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

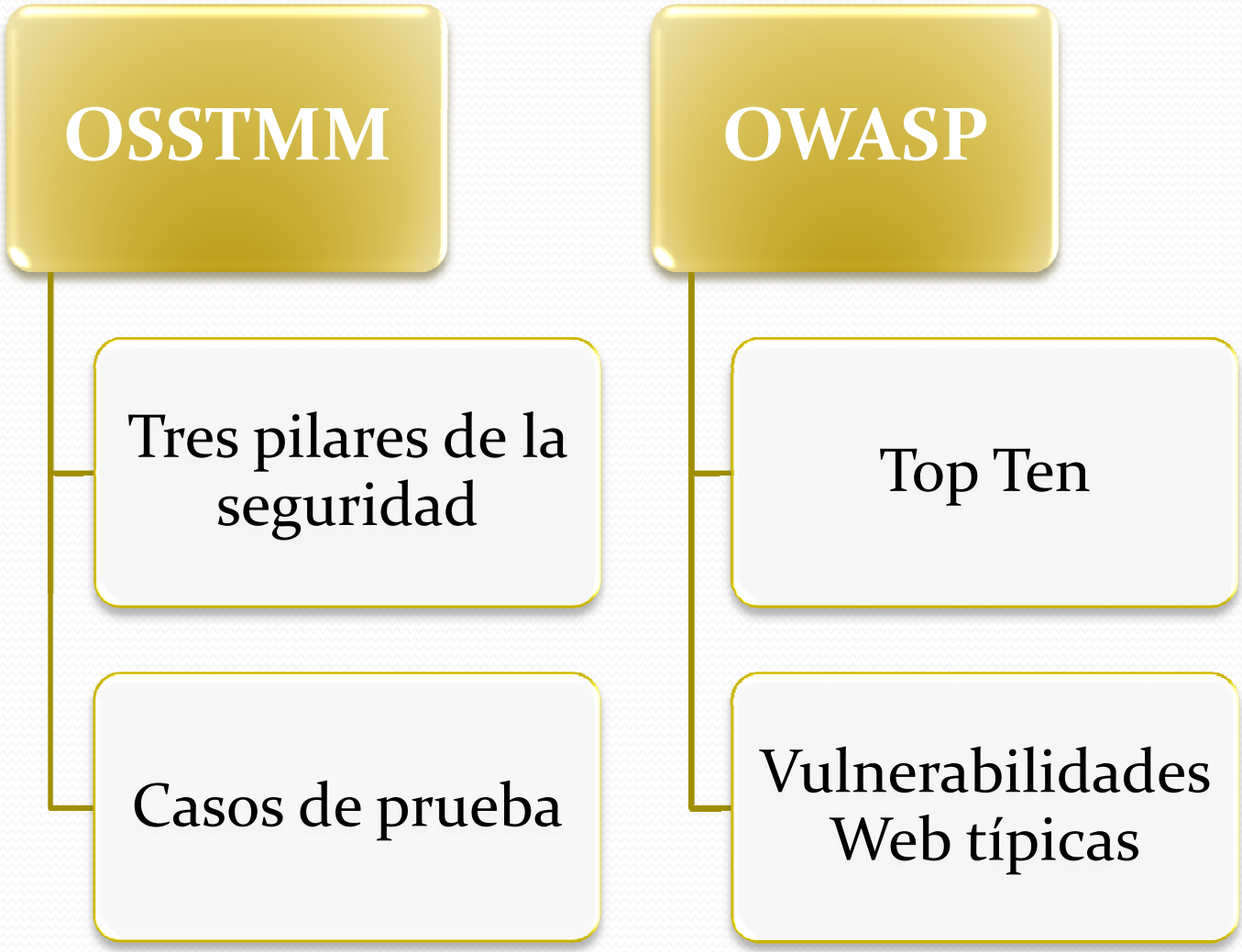
Objetivos

- Ejercicio práctico
- Método en cuatro fases

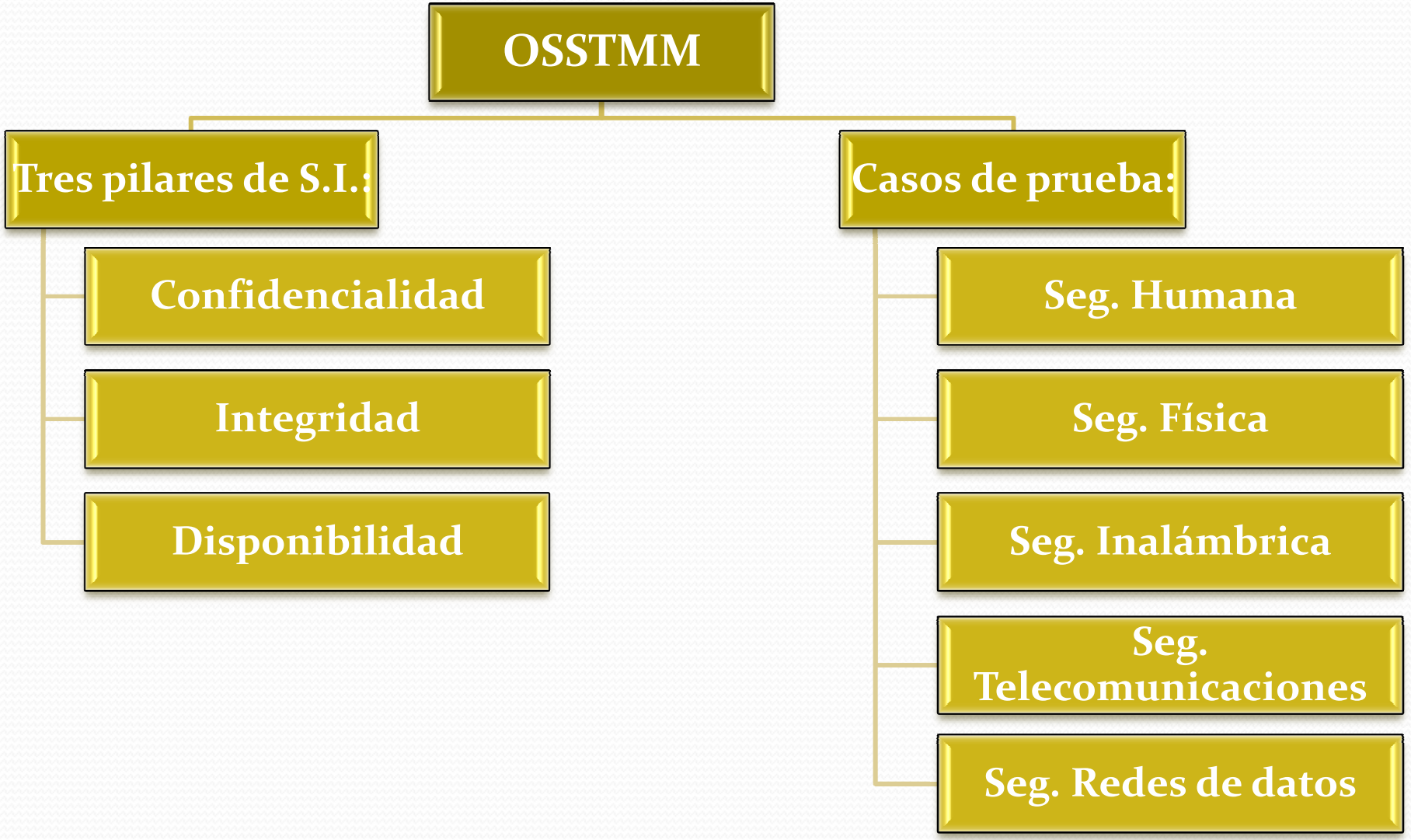
