría aparece el número de vulnerabilidades en esa categoría. Se puede abrir la lista completa de resultados en una categoría particular. Incluso se puede abrir la “tarjeta índice” para cada resultado (nivel 3). Para examinar los resultados con un grupo se siguen los pasos siguientes:

1. Usar la lista que muestra los métodos, como se muestra en la figura 3.53:

Tests Grouped By:		Result				
No.	Name	Tests	 Vulnerable	 Highly Suspicious	 Suspicious	 Not Vulnerable
1	Not tested		0	0	0	0
2	Not vulnerable		0	0	0	166

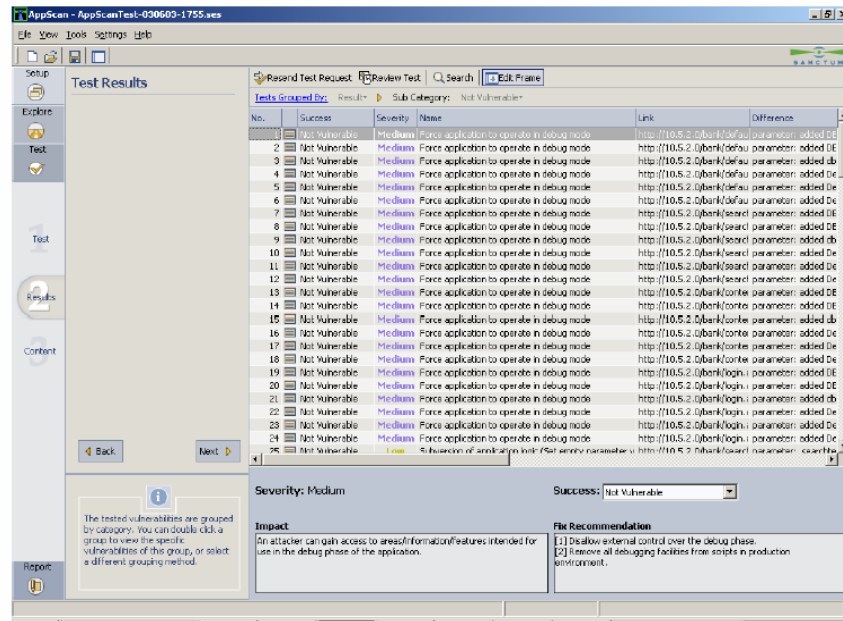
- Result
- Category
- Safety
- Severity
- Link
- Name
- Auto/Manual

**Figura 3.53.** Examinando los resultados con un grupo seleccionado [Sanctum, 2004].

Los resultados de la Prueba se listan de acuerdo al método escogido.



2. Mover el ratón hacia abajo en los nombres de la lista (el cursor se vuelve una mano y el nombre seleccionado se vuelve activo) y hacer clic en el nombre para ver los resultados individuales que pertenecen a ese grupo.
3. La lista completa de los resultados para el grupo seleccionado aparece en la pantalla, así se muestra en la figura 3.54:

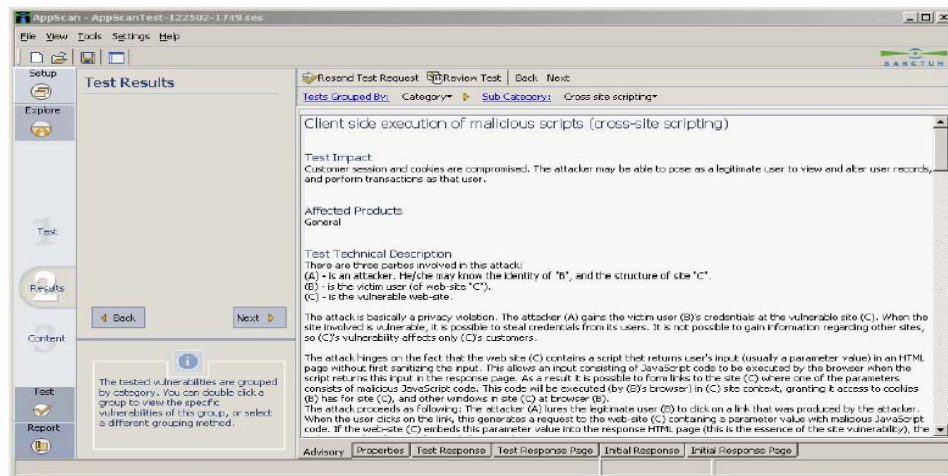


**Figura 3.54.** Lista completa de los resultados del grupo seleccionado [Sanctum, 2004].

4. Hacer clic en un artículo para ver el consejo asociado. El renglón seleccionado aparece de un color distinto a los demás, y el consejo asociado aparece en la parte de abajo/medio en la pantalla.
5. Doble clic en un artículo para abrir la tarjeta índice de **AppScan DE** para ese artículo.

**Tarjeta Índice de Resultados de AppScan DE.** Hay una tarjeta índice para cada resultado de la Prueba. Incluso hay una tarjeta índice para cada comentario html del cual **AppScan DE** sospecha que contenga información sensible. Notar que en el caso de que haya comentarios sospechosos en el código html, ninguna petición fue mandada, y antes de eso las etiquetas de Respuestas están vacías.

Haciendo doble clic en un artículo individual (en la lista de resultados del nivel 2) abre la tarjeta índice para ese artículo, como se muestra en la figura 3.55:



**Figura 3.55.** Tarjeta índice de resultados [Sanctum, 2004].

Notar que para que para cerrar la tarjeta índice y regresar a la lista de artículos, hacer clic en el botón de **Back** en el panel de instrucciones.

