

# Auditoría de aplicaciones web: metodología y práctica profesional

Titulación: Ingeniería Informática – Universitat Oberta de Catalunya (UOC).

Área de Seguridad Informática.

Enero 2014 – 2015.

Estudiante: Miriam Rodríguez Sánchez.

Tutor universitario: Cristina Pérez Solà.

# Introducción

## Definición

- Auditoría web: proceso

## Punto de partida

- Análisis de un servidor web

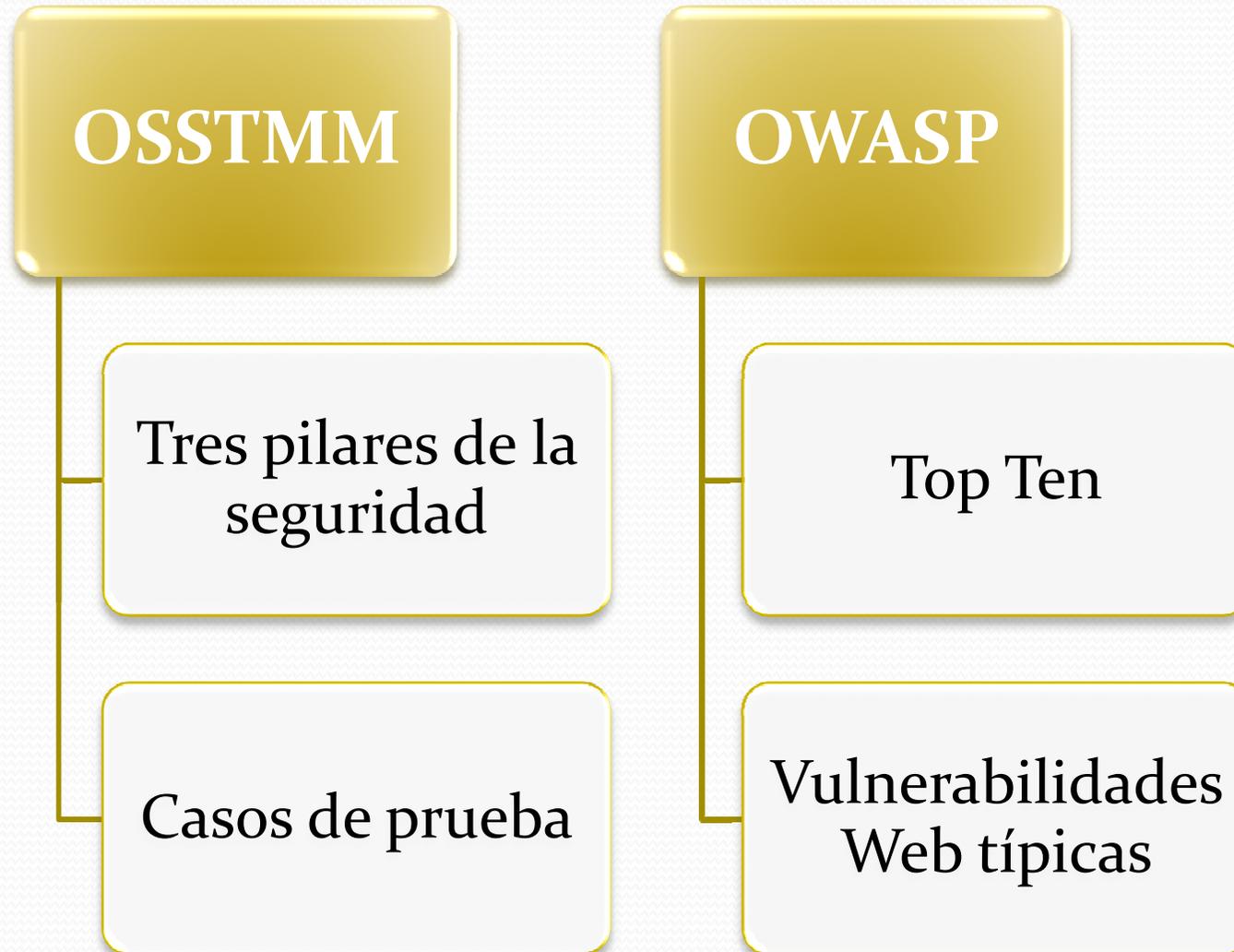
## Objetivos

- Ejercicio práctico
- Método en cuatro fases

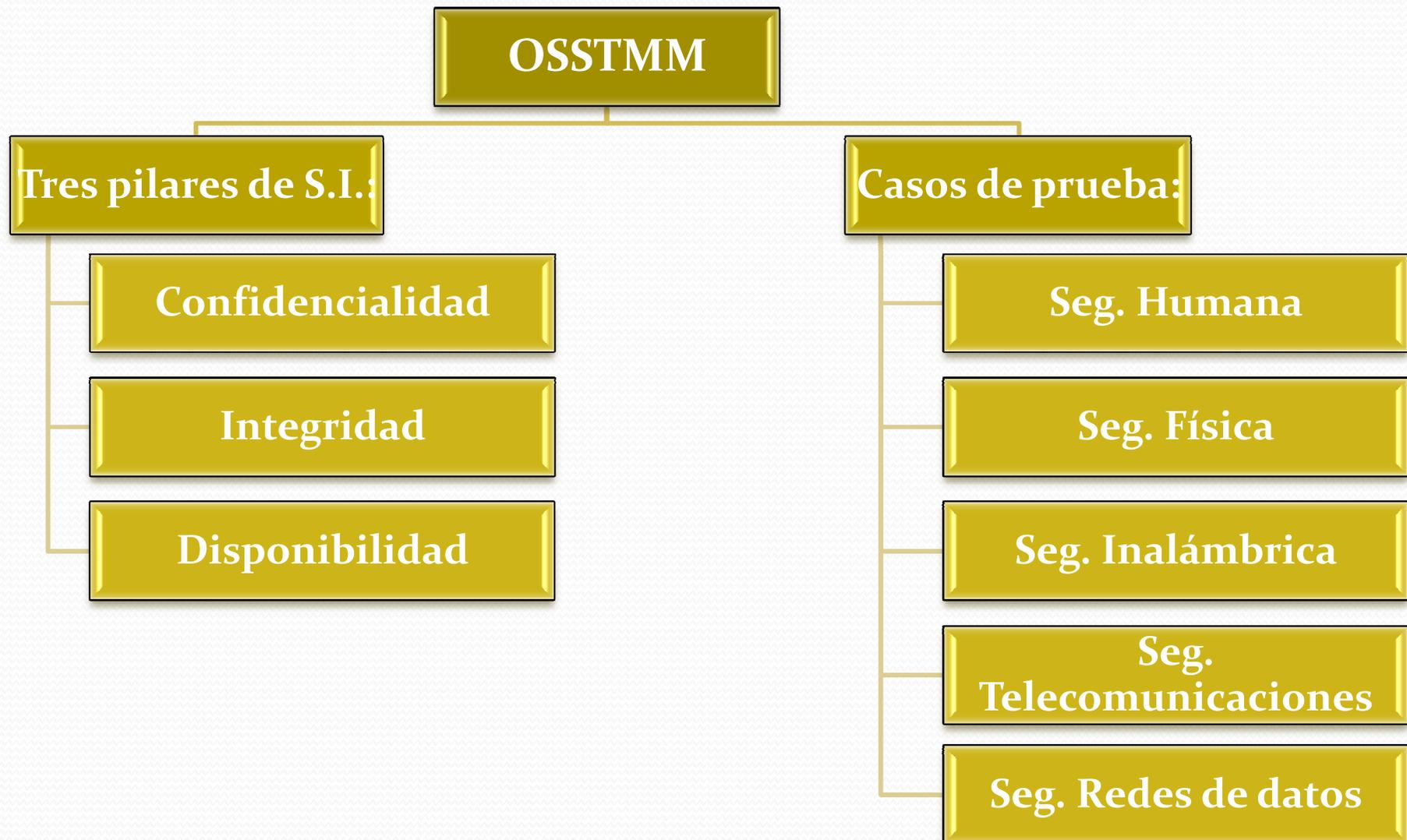
## Breve descripción

- Fases del método:
  - Reconocimiento
  - Mapeado
  - Descubrimiento
  - Explotación

