# SEGURIDAD LÓGICA USANDO ENTORNOS DE DESARROLLO EN APLICACIONES WEB EMPRESARIALES

**ALEJANDRO DAVID CERVANTES BARRAGÁN,**

**Universidad Nacional Abierta y a Distancia UNAD**
**Especialización en seguridad informática**
**ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS**
**Barranquilla Colombia**
**2020**

# SEGURIDAD LÓGICA USANDO ENTORNOS DE DESARROLLO EN APLICACIONES WEB EMPRESARIALES

**ALEJANDRO DAVID CERVANTES BARRAGÁN**

**Monografía de grado para optar al título de especialista en seguridad informática**

**DIRECTOR**
**Yesnir Antonio Redondo Daniel**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD**
**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**
**ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS**
**BARRANQUILLA COLOMBIA**
**2020**

**TABLA DE CONTENIDO**

**Pág**.

## LISTA DE FIGURAS

**Pág.**

## GLOSARIO

**CROSS SITE SCRIPTING (XSS):** ataques son un tipo de inyección, en el que los scripts maliciosos se inyectan en sitios web benignos y de confianza.

**EXPLOITS:** Son Agujeros de seguridad en un sistema tecnológico.

**FRAMEWORKS:** Es un entorno de trabajo o marco de trabajo es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.

**HTML:** Aprende a codificar HTML y CSS de forma gratuita en HTML.com. Tenemos tutoriales HTML y guías de referencia sobre etiquetas, atributos y todo lo demás que necesita para dominar HTML.

**LARAVEL:** es un marco de aplicación web con sintaxis expresiva y elegante. Ya hemos puesto las bases, liberándolos para crear sin sudar las pequeñas cosas.

**MVC:** Modelo-vista-controlador (MVC) es un patrón de arquitectura de software, que separa los datos y la lógica de negocio de una aplicación de su representación y el módulo encargado de gestionar los eventos y las comunicaciones.

**OWASP:** Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

**PENTESTING:** Pentesting o Penetration Testing es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.

**PHP:** PHP (acrónimo recursivo de PHP)

**HYPERTEXT PREPROCESSOR:** Es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML.

**STREAM:** Es la transmisión de información en tiempo real por internet.

**SYMFONY:** es un conjunto de componentes PHP reutilizables y un framework PHP para crear aplicaciones web, API, microservicios y servicios web.

**XXE:** Un ataque de entidad externa XML es un tipo de ataque contra una aplicación que analiza la entrada XML.

## RESUMEN

Bajo la condición de establecer el camino más óptimo entre el enfoque de desarrollo codificación pura o el trabajo con librerías especializadas, este estudio plantea la comparación y profundización del desarrollo de aplicaciones webs empresariales o bancarias con framework y código puro para desarrollo profesional, profundizando en los mecanismos de seguridad disponibles en el entorno de trabajo actualizado con protección a las últimas amenazas tales como; inyecciones SQL, Cross-site Scripting, etc. La descripción de usuarios antiguos en el desarrollo de aplicaciones web y sus experiencias en este campo. Soporte de comunidad. Desarrollo de aplicaciones webs empresariales y bancarias seguras, adicionalmente para todo tipo de software web.

El desarrollo de la monografía es mediante una metodología deductiva y documental, estas permiten tomar los resultados y experiencias existentes en el desarrollo de nuevo conocimiento. Los resultados arrojan un mejoramiento en la seguridad por las estructuras implementadas, métodos seguros, minimización de código y soporte de comunidad entre otros, los cuales minimizan las posibilidades de generar exploits o vulnerabilidades en transacciones bancarias, bases de datos, autenticación de usuarios y demás.

Se espera con esto dar una guía en los caminos, a los novicios en el ámbito de la informática, dentro del desarrollo de aplicaciones tanto nativas como web, estas dos vertientes presentan resultados, sin embargo, dar la orientación apropiada para acelerar el proceso al estudiante para llegar a la meta que más se proponga, ya sea la creación de prototipos y tecnologías nuevas como la producción en masa de aplicaciones escalables.



Palabras claves: Codificación pura, Framework, Seguridad, Inyecciones Sql, Owasp, Experiencias, Laravel, Información

## ABSTRACT

Under the condition of establishing the most optimal path between the pure coding development approach or working with specialized libraries, this study proposes the comparison and deepening of the development of enterprise or banking web applications with framework and pure code for professional development. Deepening the security mechanisms available in the working environment, updated with protection to the latest threats such as SQL injections, cross-site Scripting, etc. Description of older users in the development of web applications and their experiences in this field. Community support. Development of secure banking and enterprise web applications. Additionally for all kinds of web software.

The development of the monograph is through a deductive methodology and documentary methodology. These methodologies allow to take the results and experiences already existing in the development of new knowledge. The results lead to improved security by implemented structures, secure methods, code minimization, and community support among others. These results minimize the chances of generating exploits or vulnerabilities in bank transactions, databases, user authentication, and so on.

It is hoped that this is to give a guide on the roads, to novices in the field of computing, within the development of both native and web applications. These two aspects yield results, however, to give the appropriate guidance to accelerate the student's process of reaching the goal that is most proposed, whether it is prototyping and new technologies such as mass production of scalable applications.



Keywords: Pure codification, Framework, Security, Sql Owasp, Injections, Experiences, Laravel, Information

# INTRODUCCIÓN

El desarrollo de esta propuesta es la comparativa entre el desarrollo web mediante librerías de trabajo, como LARAVEL, mecanismos de seguridad y experiencias personales profesionales, entre los desarrollos de soluciones web mediante librerías o soluciones ya desarrolladas vs un planteamiento nuevo desde cero, que permite una orientación más apropiada para los ingenieros informáticos en seguridad sobre el desarrollo web.

La comparación entre un ataque con y sin un framework de desarrollo, de igual forma, entre las estructuras de trabajo MVC (Model Visual Controller) y código puro, además, las estructuras de visualización estructurada vs las de código puro. Todo esto como primera instancia, más adelante el área de la seguridad.

Se profundiza más en los mecanismos de seguridad disponibles en los entornos de trabajo, como son; los que se van a dar en el documento, los sistemas de seguridad para “SQL injection”, entre otros sistemas implementados contra “Tampering o manipulación de parámetros del servidor”, es el caso de la descripción de usuarios antiguos en el desarrollo de aplicaciones web y sus experiencias en este campo.

# 1 PLANTEAMIENTO DEL PROBLEMA

El desarrollo por codificación pura es el diseño y construcción del software sin respaldo o apoyo externo, esto nos señala una desventaja como la solución a problemas ya resueltos que toman tiempo y dinero en contraste a su curva de aprendizaje más plana. La programación por librerías especializadas, el opuesto, es el diseño y codificación de programa de computador con respaldo o apoyo externo, posee un gran avance y ventajas en contraste al anterior, así como una curva de aprendizaje más inclinada para su implementación, por supuesto depende de la librería.

El desarrollo web se compone de múltiples lenguajes trabajando en conjunto. Tecnologías como HTML, CSS, JavaScript, PHP, SQL bases de datos y demás, si se enfocan en la programación pura, el o los desarrolladores deben implementar todos los mecanismos de seguridad desde cero, reinventar la rueda, es una clara desventaja, sin embargo, una ventaja es la posibilidad de diseñar e implementar nuevas estrategias y componentes que superen las expectativas.

En el top 10 de la web OWASP, que es un sitio web especializado en seguridad, existen listas de ataques informáticos más comunes cada año, esta es una organización libre sin ánimo de lucro por lo que la comunidad es quien lo soporta y mantiene funcionando. Uno de los métodos de intrusión más comunes a una base de datos son los ataques de inyección mediante instrucciones, proactivamente voluntarias, incompletas o manipuladas[1], las webs empresariales, generalmente, cubren estos problemas.

La pérdida de autenticación consiste en el grupo de estrategias y herramientas que cubren la protección de información bancaria dentro de aplicaciones, en general es el conjunto de usos de componentes y técnicas para la explotación de usuarios y contraseñas[2].

La exposición de datos sensibles con poca o nula encriptación, el cifrado de datos sensibles ya sea de contraseñas o archivos, como envío de paquetes de datos no encriptados, este último puede ser consultado en la página OWASP tm foundation para obtener una orientación mayor de por dónde se debe seguir.

Las vulnerabilidades presentadas como es el caso de las entidades externas XML (XXE) buscan aprovechar la configuración equivocada de parámetros en el intérprete de XML[3],

[1] OWASP. ¿Quién es la Fundación OWASP? Owasp [sitio web]. 2019. [Consultado: 12 mayo 2019]. Disponible en: https://www.owasp.org/index.php/Main_Page

[2] FROUFE GUTIERREZ, A. Defective code II. Pérdida de autenticación. Betabeers [sitio web]. 2018, abril. [Consultado: 12 mayo 2019]. Disponible en: https://betabeers.com/blog/defective-code-ii-perdida-autenticacion-358/

[3] PALMA P, Cristian. Explorando la vulnerabilidad XXE: XML External Entity. Backtrack academy [sitio web]. 2017, septiembre. [Consultado: 20 mayo 2019]. Disponible en: https://backtrackacademy.com/articulo/explorando-la-vulnerabilidad-xxe-xml-external-entity

además, la pérdida del control de acceso o también conocido como seguridad oscura, se enfoca en el ocultamiento de una URL dentro de un sitio web[4].

Es por ello que es importante que no se presenten configuraciones de seguridad de forma incorrecta y mucho menos la no aplicación de parches regulares. Un ejemplo de esto son los sistemas operativos como Windows para uso doméstico donde se encuentran puertos abiertos sin necesidad, parches no instalados, ingreso de usuario con contraseñas en blanco y demás.

Los problemas de Cross Site Scripting (XSS) que es enfocado en la manipulación del intérprete de código web del lado del cliente[5] se encuentran comúnmente en aplicaciones codificadas en lenguaje PHP, deserialización insegura que es el momento en el cual un paquete de datos y viajero en la red llega a su destino y al momento de descodificarlo, el atacante corrompa, cambie o modifique, y genera un error, muy usado por los crackers para lograr conseguir acceso a un servidor, uso de componentes con vulnerabilidades conocidas que es muy popular al momento de instalar aplicaciones o características de aplicación, pero en versiones con huecos de seguridad, muy comunes en los sistemas operativos Windows en nuevas versiones.

Al momento de desarrollar software, ya sea web o no, ocurren siempre problemas que necesitan ser resueltos, en estas circunstancias es donde la comunidad ayuda con nuevos descubrimientos, resoluciones de problemas e incluso ayuda personalizada.

El adelanto en entornos empresariales, en especial a nivel bancario, exigen, demandan y solicitan garantías de seguridad por sus altos riesgos en la confidencialidad, cuidado de los datos y acceso a ellos.

## 1.1 FORMULACIÓN DEL PROBLEMA

¿Cuál de los dos enfoques es el camino más óptimo para el de desarrollo de sitios web seguros, en las organizaciones?

[4] OWASP. Top 10 2007: Las 10 vulnerabilidades de seguridad más críticas en aplicaciones web: Falla de restriccion de acceso a URL. Owasp [sitio web]. 2008 septiembre. [Consultado: 28 noviembre 2019]. Disponible en: https://owasp.org/www-pdf-archive/OWASP_Top_10_2007_Spanish.pdf

[5] SÁNCHEZ GONZÁLEZ, Javier. Ciberseguridad: mecanismos de ataque y defensa másextendidos. [en línea]. Tesis profesional. Universidad Politecnica de Madrid, 2016. [Consultado de noviembre 2019]. Disponible en: http://oa.upm.es/44509

# 2 JUSTIFICACIÓN

La investigación actual resuelve la incógnita de si es mejor desarrollar software sin previa codificación o no, esta incógnita es bastante extendida debido a las debilidades y fortalezas de cada paradigma, en la codificación de software de alto nivel aún se implementa código puro.

Los framework resuelven muchos problemas comunes que la codificación pura, ya que esta última, no contiene soluciones comprobadas porque su desarrollo comienza con un texto en blanco. Los inconvenientes comunes se resuelven y distribuyen en cada versión del entorno de desarrollo, además, permiten a los desarrolladores enfocarse en los problemas más directos con la certeza en mantener la seguridad.

La implementación de framework mejoran sin duda la seguridad en el transcurso del tiempo. A corto plazo el progreso mediante framework aumenta el rendimiento y los tiempos de desarrollo decrecen, a mediano plazo las aplicaciones demuestran mayores garantías y a largo plazo el desarrollo voluntario por la comunidad resuelve y mejora el entorno de trabajo.

En comparación existen beneficios, paradójicamente, en el desarrollo de software puro, tales como la posibilidad de mejorar las librerías de soporte si no satisfacen las necesidades de los proyectos, desarrollo rápido en proyectos agiles, implementación en la seguridad más integrada y demás.

Existen innumerables razones por la que esta investigación soporta las necesidades de muchos desarrolladores tanto nuevos como experimentados.

# 3 OBJETIVOS

## 3.1 OBJETIVO GENERAL

Demostrar la implantación de seguridad lógica usando entornos de desarrollo en aplicaciones web empresariales, mediante el framework o librería de desarrollo de aplicaciones web LARAVEL para minimizar o eliminar la mayor cantidad de exploits o vulnerabilidades posibles.

## 3.2 OBJETIVOS ESPECÍFICOS

- Comparar entre un desarrollo sin un framework vs Desarrollo con un framework, sus diferencias y fortalezas en entornos de aplicaciones web empresariales mediante una tabla de análisis comparativo cuanto respecta a la herramienta laravel.

- Determinar los mecanismos de seguridad disponibles en el entorno de trabajo para aplicaciones webs seguras dentro del entorno de desarrollo laravel mediante un estudio profundo dentro de la documentación de esta herramienta.