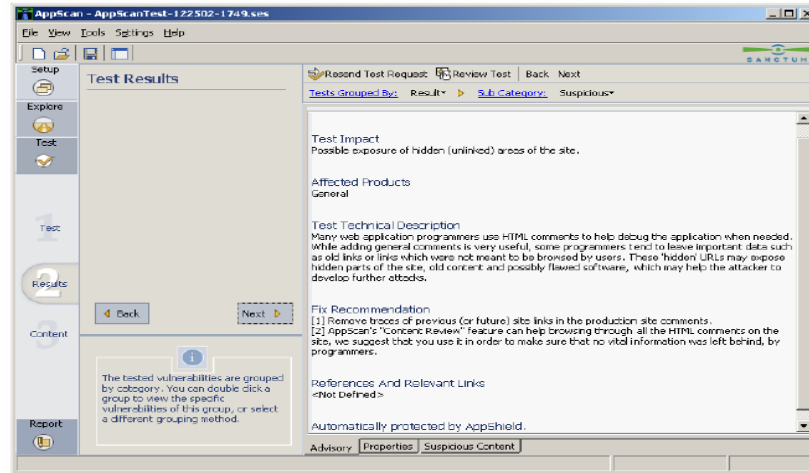
Las etiquetas de la tarjeta índice son explicadas en la Tabla que se muestra a continuación:

**Tabla 10: Index card tabs summary**

Nombre de la Etiqueta	Contenido
Advisory.	El texto completo del consejo asociado con esta vulnerabilidad.
Properties	Presenta la severidad y el resultado de la prueba, también contiene un campo de comentarios, donde se puede escribir comentarios que aparecerán en el reporte final.
Test Response Source	Contiene el código fuente del http de la página de respuesta del sitio a la Prueba.
Test Response Page	Contiene el sitio de respuesta a la Prueba que aparece como un Web Browser.
Initial Response Source	Contiene el código del http de la respuesta inicial del sitio; valida/espera la petición del http que se mando durante la etapa "Explore".
Initial Response Page	Contiene la respuesta inicial del sitio, valida/espera la petición del http que aparece como un Web Browser.

**Etiqueta de Consejos.** Cuando se hace doble clic en una entrada en la lista de resultados en el nivel 2, se abre la tarjeta índice para ese resultado.

La etiqueta más relevante en esta tarjeta es la etiqueta de consejos, como se muestra en la figura 3.56:



**Figura 3.56.** Etiqueta de consejos [Sanctum, 2004].

En la Tabla siguiente se explica cada punto que aparece en la etiqueta de Consejos:

Tabla 11: Advisory tab field summary

Nombre	Explicación
Header.	Nombre del consejo.
Category.	La categoría de los resultados de la Prueba que ese consejo aplica.
Test Impact.	El posible impacto en el sistema de un hacker utilizando esta vulnerabilidad.
Affected Products.	Productos afectados por esta vulnerabilidad.
Technical Description.	Descripción detallada de un posible ataque utilizando esta vulnerabilidad.
Recommended Fix.	Una acción recomendada que puede resolver esta vulnerabilidad.
References & links.	Referencia adicional con respecto a esta vulnerabilidad.
AppShield	¿Protege AppShield contra esto? Sí/no.

**Cambiar el Score de la Prueba.** Se puede cambiar manualmente el *score* o resultado, esto se puede hacer de dos formas:

Método 1:

1. Seleccionar el resultado de la prueba que se quiere editar.

No.	Success	Severity	Name	Link	Difference
1	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/parameter: us	
2	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/parameter: us	
3	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/parameter: us	
4	Not Vulnerable	High	Cross site scripting using HTML entities	http://10.8.2.4/scripts/parameter: us	
5	Not Vulnerable	High	Cross site scripting without using '<' and '>' symbols	http://10.8.2.4/scripts/parameter: us	

**Figura 3.57.** Seleccionar el resultado [Sanctum, 2004].

2. Hacer clic con el botón derecho en el record seleccionado.
3. En el menú que aparece hacer clic en **Success**.

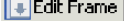
Resend Test Request Review Test Search Edit Frame					
Tests Grouped By: Category Sub Category: Cross site scripting					
No.	Success	Severity	Name	Link	Difference
1	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: use	
2	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: use	
3	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: use	
4	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: use	
5	Not Vulnerable	High	Cross site scripting using HTML entities	http://10.8.2.4/scripts/user parameter: use	
6	Not Vulnerable	High	Cross site scripting without using '<' and '>' symbols	http://10.8.2.4/scripts/user parameter: use	
7	Not Vulnerable	High	Cross site scripting (By escaping from HTML comments	http://10.8.2.4/scripts/user parameter: use	
8	Not Vulnerable	High	Cross site scripting (In JavaScript context)	http://10.8.2.4/scripts/user parameter: use	
9	Not Vulnerable	High	Cross site scripting (In JavaScript context)	http://10.8.2.4/scripts/user parameter: use	
10	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: last	
11	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: last	
12	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: last	
13	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: last	
14	Not Vulnerable	High	Cross site scripting using HTML entities	http://10.8.2.4/scripts/user parameter: last	
15	Not Vulnerable	High	Cross site scripting without using '<' and '>' symbols	http://10.8.2.4/scripts/user parameter: last	
16	Not Vulnerable	High	Cross site scripting (By escaping from HTML comments	http://10.8.2.4/scripts/user parameter: last	
17	Not Vulnerable	High	Cross site scripting (In JavaScript context)	http://10.8.2.4/scripts/user parameter: last	
18	Not Vulnerable	High	Cross site scripting (In JavaScript context)	http://10.8.2.4/scripts/user parameter: last	
19	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: REG	
20	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: REG	
21	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: REG	
22	Not Vulnerable	High	Cross site scripting (Standard variants)	http://10.8.2.4/scripts/user parameter: REG	
23	Not Vulnerable	High	Cross site scripting using HTML entities	http://10.8.2.4/scripts/user parameter: REG	
24	Not Vulnerable	High	Cross site scripting without using '<' and '>' symbols	http://10.8.2.4/scripts/user parameter: REG	
25	Not Vulnerable	High	Cross site scripting (By escaping from HTML comments	http://10.8.2.4/scripts/user parameter: REG	
26	Not Vulnerable	High	Cross site scripting (In JavaScript context)	http://10.8.2.4/scripts/user parameter: REG	

**Figura 3.58.** Menú [Sanctum, 2004].

4. En el menú que se abre hacer clic en el *score* que se quiere dar.

## Método 2:

1. Seleccionar el resultado de la prueba que se quiere editar.
2. En el **Edit Frame**, se puede editar el valor dado por la prueba, el cual aparece en la parte de abajo/medio en el área de administración donde dice **Success**, como se muestra en la figura a continuación:

Notar que el Edit Frame puede abrirse y cerrarse haciendo clic en .

