OWASP

The Open Web Application Security Project

OWASP
The Open Web Application Security Project

somosDAS.com

[IN]SEGURIDAD WEB

#LaCulpaEsDelProgramador

ING. SAUL MAMANI M.

Sobre mi

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

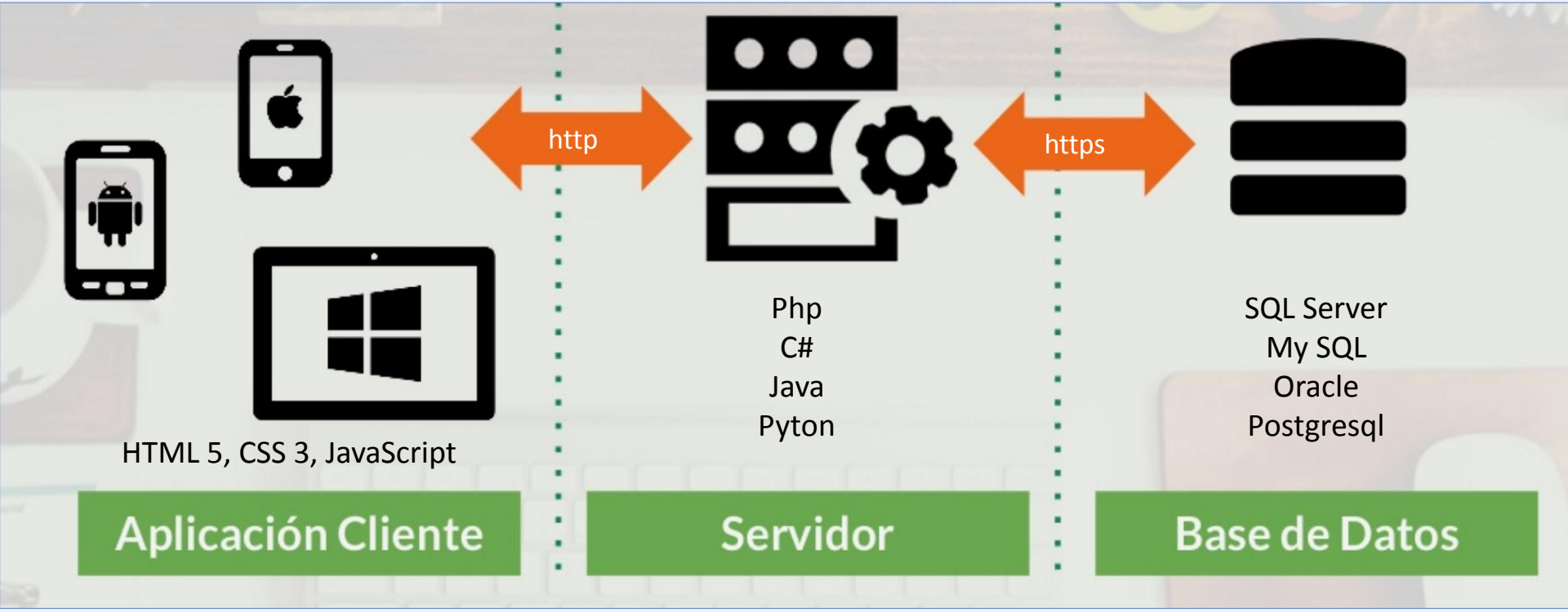
Páginas Web

Servicios Web

Aplicaciones Web

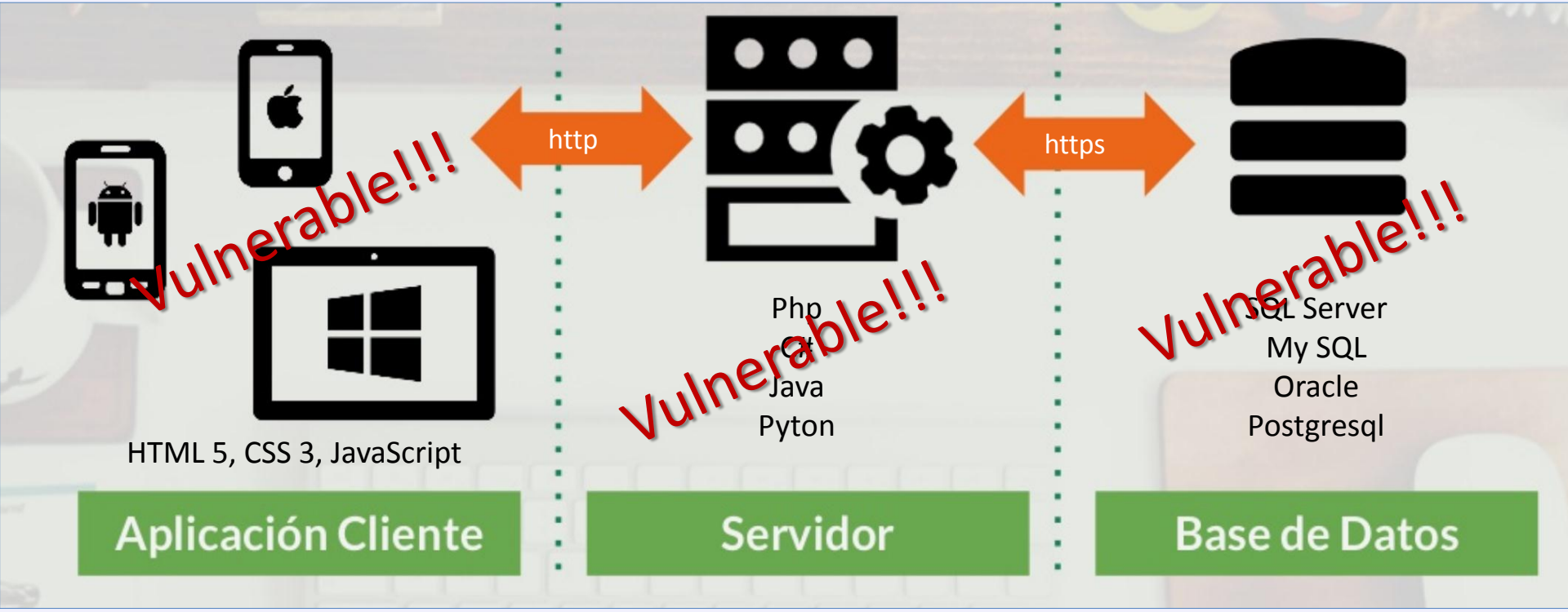
OWASP
The Open Web Application Security Project

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.

¿Por qué?

OWASP
The Open Web Application Security Project

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

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


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 !!!

No es lo mismo construir, esto…

No es lo mismo construir, esto…

Que…

OWASP
The Open Web Application Security Project

No es lo mismo construir, esto…

o…

Que…

OWASP
The Open Web Application Security Project

