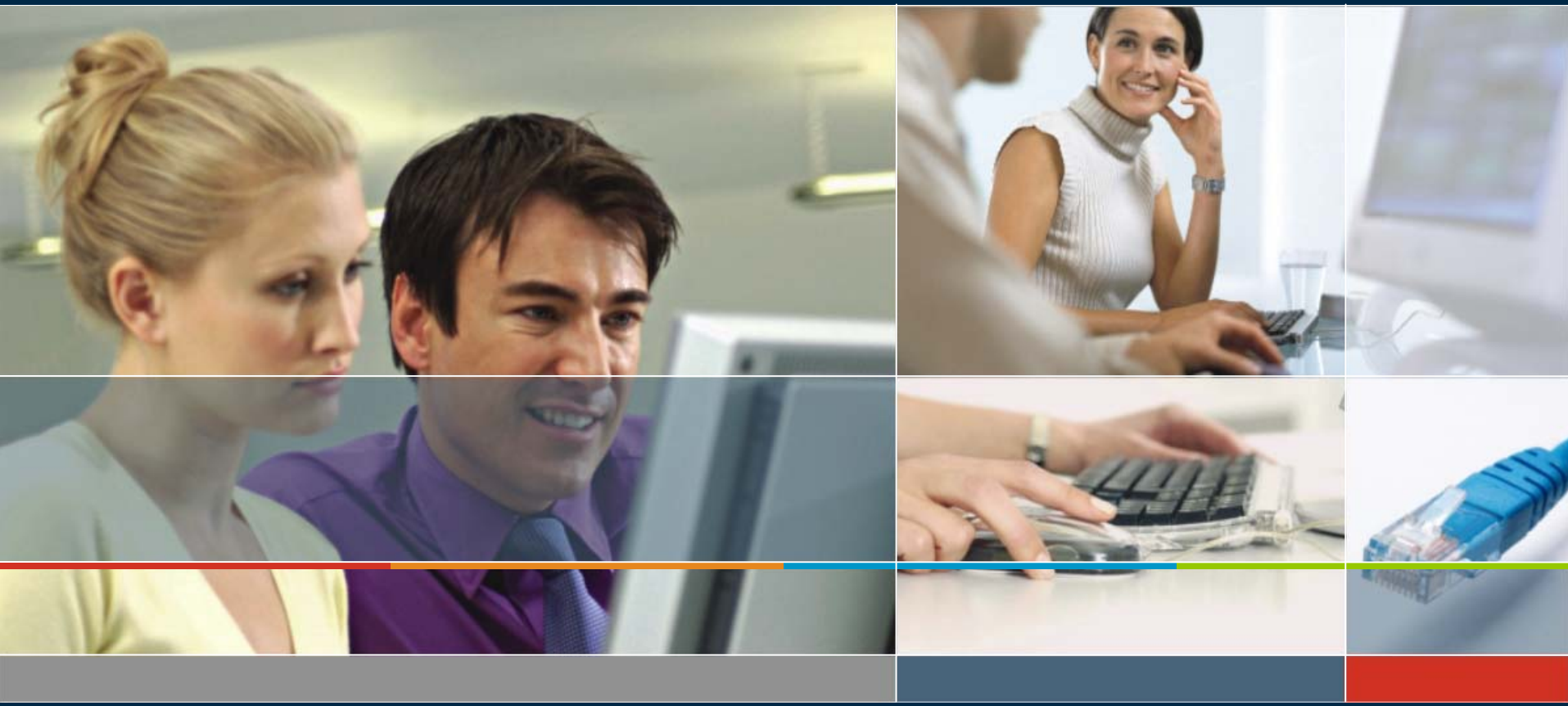
Su Seguridad es Nuestro Éxito

internet security auditors

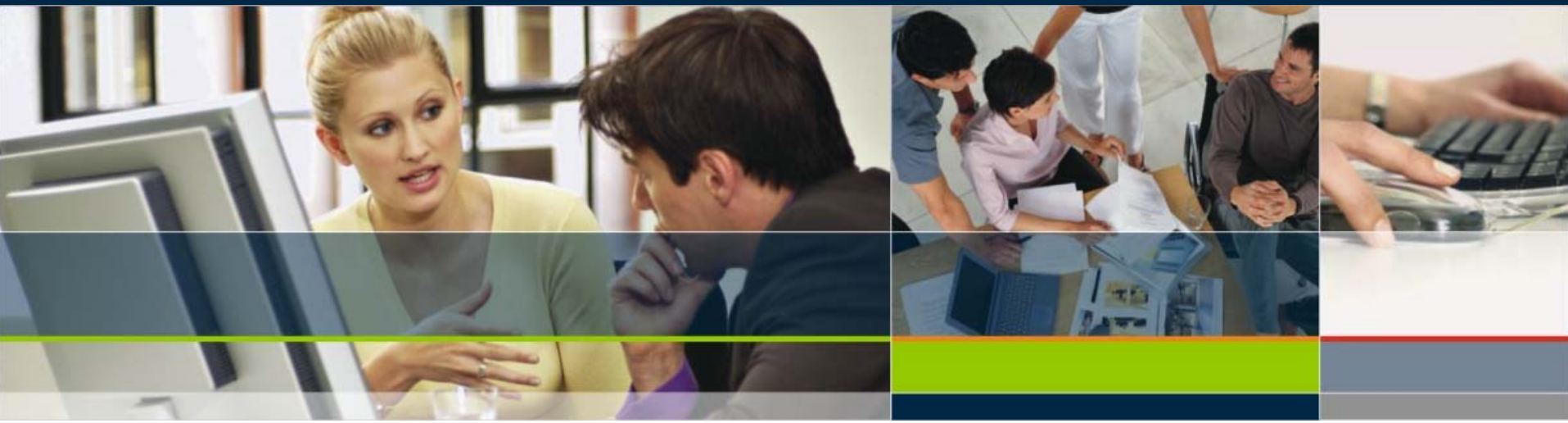


c. Santander, 101. Edif. A. 2º I 08030 Barcelona I Tel.: 93 305 13 18 I Fax: 93 278 22 48 I **info@isecauditors.com** I **www.isecauditors.com**

Tratamiento seguro de datos en aplicaciones