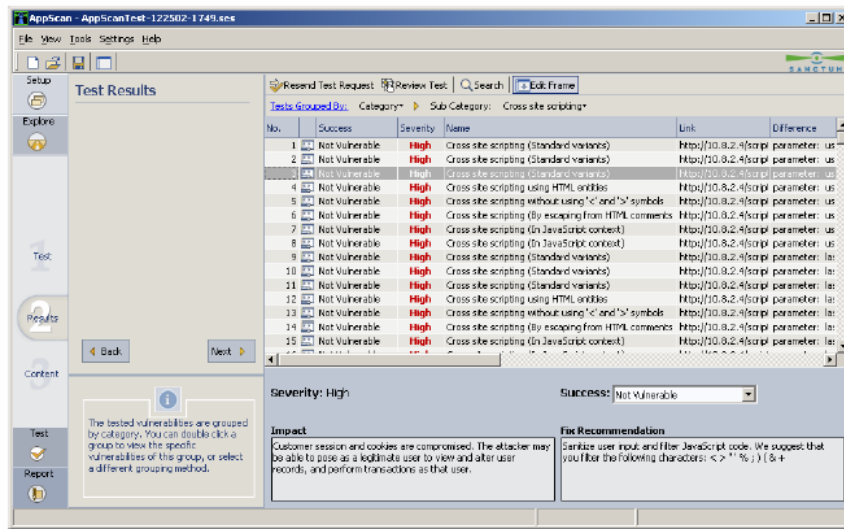



Figura 3.59. Editar frame [Sanctum, 2004].

**Volver a mandar una Petición de la Prueba.** En ocasiones se necesita volver a mandar una petición de la prueba sin que se edite, por ejemplo, si el sitio no estaba en la red cuando la petición se mando originalmente. Se puede volver a mandar una o más peticiones de la prueba de la ventana de resultados de la Prueba a la vista de nivel 2 o nivel 3. Esto se hace de la manera siguiente:

1. En la lista de Resultados en el nivel 2, seleccionar la Prueba (s) que se quiere volver a mandar, (usar **Shift + Control** para seleccionar más de un artículo). Los artículos seleccionados se ponen de otro color.
2. Clic en . La petición o peticiones se mandan otra vez, y los nuevos resultados son incluidos en la página actual de Resultados.

**Revisar una Prueba.** La caja de diálogo de revisar una prueba permite volver a revisar la petición de una prueba seleccionada. Para hacer estos se siguen estos pasos:

1. De la lista de peticiones de la Prueba, seleccionar el texto que se desea revisar.
2. Clic en **Review Test**.
3. Para cerrar el panel de revisión hacer el clic en **Close**.

**Facilidades de Búsqueda.** El área de administración de resultados de la prueba tiene un panel de búsqueda, el cual puede abrirse o cerrarse haciendo clic en él. El panel de búsqueda permite hacer una búsqueda por el *Path*, *Success*, *Request*, *Response* and *Keywords*. Como se muestra en la figura 3.60:

No.	Success	Severity	Name	Link	Difference
1	Not Vulnerable	Medium	Force application to operate in debug mode	http://10.5.2.0/bank/default.aspx?parameter=a	
2	Not Vulnerable	Medium	Force application to operate in debug mode	http://10.5.2.0/bank/default.aspx?parameter=a	
3	Not Vulnerable	Medium	Force application to operate in debug mode	http://10.5.2.0/bank/default.aspx?parameter=a	
4	Not Vulnerable	Medium	Force application to operate in debug mode	http://10.5.2.0/bank/default.aspx?parameter=a	
5	Not Vulnerable	Medium	Force application to operate in debug mode	http://10.5.2.0/bank/default.aspx?parameter=a	
6	Not Vulnerable	Medium	Force application to operate in debug mode	http://10.5.2.0/bank/default.aspx?parameter=a	
7	Not Vulnerable	Medium	Force application to operate in debug mode	http://10.5.2.0/bank/default.aspx?parameter=a	

**Figura 3.60.** Panel de búsqueda [Internet 13].

### c) Contenido.



**Content (Revisar el Contenido):** el paso final en la etapa de Prueba es revisar el contenido. Esto ayuda a crear futuras pruebas para el sitio, basado en el contenido y la estructura del sitio. Se puede revisar *Scripts* para comentarios vulnerables escondidos, los cuales **AppScan DE** no descubrió automáticamente; también se puede ver *cookies* y CGI's.

La página que Revisa el Contenido aparece como se muestra en la figura 3.61:

Object:	Count:
Scripts	0
Cookie (Request)	3
Cookie (Response)	4
Comment	5
Java Script	2

**Figura 3.61.** Página que revisa el contenido [Sanctum, 2004].

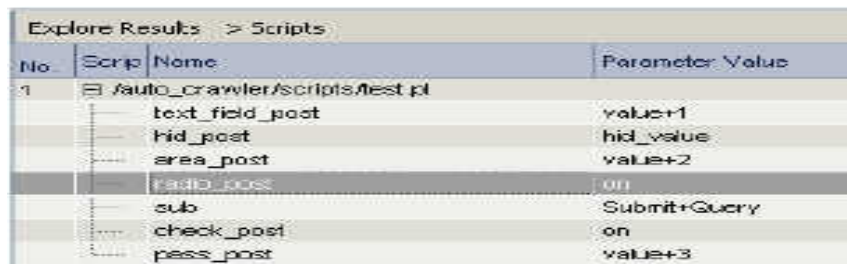
Y la Tabla siguiente explica los objetos que aparecen en la página que revisa el contenido:

Tabla 12: Content Review page objects

Objeto	Descripción
Scripts.	Lista de todas las peticiones que se mandaron durante la etapa "Exploración" que contiene parametros (estos pueden indicar vulnerabilidades potenciales).
Cookie (Response).	Lista de todas las "cookies" recibidas del sitio, en respuesta a la petición inicial.
Cookie (Request).	Lista de todas las "cookies" mandadas al sitio (basado en la respuesta de las "cookies" recibidas), durante la etapa de "Exploración".
Comment.	Lista de todos los comentario encontrados en el texto html.
Java Script.	Lista de todos los Java Script encontrados en el texto html.

**Scripts.** En esta sección se lista todas las ligas encontradas en el sitio que incluyen parámetros. Sobre cada *Script* hay una lista de parámetros asociados con la petición. Para cada parámetro se muestra el nombre, valor (es) y el tipo.

Por ejemplo, sobre el *Script* seleccionado “*radio\_post*” en la figura 3.62 el parámetro es: “*on*”.

