



Mundo web: Ataques y Defensas

<Diego Subero>

- <*diego.subero@gmail.com*>

*<0426518053>

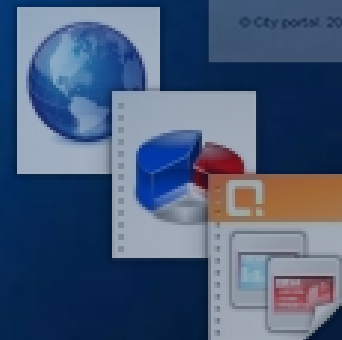
Agenda

- Crecimiento de las web app
- Estructura de una web app
- Vulnerabilidades comunes en Venezuela
- ¿Como atacan?
- Herramientas de defensa inmediata





A simple vista



Registros



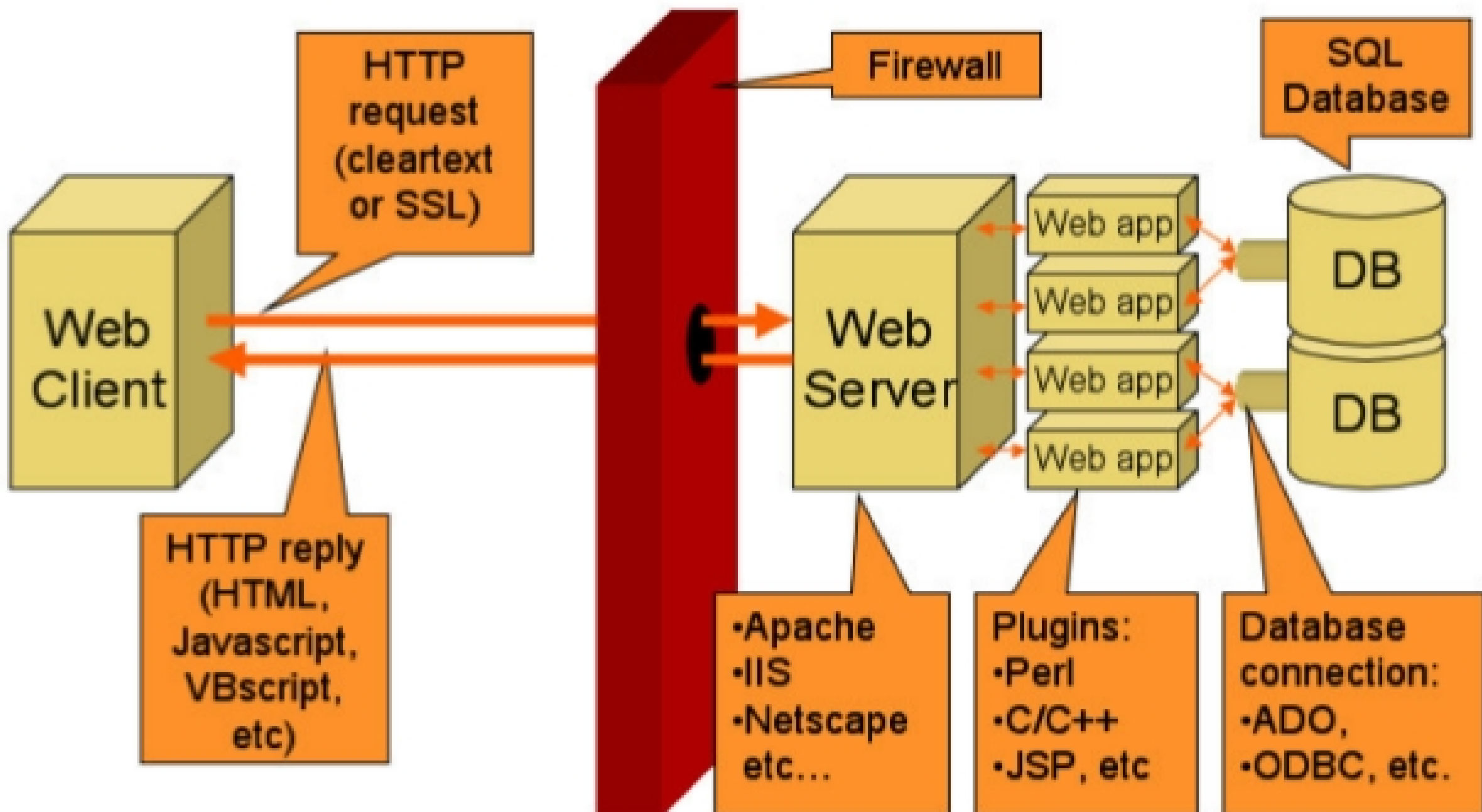
Código fuente

Lo que no se observa...