OWASP Conference 2007

Barcelona, Julio 2007



Su Seguridad es Nuestro Éxito

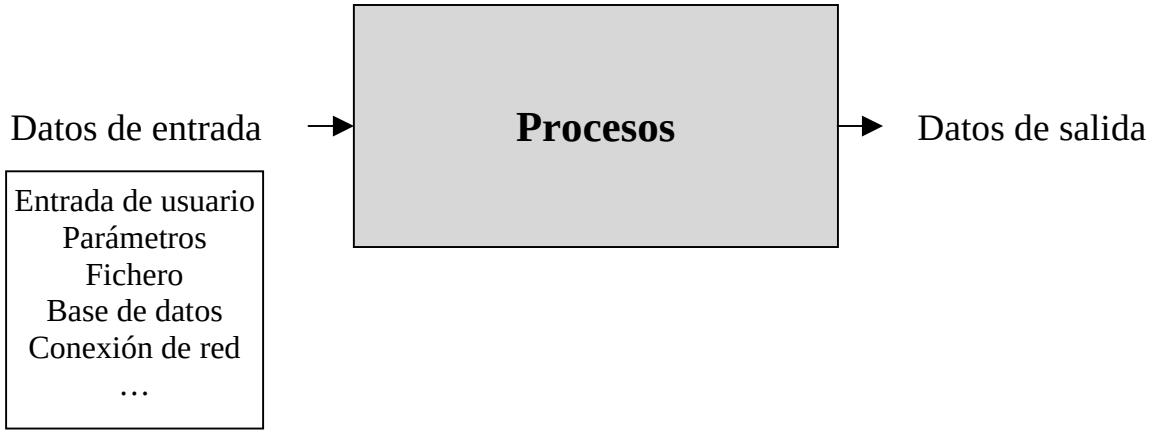
internet security auditors

Definición de Aplicación:

"Una aplicación es un programa informático diseñado para facilitar al usuario un determinado tipo de trabajo." (Fuente: Wikipedia)

Compentes de una Aplicación:

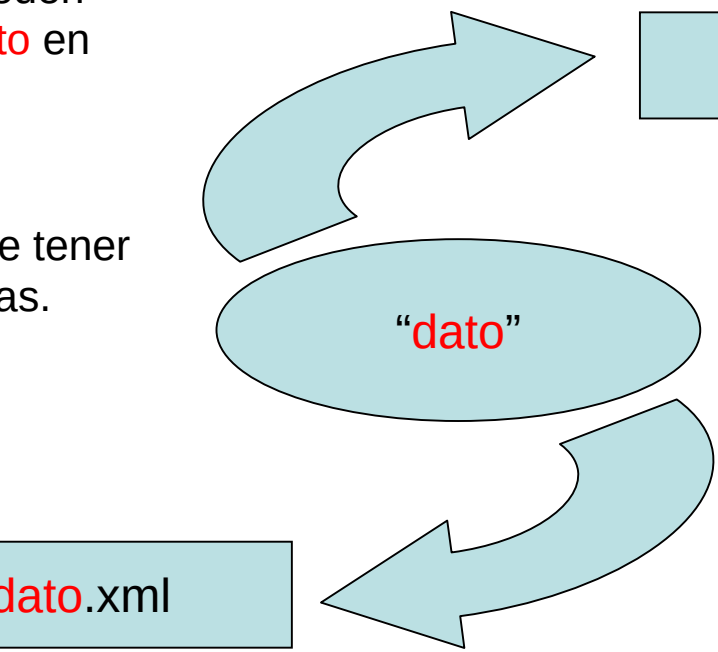
- Procesos
- Datos



- Las aplicaciones reciben datos, los procesan y luego muestran los resultados.
- Los datos introducidos en una aplicación pueden utilizarse en distintos contextos.
  - Nombre de fichero
  - Consultas SQL
  - Consultas XPATH
  - En códigos de marcas (XML, HTML, etc)
  - …

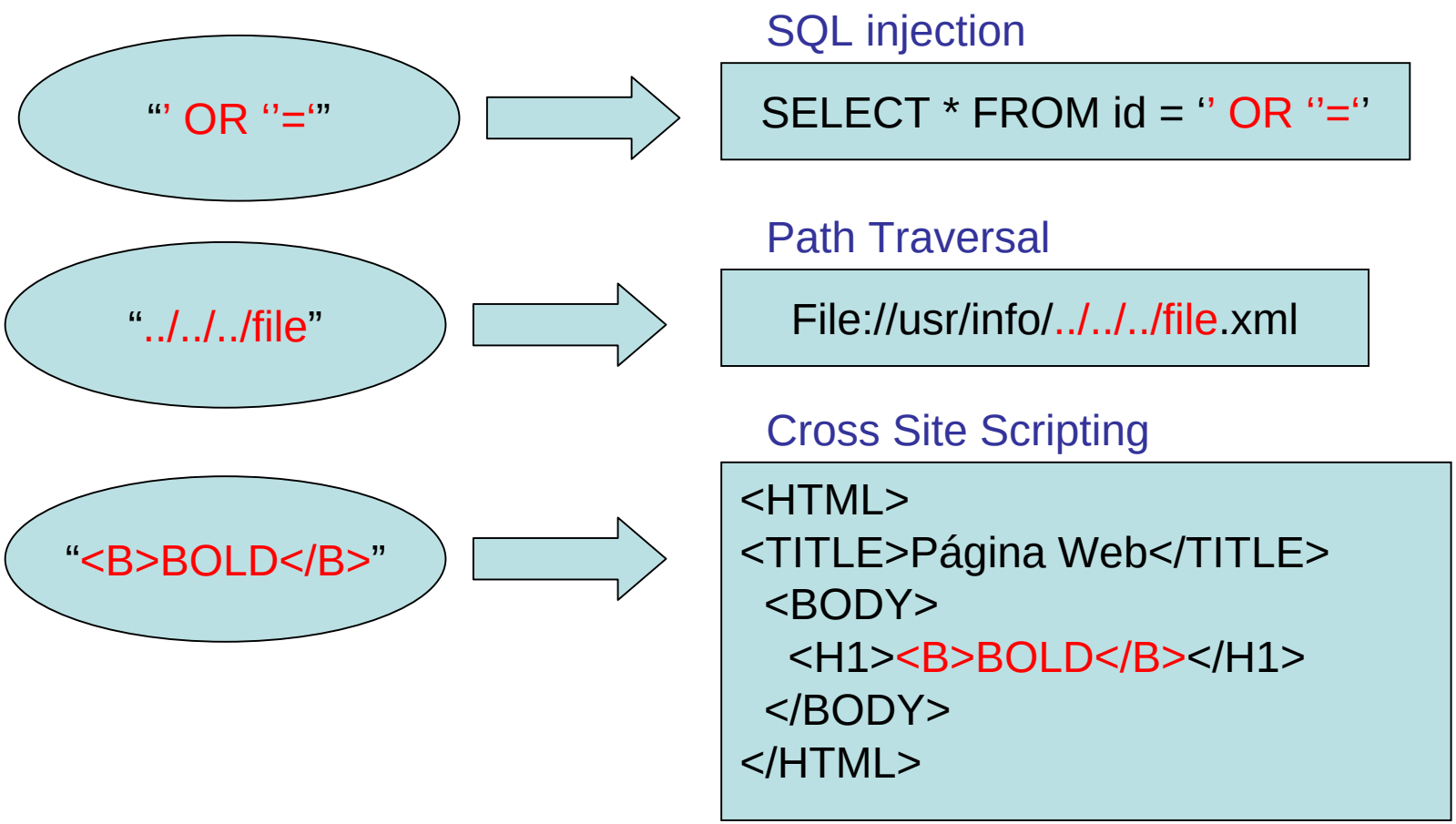
Las aplicaciones pueden utilizar un mismo dato en distintos contextos.