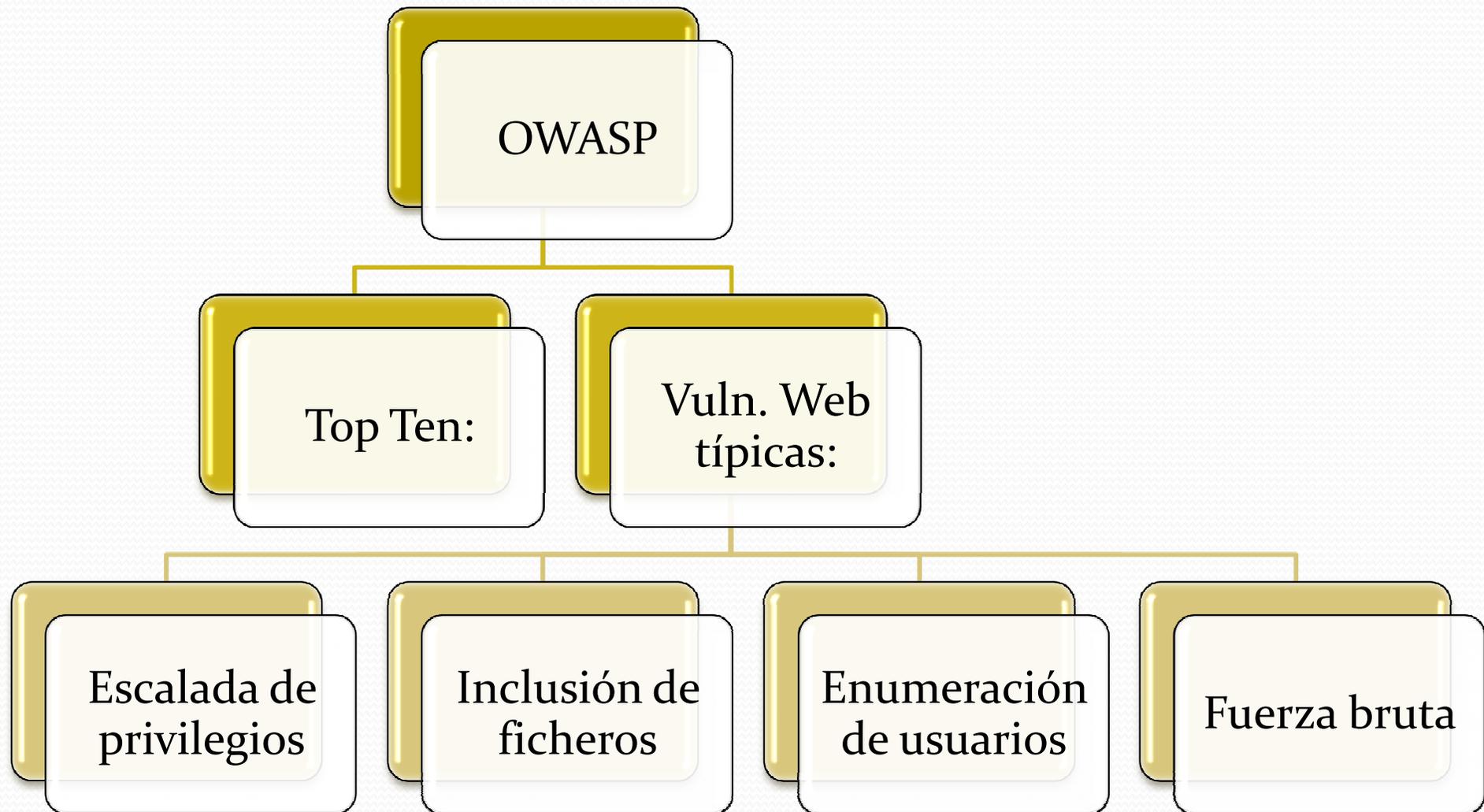
# Metodologías de partida (I)



