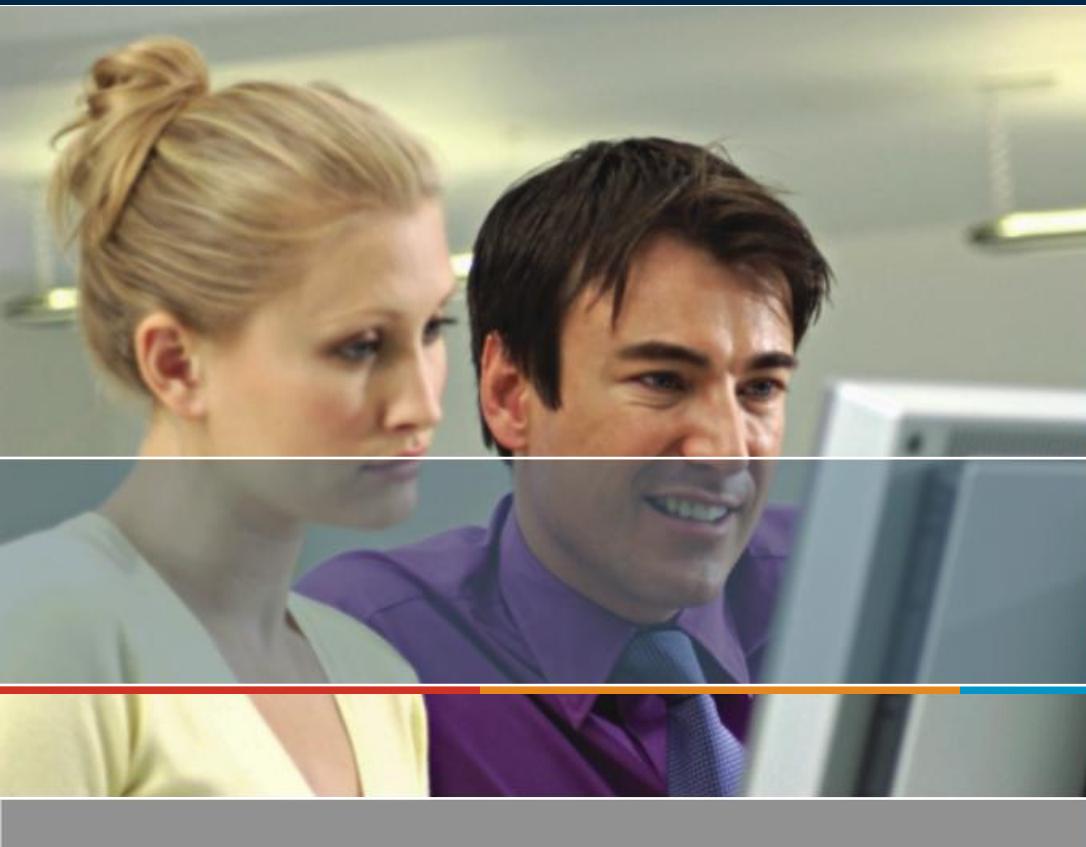


**Su Seguridad es Nuestro Éxito**

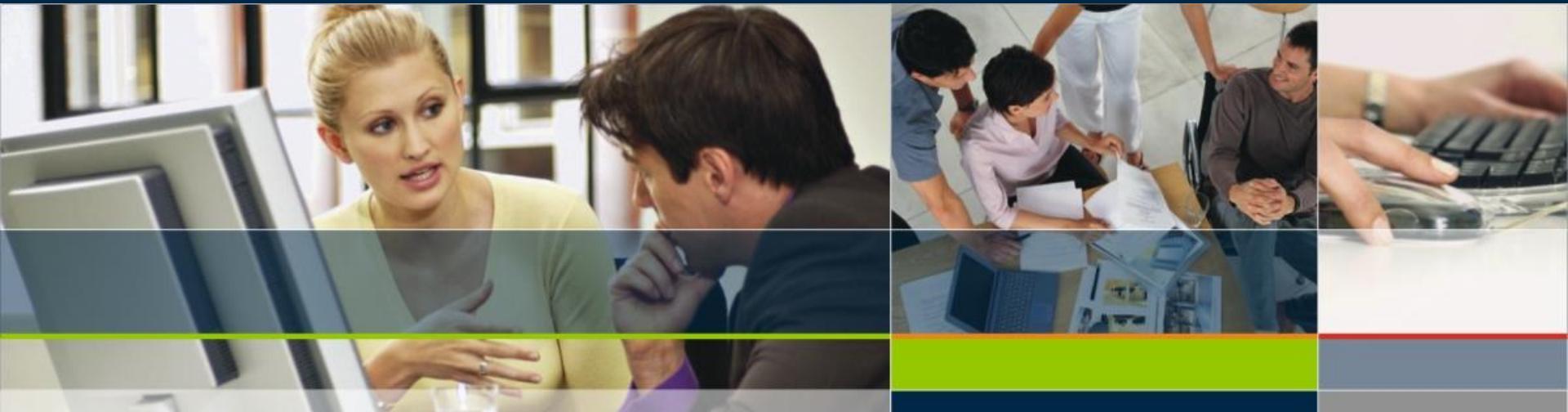




## Análisis de Eco

OWASP Conference, Noviembre 2008

Jesus Olmos Gonzalez ([jolmos@isecauditors.com](mailto:jolmos@isecauditors.com))