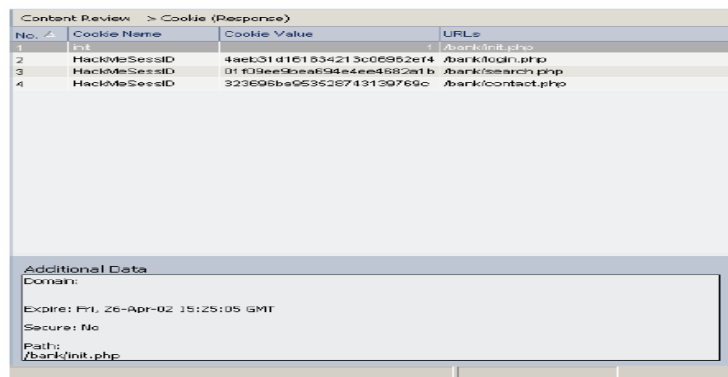


No.	Script Name	Parameter Value
1	/auto_crawler/scripts/test.pl	
	text_field_post	value+1
	hid_post	hid_value
	area_post	value+2
	radio_post	on
	sub	Submit+Query
	check_post	on
	pass_post	value+3

**Figura 3.62.** Scripts [Sanctum, 2004].

**Cookies (Respuesta/Petición).** Las dos lista de *Cookies*, Respuesta y petición, listan todas las *cookies* mandadas por o para el sitio, respectivamente. Para cada *cookie*, el nombre, valor, y URL (de la primera petición/respuesta en la cual fue encontrada) es mostrada. En el caso de respuesta de *cookies*, la parte de abajo/medio en la pantalla muestra el Dominio, Expiración Fecha/Tiempo, y valor de la Seguridad (*Yes=Secure*, *No=Not Secure*) de la *cookie* seleccionada. (Esto es relevante para la petición de la *cookie*).

Esto se muestra en la figura 3.63:



No.	Cookie Name	Cookie Value	URLs
1	id	1000000000	/bank/init.php
2	HackMeSessID	4aeb31d161534213c06952ef4	/bank/login.php
3	HackMeSessID	01f09ee9bea694e4ee4582a1b	/bank/search.php
4	HackMeSessID	323696ba953528743139769c	/bank/contact.php

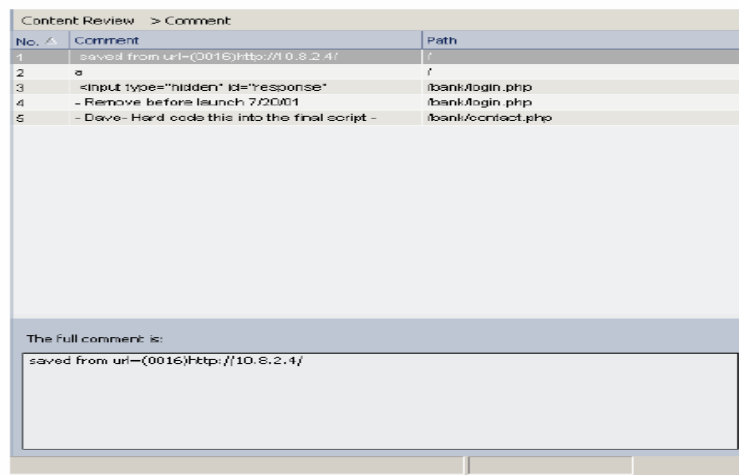
  

Additional Data	
Domain:	
Expire:	Fri, 26-Apr-02 15:25:05 GMT
Secure:	No
Path:	/bank/init.php

**Figura 3.63.** Respuesta/Petición [Sanctum, 2004].



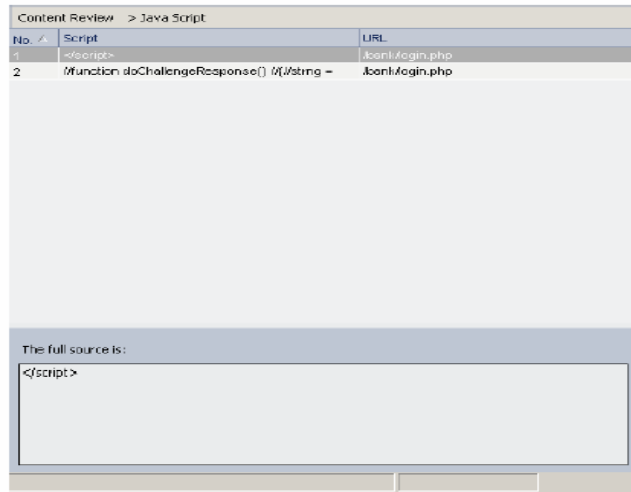
**Comentarios.** Comentarios escondidos en una página html pueden contener información útil para los hackers. En ocasiones el autor del html, intencionalmente o por accidente, deja comentarios para él mismo o para otros desarrolladores en la página final, y esta queda en línea, asumiendo que nadie más lo verá. Un hacker puede cosechar información interna útil de esos comentarios, tal como un “*debug password*”. La ventana de Comentarios lista el inicio de cada comentario y su *path*. La parte de abajo/medio de la pantalla muestra el texto completo del comentario seleccionado, como se muestra en la figura 3.64:



**Figura 3.64.** Comentarios [Sanctum, 2004].

**JavaScript.** Comentarios con un *JavaScript* puede revelar información sensible para un hacker, como un resultado analizando *JavaScript* en un HTML, el archivo puede revelar vulnerabilidades potenciales.

