



OWASP

The Open Web Application Security Project



OWASP

The Open Web Application Security Project

somosDAS.com

[IN]SEGURIDAD WEB



#LaCulpaEsDelProgramador



OWASP

The Open Web Application Security Project



Saúl Mamani M.

Ingeniero Informático

Facultad Nacional de Ingeniería

Oruro – Bolivia

@kanito777

mail: luas0_1@yahoo.es

cel: +591 76137269

www.somosdas.com

✖ ! hacker

✖ ! cracker

❤ Seguridad Informática



OWASP

The Open Web Application Security Project

Páginas Web



OWASP

The Open Web Application Security Project



Páginas Web

Aplicaciones Web



OWASP

The Open Web Application Security Project



Páginas Web

Servicios Web

Aplicaciones Web



OWASP

The Open Web Application Security Project

Páginas Web

Servicios Web

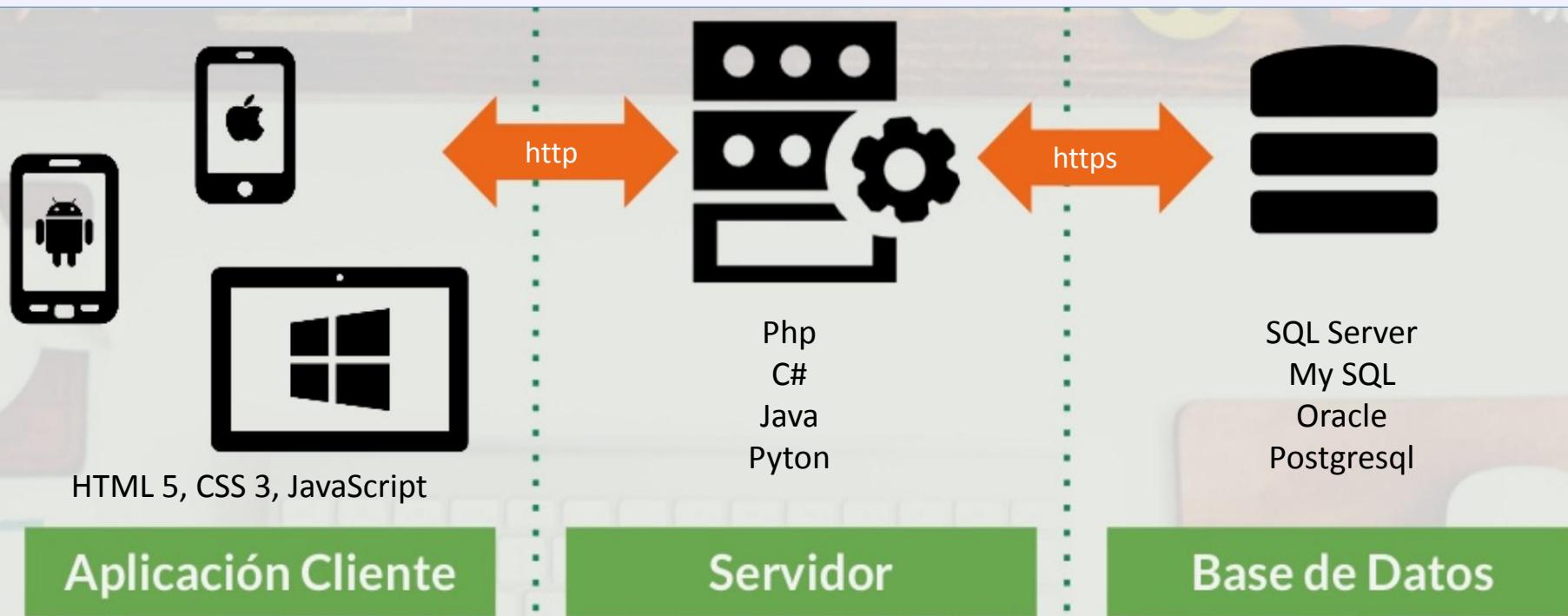
Aplicaciones Web



OWASP

The Open Web Application Security Project

Fundamentos de las Aplicaciones Web:

