

Diseño e implementación de una arquitectura LAMP para La compañía For Life, S.A

Grupo 1

David Castillo Marin

Jordy Esquivel Vargas

Cheryl Robles Quesada

Sharon Sandí Chaves

*Ingeniería en Sistemas de Computación, Universidad Fidélitas
Heredia, Costa Rica*

dcastillo50040@ufide.ac.cr

jesquivel60795@ufide.ac.cr

crobles40102@ufide.ac.cr

ssandi10700@ufide.ac.cr

I. INTRODUCCIÓN

En este artículo se explicará cómo se desarrolla un servidor web mediante lo que conoce como arquitectura “LAMP” en un servidor Ubuntu Server, que herramientas se necesitan para desarrollarlo, cual es funcionalidad y utilidad. Para ello se explicará un ejemplo hipotético de la vida real, en el cual la Compañía: For Life S.A requiere un servidor web en Ubuntu server con esta arquitectura y requieren que el servidor logre tener un módulo de autenticación de usuarios que incluya un identificador único, nombre y dos apellidos, este módulo determinara cuales usuarios se tienen el acceso permitido al servidor y cuáles no. También aparte se explicará algunos puntos extras como conexiones de SSL, prevenciones para ataques que puede recibir el servidor de SQL Injection, la implementación del motor de cache conocido como “Zend Optimizer” y los más importante que el servidor tenga la posibilidad de modificar y crear información de usuarios que van a tener acceso a este servidor.

II. ¿QUE ES LAMP? Y SUS HERRAMIENTAS

LAMP es una palabra que se conoce mucho dentro del mundo del web hosting, el desarrollo y diseño web, también se la conoce como «servidor LAMP» o «LAMP stack». Es la plataforma que ha acompañado muchos de los grandes hitos de las últimas décadas en cuanto al desarrollo de aplicaciones web. [1]

Una pila LAMP es un conjunto de cuatro tecnologías de software diferentes que los desarrolladores utilizan para crear sitios web y aplicaciones web. LAMP es un acrónimo del sistema operativo Linux, el servidor web Apache, el servidor de base de datos MySQL y el lenguaje de programación PHP. Estas cuatro tecnologías son de código abierto, lo que significa que son mantenidas por la comunidad y están disponibles gratuitamente para que cualquiera las utilice. Los desarrolladores utilizan pilas LAMP para crear, alojar y mantener el contenido web. Es una solución popular que impulsa muchos de

los sitios web que se utilizan comúnmente en la actualidad. [3]

Los desarrolladores web eligen una pila LAMP para crear aplicaciones web por las siguientes razones.

Costo

Todas las tecnologías LAMP son de código abierto, lo que significa que cualquier desarrollador o empresa puede utilizarlas sin tener que pagar tarifas de licencia. En lugar de comprar componentes de pila propietarios, puede descargar el sistema operativo, el servidor web, la base de datos y el lenguaje de scripts de forma gratuita. Esto reduce el costo de creación de aplicaciones web.

Eficiencia

La configuración de una nueva pila de desarrollo web requiere pruebas rigurosas de diferentes marcos, módulos, bibliotecas y herramientas. Por otro lado, una pila LAMP es una solución de desarrollo web probada y comprobada. Los desarrolladores web pueden priorizar y acelerar el desarrollo de aplicaciones para centrarse en lo que están creando en lugar de en cómo lo están creando. [3]

Mantenimiento

Los expertos en software de todo el mundo contribuyen al desarrollo de las tecnologías de pilas LAMP cambiando, comentando y revisando los códigos fuente disponibles públicamente. Mantienen y actualizan regularmente las tecnologías para que sigan siendo relevantes y seguras.

