



ESCUELA POLITÉCNICA NACIONAL



Universitat d'Alacant
Universidad de Alicante

Seguridad de las aplicaciones web

Sergio Luján Mora

sergiolujanmora.es

sergio.lujan@ua.es

[@sergiolujanmora](#)

->> SLM <<-

S

Bienvenido a mi página personal. Actualmente se encuentra en desarrollo, así que espero que sepas perdonar los posibles errores que encuentres. Si quieres comunicarme un error en las páginas, tu crítica o una queja, puedes mandarme un correo electrónico a: slujan@dlsi.ua.es

La vida es aquello que te va sucediendo mientras tú te empeñas en hacer otros planes.
John Lennon (1940-1980), compositor británico.

— Presentación

— Viajes

— Senderismo

— Carreras

— Orientación

slujan@dlsi.ua.es

(c) Sergio Luján Mora, 1999

Última actualización:
12/02/2006

1998

HTML

CSS

JS

DOM

ASP

ActiveX

Applets

Servlets y JSP

ColdFusion

PHP

PROGRAMACIÓN EN INTERNET

Cientes Web

Sergio
Luján Mora

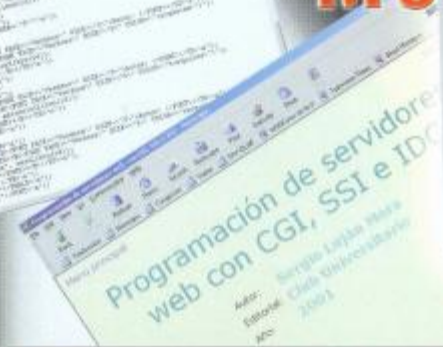


```
index.asp   
scriba.gif" height="28" width="100" valign="bottom" />  
cajete.gif" width="57" height="37" />  
"src" />  
border="1" cellpadding="5" cellspacing="1" />
```

PROGRAMACIÓN DE SERVIDORES WEB

con CGI, SSI e IDC

Sergio
Luján
Mora



ECU
EDITORIAL
CLUB
UNIVERSITARIO



PROGRAMACIÓN DE APLICACIONES WEB:
HISTORIA, PRINCIPIOS BÁSICOS Y CLIENTES WEB.
Sergio Luján Mora

Hand-drawn diagram of a web page layout with labels: LOGO, LISTA DESPLEGABLE, COLOR YELLOW, CUADRO DE TEXTO, BOTONES, OPCIONES MENU, MARCO RECTANGULAR, BORDE INVISIBLE, MARCO.

```

<div style="display: flex; justify-content: space-between; align-items: center;">
  <span>LOGO</span>
  <span>LISTA DESPLEGABLE</span>
</div>
<div style="border: 1px solid yellow; padding: 5px; margin: 10px 0;">
  <span>CUADRO DE TEXTO</span>
  <span>BOTONES</span>
</div>
<div style="display: flex; justify-content: space-between;">
  <span>OPCIONES MENU</span>
  <span>MARCO RECTANGULAR</span>
  <span>BORDE INVISIBLE</span>
  <span>MARCO</span>
</div>
  
```

Hand-drawn code snippets:

```

<div style="display: flex; justify-content: space-between; align-items: center;">
  <span>LOGO</span>
  <span>LISTA DESPLEGABLE</span>
</div>
<div style="border: 1px solid yellow; padding: 5px; margin: 10px 0;">
  <span>CUADRO DE TEXTO</span>
  <span>BOTONES</span>
</div>
<div style="display: flex; justify-content: space-between;">
  <span>OPCIONES MENU</span>
  <span>MARCO RECTANGULAR</span>
  <span>BORDE INVISIBLE</span>
  <span>MARCO</span>
</div>
  
```

Hand-drawn code snippets:

```

<div style="display: flex; justify-content: space-between; align-items: center;">
  <span>LOGO</span>
  <span>LISTA DESPLEGABLE</span>
</div>
<div style="border: 1px solid yellow; padding: 5px; margin: 10px 0;">
  <span>CUADRO DE TEXTO</span>
  <span>BOTONES</span>
</div>
<div style="display: flex; justify-content: space-between;">
  <span>OPCIONES MENU</span>
  <span>MARCO RECTANGULAR</span>
  <span>BORDE INVISIBLE</span>
  <span>MARCO</span>
</div>
  
```

Hand-drawn code snippets:

```

<div style="display: flex; justify-content: space-between; align-items: center;">
  <span>LOGO</span>
  <span>LISTA DESPLEGABLE</span>
</div>
<div style="border: 1px solid yellow; padding: 5px; margin: 10px 0;">
  <span>CUADRO DE TEXTO</span>
  <span>BOTONES</span>
</div>
<div style="display: flex; justify-content: space-between;">
  <span>OPCIONES MENU</span>
  <span>MARCO RECTANGULAR</span>
  <span>BORDE INVISIBLE</span>
  <span>MARCO</span>
</div>
  
```

Hand-drawn code snippets:

```

<div style="display: flex; justify-content: space-between; align-items: center;">
  <span>LOGO</span>
  <span>LISTA DESPLEGABLE</span>
</div>
<div style="border: 1px solid yellow; padding: 5px; margin: 10px 0;">
  <span>CUADRO DE TEXTO</span>
  <span>BOTONES</span>
</div>
<div style="display: flex; justify-content: space-between;">
  <span>OPCIONES MENU</span>
  <span>MARCO RECTANGULAR</span>
  <span>BORDE INVISIBLE</span>
  <span>MARCO</span>
</div>
  
```

Hand-drawn code snippets:

```

<div style="display: flex; justify-content: space-between; align-items: center;">
  <span>LOGO</span>
  <span>LISTA DESPLEGABLE</span>
</div>
<div style="border: 1px solid yellow; padding: 5px; margin: 10px 0;">
  <span>CUADRO DE TEXTO</span>
  <span>BOTONES</span>
</div>
<div style="display: flex; justify-content: space-between;">
  <span>OPCIONES MENU</span>
  <span>MARCO RECTANGULAR</span>
  <span>BORDE INVISIBLE</span>
  <span>MARCO</span>
</div>
  
```



CUESTIONARIO BÁSICO SOBRE PROGRAMACIÓN EN INTERNET

Pruebe lo siguiente:

- Modifique la dirección de la página para quitar global.asax y volver a ejecutarla.
- Si llegó a esta página, compruebe que el contenido sea el esperado.

SERGIO LUJÁN MORA
JAUME ARAGONÉS FERRERO

Información:

- Más información...

ECU

Yo, confieso...

¡He sido hackeado!



Este año se cumple el 25 aniversario de...

World Wide Web

WWW

Web





**Tim
Berners-Lee**

Impreciso pero emocionante...

Vague but exciting ...

CERN DD/OC

Tim Berners-Lee, CERN/DD

Information Management: A Proposal


March 1989

Information Management: A Proposal

Abstract

This proposal concerns the management of general information about accelerators and experiments at CERN. It discusses the problems of loss of information about complex evolving systems and derives a solution based on a distributed hypertext system.

Keywords: Hypertext, Computer conferencing, Document retrieval, Information management, Project control



¿Ha sido emocionante?



Ir al banco

Comprar en tiendas

Ir al banco



POR TU SEGURIDAD Antes de ingresar sus datos en esta pantalla, verifique si la dirección en la barra superior es: <https://www.intermatico.com/intermatico/publico/default.asp>
Adicionalmente, verifique el Certificado de Seguridad emitido por VeriSign haciendo doble clic en el icono del candado (🔒). [Más información](#)

Si eres un usuario ya existente, te invitamos a que realices el cambio de tu usuario de Intermático actual por uno nuevo con el propósito de brindarte un mejor servicio y reforzar los niveles de seguridad. Este nuevo usuario deberá contener por lo menos un número y así mismo tu clave de ingreso.

ACCESO INTERMÁTICO



SISTEMA DE AUTENTICACIÓN ACTUAL

Si deseas ingresar a INTERMÁTICO para acceder a nuestros servicios y realizar en otro momento la actualización de tu usuario ingresa aquí.

INICIAR

Si aún no tienes tu usuario registrado en el nuevo sistema.



NUEVO SISTEMA DE AUTENTICACIÓN

Si deseas **CREAR/ACTUALIZAR** tu usuario o **INICIAR SESIÓN** en nuestro NUEVO Sistema de Autenticación ingresa aquí.

INICIAR





- Resumen
- Cuentas >>
- Declaración Cuentas >>
- Mi Ahorro Cuenta >>
- Pagos >>
- Pagos en 1 click
- Transferencias >>
- Compras >>
- Comercio Exterior >>
- Consultas >>
- Pacífico Informa >>
- Favoritos >>

Cuentas / Movimientos

Costo de Transacción \$ 0.00

Aquí puede consultar los movimientos de sus cuentas del Banco del Pacífico, Pacific National Bank y Banco del Pacífico (Panamá).

Datos consultados el 2014-3-5, a las 7:23:44.
 Cuenta Consultada:
 Nombre de Cliente:
 Saldo al 2014-03-05:

Si desea cambiar el orden de los datos en pantalla, seleccione del título de las columnas ▲ o ▼ para ordenarlos ascendente o descendente.

Movimientos

Fecha/Hora	Ciudad-Agencia	Papeleta	Tipo	Número	Valor	Estado	Referencia	Saldo Desp.Mov.
2014-02-22 13:44:34	gua-principal		N/D	2867			1 supermaxi av. 6 de d i uio ecu*cir*2014-02-22*0071	
2014-03-01 03:01:02	qui-amazonas		N/C	676			1 n/c pago intereses de ctas.	
2014-03-01 18:02:59	gua-principal		N/D	2867			1 supermaxi av. 6 de d i uio ecu*cir*2014-03-01*0071	
2014-03-03 14:23:49	gua-principal		N/D	2867			1 los cebiches de la rum quito ecu*cir*2014-03-03*6608	
2014-03-03 15:08:30	gua-principal		N/D	2867			1 opticas gmo quicentro quito ecu*cir*2014-03-04*6654	
2014-03-03 16:14:20	gua-principal		N/D	2867			1 superdeportes quicen t uio ecu*cir*2014-03-03*2038	
2014-03-04 14:14:47	gua-principal		N/D	2867			1 t.g.friday quito ecu*cir*2014-03-04*tc60	
2014-03-04 15:26:59	gua-principal		N/D	2867			1 supermaxi av. 6 de d i uio ecu*cir*2014-03-04*0071	

Esta información esta sujeta a verificaciones. La información oficial consta en tu estado de cuenta emitido por el banco.