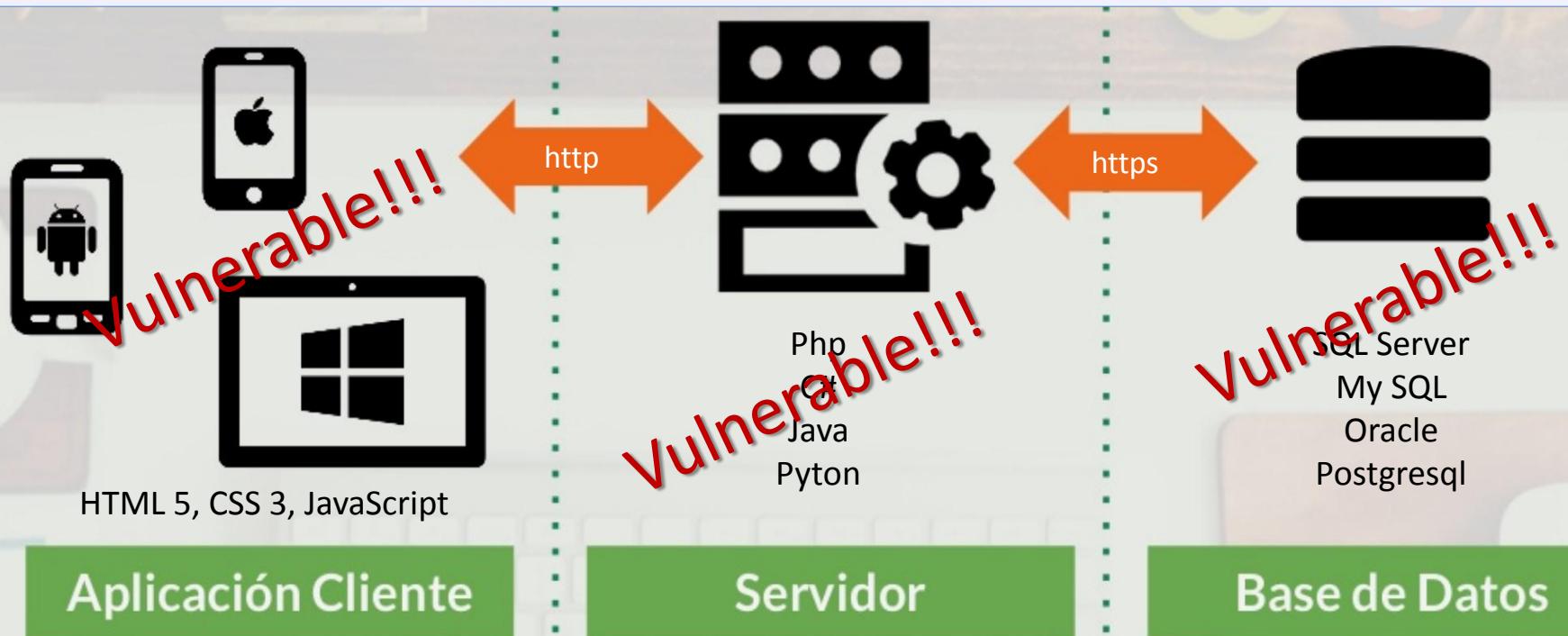




OWASP

The Open Web Application Security Project

Fundamentos de las Aplicaciones Web:





OWASP

The Open Web Application Security Project

La mayoría de los **problemas de seguridad** en los sistemas web se encuentran a **nivel de aplicación** y son el resultado de **escritura defectuosa** de código. (malos hábitos de los **programadores**).

Programar aplicaciones web seguras, no es una tarea fácil.



OWASP

The Open Web Application Security Project

¿Por qué?



OWASP

The Open Web Application Security Project

La probabilidad que un mono se siente delante de una maquina y escriba una poesía...





OWASP

The Open Web Application Security Project

La probabilidad que un mono se siente delante de una maquina y escriba una poesía... **NO ES CERO!**





OWASP

The Open Web Application Security Project



EL PROGRAMA FUNCIONA !!!!

Y NO TENGO IDEA DE LO QUE HIZE



OWASP

The Open Web Application Security Project

El mundo demanda software, pero...



OWASP

The Open Web Application Security Project

Software de Calidad

Concordancia del Software Desarrollado con los Requerimientos Funcionales explícitamente establecidos, con los estándares explícitamente documentados y con toda característica (escalabilidad, robustez, confiabilidad, **seguridad**, etc.) implícita que se espera un buen software.



OWASP

The Open Web Application Security Project

NO SOLO SE TRATA DE PROGRAMAR ARTESANALMENTE !!!



OWASP

The Open Web Application Security Project

No es lo mismo construir, esto...





OWASP

The Open Web Application Security Project

No es lo mismo construir, esto...



Que...



OWASP

The Open Web Application Security Project

No es lo mismo construir, esto...



0...



Que...





OWASP

The Open Web Application Security Project

TENEMOS QUE APLICAR **INGENIERIA** A NUESTROS PROYECTOS

¿y cuál de las ingenierías?



OWASP

The Open Web Application Security Project

Ingeniería de Software

Conjunto de **Métodos, Técnicas y Herramientas** para Desarrollar y MANTENER **Software de Calidad** (y su documentación asociada) de modo **Fiable, Rentable** y que trabaje en máquinas reales.



OWASP

The Open Web Application Security Project

Proceso | Metodología

RUP
AUP
Scrum
XP
Cascada



Rational Unified Process



Ingeniería
de
Software

Notación



- UML
- BPMN
- Leng. Estructurado

Herramientas



- Visual Studio, Eclipse, Netbean
- Enterprise Architect,
- C#, PHP, Python, MySQL, etc.



OWASP

The Open Web Application Security Project



Pero un proyecto sw que cumpla con todos los requisitos funcionales,
no es necesariamente seguro....