Cada contexto puede tener implicaciones distintas.



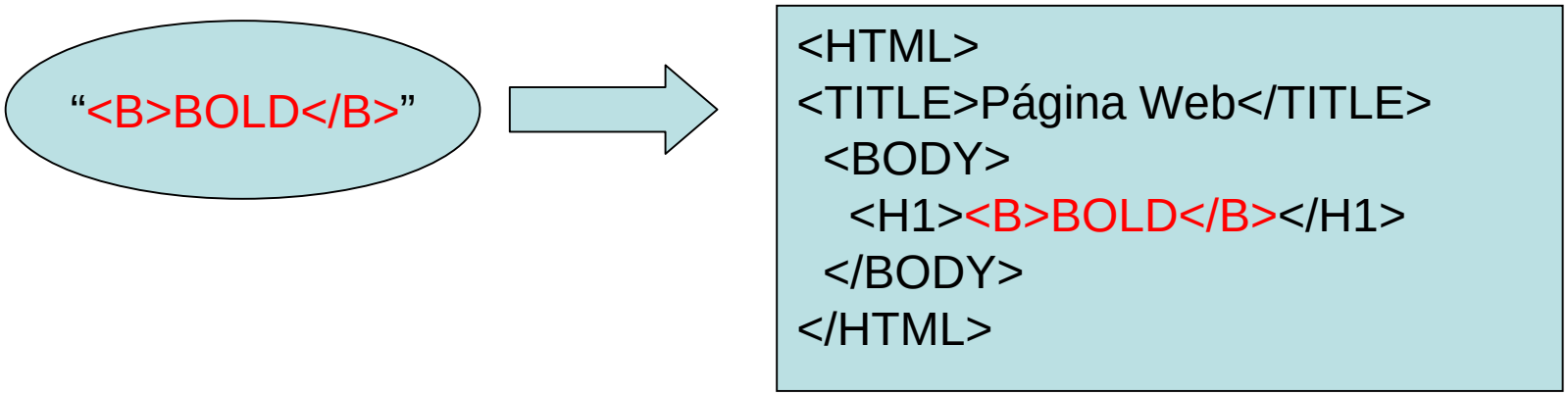

```
<HTML>
<TITLE>Página Web</TITLE>
 <BODY>
   <H1>dato</H1>
 </BODY>
</HTML>
```

- Un tratamiento incorrecto de los datos puede ocasionar que un cambio de contexto suponga una vulnerabilidad en la aplicación.



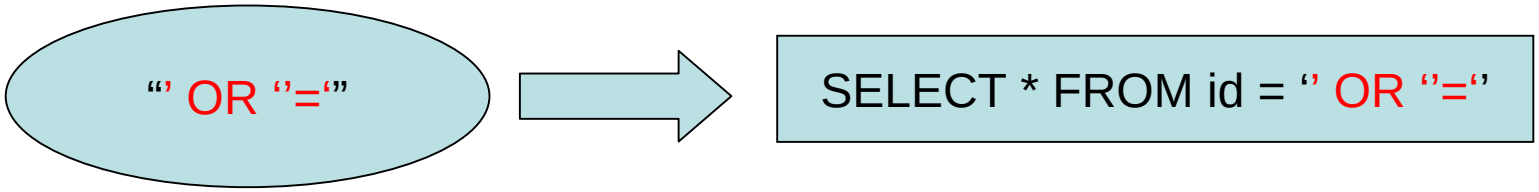
Cross Site Scriptint (XSS)

- Es un error que se produce en contexto de lenguaje de marcas HTML, al generar la presentación de una página web.
- Un usuario puede inyectar código malicioso (HTML/Javascript) que se ejecuta en el cliente.
- Permite comprometer otros usuarios (ejecutar código, robar cookies).