Su Seguridad es Nuestro Éxito

## Índice

1. Problemática en la auditoría de Caja Negra.
2. Caja Negra sin eco.
3. Deducción de código.
4. Filtros vs Saneos.
5. Búsqueda de salidas.
6. ¿Qué es el eco?
7. Análisis de los ecos.
8. Ecos indirectos.
9. Autómatas finitos de cara a deducir la evasión.
10. Conclusiones y recomendaciones.

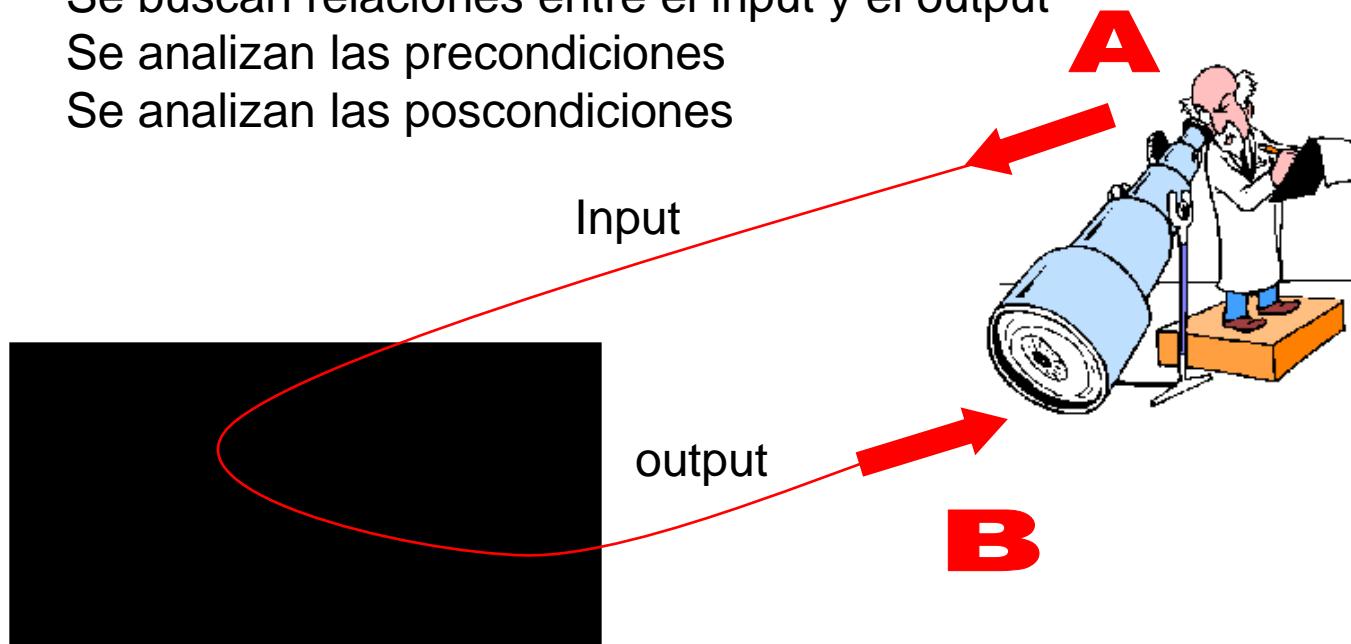
## 1. Problemática en la auditoría de Caja Negra.

- No vemos el código.
- Imposible probar todos los casos.
- Los tipos de vulnerabilidades Web hoy día son “Well Known” (la humanidad cuenta con un rico histórico de vulnerabilidades)
- Los desarrolladores validan los datos cada vez más. (pero no mejor)
- Se realizan validaciones deficientes que no protegen la vulnerabilidad y además dificultan su detección.

Ejemplo:      ‘ → \'  
                  /^.)\*(or|and)/

## 2. Caja Negra sin eco.

- Se induce un input
- Se observa el output
- Se buscan relaciones entre el input y el output
- Se analizan las precondiciones
- Se analizan las poscondiciones



## 3. Deducción de código.

- En vez de ir realizando ataques hasta que alguno “funcione” es más efectivo tantear en busca del fallo y posteriormente explotarlo.
- Este tanteo, consiste en estudiar los input/output de cara a elaborar un pseudocódigo.
- Importante no atacar, sino analizar.