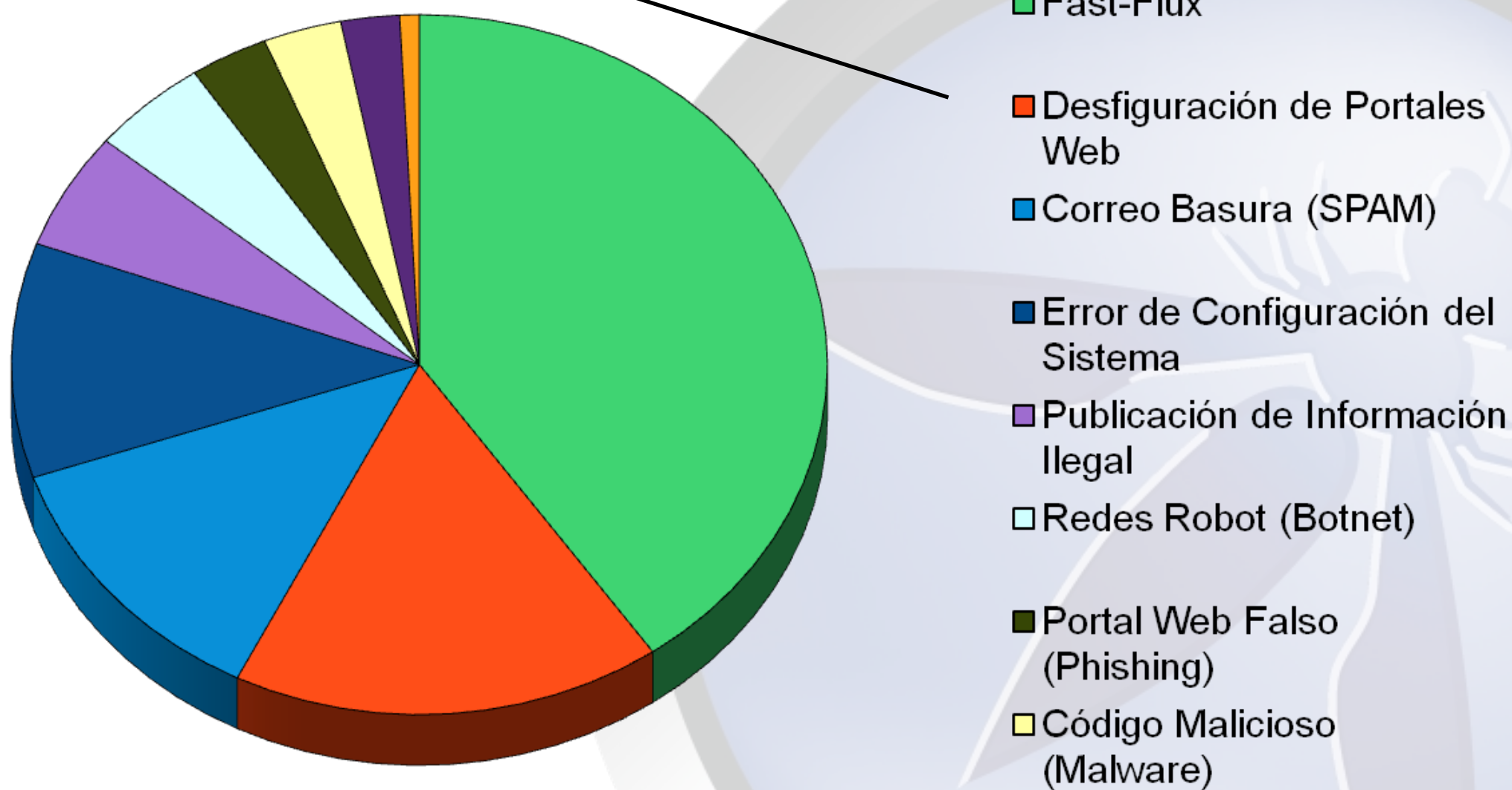


Base de datos

Estructura básica de interna de un portal



Ataque que ocurre con mucha frecuencia en Venezuela



Fuente: VenCERT



Como llegamos a un defacement



[H]acked By [G]othic-X & [D]uff

[S]ecurity OFF



SEGUN WIKIPEDIA SIGNIFICA:

Bellas Artes describe una forma de arte desarrollada principalmente por la estética que por su utilidad práctica. Históricamente las principales son: la arquitectura, la escultura, la pintura, la literatura, la danza y la música. Sin embargo, en algunas instituciones educativas y en museos de *bellas artes* se le asocia exclusivamente a las artes visuales. En este sentido, la palabra arte también es muchas veces sinónimo de bellas artes, al ser empleado en términos como "galería de arte".

PERO QUE REALMENTE ES BELLAS ARTES?

PUES para ejemplo un boton.

Como empieza el asunto?