Soporte

Las tecnologías populares de código abierto, como las pilas LAMP, cuentan con el apoyo de una gran comunidad de TI global. Por lo tanto, los usuarios de la pila LAMP pueden encontrar información con mayor facilidad en los foros públicos de TI. Los desarrolladores web pueden consultar códigos

de ejemplo o utilizar complementos probados creados por la comunidad de código abierto. [3]

Flexibilidad

Una pila LAMP ofrece fiabilidad y flexibilidad a los desarrolladores web. Si bien la arquitectura LAMP especifica los componentes de software para cada capa, los desarrolladores pueden sustituirlos como mejor les parezca. Por ejemplo, pueden utilizar otro sistema operativo además de Linux como base de la pila. [3]

LAMP es el acrónimo usado para describir un sistema de infraestructura de internet que usa las siguientes herramientas:

Linux, el sistema operativo, En algunos casos también se refiere a LDAP.

Apache, el servidor web.

MySQL, el gestor de bases de datos.

PHP, el lenguaje de programación.

a combinación de estas tecnologías es usada principalmente para definir la infraestructura de un servidor web, utilizando un paradigma de programación para el desarrollo del sistema.

III. ¿QUE ES SSL? Y PARA QUE FUNCIONA

SSL (Secure Sockets Layer) es un protocolo de seguridad que se utiliza para proteger la comunicación entre un servidor web y un navegador web. Su función principal es garantizar que la información que se intercambia entre el servidor y el navegador esté cifrada y no pueda ser interceptada por terceros. SSL funciona mediante el uso de certificados digitales, que son emitidos por una autoridad de certificación confiable. Estos certificados se utilizan para autenticar la identidad del servidor web y para establecer una conexión cifrada entre el servidor y el navegador web. Una vez que se establece la conexión cifrada, cualquier información que se intercambie entre el servidor y el navegador, como contraseñas, datos de tarjetas

de crédito y otra información confidencial, estará protegida contra la interceptación y la manipulación por parte de terceros. En resumen, SSL es una tecnología esencial para proteger la privacidad y la seguridad de la información en línea, y se utiliza ampliamente en la actualidad para asegurar las comunicaciones en línea, especialmente en el comercio electrónico y la banca en línea.

IV. SQL INJECTION

En el proyecto se requiere de instalar una inyección de SQL como mecanismo de prevención para evitar recibir ataques externos a nuestra base de datos de información. Es esencial mantener una base de datos segura contra robos y ataques maliciosos de un atacante debido a que la información brindada por el usuario es de vital importancia para el desarrollo del proyecto y programa. Sin embargo, los lectores de este proyecto se preguntarán, ¿Que es inyección de SQL?

Una inyección de SQL, a veces abreviada como SQL, es un tipo de vulnerabilidad en la que un atacante usa un trozo de código SQL (lenguaje de consulta estructurado) para manipular una base de datos y acceder a información potencialmente valiosa. Es uno de los tipos de ataques más frecuentes y amenazadores, ya que puede atacar prácticamente cualquier sitio o aplicación web que use una base de datos basada en SQL. [7]

Si un desarrollador web no es meticuloso, al crear un sitio podría dejar un resquicio que alguien con malas intenciones podría usar para provocar efectos inesperados en su base de datos. Las inyecciones de SQL (o SQLI) se producen cuando el hacker introduce o inyecta en el sitio web código SQL malicioso, un tipo de malware que se conoce como la carga útil, y consigue subrepticamente que envíe ese código a su base de datos como si de una consulta legítima se tratara. [6]

Los piratas informáticos utilizan ataques de inyección SQL para acceder a las bases de datos de los sitios web. A veces, solo desea borrar los datos para causar caos, otras veces solo desea editar la base de datos. Esto es especialmente cierto para los sitios web financieros. Hasta que los piratas

informáticos obtengan el control de la base de datos, es fácil piratear los saldos de las cuentas de los clientes y transferir fondos a sus propias cuentas. Sin embargo, lo que los ciberdelincuentes suelen querer son los datos de usuario almacenados en los sitios web, como las credenciales de inicio de sesión. Estas credenciales robadas se utilizan para realizar acciones en nombre del usuario afectado o se compilan en grandes listas que se venden a otros ciberdelincuentes en la “dark web” o bien conocida como red oscura. Las personas que compran información robada a menudo lo hacen para robar identidades y cometer fraude.