# Metodologías de partida (II)



# Metodologías de partida (III)



# Metodologías de partida (IV)



# Aspectos de la auditoría web

## Tipos de test

Caja negra

Caja blanca

Caja gris

## Aspectos normativos y legales

LOPD

PCI DSS

## Aspectos contractuales de la auditoría

Permiso explícito

Acuerdo de no divulgación

Definición del alcance

Reglas de compromiso

Ausencia de garantías

## Informe de resultados

Resumen ejecutivo

Consideraciones técnicas

Hallazgos

Herramientas

Conclusiones y apéndices

# Metodología. Reconocimiento (I)

## Definición del alcance.

## Búsquedas en registros de internet: whois, nslookup, dig.

```
Server:          tethys.ringofsaturn.com
Address:         71.252.219.43#53

Non-authoritative answer:
owasp.org       text = "google-site-verification=I9qx_X9EK1R_rfceG25-iXHBXJvLrmeNbkEdyl82iI"
owasp.org       text = "v=spf1 include:aspmx.googlemail.com ~all"
Name:   owasp.org
Address: 192.237.166.62
owasp.org      has AAAA address 2001:4801:7821:77:cd2c:d9de:ff10:170e
owasp.org      mail exchanger = 20 ALT1.ASPMX.L.GOOGLE.com.
owasp.org      mail exchanger = 20 ALT2.ASPMX.L.GOOGLE.com.
owasp.org      mail exchanger = 30 ASPMX2.GOOGLEMAIL.com.
owasp.org      mail exchanger = 30 ASPMX4.GOOGLEMAIL.com.
owasp.org      mail exchanger = 30 ASPMX5.GOOGLEMAIL.com.
owasp.org      mail exchanger = 10 ASPMX.L.GOOGLE.com.
owasp.org      mail exchanger = 30 ASPMX3.GOOGLEMAIL.com.
owasp.org
origin = dns1.stabletransit.com
mail addr = ipadmin.stabletransit.com
serial = 1410656493
refresh = 3600
retry = 300
expire = 1814400
minimum = 300
owasp.org      nameserver = dns2.stabletransit.com.
owasp.org      nameserver = dns1.stabletransit.com.

Authoritative answers can be found from:
owasp.org      nameserver = dns2.stabletransit.com.
owasp.org      nameserver = dns1.stabletransit.com.
```

# Metodología. Reconocimiento (II)

## Consultas en páginas públicas:

- **Noticias.**
- **Grupos de soporte técnico.**
- **Listas de correo o foros.**
- **Redes sociales profesionales.**
- **Ofertas de empleo.**

## Motores de búsqueda:

- **Robots.txt**
- **Directivas y operadores.**

## Búsqueda de sub-dominios:

- **Fierce domain scan:** # `fierce -dns owasp.org.`

## Elaboración de diccionarios:

- **Cewl:** # `cewl -w fichero.txt dominio_objetivo.com.`

# Metodología. Mapeado (I)

## Escaneo de puertos y versiones.

- **Nmap:**
  - **TCP SYN SCAN.**
  - **UDP SCAN.**
  - **# nmap -sV -sS -O -sC --top-ports 4000 dominio\_cliente.com -oA nmap-TCP4000**

```
root@kali:~# nmap -sS -sV -O -sC --top-ports 4000 dominio_cliente.com -oA nmap-TCP4000
Starting Nmap 6.47 ( http://nmap.org ) at 2014-10-25 09:26 EDT
Nmap scan report for dominio_cliente.com
Host is up (0.014s latency).
rDNS record for dominio_cliente.com: 192.168.1.104.dyn.user.ono.com
Not shown: 3997 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u1 (protocol 2.0)
| ssh-hostkey:
|   1024 27:60:70:a6:2b:d8:b9:2f:fd:e4:c5:84:6d:09:bb:f4 (DSA)
|   2048 eb:52:d4:a7:0a:a0:51:bd:6a:49:a7:b1:3f:26:32:d2 (RSA)
|   256  ee:2f:23:a9:82:70:14:b5:d3:f0:b6:ac:a8:94:09:4e (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Debian))
|_ http-title: Site doesn't have a title (text/html).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
Device type: general purpose
Running: Linux 2.4.X|3.X, Microsoft Windows 7|XP
OS CPE: cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:3 cpe:/o:microsoft:windows_7::er
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows 7 Enterprise, Microsoft V
Service Info: Host: our; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 160.83 seconds
```

# Metodología. Mapeado (II)

## Análisis SSL:

versión,

tamaño de las claves,

tipos de cifrado,

certificados mostrados.