¿Los bancos son seguros?



Acción SAN 📈 7.293 | -1.47% | 13:28

Buscar: **Buscar**

[Atención al Cliente](#) | [Trabaja con Nosotros](#) | [Web Corporativa](#) | [Mapa Web](#)

- [Particulares](#)
- [Santander Select](#)
- [Banca Privada](#)
- [Empresas](#)
- [Instituciones](#)



Bienvenidos a la nueva web del **Santander**



Scan Your Website for SQL Injection and XSS Vulnerabilities

Secure Your Website with Acunetix

- Nmap Security Scanner**
- Intro
 - Ref Guide
 - Install Guide
 - Download
 - Changelog
 - Book
 - Docs

- Security Lists**
- Nmap Hackers
 - Nmap Dev
 - Bugtraq
 - Full Disclosure
 - Pen Test
 - Basics
 - More

- Security Tools**
- Pass crackers
 - Sniffers
 - Vuln Scanners
 - Web scanners
 - Wireless
 - Exploitation
 - Packet crafters
 - More

FULL DISCLOSURE Full Disclosure mailing list archives

Is it OK to hold credit card numbers in cookies? Santander?

From: auto62098873 () hushmail.com
 Date: Sun, 14 Oct 2012 16:15:05 +0100

Santander are a joke when it comes to security. Fed up of two years of battling with them to fix issues any other bank would have fixed in seconds, things like XSS on login pages etc. Time to hit full disclosure with some of these issues in the hope they'll change their game and start to take their customers security seriously:

Advisory Information

Title: Sensitive Data In Cookies
 Date published: 2012-03-31 08:16:26 PM
 upSploit Ref: UPS-2012-0004

Advisory Summary
 Santander's online banking stores a sensitive, including full credit card numbers, in its cookies putting this information at risk.

Vendor
 Santander (UK)

Affected Software

¿Qué son las cookies?

<http://youtu.be/8LaTgXMhgtE>



**Cookies:
¿Qué son y
para qué sirven?**

Sergio Luján Mora
sergio.lujan@ua.es

<http://youtu.be/5sSideuXCFQ>



Cookies: ¿Cómo funcionan?

Sergio Luján Mora
sergio.lujan@ua.es



0011010101

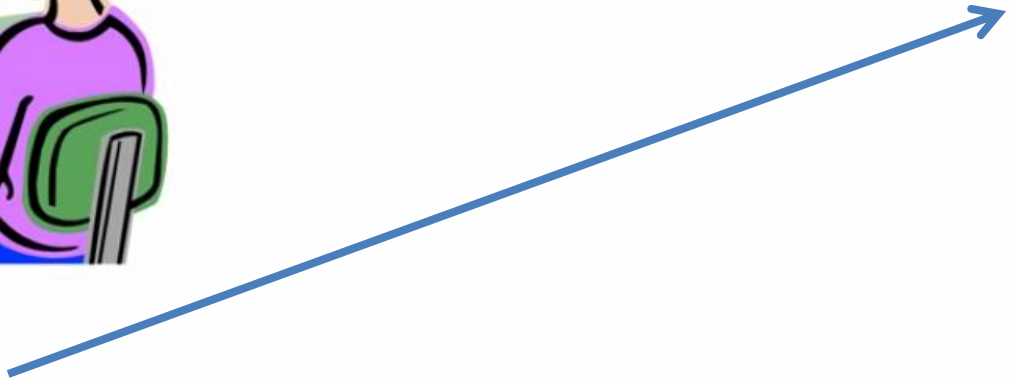




0011010101



0011010101



Santander are a joke when it comes to security. Fed up of two years of battling with them to fix issues any other bank would have fixed in seconds, things like XSS on login pages etc. Time to hit full disclosure with some of these issues in the hope they'll change their game and start to take their customers security seriously.

Santander online banking unnecessarily stores sensitive information within cookies. Depending on which areas of online banking the user visits this information may include the following:

- * Full name
- * PAN (Credit card number)
- * Bank account number and sort code
- * Alias
- * UserID

It should be noted that the HTTPOnly flag is not used on any cookies exposing them to increased greater risk of exposure (for example through XSS) - such as the XSS which was present on the login page for ~1 year before being inadvertently fixed!!

Additionally, whilst the cookies expire at the end of a session, they are not overwritten on logout. This means any user who does not close their browser, even if they log out correctly, will still have these cookies present until they close their browser. Thus increasing the window for exposure.

Compras



Shop by Department

Search All

Go

Hello, Sign in Your Account

Try Prime

Cart

Wish List

- Unlimited Instant Videos
- MP3s, Cloud Player
- Amazon Cloud Drive
- Kindle Books, Kindle E-readers
- Kindle Fire Tablets
- Appstore for Android
- Digital Games, Software
- Books, Audible
- Movies, Music, Games
- Electronics, Computers
- Home, Garden, Tools
- Beauty, Health, Grocery
- Toys, Kids, Baby
- Clothing, Shoes, Jewelry
- Sports, Outdoors
- Automotive, Industrial
- Full Store Directory

Instant Video MP3 Store Cloud Player Kindle Appstore for Android Digital Games & Software Audible Audiobooks

CELEBRATE NATIONAL READING MONTH

\$20 Off Today Only

Kindle ~~\$69~~ \$49 [Shop now](#)

Kindle Paperwhite ~~\$149~~ \$99 [Shop now](#)

St. Patrick's Day

[Shop now](#)

Unlimited access to thousands of movies Prime Instant Video

[Start Free Trial](#)

New Dresses The End of Snow? Give Free Shipping

The Future of Snow in a Warming World

Author and skier Porter Fox was shocked to learn how much snow has already disappeared in the mountains. Now he's getting the word out.

[What climate change means for snow](#)

[Get Deep: The Story of Skiing and the Future of Snow on Kindle](#)

One of thousands of authors being discovered by Amazon customers.

40% or More Off

Select Internal Hard Drives

[Shop now](#)

Related to Items You've Viewed

You viewed Customers who viewed this also viewed

20% or More Off

Select Solid-State Drives



MERCADONA

SUPERMERCADOS DE CONFIANZA



COMPRA
ON LINE



FACTURA
ON LINE



TARJETA
MERCADONA



TRABAJA CON
NOSOTROS



NUESTRA
EMPRESA

CANAL MERCADONA



- Inicio
- Dónde Estamos
- Seguridad
- Condiciones generales
- Modificar Datos
- Tramos de entrega
- Modificar Pedido

Buscador

Producto:

Marca:

Nuevo Pedido - Avenida MÉDICO RICARDO FERRE, 42, , ALICANTE, 03005, ALICANTE

- SECCIONES
- NOVEDADES
 - ALIMENTACION
 - ALÍOS Y CONDIMENTOS
 - ARROZ Y LEGUMBRES
 - ARROZ
 - LEGUMBRES
 - COCIDAS
 - LEGUMBRES SECAS
 - AZUCAR Y EDULCORANTES
 - CAFES E INFUSIONES
 - CEREALES
 - CONSERVAS DE PESCADO
 - CONSERVAS DULCES
 - CONSERVAS VEGETALES
 - DESAYUNO Y CREMAS DE CACAO
 - DIETETICOS
 - GOLOSINAS
 - HARINAS
 - HUEVOS
 - PASTAS
 - PIZZA Y ROSCA PAN
 - PLATOS PREPARADOS
 - PREPARADOS POSTRE
 - SOPAS CALDOS Y PURES
 - APERITIVOS
 - BEBES
 - BEBIDAS
 - CARNES
 - CHARCUTERIA
 - COMPLEMENTOS DE

ARROZ
17 productos encontrados.

Descripción	EUROS <small>(ver en PTA.)</small>	Cantidad	Incluir
ARROZ BASMATI, HACENDADO, PAQUETE 1 KG	1,95	- 1 +	
ARROZ BOMBA, HACENDADO, PAQUETE 1 KG	2,99	- 1 +	
ARROZ COCIDO BASMATI, BRILLANTE, PACK TARRINA 2 X 125 G - 250 G	1,39 1 KILO: 5,56 Euros	- 1 +	
ARROZ COCIDO BASMATI, HACENDADO, PACK TARRINA 2 X 125 G - 250 G	1,30 1 KILO: 5,20 Euros	- 1 +	
ARROZ COCIDO INTEGRAL, BRILLANTE, PACK TARRINA 2 X 125 G - 250 G	1,32 1 KILO: 5,28 Euros	- 1 +	
ARROZ COCIDO INTEGRAL, HACENDADO, PACK TARRINA 2 X 125 G - 250 G	1,25 1 KILO: 5,00 Euros	- 1 +	
ARROZ COCIDO REDONDO, BRILLANTE, PACK TARRINA 2 X 125 G - 250 G	1,29 1 KILO: 5,16 Euros	- 1 +	
ARROZ COCIDO REDONDO, HACENDADO, PACK TARRINA 2 X 125 G - 250 G	1,20 1 KILO: 4,80 Euros	- 1 +	
ARROZ ESPECIAL ENSALADA Y GUARNICION, HACENDADO, PAQUETE 1 KG	2,19	- 1 +	
ARROZ INTEGRAL, HACENDADO, PAQUETE 1 KG	1,49	- 1 +	
ARROZ LARGO ***LE RECOMENDAMOS***, HACENDADO, PAQUETE 1 KG	0,71	- 1 +	
ARROZ REDONDO ***LE RECOMENDAMOS***, HACENDADO, PAQUETE 1 KG	0,68	- 1 +	
ARROZ REDONDO SABROZ, BRILLANTE, PAQUETE 1 KG	1,62	- 1 +	

902 113 177
Horario: 9 a 21'30h de L a S

Ticket actual | Mis listas

Descripción	Cant.	EUROS <small>(Ver En PEBETA)</small>

Tarifa de Servicio 7,21 Eur.
Total 0 Pts. 0,00 Eur.