**Reconocimien
to**

Google

<http://www.hackersforcharity.org/ghdb/>

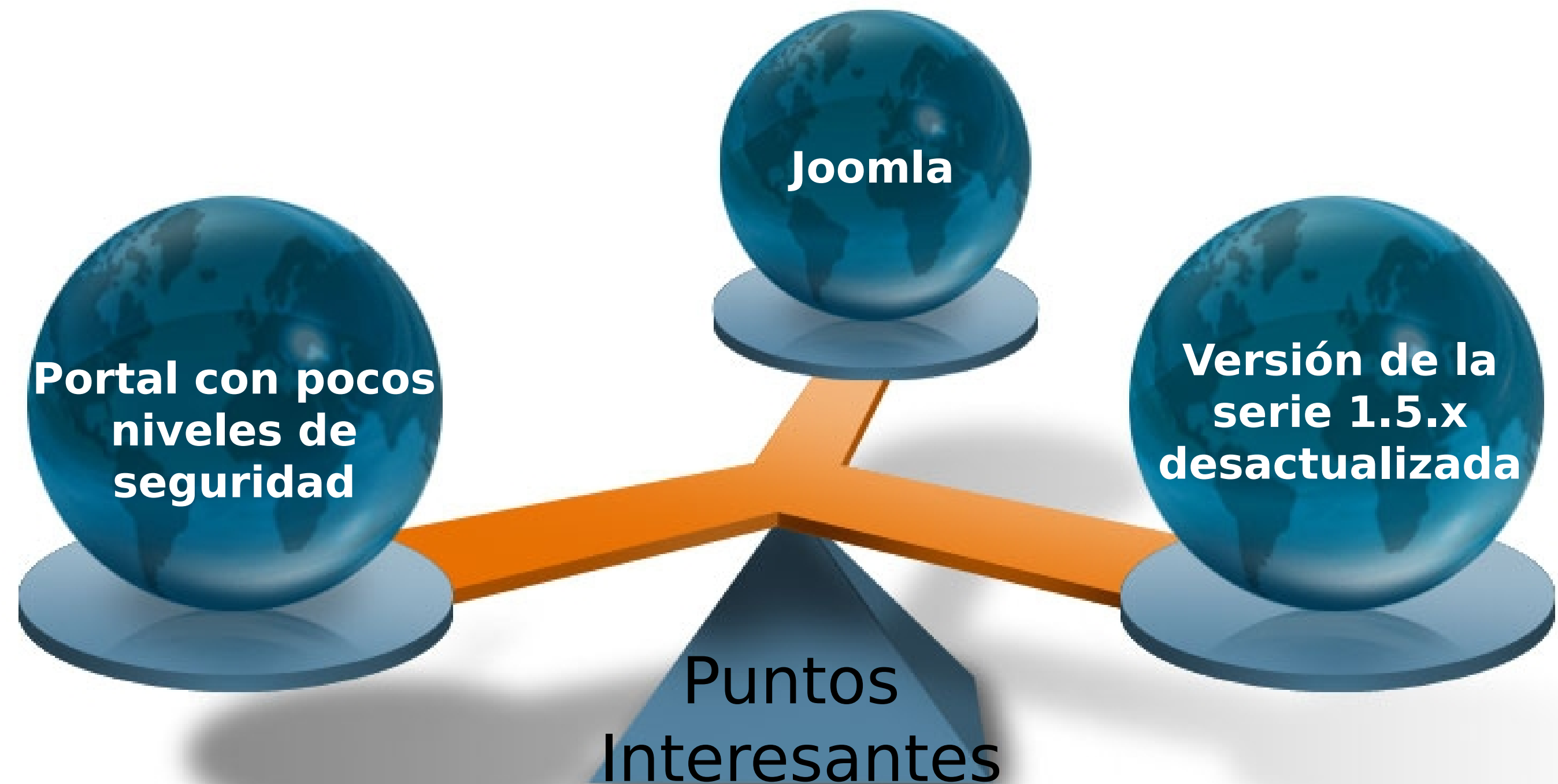
Navegación

Navegación Manual, búsqueda de subdominios, análisis de URL's ...

Identificación

Whatweb, Wafp...