USABILIDAD <> SEGURIDAD

No solo deben cumplir con la funcionalidad, sino que también deben ser seguros
La seguridad debe ser transparente al usuario

No existe un manual que te diga como desarrollar aplicaciones web 100% seguras



OWASP

The Open Web Application Security Project

Principales Vulnerabilidades Owasp TOP 10

(errores de programación)

<https://www.owasp.org>

OWASP Top 10 – 2013 (Nuevo)

A1 – Inyección

A2 – Pérdida de Autenticación y Gestión de Sesiones

A3 – Secuencia de Comandos en Sitios Cruzados (XSS)

A4 – Referencia Directa Insegura a Objetos

A5 – Configuración de Seguridad Incorrecta

A6 – Exposición de Datos Sensibles

A7 – Ausencia de Control de Acceso a las Funciones

A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)

A9 – Uso de Componentes con Vulnerabilidades Conocidas

A10 – Redirecciones y reenvíos no validados

Fusionado con 2010 A7 en la nueva 2013 A6



OWASP

The Open Web Application Security Project

Principales Vulnerabilidades Owasp TOP 10

(errores de programación)

<https://www.owasp.org>

OWASP Top 10 – 2013 (Nuevo)

A1 – Inyección

A2 – Pérdida de Autenticación y Gestión de Sesiones

A3 – Secuencia de Comandos en Sitios Cruzados (XSS)

A4 – Referencia Directa Insegura a Objetos

A5 – Configuración de Seguridad Incorrecta

A6 – Exposición de Datos Sensibles

A7 – Ausencia de Control de Acceso a las Funciones

A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)

A9 – Uso de Componentes con Vulnerabilidades Conocidas

A10 – Redirecciones y reenvíos no validados

Fusionado con 2010 A7 en la nueva 2013 A6

FINGERPRINTERING

ATAQUES DE



ATAQUE: FINGERPRITING

Recolectar información, analizarla y clasificarla para identificar los recursos tecnológicos utilizados por un objetivo determinado.



Herramientas:



https://www.owasp.org/index.php/Main_Page

HTTPRECON <https://w3dt.net/tools/httprecon>



<http://tools.whois.net/>

ATAQUE: FINGERPRITING

Los Mensajes de Error, siempre muestran información vulnerable

```
System.ArgumentException: No se puede convertir saul en System.Double.  
Nombre del parámetro: type ---> System.FormatException: La cadena debe ser un número válido.  
en System.Number.StringToNumber(String str, NumberStyles options, NumberFormatInfo info)  
en System.Number.ParseDouble(String value, NumberStyles options, NumberFormatInfo info)  
en System.Double.Parse(String s, NumberStyles style, NumberFormatInfo info)
```

Asp.Net

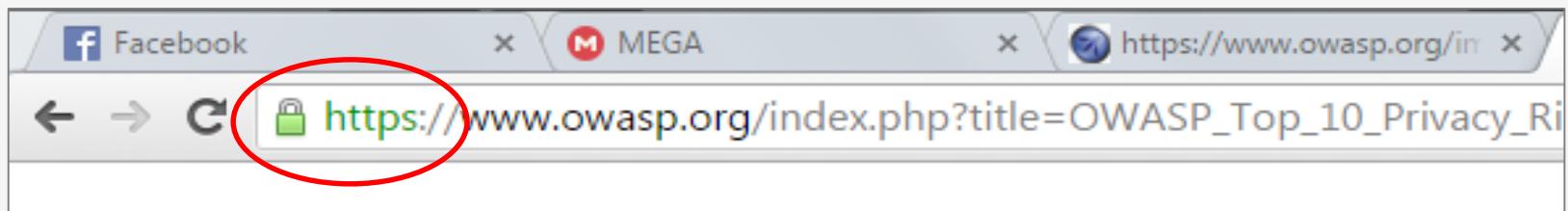
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
C:\xampp\htdocs\malditaweb\perfil.php on line **20**

© Saul Mamani

Php

TECNICAS DEFENSIVAS: FINGERPRITING

Utilice certificados de seguridad (SSL)



Deshabilite los mensajes de error del servidor de app.

```
<customErrors mode="On" defaultRedirect="error.html" />
</system.web>
</configuration>
```

**Web.config
ASP.Net**

error_reporting=~E_ALL & ~E_DEPRECATED & ~E_STRICT

php.ini

TECNICAS DEFENSIVAS: FINGERPRITING



Mostrar Mensajes de Error Genéricos

```
<string xmlns="http://dasinf.org/">
    <script id="tinyhippos-injected"/>
    Ha ocurrido un Error
</string>
```

Maneje excepciones a la hora de programar sus código fuente

```
public String RaizCuadrada(string a)
{
    try
    {
        return Math.Sqrt(Convert.ToDouble(a)).ToString();
    }
    catch (Exception)
    {
        return "Ha ocurrido un Error";
    }
}
```



ATAQUES DE INYECCION SQL – XSS

ATAQUE: SQL Injection



Inyección SQL. La inyección de comandos SQL es una técnica donde un atacante crea o altera comandos SQL existentes para exponer datos ocultos...