## 3. Deducción de código.

- Es más importante una interpretación correcta del output, que emitir un input acertado.
- Que componente interno nos da el error (BBDD, SA, SW, FWA, ..)  
(Ejemplo real: percepción subconsciente de un FWA mediante un cambio de fuente)
- Que inputs “hacen daño”  
(cancelación de operativa, timmings largos, errores no controlados)
- Cada aplicación funciona diferente, entender a los programadores, estudiar código de cliente, analizar errores.
- Variables de decisión, variables permanentes, variables de llamada externa.

## 3. Deducción de código.

- Correlación input → error, que input provoca que error.
- Significado subyacente de los errores y de los timmings.

Ejemplo de análisis de una operativa:

- ‘ → Error genérico.
- > → Continua la operativa correctamente.
- } → Tiempo de espera largo + Error genérico.
- | → Continúa la operativa + Error genérico.

¿Qué byte ha hecho más daño?

## 3. Deducción de código – Timmings.

Acceso a Datos	Segundos
Acceso a Sistema de Ficheros	Milisegundos
Acceso a memoria	Nanosegundos
Retardo Internet	Milisegundos

## 4. Filtros vs Saneos.

- Los filtros permiten detectar y registrar el intento de ataque.
- Los filtros deniegan la operativa, el atacante puede darse cuenta que no se ha realizado la operativa. De manera que son más fáciles de analizar.
- Los saneos limpian las variables y proceden con la operativa.
- Los filtros y saneos se pueden hacer en una sola instrucción de código o diversas, el resultado no será el mismo. (análisis de orden de filtros)
- Los saneos se pueden entorpecer entre ellos.
- En ambos casos hay que tener en cuenta las transformaciones de datos, por ejemplo decodificaciones. En cuanto se codifique o decodifique o se transforme el valor se puede crear el ataque.

## 4. Filtros vs Saneos.

- La mayoría vulnerabilidades existen simplemente por el escape de contexto.

Ejemplo:

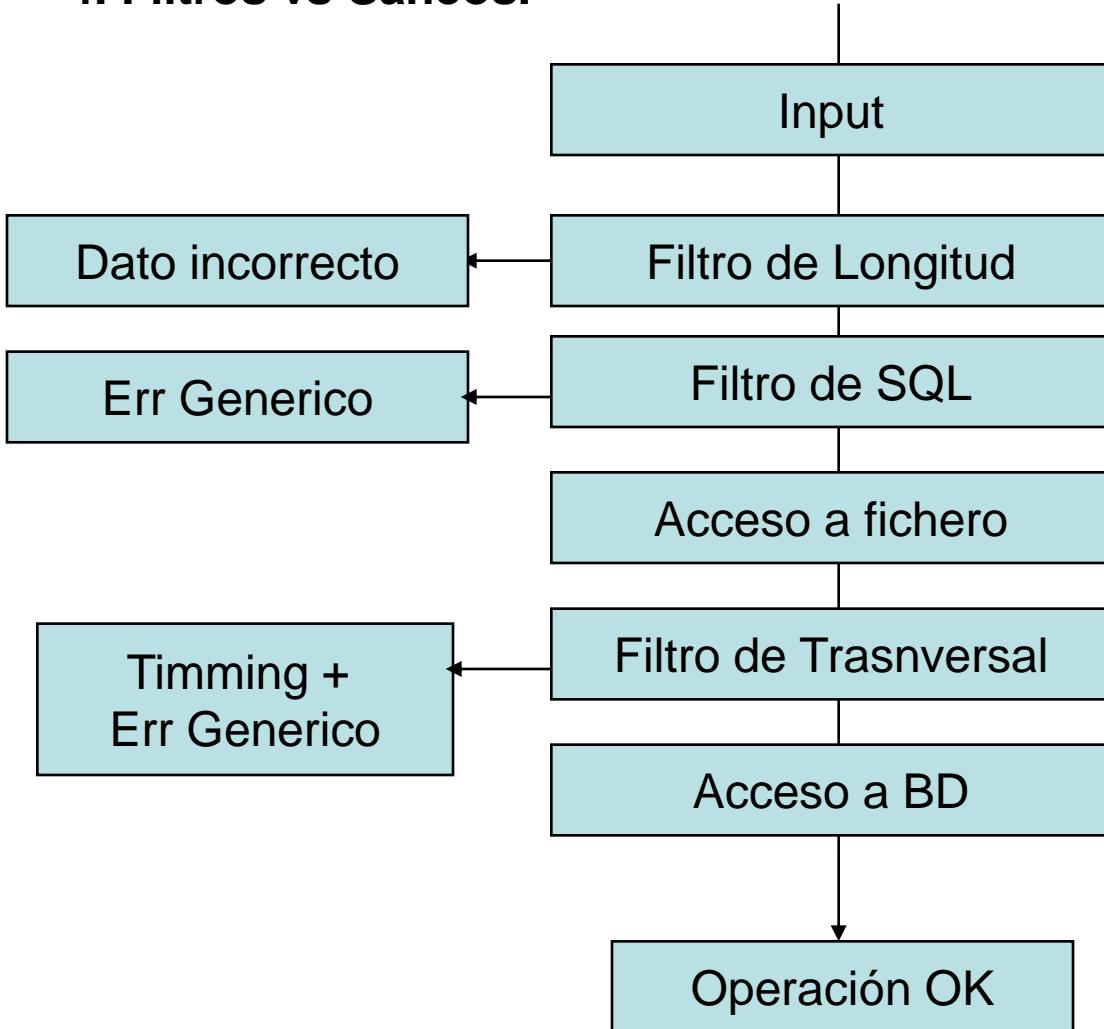
'input' → El input no deberá de contener '

