Auditoría Técnica de Seguridad de Aplicaciones Web

Estudiante: Isaac Peña Torres
Consultor: Rafael Estevan de Quesada
Profesor responsable de la asignatura: Carles Garrigues Olivella
Centro: Universitat Oberta de Catalunya

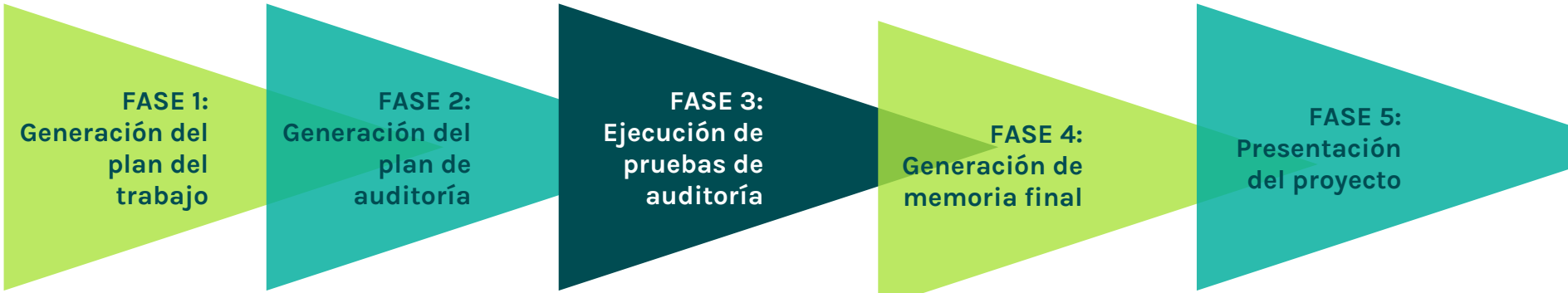
Contexto y justificación

- Casi 3.500 millones de usuarios en Internet
- Generan gran cantidad de información
- Más de 1.000 millones de web online
- Tendencia de presentar la información usando webs
- Compromiso de la información: pérdidas económicas, de imagen, de confianza.
- Es necesario entender los principales riesgos a los que está expuesta la información
- Realizar auditorías periódicas para comprobar los controles implementados para proteger la información

Objetivos

- Desarrollar un **procedimiento de auditoría web**
- Generación de **documentación** para ofrecer un servicio de auditoría
- **Identificar y conocer los principales riesgos** presentes en las aplicaciones web
- Identificar y saber utilizar las principales **técnicas y herramientas para detectar problemas de seguridad** en el entorno web
- **Analizar la información resultante** de las pruebas realizadas
- **Presentación** de la información