Top 1 OWASP

Herramientas:



<https://www.mozilla.org/es-ES/firefox/developer/>



http://sourceforge.net/projects/sqlmap/?source=typ_redirect



<http://www.sqlpowerinjector.com/>



OWASP

The Open Web Application Security Project

Inyección SQL:

```
select *  
from usuario  
where  
Cuenta = 'admin' and Clave = 'admin123'
```



OWASP

The Open Web Application Security Project

Inyección SQL:

```
select *  
from usuario  
where      V      y      V      = V  
Cuenta = 'admin' and Clave = 'admin123'
```



OWASP

The Open Web Application Security Project

Inyección SQL:

```
select *  
from usuario  
where      F      y      F      o      v  = V  
Cuenta = ' xxx' and Clave = '' or ' 1 ' = ' 1 '
```



OWASP

The Open Web Application Security Project

Inyección SQL:

' OR '='

' or true --

' OR '1'='1' --

The screenshot shows a login interface for a system named MUÑA. The title is "Ingreso al Sistema". There are two input fields: one for "Nombre de Usuario" (Username) containing "' or '1'='1" and another for "Contraseña" (Password) containing a series of dots (...). A large blue button labeled "Ingresar" (Login) is at the bottom. Below the button, a link "(Regístrate para obtener una cuenta)" (Register to get an account) is visible.

MUÑA

Ingreso al Sistema

' or '1'='1

Contraseña

Ingresar

(Regístrate para obtener una cuenta)



OWASP

The Open Web Application Security Project

Inyección SQL:

http://.../xyz.php?id=-1 UNION SELECT ALL
1,2,3,4,5,6

http://.../xyz.php?id=-1 UNION SELECT
1,2,DATABASE(),4,5,6



OWASP

The Open Web Application Security Project

Inyección SQL:

Screenshot of a web browser showing a SQL injection exploit on a user profile page.

URL bar: localhost:3000/muna/perfil.php?id=id=-1 UNION SELECT 1,2,DATABASE(),4,5,6

Page Title: Mi Perfil

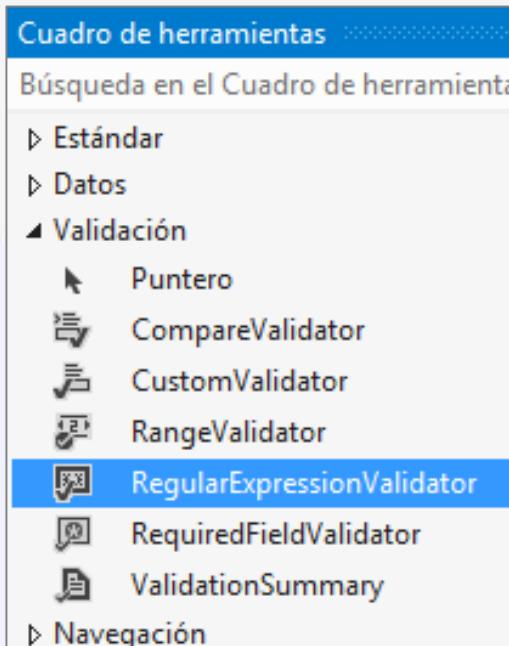
User Profile Information:

- Cuenta: 2
- Clave: malditawebd
- Nombre: 4
- Apellido: 5

The "Clave" field is highlighted with a red oval, indicating it is the target for the exploit.

TECNICAS DEFENSIVAS: SQL Injection

Valide los datos, tanto en el **Cliente** como en el **Servidor**



Autenticación

Cuenta: Formato no Válido
Clave: Requerido

Los componentes de validación de Visual Studio, validan los datos en el cliente (Java Script) y en el Servidor (C#, VB)

TECNICAS DEFENSIVAS: SQL Injection

Valide los datos, tanto en el **Cliente** como en el **Servidor**

```
27     function sanatizar($dato)
28     {
29         // limpiando espacio en blanco
30         $dato = trim($dato);
31         // aplicando stripslashes si magic_quotes
32         if(get_magic_quotes_gpc())
33         {
34             $dato = stripslashes($dato);
35         }
36         // un mySQL connection es requerido antes
37         $dato = mysql_real_escape_string($dato);
38         return $dato;
39     }
```

Método PHP para filtrar datos de entrada. Protección SQL injection
Utilice consultas parametrizadas.
Sería interesante utilizar Listas Blancas

TECNICAS DEFENSIVAS: SQL Injection



- Utilice Ajax para enviar datos de formularios



<https://norfipc.com/inf/como-proteger-formularios-web-evitar-inyección-código-sql.php>

- Evítese de enviar datos por la URL (Método GET)
- No confíe en los datos ingresado por el cliente (Pruebas de Software Caja Negra).

Válido también para SQL Injection, XSS, XML Injection, entre otros.

TECNICAS DEFENSIVAS: SQL Injection



- Utilice un framework de desarrollo



Symfony



Equilibrio!!!



ATAQUE: XSS Cross-Site Scripting

XSS. Permite a una tercera persona injectar código JavaScript, HTML u otro lenguaje similar a una pagina web.