Información encontrada





Escaneo y Vulnerabilidades

Escaneos

✓ W3AF, **Joomscan (Owasp)**, Acunetix

Vulnerabilidad

✓ <http://www.exploit-db.com>



Explotación

Ejecución

✓ **Manual** o automatizada



Mecanismos
de defensa
inmediata o
contención



**OWASP Zed
Attack Proxy
Project**

Actualizar versión de Joomla

Elevar niveles de seguridad

Sanitizar el código del portal

Implementar firewall de aplicaciones
Modsecurity

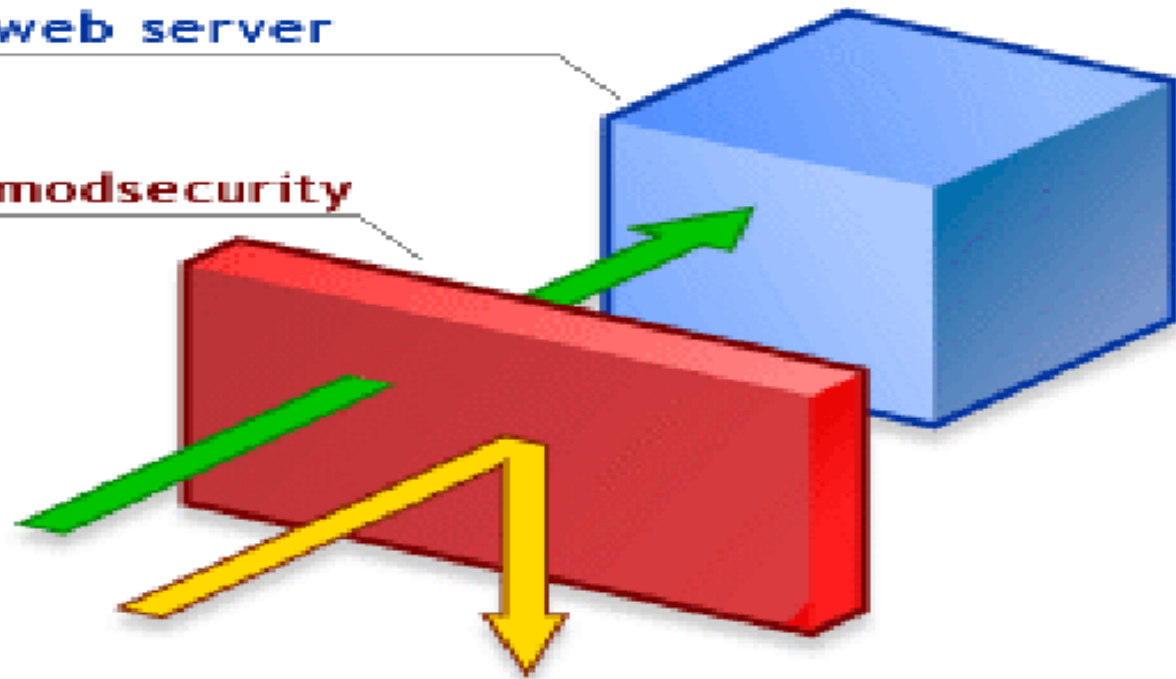
Implementar mecanismos o
herramientas de monitoreo
OSSEC