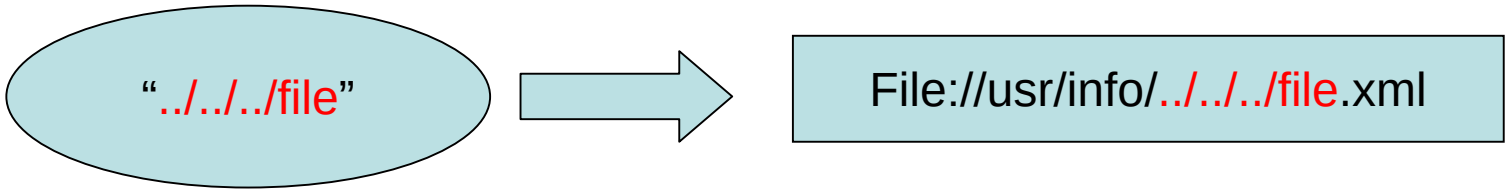
SQL Injection

- Es un error que se produce en contexto de sentencia SQL.
- Un usuario es capar de alterar la sentencia SQL y alterar el comportamiento de la aplicación.
  - Añadir datos
  - Borrar datos
  - Extraer datos
  - Ejecutar comandos del sistema
  - …
- Se puede comprometer datos y servidores.



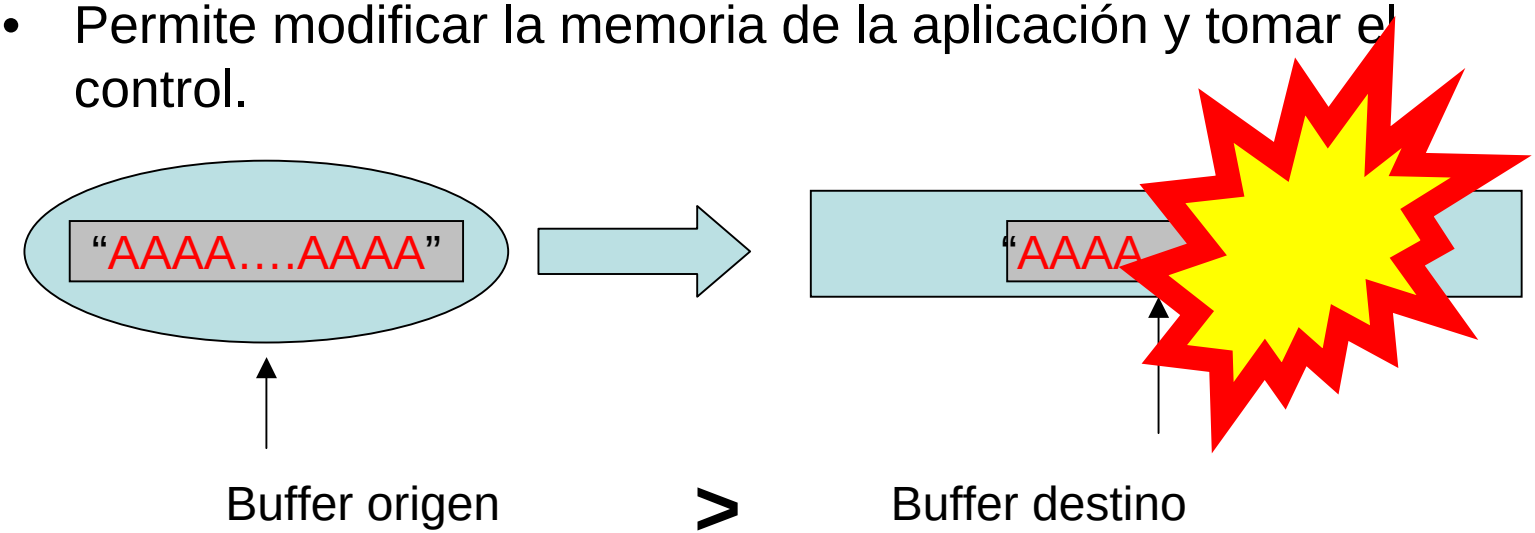
PATH Traversal

- Es un error que se produce en contexto de ruta de fichero.
- El usuario es capaz de manipular la ruta de un fichero para que se acceda a ficheros de forma no controlada, generalmente escapando del directorio mediante '..'
- Se pueden comprometer datos y servidores, dependiendo del uso que se le de los ficheros a los que se accede.