Herramientas:



http://sourceforge.net/projects/sqlmap/?source=typ_redirect



<http://jcarlosrendon.morelosplaza.com/herramientas/ofuscador.php>
<http://myobfuscate.com/?lang=es>





OWASP

The Open Web Application Security Project

XSS:

Nombre:

```
<script>alert('Has sido hackeado!');</script>
```

Descripcion:

```
Lamentablemente has sido hackeado
```

Aceptar [Cancelar](#)



OWASP

The Open Web Application Security Project

XSS:

A screenshot of a web browser window titled "Maldita Aplicacion Web". The address bar shows "localhost:3000/malditaweb/perfil.php?id=11". The main content area displays a profile page with fields for "Cuenta: lidia" and "Clave: 123456". A modal dialog box is overlaid on the page, containing the message "Mensaje de la página localhost:3000:" followed by "Has sido hackeado". There is a checkbox labeled "Evita que esta página cree cuadros de diálogo adicionales." and a blue "Aceptar" button.



OWASP

The Open Web Application Security Project

XSS:

```
http://.../xyz.php?id  
=<SCRIPT>alert('hacked by me');</SCRIPT>
```

```
http://.../xyz.php?id  
=<SCRIPT>while(1);</SCRIPT>
```



OWASP

The Open Web Application Security Project

XSS:

A screenshot of a website for 'Proimágenes Colombia' (Comisión Filmica). The URL in the browser is www.locationcolombia.com/oldsite_2014/secc. A modal dialog box is displayed in the center of the page with the text 'hacked by me:
Saul Mamani'. Below the dialog is a button labeled 'Aceptar'. The main content area shows sections like 'COLOMBIA: UN MUNDO POR DESCUBRIR', 'REGIONES Y LOCACIONES', 'GUÍA DE PRODUCCIÓN', 'DIRECTORIO DE', 'COMISIÓN FÍLMICA', and 'PRODUCCIONES'. There are also links for 'MIEMBRO DE AFCI', 'NOTICIAS', 'ENGLISH V', and 'Convenciones'.

A screenshot of a web application titled 'Perfil de Usuario' (User Profile) from the URL localhost:3000/malditaweb/perfil.php?id=12. The page displays user information: 'Cuenta: lisa', 'Clave: 12345', 'Nombre: lisa del monte', and 'Descripción:'. Below this, a large bold message reads 'Has sido hackeado por kanito'. At the bottom is a photo of a brown rabbit sitting at a desk with a computer monitor.



TECNICAS DEFENSIVAS: XSS

- Al igual que en el ataque por *sql injection* VALIDAR y ESCAPAR datos de entrada y salida.

Php

```
<td><?php echo utf8_encode($f['cuenta']); ?></td>
<td><?php echo htmlentities(utf8_encode($f['Nombre'])); ?></td>
<td><?php echo htmlentities(utf8_encode($f['Descripcion'])); ?></td>
<td><?php echo utf8_encode($f['FechaRegistro']); ?></td>
<td><a href="perfil.php?id=<?php echo $f['Id']; ?>">ver</a></td>
'
```

Asp.Net

```
Server.HtmlEncode("<your string>");
```

```
Server.HtmlDecode("&lt;your string&gt;");
```

Válido también para SQL Injection, XSS, XML Injection, entre otros.

TECNICAS DEFENSIVAS: XSS



- Cifra, encripta u ofusga tu código, para evitar que te envíen parámetros manipulados.

```
<html>
  <head>
    <title>Maldita Aplicacion Web</title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, i
  </head>
  <body>
    <div style="text-align: left; margin-top: 70px; padding-left: 10px;>
      <h1>Nuevo Usuario</h1>
      <hr>
      <form name="frmLogin" action="nuevoController.php" method="post">
        <label for="txtCuenta">Cuenta:<br> </label><input type="text" name="txtCuenta" value="<script>document.write('
        <label for="txtClave">Clave:<br> </label><input type="password" name="txtClave" value="<script>document.write('
        <label for="txtNombre">Nombre:<br> </label><input type="text" name="txtNombre" value="<script>document.write('
        <label for="txtDesc">Descripcion:<br> </label><input type="text" name="txtDesc" value="<script>document.write('
        <input type="submit" value="Aceptar" name="btnAceptar">
        <a href="listar.php">(Cancelar)</a>
      </form>
```



```
<script language="javascript" type="text/javascript">
3c0V2Z81mcvZ2Qzw3bpJXY1NXVwIDfu9WajBXayN2c1RURzwXMoxn
GbyIDf5R2bixHf5B3bjZjM852bpR3YhBjM85Wan9GTtJnZyIDf21G
3YzxXYDNDf01WbiV3cyIDfv2XZ15URzwHbtRHa8JXY0BXZjFkMywH
3cDNDf0J3bwXZpZnMywXMENDf05WZ052bjBjM8xWZiFGbwIDfhRX
wBjNwIDf39GbmJXZ29GMywXZs1HdzBjM8ZXakN0M81HzvJ2Qzwnbn
c3xHd1BnbpBjM85WZkRWaoBjM8RHan1WZoBjM8hHcwAzMwIDf4BH
Ed4RnMywXZwF2YzV2X8Vmduh2Q0hHdyIDf0ZWZsxXSwwGfyFmd8BH
NDf3ITM8hGdkl2dwIDfBBdfyJ2QzwXZtFmbwIDf1BXe0BjM8dmbpJ
ONmb12GfuJXd0Vmc8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8
f8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf
Hf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf
NUN8NXN8RVN8RXN8JXN8FXN85WN89WN8BXN8VXN8ZXN8FUN8JUN8p
VVdfWVdfXVDfxYDfzYDf4YDf5YDf3YDf2YDf12Df0Rdf1YDfJVdfj
Q0wHc0wHe0wHb0wnco0wxe0wxd0wHfLRDfsVdfiVdfRRDfhVdf5UDf
```