\*input\* → El input no deberá de contener \*

comando del sistema ping 'input' → input no deberá contener '

- Filtraremos o sanearemos el delimitador, para evitar escapes de contexto.

## 4. Filtros vs Saneos.



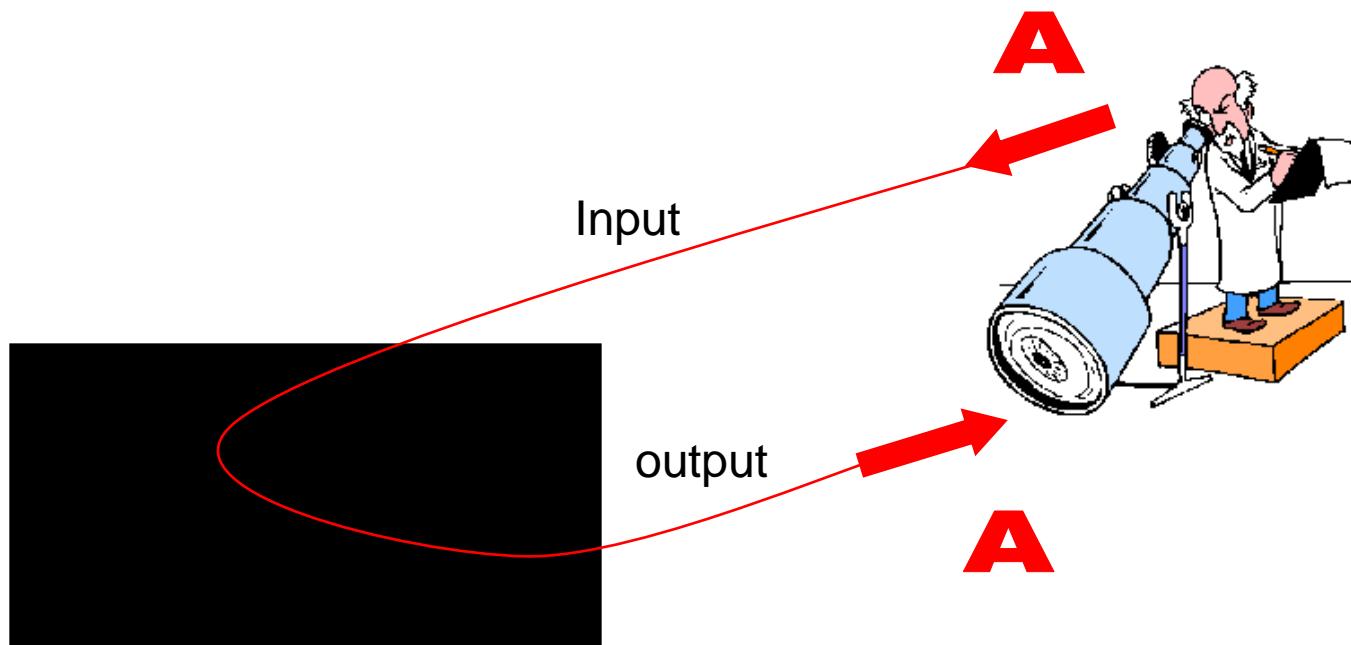
¿El código conduce al usuario o el usuario conduce al código?