Se muestra a continuación un ejemplo de ataque de inyección SQL:

Una vez que un atacante se da cuenta de que su base de datos es vulnerable, puede lanzar un ataque. Por ejemplo, puede editar su correo electrónico desde su cuenta de usuario. [8]

```
Y';  
UPDATE table  
SET email = 'atacante@ejemplo.com'  
WHERE email = 'usuario@ejemplo.com';
```

Fig. 1 Ejemplo de ataque en inyección SQL en PHP.

Después de la Y hay una comilla y un punto y coma, lo que permite al atacante cerrar la sentencia y ejecutar otra. Lo anterior resultaría en el siguiente código:

```
SELECT data  
FROM table  
WHERE Emailinput = 'Y';  
UPDATE table  
SET email = 'atacante@ejemplo.com'  
WHERE email = 'usuario@ejemplo.com';
```

Fig. 2 Código de ataque en inyección SQL en PHP.

Para llevar a cabo el ataque, el atacante primero tenía que conocer el nombre y la estructura de la tabla. Una técnica para recuperar más datos de los que devuelven las sentencias SQL de su aplicación es usar `1=1`. Esto siempre es cierto. La forma es:

```
SELECT * FROM users WHERE id = 10 or 1=1
```

Fig. 3 Ejemplo de ataque en inyección SQL en PHP.

Esto devolvería toda la tabla de usuarios, ya que `WHERE 1=1` es true. [8]

Los ataques de inyección SQL pueden tener una variedad de consecuencias. Un solo ataque SQLI puede tener un impacto devastador tanto en el usuario afectado como en la empresa o negocio objetivo.

Observando que un ataque es posible, además de una actividad frecuente por los ciber atacantes para obtener información, es necesario de contar con inyección SQL instalado en Ubuntu server para poder contrarrestar dichos ataques. En este caso la herramienta a utilizar será “sqlmap”

SQLMap es una herramienta de pruebas de penetración de código abierto que automatiza el proceso de identificar y explotar fallos de inyección SQL y tomar el control de servidores de bases de datos. Este dispositivo tiene muchas características especiales como tener un potente motor de detección, huella digital de base de datos, obtención de datos de la base de datos, acceso al sistema de archivos subyacente y ejecución de comandos en el sistema operativo a través de conexiones fuera de banda. [9]

Para instalar SQLMap en el servidor vamos a realizar los siguientes pasos:

En el servidor de Ubuntu vamos a ingresar con el usuario y contraseña, una vez con los datos ingresados se utiliza el siguiente comando: “sudo snap install sqlmap”. Una vez digitado el comando se empezará a descargar el sqlmap como se muestra en la fig 4.

```
cherylroble@sistemaoper1:~$ sudo snap install sqlmap  
Download snap "core18" (2721) from channel "stable" 5% 1.37MB/s 40.4s
```

Fig. 4 Proceso de descarga sqlmap en ubuntu server.

Luego aparecerá un mensaje que indica que ya el sqlmap fue instalado como aparece en la figura 5.

```
cherylroble@sistemaoper1:~$ sudo snap install sqlmap  
sqlmap 1.7.tar from Khiem Doan (khiemdoan) installed
```

Fig. 5 Descarga finalizada de sqlmap en ubuntu server.

Una vez ya instalado el sqlmap se puede digitar nuevamente el comando: “sudo snap install sqlmap”, e indicara que sqlmap ya se encuentra previamente instalado tal y como los muestra la figura 6.

```
cheryroble@sistemaoper1:~$ sudo snap install sqlmap
snap "sqlmap" is already installed, see 'snap help refresh'
cheryroble@sistemaoper1:~$
```

Fig. 6 sqlmap instalado en ubuntu server.

V. ZEND OPTIMIZER

¿Qué es Zend Optimizer?