- Describir las impresiones personales de desarrolladores web independientes en la aplicación de soluciones, en cuanto respecta a herramientas desarrollo de aplicaciones web seguras, mediante sus experiencias en este campo con el framework laravel.

# 4 MARCO HISTÓRICO

Al observar la historia vemos la automatización de procesos repetitivos de información, este nuevo paradigma ha direccionado los paradigmas sociales, tecnológicos, científicos, médicos, e innumerables cambios en el área del conocimiento. Un ejemplo claro de ello en las fechas presentes son los equipos celulares, que ofrecen nuevos cambios de paradigmas.

Las primeras máquinas para el manejo de la información fueron el ábaco chino. esta herramienta facilitaba la contabilidad. “En el siglo XVII el científico francés Blas Pascal desarrolló una maquina calculadora que permite realizar sumas y restas con cifras altas, en honor al científico mencionado, su nombre se adoptó para nombrar un lenguaje de programación conocido como Pascal”[6], a partir del año1940 hasta la actualidad, el fruto de generaciones de cambios en múltiples áreas de las tecnologías, como la electrónica, muestra el nivel que se conoce hoy, como lo es los teléfonos móviles.

Señalando pioneros en el campo de la informática tenemos a Charles Babbage, Richard Karp, Kenneth Late Thompson y Dennis Ritchie; una referencia completa conlleva una investigación mayor y diferente al documento actual.

En el siglo XX, con la gran revolución tecnológica, se desarrolló el concepto binario, al comienzo todo era ceros y uno (0, 1), es decir código binario, cada aplicación desarrollada debía ser escrita directamente en binario y esto exclusivamente con especialistas informáticos de la época, el paso siguiente fue el desarrollo de tres (3) lógicas, esto gracias al aporte de la psicología a la informática, como mínimo, que permiten el desarrollo de cualquier programa informático, estas son variables, condicionales y bucles, esto generó cambios en el desarrollo de aplicaciones informáticas y fueron las bases para el futuro del software.

El internet fue otro gran giro en la historia, nos permite interconectarnos los unos a los otros sin importar la distancia física. “A principio de los años 60, la idea flotaba entre diversas instituciones americanas, como el Massachussetts Institute of Technology y la corporación RAND”[7]. Cuando se popularizo en la década de los 80 en adelante, el ingenio humano lo adopto en el área personal como en el área comercial. se desarrollaron sitios webs como Facebook para compartir vidas sociales, así como para impulsar el comercio

---

[6] PUCHE GARCíA, Sergio. Arqueología informática: Análisis, diseño e implementación del funcionamiento del ábaco matemático con Scratch [en linea] tesis profesional. Universidad Politécnica de Valéncia, 2017 – 2018. [Consultado: 16 diciembre 2018]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/106945/PUCHE%20-%20Arqueolog%C3%ADa%20inform%C3%A1tica:%20an%C3%A1lisis,%20dise%C3%B1o%20e%20implementaci%C3%B3n%20del%20funcionamiento%20del%20%C3%A1baco%20m....pdf?sequence=1. P. 7.

[7] MILLAN, José Antonio. Breve Historia de la Internet: El fruto caliente de la guerra fría [en línea]. 2006, febrero. [Consultado: 16 octubre 2018]. Disponible en: http://cv.udl.cat/cursos/elsmitjans/t1/docs/internet2.pdf. P. 2.

internacional, sin duda alguna un gran anclaje en el comercio internacional se dio con la adopción de la globalización de los bancos a través de internet, hoy en día todo banco es internacional accesible desde cualquier parte del mundo y precisamente esto trae de forma inherente los peligros de esta expansión.

Tanto el software como hardware, utilizados para el internet o el compendio de equipos informáticos o dispositivos interconectados entre sí mediante sistema alámbricos o inalámbricos, son programas informáticos dentro de equipos o dispositivos informáticos interactuando entre sí como un gran sistema, la estructura más implementada son la estructura cliente – servidor, donde, un computador personal, generalmente se conecta o solicita un servicio a un computador central que lo presta.

Estos servicios se construyen gracias innumerables implementaciones de lenguajes de programación que colaboran entre sí, no existe un solo programa en el entorno web, son colaboraciones de muchos tipos diferentes de programas informáticos a diferencia de trabajar dentro de un PC personal, estos se escriben en lenguajes como PHP, HTML, CSS y programas servidor a nivel de software, todos los lenguajes mencionados anteriormente son los más comunes en la actualidad, pero existen muchos más.

# 5 MARCO TEÓRICO

Cortes Robles[8], indica que la seguridad de la información contiene 3 objetivos los cuales son muy importantes y son la confidencialidad de los datos, la integridad de estos y la disponibilidad o acceso a ellos; en ingles se conoce como AIC, siendo estos sus principios básicos.

Laravel desarrollado por Taylor Otwell en el año 2011[9]. Esto lo convierte en un instrumento nuevo en comparación con otras como Symfony, posee un estilo artesanal que permite desarrollar de forma sencilla y cómoda, muy diferente en cuanto respecta al código puro, es en la actualidad la mejor herramienta, en lenguaje PHP, de desarrollo en aplicaciones web porque laravel es el framework de mayor notoriedad por desarrollo en tecnologías open-source, aplicaciones complejas seguras, rendimiento y simplificación[10]. Fácil, sencillo y seguro.

Laravel es una librería de desarrollo, también conocida en inglés como framework, que facilita al desarrollador la codificación al tener mucho código resuelto para así poder enfocarse en los aspectos y problemas reales de su trabajo, para cubrir con la pregunta de investigación, la librería y herramienta de desarrollo LARAVEL contiene soluciones a los problemas actuales, o al menos dentro del TOP 10, de ataques informáticos, cabe aclarar que la solución total de seguridad en aplicaciones web no se debe explícitamente a la codificación de la aplicación sino también a otras variables que podemos evidenciar dentro de las prácticas de una de las ramas dentro de la seguridad informática conocida como pentesting.

Como una evidencia de ello vemos a continuación una comparativa entre un desarrollo de software mediante codificación pura y desde cero a una a través de esta Liberia conocida como LARAVEL, el contenido a continuación cubre muchas deficiencias que permiten o facilitan los ataques mencionados anteriormente (ver planteamiento del problema).

Por el otro extremo se encuentran los enfoques puristas, es el enfoque de realizar todo desde cero, escribir toda la aplicación sin ayudas externas o librerías básicas, cada parte del código de la aplicación es de autoría del programador encargado, un ejemplo de ello se encuentra al momento de programar o codificar en lenguaje Python para la web, dicho lenguaje permite desarrollar aplicaciones webs y conexiones a servidor sin necesidad de librerías intermedias como el framework LARAVEL que está escrito en PHP, la desventaja

[8] CORTES ROBLES, Diego. Fundamentos Básicos de Seguridad de la Información [sitio web] Seguridad y Firewall. 2016. [Consultado: 20 de enero de 2020]. Disponible en: https://www.seguridadyfirewall.cl/2016/01/fundamentos-basicos-de-seguridad-de-la.html

[9] ECURED. Pascal. Ecured [sitio web]. 2019. [Consultado: 27 de 06 de 2019]. Disponible en: https://www.ecured.cu/Pascal

[10] NJENGA, A. 10 marcos PHP populares en 2019. Raygun [sitio web]. 2018, noviembre. [Consultado: 15 mayo 2019 Disponible en: https://raygun.com/blog/top-php-frameworks/

es precisamente la escritura completa de todas las rutinas necesarias y el conocimiento en redes implícito para lograr el objetivo, aunque, al mismo tiempo es su fortaleza, ya que permite personalizar y fortalecer aún mejor la estructura interna de la aplicación.

"Los Desarrolladores de código puro o puristas" son aquellos quienes implementan funciones sin apoyo de librerías o frameworks, estos desarrolladores tienen una importante afinidad por la codificación tradicional y consideran molesto realizar trabajos tanto personales como ajenos mediante el uso de estas. En caso tal de uso de alguna librería, será implementada por ellos"[11].

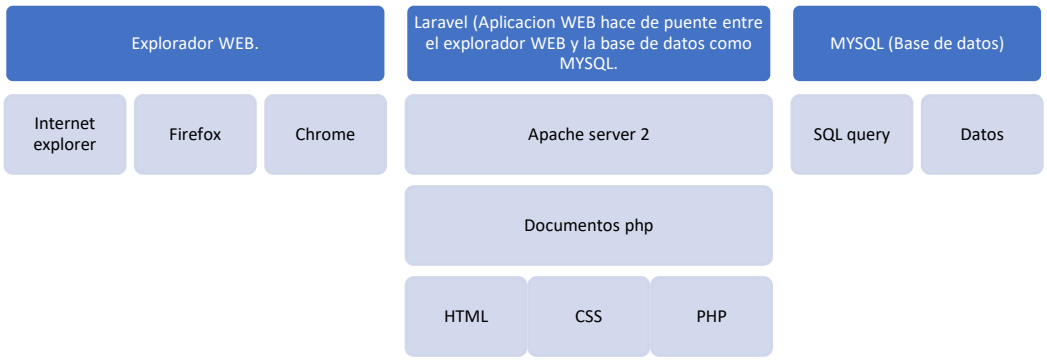
[11] PROGRAMACION.NET. Los 10 tipos de desarrollador web más comunes - Parte 1. Programación en Castellano [sitio web]. Programacion.Net. 2019. [Consultado: 20 de enero de 2020]. Disponible en: https://programacion.net/articulo/los_10_tipos_de_desarrollador_web_mas_comunes_parte_1_1128

# 6 MARCO CONCEPTUAL

## 6.1 ESTRUCTURA INTERNA DEL SISTEMA DE UN SITIO WEB

La estructura general de un sitio web está formada por un explorador web, un servidor web y una base de datos, a continuación, vemos cómo funciona generalmente; por supuesto en este caso usando la Liberia LARAVEL.

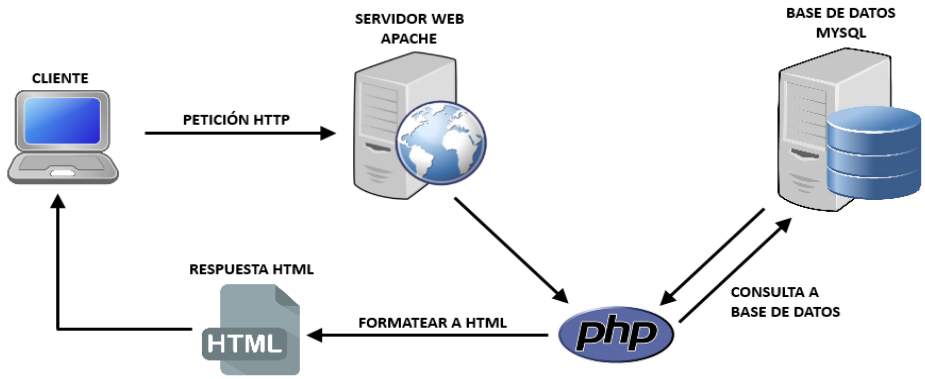
Figura 1. Usuario - aplicación web - Base de datos




Fuente: Elaboración propia

Vemos que el explorador envía y recibe información de la aplicación web, que en este caso es desarrollada en LARAVEL. La aplicación web se encarga de ser un puente, lógico, entre el usuario y una base de datos. Por supuesto la base de datos, MySQL, recibe y envía peticiones de la aplicación web facilitando las comunicaciones con el mundo exterior.

Figura 2. Esquema básico de una aplicación web

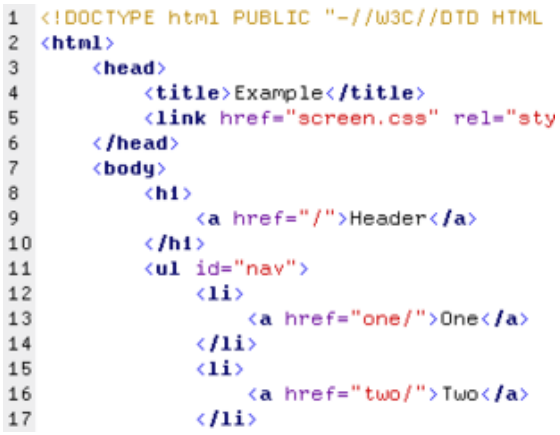



Fuente: “RASPBERRY PI COMO SERVIDOR WEB –[imagen]. DIYMakers. [Consultado: 20 de septiembre de 2019]. Disponible en: http://diymakers.es/raspberry-pi-como-servidor-web/

## 6.2 HTML

Lenguaje de etiquetado que define la estructura de presentación en una aplicación web. HTML es el lenguaje principal de la Web para desarrollar contenido de uso global[12]. De la misma forma que PHP maneja la parte lógica de una aplicación web, HTML maneja la parte estructural del lado visual de la aplicación.

Figura 3. Lenguaje HTML




Fuente: Web Master, “Lenguaje de Marcas de Hipertexto: La evolución del HTML [imagen]. hipertexto. 2008 [Consultado: 28 de abril de 2019]. Disponible en: http://hipertexto2008.blogspot.com/2008/08/la-evolucin-del-html.html

HTML es un lenguaje de formato de documentos determinado de acuerdo con SGML (o en otro termino una aplicación de SGML) para proporcionar formato a documentos de hipertexto[13]. El código, como podemos observar más atrás, es un lenguaje que diferente a los lenguajes de programación ya que no posee estructuras de condicionamiento, bucles o variables como en PHP, son etiquetas o nombres que definen completa o parcial mente una estructura ya sea una tabla, imagen e incluso texto sencillo, ahora, este sistema de etiquetado trabaja, preferentemente, con otro sistema de etiquetado conocido como CSS el cual veremos a continuación.

