Desarrollo seguro de Aplicaciones Web basado en OWASP

Por: Carlos Carreño,

OCP, ScrumMaster, Solution Architect

Email: ccarrenovi@Gmail.com

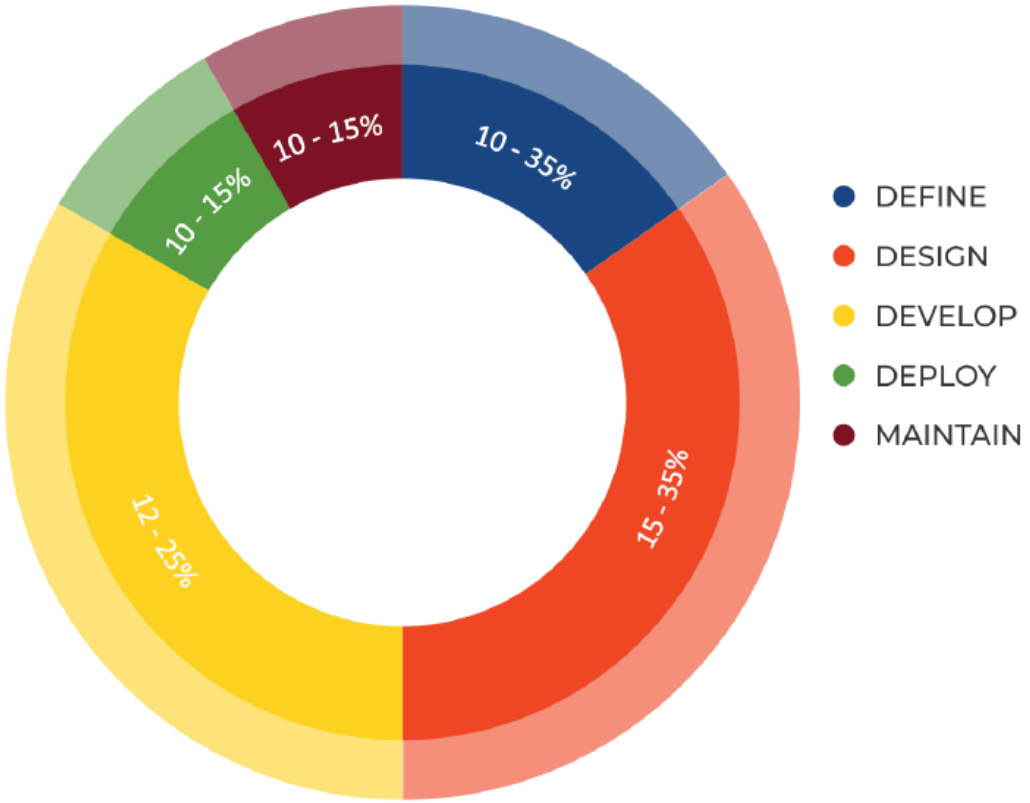
Unidad 6 Testing de seguridad de software