La ventana de *JavaScript* lista el inicio de cada comentario y su relevante URL. En la parte de abajo/medio de la pantalla muestra el texto completo del *script* seleccionado, como se muestra en la figura 3.65:



**Figura 3.65.** JavaScript [Sanctum, 2004].

#### 3.6.4. Etapa del Reporte.

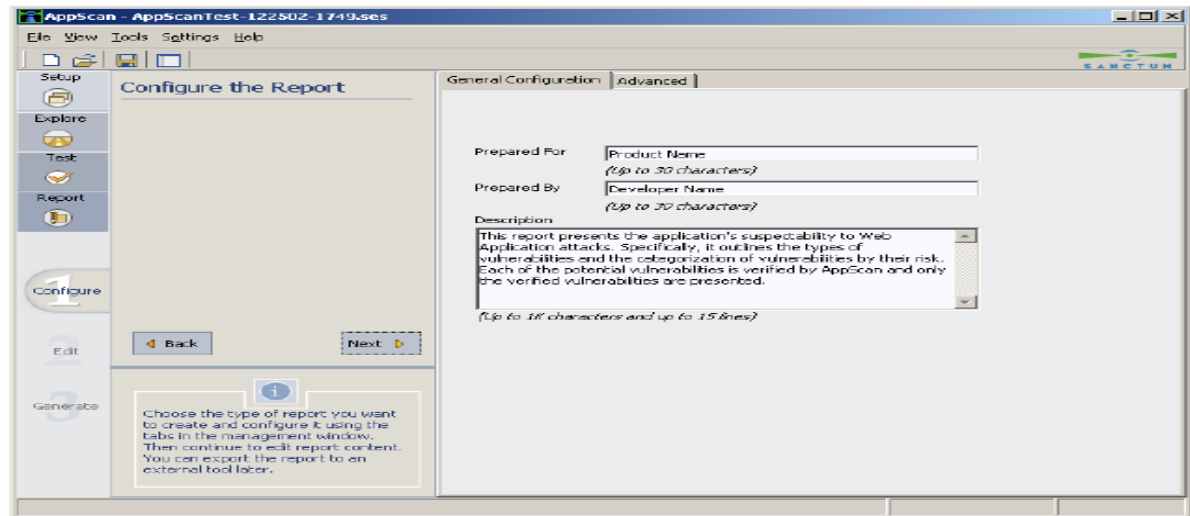
La tercera y final parte de **AppScan DE** es la etapa del Reporte, en la cual se recibe un reporte detallada del resultado del Scan. La etapa del Reporte esta subdivido en tres partes:

##### a) Configuración.



**Configure:** conjunto de información para ser desplegado y despliega un formato.

**Reporte de la Prueba.** El reporte de la prueba contiene una lista completa de todas las vulnerabilidades (listadas por título de la Prueba). Los títulos de la Prueba están listados por Consejos. Cada relevante Consejo es detallado completamente, y seguido por una lista de la Prueba realizada, y de las ligas vulnerables por cada prueba. La figura 3.66 muestra la pantalla de la etapa del Reporte:



**Figura 3.66.** Etapa del reporte [Sanctum, 2004].

Y la Tabla siguiente explica las secciones del Reporte de AppScan DE:

**Tabla 13:** Report fields

Artículo	Explicación
General	Título, compañía, Inicio/Final de Datos y Tiempos, y una breve descripción del contenido del reporte.
Vulnerabilities per Host.	Tabla de todos los hosts encontrados vulnerables y el número de vulnerabilidades por hosts.
Vulnerability Highlights	Tabla de todas la vulnerabilidades encontradas donde están agrupadas de acuerdo al riesgo, éxito, título y categoría.
Scan Statistics	Los URLs en la aplicación, todos los links descubiertos/escaneados presentados como tabla y gráfica.  Vulnerabilidades de la aplicación (sitio); las potenciales y verificadas son presentadas como tabla y gráfica.  Contenido de la aplicación; avería estadística del número total de contenido de Script, Comentarios, Java Script, peticiones de "cookies" y respuesta de "cookies".
Vulnerabilities	Lista completa de todos los links vulnerables, clasificados por el consultor y el título de la vulnerabilidad.
Cookies	Lista completa de las "cookies" de petición y respuesta, clasificadas por nombre del "cookie".
Scripts	Lista completa de los Script encontrados en en sitio, clasificados por título del Script.
Comments	Lista completa de los comentarios encontrados en el sitio, clasificados por título del comentario.
JavaScript	Lista completa de los Java Scripts encontrados en el sitio, clasificados por título del Script.  (Solo para información detallada del Reporte del Scan).
Terms and Definitions	Apéndice uniforme que contiene los términos y las definiciones añadido a todo reporte.

**Configuración del Reporte.** El primer paso de la etapa del Reporte es hacer la apariencia del reporte y proveer a **AppScan DE** con la información necesaria para ser llenada en la plantilla del reporte. (La plantilla del reporte se define durante la etapa de *Setup*).

**Configuración General del Reporte.** En la etiqueta de la configuración general del reporte se puede dar a **AppScan DE** información general para ser añadida al reporte del Scan, como se aprecia en la figura anterior:

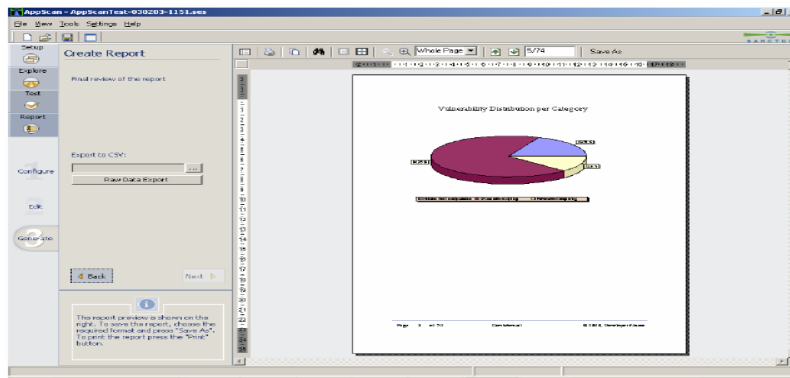
- Nombre del Producto.
- Nombre del Desarrollador.
- Editar una corta descripción del reporte. Se puede cambiar opcionalmente el comentario original que aparece en el campo de comentarios.

Toda esta información será añadida a la página principal del reporte una vez seleccionada.