## 5. Búsqueda de salidas.

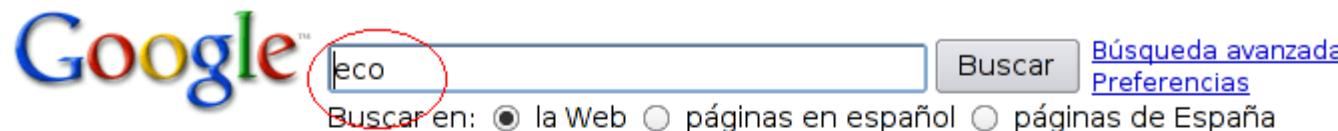
- Existe una vulnerabilidad, pero el filtro nos impide ver su existencia.
  - Analizar los filtros en vez de atacar directamente.
  - Aplicar evasiones.
- Es posible incluso estar explotándola correctamente pero no percibirlo.
  - Buscar una salida.
    - Provocar retardos.  
(sleeps de SO, BD, ..., carga de ficheros largos, SQL pesada)
    - Retroconexiones.
    - Envío por email
    - Aprovechar componentes que permitan una salida  
(ej envío de sms)
    - DoS en terceras aplicaciones

## 6. ¿Qué es el eco o echo?

- Si input ~= output → eco



## 6. ¿Que es el eco o echo?



La Web

Búsquedas relacionadas: [ecobolsa](#) [eco cereijo](#)

[Eco - Wikipedia, la enciclopedia libre](#)

El **eco** es un fenómeno relacionado con la reflexión del sonido. La señal acústica original se ha extinguido, pero aún devuelve sonido en forma de onda ...

[es.wikipedia.org/wiki/Eco](http://es.wikipedia.org/wiki/Eco) - 18k - [En caché](#) - [Páginas similares](#)

Búsquedas relacionadas con: [eco](#)

[ecobolsa](#)

[heco](#)

[evaporadores eco](#)

[mito eco](#)

[eco mitología](#)

[eco cereijo](#)

[ecografia](#)

[reverberacion](#)

Gooooooooooooogle ►  
1 2 3 4 5 6 7 8 9 10 [Siguiente](#)

## 7. Análisis de eco

Ejemplo:

eco'|"< → Búsquedas relacionadas con: <b>eco'|"</b>  
eco\* → <title>eco\* - Buscar con Google</title>

- Saneados = { ',', '<' }
- Aceptados = {e,c,o,|,\*}
- Se puede determinar el alfabeto permitido con el cual crear palabras de ataque.
- El eco permite analizar con mayor exactitud las alteraciones que ha sufrido el input antes de llegar al output.

## 7. Análisis de eco

- Chequeo automatizado:

Is vulnerable to echo analysis

- ' ==> ' Sanitized
- " ==> " Sanitized
- ` ==> ` Accepted
- \$ ==> \$ Accepted
- ==> - Accepted
- \* ==> \* Accepted
- %3f(?) ==> ? Accepted
- %26(%26) ==> & Sanitized
- < ==> < Sanitized
- > ==> > Sanitized
- ( ==> ( Accepted
- ) ==> ) Accepted

- ...  
%39(9) ==> 9 Accepted
- %3a(:) ==> : Accepted
- %3b(;) ==> ; Accepted
- %3c(%3c) ==> < Sanitized
- %3d(=) ==> = Accepted
- %3e(%3e) ==> > Sanitized
- %3f(?) ==> ? Accepted
- %40(@) ==> @ Accepted
- %41(A) ==> A Accepted
- %42(B) ==> B Accepted
- %43(C) ==> C Accepted
- ...

## 8. Eco indirecto

- No hay eco pero se puede intuir a partir de la respuesta.



The screenshot shows a Google search results page. The search bar contains "owasp". Below the search bar are links for "Búsqueda avanzada" and "Preferencias". Underneath the search bar, there are options to "Buscar en: ● la Web ○ páginas en español ○ páginas de España". A blue header bar says "La Web". The main content area displays search results for OWASP:

[Main Page - OWASP](#) - [ [Traducir esta página](#) ]  
How to build, design and test the security of web applications and web services.  
[www.owasp.org/](http://www.owasp.org/) - 49k - [En caché](#) - [Páginas similares](#)

<a href="#">Top Ten</a>	<a href="#">Attacks</a>
<a href="#">Downloads</a>	<a href="#">Vulnerabilities</a>
<a href="#">Guide Project</a>	<a href="#">Code Review</a>
<a href="#">Testing Project</a>	<a href="#">Local Chapters</a>

[Más resultados de owasp.org »](#)

### [Spain - OWASP](#)

OWASP chapter meetings are free and open to anyone interested in application security. We encourage members to give presentations on specific topics and to ...  
[www.owasp.org/index.php/Spain](http://www.owasp.org/index.php/Spain) - 40k - [En caché](#) - [Páginas similares](#)

## 8. Eco indirecto

Google™   [Búsqueda avanzada](#) [Preferencias](#)

Buscar en:  la Web  páginas en español  páginas de España

**La Web** R

[Main Page - OWASP](#) - [ [Traducir esta página](#) ]  
How to build, design and test the security of web applications and web services.  
[www.owasp.org/](http://www.owasp.org/) - 49k - [En caché](#) - [Páginas similares](#)