GUARDAR | FORMALIZAR

Recomendamos:

Compy





Inicio

Dónde Estamos

Seguridad

Condiciones generales

Modificar Datos

Tramos de entrega

Modificar Pedido

Buscador

Nuevo Pedido - Avenida MÉDICO RICARDO FERRE, 42, , ALICANTE, 03005, ALICANTE

Producto:

Marca:



SECCIONES

▶ NOVEDADES

▼ ALIMENTACION

 ▼ ALIÑOS Y
CONDIMENTOS

- ▶ ACEITES
- ▶ ADEREZOS
- ▶ ESPECIAS
- ▶ KETCHUP / MOSTAZA
- ▶ MAYONESAS / ALLIOLI
- ▶ SAL / BICARBONATO
- ▶ SALSAS PARA PREPARAR
- ▶ SALSAS PREPARADAS
- ▶ SALSAS REFRIGERADAS
- ▶ VINAGRES

▶ ARROZ Y LEGUMBRES

▶ AZÚCAR Y

EDULCORANTES

▶ CAFES E INFUSIONES

▶ CEREALES

▶ CONSERVAS DE
PESCADO

▶ CONSERVAS DULCES

▶ CONSERVAS

VEGETALES

▶ DESAYUNO Y CREMAS

DE CACAO

▶ DIETETICOS

▶ GOLOSINAS

▶ HARINAS

▶ HUEVOS

▶ PASTAS

▶ PIZZA Y ROSCA PAN

ACEITES

30 productos encontrados.

Descripción	EUROS <small>(ver en PTAS)</small>	Cantidad	Incluir
ACEITE GIRASOL TAPON AMARILLO, HACENDADO, BOTELLA 1 L	1,22	<input type="text" value="1"/>	
ACEITE GIRASOL TAPON AMARILLO, HACENDADO, GARRAFA 5 L	5,95 1 LITRO: 1,19 Euros	<input type="text" value="1"/>	
ACEITE GIRASOL TAPON AMARILLO, KOIPESOL, BOTELLA 1 L	1,65	<input type="text" value="1"/>	
ACEITE MAIZ, HACENDADO, BOTELLA 1 L	1,87	<input type="text" value="1"/>	
ACEITE OLIVA SABOR INTENSO TAPON VERDE ***LE RECOMENDAMOS***, FONTOLIVA, BOTELLA 1 L	2,40	<input type="text" value="1"/>	
ACEITE OLIVA SABOR INTENSO TAPON VERDE, CARBONELL, BOTELLA 1 L	3,35	<input type="text" value="1"/>	
ACEITE OLIVA SABOR INTENSO TAPON VERDE, HACENDADO, GARRAFA 5 L	13,50 1 LITRO: 2,70 Euros	<input type="text" value="1"/>	
ACEITE OLIVA SABOR INTENSO TAPON VERDE, HACENDADO, BOTELLA 1 L	2,75	<input type="text" value="1"/>	
ACEITE OLIVA SABOR SUAVE TAPON ROJO ***LE RECOMENDAMOS***, FONTOLIVA, BOTELLA 1 L	2,40	<input type="text" value="1"/>	
ACEITE OLIVA SABOR SUAVE TAPON ROJO, CARBONELL, BOTELLA 1 L	3,35	<input type="text" value="1"/>	
ACEITE OLIVA SABOR SUAVE TAPON ROJO, HACENDADO, BOTELLA 1 L	2,75	<input type="text" value="1"/>	
ACEITE OLIVA SABOR SUAVE TAPON ROJO, HACENDADO, GARRAFA 5 L	13,50 1 LITRO: 2,70 Euros	<input type="text" value="1"/>	
ACEITE OLIVA VIRGEN EXTRA GRAN SELECCION (TAPON DOSIFICADOR), HACENDADO, BOTELLA CRISTAL 750 CC	3,35 1 LITRO: 4,47 Euros	<input type="text" value="1"/>	

902 113 177

Horario: 9 a 21'30h de L a S

Ticket actual

Mis listas

Descripción	Cant.	EUROS <small>(Ver En PESETA)</small>

Tarifa de Servicio 7,21 Eur.

Total 0 Pts. 0,00 Eur.



GUARDAR

FORMALIZAR

Recomendamos:

Compy

Página 1 de 2

Volver

Página siguiente

SIEMPRE PRECIOS BAJOS



¿Las tiendas online son seguras?

AVANCE Consulta en pdf la primera página de EL PAÍS, Edición Nacional, del jueves 22 de mayo >

eBay pide a sus 128 millones de clientes que cambien las claves

- El sitio de subastas reconoce que sufrió un robo de datos personales en marzo

JAVIER MARTÍN | Madrid | 21 MAY 2014 - 16:10 CET

Archivado en: Ebay Amazon Comercio electrónico Empresas Internet Economía Telecomunicaciones Comunicaciones Comercio



PUBLICIDAD

HAZ CLICK AQUI

MIAMI CRUCERO ORLANDO

CARNIVAL DREAM

3X1

UNIVERSAL Orlando

\$299 P.P.

¡3 DESTINOS! ¡INCREÍBLE PRECIO!

EL PAÍS

Eskup

Twitter

Google+

Francisco Javier Martin Del Barrio

Periodista interesado en Internet, fútbol y viaje

PUBLICIDAD

Planificación de las comidas Fácil.

La compañía de comercio electrónico eBay ha pedido a sus 128 millones de clientes que cambien las contraseñas, tras reconocer que había sufrido hace unos meses un ataque cibernético a la base de datos.

La base de datos contenía nombres, edad, contraseñas de correos, direcciones físicas y números de teléfono, aunque la empresa señala que no tienen evidencia de que los piratas informáticos hubieran accedido al sistema de pagos Paypal, del que es propietaria.

El ataque se realiza a través de "un pequeño número" de cuentas de empleados que permitían el acceso no autorizado a la red corporativa, explicó la compañía en un comunicado. El infringingimiento de las normas se detectó por primera vez hace unas dos semanas y, según la compañía, desde entonces no se ha descubierto un incremento de las actividades fraudulentas en su web.

¿Es un caso aislado?

https://haveibeenpwned.com/

The screenshot shows the homepage of the website 'Have I Been Pwned'. The browser's address bar displays 'https://haveibeenpwned.com'. The navigation menu includes 'Home', 'Notify me', 'Domain search', 'Pwned sites', 'FAQs', 'API', 'Twitter', and 'Donate'. The main heading is '';--have i been pwned?' with the subtext 'Check if you have an account that has been compromised in a data breach'. A search input field contains the placeholder text 'email address or username' and a 'pwned?' button. Below the search field, statistics are shown: '22 pwned websites' and '162,080,019 pwned accounts'. At the bottom, there are two featured items: '152,445,165 Adobe accounts' and '55,622 Spirol accounts'.

Home Notify me Domain search Pwned sites FAQs API Twitter Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username pwned?

22 pwned websites

162,080,019 pwned accounts

152,445,165 Adobe accounts












55,622 Spirol accounts











22

pwned websites

162,080,019

pwned accounts

	152,445,165 Adobe accounts
	4,609,615 Snapchat accounts
	1,247,574 Gawker accounts
	1,057,819 Forbes accounts
	859,777 Stratfor accounts
	530,270 Battlefield Heroes accounts
	453,427 Yahoo accounts
	191,540 hackforums.net accounts
	158,093 Boxee accounts
	148,366 WPT Amateur Poker League accounts
	56,021 Vodafone accounts

	55,622 Spirol accounts
	38,108 Pixel Federation accounts
	37,784 Muslim Directory accounts
	37,103 Sony accounts
	36,789 BigMoneyJobs accounts
	35,368 Fridae accounts
	28,641 hemmelig.com accounts
	26,596 Business Acumen Magazine accounts
	20,902 Bell accounts
	3,200 UN Internet Governance Forum accounts
	2,239 Tesco accounts

¿Una contraseña segura?

Soporte

[Página de inicio](#)[Centro de soluciones](#)[Búsqueda avanzada](#)[Comunidades](#)[Comprar productos](#)[Contáctenos](#)[Mapa del web](#)[Compartir](#)

Mensaje de error: La contraseña debe tener al menos 18770 caracteres y no puede repetir ninguna de las 30689 contraseñas anteriores

Id. de artículo: 276304 - [Ver los productos a los que se aplica este artículo](#)

Nota acerca de su sistema operativo

Este artículo se aplica a una versión de Windows distinta la que está utilizando. Puede que el contenido en este artículo no sea relevante para usted.

[Visite el Centro de soluciones de Windows 7](#)

Este artículo se publicó anteriormente con el número E276304

[Expandir todo](#) | [Contraer todo](#)

− Síntomas

Si inicia sesión en un territorio MIT, presiona CTRL+ALT+SUPR, hace clic en **Cambiar contraseña**, escribe su contraseña MIT existente, y a continuación escribe una contraseña nueva y simple que no pase la revisión del diccionario de Kadmind, es posible que reciba el siguiente mensaje de error:

su contraseña debe tener por lo menos 18770 caracteres y no puede ser igual que ninguna de las 30689 contraseñas previas. Escriba una contraseña distinta. Escriba una contraseña que cumpla los requisitos de los dos cuadros de texto.

Tenga en cuenta que el número de caracteres requeridos cambia de 17145 a 18770 con la instalación de SP1.