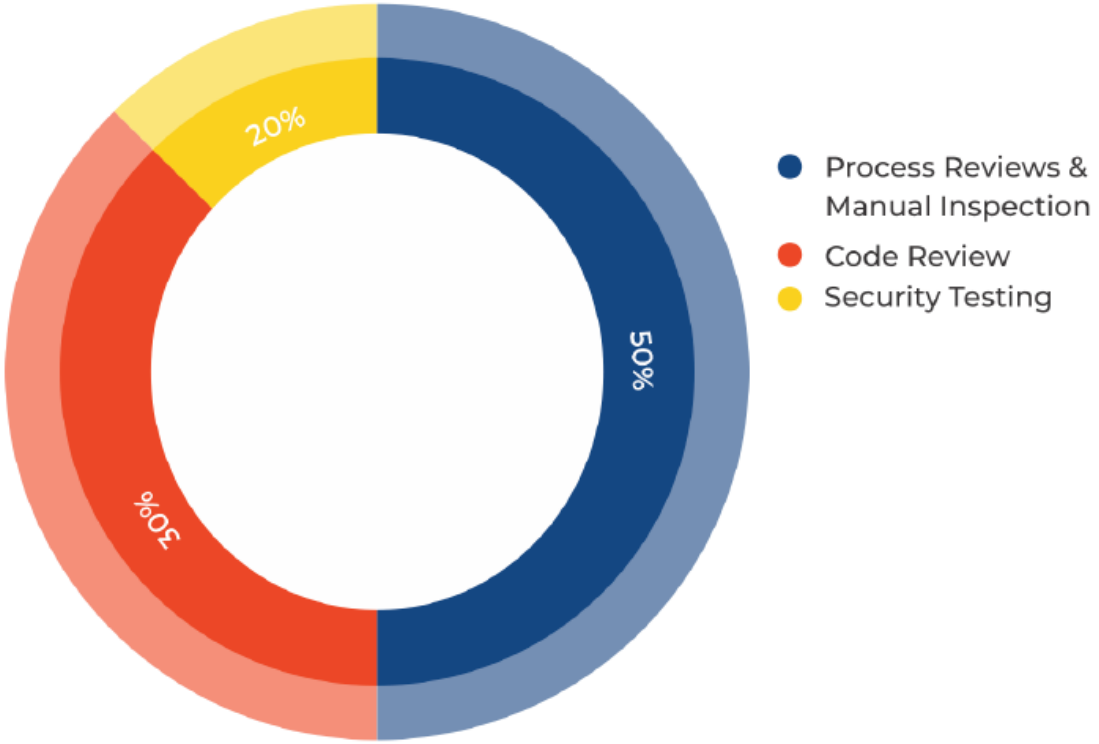
- Técnicas de testing de seguridad
- Testing de seguridad vs testing funcional
- Revisión de código
- Recursos de OWASP para testing de seguridad
- OWASP Testing Project
- OWASP Code Review Guide
- Testing de seguridad en el ciclo de vida del software
- Escalamiento de privilegios
- Herramientas de testing de seguridad
- Burp, Dirbuster, Nikto, W3af, Nessus

Técnicas de testing de seguridad

- Manual Inspections & Reviews
- Threat Modeling
- Code Review
- Penetration Testing

Nivel de Esfuerzo en Testing





Autor: ccarrenovi@Gmail.com

Testing de seguridad vs testing funcional

- Una prueba funcional es una prueba basada en la ejecución, revisión y retroalimentación de las funcionalidades previamente diseñadas para el software (requisitos funcionales).
- El testing de seguridad se refiere a realizar las pruebas con la finalidad de validar si el sistema cumple los requisitos de seguridad identificados durante la etapa de análisis y diseño

Revisión de código

- La revisión del código fuente es el proceso de verificar manualmente el código fuente de una aplicación web en busca de problemas de seguridad.
- Muchas vulnerabilidades de seguridad graves no se pueden detectar con ninguna otra forma de análisis o prueba.

"si quieres saber qué está pasando realmente, ve directamente a la fuente"

...

- **Ventajas**
  - Integridad y eficacia
  - Exactitud
  - Rápido (para revisores competentes)

- **Desventajas**
  - Requiere desarrolladores de seguridad altamente capacitados
  - Puede perder problemas en bibliotecas compiladas
  - No se pueden detectar errores en tiempo de ejecución fácilmente
  - El código fuente realmente implementado puede diferir del que se está analizando

