Universidad de Costa Rica
Seguridad de Sistemas Computacionales
CI0143 - I Semestre 2022

Desarrollo (Parte I), Seguridad (Parte II) y Pruebas de Seguridad (Parte III) de una Aplicación Web
Fecha entrega: 17 de mayo 2022

Prof. Ricardo Villalón Fonseca

1. Objetivo General

Desarrollar (Parte I) una aplicación web simple en versión inicial, sin controles exhaustivos de seguridad, para ser mejorada y evaluada en una etapa posterior.

2. Objetivos Específicos

1. Implementar una aplicación web con las características, herramientas y lenguajes definidos en este enunciado.
2. Instalar la aplicación en un servidor de pruebas, para ser evaluada y mejorada en su seguridad en una etapa posterior.

3. Descripción General

Esta tarea consiste en desarrollar una aplicación web simple, que será evaluada desde la perspectiva de seguridad. Para desarrollarla, usted debe usar las funciones básicas provistas por los lenguajes y entornos de programación indicados más adelante, es decir, no debe usar frameworks, bibliotecas o herramientas de software adicionales que incluyan o generen código para acelerar el proceso de desarrollo. Por esta misma razón, no se espera que su aplicación tenga una interfaz de alta calidad, sino más bien se espera que sea simple, pero organizada.

4. Herramientas de hardware y software

A continuación se listan las herramientas de software a ser usadas para implementar la aplicación:

1. Servidor web: Apache.
2. Plataforma/lenguaje de desarrollo: CGI con lenguaje C o C++.

3. Servidor de base de datos: MySQL (MariaDB).

El computador donde se ejecutará su aplicación es un equipo con arquitectura Intel de 64 bits y con sistema operativo Linux.

5. Características de la aplicación web

El sistema a desarrollar permite colocar artículos para su venta por Internet a usuarios registrados. Los artículos puestos en venta pueden ser adquiridos por usuarios registrados en el sistema, aunque el acceso a las páginas con la información de los artículos en venta debe estar disponible para todo público. Antes de iniciar con el proyecto seleccione una temática para los artículos a ofrecer en el sitio, así como detalles organizacionales y técnicos (por ejemplo, dominio DNS) para el sitio web a ser implementado.

5.1. Base de datos

La base de datos del sistema debe ser diseñada según los requerimientos indicados más adelante en este enunciado.

5.2. Usuario visitante

Las funciones disponibles para un usuario no registrado son:

1. Página de registro: debe solicitar al menos el nombre completo, usuario, email, teléfono, dirección, así como otros datos que considere pertinentes.
2. Consultar productos para la venta en el sitio, incluya alguna funcionalidad básica de búsqueda.
3. Formulario de consultas, retroalimentación o reclamos del sitio web.

5.3. Usuario registrado

Las funciones disponibles para un usuario registrado son:

1. Ingresar al sistema proporcionando alguna identificación.
2. Agregar información de un artículo para ponerlo en venta.
3. Agregar un artículo al carrito de compras.
4. Concretar/finalizar el proceso de compra/entrega por medio de una tarjeta de crédito.
5. Salir del sistema.

6. Consideraciones para el desarrollo de la aplicación web

Usted debe desarrollar la aplicación usando el estándar CGI, por medio de los lenguajes C o C++. Puede usar las bibliotecas básicas disponibles en dichos lenguajes para acceder a la base de datos MySQL, pero no puede usar frameworks o bibliotecas adicionales que realicen las operaciones o funciones propias del estándar CGI. Como excepción al uso de blibliotecas de terceros, puede usar blibliotecas en JavaScript y facilidades en el lenguaje de estilos CSS, para mejorar la apariencia gráfica de su aplicación, si lo desea.

Cualquier consideración funcional debe resolverla de forma directa usando las capacidades del protocolo CGI, sin bibliotecas de apoyo, solamente usando la funcionalidad de las funciones para acceso a la base de datos y otras de biblioteca estándar del lenguaje, sin incorporar bibliotecas o elementos que implementen funciones de red.

Detalles del proceso de cobro con tarjeta de crédito así como otros aspectos técnicos y de seguridad en general serán definidos durante el tiempo de clases.

7. Reporte del laboratorio

Usted debe generar la documentación de diseño e implementación que sea pertinente (por ejemplo, la arquitectura de la aplicación) y las indicaciones apropiadas para la instalación de la aplicación en un servidor de pruebas.