OWASP

Venezuela Chapter

Todos Somos parte de la seguridad en el Desarrollo de Software...

Acerca de mí

- Especialista en Seguridad de la Información
- IBM ACE/ACSE y Oracle SCSAS - SCSECA
- Pentester de Aplicaciones Web & Móvil
- Líder OWASP Capítulo Venezuela

Todos Somos parte de la seguridad en el Desarrollo de Software...

Seguridad de la Información

- Ausencia de políticas de Seguridad en el Desarrollo de Software.
- Falta de estrategias y métricas que involucren a la dirección global y areas involucradas en el programa de aseguramiento de software y métricas acerca de la postura de seguridad de la organización.

Gestión y planificación de Proyectos

- Los responsables de proyectos creen que la seguridad no aporta ningùn valor.
- La seguridad no es concebida como un proceso.
- Las organizaciones suelen premiar tiempos de entregas, usabilidad y eventualmente performance... NO Seguridad.

Diseño y Desarrollo

- Inexistencia de un plan para incrementar el conocimiento de seguridad entre el personal de desarrollo de software a través de entrenamientos y orientación en temas de seguridad pertinentes a funciones del trabajo individual.
- Los usuarios finales en general, no suelen demandar software inseguro.
- Ausencia de Proceso de SDLC.
- Poco espacio en el tiempo para atender vulnerabilidades, púes siempre estan desarrollando...

Desarrolladores

- Diseño orientado a funcionabilidad.
- Desarrolladores sin entrenamiento en seguridad.
- Pobre conocimiento de amenazas.
- Ausencia de políticas de codificación segura.
- No emplean APIs de Seguridad.

DBA

- Privilegios de usuarios de aplicaciones no muy bien definidos.
- Ausencia de uso de técnicas de cifrado.
- Inexistencia de mecanismo de vistas para ocultamiento de tablas y columnas.
- Irregularidades al realizar copias de seguridad.

Sysadmin

- Utilización de contraseñas debiles.
- Ausencia de mecanismos de Hardening.
- Pobre gestión de parches de seguridad.
- Excepciones de seguridad injustificadas.

Esp. Seguridad Informática

- No aplica requisitos de seguridad en los procesos de desarrollo.
- No emplea un modelado de amenazas para determinar puntos críticos.
- Inexistencia del proceso de revisión de código fuente.
- Pruebas de seguridad no soportadas por ninguna metodología o buena practica.

Todos Somos parte de la seguridad en el Desarrollo de Software...