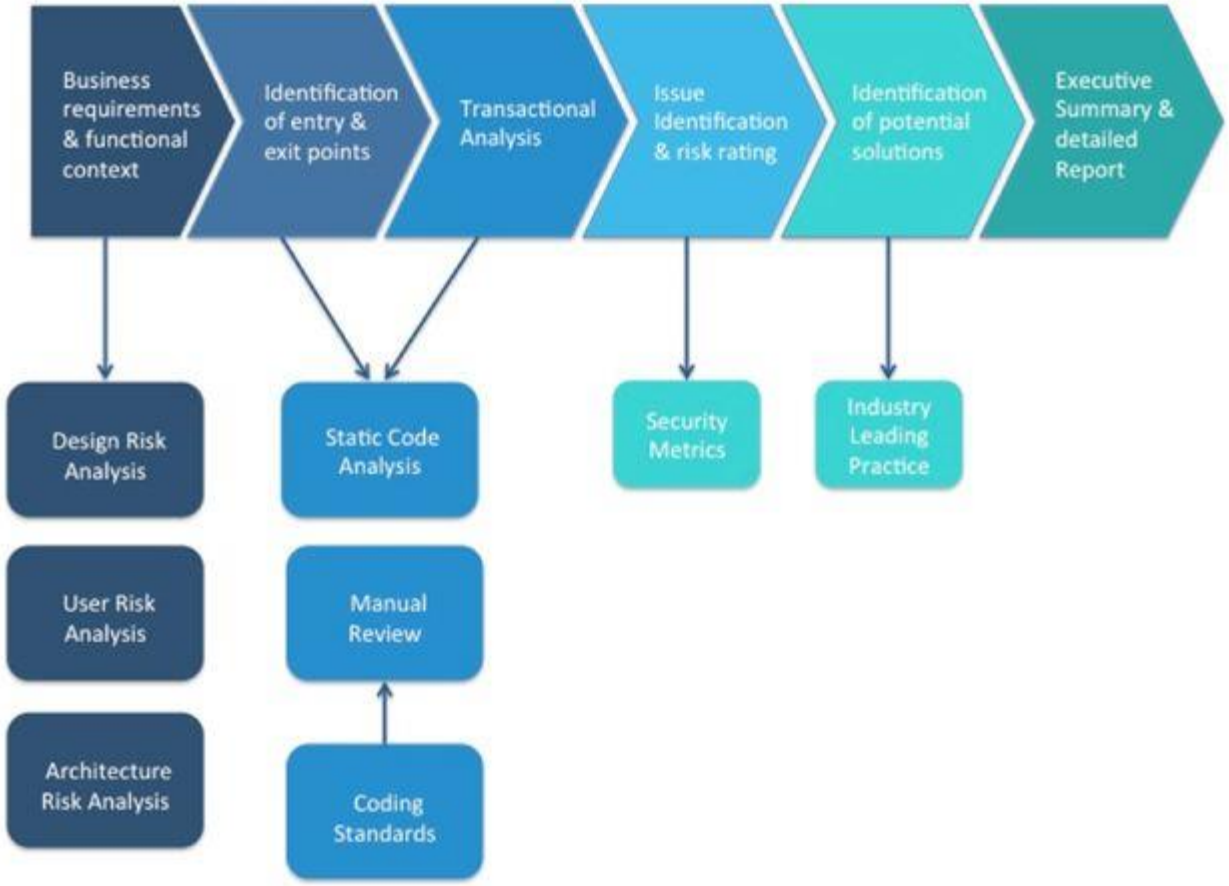
Recursos de OWASP para testing de seguridad

- Guías
  - OWASP Application Security Verification Standard
  - OWASP Web Security Testing Guide
  - OWASP Code Review Guide
- Herramientas

