

Seguridad en Servidores Web

Resumiendo sus principales aspectos

Jose Ignacio Recuerda Cambil Antonio Miguel Pozo Cámara Ignacio Cabrerizo Romero

ignaciorecuerda@correo.ugr.es

apozoetsit@correo.ugr.es

nachorc@correo.ugr.es

Índice

- Nota introductoria
- Tipología de ataques
- Búsqueda de vulnerabilidades y su análisis
- Técnicas de prevención
- Solución a ataques

1. Nota introductoria

¿POR QUÉ SIGUE HABIENDO ATAQUES A SERVIDORES WEB?

WhiteHACK

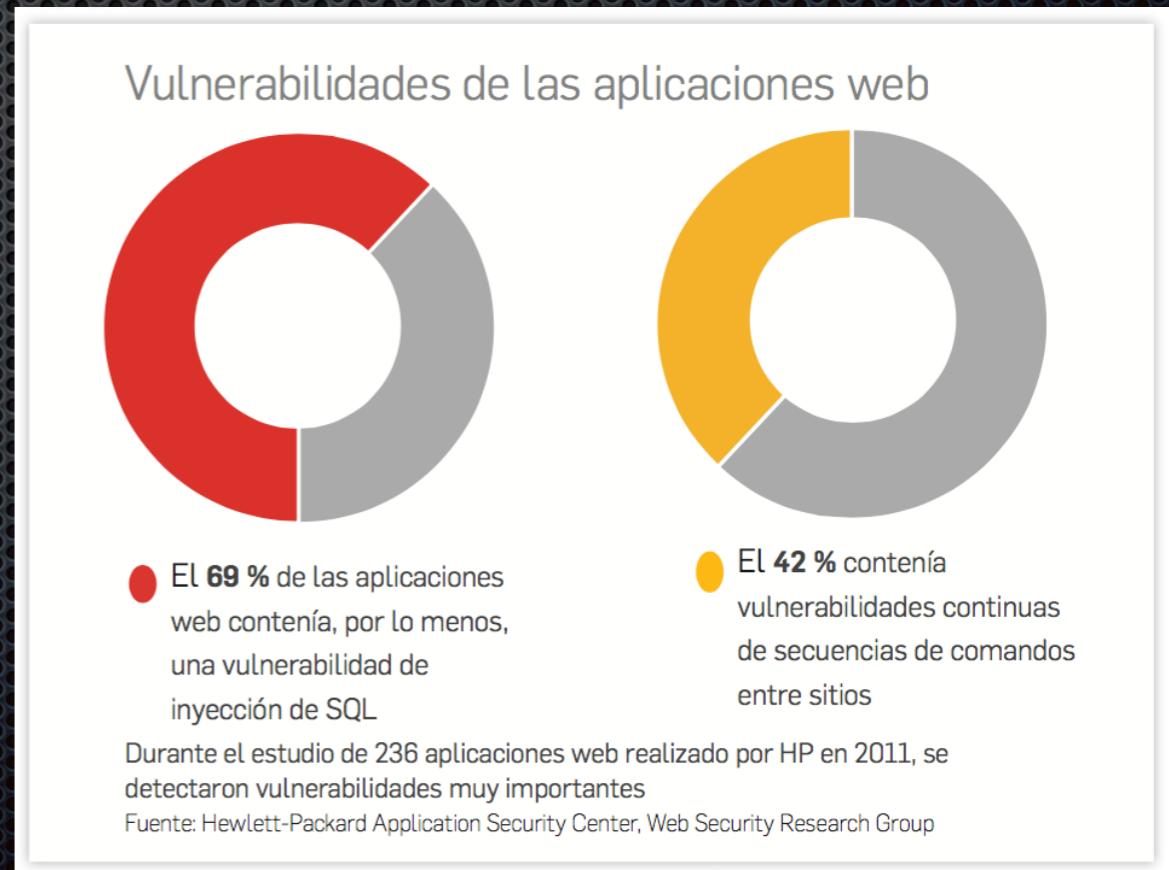
↓
¿RESPONSABLES?