Breve descripción

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

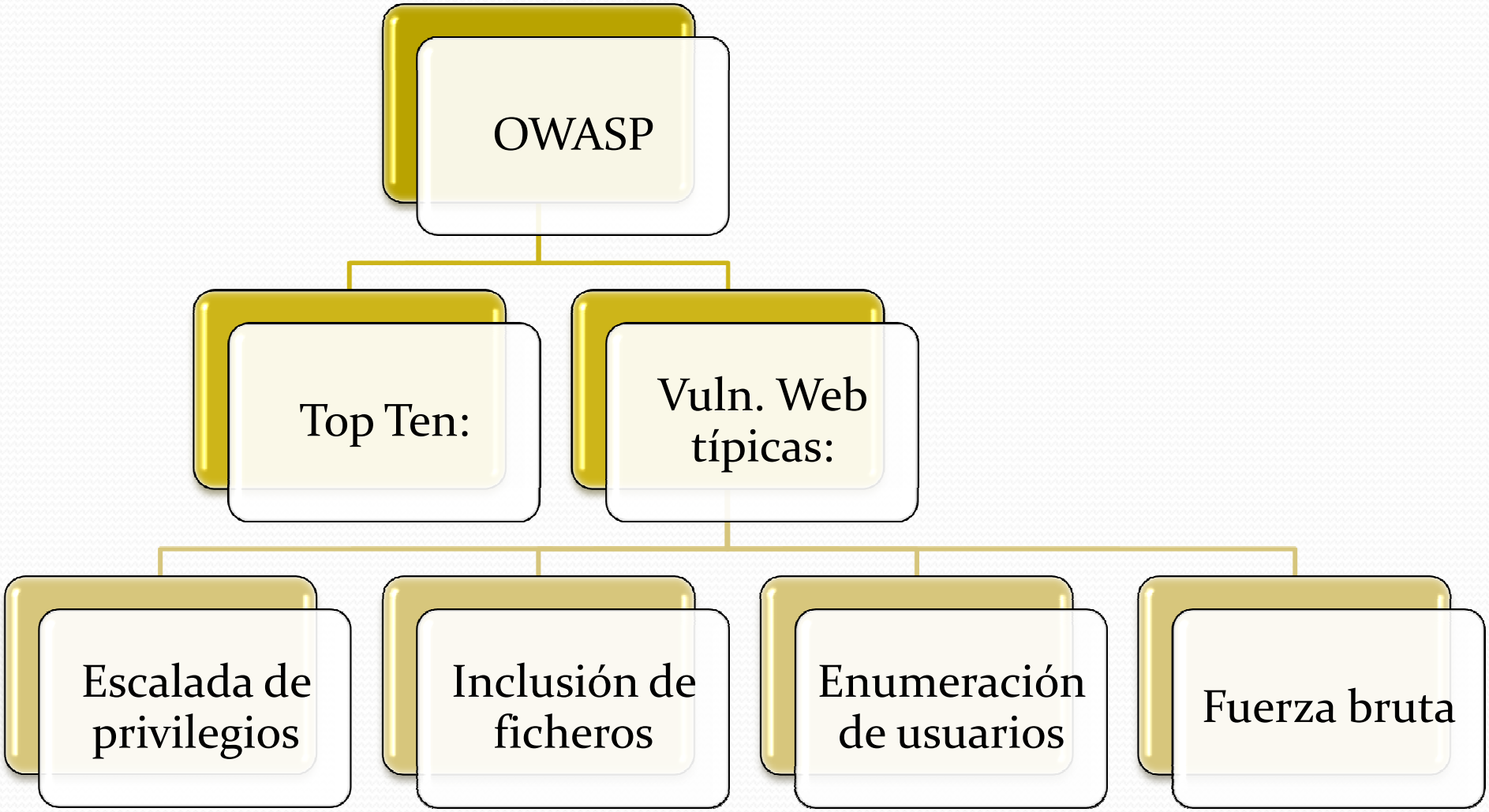
Metodologías de partida (I)



Metodologías de partida (II)

