Universidad Fidélitas



Ingeniería en Sistemas de Computación

Análisis y Mejoras en la Gestión de Sesiones y Seguridad en Aplicaciones PHP y SEO

Alumnos:

Anchía Rodríguez Jonathan

Castro Hernández Luis Carlos

Jiménez Carvajal Keylor

Kim Rodríguez Hyun Jin

SC-502 Ambiente web cliente/servidor

San José, Costa Rica

Agosto de 2023

Primeramente en la investigación se abarcarán conceptos teóricos de la seguridad de aplicaciones y gestión de la misma, así como el manejo de sesiones en PHP y su importancia en el desarrollo del proyecto y su implementación como buenas prácticas de seguridad e integralidad de datos.

Protocolo HTTP y Limitaciones: El protocolo HTTP, aunque es fundamental para la comunicación en la web, presenta limitaciones en la persistencia de datos entre solicitudes. Esta limitación da lugar a la necesidad de sesiones para mantener la coherencia de la experiencia del usuario. (Palomo, 2023)

Sesiones: Las sesiones, en el contexto de aplicaciones web o de cliente-servidor, son una herramienta esencial para mantener la conexión entre el cliente y el servidor a lo largo de múltiples solicitudes. El uso de identificadores únicos (session\_id) y el almacenamiento de datos en el lado del servidor permiten mantener la continuidad de la interacción bajo un mismo usuario. (Palomo, 2023)

Manejo de Sesiones en PHP: PHP tiene una función "session\_start()" para iniciar las sesiones y la variable global "$\_SESSION" para almacenar los datos específicos de la sesión. El uso de cookies o implementación del mismo comúnmente utilizado para mantener la identificación entre las solicitudes. (Palomo, 2023)

**Seguridad en Aplicaciones Web**

La seguridad en aplicaciones web es un componente crítico en el desarrollo de Software sobre todo con un enfoque cliente-servidor.

Evaluación de la seguridad: Las vulnerabilidades potenciales que se pueden presentar aplicaciones tipo cliente-servidor deben evaluarse minuciosamente, incluyendo posibles inyecciones, ataques de robo de sesiones y entre otros. (Palomo, 2023)

Eficiencia y Escalabilidad: Además de la seguridad, se debe evaluar cómo el no tener mecanismos de seguridad adecuados afecta la eficiencia y la escalabilidad del sistema, considerando el uso eficiente de recursos y la capacidad de manejar múltiples sesiones simultáneas. (Palomo, 2023)

**Herramientas y mejoras en seguridad existentes**

Autenticación y Autorización: Las mejoras más populares del mercado incluyen la implementación de autenticación de dos factores (2FA) para elevar la seguridad de las cuentas de usuario y la asignación de roles de usuario para controlar el acceso a diferentes niveles de funcionalidad.

Protección contra Ataques: Hoy en día en el desarrollo de Software se propone una estrategia integral para prevenir ataques de inyección, incluyendo la validación y el saneamiento de entradas de usuario.

Manejo de Sesiones: Para mejorar la gestión de sesiones, se suele hacer uso de tokens CSRF (Cross-Site Request Forgery) y la implementación de expiración de sesiones para prevenir ataques de robo de sesiones. (Palomo, 2023)

Seguimiento y Registro: Es de suma importancia y necesidad la implementación de un sistema de registro y seguimiento de actividades como medida para detectar posibles amenazas y ataques y poner tomar medidas de contingencia contra los mismos.

Importancia y Relevancia

Se destaca la importancia crítica de abordar la gestión de sesiones y la seguridad en aplicaciones PHP, subrayando los beneficios tanto para el desarrollo de la aplicación del proyecto del salón de belleza.

La investigación realizada plantea que en el futuro, se sugiere explorar áreas adicionales de investigación, como la implementación de autenticación de dos factores más avanzada y la exploración de marcos de seguridad más robustos.

**Aplicación de los Conceptos de OWASP al Proyecto de Salón de Belleza y Manicura en PHP:**

En el contexto del proyecto de salón de belleza y manicura en PHP, se aplicaron algunos de los principios de seguridad de OWASP:

Inyección: Se realizaron procedimientos almacenados para prevenir inyecciones SQL, garantizando que los datos del usuario no puedan ser interpretados como instrucciones de SQL maliciosas. (OWASP, 2017)

Exposición de Datos Sensibles: Se destaca la aplicación de la encriptación de datos sensibles almacenados en la base de datos, para prevenir cualquier robo de información.