TLSSLED/SSLDIGGER

## Balancedores de carga y WAF:

Rastro mínimo,

Webshell única,

Errores.

WAFWOOF / Halberd

# Metodología. Mapeado (III)

```
# tlssled dominio_cliente.com 80
```

```
[*] Running sslscan on 192.168.1.100 dominio_cliente.com:80 ...  
[-] Testing for SSLv2 ...  
[-] Testing for the NULL cipher ...  
[-] Testing for weak ciphers (based on key length - 40 or 56 bits) ...  
[+] Testing for strong ciphers (based on AES) ...  
[-] Testing for MD5 signed certificate ...  
[.] Testing for the certificate public key length ...  
[.] Testing for the certificate subject ...  
[.] Testing for the certificate CA issuer ...  
[.] Testing for the certificate validity period ...  
Today: Sat Oct 25 14:19:27 UTC 2014  
[.] Checking preferred server ciphers ...
```

# Metodología. Mapeado (IV)

Configuración del software:  
Nikto.



# nikto -host dominio\_cliente.com

```
root@kali:~# nikto -host dominio_cliente.com
- Nikto v2.1.6
-----
+ Target IP:          192.168.1.174
+ Target Hostname:    dominio_cliente.com
+ Target Port:        80
+ Start Time:         2014-11-06 08:34:03 (GMT-5)
-----
+ Server: Apache/2.2.22 (Debian)
+ Server leaks inodes via ETags, header found with file /, inode: 4461759, size: 143, mtime: 0
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force
  d index.html
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.7). Apache 2.0.65
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ Retrieved x-powered-by header: PHP/5.4.4-14+deb7u10
+ OSVDB-3092: /demo/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 7471 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:          2014-11-06 08:39:08 (GMT-5) (305 seconds)
-----
+ 1 host(s) tested
```

# Metodología. Mapeado (V)

Spidering:

- Navegación manual. ZAP.
- Análisis de resultados.

The screenshot displays the OWASP ZAP (Zed Attack Proxy) interface during a spider scan. The main window shows a tree view of discovered URLs under the site 'http://[redacted].com'. The right-hand pane displays the raw HTTP request for a GET request to 'http://[redacted].com'. The bottom status bar indicates that the spider scan is active, with 0 current scans, 0 alerts, 2 warnings, 10 errors, and 1 critical error. The 'Spider' tool is highlighted in the bottom toolbar.

Consola de secuencia de comandos

```
GET http://[redacted].com HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-control: no-cache
Content-Length: 0
Host: [redacted].com
```

Processed	Método	URI	Flags
✓	GET	http://[redacted].com	SEED
✓	GET	http://[redacted].com/demo/	SEED
✓	GET	http://[redacted].com/demosmelting/	SEED
✓	GET	http://[redacted].com/admin_destinos	SEED
✓	GET	http://[redacted].com/admin_destinos/admin_destinos.php	SEED
✓	GET	http://[redacted].com/demoepv/	SEED
✓	GET	http://[redacted].com/demoaudit/	SEED
✓	GET	http://[redacted].com/demoaudit/	SEED

Alertas 4 2 10 1

Escaneo actual 0 0 0 0 0 0

# Metodología. Descubrimiento y explotación (I)

## Detección:

- Comportamiento ante errores.