[↑ Volver al principio](#) | [Propocionar comentarios](#)

− Solución

Actualmente existe una corrección compatible en Microsoft, pero sólo está diseñada para corregir el problema descrito en este artículo y, por tanto, sólo debe aplicarse a sistemas que presenten este problema específico. Es probable que posteriormente se realicen pruebas adicionales de esta corrección para asegurar la calidad del producto. Por lo tanto, si no se ve muy afectado por este problema, Microsoft recomienda que espere al próximo service pack de Windows 2000 que contenga esta corrección.

Centros de Soluciones relacionados

- [Windows 2000 Professional Edition](#)
- [Windows 2000](#)

Otros sitios de soporte

- [Conversaciones paso a paso PC Talk](#)
- [Artículos paso a paso](#)
- [Centros de soluciones](#)
- [Office Online](#)
- [Microsoft Partner Network](#)
- [Ayuda y procedimientos de Windows](#)

Comunidades

- [Microsoft Developer Network \(MSDN\)](#)
- [Foros Technet](#)



Seleccione idioma

¿Cómo almacenar las contraseñas?

function md5()

Online generator [md5 hash](#) of a string

md5 ()

hash darling, hash!

md5 checksum:

--



[php manual function md5\(\)](#)

[MD5 on Wikipedia.org](#)

function md5()

Online generator [md5 hash of a string](#)

md5 ()

hash darling, hash!

md5 checksum:

21232f297a57a5a743894a0e4a801fc3

[php manual function md5\(\)](#)

[MD5 on Wikipedia.org](#)

21232f297a57a5a743894a0e4a801fc3



admin

Rainbow table

Tabla arcoiris

Aproximadamente 24.900 resultados (0,23 segundos)

Decrypt MD5 hash 21232f297a57a5a743894a0e4a801fc3

www.md5-hash.com/.../21232f297a57a5a743894a0e4a801fc3 ▾ Traducir esta página
> 40 elementos - Your Decrypt Results. Decrypted text for MD5 hash ...
md2('admin 3e3e6b0e5c1c68644fc5ce3cf060211d.
md5('admin 21232f297a57a5a743894a0e4a801fc3.

21232f297a57a5a743894a0e4a801fc3 - MD5rainbow.com

www.md5rainbow.com/21232f297a57a5a743894a0e4a801fc3 ▾ Traducir esta página
21232f297a57a5a743894a0e4a801fc3 Decrypted MD5.

MD5 reverse for 21232f297a57a5a743894a0e4a801fc3

md5.gromweb.com/?...21232f297a57a5a743894a0e4a801fc3 ▾ Traducir esta página
MD5 reverse for MD5 hash 21232f297a57a5a743894a0e4a801fc3.

Google Hash: md5(admin ...

sandbox.machine.org.uk/GoogleHash/index.php?... ▾ Traducir esta página
md5(admin) = 21232f297a57a5a743894a0e4a801fc3. Next >> · 000000 00000000 0007
007 007007 0246 0249 1 111 1022 10sne1 111111 121212 1225 123 ...

21232f297a57a5a743894a0e4a801fc3 - MD5 decoder ...

md5decoder.com/21232f297a57a5a743894a0e4a801fc3 ▾ Traducir esta página
Success, match found for 21232f297a57a5a743894a0e4a801fc3: admin ... 1,
21232f297a57a5a743894a0e4a801fc3, admin.

21232f297a57a5a743894a0e4a801fc3 - [MD5RDB ...

md5.noisette.ch/?...21232f297a57a5a743894a0e4a801fc3 ▾ Traducir esta página
md5(admin) = 21232f297a57a5a743894a0e4a801fc3; md5(

Other encryption algorithms

Algorithms	Encrypted text
md2('admin')	3e3e6b0e5c1c68644fc5ce3cf060211d
md4('admin')	f9d4049dd6a4dc35d40e5265954b2a46
md5('admin')	21232f297a57a5a743894a0e4a801fc3
sha1('admin')	d033e22ae348aeb5660fc2140aec35850c4da997
sha256('admin')	8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918
sha384('admin')	9ca694a90285c034432c9550421b7b9dbd5c0f4b6673f05f6dbce58052ba20e4248041956ee8c9e
sha512('admin')	c7ad44cbad762a5da0a452f9e854fdc1e0e7a52a38015f23f3eab1d80b931dd472634dfac71cd34
ripemd128('admin')	ed4060702b42311eb4f6c707b11f1999
ripemd160('admin')	7dd12f3a9afa0282a575b8ef99dea2a0c1becb51
ripemd256('admin')	f87f405941cf41f0c2b5b1939e8a1f9edac7e03c7ceb1491ca5ef467f3bdc6db
ripemd320('admin')	960a7b8e2061b3b9eb87e882d0b1953e9a144b1c780c503c0f2d3d9c6bb1e4feb78b55e1a377
whirlpool('admin')	6a4e012bd9583858a5a6fa15f58bd86a25af266d3a4344f1ec2018b778f29ba83be86be45e6dc20
tiger128,3('admin')	9254a6bc274761a22a121e2e3970c436
tiger160,3('admin')	9254a6bc274761a22a121e2e3970c436ac30cb1e
tiger192,3('admin')	9254a6bc274761a22a121e2e3970c436ac30cb1e3b0835c1
tiger128,4('admin')	0b83a8d8f5f5c351df1757cbabb7d8c5
tiger160,4('admin')	0b83a8d8f5f5c351df1757cbabb7d8c57da7c266
tiger192,4('admin')	0b83a8d8f5f5c351df1757cbabb7d8c57da7c266472d89b4
snefru('admin')	1cf9fdd774e8fb63bfdaad1baaec2231f7a3de7f6ee42f8d396e39107b968e47
qost('admin')	0e8cd409a23c2e7ad1c5b22b101dfa16720550dc547921c7a099b75c7f405fd4
adler32('admin')	0601020a
crc32('admin')	44ce9c5f
crc32b('admin')	880e0d76
haval128,3('admin')	4691d973de3ad6d79321d7bff4757b59
haval160,3('admin')	21b54cd74fb54c7911a1e7077d5ac4fc90df7228
haval192,3('admin')	239169f332a1231516483b7122a23dc90fc026201b7ccedd
haval224,3('admin')	0b3fb65f0ca5628e1674cd34f3e56a00e151e2241eb07fafd07c663b
haval256,3('admin')	77c33a964e34c9feb8fec535b8632572e570533a47cd68a51fd633ea127c8a37
haval128,4('admin')	517e4acb1faae2fd2c6ee83499b3d1cb

pepeluis

ce28b4838c0d053574e6e96ff8c03062

5 resultados (0,20 segundos)

md5.znaet.org - ce28b4838c0d053574e6e96ff8c03062

md5.znaet.org/.../ce28b4838c0d053574e6e96ff8c0... Traducir esta página
24/10/2013 - show|hide md5: ce28b4838c0d053574e6e96ff8c03062 ntlm:
4a6dd06666a40e19f83d56e5b74a3633 sha1: ...


pepeluis хеш-код - ce28b4838c0d053574e6e96ff8c03062

md5-online.ru/pepeluis Traducir esta página
> 40 elementos - Другие алгоритмы. Алгоритм, Зашифрованный текст.
md2(pepeluis) 751cc90d1f3b9e00eeb2a4fe1b8a82d0.
md5(pepeluis) ce28b4838c0d053574e6e96ff8c03062.

62962 - Requested MD5 Hash queue

md5this.com/list.php?page=62962&key... Traducir esta página
Added: Mon 29th Nov,2010 04:46 am, Hash: ce28b4838c0d053574e6e96ff8c03062,
Plain: pepeluis. Added: Mon 29th Nov,2010 04:47 am, Hash: ...

Seite 272 - MD5 Passwörter entschlüsseln

 md5-passwort.de/md5-hash...p/272 Traducir esta página
de Christian Wenzl
> 150 elementos - MD5-Passwörter beginnend mit p - Seite 272.
pepedelepe 01cc6f79c38ab4b30806d98ff6d7d6fa.
pepedropo 9ea37d8fdc2a38b936458eeca812d9e2.

www.OnlineHashCrack.com # 26/06/11 : lulzsec released ...

www.onlinehashcrack.com/forfun/rec__am.txt Traducir esta página
... ce28890a341f25705fd9f372cc10e422:connect1bfh
ce28b4838c0d053574e6e96ff8c03062:pepeluis
00-100-1-71-057-014-003644115-1-77

[1С Аутсорсинг](#)

[home](#) [top](#) [last list](#)



ce28b4838c0d053574e6e96ff8c03062



plain text

pepeluis	
added	2013-10-24 23:08:28.164548
solved	2013-10-24 23:08:28.164548
source	anonymous
viewed	times
base64	cGVwZWx1aXM=
wrongkey	йуйуьмше

major hashes

md5	ce28b4838c0d053574e6e96ff8c03062
ntlm	4a6dd06666a40e19f83d56e5b74a3633
sha1	5d4a49822f45a0dbcfa954a84b36612...
mysql	*248ca80d60fc8ee699357b9b1d66ba...
md4	51563e8e485259594400db7f37e41fea
md2	751cc90d1f3b9e00eeb2a4fe1b8a82d0

minor hashes

sha224	032696a9866471a78ee3dc7a2d99a8...
sha384	c6fa8c06e9f5086e051def68a5f26ce7...
sha512	5a14cf7d3ea685f5191a708b21c56c9...
ripemd160	bdd414a342c60d811a9f39c82bce5cc...
ripemd256	68b89377ea4339c8004bc65b063117...
ripemd320	aa408cc9553122ccddfa0baec43c2e...
tiger160,3	2ea125b1639b600b88a1098ab62fcc...
tiger192,3	2ea125b1639b600b88a1098ab62fcc...
tiger128,4	48c40b7ef0d80103c1e340f9d41b550c
tiger160,4	48c40b7ef0d80103c1e340f9d41b550...
tiger192,4	48c40b7ef0d80103c1e340f9d41b550...
haval160,3	ef900c271f0636dab32c346acd8b35e...
haval192,3	611ba713b9735509868e294d2f1e2c...
haval224,3	c6f344e6d52e221cac45bffa1b544148...
haval256,3	df85f22fb8cd84d6d168b4d62b6339b...
haval128,4	16a8dfd0d1504bbaaae825f2b5337c27
haval160,4	d67b5bdc52b5187c3dfefb2844276b0...