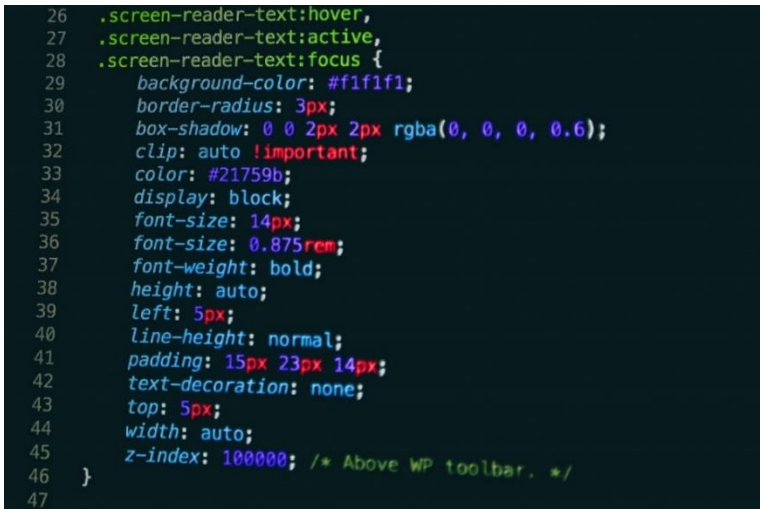
## 6.3 CSS

Lenguaje de etiquetado que define la apariencia de presentación en una aplicación web. Cascading Style Sheets (CSS) es un componente simple para añadir estilo a documentos

[12] BOS, Bert. ¿Qué es el CSS? W3C [sitio web]. 2019. [Consultado 26 de 10 de 2019]. Disponible en: https://www.w3.org/Style/CSS/Overview.en.html
[13] POZO, Juan. HTML, SGML, XHTML y XML. HTML con clase [sitio web]. 2003. [Consultado 18 diciembre 2019]. Disponible en: http://html.conclase.net/articulos/xml

de internet[14], en conjunto con el HTML, el CSS maneja estrictamente la configuración visual, el maquillaje, en el navegador o explorador web.

Figura 4. CSS




Fuente: PNTE, “Personalización del tema mediante CSS. [imagen]. Curso de WordPress. 2008. [Consultado: 28 de abril de 2019]. Disponible en: https://cursoswp.educacion.navarra.es/cursowp2018/personalizacion-de-los-sitios-mediante-css/

## 6.4 PHP

PHP es un lenguaje que suministra acceso a bases de datos y demás funciones[15]. PHP es uno de los muchos lenguajes de programación para realizar aplicaciones web, maneja la parte lógica del programa.

Figura 5. PHP


Fuente: TechGib Bureau, PHP 7.3 lanzado; viene con soporte para interfaz de funciones foráneas [imagen]. TechGig, 2018. [Consultado: 26 de septiembre de 2019]. Disponible en: https://content.techgig.com/php-7-3-released-comes-with-support-for-foreign-function-interface/articleshow/67002565.cms

[14] BOS, Bert. ¿Qué es el CSS? W3C [sitio web]. 2019. [Consultado 26 de 10 de 2019]. Disponible en: https://www.w3.org/Style/CSS/Overview.en.html

[15] PHP.NET. Introduccion PHP. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.intro.php

## 6.5 SQL Y MYSQL

Es una aplicación que guarda información en forma de tablas relacionadas para su posterior gestión. MySQL es una base de datos popular para web de rápido crecimiento, ISV de tecnología o gran empresa[16]. Aquí se guardan los datos de la aplicación web en grandes tablas interminables si es necesario para su uso posterior.

Figura 6. SQL

```
-- View: oeti.v_kat_oet

-- DROP VIEW oeti.v_kat_oet;

CREATE OR REPLACE VIEW oeti.v_kat_oet AS
 SELECT ko.cat_id, c.cat, k.kat, ko.kat_id
   FROM oeti.kat_oet ko
   LEFT JOIN kat k USING (kat_id)
   LEFT JOIN oeti.cat c USING (cat_id)
  ORDER BY ko.cat_id, ko.kat_id;

ALTER TABLE oeti.v_kat_oet
  OWNER TO postgres;
GRANT ALL ON TABLE oeti.v_kat_oet TO postgres;
GRANT SELECT ON TABLE oeti.v_kat_oet TO adminread;
COMMENT ON VIEW oeti.v_kat_oet
  IS 'Verknüpfung cat <--> kat mit sprechenden Feldern
# Siehe auch ->oeti.kat_oet';
```

Fuente: TechGib Bureau, PHP 7.3 lanzado; viene con soporte para interfaz de funciones foráneas [imagen]. TechGig, 2018. [Consultado: 26 de septiembre de 2019]. Disponible en: https://content.techgig.com/php-7-3-released-comes-with-support-for-foreign-function-interface/articleshow/67002565.cms

## 6.6 APACHE SERVER

Programa informático cuya función es la de prestar un servicio específico a una red, en este caso una aplicación web. Apache es el servidor local por excelencia, aunque existen otros servidores, este es designado punto de referencia[17]. Así mismo como existen servidores equipos, también es necesario que existan programas de computador para servidores. Apache es una aplicación que crea un servidor listo para su uso inmediato; es muy usado por los desarrolladores independiente por su fácil uso.

Figura 7. Logo del servidor Apache


Fuente: Keliweb, Alcuni consigli utili per la protezione del Web Server Apache “Alcuni consigli utili per la protezione del Web Server Apache • Keliweb Blog [imagen]. Keliweb. 2015. [Consultado: 20 de septiembre de 2019]. Disponible en:https://blog.keliweb.it/2015/07/alcuni-consigli-utili-per-la-protezione-del-web-server-apache/

[16] MYSQLTM. Ediciones MySQL. MySQL editions [sitio web]. 2019. [Consultado: 30 octubre 2019]. Disponible en: https://www.mysql.com/products/

[17] DE LEÓN, Á. Servidor apache. Infranetworking Internacional [sitio web]. 2019, junio. [Consultado: 17 septiembre 2019]. Disponible en: https://blog.infranetworking.com/que-es-apache-servidor/

## 6.7 EXPLORADOR WEB

Es el programa de computador que nos permite navegar por internet.

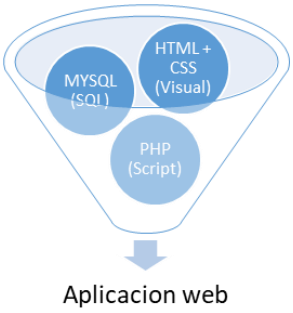
Figura 8. Exploradores web

Fuente: Jeffs Blog, “Safari ist der neue IE | Jeff [imagen]. Blog Welt. 2015. [Consultado: 28 de abril de 2020]. Disponible en: https://www.jeffsblog.at/2015/07/07/safari-ist-der-neue-ie/

## 6.8 APLICACIÓN WEB

Una aplicación web es un programa de computador que se ejecuta en un servidor y puede ser usado desde cualquier navegador web. Una aplicación web es un programa de computador que usamos en un explorador web. Una aplicación web es una aplicación con énfasis en usuario público dentro de la red global

Figura 9. Componentes de una aplicación web




Fuente: Elaboración propia

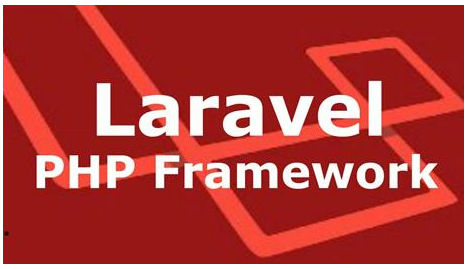
## 6.9 LARAVEL

Laravel es un entorno de desarrollo de aplicaciones web en lenguaje PHP[18]. Conociendo que es posible realizar aplicaciones web desde 0 usando PHP, HTML, CSS y demás

[18] HERNANDEZ, A. Introduccion a laravel. Meetup [sitio web]. 2018, mayo. [Consultado: 10 julio 2019]. Disponible en: https://www.meetup.com/es-ES/PHPGranada/events/250803700/

tecnologías, no es recomendable si su enfoque es a nivel profesional. LARAVEL, así como otras librerías, facilitan el desarrollo de las aplicaciones web para que el desarrollador se enfoque más en lo que es importante y no en los detalles técnicos de la tecnología.

Figura 10. Laravel PHP framework




Fuente: Ajay Gupta, Voyager - Crear paquete de panel de administración de backend para PHP Laravel. PHP Expert. 2017. [Consultado: 06 de octubre de 2019]. Disponible en: http://www.expertphp.in/article/voyager-create-backend-admin-panel-package-for-php-laravel-5

## 6.10 RESOLUCIÓN

Cada tecnología, que vemos previamente, señala soluciones ya existentes a problemas anteriores, se puede ver esto en la década de los 90, al momento de desarrollar software para la web. El enfoque purista o codificación pura permite profundizar y personalizar una solución tal cual ocurre en la creación de prototipos de tecnologías informáticas pioneras, a cambio de las librerías especializadas que se enfocan en el área de producción tal como lo haría una fábrica de textiles, por ejemplo, dependiendo del objetivo final así son los enfoques por tomar; Generalmente los desarrolladores más experimentados toman la vía purista, pero son los programadores senior de muchos años de experiencia.

La herramienta LARAVEL, la herramienta de ejemplo en esta investigación, contiene partes o componentes tanto del enfoque purista, como del enfoque especializado, dicha herramienta posee componentes de Symfony, otra herramienta para el desarrollo web, esta información la vemos en una comunidad de programadores donde se enseñan tecnologías web[19]

## 6.11 MODELO MVC (MODELO VISTA CONTROLADOR)

La estructura interna de la mayoría de las librerías de trabajo.

[19] POTENCIER, Fabian. Componentes de Symfony en Laravel. Rimorsoft Online [sitio web]. 2019. [Consultado: 20 noviembre 2019]. Disponible en: https://rimorsoft.com/componentes-symfony-en-laravel

Figura 11. Modelo Vista Controlador


Fuente: Elaboración propia

Este es el modelo esquemático de trabajo, actualmente, recomendado para la realización de aplicaciones en general y predeterminado en aplicaciones web. Toda librería conocida popular implementa este esquema. Recordando que esta estructura se encuentra dentro de la aplicación y no es un elemento externo.

La estructura básica descrita anteriormente posee fortalezas y debilidades. Como toda tecnología posee limitaciones, estas limitaciones son aprovechadas, en el caso actual, por sus interacciones con otros softwares. Como lo son las inyecciones SQL, Cross site scripting, perdida de autenticaciones de usuarios, deserialización insegura y prácticas equivocadas en la configuración en la seguridad del sistema. La web redeszone.net provee las siguientes definiciones de ataques informáticos.

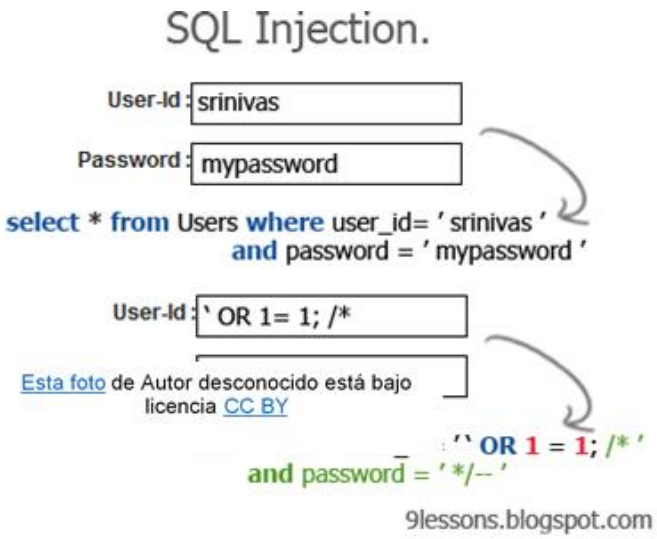
## 6.12 TIPOS DE ATAQUES INFORMÁTICOS

Se nombran los ataques más comunes dentro del ámbito web.

### 6.12.1 SQL Injection

Tenemos ejemplos como el presente donde se solicita un usuario y contraseña "SELECT * FROM Usuarios WHERE usur_id = ‘pedro’ AND contraseña = ‘123 ‘;. Alterando la consulta Podemos, con mucha creatividad, obtener información confidencial ejemplo “SELECT * FROM Usuarios WHERE usur_id = ‘’ OR 1 = 1;. Las expresiones de consultas SQL, NoSQL o LDAP son alterables a al punto de poder confundir al intérprete del servidor y permitir acceso a la base de datos sin autorización.

Figura 12. SQL Injection




Fuente: Sites Jariro. Seguridad Informática-Jairo: SQL Injection: [imagen]. 2015. [Consultado: 28 de septiembre de 2019]. Disponible en: https://sites.google.com/site/seguridadinformaticajairo/casos-practicos/sql-injection

### 6.12.2 Broken Authentication

Figura 13. Ataque de fuerza bruta

| Session Identifier : | 127.0.0.1/WebGoat WEAKID |
|---|---|
| Date | Value |
| 2006/11/11 14:33:27 | 12430116325200 7028 |
| 2006/11/11 14:33:27 | 12431116325200 7138 |
| 2006/11/11 14:33:27 | 12432116325200 7247 |
| 2006/11/11 14:33:27 | 12433116325200 7435 |
| 2006/11/11 14:33:27 | 12434116325200 7544 |
| 2006/11/11 14:33:27 | 12435116325200 7653 |
| 2006/11/11 14:33:27 | 12436116325200 7763 |
| 2006/11/11 14:33:27 | 12437116325200 7872 |
| 2006/11/11 14:33:28 | 12438116325200 7982 |
| 2006/11/11 14:33:28 | 12439116325200 8091 |
| 2006/11/11 14:33:28 | 12440116325200 8200 |
| 2006/11/11 14:33:28 | 12442116325200 8310 |
| 2006/11/11 14:33:28 | 12443116325200 8419 |
| 2006/11/11 14:33:28 | 12444116325200 8528 |
| 2006/11/11 14:33:28 | 12445116325200 8638 |
| 2006/11/11 14:33:28 | 12446116325200 8747 |
| 2006/11/11 14:33:28 | 12447116325200 8857 |
| 2006/11/11 14:33:28 | 12448116325200 8966 |
| 2006/11/11 14:33:29 | 12449116325200 9075 |

Fuente: Owasp, Prueba para omitir el esquema de autenticación (OTG-AUTHN-004). [imagen]. 2014. [Consultado: 28 de septiembre de 2019]. Disponible en: https://wiki.owasp.org/index.php/Testing_for_Bypassing_Authentication_Schema_(OTG-AUTHN-004).