Configuración de Seguridad Incorrecta: Se recomienda mantener al día todas las bibliotecas y componentes, junto con la implementación de políticas de seguridad que podamos considerar en el proyecto adecuadas, para evitar configuraciones incorrectas que puedan ser vulneradas.

Deserialización Insegura: Se resalta la necesidad de implementar deserialización segura y validación adecuada de objetos para prevenir ataques de deserialización insegura, que pueden conducir a ejecución de código no autorizado. (OWASP, 2017)

Componentes con Vulnerabilidades Conocidas: Se recomienda mantener todas las bibliotecas y componentes actualizados para evitar vulnerabilidades conocidas y mitigar posibles vectores de ataque.

**Optimización de Motores de Búsqueda (SEO)**

La optimización de motores de búsqueda (SEO) es una disciplina fundamental para aumentar la visibilidad y el tráfico orgánico de un sitio web en los resultados de búsqueda. En el contexto de un salón de belleza y manicura, la implementación de estrategias de SEO es esencial para atraer clientes potenciales interesados en los servicios ofrecidos. A continuación, se describen los principales componentes de la optimización de motores de búsqueda y cómo se aplican en el contexto de un sitio web para el salón de belleza y manicura. (Rojas, 2021)

Optimización de Contenido: Se crea contenido relevante y valioso para los visitantes del sitio, incluyendo descripciones detalladas de los servicios de belleza y manicura, consejos de cuidado personal y tendencias en la industria. El contenido se organiza en secciones y páginas específicas para facilitar la navegación.

Palabras Clave Relevantes: Se identifican palabras clave relevantes para el negocio, como "salón de belleza", "manicure", "tratamientos", entre otras. Estas palabras clave se integran de manera natural en el contenido del sitio, incluyendo títulos, encabezados y descripciones.

Optimización Técnica: Si bien es cierto no ha sido implementado en el proyecto pero es una estrategia de gestión de recursos y optimización técnica del sitio, incluyendo la optimización de imágenes, la reducción del tiempo de carga de la página, la corrección de enlaces sin sitio. En PHP, se busca optimizar el rendimiento utilizando técnicas como compresión GZIP, compresión de archivos CSS y JavaScript, en el archivo .htaccess o en la configuración del servidor. (Rojas, 2021)

Estrategia de Enlaces: Se implementa una estrategia de enlaces internos y externos para mejorar la navegación y la autoridad del sitio, como redes sociales del propio salón de belleza.

Redes Sociales: Se integran botones de redes sociales para permitir que los visitantes compartan contenido fácilmente. Además, se establecen perfiles en plataformas de redes sociales como Instagram y Facebook para fortalecer la presencia en línea.

**Buscadores y Alta en Sitios Web**

Registro en Motores de Búsqueda: Se recomienda para el proyecto registrar el sitio en motores de búsqueda líderes del mercado como Google, Bing, etc. Esto permite que los motores de búsqueda indexen y muestren el sitio en los resultados de búsqueda relacionados a los temas de salón de belleza.

Google My Business: Esto permitiría que el salón de belleza y manicura se muestre en los resultados locales de búsqueda, con información como dirección, horario de atención y reseñas. (Rojas, 2021)

Los archivos robots.txt son útiles para indicar a los motores de búsqueda qué partes del sitio deben ser indexadas y cuáles no. Además, se recomienda para el futuro del proyecto utilizar un archivo sitemap.xml que sirve para proporcionar un mapa del sitio a los motores de búsqueda.

**Publicidad Web**

Publicidad PPC: Se considera la posibilidad de implementar campañas de publicidad de pago por clic (PPC) en plataformas como Google Ads. Estas campañas permiten mostrar anuncios relevantes a usuarios específicos y aumentar la visibilidad en los resultados de búsqueda. (Rojas, 2021)

Publicidad en Redes Sociales: Se exploran opciones de publicidad en redes sociales como Facebook e Instagram, donde se pueden segmentar audiencias específicas en función de intereses y demografía y como tal también en mercado meta del salón.

**Desarrollo del Sitio**

Implementación del Sitio: El sitio web del salón de belleza y manicura se desarrolla utilizando PHP como lenguaje de programación principal. PHP ofrece flexibilidad y funcionalidad para construir un sitio interactivo y dinámico que permita la realización de citas de una manera más eficiente.