<http://jcarlosrendon.morelosplaza.com/herramientas/ofuscador.php>
<http://myobfuscate.com/?lang=es>

Index of /biblioteca/Libros varios

Name

Exposición insegura de RECURSOS

[Parent Directory](#)

[ética en Primaria.ppt](#)

24-Jan-2014 17:09 52K

[50sombras.pdf](#)

16-Jun-2015 09:23 2.4M

[APUNTES SOBRE LA CIBERCULTURA.pdf](#)

24-Jan-2014 17:09 2.1M

[APUNTES SOBRE LA PEDAGOGÍA CRÍTICA.pdf](#)

24-Jan-2014 17:04 1.4M

[APUNTES SOBRE LA PEDAGOGÍA CRÍTICA II .pdf](#)

24-Jan-2014 17:04 2.0M

[Alicia En El pais De Las Maravillas.pdf](#)

24-Jan-2014 17:09 397K

[Analisis y diseno de experimentos Salazar.pdf](#)

16-Jun-2015 09:23 330K

[Antigonas.pdf](#)

24-Jan-2014 17:08 259K

[Articulo Ética en los maestros.pdf](#)

24-Jan-2014 17:04 197K

[BOOKS \(DOC\)/](#)

24-Jan-2014 17:08 -

[BOOKS \(LIT\)/](#)

24-Jan-2014 17:06 -

[BOOKS \(PDF\)/](#)

24-Jan-2014 17:09 -

[BOOKS \(TXT\)/](#)

24-Jan-2014 17:09 -

[BOOKS \(ZIP\)/](#)

24-Jan-2014 17:06 -

[Brown, Dan - Angeles y demonios.doc](#)

24-Jan-2014 17:06 2.5M

[Coelho, Paulo - Brida.doc](#)

24-Jan-2014 17:08 450K

[Coelho, Paulo - El Zahir.doc](#)

24-Jan-2014 17:06 896K

[García, Raúl - Un libro de 144 páginas.pdf](#)

24-Jan-2014 17:06 441K

TECNICAS DEFENSIVAS: EXPOSICION



- Utiliza Robots.txt para ocultarlo de los navegadores y .htaccess para proteger los archivos y las carpetas

A screenshot of a code editor showing a file named "Robots.txt". The content of the file is:

```
1 User-Agent: *
2 Disallow: /*.asmx
3 Disallow: /*?wsdl
```

Robots.txt

A screenshot of a code editor showing a file named ".htaccess". The content of the file is:

```
1 Options All -Indexes
2
3 # Error
4 ErrorDocument 403 /muna/error.html
5 ErrorDocument 404 /muna/error.html
```

