OWASP DJANGO-ANGULAR

Autor: Jorge Luis Malla Sánchez
jorge.malla@unl.edu.ec

Agenda

1. Introducción
2. Owasp Top Ten 2013
3. Inyección sql
4. XSS
5. CSRF
6. Exposición de datos sensibles
7. Inexistente Control de Acceso a nivel de funcionalidades

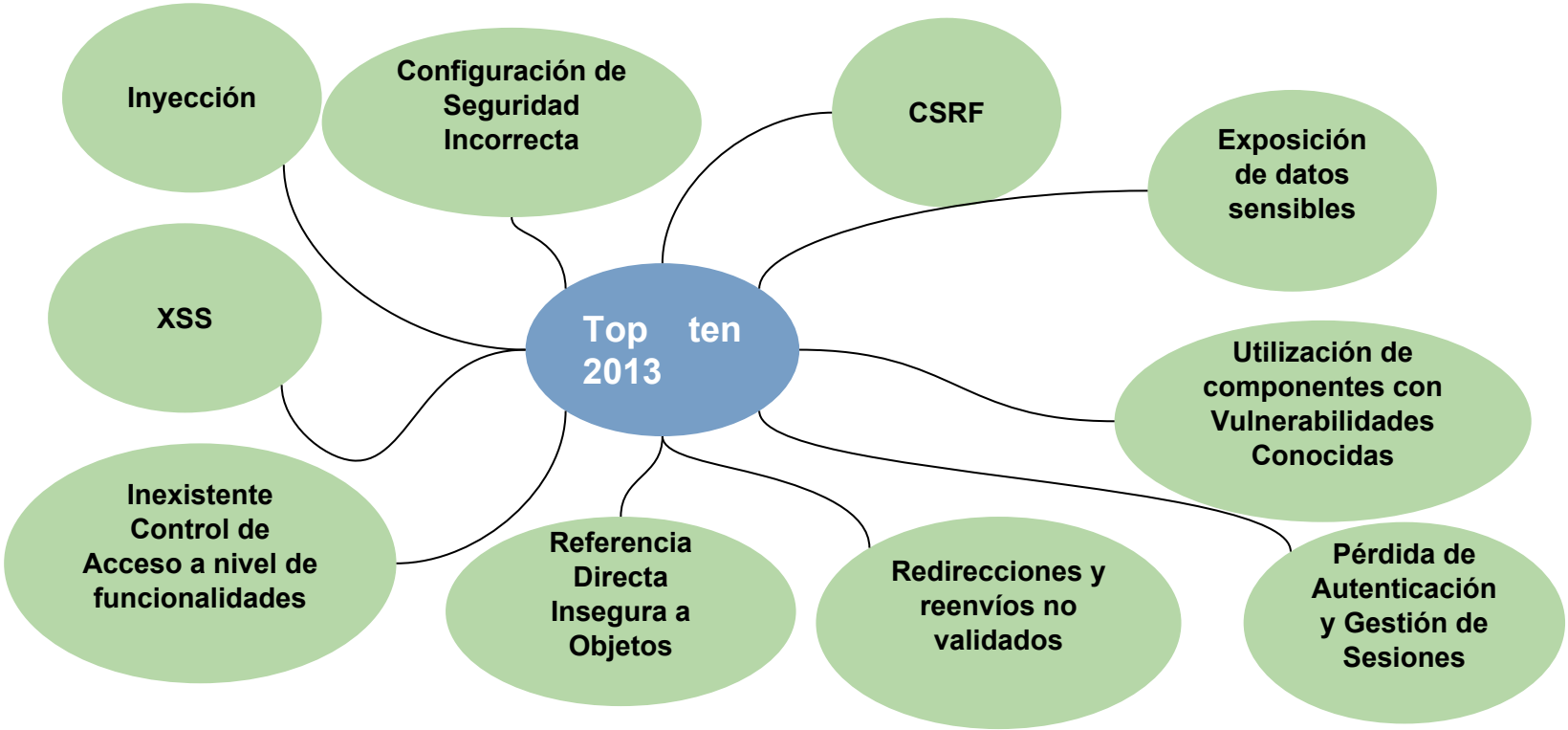
Introducción

Uno de los mayores retos para un equipo de desarrollo de aplicaciones web es el problema de seguridad

OWASP es es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

Desarrollar aplicaciones web seguras con Django y Angular con ayuda de la guía OWASP.

OWASP TOP TEN 2013



Inyección SQL

Inyección SQL

Enviar una consulta sql para que sea interpretada

XSS

XSS
(Secuencias de órdenes en sitios cruzados)

Enviar comandos en el navegador de la víctima para dirigirla a un sitio malicioso

CSRF

CSRF
(Falsificación de peticiones en sitios cruzados)

Se presenta cuando un sitio Web malicioso induce a un usuario a cargar sin saberlo una URL desde un sitio al cual dicho usuario ya se ha autenticado

Inexistente Control de Acceso a nivel de funcionalidades

Inexistente Control de Acceso a nivel de funcionalidades

Accesso o Peticiones a usuarios no autorizados

Exposición de Datos Sensibles

Exposición de Datos Sensibles

Exposición de datos en tránsito en el navegador del cliente, como la contraseña.

django-secure,
django sslserver