Any questions? Just ask!

¿Cuál es la solución?

Usar un salt

Encriptar varias veces

Pero...

¿cómo se ataca un sitio web?

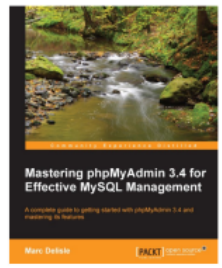


Bringing MySQL to the web

- Download 4.2.2
- Try demo
- Donate
- GSoC 2014

About

phpMyAdmin is a free software tool written in [PHP](#), intended to handle the administration of [MySQL](#) over the Web. phpMyAdmin supports a wide range of operations on MySQL, MariaDB and Drizzle. Frequently used operations (managing databases, tables, columns, relations, indexes, users, permissions, etc) can be performed via the user interface, while you still have the ability to directly execute any SQL statement.



phpMyAdmin comes with a wide range of [documentation](#) and users are welcome to update [our wiki pages](#) to share ideas and howtos for various operations. The [phpMyAdmin team](#) will try to help you if you face any problem; you can use a [variety of support channels](#) to get help.

phpMyAdmin is also very deeply documented in a book written by one of the developers – [Mastering phpMyAdmin for Effective MySQL Management](#), which is available in English and [Spanish](#).

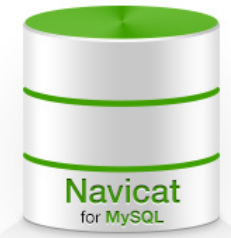
To ease usage to a wide range of people, phpMyAdmin is being translated into [72 languages](#) and supports both LTR and RTL languages.

phpMyAdmin has won several [awards](#). Among others, it was chosen as the best PHP application in various awards and has won every year the SourceForge.net Community Choice Awards as "Best Tool or Utility for SysAdmins".

phpMyAdmin is a fifteen-year-old project with a stable and flexible code base; you can find out more about the [project and its history](#). When the project turned 15, we published a [celebration page](#).

Features

Platinum sponsor



Intelligent **MySQL** GUI
Full-featured Database Manager

Gold sponsor





- [Útiles Gratuitos](#)
- [Taller: Firma-e](#)
- [Gestión de Incidencias](#)
- [Informes y Estudios](#)

- Actualidad
- Virus
- Vulnerabilidades
- Avisos de seguridad*
- Protección
- Infraestructuras críticas
- Respuesta y Soporte
- Catálogo STIC



[Encuesta de calidad de contenidos](#)

Detalle de aviso de seguridad para usuarios técnicos

[Volver](#)

Puerta trasera en phpMyAdmin

Importancia: 5 - Crítica ■■■■■

Fecha de publicación: 26/09/2012

Recursos afectados

En este momento sólo se conoce phpMyAdmin-3.5.2.2-all-languages.zip como la única versión afectada.

Descripción

Uno de los servidores espejos de SourceForge ha sido utilizado para distribuir una versión maliciosa de phpMyAdmin

Solución

Revise su distribución de phpMyAdmin y, si su versión actual contiene un archivo denominado server_sync.php, descárguelo de nuevo desde un servidor de confianza.

Detalle

El servidor [cdnetworks-kr-1](#), uno de los *mirrors* de [SourceForge](#), ha sido comprometido y utilizado para distribuir un archivo modificado de phpMyAdmin el cual incluye un puerta trasera. El malware se encuentra en el fichero `server_sync.php` y permite a un atacante ejecutar

El servidor cdnetworks-kr-1, uno de los mirrors de SourceForge , ha sido comprometido y utilizado para distribuir **un archivo modificado** de phpMyadmin el cual incluye un **puerta trasera**. El malware se encuentra en el fichero server_sync.php y permite a un atacante ejecutar remotamente código PHP. Además, el archivo js/cross_framing_protection.js ha sido modificado.

http://arstechnica.com/security/2013/03/how-i-became-a-password-cracker/



COURT AUTHORIZED NOTICE

If you used Google Search, your rights may be affected by a class action settlement.

PLEASE CLICK FOR MORE INFORMATION

MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS

RISK ASSESSMENT / SECURITY & HACKTIVISM

How I became a password cracker

Cracking passwords is officially a "script kiddie" activity now.

by Nate Anderson - Mar 24 2013, 7:55pm HPS

HACKING 237



COURT AUTHORIZED NOTICE



If you used Google Search, your rights may be affected by a class action settlement.