Un ataque de fuerza bruta es un procedimiento automatizado de ensayo y error que permite conseguir la contraseña con una cantidad de intentos limitados o ilimitados. Las contraseñas débiles permiten a los ataques de fuerza bruta como otros métodos conseguir, incluso adivinar, las contraseñas de acceso. Contraseñas como “123”,

“admin”, fecha de cumpleaños, etc. La encriptación débil o desactualizadas de las contraseñas permiten su descifrado. Por ejemplo, tenemos el hash MD5, el cual ya fue descifrado y vulnerado y no se toma como sistema de seguridad. Cada sesión debe ser única para asegurar el ingreso del usuario real al sistema. La no aplicación de tokens, o números seriales, en cada sesión evita esta medida de seguridad. Errores en el desarrollo en los códigos de autenticación son otra debilidad ya que, al momento de codificar los sistemas de autenticación, son posibles dejar errores que permitan tomar ventaja de ellos. Las configuraciones y desarrollo de aplicaciones, web o nativas, débiles permiten a los, generalmente, delincuentes obtener contraseñas para acceso parcial o permanente al sistema.

### 6.12.3 Sensitive Data Exposure

El robo contraseñas o claves de usuarios, se presenta por las sesiones abiertas en lugares públicos o inseguros, las cookies, o archivos planos con información en los exploradores de internet, también se puede mencionar como otra fuente de información muy insegura, confiar información sensible a personas inadecuadas, todos estos casos y más son una larga lista de errores entre usuarios novicios que exponen y se etiqueta como, información sensible.

### 6.12.4 XML External Entities (XXE)

Un xml, extensible markup language (xml), según Owasp[20] es un archivo plano de etiquetado, similar al lenguaje html, que permite guardar información, de corta cantidad, que se utiliza, mayormente, en transferencia de información por la web. un procesador xml, así como los intérpretes de bases de datos relacionales sql, son los encargados de interpretar las instrucciones dadas por estos archivos. mal configuración en procesadores xml, permiten ver archivos ocultos del sistema.

### 6.12.5 Control de acceso roto

“A veces llamado autorización, es cómo una aplicación web otorga acceso a contenido y funciones a algunos usuarios y no a otros”[21]. Un atacante puede intentar ingresar a información de la compañía mediante los enlaces oscuros, existen diferentes formas de disminuir o minimizar este tipo de ataques, ejemplo por definición toda búsqueda de un enlace debe ser denegado como predeterminado, realizar una plantilla maestra fuerte en seguridad en el momento de desarrollo de código y siempre tener un sistema de registro que tome los errores que ocurran en todo momento para ser revisados y corregidos por los expertos; y estos son solo unos cuantos. existen múltiples formas de ingresar a un sistema, web en este ejemplo, y desde una perspectiva no muy común, como son los enlaces ocultos, la seguridad de un sistema es más intrínseca y compleja de lo aparente.

[20] OWASP. Procesamiento de entidad externa XML (XXE) [sitio web]. Owasp. 2020. [Consultado: 20 de marzo de 2020]. Disponible en: https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing

[21] OWASP. Control de acceso roto [sitio web]. Owasp. 2020. [Consultado: 20 de marzo de 2020]. Disponible en: https://owasp.org/www-community/Broken_Access_Control

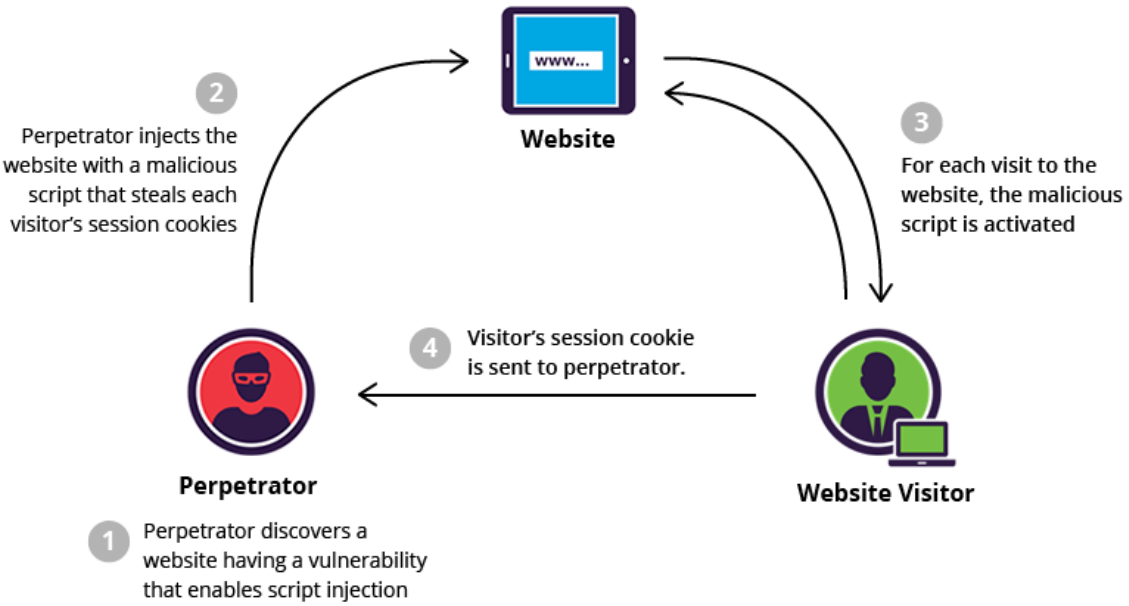
### 6.12.6 Configuración incorrecta de seguridad

Mínima configuración, si una utilidad no es necesaria, eliminarla. cambiar el usuario y contraseña de cuenta de administrador que viene por defecto. nunca dar información de más ejemplo en los mensajes de errores. todos los servidores deben se correctamente configurados. a diferencia del anterior se trata de no solo fallas en la configuración, sino del sistema completo por falta de capacitación.

### 6.12.7 A7:2017-Cross-Site Scripting (XSS)

El delincuente cambia, modifica scripts dentro del servidor y cuando el usuario visita, el web seguro, es vulnerado por estos, la imagen resuelve mejor.

Figura 14. Esquema de ataque XSS

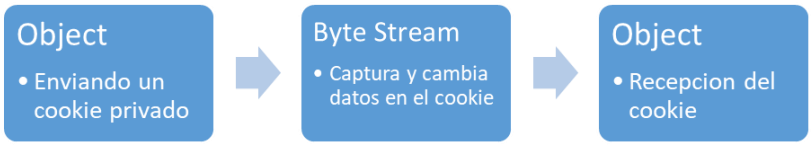



Fuente: Imperva, Ataques de secuencias de comandos de sitios cruzados (XSS). [imagen]. Imperva. 2015. [Consultado: 28 de septiembre de 2019]. Disponible en:https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/

### 6.12.8 Deserialización insegura

Capturas y modificación en los objetos que se envían por la web, la serialización es el stream con la información necesaria para acceder al, o a un, sistema.

Figura 15. Deserialización insegura




Fuente: Elaboración propia

### 6.12.9 A9:2017- Uso de componentes con vulnerabilidades conocidas

Parches, software o programas utilitarios que no son seguros, automáticamente este se vuelve frágil, quedando en peligro a través de estos recursos.

### 6.12.10 A10:2017-Insuficiente monitoreo y registro

Debido a la falla de monitorización, la mayoría de las veces se aplaza hasta 200 días en detectar una debilidad en un programa de computador o una plataforma web, tiempo que se podría reducir notablemente simplemente configurando mayores controles, mejor monitorización y más registros a estas plataformas.

Según un artículo web realizado por el periódico digital “el confidencial”, la seguridad en la banca es "La ciberseguridad de los bancos es un festival del humor"[22], el alto índice de exigencia comercial e interconexión entre bancos obstaculiza el trabajo de los especializas en seguridad informática, tanto es que, según el artículo, nadie quiere trabajar en ellos, los pequeños son los más vulnerables a los ataques informáticos, presentan problemas como; las certificaciones no son seguras, sus enfoques son equivocados en la documentación de los códigos de las aplicaciones web y que hoy día no existe un medio o método, hasta el momento, que garantice seguridad absoluta.

[22] EL CONFIDENCIAL. Bancos bajo ataque: "La ciberseguridad de entidades es un festival del humor". El Confidencial [sitio web]. 2018, septiembre. [Consultado 27 de 06 de 2019]. Disponible en: https://www.elconfidencial.com/tecnologia/2018-09-15/banca-online-seguridad-agujeros_1615928/

# 7 COMPARATIVA ENTRE UNA CODIFICACIÓN PURISTA Y UN DESARROLLO CON LIBRERÍAS ESPECIALIZADAS EN ENTORNOS DE PRODUCCIÓN

Tabla 1. Ejemplo Framework vs Código puro

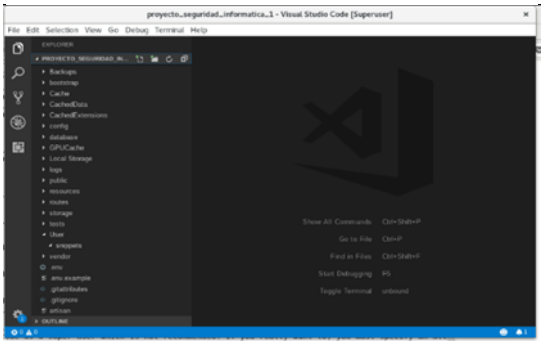
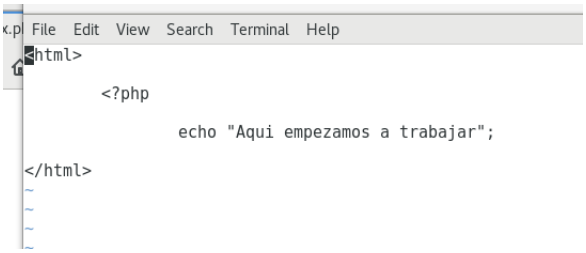
<table>
<tr><th>Laravel</th><th>Código puro</th></tr>
<tr><td>Nuevo proyecto<br>Mediante un componente conocido como “composer”, se crea y estructura de forma organizada y correcta el entorno de trabajo.</td><td>Nuevo proyecto<br>Comenzamos a partir de un archivo de texto sin estructura alguna.</td></tr>
<tr><td>Figura 16. Estructura del entorno de codificacion<br>  <br>Fuente: Elaboracion propia</td><td>Figura 17. Estructura del entorno de codificacion en bloc de notas<br>  <br>Fuente: Elaboracion propia</td></tr>
<tr><td>Conexión con base de datos (Modelo en MVC)<br>Menor cantidad de código. El usuario y la contraseña no se codifican, solo se asigna su usuario y contraseña en un documento aparte cuidando la seguridad.</td><td>Conexión con base de datos<br>Debe ser codificado absolutamente todo dentro de un archivo PHP. No se encuentra testeado de la posibilidad de ataques informáticos.</td></tr>
<tr><td>public function index()<br>{<br>$users = DB::table('users')->get();<br>return view('user.index', ['users' => $users]);<br>}</td><td><?php<br>$servername = "localhost";<br>$username = "username";<br>$password = "password";<br><br>try {<br>$conn<br>= new PDO("mysql:host=$servername;dbname=myDB", $username, $password);<br>// set the PDO error mode to exception<br>$conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);<br>echo "Connected successfully";<br>}<br>catch(PDOException $e)<br>{<br>echo "Connection failed: " . $e->getMessage();<br>}<br>?></td></tr>
</table>

Tabla 1. (Continuación)

| **Laravel** | **Código puro** |
|---|---|
| Estructura de visualización (Vista en MVC)<br>Esquema de estructura visual del sitio web propio de la librería LARAVEL, otras librerías también desarrollan los suyos propios, con el propósito de un desarrollo más controlado y mayor seguridad. | Estructura de visualización<br>Mayor complejidad, manejo de variables sin seguridad y menos intuitivo. |
| <!-- Stored in resources/views/child.blade.php --><br><br>@extends('layouts.app')<br><br>@section('title', 'Page Title')<br><br>@section('sidebar')<br>  @parent<br><br>  This is appended to the máster sidebar. <br>@endsection<br><br>@section('content')<br>  This is my body content. <br>@endsection | <br><br><br><br><br><!DOCTYPE html><br><html><br><body><br><br><?php<br>echo "My first PHP script!";<br>?><br><br></body><br></html> |

Fuente: Elaboración propia

# 8 ELEMENTOS DE SEGURIDAD DISPONIBLES EN LOS ENTORNOS DE PRODUCCIÓN TANTO EN EL CÓDIGO PURO COMO CON LIBRERÍAS ESPECIALIZADAS.

## 8.1 CÓDIGO PURO

Las siguientes funciones directas dentro del lenguaje php que se pueden acceder para al momento de codificar, una Configuración correcta del motor de código PHP permite minimizar los riesgos[23]. Sin embargo, el motor de PHP y su lenguaje no permite resguardar las bases de datos por sí misma[24].

A continuación, algunos mecanismos de seguridad directos en el lenguaje de programación PHP.

- Password_hash() El método señalado permite convertir una cadena de texto en una cadena alfanumérica mediante encriptación, generalmente usada para contraseñas.

- Password_verify() En contrapartida este método permite la verificación de las contraseñas con sus cadenas de caracteres alfanuméricos[25].

