

Retos de las herramientas de escaneo de vulnerabilidades web

Gonzalo Álvarez Marañón

Limitaciones de los escáner

- ❑ Gestión de excepciones
- ❑ Estructura de URL inusual
- ❑ Autenticación
- ❑ Detección de fin de sesión
- ❑ Sitios web infinitos
- ❑ Procesos en múltiples pasos
- ❑ Enlaces generados en JavaScript
- ❑ Técnicas anti-automatización
- ❑ Número abrumador de falsos positivos

Gestión de excepciones

- ❑ Se captura el error y se presenta una página personalizada
- ❑ Incrementa el número de falsos positivos
- ❑ El escáner debe ser entrenado para cada sitio particular



URL inusuales

- ❑ La estructura convencional de un URL:
recurso?arg1=valor1&arg2=valor2
- ❑ Algunos sitios web cambian la estructura:
 - ❑ No hay ?
 - ❑ No hay &
- ❑ Problemas para el escáner
 - ❑ Difícil identificar el nombre del archivo
 - ❑ Difícil identificar parámetros y sus valores

Comparación de URL

❑ Normal

</dsp/?servlet=login.HomeLoginServlet&Code1=4230051722&Code2=135&cmd=0>

</NASApp/BesaideNet/Gestor?prestacion=Login&funcion=PreLogin&portal=false&idioma=ES>

</ym/ShowFolder?rb=Inbox&reset=1&YY=2165>

❑ Extraño

/exec/obidos/ASIN/0735618909/qid=1117961811/sr=2-1/ref=pd_bbs_b_2_1/104-7081222-7135129

/Software_Education-Reference_W0QQfromZR4QQscatZ3783QQsocmdZListingItemList/4520-6501_7-6061674-1.html?tag=prmo1

</gp/browse.html/104-7081222-7135129?node=3963511&merchant=AB7N2KJ4KAXC3>

Autenticación

- ❑ Elementos de la autenticación:
 - ❑ Nombre de usuario y contraseña
 - ❑ Testigos de sesión: cookie/URL
 - ❑ Redirecciones
 - ❑ SSL
 - ❑ JavaScript
 - ❑ Coordenadas
 - ❑ Captcha

¡Renovado y mejorado!

Correo Yahoo!
me ayuda.
¡Y es gratis!

¿Aún no tienes tu cuenta de Correo Yahoo!?
Obtén la tuya – y aprovecha todas las ventajas.

- Olvídate del problema de almacenamiento. **En breve** podrás disfrutar de 1GB de capacidad en tu Correo Yahoo!.
- Evita el correo basura con nuestros potentes **anti-spam** y **antivirus**.
- Accede a tu cuenta desde cualquier ordenador conectado a Internet.
- Acceso gratuito a Yahoo! Messenger, Yahoo! Fotos y todos los servicios de Yahoo! con el mismo nombre de usuario.

[Conoce más sobre las ventajas de Correo Yahoo!](#)

[Regístrate ahora](#)

¿Ya tienes ID de Yahoo!?
Por favor, entra para leer tu correo

Introduce tu ID y contraseña

ID de Yahoo!:

Contraseña:

Recordar mi ID en este ordenador

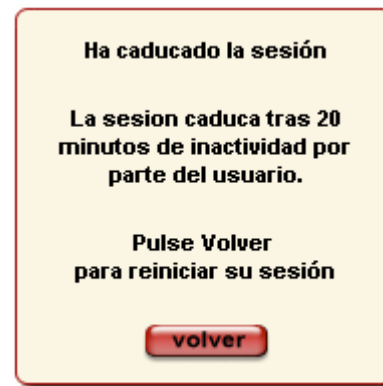
[Entrar](#)

MODO: Normal | [Seguro](#)

[¿Problemas para entrar?](#)
[¿Has olvidado tu contraseña?](#)

Detección de fin de sesión

- ❑ Un usuario es desconectado cuando:
 - ❑ Pulsa el enlace Salir, Logout, Acabar, ...
 - ❑ Expira su sesión por inactividad
 - ❑ Expira su sesión por diseño
 - ❑ Se produce un error
- ❑ ¿Cómo lo detecta un escáner?