TENEMOS QUE APLICAR **INGENIERIA** A NUESTROS PROYECTOS

¿y cuál de las ingenierías?

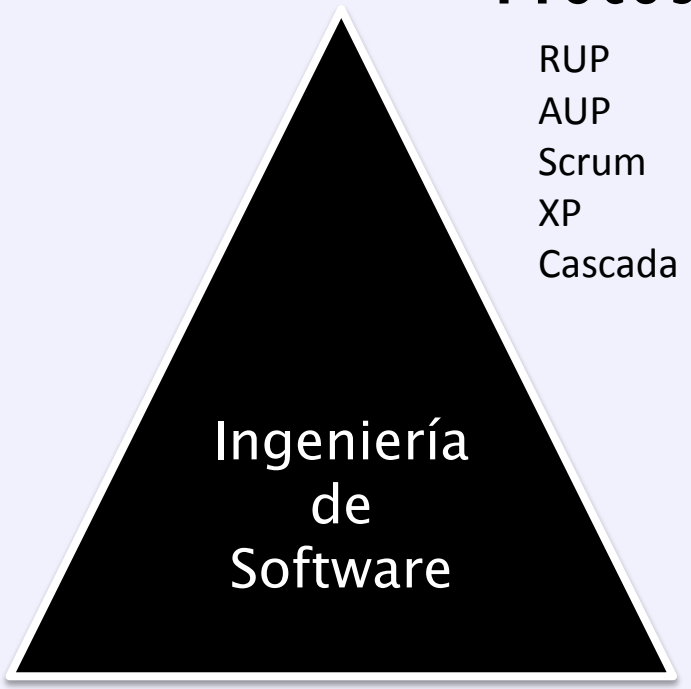
OWASP
The Open Web Application Security Project

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.

Proceso | Metodología

- RUP
- AUP
- Scrum
- XP
- Cascada



Notación

- UML
- BPMN
- Leng. Estructurado

Herramientas

- Visual Studio, Eclipse, Netbean
- Enterprise Architect,
- C#, PHP, Pyton, 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
Las 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 pogramación)

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 pogramación)

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


ATAQUES DE
FINGERPRITING

ATAQUE: FINGERPRITING

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

Herramientas:

OWASP The Open Web Application Security Project https://www.owasp.org/index.php/Main_Page