- Is_numeric() es una función para verificar que el valor de una variable, en php, es numérica.

- Ctype_digit() de forma general averiguar el tipo de dato de una variable[26].

- Settype() Cambiar el tipo de dato de una variable

- Php.ini es el archivo de configuración del motor PHP, ahí podemos configurar mayormente su comportamiento. Dentro de este podemos activar o desactivar la información para depuración como es el display_erros = off o manipular la creación y modificación de cookies con sesión_coocke_httponly = On. De forma

[23] PHP.NET. Introduccion PDO. The Php Group [sitio web]. 2019. [Consultado: 22 junio 2019]. Disponible en: https://www.php.net/manual/es/intro.pdo.php

[24] PHP.NET. Introduccion PHP. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.intro.php

[25] PHP.NET. Inyeccion sql. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.database.sql-injection.php

[26] PHP.NET. Modelo de almacenamiento cifrado. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.database.storage.php

predeterminada PHP muestra que se encuentra instalada en los servidores según nos informan grupos de seguridad[27].

## 8.2 LIBRERÍA ESPECIALIZADA PARA ENTORNOS DE TRABAJO WEB EMPRESARIALES

Señalando que la librería de desarrollo en el presente estudio se llama LARAVEL.

### 8.2.1 Tampering o manipulación de parámetros al servidor

"LaraForm es un contenedor de formularios Laravel con métodos convenientes, que incluye protección contra la manipulación de formularios y evita el envío de formularios dobles."[28], esta herramienta desarrollada en PHP permite codificar desde el servidor los formularios que se presentan al público protegiendo su código y evitando la manipulación de parámetros en el servidor.

Existen tres versiones:

#### 8.2.1.1 Community edition

- Licencias MIT.
- Elementos básicos de los formularios.
- Validadores básicos.
- Soporte Github

#### 8.2.1.2 Individual edition

Posee un costo de $699 dólares y además de tener todo de la "community edition", posee adicionalmente:

- Todo el código fuente
- Licencia permanente
- Elementos completos de formularios
- Validadores completos
- Manejador de imágenes en los formularios
- Elementos traducibles
- Condicionales lógicas
- Cantidad de usuario 1.

[27] ACUNETIX. PHP Security 4: mejores prácticas de seguridad de PHP. [sitio web]. Acunetix. [Consultado: 15 septiembre 2019]. Disponible en: https://www.acunetix.com/websitesecurity/php-security-4/

[28] BEK, Davit. Lara Form: Paquete Laravel Form con protección contra manipulaciones de formularios. GitHub [sitio web]. 2018. [Consultado: 15 mayo 2019]. Disponible en: https://github.com/omnicode/lara-form

- Cantidad de tiempo posible permitido para la descarga he implementación de la herramienta a través de manejadores como “composer” durante 1 año.
- Durante 1 año de actualizaciones gratuitas.
- Descuento por renovación de compra al 30%.

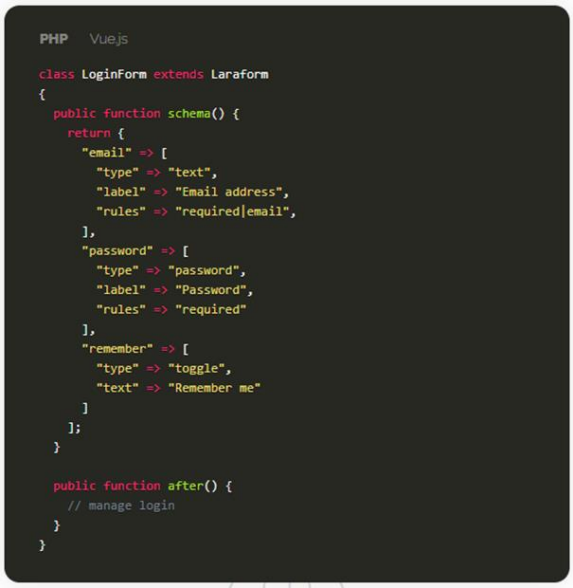
#### 8.2.1.3 Company edition

Costo de $1.999 además de obtener todo lo que posee la edición individual posee:

- Cantidad de usuarios 10
- Soporte técnico directamente con los desarrolladores de la herramienta.
- Manejadores de código CSS como Sass.
- La posibilidad de implementar el código fuente de la distribución de “LARAFORM” en, por ejemplo, manejadores de contenido CMS, administradores de sistemas, etc. ….

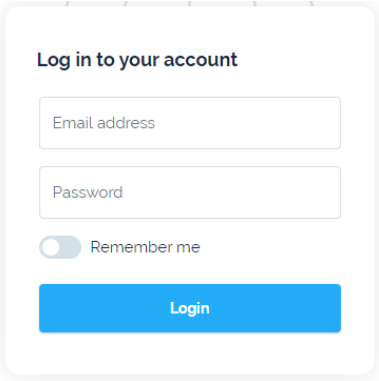
Ejemplo

Figura 18. Lara Form back end PHP code




Fuente: BERECZ, Adam Laraform | Reactive Form Builder for Vue.js with Laravel Support [imagen] LaraForm. 2018. [Online]. [Consultado: 30 de septiembre de 2019]. Disponible en: https://laraform.io/

Figura 19. LaraForm Front end render




Fuente: BERECZ, Adam Laraform | Reactive Form Builder for Vue.js with Laravel Support [imagen] LaraForm. 2018. [Online]. [Consultado: 30 de septiembre de 2019]. Disponible en: https://laraform.io/

La implementación de seguridad lógica es posible ser aplicada dentro de la estructura interna dentro del servidor y evitar ser manipulada directamente en los equipos locales

### 8.2.2 CSRF (cross-site request forgery)

Los tokens se utilizan para garantizar que terceros no puedan iniciar dicha solicitud. Esto se hace generando un token que se debe pasar junto con el contenido del formulario, este se comparará con un valor adicionalmente guardado en la sesión del usuario, si coincide, la solicitud se considera válida, de lo contrario se considera inválida."[29]. La herramienta CSRF proporciona un TOKEN o número serial único que permite mantener a un formulario un único acceso cada vez que se le llame, incluyendo navegación.

### 8.2.3 X-Csrf-Token Protección para programas AJAX.

Figura 20. Etiqueta meta con token

```
<meta name="csrf-token" content="{{ csrf_token() }}">
```

Fuente: OTWELL, Taylor. Protección CSRF [imagen]. Laravel. 2018. [Consultado: 26 de septiembre de 2019]. Disponible en: https://laravel.com/docs/5.7/csrf

Figura 21. Configuración de la etiqueta en meta

```
$.ajaxSetup({
    headers: {
        'X-CSRF-TOKEN': $('meta[name="csrf-token"]').attr('content')
    }
});
```

Fuente: OTWELL, Taylor. Protección CSRF [imagen]. Laravel. 2018. [Consultado: 26 de septiembre de 2019]. Disponible en: https://laravel.com/docs/5.7/csrf

[29] MUHAMMED DASTAGIR, Hussein. Ways for securing Laravel Application. Viblo [sitio web]. 2016, mayo. [Consultado: 16 octubre 2019]. Disponible en: https://viblo.asia/p/ways-for-securing-laravel-application-NPVMaDygRQOk

### 8.2.4 X-Xsrf-Token Protección para programas con JavaScript

Ejemplo básico general

Figura 22. CSRF (Cross-site request forgery) apply code

```
<form method="POST" action="/profile">
    @csrf
    ...
</form>
```

Fuente: OTWELL, Taylor. Protección CSRF [imagen]. Laravel. 2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.7/csrf

### 8.2.5 SQL injection o inyección SQL

"El ORM elocuente de Laravel utiliza el enlace de parámetros PDO para evitar la inyección de SQL"[30]. Laravel, así como otras librerías, poseen respuestas a los distintivos ataques como las inyecciones SQL, por ejemplo, laravel en su flujo de trabajo con las bases de datos implementa una herramienta conocida como "ORM eloquent" que permite una seguridad mayor como una estructura de comunicación con la base de datos más fácil.

Figura 23. Definiendo modelos

```
php artisan make:model Flight
```

Fuente: OTWELL, Taylor. Elocuente: Comenzando [imagen]. Laravel .2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.8/eloquent#introduction.

Figura 24. Definiendo modelos 2

```
php artisan make:model Flight --migration

php artisan make:model Flight -m
```

Fuente: OTWELL, Taylor. Elocuente: Comenzando [imagen]. Laravel .2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.8/eloquent#introduction.

[30] EASY LARAVEL BOOK. Laravel 5 Prevents Sql Injection, Cross-Site Request Forgery, And Cross-Site Scripting. Easy laravel 5 [sitio web]. 2015, junio. [Consultado: 15 septiembre 2019]. Disponible en: https://www.easylaravelbook.com/blog/how-laravel-5-prevents-sql-injection-cross-site-request-forgery-and-cross-site-scripting/

Figura 25. Convenciones del modelo eloquent

```php
namespace App;

use Illuminate\Database\Eloquent\Model;

class Flight extends Model
{
    //
}
```

Fuente: OTWELL, Taylor. Elocuente: Comenzando [imagen]. Laravel .2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.8/eloquent#introduction.

Figura 26. Nombrando tablas

```php
<?php

namespace App;

use Illuminate\Database\Eloquent\Model;

class Flight extends Model
{
    /**
     * The table associated with the model.
     *
     * @var string
     */
    protected $table = 'my_flights';
}
```

Fuente: OTWELL, Taylor. Elocuente: Comenzando [imagen]. Laravel .2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.8/eloquent#introduction.

Figura 27. Primary keys (índices claves)

```php
<?php

namespace App;

use Illuminate\Database\Eloquent\Model;

class Flight extends Model
{
    /**
     * The primary key associated with the table.
     *
     * @var string
     */
    protected $primaryKey = 'flight_id';
}
```

Fuente: OTWELL, Taylor. Elocuente: Comenzando [imagen]. Laravel .2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.8/eloquent#introduction

Figura 28. Incremento en los índices de claves

```php
<?php

class Flight extends Model
{
    /**
     * Indicates if the IDs are auto-incrementing.
     *
     * @var bool
     */
    public $incrementing = false;
}
```

Fuente: OTWELL, Taylor. Elocuente: Comenzando [imagen]. Laravel .2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.8/eloquent#introduction

Figura 29. Cambiar tipo de numeración de índice

```php
<?php

class Flight extends Model
{
    /**
     * The "type" of the auto-incrementing ID.
     *
     * @var string
     */
    protected $keyType = 'string';
}
```

Fuente: OTWELL, Taylor. Elocuente: Comenzando [imagen]. Laravel .2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.8/eloquent#introduction

### 8.2.6 Encriptación

"El cifrador de Laravel utiliza OpenSSL para proporcionar cifrado AES-256 y AES-128"[31]. Encriptación mediante OpenSSL usando AES-256 y AES-128 como selección de codificación.

[31] LARAVEL. Cifrado. Laravel [sitio web]. 2019. [Consultado: 20 julio 2019]. Disponible en: https://laravel.com/docs/5.7/encryption

### 8.2.7 Hashing

La fachada de Laravel Hash proporciona hash Bcrypt y Argon2 seguro para almacenar contraseñas de[32] usuario. Encriptación para contraseñas con Bcrypt y Argon2.

## Uso básico

Figura 30. Encriptación de una contraseña con Bcrypt

```
$password = Hash::make('secret');
```

Fuente: OTWELL, Taylor. Elocuente: Comenzando [imagen]. Laravel .2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.8/eloquent#introduction

Figura. Encriptacion de una contraseña con Bcrupt 2

```
$password = bcrypt('secret');
```

Fuente: OTWELL, Taylor. Elocuente: Comenzando [imagen]. Laravel .2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.8/eloquent#introduction

Figura 31. Verificando una contraseña encriptada

```
if (Hash::check('secret', $hashedPassword))
{
    // The passwords match...
}
```

Fuente: OTWELL, Taylor. Elocuente: Comenzando [imagen]. Laravel .2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.8/eloquent#introduction

Figura 32. Verificando si una contraseña necesita ser encriptada nuevamente

```
if (Hash::needsRehash($hashed))
{
    $hashed = Hash::make('secret');
}
```

Fuente: OTWELL, Taylor. Elocuente: Comenzando [imagen]. Laravel .2018. [Consultado: 01 de octubre de 2019]. Disponible en: https://laravel.com/docs/5.8/eloquent#introduction

[32]LARAVEL. Hashing. Laravel [sitio web]. 2019. [Consultado: 20 julio 2019]. Disponible en: https://laravel.com/docs/5.7/hashing

# 9 EXPERIENCIAS DE USUARIOS EN EL USO DE HERRAMIENTAS ESPECIALIZADAS, CASO ACTUAL LARAVEL

Para principiantes la herramienta de trabajo LARAVEL facilita mucho el trabajo por su lista de funciones necesarias no solo en la productividad sino en la seguridad, como lo expresa el siguiente autor. “Si eres principiante, para la seguridad de tu sistema Laravel es tu mejor opción, posee funciones potentes y fáciles de usar para la autenticación de usuarios”[33].

“La implementación de la autenticación es muy simple con Laravel porque casi todo se modifica de fábrica, el marco de trabajo proporciona una manera fácil de organizar la lógica de autorización y controlar el acceso a todos los recursos, por lo tanto, el propietario de una aplicación web puede estar seguro de que el acceso a los recursos protegidos no se concederá a los usuarios no autorizados.”[34]

La tecnología “middleware”, o capa intermedia, es el espacio donde se implementan tecnologías tipo filtro, generalmente, usado, tanto, en las autenticaciones de usuarios como protección contra ataques tipo “Cross-Site-Scripting(XSS)”.