BlackHACK

PENETRATION TEST (PENTESTING) → Pentesting by Design

Principales riesgos para la seguridad de aplicaciones web:

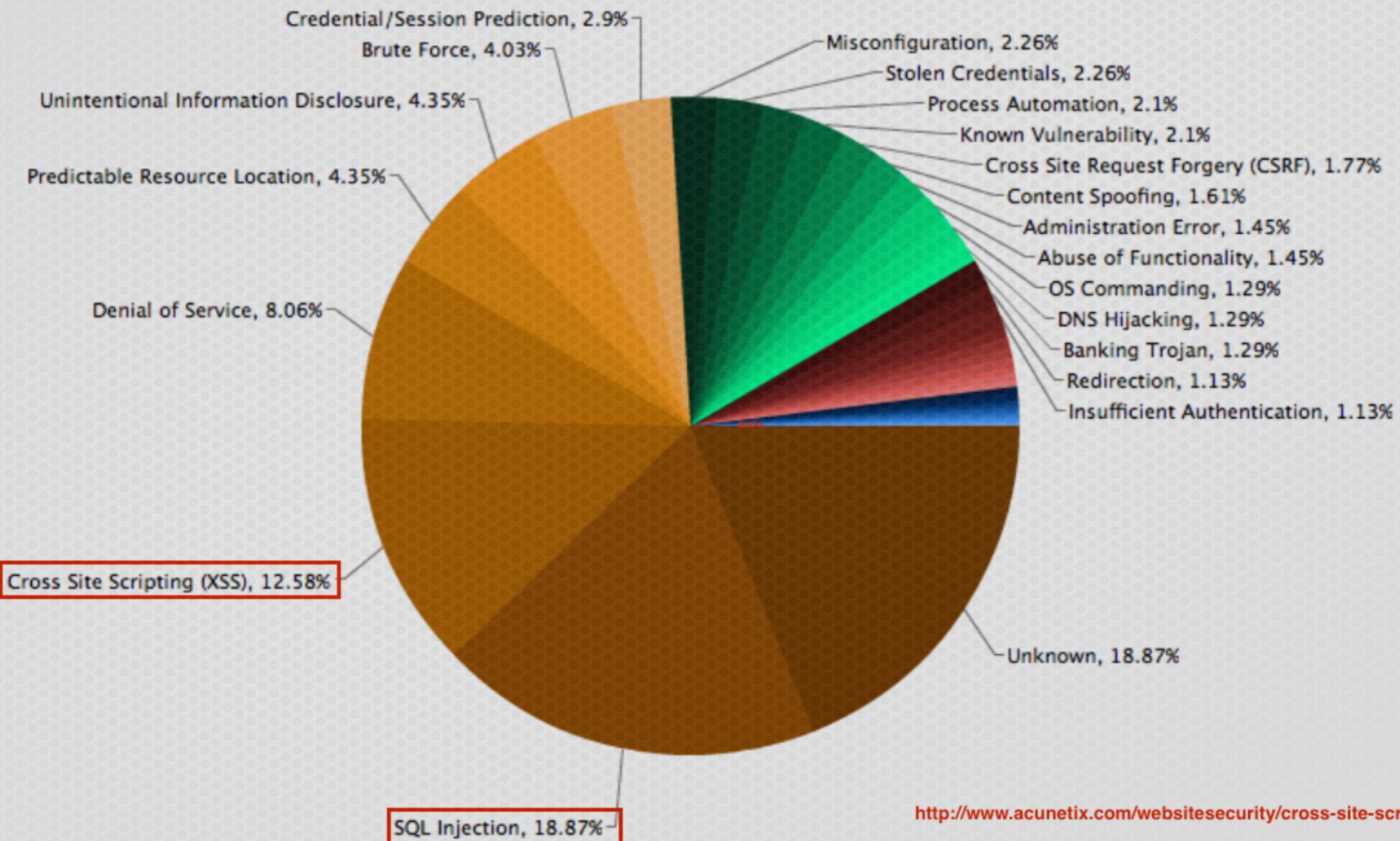
- Inyección
- Secuencias de comandos entre sitios (XSS)
- Referencias directas no seguras a objetos
- Pérdida de autenticación y gestión de sesiones
- Falsificación de peticiones entre sitios (CSRF)
- Errores en la configuración de la seguridad
- Almacenamiento criptográfico poco seguro
- Protección insuficiente de la capa de transporte
- Redirecciones y desvíos no validados
- Falta de restricción del acceso a direcciones web