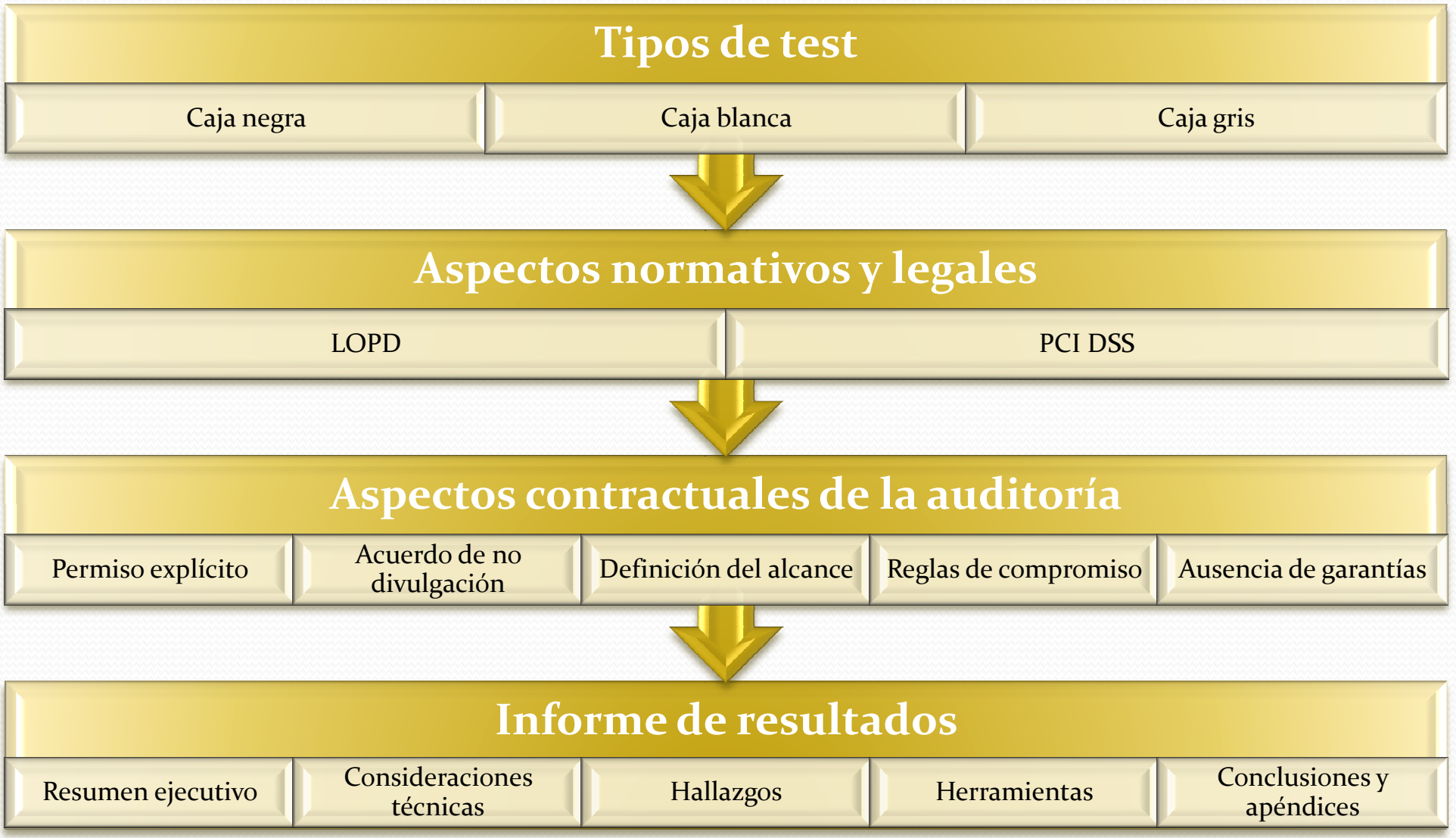


Metodologías de partida (III)



Metodologías de partida (IV)

Aspectos de la auditoría web



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_X9EKlR_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 [redacted] -oA nmap-TCP4000

Starting Nmap 6.47 ( http://nmap.org ) at 2014-10-25 09:26 EDT
Nmap scan report for [redacted]
Host is up (0.014s latency).
rDNS record for [redacted].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 W
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

Balanceadores de carga y WAF:

- Rastro mínimo,
- Webshell única,
- Errores.
- WAFWOOF / Halberd

Metodología. Mapeado (III)