<a href="#">Top Ten</a>	<a href="#">Attacks</a>
<a href="#">Downloads</a>	<a href="#">Vulnerabilities</a>
<a href="#">Guide Project</a>	<a href="#">Code Review</a>
<a href="#">Testing Project</a>	<a href="#">Local Chapters</a>

[Más resultados de owasp.org »](#)

**Spain - OWASP**  
OWASP chapter meetings are free and open to anyone interested in application security. We encourage members to give presentations on specific topics and to ...  
[www.owasp.org/index.php/Spain](http://www.owasp.org/index.php/Spain) - 40k - [En caché](#) - [Páginas similares](#)

Resultados 1 - 10 de aproximadamente 386.000 de **owasp**. (0,05 segundos)

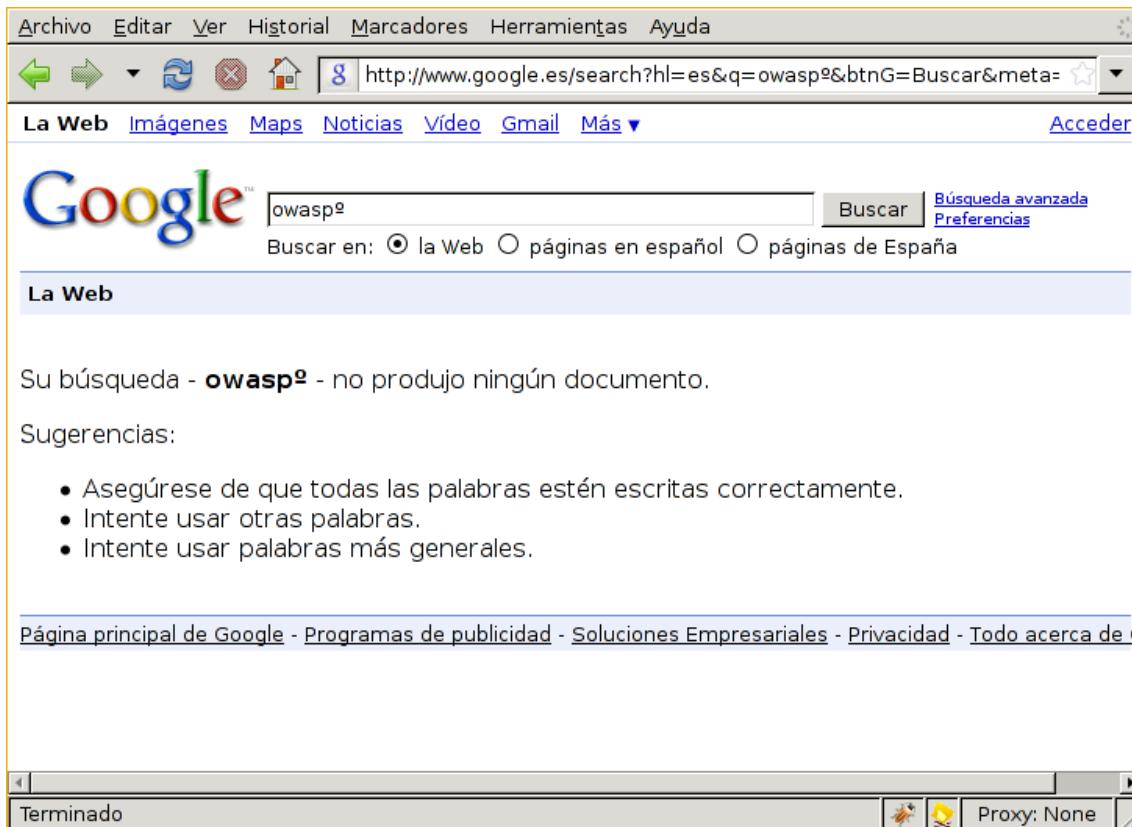
## 8. Eco indirecto



The screenshot shows a Google search results page. The search bar contains "owasp\*". Below the search bar are options: "Buscar en:  la Web  páginas en español  páginas de España". To the right of the search bar are links for "Búsqueda avanzada" and "Preferencias". The main search results are displayed under the heading "La Web". The first result is "Main Page - OWASP - [ Traducir esta página ]" with the description "How to build, design and test the security of web applications and web services." and the link "www.owasp.org/ - 49k - En caché - Páginas similares". The second result is "Spain - OWASP" with the description "OWASP chapter meetings are free and open to anyone interested in application security. We encourage members to give presentations on specific topics and to ..." and the link "www.owasp.org/index.php/Spain - 40k - En caché - Páginas similares". There is also a link "Más resultados de www.owasp.org »".

- No filtran ni sanean el asterisco.