.htaccess

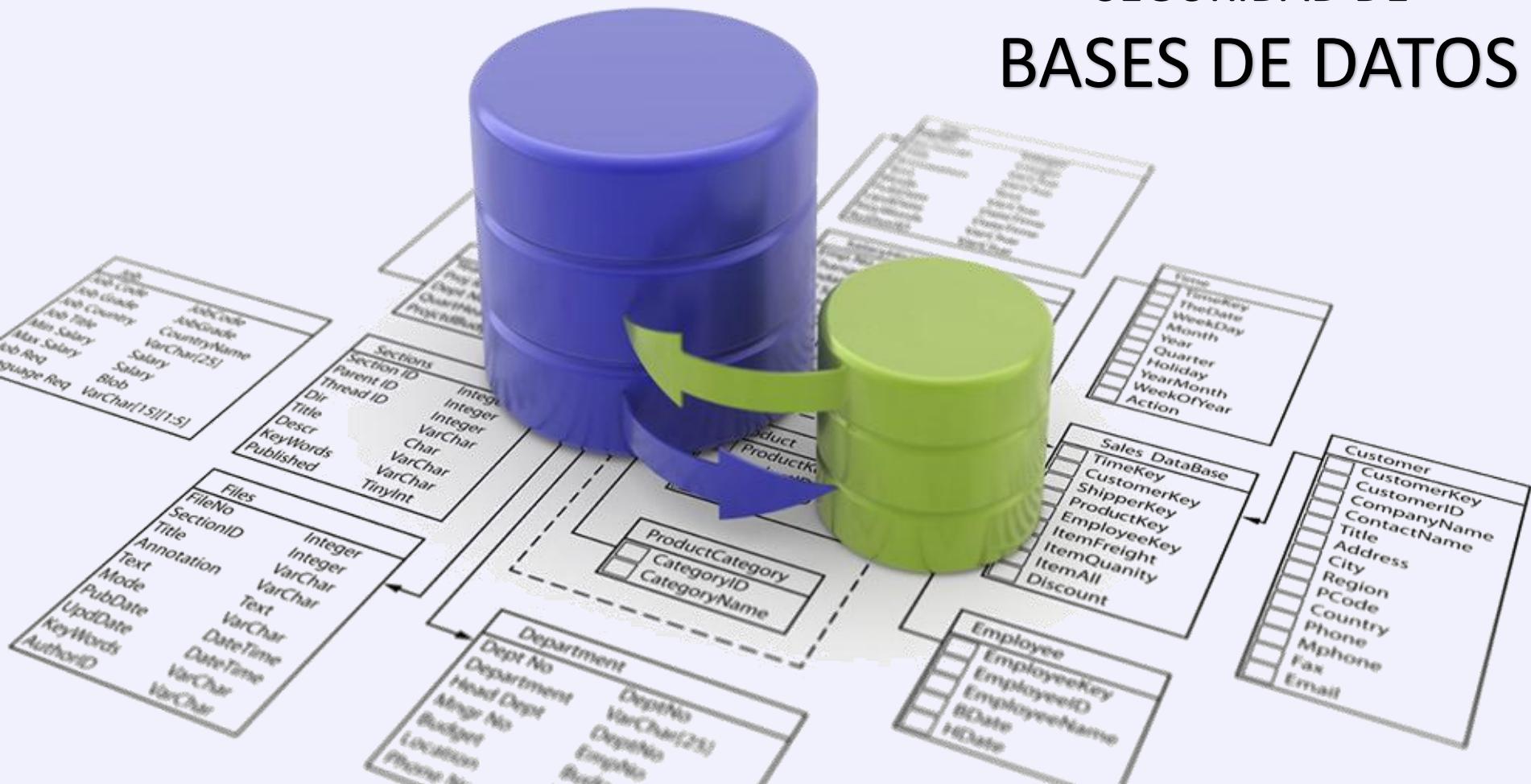


OWASP

The Open Web Application Security Project

https://www.owasp.org

SEGURIDAD DE BASES DE DATOS



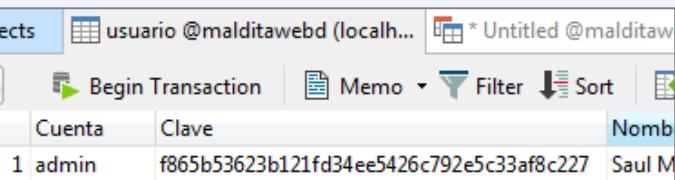


OWASP

The Open Web Application Security Project

Las contraseñas nunca se guardan en texto plano.

```
md5("miclave")
Sha1("miclave") ...
(encriptación solo de ida)
```



A screenshot of a database management system interface showing a table with user data. The table has columns: Cuenta, Clave, and Nombre. One row is visible: admin, f865b53623b121fd34ee5426c792e5c33af8c227, Saul M.

Cuenta	Clave	Nombre
1 admin	f865b53623b121fd34ee5426c792e5c33af8c227	Saul M

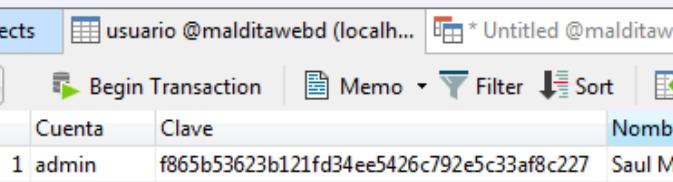


OWASP

The Open Web Application Security Project

**Las contraseñas nunca se
guardan en texto plano.**

```
md5("miclave")
Sha1("miclave") ...
(encryptación solo de ida)
```



A screenshot of a database management system interface showing a table of user credentials. The table has columns for Cuenta (Account), Clave (Password), and Nombre (Name). One row is visible: admin with password f865b53623b121fd34ee5426c792e5c33af8c227 and name Saul M.

Cuenta	Clave	Nombre
1 admin	f865b53623b121fd34ee5426c792e5c33af8c227	Saul M



Usuarios y Privilegios.

Usuarios solo con los privilegios necesarios



OWASP

The Open Web Application Security Project

**Las contraseñas nunca se
guardan en texto plano.**

```
md5("miclave")
Sha1("miclave") ...
(encryptación solo de ida)
```

Projects		
usuario @malditawebd (localhost)		
* Untitled @malditawebd		
	Begin Transaction	Memo
	Filter	Sort
Cuenta	Clave	Nomb
1 admin	f865b53623b121fd34ee5426c792e5c33af8c227	Saul M



Replicación de Datos.

Servidores de Base de datos con réplica

Usuarios y Privilegios.

Usuarios solo con los privilegios necesarios



OWASP

The Open Web Application Security Project

**Las contraseñas nunca se
guardan en texto plano.**

```
md5("miclave")
Sha1("miclave") ...
(encryptación solo de ida)
```

Projects			
usuario @malditawebd (localhost)		* Untitled @malditawebd	
		Begin Transaction	Memo
		Filter	Sort
Cuenta	Clave	Nomb	
1 admin	f865b53623b121fd34ee5426c792e5c33af8c227	Saul M	



Replicación de Datos.