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

```
[*] Running sslscan on [redacted].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.

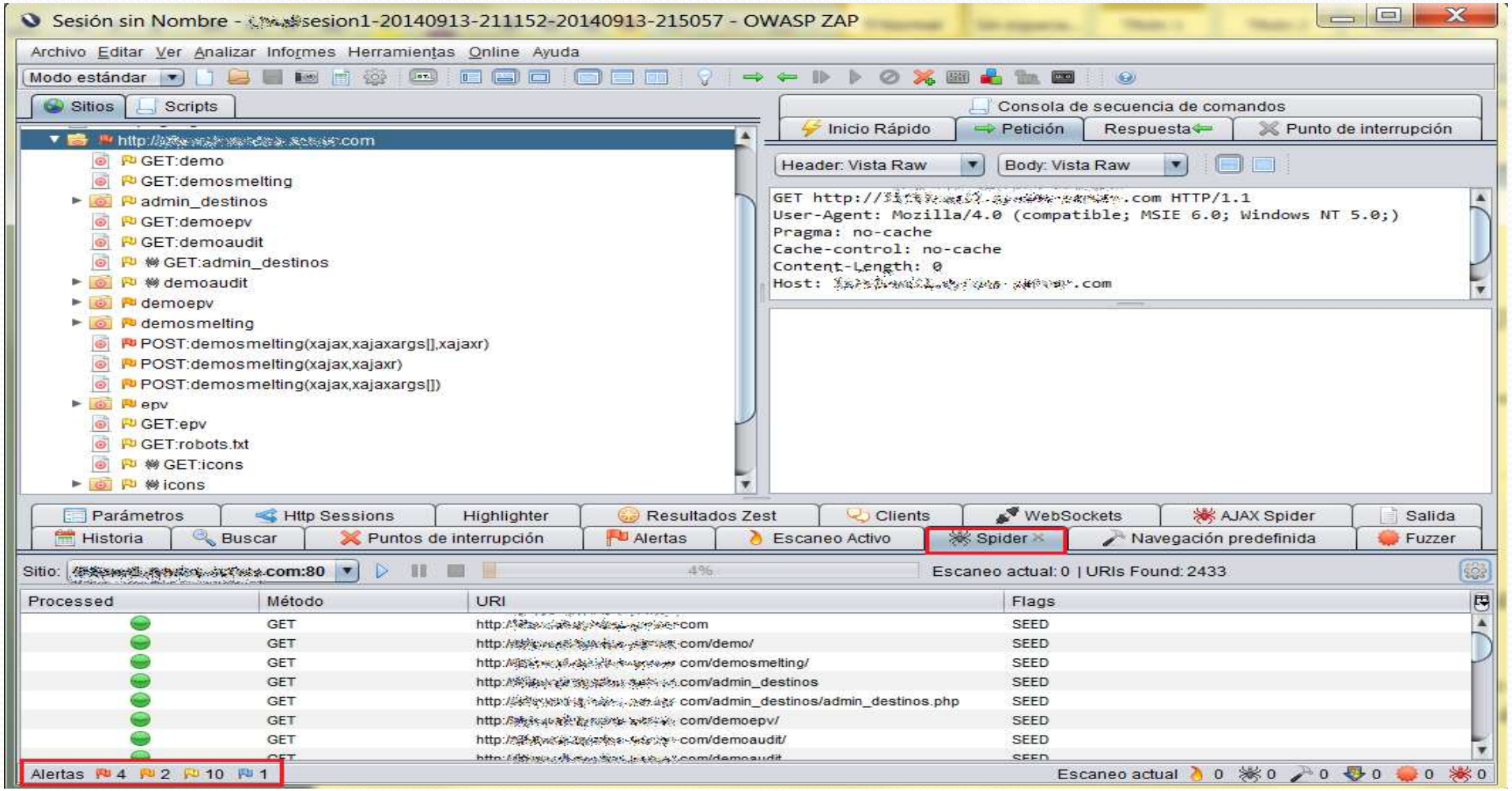
nikto –host dominio_cliente.com

```
root@kali:~# nikto -host [redacted].com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          [redacted]
+ Target Hostname:    [redacted].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, mti
+ 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 bru
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.



Metodología. Descubrimiento y explotación (I)

Detección:

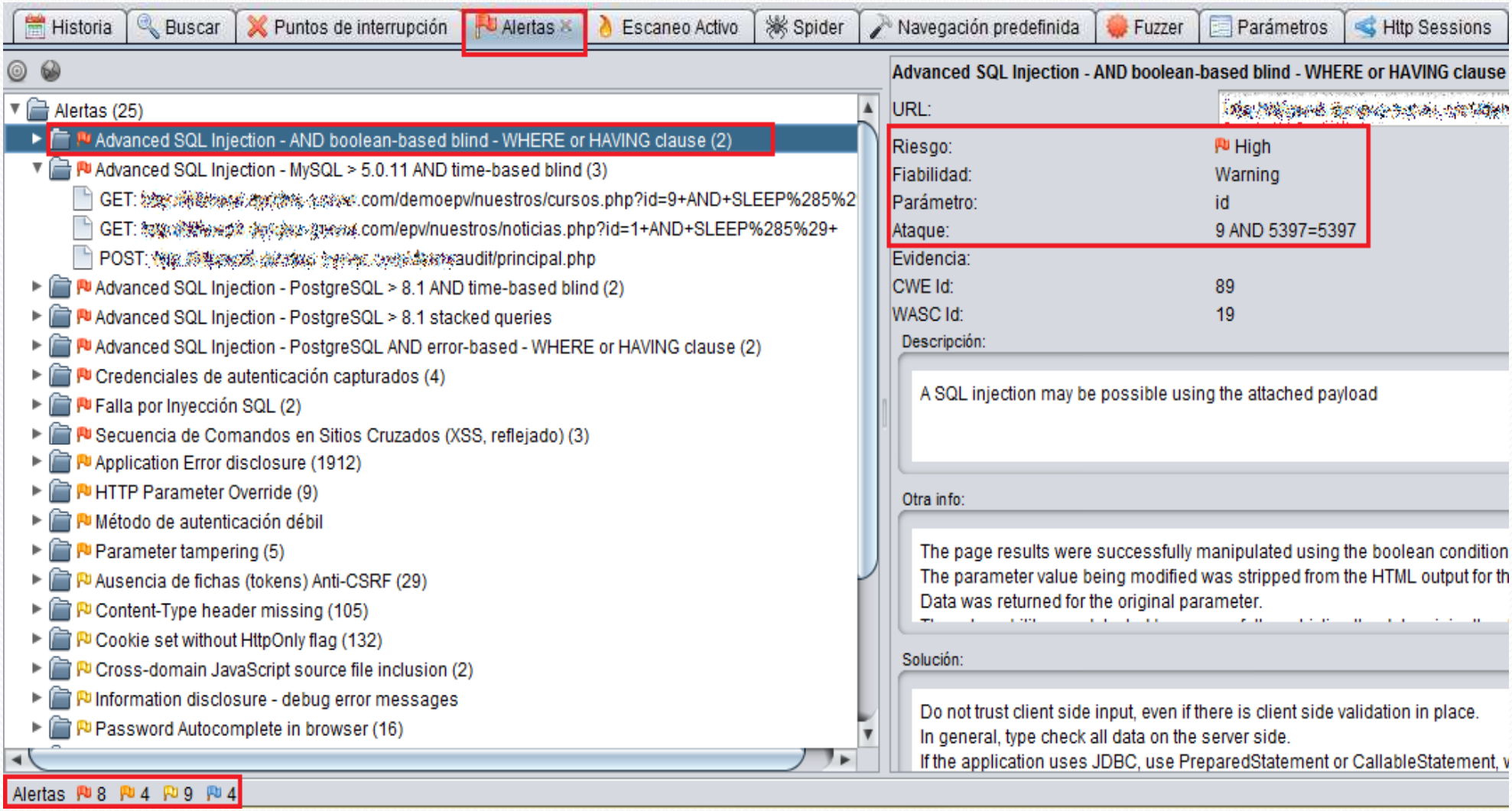
- Comportamiento ante errores.