Enfoque y método seguido

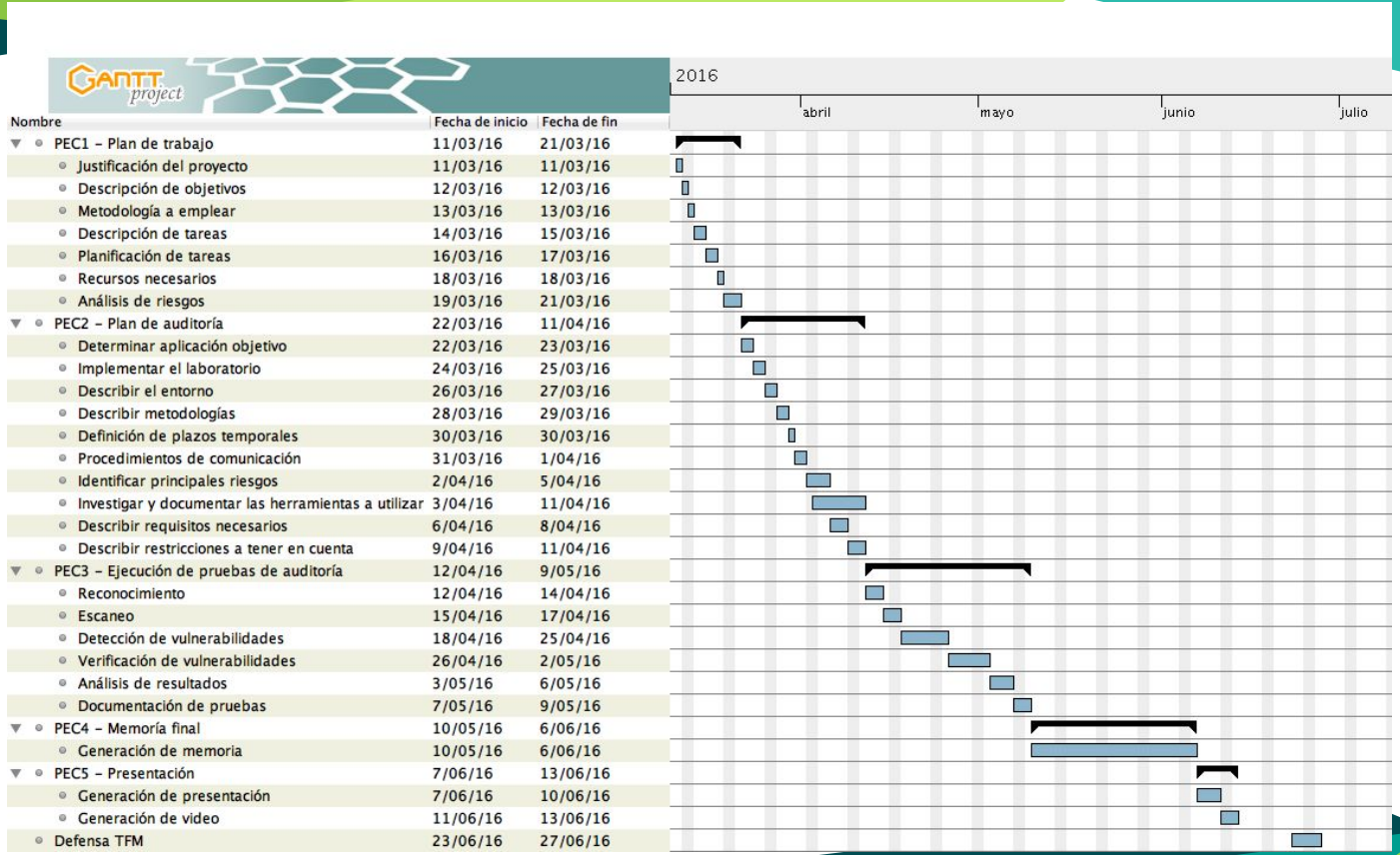


Enfoque y método seguido

Documentación de referencia:

- OWASP Testing Guide v4
- OWASP Top Ten 2013
- Open Source Security Testing Methodology Manual (OSSTMM v3)
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Planificación en tiempo



Nombre	Fecha de inicio	Fecha de fin
PEC1 – Plan de trabajo	11/03/16	21/03/16
Justificación del proyecto	11/03/16	11/03/16
Descripción de objetivos	12/03/16	12/03/16
Metodología a emplear	13/03/16	13/03/16
Descripción de tareas	14/03/16	15/03/16
Planificación de tareas	16/03/16	17/03/16
Recursos necesarios	18/03/16	18/03/16
Análisis de riesgos	19/03/16	21/03/16
PEC2 – Plan de auditoría	22/03/16	11/04/16
Determinar aplicación objetivo	22/03/16	23/03/16
Implementar el laboratorio	24/03/16	25/03/16
Describir el entorno	26/03/16	27/03/16
Describir metodologías	28/03/16	29/03/16
Definición de plazos temporales	30/03/16	30/03/16
Procedimientos de comunicación	31/03/16	1/04/16
Identificar principales riesgos	2/04/16	5/04/16
Investigar y documentar las herramientas a utilizar	3/04/16	11/04/16
Describir requisitos necesarios	6/04/16	8/04/16
Describir restricciones a tener en cuenta	9/04/16	11/04/16
PEC3 – Ejecución de pruebas de auditoría	12/04/16	9/05/16
Reconocimiento	12/04/16	14/04/16
Escaneo	15/04/16	17/04/16
Detección de vulnerabilidades	18/04/16	25/04/16
Verificación de vulnerabilidades	26/04/16	2/05/16
Análisis de resultados	3/05/16	6/05/16
Documentación de pruebas	7/05/16	9/05/16
PEC4 – Memoría final	10/05/16	6/06/16
Generación de memoria	10/05/16	6/06/16
PEC5 – Presentación	7/06/16	13/06/16
Generación de presentación	7/06/16	10/06/16
Generación de video	11/06/16	13/06/16
Defensa TFM	23/06/16	27/06/16

Presupuesto del proyecto

Fase	Tarea	Cantidad	Precio	Total
Fase 1 - Plan de trabajo	1.1 Documento de planificación de tareas	24	25	600
Fase 2 - Plan de auditoría	2.1 Implementación de laboratorio	8	25	200
	2.2 Identificar principales riesgos	16	25	400
	2.3 Investigar herramientas a utilizar	24	25	600
	2.4 Generación del Plan de Auditoría	24	25	600
Fase 3 – Ejecución de pruebas	3.1 Reconocimiento	2	25	50
	3.2 Escaneo	2	25	50
	3.3 Detección de vulnerabilidades	32	25	800
	3.4 Verificación de vulnerabilidades	32	25	800
	3.5 Análisis de la información	16	25	400
Fase 4 – Memoria final	4.1 Generación de memoria	40	25	1000
Fase 5 – Presentación	5.1 Generación de presentación	16	25	400
	5.2 Generación de video	16	25	400
	Total	**252**		**6300**

Análisis de riesgo

- **Correcta determinación del alcance:** motivaciones del cliente, recursos necesarios.
- **Correcta planificación del esfuerzo y recursos destinados:** limitaciones del entorno, ubicación geográfica, sistemas a auditar, procesos, etc.
- **Correcta selección del equipo auditor:** contar con personal experto en esas tecnologías.