> Tus aplicaciones estarán blindadas usando Middleware; ya que se encarga de analizar y filtrar las llamadas HTTP en tu servidor, puedes instalarlo para que se encargue de verificar que se trate de un usuario registrado, de evitar problemas de tipo Cross-Site-Scripting (XSS) y otras medidas de seguridad. Laravel viene listo para implementar autenticación de usuarios de forma nativa e incluye la opción de “recordar” al usuario, además, te permite incluir parámetros adicionales, lo que nos asegurará, por ejemplo, si se trata de un usuario activo. Una aplicación segura necesita ser capaz de encriptar sus datos, con Laravel tienes todo lo necesario para empezar a usar seguridad OpenSSL y cifrado AES-256-CBC, adicionalmente, todos los valores encriptados están firmados por un Código [35]

Otra evidencia de lo completo qué es una librería de trabajo framework es la implementación junto con su núcleo de las pruebas linternas de corrección de código. cómo lo explica a Clarión Technologies en el siguiente párrafo.

“Cuando se trata de la prueba de la aplicación Laravel de forma predeterminada proporciona la prueba unitaria para la aplicación, que a su vez contiene pruebas que detectan y previenen regresiones en el marco de trabajo. La integración de la unidad PHP como un marco de pruebas es muy fácil en la aplicación Laravel, además de eso, las

[33] GOMEZ, A. Mi experiencia usando laravel. Steemit [sitio web]. 2017. [Consultado: 15 mayo 2019]. Disponible en: https://steemit.com/spanish/@angelggomz/mi-experiencia-usando-laravel

[34] MATRUNCHYK, Serhii. Las 7 razones principales por las que Laravel es mejor para las empresas que otros frameworks PHP. Medium [sitio web]. 2018, febrero. [Consultado: 16 de junio de 2019]. Disponible en: https://medium.com/@serhii.matrunchyk/top-7-reasons-why-laravel-is-better-for-businesses-than-other-php-frameworks-c0f5e85c5b85

[35] ANTÓN DORANTES, C. Laravel, el mejor framework en PHP. PLATZI. [en línea]. 2015. [Consultado: 17 junio 2019]. Disponible en: https://platzi.com/blog/laravel-framework-php/

pruebas unitarias se pueden ejecutar a través de la utilidad de línea de comandos artesanal proporcionada".[36]

Cómo lo explican en balears laravel contiene un marco de seguridad bastante extenso, recordando que es, en la actualidad, la librería más completa que hay en cuanto respecta a funcionalidades hasta el día de hoy, que funcionan de forma interna y total y completamente fijada en los procesos internos de la aplicación dando nos la oportunidad enfocarnos en la lógica del trabajo.

> Mientras desarrolla una aplicación, todo el mundo tiene que utilizar algunas de las otras formas de hacer que la aplicación sea segura. Laravel se encarga de la seguridad en su marco, utiliza una contraseña con sal y hash, lo que significa que la contraseña nunca se guardaría como texto sin formato en la base de datos, el algoritmo hash Bcrypt para generar una representación cifrada de una contraseña, además, utiliza instrucciones SQL preparadas que hacen que los ataques de inyección sean inimaginables, junto con esto, proporciona una manera sencilla de escapar la entrada del usuario para evitar la inyección del usuario de la etiqueta <script>, estas son las características de seguridad que Ofrece Laravel:[37]

La siguiente ilustración 22 lista la mayoría de los sistemas de seguridad en Lavavel, que, a diferencia de un enfoque purista, posee cubiertos ya la mayoría de las perspectivas necesarias en la implementación de seguridad en aplicaciones webs.

Figura 33. Lista de sistemas de seguridad en LARAVEL

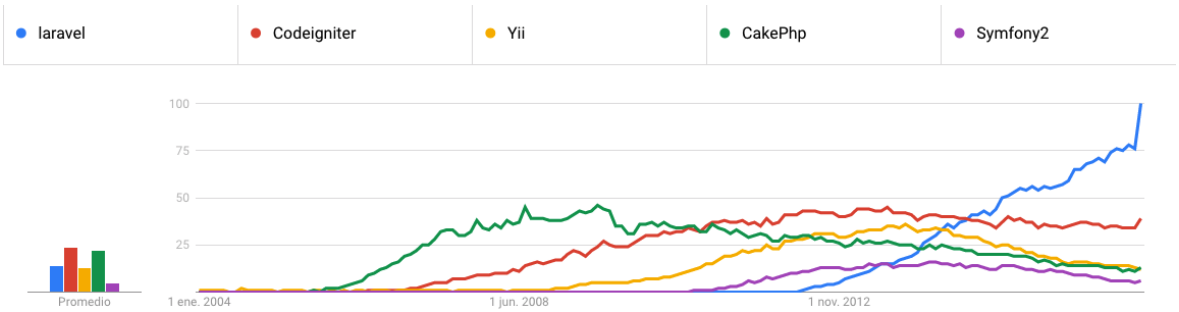

Fuente: ValueCoders. Compañía India de Outsourcing de TI para servicios de desarrollo de software offshore [imagen]. ValueCors. 2019. [Consultado: 26 de noviembre de 2019]. Disponible en: https://www.valuecoders.com/

La siguiente ilustración nos permite ver cómo ha ido progresando en la herramienta Laravel en el transcurso de los años en cuanto respecta a otras soluciones en el marco de desarrollo de aplicaciones web serias.

[36] PATIL, Akshay. 10 razones por las que Laravel es el mejor framework PHP para 2019. Clarion Technologies [en linea]. 2019. [Consultado: 17 junio 2019]. Disponible en: https://www.clariontech.com/blog/10-reasons-why-laravel-is-the-best-php-framework-for-2019

[37] MALHOTRA, Mantra. ¿Por qué laravel es el mejor marco php en 2019? Valuecoders [sitio web]. 2019, marzo. [Consultado: 17 junio 2019]. Disponible en: https://www.valuecoders.com/blog/technology-and-apps/laravel-best-php-framework-2017/

Figura 34. Grafica de aceptación de librerías framework




Fuente: RODRÍGUEZ Francisco, De 5, este es el mejor y más joven: Laravel [imagen]. 2017 [Consultado: 26 de noviembre de 2019]. Disponible en: https://medium.com/oja-la/de-5-este-es-el-mejor-y-más-joven-laravel-7b40d5f9dcb0

## CONCLUSIONES

En este trabajo se demostró la implantación de seguridad lógica usando entornos de desarrollo en aplicaciones web empresariales, mediante el framework o librería de desarrollo de aplicaciones web LARAVEL para minimizar o eliminar la mayor cantidad de exploits o vulnerabilidades posibles.

Lo más relevante del objetivo a conseguir en la investigación es demostrar cuál de las 2 perspectivas o enfoques es la óptima porque, a pesar de que no es una necesidad como tal escoger entre una o la otra, el desarrollador al momento de prestar sus servicios, si desea mantenerse comercialmente competitivo ha de elegir la mejor estrategia de trabajo.

Después de un background en programación, pasando desde lenguaje ensamblador, java, visual basic, php, HTML, Css, c++ y otros lenguajes porque esta experiencia se genera el siguiente cuestionamiento, antes de tan siquiera conocer el término “purista”, si existen mejores formas más optimas, métodos más agiles, para construir cualquier aplicación en menos tiempo, mayor rendimiento y con todos los requisitos necesarios para considerarse el objeto de desarrollo como una aplicación sólida.

Claramente se observa la cantidad de mejoras he implementaciones dadas por los desarrolladores de la herramienta LARAVEL, la comparativa entre un desarrollo sin un framework vs desarrollo con un framework de desarrollo. Podemos observar las mejoras en rendimiento y seguridad en el código implementado. Profundización en los mecanismos de seguridad disponibles en el entorno de trabajo. La solución a múltiples debilidades en los intérpretes de bases de datos, estructura de transferencia de información y las incontables oportunidades que se encuentran todos los días, no solo en el área del rendimiento, en el área de la seguridad garantizan una disminución en las aperturas, a nivel de software, en la estructura informática.

La descripción de usuarios antiguos en el desarrollo de aplicaciones web y sus experiencias en este campo, son garantías del trabajo especializado en la herramienta mencionada, los desarrollos de sus aplicaciones se encuentran cubiertos por soluciones profesionales, es open-source y puede ser modificada y propuesta de forma gratuita. La seguridad dentro del desarrollo de las aplicaciones se encuentra actualizadas y se soportan por una gran comunidad quienes aportan libremente en su desarrollo. En conclusión, no existe la posibilidad de elaborar soluciones completas y seguras dejando de lado herramientas como la actualmente señalada.

## BIBLIOGRAFÍA


ACUNETIX. PHP Security 4: mejores prácticas de seguridad de PHP. [sitio web]. Acunetix. [Consultado: 15 septiembre 2019]. Disponible en: https://www.acunetix.com/websitesecurity/php-security-4/

ANTÓN DORANTES, C. Laravel, el mejor framework en PHP. PLATZI. [en linea]. 2015. [Consultado: 17 junio 2019]. Disponible en: https://platzi.com/blog/laravel-framework-php/

BEK, Davit. Lara Form: Paquete Laravel Form con protección contra manipulaciones de formularios. GitHub [sitio web]. 2018. [Consultado: 15 mayo 2019]. Disponible en: https://github.com/omnicode/lara-form

BOS, Bert. ¿Qué es el CSS?. W3C [sitio web]. 2019. [Consultado 26 de 10 de 2019]. Disponible en: https://www.w3.org/Style/CSS/Overview.en.html

BOS, Bert. ¿Qué es HTML?. W3C [sitio web]. 2019. [Consultado 05 de noviembre de 2019]. Disponible en: https://www.w3.org/html/

BOS, Bert. Normas. W3C [sitio web]. 2019. [Consultado: 16 noviembre 2018]. Disponible en: https://www.w3.org/html/

CORTES ROBLES, Diego. Fundamentos Básicos de Seguridad de la Información [sitio web] Seguridad y Firewall. 2016. [Consultado: 20 de enero de 2020]. Disponible en: https://www.seguridadyfirewall.cl/2016/01/fundamentos-basicos-de-seguridad-de-la.html

DE LEÓN, Á. Servidor apache. Infranetworking Internacional [sitio web]. 2019, junio. [Consultado: 17 septiembre 2019]. Disponible en: https://blog.infranetworking.com/que-es-apache-servidor/

EASY LARAVEL BOOK. Laravel 5 Prevents Sql Injection, Cross-Site Request Forgery, And Cross-Site Scripting. Easy laravel 5 [sitio web]. 2015, junio. [Consultado: 15 septiembre 2019]. Disponible en: https://www.easylaravelbook.com/blog/how-laravel-5-prevents-sql-injection-cross-site-request-forgery-and-cross-site-scripting/

ECURED. Laravel. Ecured [sitio web]. 2018. [Consultado: 15 de Mayo de 2019]. Disponible en: https://www.ecured.cu/Laravel

ECURED. Pascal. Ecured [sitio web]. 2019. [Consultado: 27 de 06 de 2019]. Disponible en: https://www.ecured.cu/Pascal

EL CONFIDENCIAL. Bancos bajo ataque: "La ciberseguridad de entidades es un festival del humor". El confidencial [sitio web]. 2018, septiembre. [Consultado 27 de 06 de 2019].

Disponible en: https://www.elconfidencial.com/tecnologia/2018-09-15/banca-online-seguridad-agujeros_1615928/

ENGIN , K. y KRUEGEL, C. Noxes: una solución del lado del cliente para mitigar los ataques de secuencias de comandos entre sitios. Digital library [sitio web]. 2006, julio. [Consultado: 12 mayo 2019]. Disponible en: https://dl.acm.org/doi/abs/10.1145/1141277.1141357

FROUFE GUTIERREZ, A. Defective code II. Pérdida de autenticación. Betabeers [sitio web]. 2018, abril. [Consultado: 12 mayo 2019]. Disponible en: https://betabeers.com/blog/defective-code-ii-perdida-autenticacion-358/

GOMEZ, A. Mi experiencia usando laravel. Steemit [sitio web]. 2017. [Consultado: 15 mayo 2019]. Disponible en: https://steemit.com/spanish/@angelggomz/mi-experiencia-usando-laravel

GUTIERREZ FROUFE, A. Defective code II. Pérdida de autenticación. Betabeers [sitio web]. 2018, abril. [Consultado: 15 julio 2019]. Disponible en: https://betabeers.com/blog/defective-code-ii-perdida-autenticacion-358/

HERNANDEZ, A. Introduccion a laravel. Meetup [sitio web]. 2018, mayo. [Consultado: 10 julio 2019]. Disponible en: https://www.meetup.com/es-ES/PHPGranada/events/250803700/

KUMAR, R. Cómo ocultar la versión de Apache y PHP de los encabezados HTTP. Tecadmin [sitio web]. 2019, septiembre. [Consultado: 20 agosto 2019]. Disponible en: https://tecadmin.net/basic-security-tips-hide-apachephp-information/

LARAVEL. Cifrado. Laravel [sitio web]. 2019. [Consultado: 20 julio 2019]. Disponible en: https://laravel.com/docs/5.7/encryption

LARAVEL. Hashing. Laravel [sitio web]. 2019. [Consultado: 20 julio 2019]. Disponible en: https://laravel.com/docs/5.7/hashing

LÓPEZ TORRALBA, M. Definición de aplicación web. Mialtoweb. [sitio web]. 2015, enero. [Consultado: 20 octubre 2019]. Disponible en: http://mialtoweb.es/definicion-de-aplicacion-web/

MALHOTRA, Mantra. ¿Por qué laravel es el mejor marco php en 2019?. Valuecoders [sitio web]. 2019, marzo. [Consultado: 17 junio 2019]. Disponible en: https://www.valuecoders.com/blog/technology-and-apps/laravel-best-php-framework-2017/

MARTÍNEZ, A. , R., & GARCÍA BELTRÁN. Breve Historia De La Informática. Monografias [sitio web]. 2000. [Consultado: 27 junio 2019]. Disponible en: https://www.monografias.com/trabajos46/la-informatica/la-informatica.shtml