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

Whois.Net DOMAIN-BASED RESEARCH SERVICES 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 par&#225;metro: type ---> System.FormatException: La cadena d
   en System.Number.StringToNumber(String str, NumberStyles options, Num
   en System.Number.ParseDouble(String value, NumberStyles options, Numb
   en System.Double.Parse(String s, NumberStyles style, NumberFormatInfo
```

Asp.Net

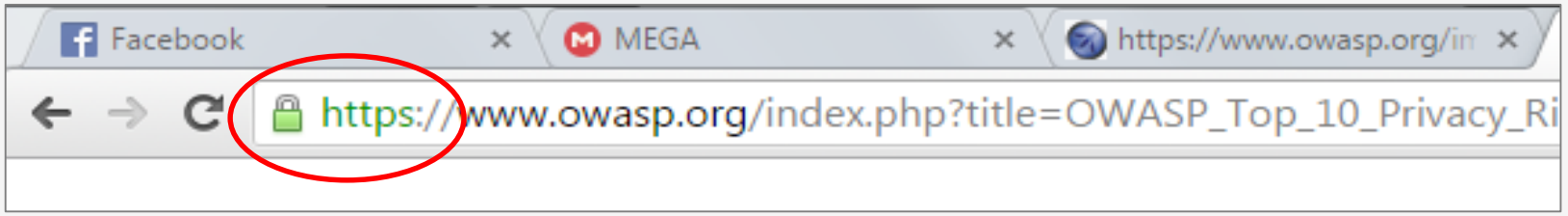
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in **C:\xampp\htdocs\malditaweb\perfil.php** on line **20**

© 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:

KALI LINUX

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
Cuenta = 'admin' and Clave = 'admin123'
```

V y V = V

Inyección SQL:

```
select *
from usuario
where
Cuenta = ' xxx' and Clave = '' or '1' = '1'
```

F y F o V = V

OWASP
The Open Web Application Security Project

Inyección SQL:

' OR ''='

' or true --

' OR '1'='1' --

OWASP
The Open Web Application Security Project

Inyección SQL:

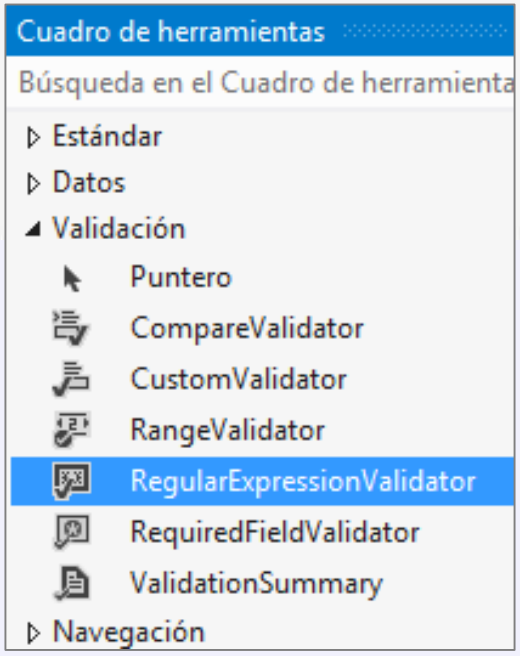
```
http://.../xyz.php?id=-1 UNION SELECT ALL
1,2,3,4,5,6
```

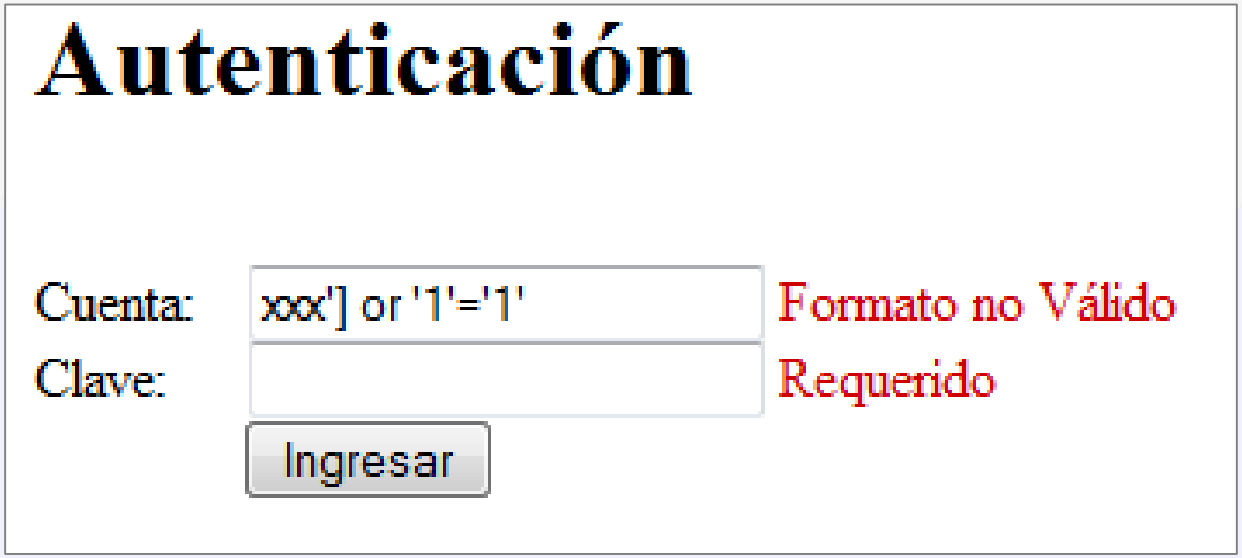
```
http://.../xyz.php?id=-1 UNION SELECT
1,2,DATABASE(),4,5,6
```