Servidores de Base de datos con réplica

Usuarios y Privilegios.

Usuarios solo con los privilegios necesarios

Federación de Datos.

Base de Datos federados
(solo estructura)



OWASP

The Open Web Application Security Project

Muña v0.9

Es una aplicación web vulnerable para practicar ataques del tipo inyección sql, xss, span, base de datos, exposición de recursos. etc.

Descargar:

www.somosdas.com/muna

The screenshot shows the login interface of the Muña application. At the top right, there are links for 'Ataque' (Attack) and 'Defensa' (Defense). The main title is 'MUÑA' with a leaf icon. Below it is the subtitle 'Ingreso al Sistema'. There are two input fields: the first contains the value "' or '1'='1' --" and the second contains a series of dots. A large blue button labeled 'Ingresar' (Enter) is positioned below the inputs. To the right of the inputs, a link says '(Regístrate para obtener una cuenta)' (Register to get an account). A yellow callout box at the bottom left contains the text 'Bienvenidos:' (Welcome) and a descriptive paragraph about the application's purpose. Another link in the callout box says 'Aqui puede descargar el código fuente' (Here you can download the source code). At the very bottom of the page, there is a copyright notice: '© Ing. Saul Mamani M.'



OWASP

The Open Web Application Security Project



Conclusiones:

Entendamos **como funcionan las Aplicaciones Web** para conocer que **tipo de ataques** nos pueden realizar y saber **cómo defendernos**

Mantener **actualizados nuestros sistemas**

cambia periódicamente tus **credenciales de acceso**

Adoptar buenas **prácticas de programación**

Aplica normas y estándares de seguridad (**owasp, ISO27001, ISO 27002, etc.**)



OWASP

The Open Web Application Security Project

Conclusiones:

Usabilidad o Seguridad,
llegue a un punto de equilibrio (transparencia)

Personas y Procesos sobre Herramientas

Filtra, valida tus entradas y escapa tus salidas

Propone Soluciones Inteligentes

Módulo Administrador (escritorio) – Módulo Cliente (aplicación web)



OWASP

The Open Web Application Security Project



**TODO ESTO SIRVE,
PERO....**

¿CUÁL ES LA MEJOR HERAMIENTA DEFENSIVA?

Recuerda que la mayoría de los ataques a las aplicaciones web se deben a errores de programación... La culpa es del programador!!



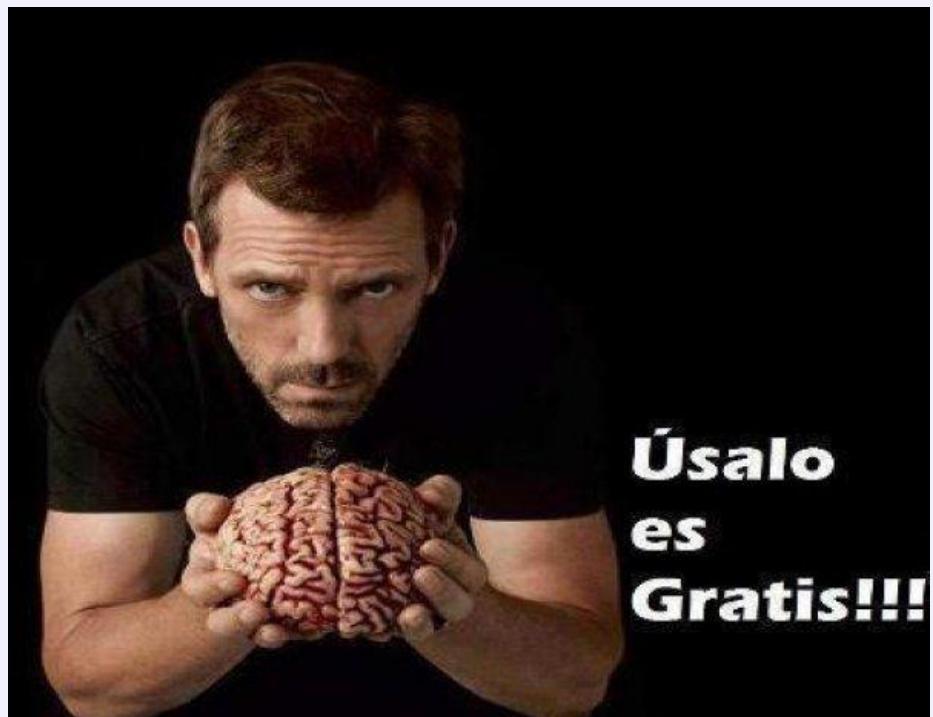
OWASP

The Open Web Application Security Project

TÚ Y TU CEREBRO....

Certificaciones:

- CEH: Certified Ethical Hacking
- CompTIA Security+
- Cisco CCNA Security
- CISSP: Certified Information System Security Professional
- Owasp



**Úsalo
es
Gratis!!!**



OWASP

The Open Web Application Security Project

MD5("GRACIAS");

3e0a5f7ef3ae90289abe88023b987cd9



OWASP

The Open Web Application Security Project

“ cebdb288f4f5c43a9219ceab15a7556404675dd3 ”