MATRUNCHYK, Serhii. Las 7 razones principales por las que Laravel es mejor para las empresas que otros frameworks PHP. Medium [sitio web]. 2018, febrero. [Consultado: 16 de junio de 2019]. Disponible en: https://medium.com/@serhii.matrunchyk/top-7-reasons-why-laravel-is-better-for-businesses-than-other-php-frameworks-c0f5e85c5b85

MERCE, Molist. Bancos bajo ataque: "La ciberseguridad de las entidades es un festival del humor". El confidencial [sitio web]. 2018, septiembre. [Consultado: 16 octubre 2019]. Disponible en: https://www.elconfidencial.com/tecnologia/2018-09-15/banca-online-seguridad-agujeros_1615928/

MILLAN, José Antonio. Breve Historia de la Internet: El fruto caliente de la guerra fría [en línea]. 2006, febrero. [Consultado: 16 octubre 2018]. Disponible en: http://cv.udl.cat/cursos/elsmitjans/t1/docs/internet2.pdf

MUHAMMED DASTAGIR, Hussein. Ways for securing Laravel Application. Viblo [sitio web]. 2016, mayo. [Consultado: 16 octubre 2019]. Disponible en: https://viblo.asia/p/ways-for-securing-laravel-application-NPVMaDygRQOk

MYSQLTM. Ediciones MySQL. MySQL editions [sitio web]. 2019. [Consultado: 30 octubre 2019]. Disponible en: https://www.mysql.com/products/

NAWAZ, Shahroze. Las mejores prácticas de seguridad de PHP. Cloudways [sitio web]. 2019, junio. [Consultado: 16 octubre 2019]. Disponible en: https://www.cloudways.com/blog/php-security/

NJENGA, A. 10 marcos PHP populares en 2019. Raygun [sitio web]. 2018, noviembre. [Consultado: 15 mayo 2019 Disponible en: https://raygun.com/blog/top-php-frameworks/

ORDUZ RODRÍGUEZ, B y FIGUEROA LIZCANO, G. Análisis de seguridad contra ataques Cross site en sitios CSM aplicando la herramienta OWASAP ZAP: Caso de estudio Wordpress versión 4.7.4. [sitio web]. 2016. [Consultado: 26 noviembre 2019]. Disponible en: https://repository.ucc.edu.co/handle/20.500.12494/12961

OWASP. Control de acceso roto [sitio web]. Owasp. 2020. [Consultado: 20 de marzo de 2020]. Disponible en: https://owasp.org/www-community/Broken_Access_Control

OWASP. Inyección SQL. Owasp [sitio web]. 2019. [Consultado: 12 Mayo 2019]. Disponible en: https://www.owasp.org/index.php/SQL_Injection

OWASP. Procesamiento de entidad externa XML (XXE) [sitio web]. Owasp. 2020. [Consultado: 20 de marzo de 2020]. Disponible en: https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing

OWASP. ¿Quién es la Fundación OWASP?. Owasp [sitio web]. 2019. [Consultado: 12 Mayo 2019]. Disponible en: https://www.owasp.org/index.php/Main_Page

OWASP. Top 10 2007: Las 10 vulnerabilidades de seguridad más críticas en aplicaciones web: Falla de restriccion de acceso a URL. Owasp [sitio web]. 2008 septiembre. [Consultado: 28 noviembre 2019]. Disponible en: https://owasp.org/www-pdf-archive/OWASP_Top_10_2007_Spanish.pdf

OWASP. Top 10 de Owasp. Owasp [sitio web]. 2019. [Consultado: 12 Mayo 2019]. Disponible en: https://www.owasp.org/index.php/Top_10_2007-Falla_de_restricci%C3%B3n_de_acceso_a_URL#Ejemplos

PALMA P, Cristian. Explorando la vulnerabilidad XXE: XML External Entity. Backtrack academy [sitio web]. 2017, septiembre. [Consultado: 20 Mayo 2019]. Disponible en: https://backtrackacademy.com/articulo/explorando-la-vulnerabilidad-xxe-xml-external-entity

PATIL, Akshay. 10 razones por las que Laravel es el mejor framework PHP para 2019. Clarion Technologies [en linea]. 2019. [Consultado: 17 junio 2019]. Disponible en: https://www.clariontech.com/blog/10-reasons-why-laravel-is-the-best-php-framework-for-2019

PHP.NET. Introduccion PDO. The Php Group [sitio web]. 2019. [Consultado: 22 junio 2019]. Disponible en: https://www.php.net/manual/es/intro.pdo.php

PHP.NET. Introduccion PHP. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.intro.php

PHP.NET. Inyeccion sql. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.database.sql-injection.php

PHP.NET. Modelo de almacenamiento cifrado. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.database.storage.php

PHP.NET. Seguridad en bases de datos. The PHP Group [sitio web]. 2018. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.database.php

PHP.NET. SQL injection. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.database.sql-injection.php

PONCE SUBÍA, P. Análisis de los ataques a aplicaciones web SQL Injection y Cross Site Scripting y sus medidas de precaución y defensa. [en línea]. Tesis profesional. Universidad tecnica del norte, 2018. [Consultado: 26 noviembre 2019]. Disponible en: http://repositorio.utn.edu.ec/bitstream/123456789/7803/1/04 isc 392 trabajo grado.pdf

PONCE VÁSQUEZ. Diego. Contribución al desarrollo de un entorno seguro de m-commerce [en linea]. Tesis doctoral. Universitat Politécnica de Catalunya (UPC). España, 2003. [Consultado: 16 noviembre 2018]. Disponible en: https://dialnet.unirioja.es/servlet/tesis?codigo=6403

POTENCIER , Fabian. Componentes de Symfony en Laravel. Rimorsoft Online [sitio web]. 2019. [Consultado: 20 noviembre 2019]. Disponible en: https://rimorsoft.com/componentes-symfony-en-laravel

POZO, Juan. HTML, SGML, XHTML y XML. HTML con clase [sitio web]. 2003. [Consultado 18 diciembre 2019]. Disponible en: http://html.conclase.net/articulos/xml

PROGRAMACION.NET. Los 10 tipos de desarrollador web más comunes - Parte 1. Programación en Castellano [sitio web]. Programacion.Net. 2019. [Consultado: 20 de enero de 2020]. Disponible en: https://programacion.net/articulo/los_10_tipos_de_desarrollador_web_mas_comunes_parte_1_1128

PUCHE GARCíA, Sergio. Arqueología informática: Análisis, diseño e implementación del funcionamiento del ábaco matemático con Scratch [en línea] tesis profesional. Universidad Politécnica de Valéncia, 2017 – 2018. [Consultado: 16 diciembre 2018]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/106945/PUCHE%20-%20Arqueolog%C3%ADa%20inform%C3%A1tica:%20an%C3%A1lisis,%20dise%C3%B1o%20e%20implementaci%C3%B3n%20del%20funcionamiento%20del%20%C3%A1baco%20m....pdf?sequence=1

SÁNCHEZ GONZÁLEZ, Javier. Ciberseguridad: mecanismos de ataque y defensa másextendidos. [en línea]. Tesis profesional. Universidad Politecnica de Madrid, 2016. [Consultado de noviembre 2019]. Disponible en: http://oa.upm.es/44509

Servidor HTTP Apache. Wikipedia, la enciclopedia libre [sitio web]. 2019 julio. [Consultado: 16 noviembre 2018]. Disponible en: http://es.wikipedia.org/wiki/Servidor_HTTP_Apache

TORRES VILLALTA, Alfredo David. Guía de ciberseguridad para arquitectura empresarial [En línea]. Titulo profesional. Universidad Católica de Loja. Ecuador, 2015. [Consultado 16 noviembre 2018]. Disponible en: http://dspace.utpl.edu.ec/bitstream/123456789/12665/1/torres_villalta_alfredo_david.pdf

## ANEXOS

## DIAGRAMA DE GANTS

**RESUMEN RAE**

| | |
|---|---|
| | FORMATO |
| | RESUMEN ANALÍTICO EN SEGURIDAD INFORMATICA - RAE |

| 1. Información General | |
|---|---|
| **Tipo de documento** | Monografía final de trabajo de grado |
| **Acceso al documento** | Universidad Nacional Abierta y a Distancia UNAD<br>Facultad de Ingeniería de sistemas<br>Programa de Especialización en Seguridad informática |
| **Título del documento** | SEGURIDAD LÓGICA USANDO ENTORNOS DE DESARROLLO EN APLICACIONES WEB EMPRESARIALES |
| **Autor(es)** | Alejandro David Cervantes Barragán |
| **Tutor** | Frey Jesús de Castro |
| **Publicación** | Digitado en computador |
| **Unidad Patrocinante** | Universidad Nacional Abierta y a Distancia UNAD<br>Facultad de Ingeniería de sistemas<br>Programa de Especialización en Seguridad informática |
| **Palabras Claves** | Codificación pura, Framework, Seguridad, Inyecciones Sql, Owasp, Experiencias, Laravel, Información |

| 2. Descripción |
|---|
| En la monografía el autor plantea las necesidades de los programadores informáticos al momento de realizar proyectos de software. El autor plantea la necesidad de la utilización de framework o librerías avanzadas para la gestión de trabajos informáticos. El enfoque de estas necesidades se debe a la entrega de proyectos de alto nivel para empresas multinacionales o bancos. La seguridad es una necesidad y el autor implementa profundiza en los mecanismos de seguridad que contienen herramientas como estas. En este caso la herramienta a demostrar como ejemplo es LARAVEL. Las comunidades de desarrollo son necesarias para estos proyectos ya que proseen soluciones y asistencia en el desarrollo.<br>La monografía se desarrolla bajo la metodología deductiva con el propósito de tomar las experiencias existentes y construir una conclusión. El marco histórico nos contextualiza la investigación y nos permiten proyectar al futuro. La investigación se encuentra enfocada en programadores nuevos más que en los experimentados. |

3. Fuentes

## Bibliografía


ACUNETIX. PHP Security 4: mejores prácticas de seguridad de PHP. [sitio web]. Acunetix. [Consultado: 15 septiembre 2019]. Disponible en: https://www.acunetix.com/websitesecurity/php-security-4/

ANTÓN DORANTES, C. Laravel, el mejor framework en PHP. PLATZI. [en linea]. 2015. [Consultado: 17 junio 2019]. Disponible en: https://platzi.com/blog/laravel-framework-php/

BEK, Davit. Lara Form: Paquete Laravel Form con protección contra manipulaciones de formularios. GitHub [sitio web]. 2018. [Consultado: 15 mayo 2019]. Disponible en: https://github.com/omnicode/lara-form

BOS, Bert. ¿Qué es el CSS?. W3C [sitio web]. 2019. [Consultado 26 de 10 de 2019]. Disponible en: https://www.w3.org/Style/CSS/Overview.en.html

BOS, Bert. ¿Qué es HTML?. W3C [sitio web]. 2019. [Consultado 05 de noviembre de 2019]. Disponible en: https://www.w3.org/html/

BOS, Bert. Normas. W3C [sitio web]. 2019. [Consultado: 16 noviembre 2018]. Disponible en: https://www.w3.org/html/

CORTES ROBLES, Diego. Fundamentos Básicos de Seguridad de la Información [sitio web] Seguridad y Firewall. 2016. [Consultado: 20 de enero de 2020]. Disponible en: https://www.seguridadyfirewall.cl/2016/01/fundamentos-basicos-de-seguridad-de-la.html

DE LEÓN, Á. Servidor apache. Infranetworking Internacional [sitio web]. 2019, junio. [Consultado: 17 septiembre 2019]. Disponible en: https://blog.infranetworking.com/que-es-apache-servidor/

EASY LARAVEL BOOK. Laravel 5 Prevents Sql Injection, Cross-Site Request Forgery, And Cross-Site Scripting. Easy laravel 5 [sitio web]. 2015, junio. [Consultado: 15 septiembre 2019]. Disponible en: https://www.easylaravelbook.com/blog/how-laravel-5-prevents-sql-injection-cross-site-request-forgery-and-cross-site-scripting/

ECURED. Laravel. Ecured [sitio web]. 2018. [Consultado: 15 de Mayo de 2019]. Disponible en: https://www.ecured.cu/Laravel

ECURED. Pascal. Ecured [sitio web]. 2019. [Consultado: 27 de 06 de 2019]. Disponible en: https://www.ecured.cu/Pascal

EL CONFIDENCIAL. Bancos bajo ataque: "La ciberseguridad de entidades es un festival del humor". El confidencial [sitio web]. 2018, septiembre. [Consultado 27 de 06 de 2019]. Disponible en: https://www.elconfidencial.com/tecnologia/2018-09-15/banca-online-seguridad-agujeros_1615928/

ENGIN , K. y KRUEGEL, C. Noxes: una solución del lado del cliente para mitigar los ataques de secuencias de comandos entre sitios. Digital library [sitio web]. 2006, julio. [Consultado: 12 mayo 2019]. Disponible en: https://dl.acm.org/doi/abs/10.1145/1141277.1141357

FROUFE GUTIERREZ, A. Defective code II. Pérdida de autenticación. Betabeers [sitio web]. 2018, abril. [Consultado: 12 mayo 2019]. Disponible en: https://betabeers.com/blog/defective-code-ii-perdida-autenticacion-358/

GOMEZ, A. Mi experiencia usando laravel. Steemit [sitio web]. 2017. [Consultado: 15 mayo 2019]. Disponible en: https://steemit.com/spanish/@angelggomz/mi-experiencia-usando-laravel

GUTIERREZ FROUFE, A. Defective code II. Pérdida de autenticación. Betabeers [sitio web]. 2018, abril. [Consultado: 15 julio 2019]. Disponible en: https://betabeers.com/blog/defective-code-ii-perdida-autenticacion-358/