Buffer overflow

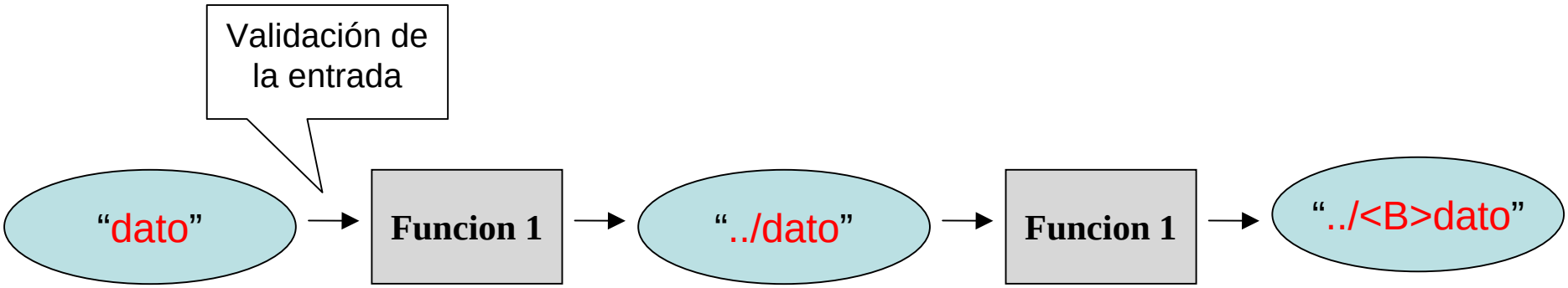
- Es un error que se produce en contexto de buffer de memoria.
- Se copia de un buffer de memoria a otro sin verificar que el buffer de destino sea mayor o igual que el buffer de origen.
- Permite modificar la memoria de la aplicación y tomar el control.



Validación de datos de entrada ¿Solución?

¡NO!

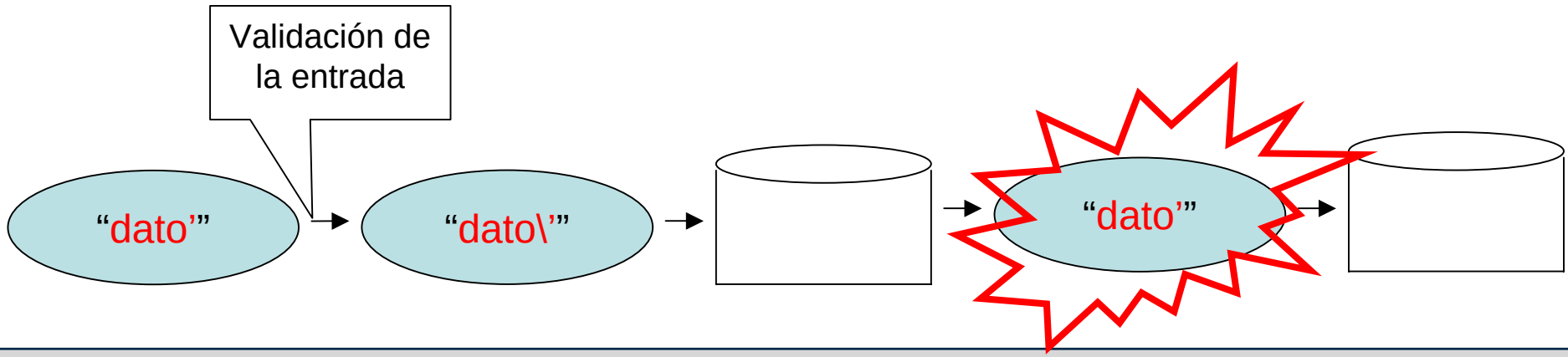
- Se suele decir que una aplicación es segura si valida sus datos de entrada, pero eso no es cierto.
- Un dato validado en la entrada de la aplicación puede ‘mutar’.



Validación de datos de entrada ¿Solución?

¡NO!