P

E

O

Problemas

En la

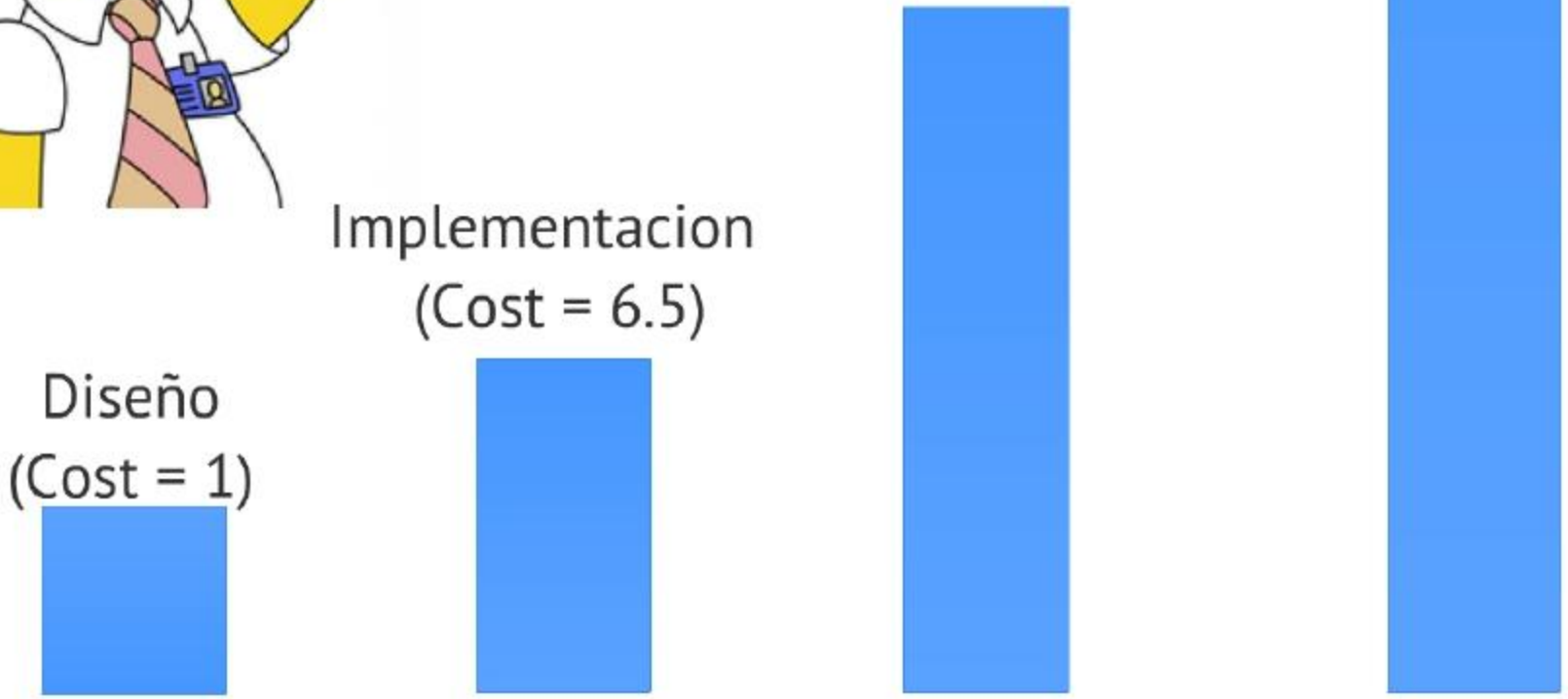
Organización

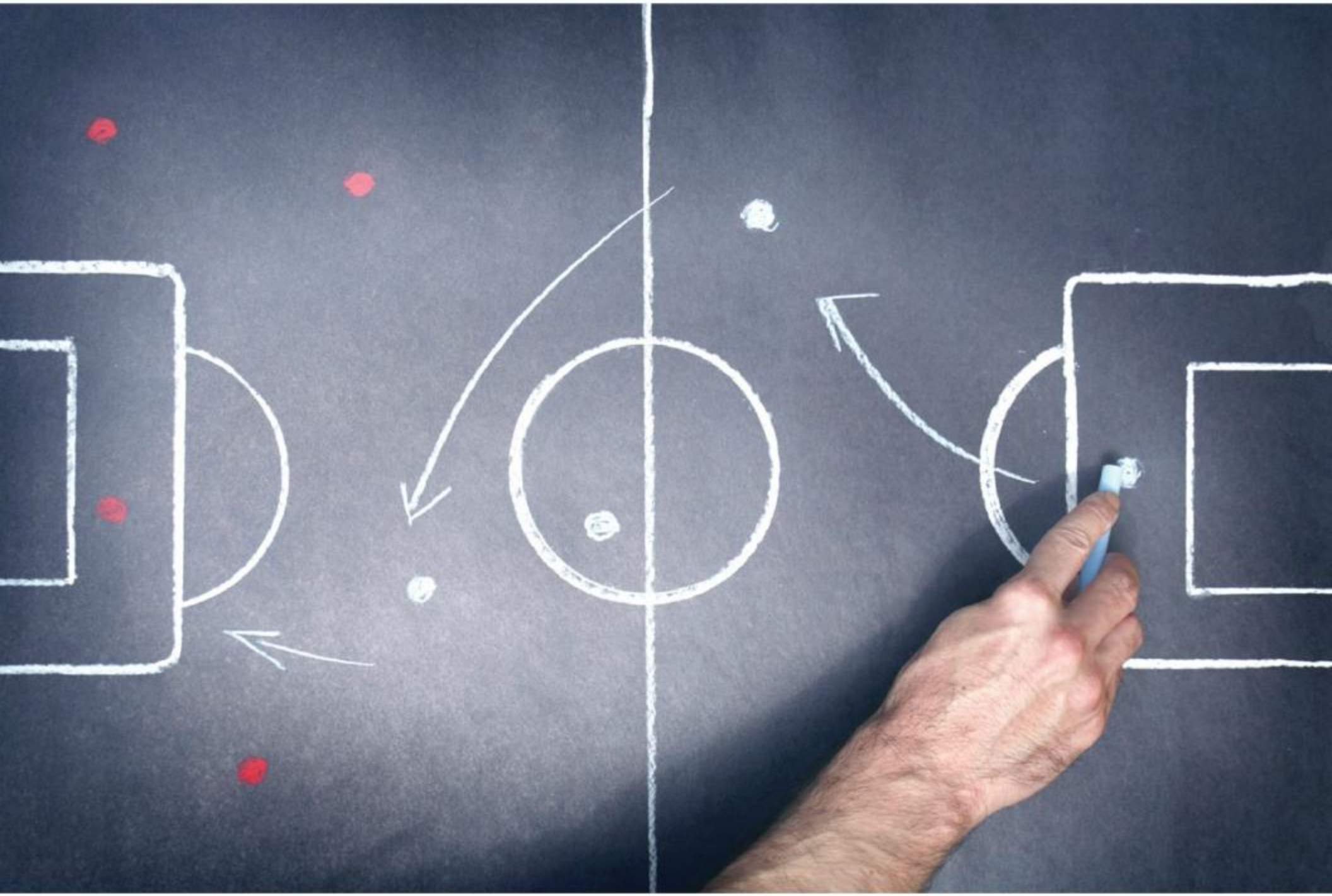
Y todos estos problemas no los llevamos a donde....