PLEASE CLICK FOR MORE INFORMATION

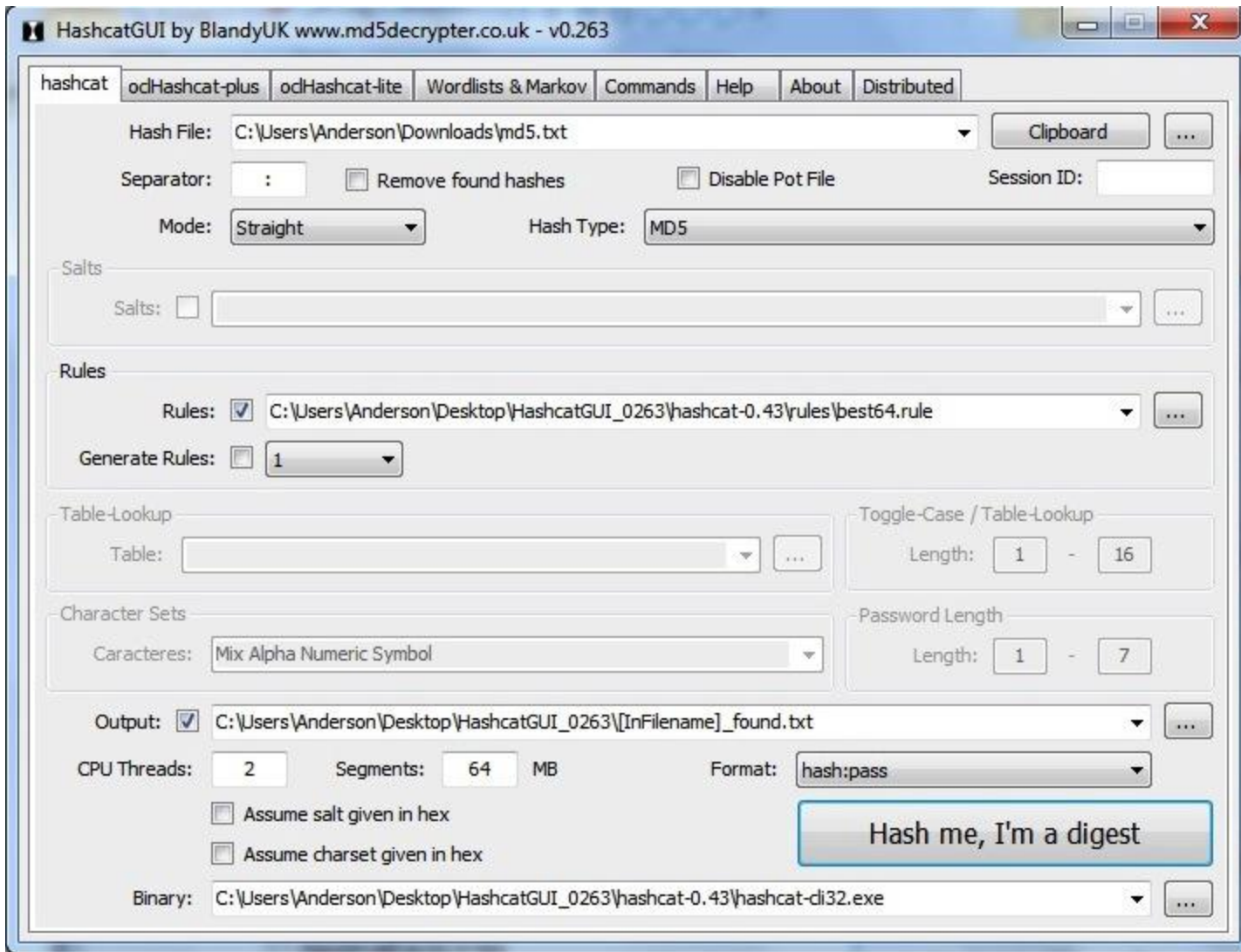
LATEST FEATURE STORY

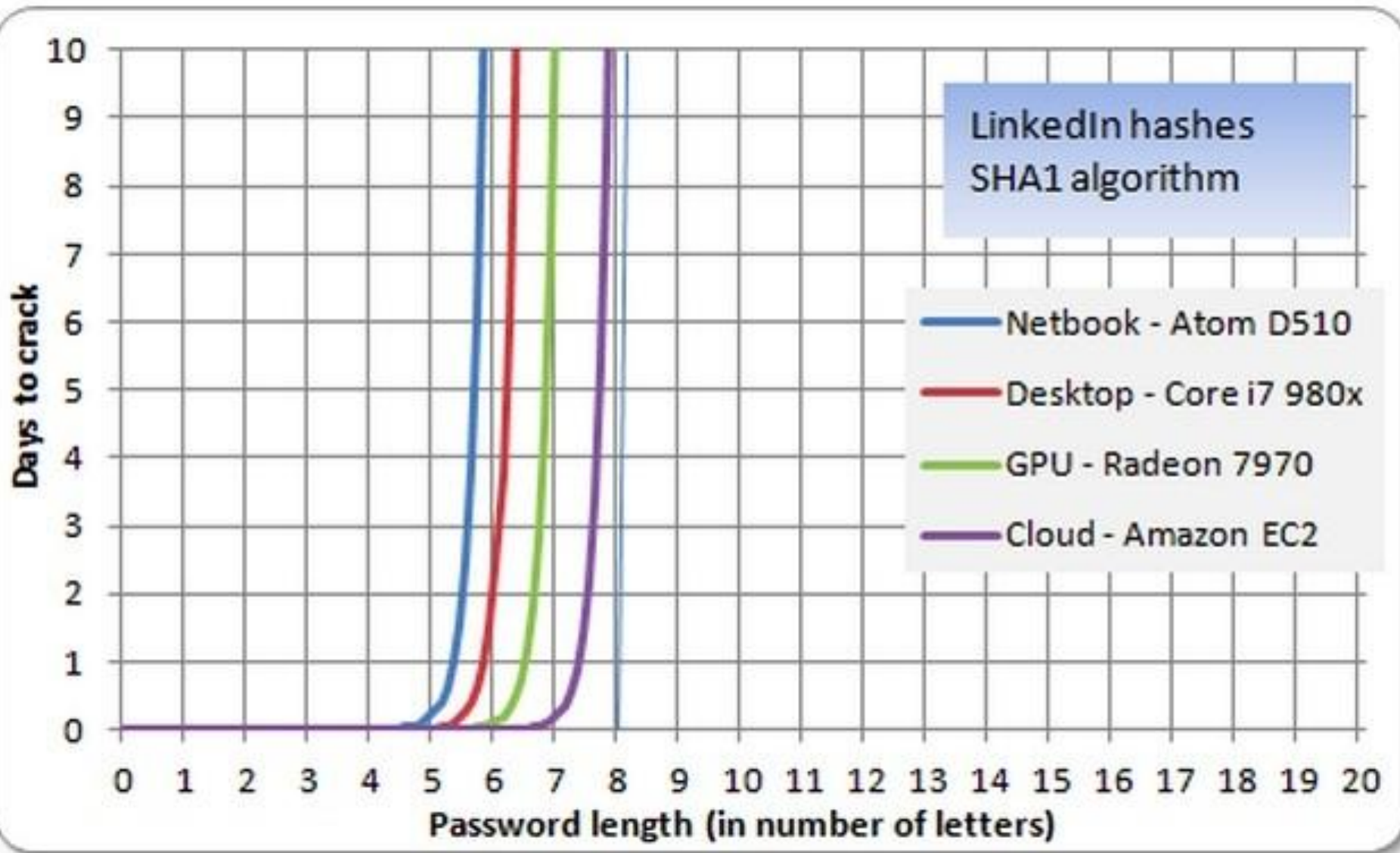


FEATURE STORY (3 PAGES)

Blinding light: The US

michael	shadow	55555	myspace	inuyasha	mustang
ashley	melissa	diamond	rebelde	peaches	isabel
qwerty	eminem	carolina	angel1	veronica	natalie
111111	matthew	steven	ricardo	chris	cuteako
iloveu	robert	rangers	babygurl	888888	javier
000000	danielle	louise	heaven	adriana	789456123
michelle	forever	orange	55555	cutie	123654
tigger	family	789456	baseball	james	sarah
sunshine	jonathan	999999	martin	banana	bowwow
chocolate	987654321	shorty	greenday	prince	portugal
password1	computer	11111	november	friend	laura
soccer	whatever	nathan	alyssa	jesus1	777777
anthony	dragon	snoopy	madison	crystal	marvin
friends	vanessa	gabriel	mother	celtic	denise
butterfly	cookie	hunter	123321	zxcvbnm	tigers
purple	naruto	cherry	123abc	edward	volleyball
angel	summer	killer	mahalkita	oliver	jasper
jordan	sweetie	sandra	batman	diana	rockstar
liverpool	spongebob	alejandro	september	samsung	january
justin	joseph	buster	december	freedom	fuckoff
		george	morgan	angelo	alicia
			marinosa	kenneth	nicholas





Mejor no usar MD5, mejor otra cosa como SHA256 o SHA512 (tendrás que cambiar la longitud del campo password).

Mejor usar un salt con el password: es un prefijo que se añade a todos los passwords y luego se pasa por la función de hash.

Mejor usar la función de hash varias veces, por ejemplo: SHA512(SHA512(SHA512(contraseña))).

https://code.google.com/p/webvulscan/wiki/WebVulScan

The screenshot shows a web browser window with the address bar containing the URL <https://code.google.com/p/webvulscan/wiki/WebVulScan>. The page title is "WebVulScan - webvulscan - 1 x". The browser's address bar shows the URL and navigation icons. The page content includes the project name "WebVulScan" and "webvulscan" with the subtitle "Web Application Vulnerability Scanner". There are navigation links for "Project Home", "Downloads", "Wiki", "Issues", and "Source". A search bar is present with the text "Search projects". The main content area is titled "WebVulScan" and includes a "Search" box with "Current pages" selected. The text describes the scanner as a web application itself written in PHP, used for testing remote or local web applications for security vulnerabilities. It lists various vulnerabilities tested, such as Reflected Cross-Site Scripting, Stored Cross-Site Scripting, Standard SQL Injection, Broken Authentication using SQL Injection, Autocomplete Enabled on Password Fields, Potentially Insecure Direct Object References, Directory Listing Enabled, HTTP Banner Disclosure, SSL Certificate not Trusted, and Unvalidated Redirects. It also lists features like Crawler, Scanner, Scan History, Register, and Login.

WebVulScan - webvulscan - 1 x

<https://code.google.com/p/webvulscan/wiki/WebVulScan>

slujanmora@gmail.com | My favorites | Profile | Sign out

WebVulScan webvulscan
Web Application Vulnerability Scanner

[Project Home](#) [Downloads](#) [Wiki](#) [Issues](#) [Source](#)

Search Current pages for

★ **WebVulScan** Updated Apr 30, 2012 by [webvuls...@gmail.com](#)

[WebVulScan](#) is a web application vulnerability scanner. It is a web application itself written in PHP and can be used to test remote, or local, web applications for security vulnerabilities. As a scan is running, details of the scan are dynamically updated to the user. These details include the status of the scan, the number of URLs found on the web application, the number of vulnerabilities found and details of the vulnerabilities found.

After a scan is complete, a detailed PDF report is emailed to the user. The report includes descriptions of the vulnerabilities found, recommendations and details of where and how each vulnerability was exploited.

The vulnerabilities tested by [WebVulScan](#) are:

- Reflected Cross-Site Scripting
- Stored Cross-Site Scripting
- Standard SQL Injection
- Broken Authentication using SQL Injection
- Autocomplete Enabled on Password Fields
- Potentially Insecure Direct Object References
- Directory Listing Enabled
- HTTP Banner Disclosure
- SSL Certificate not Trusted
- Unvalidated Redirects

Features:

- Crawler: Crawls a website to identify and display all URLs belonging to the website.
- Scanner: Crawls a website and scans all URLs found for vulnerabilities.
- Scan History: Allows a user to view or download PDF reports of previous scans that they performed.
- Register: Allows a user to register with the web application.
- Login: Allows a user to login to the web application.

Reflected Cross-Site Scripting

Stored Cross-Site Scripting

Standard SQL Injection

Broken Authentication using SQL Injection

Autocomplete Enabled on Password Fields

Potentially Insecure Direct Object References

Directory Listing Enabled

HTTP Banner Disclosure

SSL Certificate not Trusted

Unvalidated Redirects

¡He sido hackeado!

Sergio,

Nos han enviado una incidencia desde el servicio de informática porque han inyectado SQL en

<http://gplsi.dlsi.ua.es/proyectos/examinador/test.php?id=28>

y han extraído información de la base de datos (te la adjunto). Hemos quitado los permisos del directorio para evitar que sigan accediendo y te adjunto también un .tgz con el contenido del directorio. Si el algo que no se usa igual con eliminarlo acabamos con el problema...

Ya nos dices algo.

Saludos!

----- Mensaje original -----

Asunto:Fwd: [IRIS-CERT #323724] [ua.es][MUY URGENTE] SQL dumps robados y publicados aprovechando vulnerabilidad

Fecha:Thu, 30 Jun 2011 10:12:28 +0200

De:[Redacted]

Para:[Redacted]

Archivo Editar Ver Ir Mensaje Herramientas Ayuda

Bandeja de entrada - sergio.luj... Fwd: Fwd: [IRIS-CERT #32... x

Recibir Redactar Charlar Direcciones Etiqueta Imprimir Filtro rápido

Buscar... <Ctrl+K>

Responder Resp. a todos Reenviar No deseado Eliminar

Fwd: Fwd: [IRIS-CERT #323724] [ua.es][MUY URGENTE] SQL dumps robados y publicados aprovechando vulnerabilidad 30/06/2011 4:20

Buenos días,

hemos detectado que, aprovechando vulnerabilidades del sistema y junto con un exploit, han robado contenido de las bases de datos de vuestra institución. La información se ha hecho pública bajo un torrent en el siguiente link: http://158.129.2.2/uni_es_dump.torrent

El exploit utilizado se puede encontrar en <http://pastebin.com/Mi9CK6Fj>

La URL utilizada para el SQLi, es:

<http://gplsi.dlsi.ua.es/proyectos/examinador/test.php?id=28>













Aunque no sabemos a ciencia cierta cuál es la vulnerabilidad que se encuentra activa, es evidente que el acceso a la información no se está protegiendo correctamente.

Rogamos se investigue este caso y se tomen las medidas necesarias para solventar el problema.

Desde el CERT de RedIRIS hemos contactado con el CERT Lituano para que elimine de forma inminente dicho contenido.