OWASP Testing Project

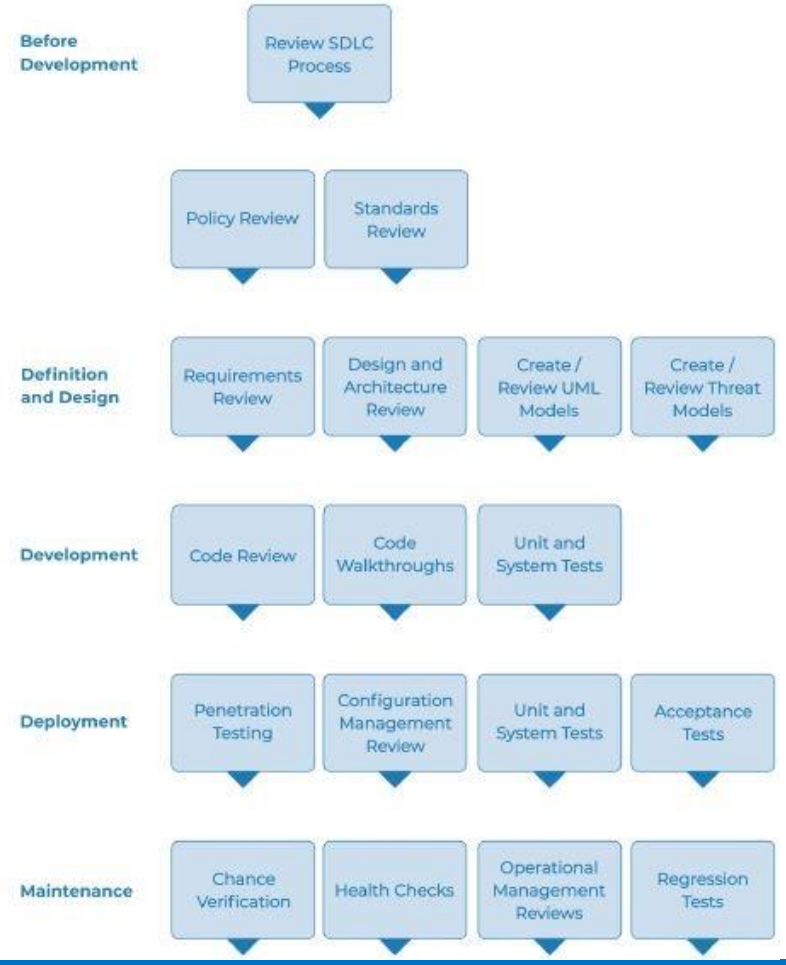
- El proyecto de pruebas OWASP ha estado en desarrollo durante muchos años. El objetivo del proyecto es ayudar a las personas a comprender el qué, por qué, cuándo, dónde y cómo probar aplicaciones web.
- El proyecto ha proporcionado un marco de prueba completo, no simplemente una simple lista de verificación o prescripción de problemas que deben abordarse.