80% de las Aplicaciones que salen a producción, Son vulnerables.

XSS representa el 53% entre las vulnerabilidades mas comunes segun **OWASP TOP 10**.

Coste de corrección de Vulnerabilidades





Desarrolladores

Diseño y Desarrollo

DBA

Gestión y planificación de Proyectos

Sysadmin

- Establecer segregacion de ambientes (Desarrollo, Calidad y Produccion).
- El Hardening debe ser obligatorio.
- Mecanismo de gestión de parches de seguridad.
- Excepciones de seguridad deben ser justificadas y llevadas a comite de riesgos tecnologicos

Seguridad de la Información

- La direccion Seguridad de la Informacion debesa de establecer políticas de Seguridad en los procesos de Desarrollo de Software.
- Cumplimiento: Establecer una estructura de control y auditoria para asegurar el cumplimiento de regulaciones y alcanzar niveles óptimos en el aseguramiento de software bajo construcción y en operación.
- Involucrar a la dirección global y a las areas de Desarrollo para establecer un modelo de madurez en la construccion del Software seguro.

Esp. Seguridad Informática

- Aplicar requisitos de seguridad en los procesos de desarrollo.
- Realizar modelados de amenazas segun los criterios propios de cada aplicacion.
- La revisión de código fuente debe ser un proceso constante, bien sea manual y/o automatizado.
- Las pruebas de seguridad deben llevarse de la mano bajo una metodología que permita calificar la evaluacion, ejmp: Owasp Testing Guide.

Todos Somos parte de la seguridad en el Desarrollo de Software...

Seguridad de la Información

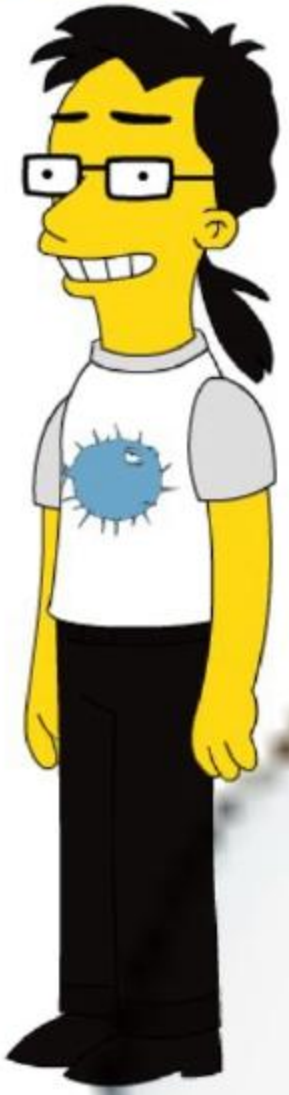
- La direccion Seguridad de la Informacion debera de establecer políticas de Seguridad en los procesos de Desarrollo de Software.
- Cumplimiento: Establecer una estructura de control y auditoria para asegurar el cumplimiento de regulaciones y alcanzar niveles óptimos en el aseguramiento de software bajo construcción y en operación.
- Involucrar a la dirección global y a las areas de Desarrollo para establecer un modelo de madurez en la construccion del Software seguro.