Inyección SQL:

TECNICAS DEFENSIVAS: SQL Injection

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





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 espacion 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

Equilibrio!!!

ATAQUE: XSS Cross-Site Scripting

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

Herramientas:

Firebug

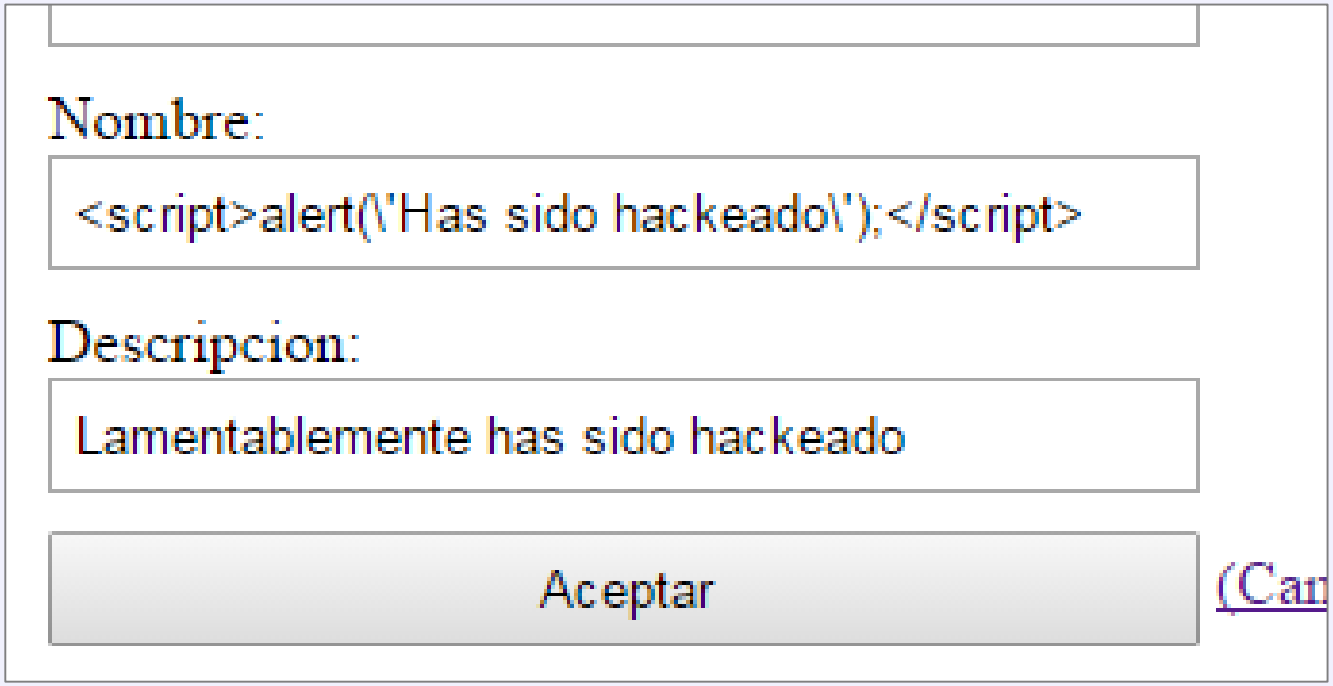
http://sourceforge.net/projects/sqlmap/?source=typ_redirect

Encriptado

http://jcarlosrendon.morelosplaza.com/herramientas/ofuscador.php

http://myobfuscate.com/?lang=es

XSS:


Nombre:
<script>alert(\'Has sido hackeado\');</script>
Descripcion:
Lamentablemente has sido hackeado
Aceptar

XSS:


Maldita Aplicacion Web
localhost:3000/malditaweb/perfil.php?id=11
Mensaje de la página localhost:3000:
Has sido hackeado
Evita que esta página cree cuadros de diálogo adicionales.
Aceptar
Perfil de Usuar
Cuenta: lidia
Clave: 123456
Nombre:

OWASP
The Open Web Application Security Project

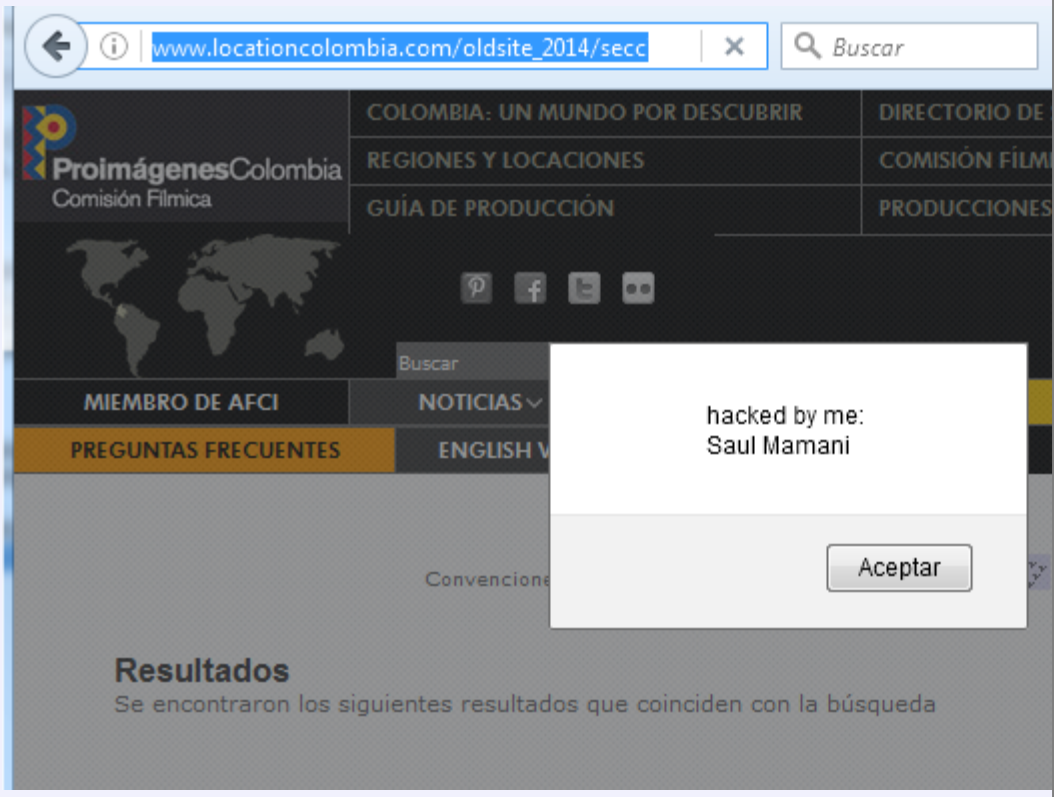
XSS:

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

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

OWASP
The Open Web Application Security Project

XSS:



TECNICAS DEFENSIVAS: XSS

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

Php

```
<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, ir
    </head>
    <body>
        <div style="text-align: left; margin-top: 70px; paddi
        <h1>Nuevo Usuario</h1>
        <hr>
        <form name="frmLogin" action="nuevoController.php" me
            <label for="txtCuenta">Cuenta:<br> </label><input
            <label for="txtClave">Clave:<br> </label><input t
            <label for="txtNombre">Nombre:<br> </label><input
            <label for="txtDesc">Descripcion:<br> </label><ir

            <input type="submit" value="Aceptar" name="btnAce
            <a href="listar.php">(Cancelar)</a>
        </form>
```

```
<script language="javascript" type="text/javascript">
3c0V2Z81mcvZ2Qzw3bpJXY1NXVwIDfu9WajBXayN2clRURzwXMoxn
GbyIDf5R2bixHf5B3bjZjM852bpR3YhBjM85Wan9GTtJnZyIDf21G
3YzxXYDNDf0lWbiV3cyIDfvZXZ15URzwHbtRHa8JXY0BXZjFkMywH
3cDNDf0J3bwdXZpZnMywXMENDf05WZ052bjBjM8xWZiFGbwIDfhRX
wBjNwIDf39GbmJXZ29GMywXZslHdzBjM8ZXakN0M8lHZvJ2Qzwnbn
c3xHd1BnbpBjM85WZkRWaoBjM8RHanlWZoBjM8hHcwAzMwIDf4BHM
Ed4RnMywXZwF2YzV2X8Vmdhx2Q0hHdyIDf0ZWZsxXSwwGfyFmd8BH
NDf3ITM8hGdkl2dwIDfBBDfyJ2QzwXZtFmbwIDflBXe0BjM8dmbpJ
0Nmb1ZGfuJXd0Vmc8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8
f8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf
Hf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xH
NUN8NXN8RVN8RXN8JXN8FXN85WN89WN8BXN8VXN8ZXN8FUN8JUN8p
VVDfWVDfXVDfxYDfzYDf4YDf5YDf3YDf2YDfiZDf0RDf1YDfJVDfj
Q0wHc0wHe0wHb0wnc0wXe0wXd0wHfLRDfsVDfiVDfRRDfhVDf5UDf
```