Un saludo,

4 adjuntos 4,2 MB Guardar todo

-  daea.ua.es_dump.7z
-  escolapau.uab.es_dump.7z
-  gib.tel.uva.es_dump.7z
-  gplsi.dlsi.ua.es_dump.7z
-  ift.uam.es_dump.7z
-  intecca.uned.es_dump.7z
-  sabia.tic.udc.es_dump.7z
-  ucm.es_dump.7z
-  uhu.es_dump.7z
-  um.es_dump.7z
-  unav.es_dump.7z
-  webs.ulpgc.es_dump.7z

 awam

 awam2

 cursosnet



 examinador

 information_schema

 lowcost

 prole03

 publicadw

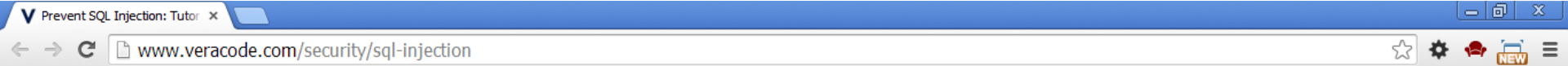
 Alumnos.csv

 Juegos.csv

 PreguntasJuegos.csv

SQL Injection

http://www.veracode.com/security/sql-injection



CONTACT US SIGN-IN SEARCH

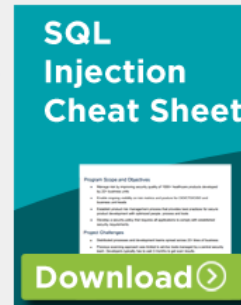
VERACODE

SOLUTIONS PRODUCTS SERVICES RESOURCES ABOUT BLOG

SQL Injection Tutorial: Learn About Injection Attacks, Vulnerabilities and How to Prevent SQL Injections

What is SQL Injection?

SQL Injection is a type of web application security vulnerability in which an attacker is able to submit a database SQL command which is executed by a web application, exposing the back-end database. A SQL Injection attack can occur when a web application utilizes user-supplied data without proper validation or encoding as part of a command or query. The specially crafted user data tricks the application into executing unintended commands or changing data. SQL Injection allows an attacker to create, read, update, alter, or delete data stored in the back-end database. In its most common form, a SQL Injection attack gives access to sensitive information such as social security numbers, credit card number or other financial data. According to Veracode's [State of Software Security Report](#) SQL Injection is one of the most prevalent types of web application security vulnerability.



Key Concepts of a SQL Injection Attack

- SQL injection is a software vulnerability that occurs when data entered by users is sent to the SQL interpreter as a part of an SQL query

Seven Days to a Secure Web Perimeter

Identify security risks in the perimeter, implement an actionable plan to mitigate risk and show immediate progress to your stakeholders.

[View the webinar >](#)

Browse Knowledge Base

- [Application Security Knowledge Base](#)
- [Software Security Testing Tools](#)
- [Web Application Vulnerabilities](#)
 - [CRLF Injection](#)

SQL injection can be prevented if you adopt an input validation technique in which user input is authenticated against a set of defined rules for length, type, and syntax and also against business rules.

You should ensure that users with the permission to access the database have the least privileges. Additionally, do not use system administrator accounts like “sa” for Web applications.

Also, you should always make sure that a database user is created only for a specific application and this user is not able to access other applications. Another method for preventing SQL injection attacks is to remove all stored procedures that are not in use.

Use strongly typed parameterized query APIs with placeholder substitution markers, even when calling stored procedures

Show care when using stored procedures since they are generally safe from injection. However, be careful as they can be injectable (such as via the use of `exec()` or concatenating arguments within the stored procedure).

OWASP x

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

Iniciar sesión / crear cuenta

Buscar Ir Buscar

Bienvenido a OWASP

la comunidad libre y abierta sobre seguridad en aplicaciones

- 2012 Project Support Initiative
- ZAP Proxy Cheat Sheets
- Top 10 ESAPI ASVS SMMM
- Development Guide AppSec Tutorial Series
- Testing Guide ModSecurity Ruleset
- More...

About · Searching · Editing · New Article · OWASP Categories

Statistics · Recent Changes

Thank you to our our corporate supporters that enable us to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks. A complete list of our current corporate and academic supporters can be found on our [Acknowledgements Page](#)

Periódicos OWASP

Los periódicos OWASP reportan eventos, proyectos, gente, herramientas, actualizaciones del Wiki y más sobre noticias de seguridad en aplicaciones en OWASP. [Lea...](#)

Who Trusts OWASP?

Citations of National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice - [Click Here](#)

How can OWASP help your org?

- Government Bodies
- Educational Institutions
- Standards Groups
- Trade Organizations
- Certifying Bodies
- Development Organizations

Security101

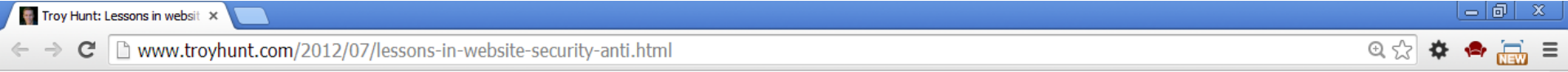
Ask a software security question - open to all, especially beginners

Navigation:

- Home
- About OWASP
- Acknowledgements
- Advertising
- AppSec Conferences
- Brand Resources
- Chapters
- Portal de la comunidad
- Donate to OWASP
- Downloads
- Governance
- Funding
- Mailing Lists
- Membership
- News
- OWASP Books
- OWASP Gear
- OWASP Initiatives
- OWASP Projects
- Presentations
- Press
- Video
- Volunteer

Reference

Activities



troyhunt.com

Observations, musings and conjecture about the world of software and technology



Search

Lessons in website security anti-patterns by Tesco

Monday, July 30, 2012

Me gusta {6} Tweet {1,921} g+ {498} Share {21}

Update, 14 Feb 2014: A year and a half on from writing this, Tesco has indeed suffered a serious security incident almost certainly as a result of some of the risks originally detailed here. Read more about it in [The Tesco hack – here’s how it \(probably\) happened](#).

Let me set the scene for this post by sharing [a simple tweet from last night](#):

TESCO Tesco Customer Care
Every little helps @UKTesco

@troyhunt Passwords are stored in a secure way. They're only copied into plain text when pasted automatically into a password reminder mail

1. Password storage should always be done using a strong hashing algorithm. IT should be one designed for password storage and also use a cryptographically random salt. It also must be a slow hashing algorithm – read [Our password hashing has no clothes](#) if this is a foreign concept.

2. Password retrieval should never happen. Indeed it can't if you've implemented the previous step correctly. Always implement a secure password reset process. Read [Everything you ever wanted to know about building a secure password reset feature](#) for some tips on this.

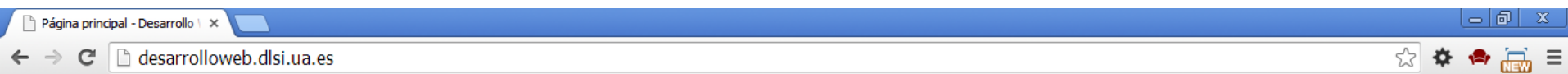
3. Never mix HTTP content into your HTTPS pages. If HTTPS is important to you – and it should be – either explicitly refer to the HTTPS protocol in your references or even easier, use protocol relative URLs. There's plenty of info in [OWASP Top 10 for .NET developers part 9: Insufficient Transport Layer Protection](#).

4. Always send authentication cookies over HTTPS. These are almost as valuable as the password itself; it gives anyone who holds them the rights to perform any tasks the user who originally authenticated to the system can. See the link in the previous point for more information.

5. There should never be restrictions on password entropy. Don't exclude special characters, don't chop the length at a short, arbitrary limit (if you have to, make it 100 chars or so) and definitely don't implement a system which is case-insensitive. See Who's who of bad password practices – banks, airlines and more for more common mistakes.

6. Ensure basic security configurations are correct. Tracing is off, custom errors are on, a default redirect page exists, debug mode is off, etc. This is obviously for ASP.NET, but there are parallels in other web stacks. Check your .NET apps with ASafaWeb.

http://desarrolloweb.dlsi.ua.es/



Desarrollo Web



Materialles docentes

- [Programación en Internet](#) (página oficial en el Departamento de Lenguajes y Sistemas Informáticos)
- [Programación en Internet](#) (página de demostración de CSS)
- [Programación en Internet \(blog\)](#)
- [Programación en Internet. curso 2006-07](#) (OpenCourseWare de la Universidad de Alicante)
- [Programación en Internet. curso 2009-10](#) (OpenCourseWare de la Universidad de Alicante)
- [Programación en Internet \(Curso 2006-2007\)](#) (RUA)
- [Programación en Internet \(Curso 2007-2008\)](#) (RUA)
- [Programación en Internet \(Curso 2008-2009\)](#) (RUA)
- [Programación en Internet \(Curso 2009-2010\)](#) (RUA)
- [Programación Hipermedia I \(Curso 2012-2013\)](#)
- [Introducción a Xampp y MySQL \(2012\)](#) (OCW)
- [Introducción a Xampp y MySQL \(2012\)](#) (YouTube EDU)

<http://desarrolloweb.dlsi.ua.es/cursos/2011/html5-css3-es/>



HTML5 y CSS3: El futuro de la programación web

HTML5 y CSS3

El futuro de la programación web

[Curso](#) [Lecciones](#) [Ejercicios](#)

<<

[Introducción](#) >>

Sobre HTML5 y CSS3 - El Futuro de la Programación Web

Este sitio web está diseñado para servir como un primer curso universitario sobre los estándares web en informática. Además de los conceptos básicos de los estándares web, también se presentan las nuevas características de HTML5

http://idesweb.es/

Introducción al desarrollo web x

idesweb.es

iDESWEB: Introducción al desarrollo web ¡Apúntate! Temario Proyecto Calendario Metodología Profesores YouTube Blog Twitter

iDESWEB: Introducción al desarrollo web

Un curso nuevo de tipo MOOC, **totalmente gratuito** y disponible en la Web (**curso online**), con el que vas a aprender los conceptos básicos del desarrollo de aplicaciones web.

Aprende HTML, CSS, JavaScript, PHP... y los principios básicos del diseño, de la usabilidad y de la accesibilidad web.