Zend Optimizer es una aplicación de tiempo de ejecución de código abierto que funciona con secuencias de comandos de archivos codificados Zend Encoder y Zend Safeguard para mejorar la velocidad general de tiempo de ejecución de la aplicación PHP. El optimizador de Zend rompe el código encriptado convirtiendo PHP de texto sin formato en código intermedio de Zend (formato binario). Zend Optimizer interpreta el código encriptado para ejecutar aplicaciones encriptadas.

El optimizador Zend requiere soporte de servidor host PHP cuando se ejecutan aplicaciones PHP codificadas. Aunque el código se ejecuta cada vez que se ejecuta la página, hay una sobrecarga pequeña pero no perceptible. Los servidores de alojamiento compatibles mejoran el rendimiento de ejecución del código PHP al optimizar el código para aumentar la velocidad de ejecución sin refactorizar el código. [10]

Los sitios web deben ser rápidos, independientemente de su tamaño. Por lo tanto, el objetivo principal de desarrollar una aplicación es optimizarla. En este artículo, descubriremos algunas cosas para tener en cuenta al optimizar una aplicación PHP.

Debemos recordar que diseñar bien nuestra tecnología de software nos ayudará a escribir código a bajo costo. Si nuestro código se ejecuta rápido o usa menos recursos, lo llamamos de bajo costo.

¿Qué es la optimización de aplicaciones?

Cuando hablamos de optimización nos referimos a que nuestras aplicaciones tienen un bajo costo, es decir, se ejecutan más rápido, pero al mismo tiempo con calidad y eficiencia. El objetivo de optimizar una aplicación PHP es minimizar la cantidad de código que resuelve el mismo problema.

¿Qué debemos optimizar?

el tamaño de nuestra aplicación.

consumo de memoria.

la velocidad a la que se mueve.

Los sitios web deben ser rápidos, independientemente de su tamaño. Por lo tanto, el objetivo principal de desarrollar una aplicación es optimizarla. En este artículo, descubriremos algunas cosas para tener en cuenta al optimizar una aplicación PHP.

Debemos recordar que diseñar bien nuestra tecnología de software nos ayudará a escribir código a bajo costo. Si nuestro código se ejecuta rápido o usa menos recursos, lo llamamos de bajo costo.

VI. My SQL:

En programación es prácticamente inevitable utilizar algún tipo de sistema de gestión de bases de datos. Tarde o temprano, todo programa que se nos ocurra necesitará almacenar datos en algún lugar, al menos para poder almacenar una lista de usuarios autorizados, sus permisos y atributos. MySQL es el sistema de administración de bases de datos relacionales más utilizado en la actualidad porque se basa en una base de datos de código abierto.

Desarrollado originalmente por MySQL AB, fue adquirido por Sun Microsystems en 2008 y por Oracle Corporation en 2010, que ya cuenta con su propio motor MySQL InnoDB. MySQL es un sistema de gestión de bases de datos con licencia dual. Por un lado, es de código abierto, pero, por otro lado, tiene una versión comercial administrada por Oracle Corporation. Enterprise Edition está destinada a empresas que desean incluirla en una oferta patentada, incluidos productos o servicios

complementarios, como herramientas de monitoreo y soporte técnico oficial. [12]

Al ser de código abierto, está fácilmente disponible y la mayoría de los programadores que trabajan en desarrollo web han utilizado MySQL en uno de sus proyectos debido a su uso generalizado y su gran comunidad que admite a otros usuarios. Pero esas no son las únicas características que cubriremos a continuación:



Arquitectura Cliente-Servidor: MySQL opera en un modelo cliente-servidor. Esto significa que el cliente y el servidor se comunican entre sí de manera diferente para un mejor rendimiento. Por ejemplo, cada cliente puede consultar el registro para recuperar datos, cambiar datos, guardar esos cambios o crear nuevos registros. **Compatibilidad con SQL:** SQL es un lenguaje ampliamente utilizado en la industria. Como estándar de MySQL, proporciona compatibilidad total, por lo que, si ha utilizado otros motores de bases de datos, no tendrá problemas para migrar a MySQL. **Vistas:** Se ha proporcionado compatibilidad desde la versión 5.0 de MySQL para poder configurar vistas personalizadas de la misma forma que lo hacemos en otras bases de datos SQL. En grandes bases de datos, las vistas se convierten en un recurso esencial. **procedimiento almacenado.** Una característica de MySQL es que no procesa tablas directamente, sino que mejora la eficiencia de nuestra ejecución mediante el uso de procedimientos almacenados. **desencadenar.** MySQL también nos permite automatizar ciertas tareas en la base de datos. Cuando ocurre un evento,

se dispara otro evento para actualizar el registro u optimizar su funcionalidad. **Actuar.** Una transacción representa la ejecución de varias operaciones en la base de datos como una unidad. El sistema basado en el registro garantiza que todos los programas se creen correctamente o ninguno. En caso de un corte de energía, como una falla del monitor u otra interrupción, el sistema elige mantener la integridad de la base de datos al proteger la información. [12]

Beneficios de usar MySQL:

Después de describir las características principales de MySQL, es fácil ver las ventajas. MySQL es la elección lógica para su uso en un entorno empresarial. Con base en el uso de código abierto, las pequeñas empresas y los desarrolladores pueden brindar soluciones confiables y estandarizadas para sus aplicaciones. Por ejemplo, si tiene una lista de clientes, una tienda en línea con un catálogo de productos o incluso una gran selección de contenido multimedia, MySQL puede ayudarlo a organizarlo todo. [12]

Historial y versiones de MySQL

La historia de MySQL comenzó cuando el programador de software Michael Widenius buscaba una solución simple para obtener los resultados de su proyecto sin usar soluciones de terceros. Al principio, MySQL carecía de elementos básicos como la integridad referencial y las transacciones, pero a pesar de esto, rápidamente se hizo popular entre los desarrolladores web. Esto condujo a la creación de MySQL AB, fundada por David Axmark, Allan Larson y Michael Widenius, para continuar con el proyecto. Luego, la empresa fue adquirida en 2008 por Sun Microsystems, que vio en MySQL una solución competitiva frente a su rival Oracle, que curiosamente adquirió la empresa en 2010. [12]

VII. Autenticación de usuarios (Creación de usuarios y contraseñas)

Para la creación de usuarios y sus respectivas contraseñas se utilizará la autenticación de usuarios se utilizará por medio de **“Basic”** para ello debemos seguir una serie de pasos.

1. Primero debemos actualizar los repositorios de Ubuntu por medio del código:

```
apt-get update
```

Fig. 7 Comando para actualizar los repositorios

2. Posteriormente instalaremos el paquete de apache2-utils:

```
apt-get install apache2 apache2-utils
```

Fig. 8 Comando para instalar el paquete de utils

Una vez tengamos este paquete instalado seguirían los pasos en los cuales se crean los usuarios y sus contraseñas para cada uno.

1. Utilizaremos el comando **“htpasswd -c /etc/apache2/.htpasswd profesor1”** para crear un nuevo usuario y se almacenará la contraseña en el fichero .htpasswd, para este ejemplo el usuario creado se llamará profesor1 en el proyecto este será dave1.

```
htpasswd -c /etc/apache2/.htpasswd profesor1
```

Fig 9. Comando para crear usuarios

2. ¡Después de ejecutar el comando anterior el sistema nos pedirá una contraseña para este usuario que hemos creado, en nuestro proyecto se utilizó la contraseña “DaveVM24!”:

```
New password:
Re-type new password:
Adding password for user profesor1
root@mab55:/var/www/html# _
```

Fig 10. Ejemplo de como el sistema nos pide la contraseña destinada al nuevo usuario creado

3. Creamos un nuevo directorio para nuestro servidor el cual estará restringido, solo tendrán acceso aquellos usuarios que tengan permisos:

```
mkdir /var/www/html/profesor
```