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

switch2011.upa.edu.mx/biblioteca/Libros varios/

Index of /biblioteca/Libros varios

Exposición insegura de
RECURSOS

Name		
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
Artículo 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

TECNICAS DEFENSIVAS: EXPOSICION

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

Robots.txt

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

Robots.txt

.htaccess

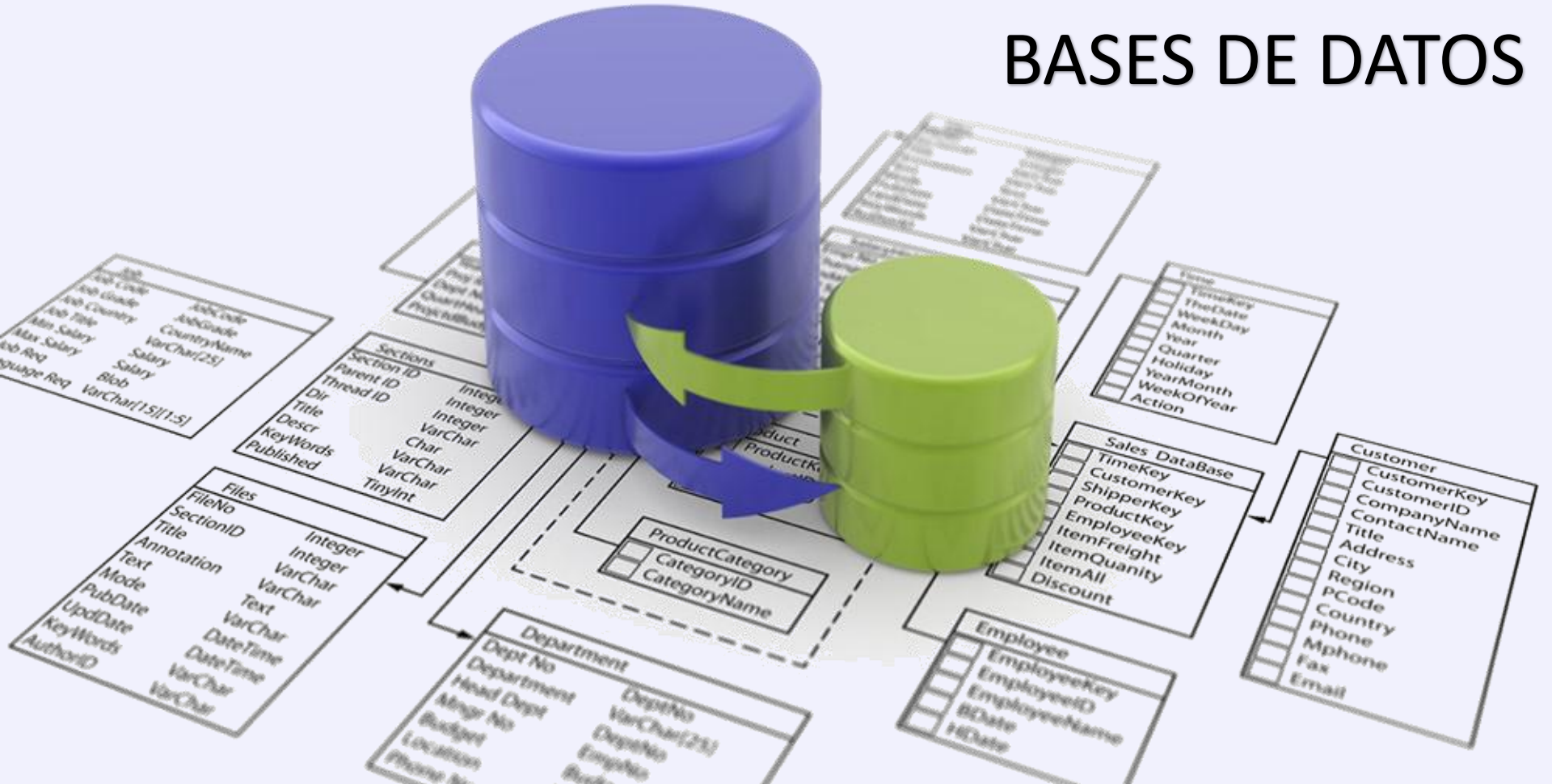
```
1  Options All -Indexes
2
3  # Error
4  ErrorDocument 403 /muna/error.html
5  ErrorDocument 404 /muna/error.html
```