La fecha de inicio de la tercera edición del curso es el 23/09/2013. El curso se desarrolla en la dirección <http://idesweb.uaedf.ua.es/>

[¡Apúntate y aprende!](#)

Introducción al desarrollo web: presentación co...

http://www.

0:00 / 2:32 YouTube

© 2012 iDESWEB idw@idesweb.es Acerca de Contacto Colaborar Reutilizar Preguntas y respuestas UA DLSI

http://ixml.es/

Intro XML x

ixml.es

<iXML>

INICIO REGISTRO CURSO PLANIFICACION METODOLOGÍA EQUIPO SOCIAL +

Google+

Segunda clase en directo
iXML

Resuelve tus dudas

En esta segunda clase resolveremos las dudas que tengas sobre XML Namespaces, XML Schema, DOM y programación.

¡VER EN YOUTUBE!

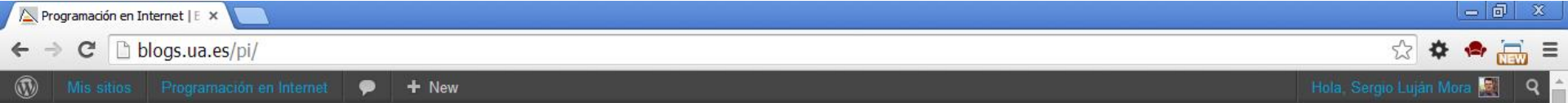
<iXML> Sergio Luján Mora

¿QUIERES APRENDER XML?

APRENDER XML NUNCA FUE TAN SENCILLO

Mediante el uso de las nuevas tecnologías, el aprendizaje estará guiado con sesiones de vídeo que podrás repetir tantas veces como necesites, también encontraras ejercicios y test para que practiques y demuestres tus avances

http://blogs.ua.es/pi/



PROGRAMACIÓN EN INTERNET

Blog de la asignatura de la titulación Ingeniero en Informática

[INICIO](#)

[INFORMACIÓN](#)

```
6 <?php
7 // (c) 2012 Sergio Luján Mora
8 define('INDEX_PHP', 'index.php');
9
10 // Main title of web site
11 $course = new Course($title);
```

21 mayo 2014
by Sergio Luján Mora
0 comments

Dos tipos de personas

Publicado en Twitter por Horace Dediu:



BUSCAR EN ESTE SITIO WEB

SEARCH

[Suscribirse a Programación en Internet por](#)

http://accesibilidadweb.dlsi.ua.es/

Accesibilidad Web: ¿Qué es? x

← → ↻ accesibilidadweb.dlsi.ua.es

Universitat d'Alacant
Universidad de Alicante

Accesibilidad Web



¿Qué es? Discapacidad Legislación Guía breve WCAG 1.0 WCAG 2.0 Hardware Software Herramientas Evaluación Vídeos Buscar

Ejemplos Futuro Cursos Traducciones Blog y noticias Mapa del sitio Declaración [Búsqueda avanzada](#)

Estás en: [Accesibilidad web](#) > [¿Qué es?](#)

¿Qué es?

- [Definición](#)
- [Introducción](#)
- [¿Por qué?](#)
- [Beneficiarios](#)
- [Mitos](#)
- [Beneficios](#)
- [Cómo se logra](#)
- [Las pautas de accesibilidad al contenido web](#)
- [Libros](#)

> ¿Qué es la accesibilidad web?

La **accesibilidad web** tiene como objetivo lograr que las páginas web sean utilizables por el máximo número de personas, independientemente de sus conocimientos o capacidades personales e independientemente de las características técnicas del equipo utilizado para acceder a la Web.

La necesidad de que la Web sea universal y accesible por cualquier persona está presente desde el principio de la Web, ya que era un requisito contemplado en su diseño por su creador Tim Berners-Lee:

"The power of the Web is in its universality. Access by everyone regardless of disability is an essential aspect."

El poder de la Web está en su universalidad. El acceso por cualquier persona, independientemente de la discapacidad que presente es un aspecto esencial.

[Tim Berners-Lee](#), Director del W3C e inventor de la World Wide Web

En la actualidad, no existe una definición formal y totalmente aceptada del concepto de accesibilidad web. En este sitio web puedes encontrar varias [definiciones](#) que existen. También puedes leer una pequeña [introducción](#) donde se explica que la Web ofrece oportunidades sin precedentes a las personas con discapacidad, pero si no se lleva cuidado, la falta de accesibilidad creará graves barreras que impedirán su uso.

Además, también existen una serie de [mitos](#) sobre la accesibilidad web que perduran desde hace años. Estos mitos se pueden resumir en que la accesibilidad web es cara y supone un coste extra en el desarrollo de un sitio web, sin que los [beneficios](#) sean importantes. Además, otro de los mitos que perdura es creer que la accesibilidad web sólo beneficia a las personas con discapacidad. Los beneficiarios de la accesibilidad web son todo el mundo.

http://accesibilidadenlaweb.blogspot.com/

Accesibilidad en la Web x

← → ↻ accesibilidadenlaweb.blogspot.com

🔍 Compartir 0 Más ▶ Siguiendo blog»

slujanmora@gmail.com Nueva entrada Diseño Salir

Accesibilidad en la Web

Todo tipo de información sobre accesibilidad en la Web: errores de accesibilidad, ejemplos de páginas inaccesibles, noticias, software, hardware, ayudas técnicas, tecnologías de apoyo, consejos, pautas y guías de accesibilidad, WAI, WCAG, Norma UNE 139803:2004, legislación, etc.

Apúntate a iDESWEB, el primer MOOC sobre desarrollo web en español

Buscar

miércoles, 21 de mayo de 2014

Conferencia "Investigación sobre accesibilidad web"

Este jueves 22 de mayo, a las 11 horas (Ecuador) impartiré la conferencia *Investigación sobre accesibilidad web* en la Escuela Politécnica Nacional.

El resumen de la conferencia es:

La accesibilidad "es el grado en el que todas las personas pueden utilizar un objeto, visitar un lugar o acceder a un servicio, independientemente de sus capacidades técnicas, cognitivas o físicas".

Cuando se habla de accesibilidad web, se hace referencia a la capacidad de acceso a la Web y a sus contenidos, tanto para usarlos como para crear contenidos nuevos, por todas las personas independientemente de la discapacidad (física, intelectual o técnica) que presenten o de las que se deriven del contexto de uso (tecnológico o ambiental).

Un diseño web accesible permite que cualquier usuario pueda percibir, entender, navegar e interactuar con la Web, aportando a su vez contenidos. Aunque las personas con discapacidad y las personas de edad avanzada son los principales beneficiarios de la accesibilidad web, el resto de personas también se ven beneficiadas.

Para lograr la accesibilidad, se han desarrollado diferentes pautas o guías que explican cómo se tienen que crear las páginas web para que sean accesibles.

Desgraciadamente, las pautas o guías sobre accesibilidad web no siempre se aplican o no se aplican correctamente. Además, las pautas son sólo eso: consejos a los que se

¿Qué es la Accesibilidad Web?

La accesibilidad Web significa que personas con algún tipo de discapacidad van a poder hacer uso de la Web. En concreto, al hablar de accesibilidad Web se está haciendo referencia a un diseño Web que va a permitir que estas personas puedan percibir, entender, navegar e interactuar con la Web, aportando a su vez contenidos. La accesibilidad Web también beneficia a otras personas, incluyendo personas de edad avanzada que han visto mermadas sus habilidades a consecuencia de la edad. [Introducción a la Accesibilidad Web, W3C](#)

Datos personales



Sergio Luján Mora

Seguir 404

Profesor Titular de Universidad del Departamento de Lenguajes y Sistemas Informáticos de la

Universidad de Alicante (España).
Twitter @sergiolujanmora

Canal personal en YouTube

https://twitter.com/sergiolujanmora

Sergio Luján Mora (sergioluja)

Twitter, Inc. [US] https://twitter.com/sergiolujanmora

Inicio Notificaciones # Descubre Cuenta

Buscar

Tweets

Siguiendo

Seguidores

Favoritos

Listas

Fotos y vídeos

Coruña = Coruña

Error: Formulario 4 en dom

Sergio Luján sergioluja

Sergio Luján Mora
@sergiolujanmora

Profesor del Departamento de Lenguajes y Sistemas Informáticos de la Universidad de Alicante (España). Interesado en el desarrollo y la accesibilidad web.

Alicante, España · desarrolloweb.dlsi.ua.es

TWEETS 6 315 SIGUIENDO 160 SEGUIDORES 2 082

Editar perfil

Tweets

Sergio Luján Mora @sergiolujanmora · 3 h
Que tus usuarios sean el centro de tu proyecto de diseño. Sé humilde. Escúchalos. Te ayudarán a tener éxito. J.Nielsen
Abrir Responder Eliminar Favorito Más

Sergio Luján Mora @sergiolujanmora · 3 h
Vídeo: Errores web: Renfe y las fechas youtu.be/KHlaow8ifoo
Ver contenido multimedia Responder Eliminar Favorito Más

Sergio Luján Mora @sergiolujanmora · 3 h
Consejos para vender la accesibilidad web goo.gl/MskWke #accweb
Abrir Responder Eliminar Favorito Más

A quién seguir · Refrescar · Ver todos

CFA Private Wealth @CFA...
Seguir Promocionado

CES @ces_ec
Seguido por Antonio Hernán...
Seguir

teleSUR TV @teleSURtv
Seguir

Cuentas populares · Encontrar amigos

© 2014 Twitter Sobre nosotros Ayuda Condiciones Privacidad Cookies Información sobre anuncios Marca Blog Estado Aplicaciones Empleos Anunciarse Empresas Medios Desarrolladores

web site

urse (\$title)



ESCUELA POLITÉCNICA NACIONAL



Universitat d'Alacant
Universidad de Alicante

Seguridad de las aplicaciones web

Sergio Luján Mora

sergiolujanmora.es

sergio.lujan@ua.es

[@sergiolujanmora](#)