**Configuración Avanzada del Reporte.** En la etiqueta de configuración avanzada del reporte, se puede decidir entre incluir o no, información adicional en el reporte del Scan:

Información General:

- Reporte Ejecutivo. Esta versión explicada del reporte del Scan es detallada automáticamente al inicio del Reporte de la Prueba.
- Estadísticas del Scan. La información de las Estadísticas del Scan, se presenta en varios modos gráficos, como se muestra en la figura 3.67:



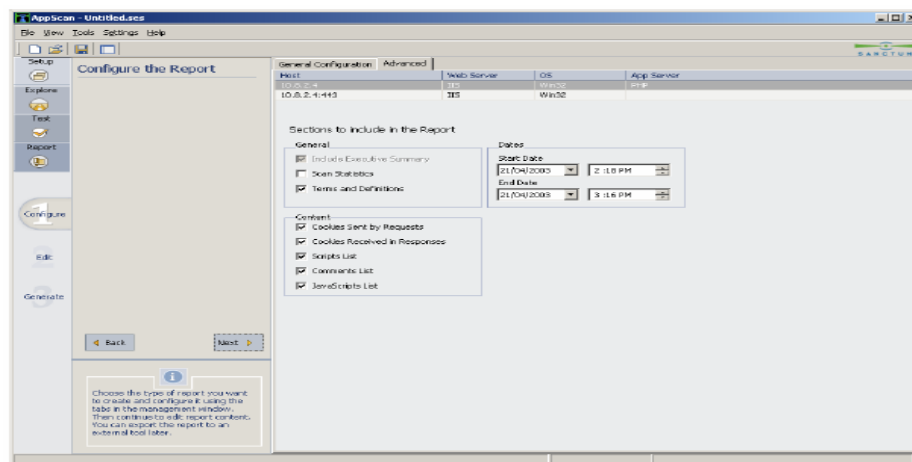
**Figura 3.67.** Estadísticas del Scan [Sanctum, 2004].

- Términos y Definiciones. Una sección de términos y definiciones, explica varios términos y definiciones en el reporte.

Contenido Técnico:

- *Cookies* mandadas por Peticiones.
- *Cookies* recibidas por peticiones.
- Lista de *Scripts*.
- Lista de Comentarios.
- Lista de *JavaScripts*.

Todo lo anterior se puede apreciar en la figura 3.68:

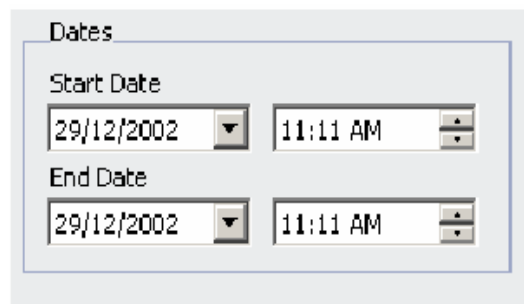


**Figura 3.68.** Contenido técnico [Sanctum, 2004].

Signatura de la fecha y el tiempo:

Tal vez se tenga que cambiar el inicio y el final de la signatura de la fecha y el tiempo en el Reporte.

- La fecha puede ser cambiada tecleando en su respectiva caja de selección, o seleccionado en el menú la fecha del calendario.
- El tiempo puede ser cambiado usando las flechas de arriba y abajo para los campos de Inicio/Final del tiempo. A continuación se muestra en la figura 3.69:



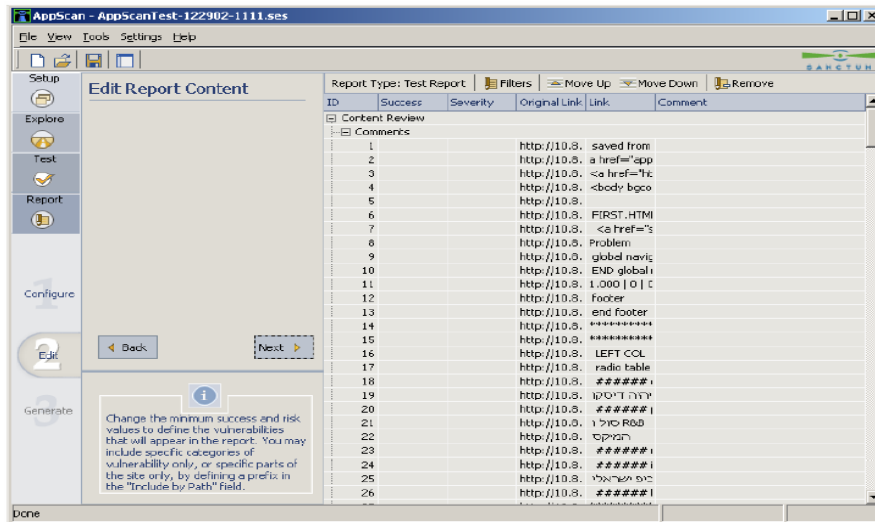
**Figura 3.69.** Fecha y tiempo [Sanctum, 2004].

#### **b) Editar.**



**Edit:** se editan los resultados antes de generar el Reporte. (Solo si el Reporte Detallado es seleccionado). Un reporte interno de **AppScan DE** aparece en la pantalla.

Las categorías pueden ser expandidas y colapsadas. Esta pantalla se muestra en la figura 3.70:

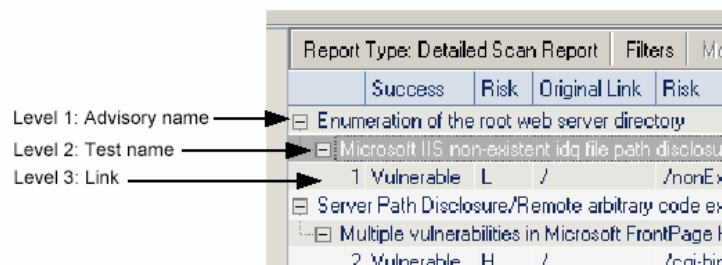


**Figura 3.70.** Editar [Sanctum, 2004].

**Estructura Interna del Reporte.** Las entradas en el Reporte Interno tiene una jerarquía de tres niveles. Los niveles pueden ser expandidos y colapsados en la pantalla, haciendo clic en “+/-“, puesto al inicio de una entrada.

- Nivel 1: entradas de los nombres del consejo.
- Nivel 2: entradas de los títulos de Verificación/Prueba.
- Nivel 3: entradas de las peticiones individuales de la prueba.

La figura 3.71 muestra la estructura de los niveles:



**Figura 3.71.** Estructura de los niveles [Sanctum, 2004].

La última entrada de Nivel 1 es única, es llamada “*Content Review*” y contiene cinco entradas de Nivel 2: CGI’s, Comentarios, *JavaScripts*, Peticiones de *cookies* y Respuestas de *cookies*. Sobre cada Nivel 2 todos los artículos que pertenecen a esa categoría son listados.

**Barra del Menú del Reporte Interno.** El reporte interno tiene su propia barra de menú, la cual se puede usar para preparar el reporte final, como se muestra en la figura 3.72:



**Figura 3.72.** Barra del menú del reporte interno [Sanctum, 2004].

Y la Tabla a continuación explica los artículos de la barra de menú:

Tabla 14: Internal Report menubar items

Artículo	Función
Filters	Abre un diálogo del Filtro, para filtrar artículos del reporte.
Move Up / Move Down	Mueve el consultor seleccionado un lugar arriba o abajo en el reporte.
Remove	Borra el link o artículo seleccionado en el reporte.

