Seguridad y Calidad en Aplicaciones Web
Trabajo Práctico

Modalidad: Grupal (5 integrantes)
Fecha de entrega: 1 de Julio del 2015, 2200hs.
Fecha de presentación Grupal: 29 de Junio del 2015.

Entregables:

1. Diseño de tablas.
2. Definición de base de datos y set de inicialización.
3. Código fuente y archivos accesorios de la aplicación.
4. Documentación
    1. Documentación de las funcionalidades requeridas en la consigna general; la misma debe estar documentada en formato OpenDocument(ODT) y contener los screenshots de las pantallas en referencia.
    2. Documentación de la ejecución del Scan de vulnerabilidades Vega 1.0 sobre la aplicación, disponible en https://subgraph.com/vega/ . Dicha documentación debe detallar el modo y procedimiento utilizado para la ejecución del scan mas la explicación y justificación de cada problema reportado, junto con el detalle de las buenas practicas y recaudos aplicados en el desarrollo para minimizar los riesgos que forman parte del OWASP Top-Ten.
    3. Detalles y documentación de la verificación de nivel 2 según OWASP ASVS-2014 (ApplicationSecurity Verification Standard), disponible en https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project. Dicho documento debe ser realizado en formato OpenDocument(ODT).
    4. Presentación de la aplicación en formato PDF.

5. Firmas OpenPGP para el paquete de entregables con los puntos 1,2,3 y 4.
6. Claves OpenPGP, accesibles en http://keys.gnupg.net, una por cada integrante del grupo con sus datos de referencia, las mismas serán utilizadas para verificar las firmas. Cada clave deberá estar firmada por el resto de los integrantes del grupo.

Modo de entrega

Se enviará un e-mail a wureta@ing.unlam.edu.ar con dos archivos adjuntos, donde X será reemplazado por el número del grupo correspondiente

A. **Entrega-GrupoX.zip.asc** : Contendrá los entregables correspondientes a los entregables **1,2,3 y 4** comprimidos en formato zip y posteriormente cifrados con modalidad asimétrica; este deberá incluir en los receptores a la clave: 4483AF7A Walter R. Ureta (Seguridad y Calidad en Aplicaciones Web - UNLaM) <wureta@ing.unlam.edu.ar> Fingerprint=8A1B E27D AE74 EACC

222E 34A4 BE05 A6FB 4483 AF7A . Dicha clave sera obtenida desde http://keys.gnupg.net.

B. **Entrega-GrupoX.zip.asc.sig** : Contendrá las firmas de TODOS los integrantes del equipo para el archivo **Entrega-GrupoX.zip.asc** , constituyendo el entregable numero **5**.

El titulo del mail estará compuesto por texto **“SCAW 2015C1 - Practico GrupoX”** (X sera reemplazado por el numero de grupo), mientras que cuerpo de este mail contendrá los datos necesarios para localizar en http://keys.gnupg.net las claves OpenPGP de cada miembro del equipo, esta información constituye el entregable numero **6** .

Consigna General

Se solicita el desarrollo de un sitio web que cumpla con los siguientes requisitos

1. Introducción
    1. Propósito
    Este documento tiene por finalidad definir los requisitos y características del sistema a desarrollar.
    2. Definiciones
    No hay definiciones particulares.
    3. Características de sistema
    El sistema permitirá a sus usuarios compartir documentos, permitiendo tanto el acceso publico, como a otros usuarios específicos.
    4. Referencias
    No hay otros documentos asociados.

2. Descripción general
    1. Perspectiva del producto
    El producto no estará integrado con otros sistemas de la empresa ni con sistemas externos.
    2. Funciones del producto
    Se espera que el desarrollo permita distribuir archivos con acceso publico o restringido a usuarios particulares. Estos archivos podrán ser de cualquier formato y se llevara registro histórico de los mismos. Adicionalmente se podrá dejar comentarios que se mostrarán al público.
    3. Características del usuario
    Todos los usuarios de la aplicación observarán los archivos que han compartido y aquellos a los que otros usuarios les han otorgado acceso.
    Los usuarios públicos de la aplicación podrán ingresar mensajes anónimos en la aplicación. Solo los usuarios registrados podrán compartir archivos; adicionalmente podrán ingresar comentarios en el sistema que serán asociados a su identificación.
    4. Dependencias y supuestos

No hay dependencias externas; se espera una implementación basada en las buenas prácticas de seguridad para el desarrollo en aplicaciones web.