%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 <b>/var/www/demosmelting/lib/dba/libgeneral_postgre.php</b> on line <b>33</b><br />
<br />
<b>Warning</b>:  pg_cmdtuples() expects parameter 1 to be resource, boolean given in <b>/var/www/demosmelting/lib/dba/libgeneral_postgre.php</b> on line <b>267
</b><br />
<?xml version="1.0" encoding="utf-8" ?><xjx><cmd n="js"><![CDATA[FinCierraPedido("", "7", "7", 1415640993);]]></cmd></xjx>
```

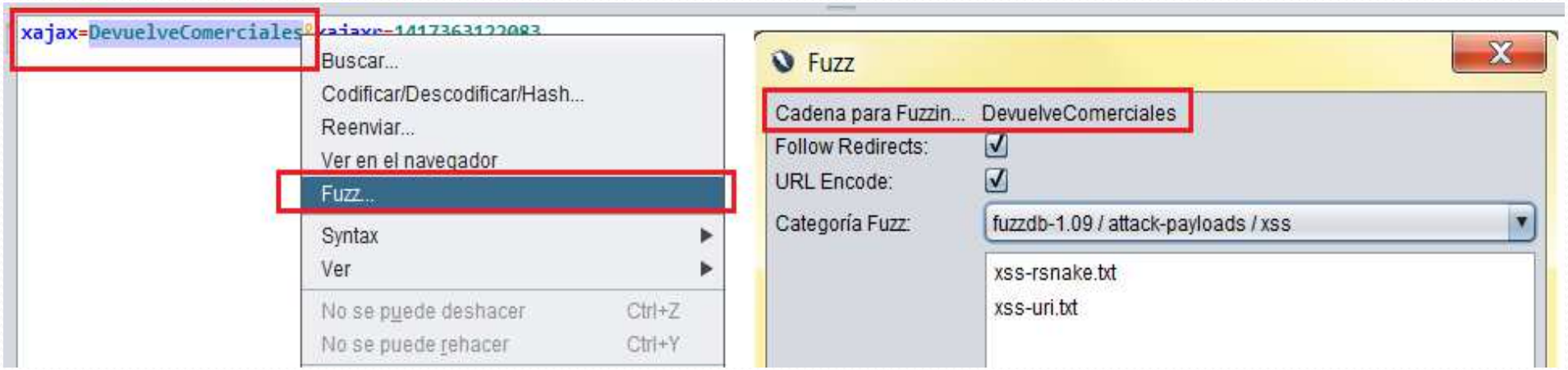