.htaccess

OWASP
The Open Web Application Security Project

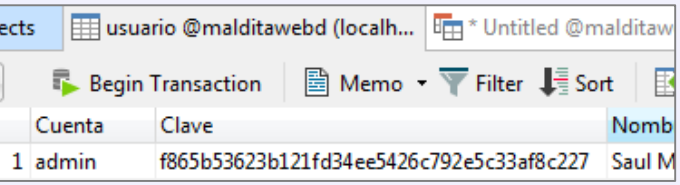
SEGURIDAD DE

BASES DE DATOS



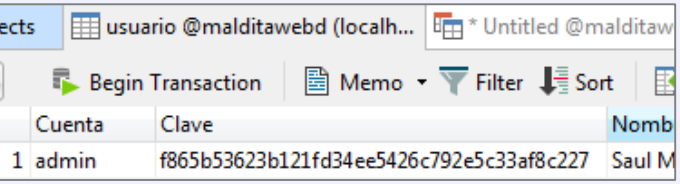
Las contraseñas nunca se guardan en texto plano.

md5(“miclave”)
Sha1(“miclave”) …
(encriptación solo de ida)



Las contraseñas nunca se guardan en texto plano.

md5(“miclave”)
Sha1(“miclave”) …
(encriptación solo de ida)

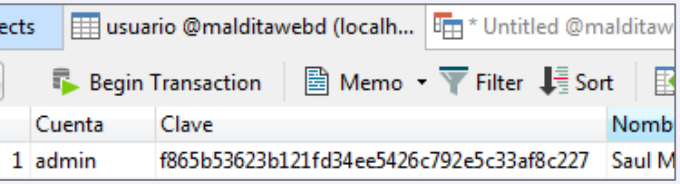


Usuarios y Privilegios.

Usuarios solo con los privilegios necesarios

Las contraseñas nunca se guardan en texto plano.

md5(“miclave”)
Sha1(“miclave”) …
(encriptación solo de ida)



Replicación de Datos.

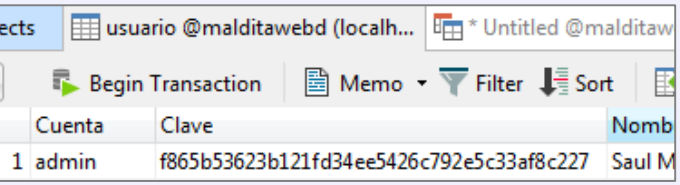
Servidores de Base de datos con réplica

Usuarios y Privilegios.

Usuarios solo con los privilegios necesarios

Las contraseñas nunca se guardan en texto plano.

md5(“miclave”)
Sha1(“miclave”) …
(encriptación solo de ida)



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)