## 8. Eco indirecto



The screenshot shows a web browser window with the following details:

- Menu Bar:** Archivo, Editar, Ver, Historial, Marcadores, Herramientas, Ayuda.
- Toolbar:** Back, Forward, Stop, Home, Refresh, Address Bar (http://www.google.es/search?hl=es&q=owasp0&btnG=Buscar&mmeta=).
- Navigation Bar:** La Web, Imágenes, Maps, Noticias, Vídeo, Gmail, Más ▾, Acceder.
- Search Bar:** Google logo, search input field containing "owasp0", a "Buscar" button, and links to "Búsqueda avanzada" and "Preferencias".
- Search Options:** Buscar en:  la Web,  páginas en español,  páginas de España.
- Results:** A message stating "Su búsqueda - **owasp0** - no produjo ningún documento." followed by "Sugerencias:" and a bulleted list:
  - Asegúrese de que todas las palabras estén escritas correctamente.
  - Intente usar otras palabras.
  - Intente usar palabras más generales.
- Page Footer:** Página principal de Google - Programas de publicidad - Soluciones Empresariales - Privacidad - Todo acerca de G.
- Bottom Bar:** Terminado, two small icons, Proxy: None, and a refresh icon.

- No filtra el byte `^<b>owasp0</b>`
- Parece un error interno bien disimulado, pero no lo es.

## 8. Eco indirecto



Google™

owasp<

Buscar Búsqueda avanzada  
Preferencias

Buscar en:  la Web  páginas en español  páginas de España

**La Web**

[Main Page - OWASP](#) - [ Traducir esta página ]  
How to build, design and test the security of web applications and web services.  
[www.owasp.org/](http://www.owasp.org/) - 49k - [En caché](#) - [Páginas similares](#)

<a href="#">Top Ten</a>	<a href="#">Attacks</a>
<a href="#">Downloads</a>	<a href="#">Vulnerabilities</a>
<a href="#">Guide Project</a>	<a href="#">Code Review</a>
<a href="#">Testing Project</a>	<a href="#">Local Chapters</a>

[Más resultados de owasp.org »](#)

### Spain - OWASP

OWASP chapter meetings are free and open to anyone interested in application security. We encourage members to give presentations on specific topics and to ...  
[www.owasp.org/index.php/Spain](http://www.owasp.org/index.php/Spain) - 40k - [En caché](#) - [Páginas similares](#)

- En una variable cambia < por &lt; sin embargo en otra lo suprime y no influye en la búsqueda ni a 3º party apps.