Metodología. Descubrimiento y explotación (II)

Escaneo de vulnerabilidades: Alertas.

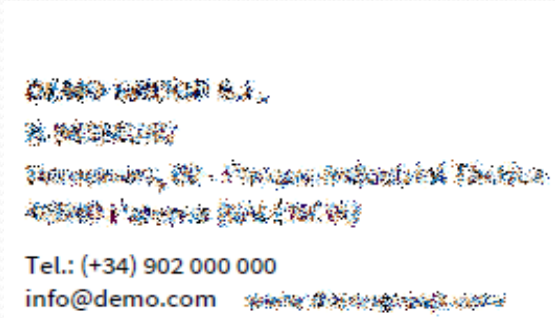


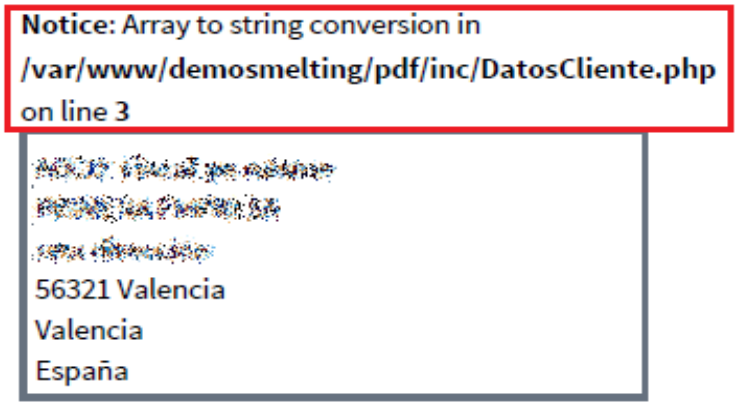
Metodología. Descubrimiento y explotación (III)

Fuzzing de parámetros.

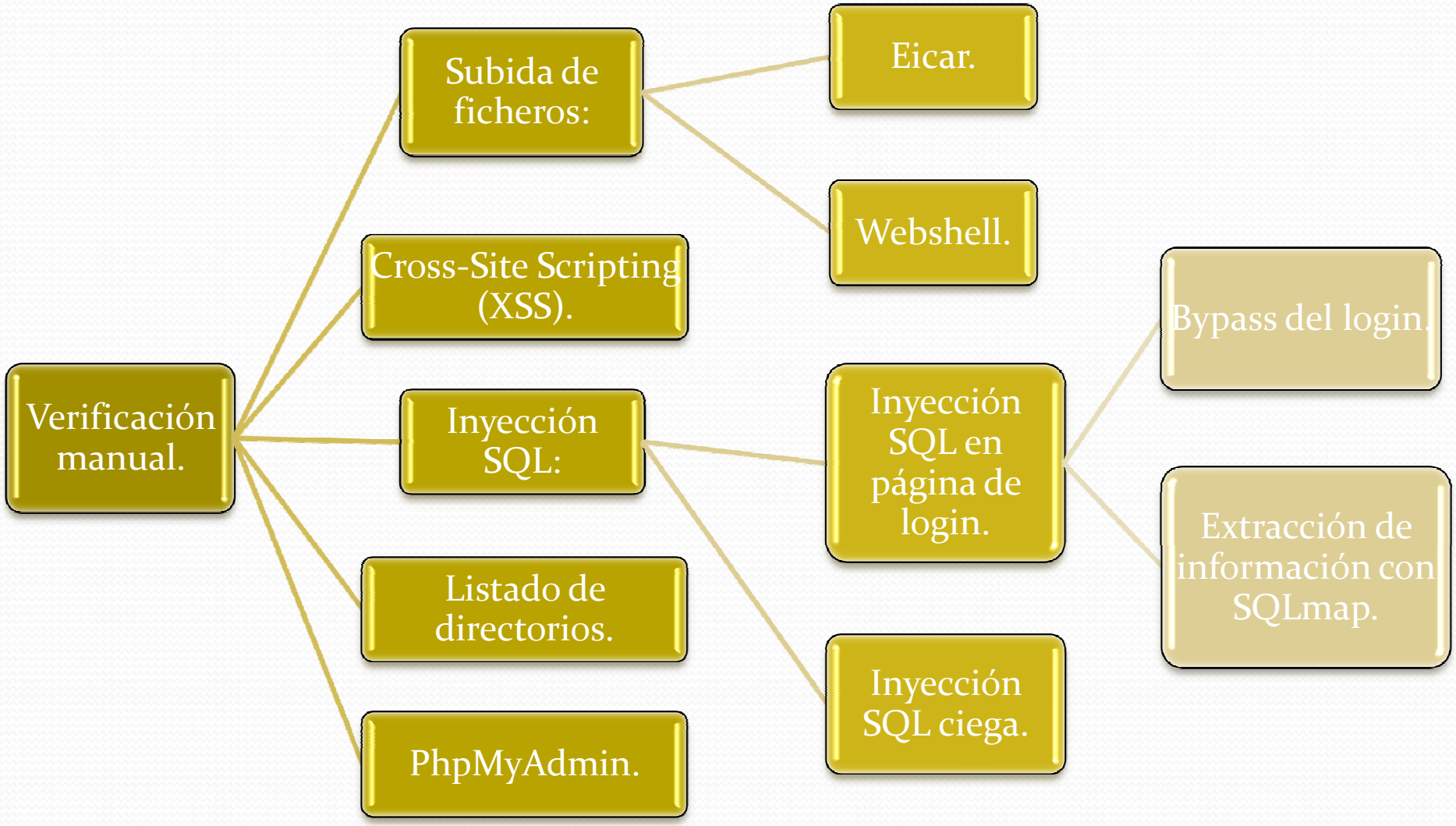


Divulgación de información.





Metodología. Descubrimiento y explotación (IV)



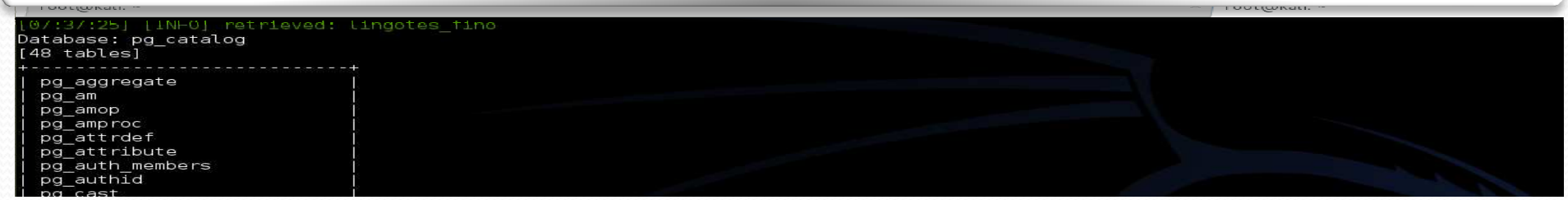
Metodología. Descubrimiento y explotación (V)

Inyección SQL: → **Bypass del login.**