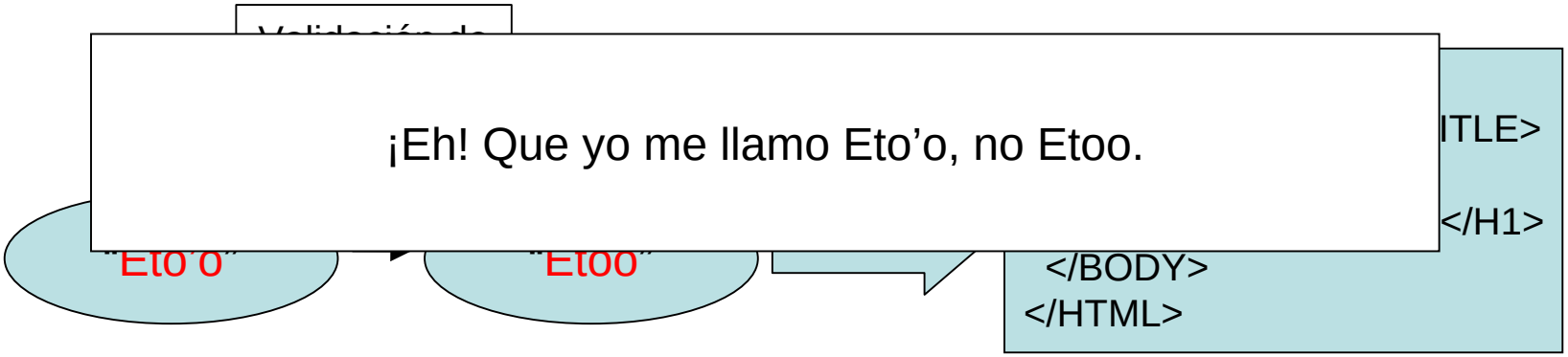
- Si se verifican únicamente las entradas de datos se pueden producir ataques ‘de segundo nivel’.
- Ejemplo: Un dato se verifica, se introduce en la base de datos pero luego al reutilizarse no se verifica de nuevo.



Validación de datos de entrada ¿Solución?

¡NO!

- No podemos “generalizar” la validación de datos en la entrada, ya que podemos perder la usabilidad.
- Ejemplo: Una validación que “generalizada” que elimina (o escapa) todos los caracteres sospechosos (>, <, ‘, etc).



Validación de datos en cambios de contexto ¿Solución?

¡SI!

- Te garantiza que SIEMPRE estarás tratando con datos de forma segura en todo momento.
- En cada cambio de contexto deberían aplicarse únicamente las medidas necesarias para asegurar el dato en ese contexto, de manera se mejora la usabilidad.

Tratamiento seguro de datos en aplicaciones

Contexto	Validaciones
Sentencia SQL	Escapar caracteres (comillas, contrabarra)
Código HTML	Codificar los datos en HTML (HTMLencode)
Nombre de un fichero	Filtrar caráracteres (barra, contrabarra, puntos al inicio de fichero)
Buffer de memoria	Verificar tamaño de origen y destino.
…	…