ABCD: Yo Mismo [PRIMERA EMPRESA]

Recepción: ahora

Metal

Oro

Peso

Servicio

Afinaje

1

Destino

demolines

Referencia

+

%3E**peso**%3C%2Fk%3E%3Cv%3E**aaaa**%3

```
<br />
<b>Warning</b>: pg_query(): Query failed: ERROR: column &quot;aaaa&quot; does not exist
LINE 1: INSERT INTO encargos_procesado VALUES (10,1,7,1,1,aaaa,0,30,...
                                     ^ in /var/www/demosmelting/lib/dba/libgeneral_postgre.php on line 33<br />
<br />
<b>Warning</b>: pg_cmdtuples() expects parameter 1 to be resource, boolean given in /var/www/demosmelting/lib/dba/libgeneral_postgre.php on line 267
</b><br />
<?xml version="1.0" encoding="utf-8" ?><xjx><cmd n="js"><![CDATA[FinCierraPedido("", "7", "7", 1415640993);]]></cmd></xjx>
```

# Metodología. Descubrimiento y explotación (II)

## Escaneo de vulnerabilidades: Alertas.

The screenshot displays the Nessus scanner interface. The top toolbar includes buttons for 'Historia', 'Buscar', 'Puntos de interrupción', 'Alertas', 'Escaneo Activo', 'Spider', 'Navegación predefinida', 'Fuzzer', 'Parámetros', and 'Http Sessions'. The 'Alertas' button is highlighted with a red box.

The left sidebar shows a tree view of alerts under 'Alertas (25)'. The selected alert is 'Advanced SQL Injection - AND boolean-based blind - WHERE or HAVING clause (2)'. Other alerts include 'Advanced SQL Injection - MySQL > 5.0.11 AND time-based blind (3)', 'Advanced SQL Injection - PostgreSQL > 8.1 AND time-based blind (2)', 'Advanced SQL Injection - PostgreSQL > 8.1 stacked queries', 'Advanced SQL Injection - PostgreSQL AND error-based - WHERE or HAVING clause (2)', 'Credenciales de autenticación capturados (4)', 'Falla por Inyección SQL (2)', 'Secuencia de Comandos en Sitios Cruzados (XSS, reflejado) (3)', 'Application Error disclosure (1912)', 'HTTP Parameter Override (9)', 'Método de autenticación débil', 'Parameter tampering (5)', 'Ausencia de fichas (tokens) Anti-CSRF (29)', 'Content-Type header missing (105)', 'Cookie set without HttpOnly flag (132)', 'Cross-domain JavaScript source file inclusion (2)', 'Information disclosure - debug error messages', and 'Password Autocomplete in browser (16)'.

The right pane shows the details for the selected alert: 'Advanced SQL Injection - AND boolean-based blind - WHERE or HAVING clause'. The 'URL' field is partially visible. The 'Riesgo' is 'High', 'Fiabilidad' is 'Warning', 'Parámetro' is 'id', and 'Ataque' is '9 AND 5397=5397'. The 'Evidencia' section contains the text: 'A SQL injection may be possible using the attached payload'. The 'Otra info' section contains: 'The page results were successfully manipulated using the boolean condition. The parameter value being modified was stripped from the HTML output for the Data was returned for the original parameter.' The 'Solución' section contains: 'Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, v'.

At the bottom of the interface, a status bar shows 'Alertas' with icons for 8 High, 4 Warning, 9 Medium, and 4 Low severity alerts.

# Metodología. Descubrimiento y explotación (III)

## Fuzzing de parámetros.



## Divulgación de información.

DEMO SASTIC S.L.  
S. 20080207  
Calle de la Industria, 100 - Parque Empresarial El Estrecho  
46100 Sagunto (Valencia) España  
Tel.: (+34) 902 000 000  
info@demo.com

Notice: Array to string conversion in  
/var/www/demosmelting/pdf/inc/DatosCliente.php  
on line 3

DEMO SASTIC S.L.  
S. 20080207  
Calle de la Industria  
100 - Parque Empresarial El Estrecho  
46100 Sagunto (Valencia) España  
56321 Valencia  
Valencia  
España