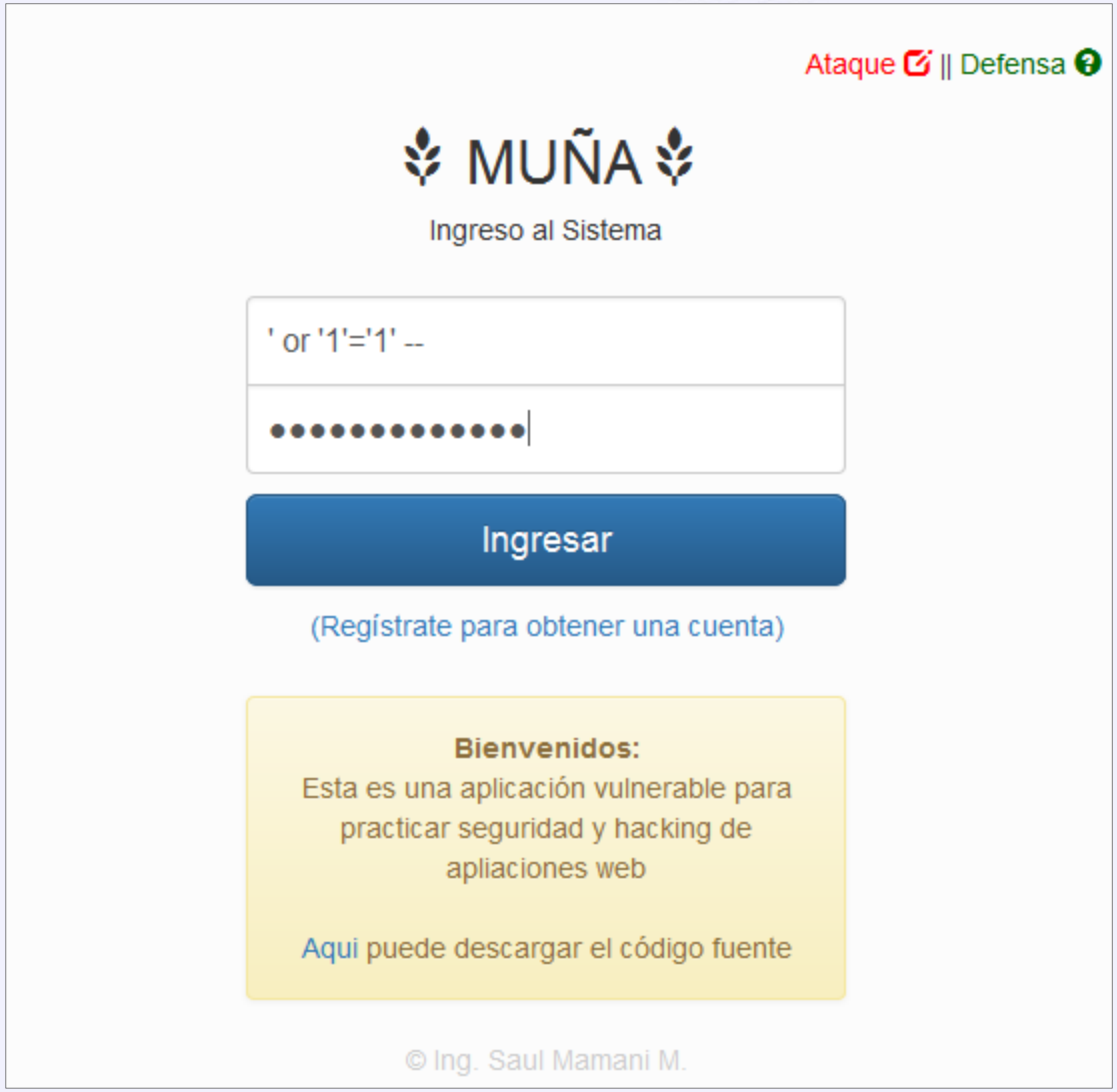
OWASP
The Open Web Application Security Project

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



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?

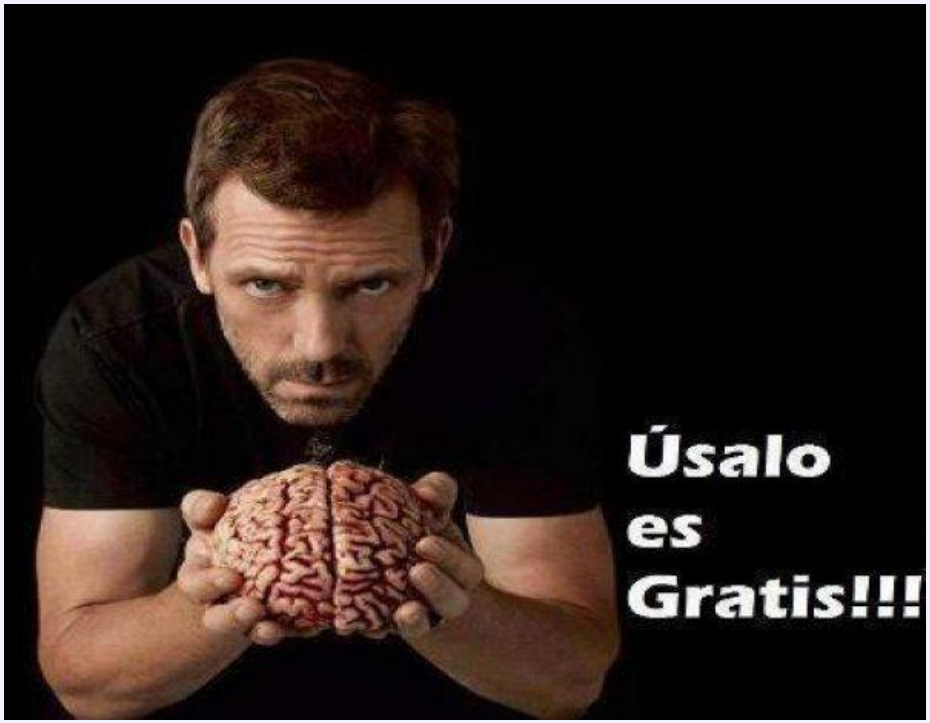
Recuerda que la mayoría de los ataques a las aplicaciones web se deben a errores de programación… La culpa es del programador!!

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



OWASP
The Open Web Application Security Project

MD5("GRACIAS");

3e0a5f7ef3ae90289abe88023b987cd9

OWASP

The Open Web Application Security Project

“ cebdb288f4f5c43a9219ceab15a7556404675dd3 ”