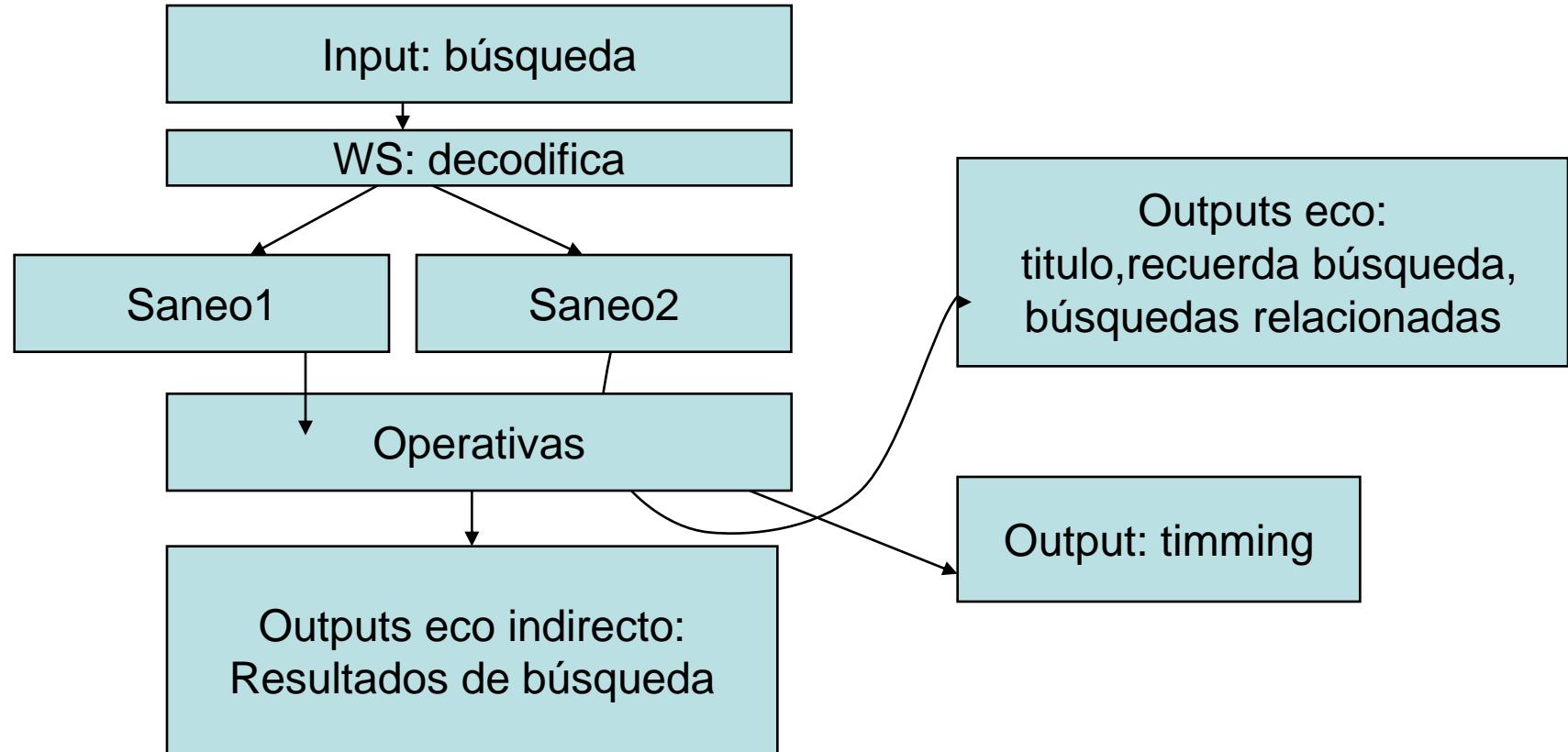
## 8. Eco indirecto



The screenshot shows a web browser window with the following details:

- Toolbar:** Archivo, Editar, Ver, Historial, Marcadores, Herramientas, Ayuda.
- Address Bar:** http://www.google.es/search?hl=es&q=owasp12&btnG=Buscar&meta=
- Navigation:** Back, Forward, Stop, Home, Refresh.
- Links:** La Web, Imágenes, Maps, Noticias, Vídeo, Gmail, Más ▾, Acceder.
- Search Bar:** Google, owasp12, Buscar, Búsqueda avanzada, Preferencias.
- Search Options:** Buscar en: (radio buttons) la Web, páginas en español, páginas de España.
- Results:** La Web, Resultados 1 - 1 de 1 de **owasp12**. (0,25 segundos)
- Result Preview:** vbCity/DevCity.NET Forums :: Login - [ Traducir esta página ]  
user:"websleuth" pass: "**owasp12**" result="200 OK" > > > > .... user:"owasp"  
pass: "**owasp12**" result="200 OK" > > > > ...  
[www.rohitab.com/discuss/index.php?act=attach&type=post&id=326](http://www.rohitab.com/discuss/index.php?act=attach&type=post&id=326) - 401k -  
En caché - Páginas similares
- Search Bar (in results area):** owasp12, Buscar.
- Links in results area:** Restringir la búsqueda a los resultados | Herramientas del idioma | Sugerencias de búsqueda
- Footer:** Página principal de Google - Programas de publicidad - Soluciones Empresariales - Privacidad - Todo acerca de Google
- Status Bar:** Terminado, Proxy: None.

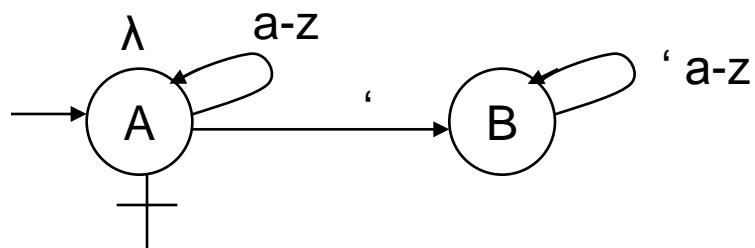
## 8. Eco indirecto



- En el eco el input está conectado con el output, en el “indirecto” tenemos un output generado a partir del input

## 9. Autómatas finitos de los filtros

- Una vez identificada la validación, se puede analizar los estados de aceptación de su autómata finito.
- Ejemplo:
  - Regexp: `/^.*/` (todo lo que comience por comilla es un ataque)
  - Alfabeto del atacante  $E = \{ ' \text{a-z} \}$
  - Serán aceptadas:  $\lambda$  (null) o comillas que no estén al inicio



## 10. Conclusiones y Recomendaciones

- Análisis de filtro en vez de probar ataques y probar evasiones. (un analizador automático que haga esto está bien, detectará rápidamente las vulnerabilidades menos escondidas)
- Solventar los problemas desde diseño, el poner una validación en algunos casos implica tapar el problema.
- Diseñar evasiones personalizadas para el filtro / saneo identificado.
- Usar variables de decisión para esquivar validaciones.
- Reducir los inputs y outputs.
- Reducir la inferencia de los outputs.