```
SELECT * FROM users WHERE usuario='$usu' and password='$pass‘
SELECT * FROM users WHERE usuario='’ OR 1=1-- and password=’ ’
```

Inyección SQL: → **Extracción con Sqlmap.**

```
# sqlmap –u página_vulnerable.php --data=”cadena_login_pass” –p “parámetro”
```

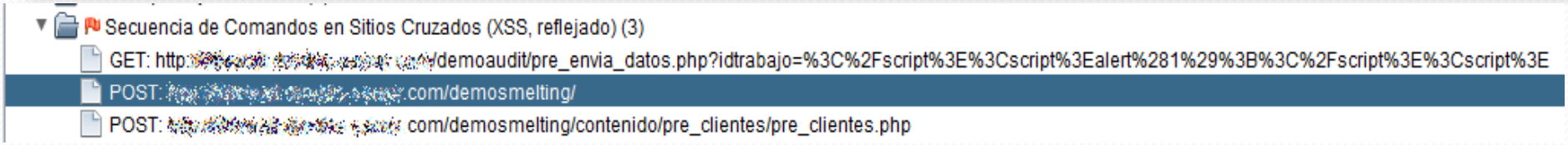


Inyección SQL: → **Ciega.**

```
http://dominio_cliente.com/nuestros/cursos.php?id=9+AND+1%3D1+
```

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.