Diseño Responsivo: Se implementa un diseño responsivo que garantiza que el sitio sea apto para dispositivos móviles. Esto implica que el contenido se adapte automáticamente a diferentes tamaños de pantalla, brindando una experiencia óptima tanto en dispositivos móviles como en computadoras de escritorio.

**Consideraciones Técnicas, Operativas y Funcionales a considerar para el desarrollo:**

**Técnicas:**

Velocidad del Sitio: Se busca optimizar las imágenes y la utilización de almacenamiento en caché para garantizar un tiempo de carga rápido.

Seguridad: Se busca implementar medidas de seguridad como el uso de HTTPS para proteger la comunicación entre el usuario y el servidor.

Compatibilidad del Navegador: Se explorará opciones para que el sitio funcione correctamente en una variedad de navegadores web populares.

**Operativas:**

Gestión de Citas: Se implementa un sistema de gestión de citas en línea, donde los clientes pueden seleccionar servicios, fechas y horarios disponibles.

Contacto y Soporte: Se proporciona información de contacto clara y se implementa un sistema de contacto en línea para consultas y preguntas de los clientes.

**Funcionales:**

Galería de Imágenes: Se crea una galería de imágenes que muestra ejemplos de trabajos realizados en el salón de belleza y también de los productos que se ofrecen.

Descripción de Servicios: Se detallan los servicios ofrecidos, sus beneficios y los precios asociados a los servicios.

Reseñas y Testimonios: Es una estrategia potencial y futura que se explorará el incluir reseñas y testimonios de clientes satisfechos para construir la confianza del cliente.

**Implementación propia del proyecto**

Login y manejo de sesión:

<?php

session\_start();

if (isset($\_SESSION["username"])) {

  header("Location: index.html"); // Redirigir a la página principal

  exit();

}

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

  $username = $\_POST["username"];

  $password = $\_POST["password"];

  $connection = new mysqli("localhost", "root", "", "wapicr");

  if ($connection->connect\_error) {

    die("Error de conexión: " . $connection->connect\_error);

  }

  $query = "SELECT id, contraseña FROM usuarios WHERE usuario = ?";

  $stmt = $connection->prepare($query);

  $stmt->bind\_param("s", $username);

  $stmt->execute();

  $stmt->bind\_result($user\_id, $stored\_password);

  $stmt->fetch();

  $stmt->close();

  if ($user\_id !== null && password\_verify($password, $stored\_password)) {

    $\_SESSION["username"] = $username;

    $\_SESSION["usuario\_id"] = $user\_id;

    header("Location: index.html"); // Redirigir a la página principal

    session\_destroy();

    exit();

  } else {

    $error\_message = "Usuario o contraseña incorrectos";

  }

  $connection->close();

}

?>

Cifrado y registro de usuarios PHP

<?php

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

  $username = $\_POST["username"];

  $password = $\_POST["password"];

  // Cifrar la contraseña antes de almacenarla

  $cifrado\_password = password\_hash($password, PASSWORD\_DEFAULT);

  $connection = new mysqli("localhost", "root", "", "wapicr");

  if ($connection->connect\_error) {

    die("Error de conexión: " . $connection->connect\_error);

  }

  $query = "INSERT INTO usuarios (usuario, contraseña) VALUES (?, ?)";

  $stmt = $connection->prepare($query);

  $stmt->bind\_param("ss", $username, $cifrado\_password);

  if ($stmt->execute()) {

    header("Location: login.html"); // Redirigir al inicio de sesión

    exit();

} else {

    $error\_message = "Error al registrar usuario.";

}

  $stmt->close();

  $connection->close();

}

?>

# **Referencias**

Palomo, M. (2023). *Programación en PHP a través de ejemplos.* España Universidad de Cadiz: Departamento de Lenguajes y Sistemas Informáticos.

Web, O. P. (2017). *Los diez riesgos más críticos en Aplicaciones web.* Creative Commons.

Rojas-Mesa Y, Molina-Gómez A, Valladares L. *Optimización para los motores de búsqueda (SEO) y la garantía de posicionamiento en los buscadores*. Medisur [revista en Internet]. 2021 [citado 2023 Ago 8]; 19(1):[aprox. 4 p.]. Disponible en: https://medisur.sld.cu/index.php/medisur/article/view/4870