→ SQL Injection

→ Cross site scripting

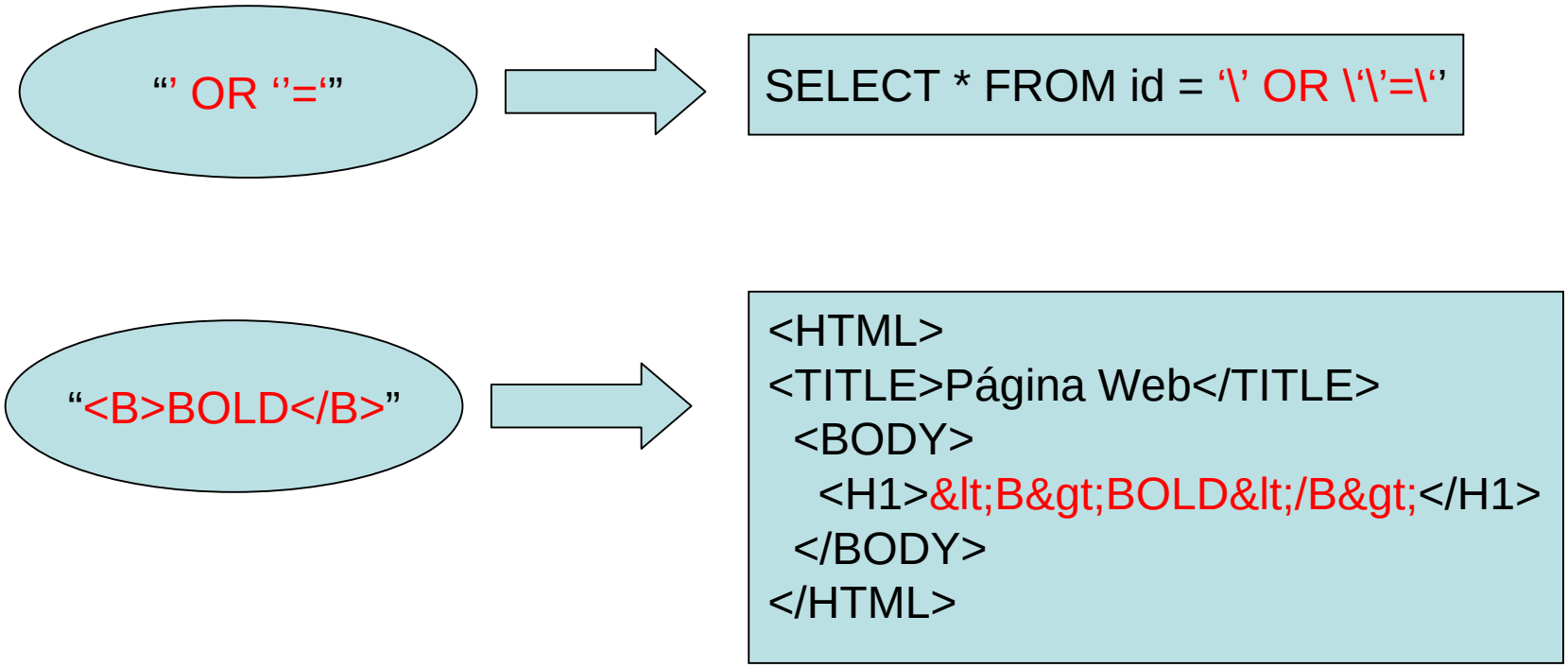
→ Path traversal

→ Buffer overflow

→ …

Validación de datos en cambios de contexto ¿Solución?

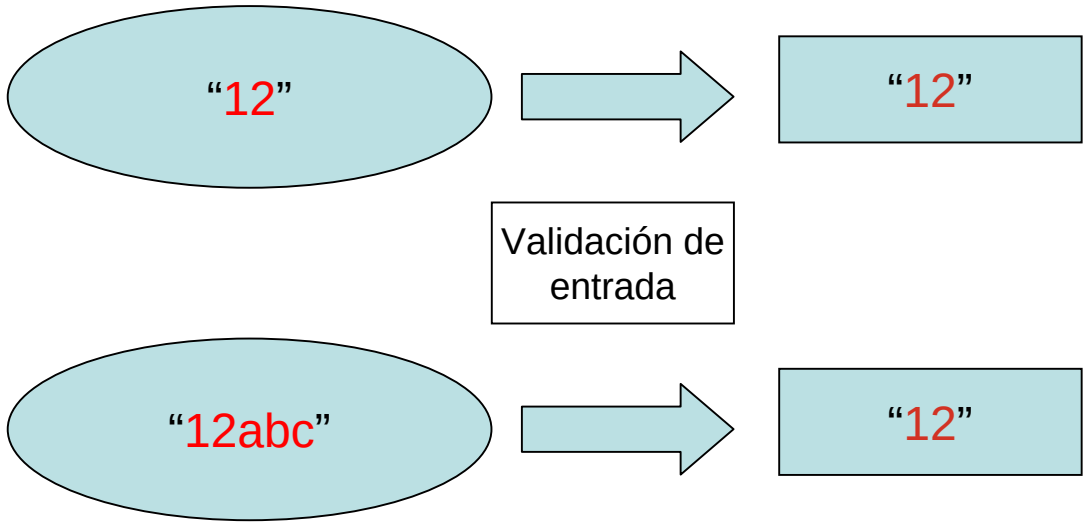
¡SI!



¿Validamos la entrada? Sí, la entrada de datos es un cambio de contexto.

•Si el dato de entrada es de un tipo cerrado o debe cumplir una serie de condiciones debemos filtrar y/o verificar que los datos son correctos.

- Ejemplo: Dato de entrada en una aplicación web que contiene un identificador numérico.



<B>’¿Dudas?\<B>

<B>\’¿Dudas?\\<B>

<B>?¿Dudas?<B>