Productos obtenidos

Ejecución de auditoría

Consideraciones:

- Tras entrevistas con el cliente hemos determinado un alcance:
  - Objetivo de la auditoría: página principal de la empresa
  - Análisis de los 10 Riesgos del Top Ten de OWASP 2013
- Se ha enviado el plan de auditoría al cliente
- Tenemos aprobado el plan de auditoría y oferta económica por el cliente
- Tenemos los contactos de la organización por si ocurriera algún problema durante las pruebas
- Comenzamos a ejecutar las pruebas de auditoría

Riesgos a comprobar

- A1 - Inyección
- A2 - Pérdida de autenticación y gestión de sesiones
- A3 - Secuencia de comandos en sitios cruzados (XSS)
- A4 - Referencia directa insegura a objetos
- A5 - Configuración de seguridad incorrecta
- A6 - Exposición de datos sensibles
- A7 - Ausencia de control de acceso a funciones
- A8 - Falsificación de peticiones en sitios cruzados (CSRF)
- A9 - Uso de componentes con vulnerabilidades conocidas
- A10 - Redirecciones y reenvíos no validados

Para revisar estos riesgos se comprueban un total de 49 controles de seguridad

Entorno de laboratorio

- Las pruebas se lanzarán contra la aplicaciones vulnerable Mutillidae 2
- Contiene los 10 riesgos descritos por OWASP en su Top 10 de 2013 y de años anteriores
- Está incluida en el proyecto OWASP Broken Web Application Project (OWASPBWA)
- Se usará la iso del proyecto (ejecutada sobre VirtualBox) que contiene múltiples aplicaciones vulnerables
- Se considerará que la aplicación de la empresa a auditar está bajo el dominio www.shopathome.com.

Resultados

A1 - Inyección

- La página es vulnerable a SQLi permitiendo saltar el control de autenticación y acceder a información interna.
- Es vulnerable a RFI y LFI pudiéndose cargar ficheros remotos y acceder a ficheros locales del sistema.
- Se pueden ejecutar comandos del sistema y mostrar la salida de los comandos en la página web.

A2 - Pérdida de autenticación y gestión de sesiones

- No existe un control en la creación de usuarios.
- Es posible la enumeración de usuarios a través de los mensajes de error de la página de login.
- Se detectan contraseñas por defecto en usuarios de la aplicación.
- No hay implementada una política de contraseñas segura.
- Las cookies pueden viajar en claro por la red.
- La cookie de sesión no se renueva.

Resultados

A3 - Secuencia de comandos en sitios cruzados (XSS)

- Se detectan varias vulnerabilidades XSS que pueden ser utilizadas para comprometer a los usuarios de la página.

A4 - Referencia directa insegura a objetos

- La página es vulnerable a directorio transversal.
- Se permite ver el código fuente de archivos php.

Resultados

A5 - Configuración de seguridad incorrecta

- Se detectan múltiples vulnerabilidades en la arquitectura del sistema.
- Se detectan ficheros con información sensible publicados en la web.
- Se detectan paneles de administración de herramientas de gestión de base de datos publicados.
- Los mensajes de error muestran información que puede ser utilizada para lanzar ataques contra la web.

A6 - Exposición de datos sensibles

- Se detectan vulnerabilidades presentes en los servicios que hacen uso de túneles cifrados.
- La web tiene publicada un fichero que contiene credenciales de usuarios.
- Se detectan credenciales publicadas en los comentarios de la página web.

Resultados

A8 - Falsificación de peticiones en sitios cruzados (CSRF)

- La página es vulnerable a CSRF. Se permite mediante la inyección de código javascript la creación de entradas de forma automática cada vez que un usuario visita la página.

A9 - Uso de componentes con vulnerabilidades conocidas

- El sistema hace uso de multitud de componentes desactualizados y con múltiples vulnerabilidades críticas.

A10 - Redirecciones y reenvíos no validados

- La página se puede utilizar para redirigir a un usuario a sitios maliciosos.

Conclusiones

- En muchos casos es necesario que los **servicios** ofrecidos a los usuarios estén **publicados en redes inseguras** como Internet.
- La **materialización de los riesgos** presentes en las aplicaciones web pueden suponer un **gran impacto** en las organizaciones.
- **Afecta** a la información que manejan, las funcionalidades que ofrecen, la **confianza** que depositan los usuarios, la **imagen** de la organización, y los **ingresos** de las compañías.
- Las **auditorías** deberían de realizarse de forma **periódica**.
- La **seguridad** debe estar **presente en todo el ciclo de desarrollo del software**.
- Y no solo hay que **aplicar medidas** en el plano **técnico**, también a nivel de **procedimientos**, en la forma de hacer las cosas y de manejar la información, y de **personas**, con formación y concienciación.
- Como **líneas de trabajo a futuro** se podría avanzar **automatizando la comprobación de los controles** para reducir el tiempo que el auditor invierte en esta fase.

Gracias!

¿Alguna pregunta?

Puedes encontrarme en @ipenat & isaac.ipt@gmail.com