### Editando el Reporte Interno:


**Se puede Cambiar el orden de los Consejos en el Reporte.** Se puede cambiar el orden en el cual los consejos aparecen en el Reporte Detallado del Scan. Para promover/degradar un consejo, se siguen los pasos siguientes:

1. Seleccionar el consejo que se quiere mover, seleccionándolo. El consejo seleccionado se pone de otro color.

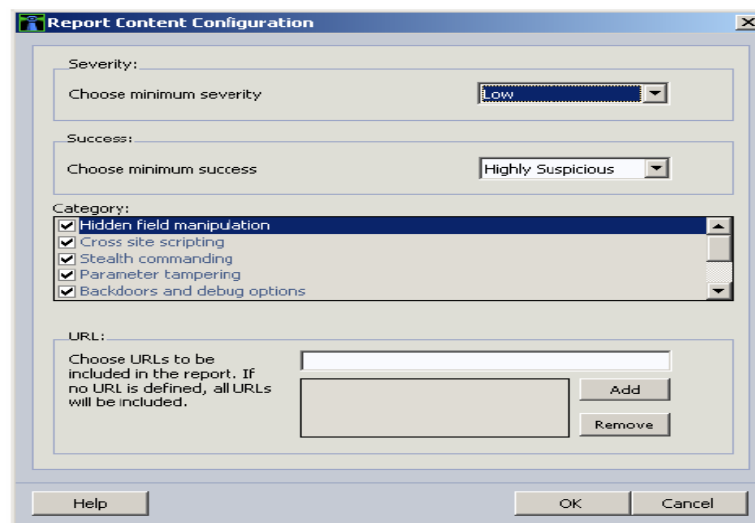


2. Clic en **Move up/Move down** para promover/degradar el consejo. El consejo es reasignado en la pantalla y aparece en el nuevo orden en el Reporte. notar que solo los artículos (consejos) del Nivel 1 pueden ser movidos.

**Borrar artículos del Reporte.** Se puede borrar ligas individuales del Reporte, para hacer esto se siguen los pasos a continuación:

1. Seleccionar el artículo que se quiere borrar, haciendo clic en él. El artículo seleccionado se pone de otro color.
2. Hacer clic en **Remove**. El artículo seleccionado es borrado y no será incluido en el Reporte. Notar que solo los artículos del Nivel 3 pueden ser borrados.
3. Para generar el reporte, clic en .

**Contenido Filtrado en el Reporte.** En adición, para escoger cuales secciones aparecen en el reporte, se puede incluso seleccionar el *nivel* de contenido en el reporte. Usando la caja de diálogo de Filtro en la barra de menú en la Edición Interna del Reporte, en la figura 3.73 se muestra esta caja de diálogo:



**Figura 3.73.** Contenido filtrado en el reporte [Sanctum, 2004].

La Tabla siguiente explica los objetos de esta caja de diálogo:

Tabla 15: Report Content Configuration

Campo	Función
Severity	Selecciona el nivel mínimo que será incluido en el reporte: High/Medium/Low
Result	Selecciona la cuenta mínima del éxito que se inculirá en el reporte: Vulnerable / Highly Suspicious / Suspicious / Not Vulnerable.
Category	Se utiliza para incluir/excluir las categorías de la Prueba en el reporte.
Path	Se puede incluir un path en el reporte poniendo uno en el campo de texto que aparece y haciendo click en Add. Si el campo esta vacío todos los path serán incluidos por default.

### c) Generar el Reporte.



**Generate:** se genera el reporte de **AppScan DE** para verlo en la pantalla, imprimirlo y exportarlo a otros formatos, esto se muestra en la figura 3.74:

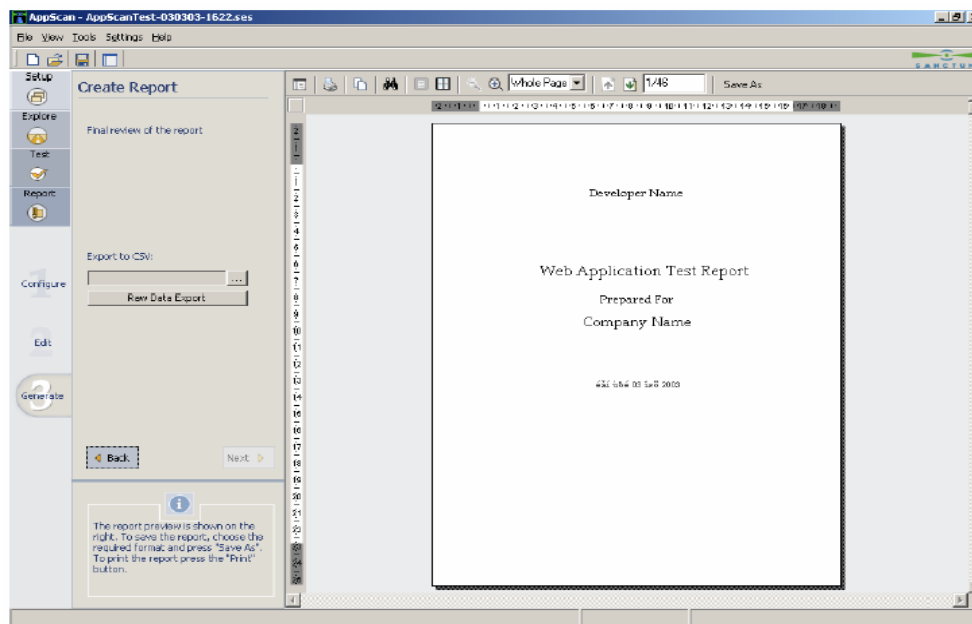


Figura 3.74. Generar el reporte [Sanctum, 2004].