Fig 11. Comando para la creación de nuestro directorio de acceso restringido

4. Entramos en el fichero de configuración 000-default.conf:

```
nano /etc/apache2/sites-enabled/000-default.conf
```

Fig 12. Comando para entrar fichero 000-default.conf

5. Dentro de este fichero, agregaremos las siguientes líneas con la información que posteriormente agregamos:

```
<Directory /var/www/html/profesor>
    AuthType Basic
    AuthName "Secure area - Authentication required"
    AuthUserFile /etc/apache2/.htpasswd
    Require user profesor1 mab55
</Directory>
```

Fig 13. Ejemplo de como debe ir ingresado la información al fichero 000-default.conf

Este método de autenticación de usuarios que utilizamos y explicamos, es muy versátil ya que permite de una manera muy simple la modificación de contraseñas y usuarios. También nos permite eliminar estos datos y así restringir el acceso de estos a nuestro directorio de servidor apache.[13]

VI. REFERENCIAS

- [1] S. Borges, “Servidor Lamp, ¿Qué es y para qué sirve?”, 2020. [Online]. Disponible en: <https://blog.infranetworking.com/servidor-lamp/>
- [2] Lamp, [Online]. Disponible en: <https://es.wikipedia.org/wiki/LAMP>
- [3] ¿Qué es una pila LAMP? - Explicación de la pila LAMP - AWS (amazon.com), 2023. [Online]. Disponible en: <https://aws.amazon.com/es/what-is/lamp-stack/#:~:text=Una%20pila%20LAMP%20es%20un,el%20lenguaje%20de%20programaci%C3%B3n%20PHP.>
- [4] Blog.hubspot, SSL: que es, como funciona y en que se diferencia de HTTPS, 2022. [Online]. Disponible en: <https://blog.hubspot.es/website/que-es-ssl>
- [5] Digicert, ¿Qué son SSL, TLS y HTTPS?, 2023 [Online]. Disponible en: [https://www.digicert.com/es/what-is-ssl-tls-and-https#:~:text=SSL%3A%20Secure%20Sockets%20Layer.\)%2C%20protegiendo%20as%C3%AD%20la%20conexi%C3%B3n.](https://www.digicert.com/es/what-is-ssl-tls-and-https#:~:text=SSL%3A%20Secure%20Sockets%20Layer.)%2C%20protegiendo%20as%C3%AD%20la%20conexi%C3%B3n.)
- [6] I. Belcic, ¿Que es inyección de SQL y cómo funciona?, 2020. [Online]. Disponible en: <https://www.avast.com/es-es/c-sql-injection>
- [7] Kaspersky, “¿Qué es la inyección de SQL? Definición y explicación”, 2023. [Online]. Disponible en: <https://latam.kaspersky.com/resource-center/definitions/sql-injection>
- [8] D. Lázaro, Ataques de SQL Injection en PHP, 2018. [Online]. Disponible en: <https://diego.com.es/ataques-sql-injection-en-php>
- [9] E. Allaband, “¿Cómo instalar SQLMap en Ubuntu 20?04 LTS [Online] Disponible en: <https://blog.eldernode.com/install-sqlmap-on-ubuntu-20-04/>
- [10] D.P. Valdés, «<https://www.maestrosdelweb.com/>,» 24 Mayo 2007. [Online]. Disponible en: <https://www.maestrosdelweb.com/como-optimizar-tus-aplicaciones-php/>. [Último acceso: 1 Abril 2023].
- [11] T.A. Page, «the astrology page,» Abril 2023. [En línea]. Disponible en: <https://es.theastrologypage.com/zend-optimizer.> [Último acceso: Abril 2023].
- [12] A. Robledano, «openwebinars.ne,» 24 septiembre 2019. [En línea]. Available: <https://openwebinars.net/blog/que-es-mysql/>.
- [13] Flota Digital, “Autenticación y Autorización en apache Ubuntu Server 20.04” Octubre 2021 [Online]. Disponible en: <https://flotadigital.com/club/tutoriales/ubuntu/autenticacion-y-autorizacion-en-apache-ubuntu-server-20-04/>