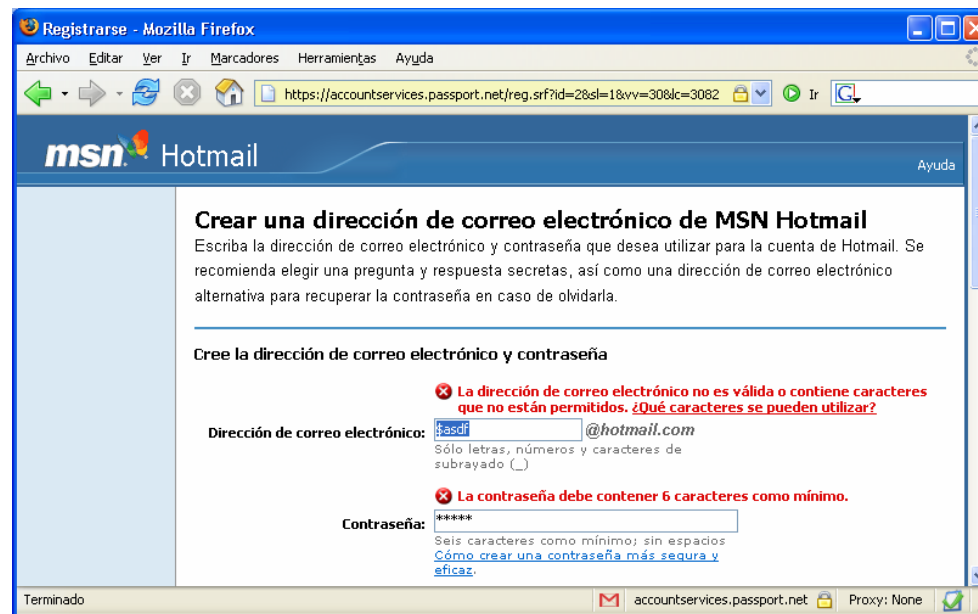
Sitios web infinitos

- ❑ Sitios web con miles y miles de páginas
- ❑ No puede esperarse que sean indexados en un tiempo razonable
- ❑ Difícil realizar mapa del sitio
- ❑ Sitios dinámicos con ritmo de aparición/desaparición de páginas muy elevado
- ❑ Objetivo: detectar estructura de páginas dinámicas y sus parámetros



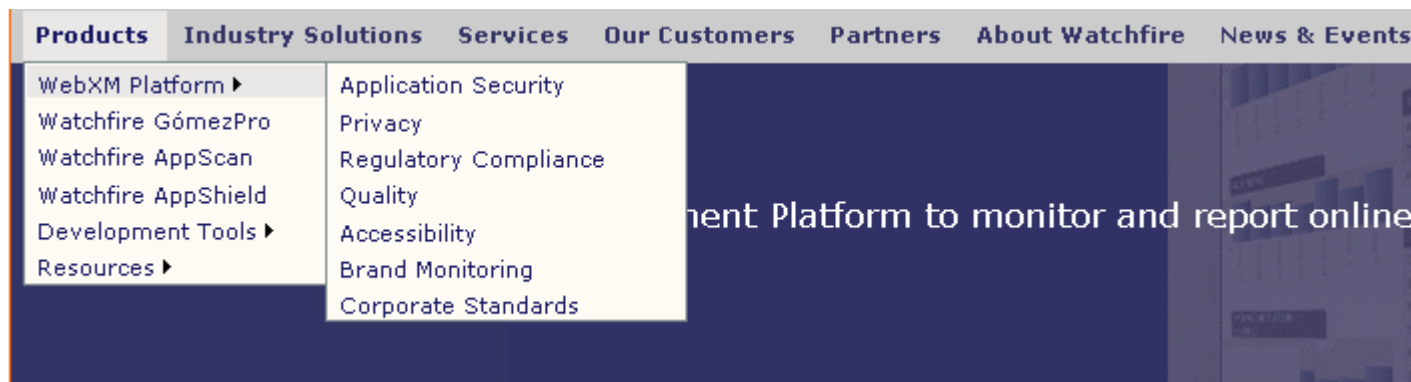
Procesos en múltiples pasos

- ❑ Se deben rellenar varios formularios en distintas páginas para completar un proceso
- ❑ El escáner no sabe qué introducir en los campos ni cómo interpretar las respuestas de error



Enlaces en javascript


- ❑ Muchos sitios web crean enlaces mediante JavaScript y CSS
- ❑ Resulta difícil recorrer el sitio, porque los enlaces no existen si no se interpreta el código
- ❑ Algunos escáneres poseen una habilidad limitada de interpretación de JavaScript



Técnicas anti-automatización

□ Tests de **Turing**: CAPTCHA


The CAPTCHA project



Choose a word that relates to all the images.

↓

bag



TIP: You can type the first letter of a word and then use the down arrow to find it.

Submit

Reproducir archivo de sonido

Números que oye:

© 2004 Carnegie Mellon University, all rights reserved.

Falsos positivos

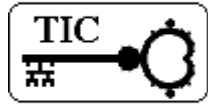
- ❑ Un número muy elevado de falsos positivos hace que la herramienta sea inservible en la práctica
- ❑ Las herramientas poseen una tasa muy baja de detección (3-15%) y muy alta de falsos positivos
- ❑ No detectan ciertos errores lógicos (diseño):
 - ❑ Mala gestión de sesión
 - ❑ Criptografía débil
 - ❑ Recuperación de contraseña deficiente
 - ❑ Cambio de datos personales vulnerable
 - ❑ Etc.

DEMO

- ❑ Herramientas gratuitas
 - ❑ Paros (www.parosproxy.org)
 - ❑ Wikto (www.sensepost.com/research/wikto)
- ❑ Herramientas comerciales
 - ❑ WebInspect de SPI Dynamics (www.spidynamics.com)

Conclusiones

- ❑ Las herramientas automatizadas aceleran el proceso de revisión de la seguridad de un sitio web
- ❑ Ellas solas no pueden detectar todos los problemas ni visitar todo el sitio
- ❑ Se requiere un humano para un análisis (casi) completo
- ❑ La mejor solución: cooperación escáner-hombre



¿Preguntas?

gonzaloalvarez.com