OWASP Code Review Guide



Autor: ccarrenovi@Gmail.com

Testing de seguridad en el ciclo de vida del software

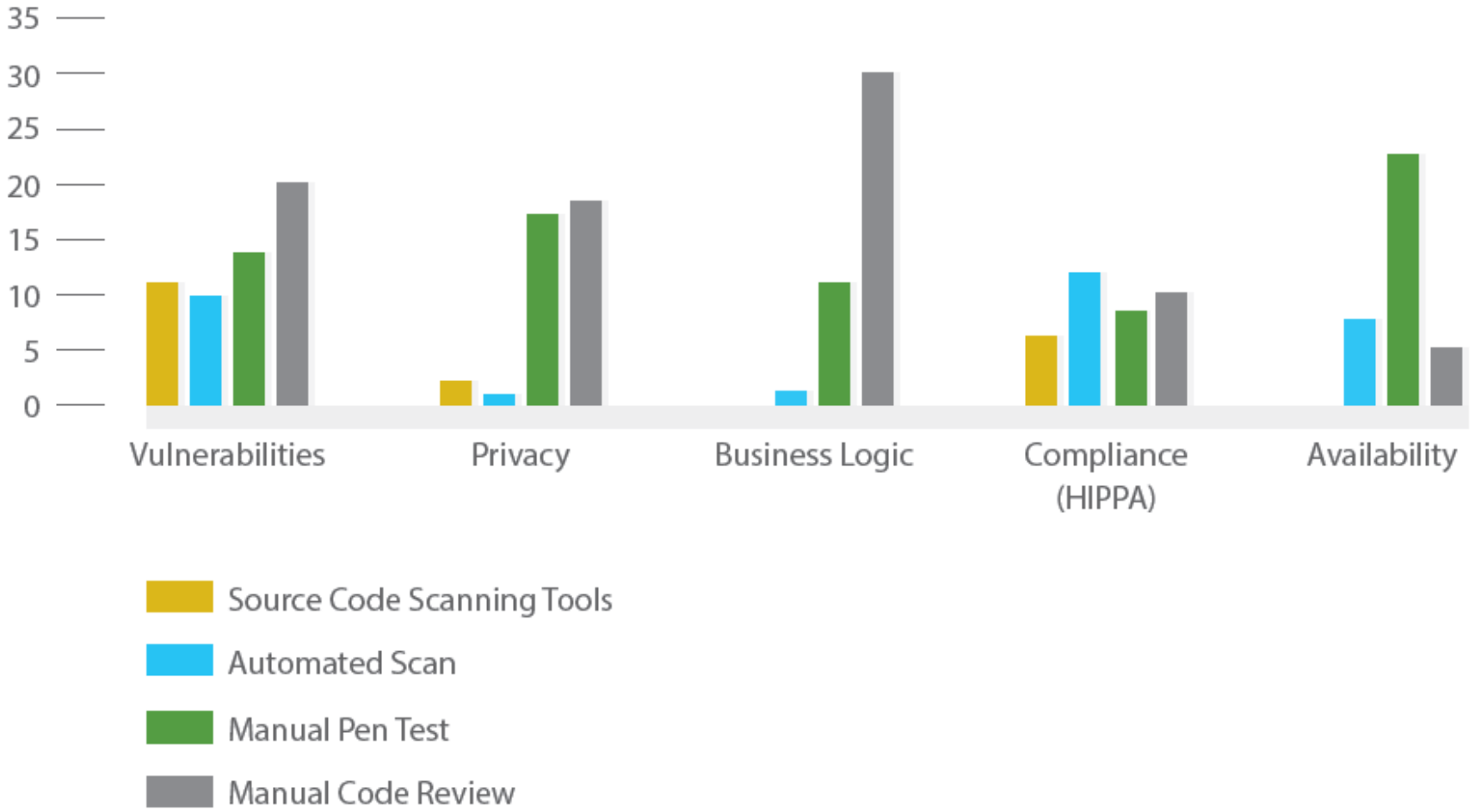


Autor: ccarrenovi@Gmail.com

Escalamiento de privilegios

- La **escalada de privilegios** es el acto de **explotar un error**, un fallo de diseño o una supervisión de la configuración en un sistema operativo o una aplicación de software para obtener un acceso elevado a los recursos que normalmente están protegidos de una aplicación o un usuario.
- El resultado es que una aplicación con más privilegios de los previstos por el desarrollador de la aplicación o el administrador del sistema puede realizar acciones no autorizadas.
- Consiste en **aprovechar vulnerabilidades** del sistema como archivos o servicios mal configurados para poder ejecutar scripts o exploits con privilegios de superusuario.

Métodos para Detectar Vulnerabilidades



Autor: ccarrenovi@Gmail.com

Herramientas de testing de seguridad

- **Burp**

  Burp Proxy es un servidor proxy de interceptación para pruebas de seguridad de aplicaciones web que permite Interceptar y modificar todo el tráfico HTTP (S) que pasa en ambas direcciones, puede trabajar con certificados SSL personalizados y clientes sin reconocimiento de proxy.

- **Dirbuster**

  DirBuster es una aplicación Java de subprocesos múltiples diseñada para forzar los nombres de archivos y directorios en servidores web / de aplicaciones.

- **Nikto**

  Nikto es una escaner de vulnerabilidades Open Source o de fuente abierta, el cual está escrito en el lenguaje Perl, siendo originalmente publicado en el año 2011.

- **W3af**

  w3af es un marco de auditoría y ataque de aplicaciones web. El objetivo del proyecto es crear un marco que lo ayude a proteger sus aplicaciones web mediante la búsqueda y explotación de todas las vulnerabilidades de las aplicaciones web.

- **Nessus**

  Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos.