HERNANDEZ, A. Introduccion a laravel. Meetup [sitio web]. 2018, mayo. [Consultado: 10 julio 2019]. Disponible en: https://www.meetup.com/es-ES/PHPGranada/events/250803700/

KUMAR, R. Cómo ocultar la versión de Apache y PHP de los encabezados HTTP. Tecadmin [sitio web]. 2019, septiembre. [Consultado: 20 agosto 2019]. Disponible en: https://tecadmin.net/basic-security-tips-hide-apachephp-information/

LARAVEL. Cifrado. Laravel [sitio web]. 2019. [Consultado: 20 julio 2019]. Disponible en: https://laravel.com/docs/5.7/encryption

LARAVEL. Hashing. Laravel [sitio web]. 2019. [Consultado: 20 julio 2019]. Disponible en: https://laravel.com/docs/5.7/hashing

LÓPEZ TORRALBA, M. Definición de aplicación web. Mialtoweb. [sitio web]. 2015, enero. [Consultado: 20 octubre 2019]. Disponible en: http://mialtoweb.es/definicion-de-aplicacion-web/

MALHOTRA, Mantra. ¿Por qué laravel es el mejor marco php en 2019?. Valuecoders [sitio web]. 2019, marzo. [Consultado: 17 junio 2019]. Disponible en:

https://www.valuecoders.com/blog/technology-and-apps/laravel-best-php-framework-2017/

MARTÍNEZ, A. , R., & GARCÍA BELTRÁN. Breve Historia De La Informática. Monografias [sitio web]. 2000. [Consultado: 27 junio 2019]. Disponible en: https://www.monografias.com/trabajos46/la-informatica/la-informatica.shtml

MATRUNCHYK, Serhii. Las 7 razones principales por las que Laravel es mejor para las empresas que otros frameworks PHP. Medium [sitio web]. 2018, febrero. [Consultado: 16 de junio de 2019]. Disponible en: https://medium.com/@serhii.matrunchyk/top-7-reasons-why-laravel-is-better-for-businesses-than-other-php-frameworks-c0f5e85c5b85

MERCE, Molist. Bancos bajo ataque: "La ciberseguridad de las entidades es un festival del humor". El confidencial [sitio web]. 2018, septiembre. [Consultado: 16 octubre 2019]. Disponible en: https://www.elconfidencial.com/tecnologia/2018-09-15/banca-online-seguridad-agujeros_1615928/

MILLAN, José Antonio. Breve Historia de la Internet: El fruto caliente de la guerra fría [en línea]. 2006, febrero. [Consultado: 16 octubre 2018]. Disponible en: http://cv.udl.cat/cursos/elsmitjans/t1/docs/internet2.pdf

MUHAMMED DASTAGIR, Hussein. Ways for securing Laravel Application. Viblo [sitio web]. 2016, mayo. [Consultado: 16 octubre 2019]. Disponible en: https://viblo.asia/p/ways-for-securing-laravel-application-NPVMaDygRQOk

MYSQLTM. Ediciones MySQL. MySQL editions [sitio web]. 2019. [Consultado: 30 octubre 2019]. Disponible en: https://www.mysql.com/products/

NAWAZ, Shahroze. Las mejores prácticas de seguridad de PHP. Cloudways [sitio web]. 2019, junio. [Consultado: 16 octubre 2019]. Disponible en: https://www.cloudways.com/blog/php-security/

NJENGA, A. 10 marcos PHP populares en 2019. Raygun [sitio web]. 2018, noviembre. [Consultado: 15 mayo 2019 Disponible en: https://raygun.com/blog/top-php-frameworks/

ORDUZ RODRÍGUEZ, B y FIGUEROA LIZCANO, G. Análisis de seguridad contra ataques Cross site en sitios CSM aplicando la herramienta OWASAP ZAP: Caso de estudio Wordpress versión 4.7.4. [sitio web]. 2016. [Consultado: 26 noviembre 2019]. Disponible en: https://repository.ucc.edu.co/handle/20.500.12494/12961

OWASP. Control de acceso roto [sitio web]. Owasp. 2020. [Consultado: 20 de marzo de 2020]. Disponible en: https://owasp.org/www-community/Broken_Access_Control

OWASP. Inyección SQL. Owasp [sitio web]. 2019. [Consultado: 12 Mayo 2019]. Disponible en: https://www.owasp.org/index.php/SQL_Injection

OWASP. Procesamiento de entidad externa XML (XXE) [sitio web]. Owasp. 2020. [Consultado: 20 de marzo de 2020]. Disponible en: https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing

OWASP. ¿Quién es la Fundación OWASP?. Owasp [sitio web]. 2019. [Consultado: 12 Mayo 2019]. Disponible en: https://www.owasp.org/index.php/Main_Page

OWASP. Top 10 2007: Las 10 vulnerabilidades de seguridad más críticas en aplicaciones web: Falla de restriccion de acceso a URL. Owasp [sitio web]. 2008 septiembre. [Consultado: 28 noviembre 2019]. Disponible en: https://owasp.org/www-pdf-archive/OWASP_Top_10_2007_Spanish.pdf

OWASP. Top 10 de Owasp. Owasp [sitio web]. 2019. [Consultado: 12 Mayo 2019]. Disponible en: https://www.owasp.org/index.php/Top_10_2007-Falla_de_restricci%C3%B3n_de_acceso_a_URL#Ejemplos

PALMA P, Cristian. Explorando la vulnerabilidad XXE: XML External Entity. Backtrack academy [sitio web]. 2017, septiembre. [Consultado: 20 Mayo 2019]. Disponible en: https://backtrackacademy.com/articulo/explorando-la-vulnerabilidad-xxe-xml-external-entity

PATIL, Akshay. 10 razones por las que Laravel es el mejor framework PHP para 2019. Clarion Technologies [en linea]. 2019. [Consultado: 17 junio 2019]. Disponible en: https://www.clariontech.com/blog/10-reasons-why-laravel-is-the-best-php-framework-for-2019

PHP.NET. Introduccion PDO. The Php Group [sitio web]. 2019. [Consultado: 22 junio 2019]. Disponible en: https://www.php.net/manual/es/intro.pdo.php

PHP.NET. Introduccion PHP. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.intro.php

PHP.NET. Inyeccion sql. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.database.sql-injection.php

PHP.NET. Modelo de almacenamiento cifrado. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.database.storage.php

PHP.NET. Seguridad en bases de datos. The PHP Group [sitio web]. 2018. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.database.php

PHP.NET. SQL injection. The PHP Group [sitio web]. 2019. [Consultado: 20 junio 2019]. Disponible en: https://www.php.net/manual/es/security.database.sql-injection.php

PONCE SUBÍA, P. Análisis de los ataques a aplicaciones web SQL Injection y Cross Site Scripting y sus medidas de precaución y defensa. [en línea]. Tesis profesional. Universidad tecnica del norte, 2018. [Consultado: 26 noviembre 2019]. Disponible en: http://repositorio.utn.edu.ec/bitstream/123456789/7803/1/04 isc 392 trabajo grado.pdf

PONCE VÁSQUEZ. Diego. Contribución al desarrollo de un entorno seguro de m-commerce [en linea]. Tesis doctoral. Universitat Politécnica de Catalunya (UPC). España, 2003. [Consultado: 16 noviembre 2018]. Disponible en: https://dialnet.unirioja.es/servlet/tesis?codigo=6403

POTENCIER , Fabian. Componentes de Symfony en Laravel. Rimorsoft Online [sitio web]. 2019. [Consultado: 20 noviembre 2019]. Disponible en: https://rimorsoft.com/componentes-symfony-en-laravel

POZO, Juan. HTML, SGML, XHTML y XML. HTML con clase [sitio web]. 2003. [Consultado 18 diciembre 2019]. Disponible en: http://html.conclase.net/articulos/xml

PROGRAMACION.NET. Los 10 tipos de desarrollador web más comunes - Parte 1. Programación en Castellano [sitio web]. Programacion.Net. 2019. [Consultado: 20 de enero de 2020]. Disponible en: https://programacion.net/articulo/los_10_tipos_de_desarrollador_web_mas_comunes_parte_1_1128

PUCHE GARCíA, Sergio. Arqueología informática: Análisis, diseño e implementación del funcionamiento del ábaco matemático con Scratch [en línea] tesis profesional. Universidad Politécnica de Valéncia, 2017 – 2018. [Consultado: 16 diciembre 2018]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/106945/PUCHE%20-%20Arqueolog%C3%ADa%20inform%C3%A1tica:%20an%C3%A1lisis,%20dise%C3%B1o%20e%20implementaci%C3%B3n%20del%20funcionamiento%20del%20%C3%A1baco%20m....pdf?sequence=1

SÁNCHEZ GONZÁLEZ, Javier. Ciberseguridad: mecanismos de ataque y defensa másextendidos. [en línea]. Tesis profesional. Universidad Politecnica de Madrid, 2016. [Consultado de noviembre 2019]. Disponible en: http://oa.upm.es/44509

Servidor HTTP Apache. Wikipedia, la enciclopedia libre [sitio web]. 2019 julio. [Consultado: 16 noviembre 2018]. Disponible en: http://es.wikipedia.org/wiki/Servidor_HTTP_Apache

TORRES VILLALTA, Alfredo David. Guía de ciberseguridad para arquitectura empresarial [En línea]. Titulo profesional. Universidad Católica de Loja. Ecuador, 2015. [Consultado 16 noviembre 2018]. Disponible en: http://dspace.utpl.edu.ec/bitstream/123456789/12665/1/torres_villalta_alfredo_david.pdf

## 4. Contenidos

La monografía presenta una propuesta que busca mejorar el desarrollo de software de alta calidad. Enseñar a los nuevos desarrolladores de software mejores prácticas para obtener aplicaciones de alto nivel. Enfatizando en la seguridad ante todo y en los mecanismos de seguridad.
La monografía se divide en:

1. Introducción
2. Resumen
3. Planteamiento del problema: Se evidencian las dificultades que existen ante el desarrollo de software de calidad.
4. Preguntas de investigación
5. Justificación: Muestra la importancia que posee la implementación de herramientas avanzadas.
6. Objetivo general: En base al problema se plantea la solución o demostración.
7. Objetivos específicos: Se especifican como se demuestra la solución.
8. Marco Histórico: Contextualización de la investigación.
9. Marco teórico: Solución al planteamiento del problema.
10. Marco conceptual: Conceptualización de la investigación.
11. Conclusiones: Realimentación final de la investigación.
12. Bibliografía: Referencias bibliográficas que soportan la investigación.
13. Anexos: Resumen rae y plan de trabajo del proyecto.

## 5. Metodología

1. Desarrollo del planteamiento del problema con el objetivo de ver de forma global el problema.
2. Planteamiento de las preguntas los objetivos generales y específicos para centralizar la investigación.
3. Repaso de la historia y conceptos generales que se usan en la investigación. Tales como el modelo MVC (Modelo Vista Controlador), tipos de ataques informáticos, la estructura interna de un sitio web y un repaso a la historia de la informática web.
4. Desarrollo de los objetivos generales y específicos para la resolución de las preguntas de investigación. Ejemplo de comparación de desarrollo entre enfoques de desarrollo, Mecanismos de seguridad y experiencias profesionales.
5. Finalización en conclusiones.

## 6. Conclusiones

En este trabajo se demostró la implantación de seguridad lógica usando entornos de desarrollo en aplicaciones web empresariales, mediante el framework o librería de desarrollo de aplicaciones web LARAVEL para minimizar o eliminar la mayor cantidad de exploits o vulnerabilidades posibles.

Lo más relevante del objetivo a conseguir en la investigación es demostrar cuál de las 2 perspectivas o enfoques es la óptima porque, a pesar de que no es una necesidad como tal escoger entre una o la otra, el desarrollador al momento de prestar sus servicios, si desea mantenerse comercialmente competitivo ha de elegir la mejor estrategia de trabajo.

Después de un background en programación, pasando desde lenguaje ensamblador, java, visual basic, php, HTML, Css, c++ y otros lenguajes porque esta experiencia se genera el siguiente cuestionamiento, antes de tan siquiera conocer el término “purista”, si existen mejores formas más optimas, métodos más agiles, para construir cualquier aplicación en menos tiempo, mayor rendimiento y con todos los requisitos necesarios para considerarse el objeto de desarrollo como una aplicación sólida.

Claramente se observa la cantidad de mejoras he implementaciones dadas por los desarrolladores de la herramienta LARAVEL, la comparativa entre un desarrollo sin un framework vs desarrollo con un framework de desarrollo. Podemos observar las mejoras en rendimiento y seguridad en el código implementado. Profundización en los mecanismos de seguridad disponibles en el entorno de trabajo. La solución a múltiples debilidades en los intérpretes de bases de datos, estructura de transferencia de información y las incontables oportunidades que se encuentran todos los días, no solo en el área del rendimiento, en el área de la seguridad garantizan una disminución en las aperturas, a nivel de software, en la estructura informática.

La descripción de usuarios antiguos en el desarrollo de aplicaciones web y sus experiencias en este campo, son garantías del trabajo especializado en la herramienta mencionada, los desarrollos de sus aplicaciones se encuentran cubiertos por soluciones profesionales, es open-source y puede ser modificada y propuesta de forma gratuita. La seguridad dentro del desarrollo de las aplicaciones se encuentra actualizadas y se soportan por una gran comunidad quienes aportan libremente en su desarrollo. En conclusión, no existe la posibilidad de elaborar soluciones completas y seguras dejando de lado herramientas como la actualmente señalada.

| | |
|---|---|
| Elaborado por: | Alejandro David Cervantes Barragán |
| Revisado por: | Yesnir Antonio Redondo Daniel |

| | | | |
|---|---|---|---|
| Fecha de elaboración del Resumen: | 04 | 03 | 2020 |