2. Tipología de ataques

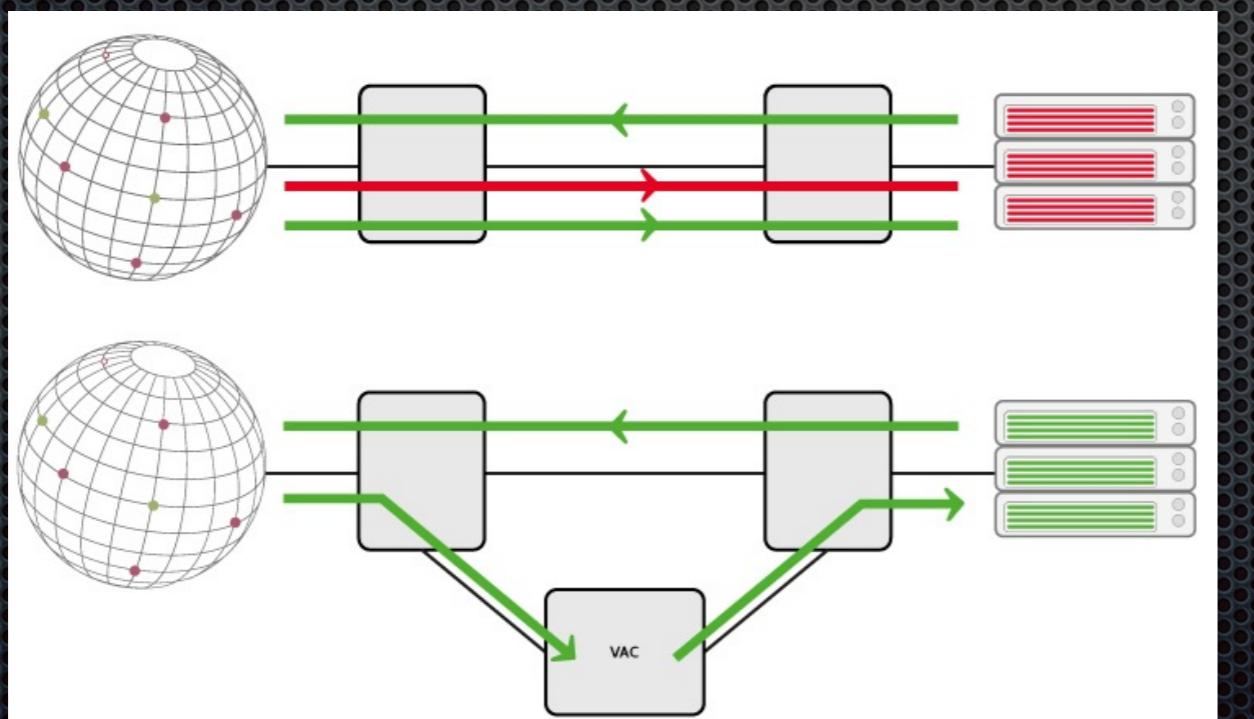
- DDOS
- Fuerza Bruta
- Inyección SQL
- XSS (Cross Site Scripting)
- Phishing

2. Tipología de ataques



2.1 DDOS

- Un número muy grande de accesos al servidor que consigue saturar el ancho de banda o sobrecargar el sistema dejándolo inaccesible.
- Los accesos se realizan desde diferentes sitios geográficos.



2.2 Fuerza Bruta

- Prueba masivamente todas las combinaciones posibles para acceder a un recurso.
- Suelen proporcionarse mediante diccionarios.
- Aplicaciones para este tipo de ataques:
 - BrutusAE.
 - thc-hydra.
 - Medusa.



2.3 Inyección SQL

- Inserta una serie de sentencias SQL mediante la entrada de datos.
- Se hacen con webs que interactúan con bases de datos.
- El objetivo suele ser sacar información de la base de datos.



2.4 XSS (Cross Site Scripting)

- Inserta código HTML o JavaScript mediante la entrada de datos.
- Compromete la seguridad del usuario.
- Se consigue acceder a las cookies o token de sesión.
- Existen dos tipos: permanentes y no permanentes.

2.4 XSS (Cross Site Scripting)



2.5 Phishing



- Técnica usada para captar información de los usuarios haciendo creer que están en una página de confianza (réplica en aspecto y funcionalidad de la original) para sustraer información sensible. Generalmente las páginas clonadas son enlazadas a través de un correo electrónico.

OpenDNS

PhishTank® Out of the Net, into the Tank.

3. Búsqueda de vulnerabilidades y su análisis

- Herramientas destacadas de escaneo/análisis:

- Nikto
- Htppanalyzer
- Archilles
- ZAP (Zed Attack Proxy) + OWASP
- NMAP + NSE Vulscan
- OpenVAS
- Nessus



3. Búsqueda de vulnerabilidades y su análisis

```
+ Target IP:          74.217.87.87
+ Target Hostname:   webscantest.com
+ Target Port:        80
+ Start Time:        2014-03-16 13:23:30 (GMT0)
-----
+ Server: Apache
+ Cookie SESSIONID_VULN_SITE created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.3
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, inode: 4920
56, size: 101, mtime: 0x4f135f9b82c00
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microso
ft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals poten
tially sensitive information via certain HTTP requests that contain specific QUERY st
rings.
+ OSVDB-3092: /cart/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 6544 items checked: 0 error(s) and 13 item(s) reported on remote host
+ End Time:         2014-03-16 13:43:12 (GMT0) (1182 seconds)
-----
+ 1 host(s) tested
```