Evaluaciones de Seguridad

ModSecurity

web server

modsecurity



XSS, scanning

Sql
injection,
DDOS



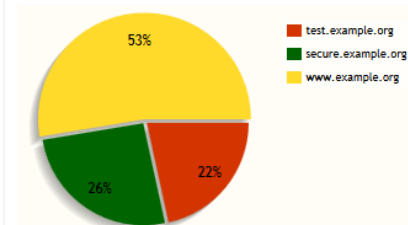
Reglas actualizadas por parte de la OWASP



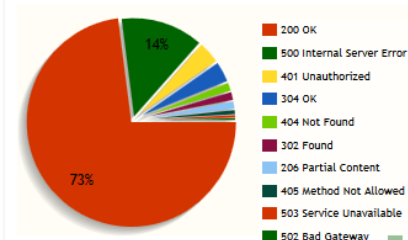
HOME | EVENTS | FILTER | MANAGEMENT

Logged User: Admin | My Preferences | Logout

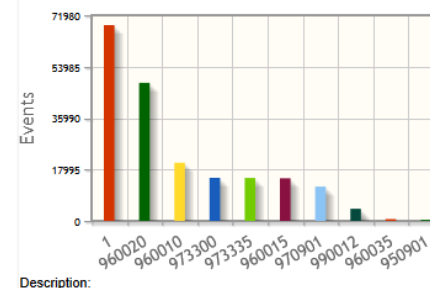
Events per sensor (last 24 hours)



Events per status (last 24 hours)

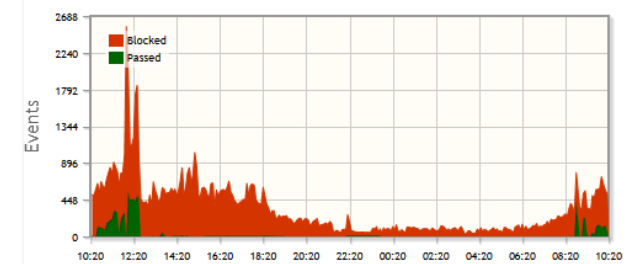


Top Rules in last 24 hours

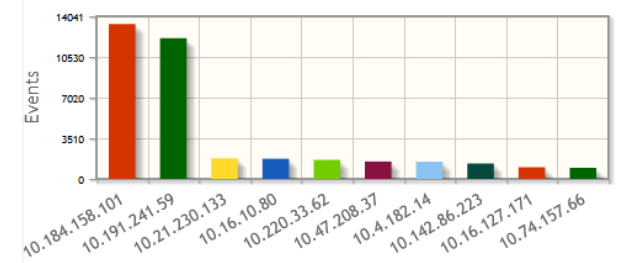


Description:

Events in last 24 hours



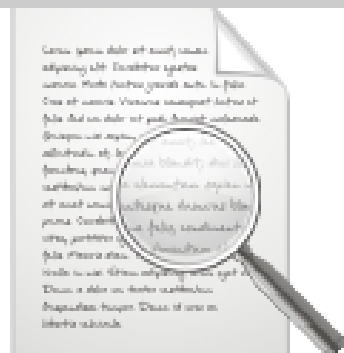
Top Sources in last 24 hours



Top Targets in last 24 hours



HIDS



Integridad de
archivos



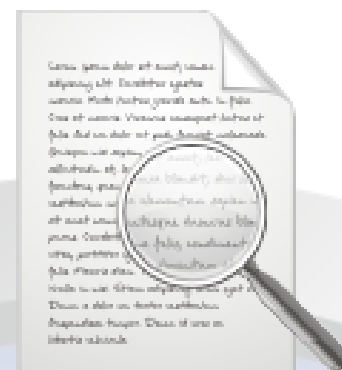
Añade reglas a la
configuración de
iptables



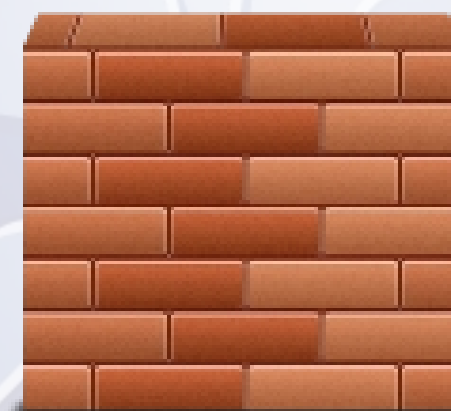
Deteccion de rootkit



Envio de alertas,
via correo



Monitoreo de logs
Y analizador



Añade una entrada
a /etc/hosts.deny
denegando
el acceso

Modo standalone Modo cliente-servidor

Hace de cliente y de servidor

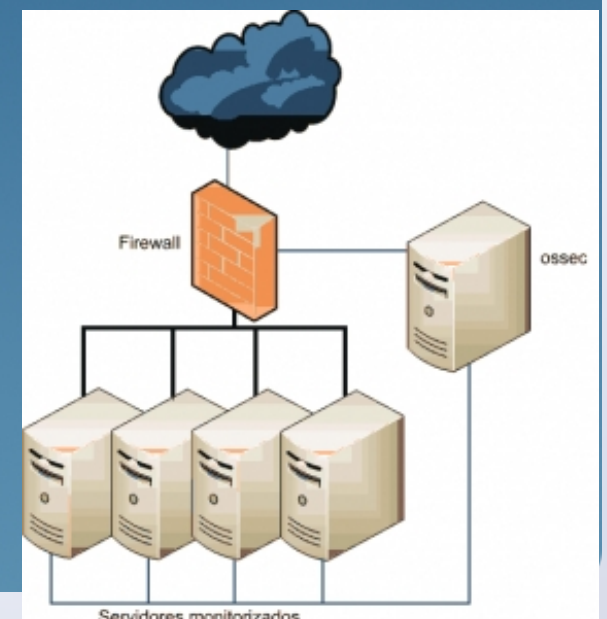
Útil para servidores expuestos a internet o ambientes limitados

Los registros quedan en el servidor

Comunicación entre el agente y el server es realizada mediante mensajes UDP

Los paquetes UDP van encriptados mediante una llave simétrica

Revisión de versionado periódica





Summary & Conclusion





SGSI

Actualizar

Validar

Revisiones de código

Monitoreo...

Indagar en lo que no esta a simple
vista