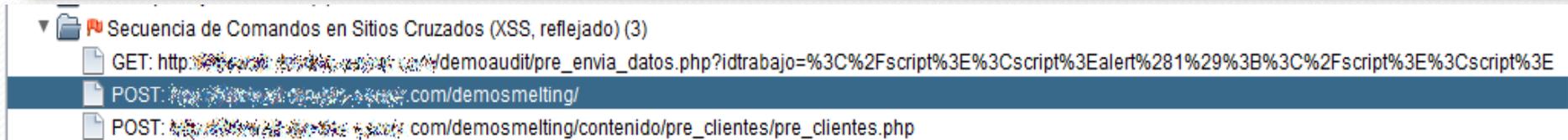
# Metodología. Descubrimiento y explotación (IV)



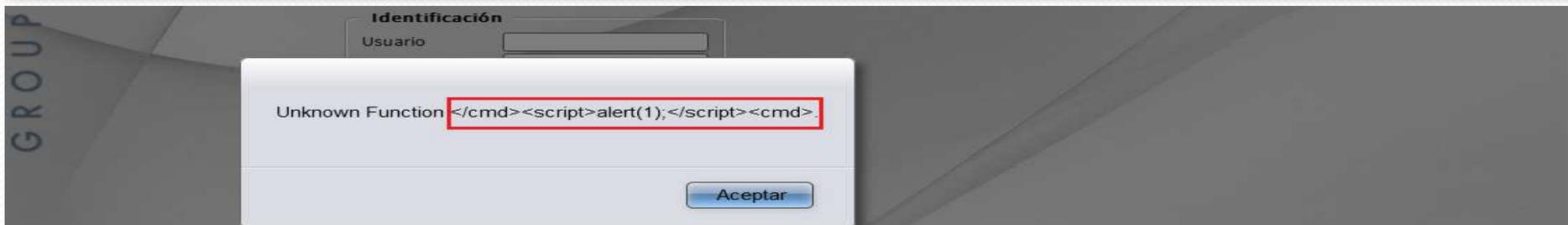


# Metodología. Descubrimiento y explotación (VI)

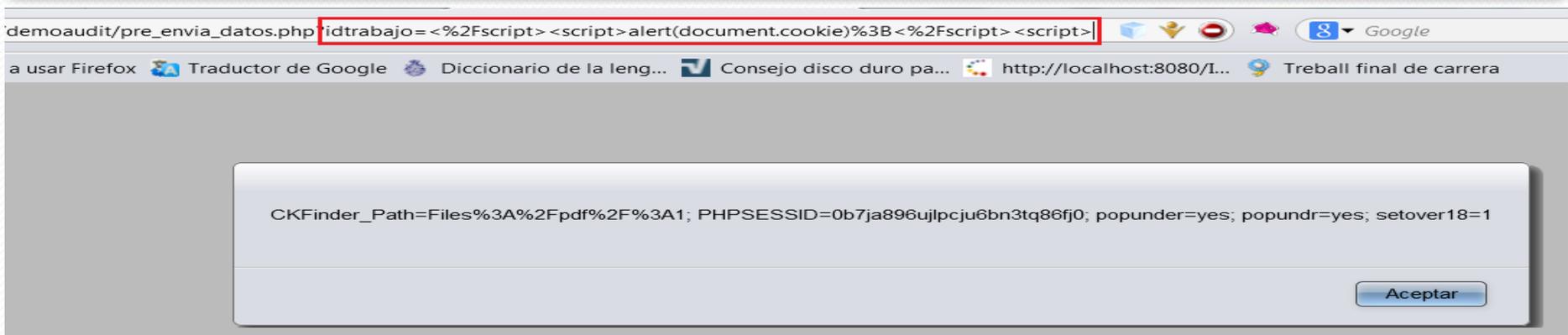
## Cross-Site Scripting (XSS).



```
xajax=</cmd><script>alert(1);</script><cmd>
```



```
http://dominio_cliente.com/pre_envia_datos.php?idtrabajo=25
```



# Conclusiones.

## Objetivos propuestos:

- Revisión de un servidor público.
- Ejercicio de auditoría completo.
- Enfoque profesional.
- Método desarrollado en 4 fases.
- Aprendizaje de las metodologías más conocidas.