Gestión y planificación de Proyectos

- Establecer la seguridad como un proceso continuo en la vida del desarrollo de software.
- Establecer dentro de la planificacion actividades que permitan el testeo de las mismas.
- La seguridad tambien debe ser premiada, gracias a ello se logran reducir en una gran cantidad el fraude o daño a la imagen de la organizacion.

Diseño y Desarrollo

- Solicitar a las areas pertinente o empresas especializadas, la asesoria y adiestramiento en Desarrollo Seguro.
- Si hay Ausencia del Proceso de SDLC, tendran que crearlo e involucrar las actividades de seguridad en cada uno de los ciclos.
- Establecer un esquema de trabajo para mitigar las vulnerabilidades que se encuentren en la fase de testing y/o produccion segun sea el caso.
- Los Usuarios van a demandar Software Inseguro



Desarrolladores

- Diseño orientado a funcionabilidad Y seguridad.
- Tendran que ser intruidos en el uso de cotramedidas para remediar software inseguro.
- Su guia sera las políticas de codificación segura.
- Tendran que usar APIs de Seguridad y bibliotecas de codigo seguro.

DBA

- Definir un esquema para el otorgamiento de privilegios a usuarios de aplicaciones
- Utilizar buenas practicas en las técnicas de cifrado.
- Establecer mecanismo de vistas para ocultamiento de tablas y columnas segun especificaciones de seguridad.
- Planificar la gestion para la realizacion de copias de seguridad.

Sysadmin

- Establecer segregacion de ambientes (Desarrollo, Calidad y Produccion).
- El Hardening debe ser obligatorio.
- Mecanismo de gestión de parches de seguridad.
- Excepciones de seguridad deben ser justificadas y llevadas a comite de riesgos tecnologicos

Esp. Seguridad Informática

- Aplicar requisitos de seguridad en los procesos de desarrollo.
- Realizar modelados de amenazas segun los criterios propios de cada aplicacion.
- La revisión de código fuente debe ser un proceso constante, bien sea manual y/o automatizado.
- Las pruebas de seguridad deben llevarse de la mano bajo una metodologia que permita calificar la evaluacion, ejmp: Owasp Testing Guide.

Desarrolladores

Diseño y Desarrollo

DBA

Gestión y planificación de Proyectos

Sysadmin

- Establecer segregacion de ambientes (Desarrollo, Calidad y Produccion).
- El Hardening debe ser obligatorio.
- Mecanismo de gestión de parches de seguridad.
- Excepciones de seguridad deben ser justificadas y llevadas a comite de riesgos tecnologicos

Seguridad de la Información

- La direccion Seguridad de la Informacion debesa de establecer políticas de Seguridad en los procesos de Desarrollo de Software.
- Cumplimiento: Establecer una estructura de control y auditoria para asegurar el cumplimiento de regulaciones y alcanzar niveles óptimos en el aseguramiento de software bajo construcción y en operación.
- Involucrar a la dirección global y a las areas de Desarrollo para establecer un modelo de madurez en la construccion del Software seguro.

Esp. Seguridad Informática

- Aplicar requisitos de seguridad en los procesos de desarrollo.
- Realizar modelados de amenazas segun los criterios propios de cada aplicacion.
- La revisión de código fuente debe ser un proceso constante, bien sea manual y/o automatizado.
- Las pruebas de seguridad deben llevarse de la mano bajo una metodología que permita calificar la evaluacion, ejmp: Owasp Testing Guide.

Todos Somos parte de la seguridad en el Desarrollo de Software...


YouTube

Preguntas?

@3ddavid

http://www.3ddavid.net

eddavid01@gmail.com

edgar.salazar@owasp.org