**Barra de Herramientas del Reporte.** El Reporte tiene una barra de herramientas intuitiva para ayudar a navegar el documento, como se muestra en la figura 3.75:



**Figura 3.75.** Barra de herramientas del reporte [Sanctum, 2004].

**Exportar el Reporte para Leer/Editar en otro Programa.** El botón de *Save As* permite salvar el Reporte en PDF/Excel/HTNL/RTF/Text/Tiff formats,

**Exportar el Reporte a un Formato CSV.** Para hacer esto se siguen los pasos a continuación:

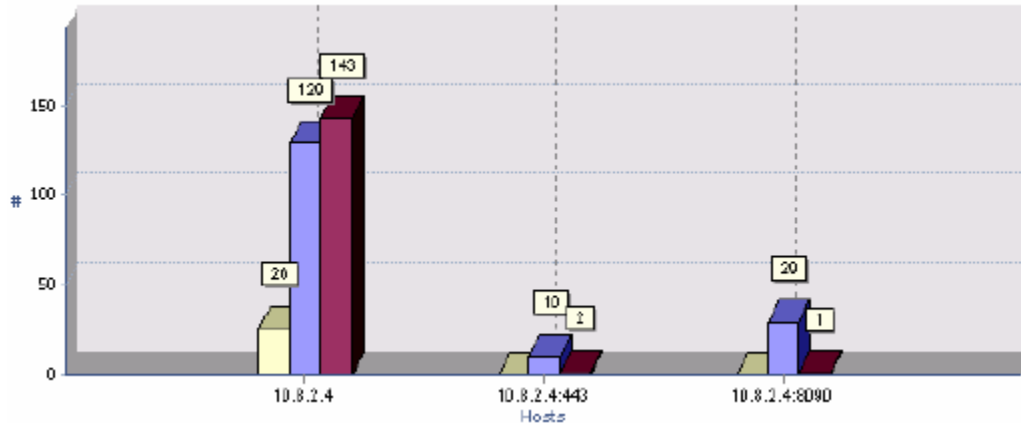
1. En el panel de instrucciones, seleccionar un directorio para salvar el reporte hecho.
2. Presionar **Raw Data Export**. Los datos del reporte son salvados en el disco en formato CSV con cada sección del reporte exportada en un archivo separado.

### Ejemplos de Reportes.

**Vulnerabilidades por Host.** Una tabla muestra el número de ligas por cada nivel de riesgos por *Host*. La tabla es seguida por un gráfico.

<i>Vulnerabilities Per Host</i>				
Host	Low Risk	Medium Risk	High Risk	Total
10.8.2.4	26	129	143	298
10.8.2.4.443	0	10	2	12
10.8.2.4.8090	0	29	1	30

**Figura 3.76.** Vulnerabilidades por host [Sanctum, 2004].



**Figura 3.77.** Vulnerabilidades por host [Sanctum, 2004].

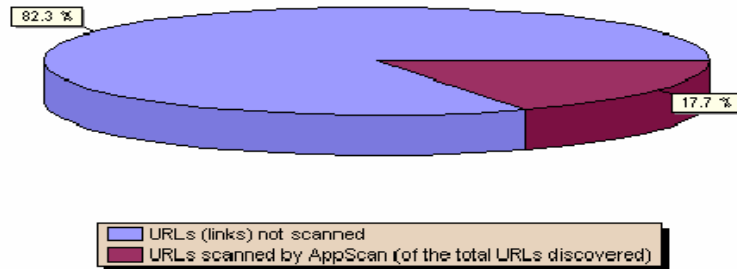
**Medidas de las Vulnerabilidades.** La tabla de medidas de las vulnerabilidades lista las ligas en orden de acuerdo al nivel de la vulnerabilidad y el nivel de riesgo, como se muestra en la figura 3.78, seguido por detalles aconsejables y el número de ligas en esa categoría.

<i>Vulnerability Highlights</i>					
Success	Severity	Name	Category	Impact	#
Highly Suspicious	Medium	Filename references found in HTML comments	Suspicious contents	[1] The computer's file system structure can be deduced from the filenames mentioned in the hidden content. [2] Exposure of filenames related to the web application.	30
Highly Suspicious	Medium	References to sensitive information found in HTML comments	Suspicious contents	Exposure of vital information such as debugging information, usernames or passwords in HTML comments.	7
Highly Suspicious	Medium	Debugging remnants found in HTML comments	Suspicious contents	Exposure of vital information such as debugging information, usernames or passwords in HTML comments.	2
Highly Suspicious	Medium	Calls to 'document.write()' found in JavaScript	Suspicious contents	Exposure of application logic to the attacker may enable him/her to bypass security mechanisms.	7
Highly Suspicious	Medium	References to cookies found in JavaScript	Suspicious contents	Attackers may be able to manipulate authorization mechanism	5

**Figura 3.78.** Medidas de las vulnerabilidades [Sanctum, 2004].

**URL's en la Aplicación.** Los URL's en la aplicación (sitio) muestra el número total de URL's encontrados, y el número total escaneado.

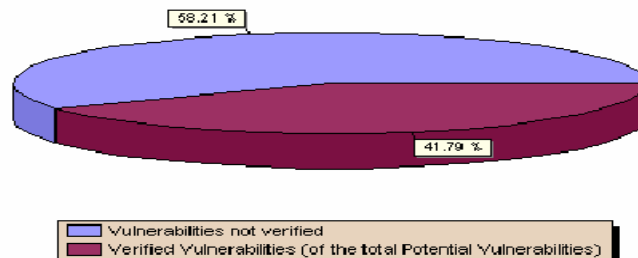
URLs in the Application	Total
URLs (links) Discovered by AppScan	2039
URLs scanned by AppScan (of the total URLs discovered)	361



**Figura 3.79.** URL's en la aplicación [Sanctum, 2004].

### **Vulnerabilidades de la Aplicación.**

Vulnerabilities of the Application	Total
Potential Vulnerabilities	6763
Verified Vulnerabilities (of the total Potential Vulnerabilities)	2826



**Figura 3.80.** Vulnerabilidades de la aplicación [Sanctum, 2004].

### **Contenido de la Aplicación.**

Application Content	Total
Scripts Scanned in the Application	51
Comments in the Application detected by AppScan	102
JavaScript Scripts detected by AppScan	170

**Figura 3.81.** Contenido de la aplicación [Sanctum, 2004].

En este capítulo hemos visto porque razones es importante contar con una herramienta de apoyo, como nos puede ayudar una herramienta contra las perversiones del Web. También analizamos cuales son las necesidades del CENTIA y que beneficios traería esta herramienta al CENTIA. Posteriormente analizamos todo el funcionamiento de la herramienta de AppScan DE.