Denial of Service

- Ataque de denegación de servicio o ataque DoS
- Un atacante intenta evitar que usuarios legítimos acceder a la aplicación, servidor o red
- Consume ancho de banda de red, sockets de servidor, subprocesos, o recursos de CPU
- Ataque distribuido de denegación de servicio o DDoS
- Técnicas populares utilizadas por hacktivistas

- ¡Los ataques DoS de capa 7 más recientes son más poderosos!
  - "DoS de capa de aplicación de ancho de banda bajo“
- Ventajas de la capa 7 DoS
  - Conexiones TCP / UDP legítimas, difíciles de diferenciar tráfico normal
  - Requiere menor número de conexiones, posibilidad de detener una web servidor de un solo ataque
  - Alcance los límites de recursos de los servicios, independientemente del hardware capacidades del servidor

...

- Los Métodos de 7 capas de ataque de DoS
  - HTTP Slow Headers
  - HTTP Slow POST
  - HTTP Slow Reading
  - Apache Range Header
  - SSL/TLS Renegotiation
  - XML Bombs

Broken Authentication

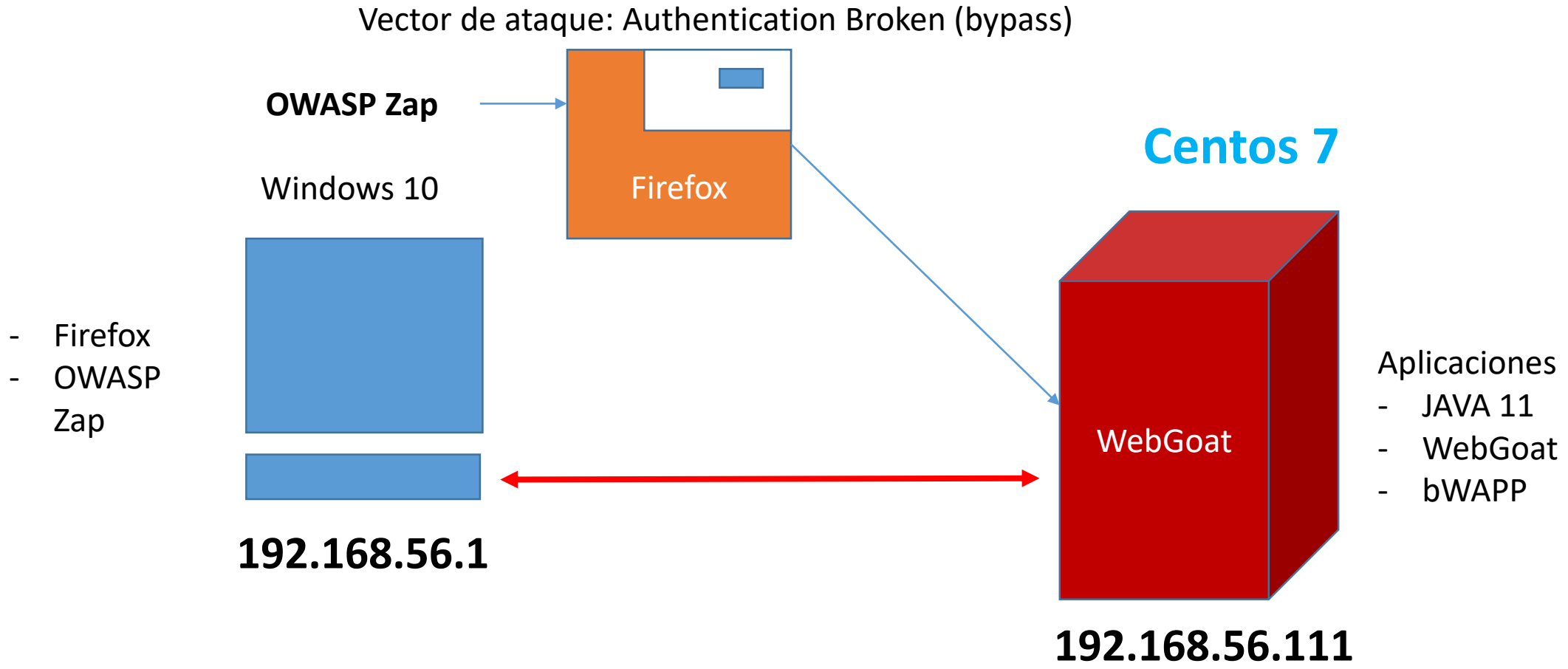
La confirmación de la identidad, la autenticación y la gestión de sesiones del usuario son fundamentales para proteger contra los ataques relacionados con la autenticación. Puede haber debilidades de autenticación si la aplicación:

- Permite ataques automatizados como el relleno de credenciales, donde el atacante tiene una lista de nombres de usuario y contraseñas válidos.
- Permite la fuerza bruta u otros ataques automatizados.
- Permite contraseñas predeterminadas, débiles o conocidas, como "Password1" o "admin / admin".

Lab

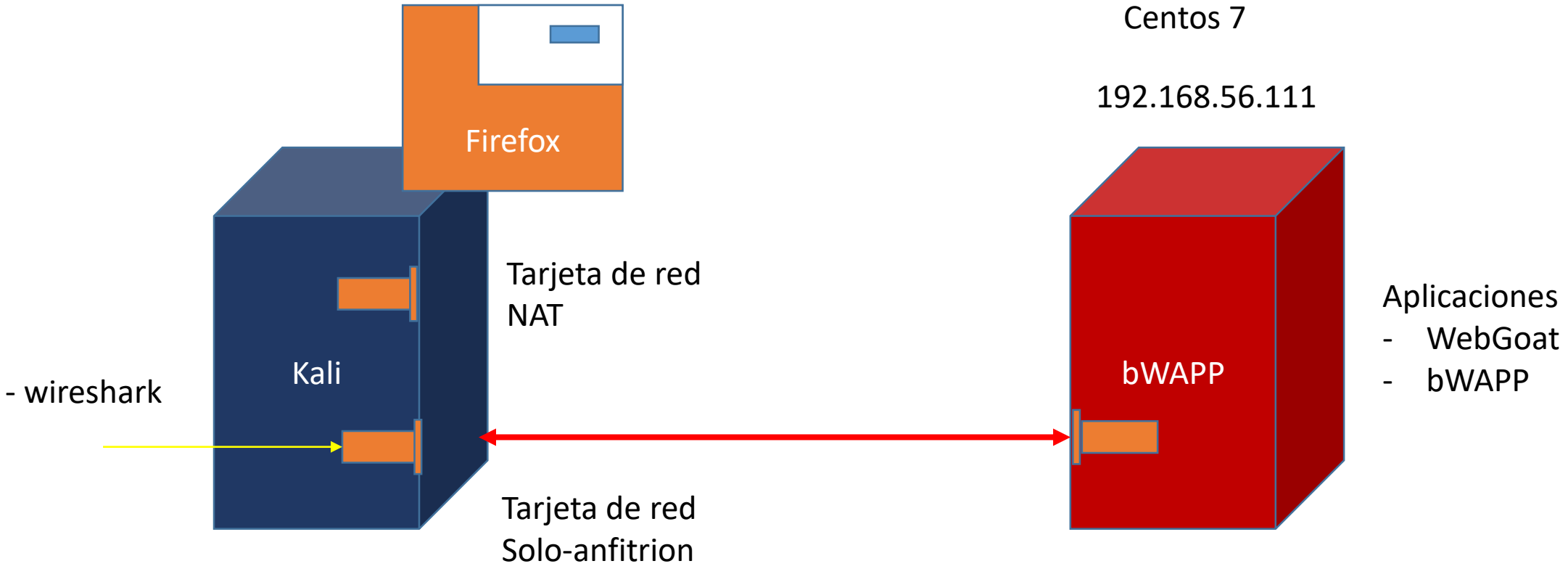
- Realizar el lab de Broken Authentication en **WebGoat**

Escenario Lab 4



Autor: ccarrenovi@Gmail.com

Escenario Lab 5



Autor: ccarrenovi@Gmail.com