3. Búsqueda de vulnerabilidades y su análisis

Obtener información de un host remoto y detección del SO (escaneo sigiloso sin ping):

```
nmap -sS -P0 -sV -o [dirección]
```

Listar servidores con un puerto específico abierto:

```
nmap -sT -p 80 -oG - 192.168.1.* | grep open
```

Detectar IP's activas en una red:

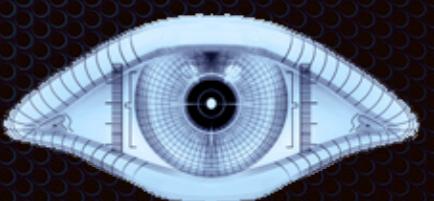
```
nmap -sP 192.168.0.*
```

Escanear en busca de AP falsos:

```
nmap -A -p1-85,113,443,8080-8100 -T4 --min-hostgroup 50 --max-rtt-timeout 2000 --initial-rtt-timeout 300 --max-retries 3 --host-timeout 20m --max-scan-delay 1000 -oA wapscan 10.0.0.0/8
```

Señueño durante escaneo de puertos para evitar detección:

```
(root) nmap -sS 192.168.0.10 -D 192.168.0.2
```



4. Técnicas de prevención

- Control de los archivos publicados
 - DocumentRoot
 - Directiva alias
 - Enlaces simbólicos
- Ocultar información
 - Deshabilitar listado de ficheros
 - Limitar acceso a archivos con determinada extensión
 - Información devuelta en caso de error

4. Técnicas de prevención

- Interfaz de entrada común y módulos
 - Controlar que la interacción cliente-servidor no sea intrusiva
- Autenticación y autorización
 - Por contraseña
 - Autorización a grupos

4. Técnicas de prevención

- Comunicación HTTPS
 - Ventajas / Inconvenientes sobre HTTP
- Monitorización
 - Monitorización del servicio (mod_status)
 - Configuración y revisión de logs
 - Detección de ataques (mod_security)
 - Violaciones HTTP
 - IPs en listas negras
 - Otros ataques comunes

5. Solución a ataques

Recogida de evidencias

Respuesta a incidentes

5.1 Recogida de evidencias

Análisis

Aplicaciones

Bases de datos

Red

RAM

SWAPPING

Discos físicos

Impresoras

Dispositivos móviles

5.2 Respuesta a incidentes

¡Fragilidad de las pruebas!

Datos de equipos implicados

Titular del equipo y organización a la que pertenece

SO y su versión

Tipo de BIOS e información hardware

Tiempo sin apagarse

Ubicación del archivo de paginación

Estructura de directorios del sistema

5.2 Respuesta a incidentes

Ataque DDOS

"Fue peor el remedio...



Seguridad en Servidores Web

...que la enfermedad"



KONA Site Defender



5000\$/mes

5.2 Respuesta a incidentes

Ataque de fuerza bruta



http://www.fail2ban.org/wiki/index.php/Main_Page

5.2 Respuesta a incidentes

Ataque Inyección SQL, XSS y Phishing



¡CORRE A POR TUS DATOS!

6. Referencias

- Libro “Hackers, Aprende a atacar y a defenderte” Capítulo 5 Hacking de Servidores Web.
- [1, <https://mmonit.com/monit/>, 12-mayo-2015]
- [2, http://www.interoute.es/sites/default/files/files/datasheet_Oddos_mitigation.pdf, 12-mayo-2015]
- [3, <http://www.corero.com/es/>, 12-mayo-2015]
- [4, <http://fail2ban.org/>, 12-mayo-2015]
- [5, <http://www.seguridadpc.net/phishing.htm>, 12-mayo-2015]
- [6, <http://www.brandprotect.com>, 12-mayo-2015]
- [7, <https://www.sophos.com/es-es/medialibrary/Gated%20Assets/white%20papers/sophosclosingbackdoornetworkapplicationvulnerabilitieswpna.pdf?la=es-ES.pdf>, 12-mayo-2015]

Otras referencias:

- [<http://www.linux-party.com/8966-25-trucos-de-seguridad-para-servidores-linux-1-de-2#>, 12-mayo-2015]
- [<http://www.escueladeinternet.com/seguridad-en-servidores-dedicados>, 12-mayo-2015]
- [<http://www.tecmint.com/linux-server-hardening-security-tips/>, 12-mayo-2015]