5. Restricciones

El software desarrollado debe ajustarse a las siguiente plataformas, productos y lenguajes:

- Lenguaje de programación PHP
- Entorno de ejecución XAMPP/LAMPP (Apache, Php, MySQL)
- Base de datos MySQL
- Compatibilidad con Firefox

3. Requisitos específicos

1. Requisitos de la interfaz externa

El sistema debe tener una única interfaz web conforme a los estándares de HTML 4.01.

2. Requisitos funcionales

a. Los usuarios anónimos podrán acceder a archivos públicos mediante una dirección que referencia a cada archivo.
b. Cada archivo podrá contener comentarios
c. Los comentarios se podrán realizar de forma anónima.
d. Los comentarios de usuarios registrados serán asociados a su perfil.
e. El sistema deberá desplegar los comentarios publicados.
f. Existirán dos roles generales: administrador y usuario.
g. Todos los usuarios registrados pueden compartir archivos
h. Un archivo puede ser compartido como publico o privado
i. Los archivos compartidos como 'privados' deben tener una lista de usuarios con permiso de acceso, cada uno tendrá un sub-rol que limitara su acceso ya sea 'Editor' o 'Lector'
j. Los archivos compartidos como públicos son de solo lectura excepto para el usuario que lo comparte, quienes tengan sub-rol de 'Editor' para el mismo y los administradores.
k. Los usuarios podrán ver las versiones históricas de cada archivo compartido, y aquellos con rol de 'Editor' podrán restaurar versiones anteriores.
l. Los usuarios que no estén registrados no podrán acceder a las versiones históricas del archivo.
m. Los usuarios con rol de administrador puede editar todos los archivos compartidos.
n. El sistema debe contener un panel de administración para el manejo de usuarios; permitiendo altas, bajas y modificaciones.
o. El panel de administración también debe permitir acceder a un listado de los archivos compartidos.
p. El sistema debe asignar una cuota de espacio a cada usuario y notificar sobre el espacio utilizado y disponible.
q. La cuota de espacio debe ser configurable para los administradores

3. Requisitos de desempeño
No hay requisitos adicionales.
4. Condiciones de diseño
El sistema no puede contener contenido de audio, video o tecnologías embebidas (Flash, Activex, Java Applets)
5. Requisitos lógico de la base de datos
No hay requisitos adicionales.
6. Atributos del sistema de Software
No hay requisitos adicionales.
7. Otros requisitos
No hay requisitos adicionales.

Grupos de Trabajo

Grupo 1
- ALANIZ ESTEBAN
- CIERI SALCEDO NICOLAS
- RODRIGUEZ ROXANA STEPHANIE
- SALAZAR MELISA AILEN
- YUCRA RODRIGO

Grupo 2
- CONTI RICARDO
- FERNANDEZ JONATHAN
- KLODI SILVIA
- SARDI FEDERICO
- VEGA LUCAS

Grupo 3
- HERRERA FERNANDO
- LAMILLA BRIAN
- PEZZUTTI FERNANDA
- PRIETO PAULA
- RAMON JULIETA

Grupo 4
- AMAYA MATIAS
- GATICA KARINA
- METALLO MARTIN
- PERINO JULIAN
- TULA MARIA LAURA

Grupo 5
- CORONEL PABLO
- MONTELEONE ANA
- PEREZ FEDERICO
- PEREZ GRACIANO WALTHER

Grupo 6
- CHAZARRETA DIEGO
- GIMENEZ PABLO
- TOBARES PAULA
- TOCCI NATALIA

Grupo 7
- BLANCO FAZANES LUCAS
- SCALZOTTO MARCOS
- VELASCO ROMINA GISELLE
- VIVONA ALAN