Tabla de contenido

1.- Portada 2

2.- Título 3

3.- Introducción 3

4.- Planteamiento del problema 4

5.- Justificación 6

6.- Objetivos 6

7.- Antecedentes 7

8.- Hipótesis 8

9.- Metodología 8

10.- Recursos materiales y humanos 9

11.- Alcances o metas 10

12.- Cronograma 10

13.- Bibliografías 11

# 1.- Portada



UNIVERSIDAD AUTÓNOMA DE ZACATECAS

UNIDAD ACADÉMICA DE INGENIERÍA ELECTRICA

TITULO: BUENAS PRÁCTICAS EN EL DESARROLLO Y DESPLIEGUE DE APLICACIONES WEB USANDO DJANGO, CON UN ENFOQUE EN SEGURIDAD.

INGENIERÍA DE SOFTWARE

Alumno: Manuel Herrera Lara

Zacatecas, Zac., a 18/10/2020

# 

# 2.- Título

BUENAS PRÁCTICAS EN EL DESARROLLO Y DESPLIEGUE DE APLICACIONES WEB USANDO DJANGO, CON UN ENFOQUE EN SEGURIDAD.

# 3.- Introducción

El enfoque de este estudio es identificar cuáles son las buenas prácticas de desarrollo y despliegue de aplicaciones web usando el framework Django; así como recopilarlas, describirlas y/o conceptualizarlas con la finalidad, de que los desarrolladores web que están empezando a trabajar con este framework logren minimizar los errores y vulnerabilidades de seguridad en los datos para las aplicaciones que van a construir. Lo que nos motiva a realizar esta investigación es crear aplicaciones web más eficientes, seguras y confiables al hacer uso de las buenas prácticas para disminuir el esfuerzo de desarrollo y tiempo de desarrollo, asi como minimizar los errores y vulnerabilidades de seguridad en los datos.

En la actualidad ha habido un incremento exponencial en el desarrollo de aplicaciones web; las cuales contienen información muy sensible y están expuestas a correr altos riesgos de seguridad; por lo que generalmente solemos culpar de las grandes fallas y/o vulnerabilidades de seguridad que las aplicaciones web presentan, a los sistemas de protección de servidores, malas configuraciones y a los lenguales o frameworks de programación; cuando en realidad gran parte de las fallas de seguridad son producidas por las malas prácticas de desarrollo y despliegue que emplearon los programadores web.

Según el proyecto OWASP (Proyecto de Seguridad De Aplicaciones Web Abiertas) hay varias vulnerabilidades y riesgos de seguridad que las aplicaciones web presentan actualmente; por lo cual nos enfocaremos en identificar y recopilar las buenas prácticas de desarrollo y despliegue que logren contrarrestar o minimizar los riesgos y vulnerabilidades que nos menciona el proyecto OWASP.

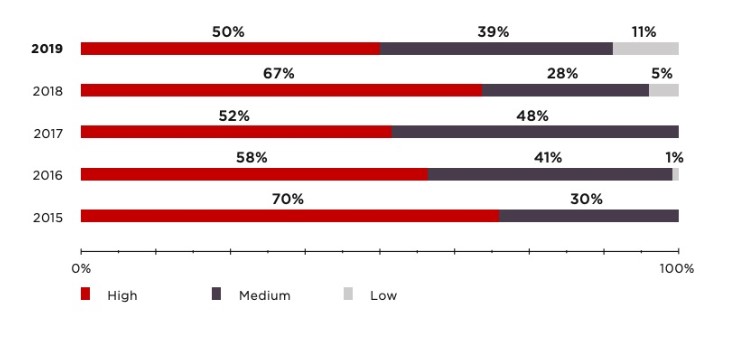
# 4.- Planteamiento del problema

En los últimos años, las aplicaciones web han tenido un gran incremento en su desarrollo y se han convertido en una parte central de nuestras vidas, tanto a nivel académico como privado. Estas aplicaciones comparten y procesan datos confidenciales del usuario que debemos protegerlos con todos los medios. Por lo tanto, estas aplicaciones son objetivos atractivos para los atacantes y suponen un alto riesgo de seguridad en los datos para los programadores web que desarrollan y despliegan aplicaciones sin seguir las buenas prácticas. (Michael Felderer, 2019) señala que “en la actualidad más del 90% de las aplicaciones web son vulnerables, con una mediana de 13 vulnerabilidades por aplicación”. Por lo tanto, la seguridad juega un papel muy importante para las aplicaciones web y según la empresa especializada en seguridad informática Positive Technologies:

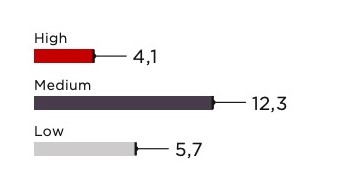
* Los piratas informáticos pueden atacar a los usuarios en 9 de cada 10 aplicaciones web.
* El acceso no autorizado a las aplicaciones web es posible en el 39% de los sitios.
* Las violaciones de datos confidenciales fueron una amenaza en el 68% de las aplicaciones web.

Y también nos indica que el 82% de las vulnerabilidades se encuentran en el código de la aplicación y una de cada cinco vulnerabilidades tiene una gravedad alta. Como resultados estadísticos nos podemos apoyar de los siguientes gráficos:

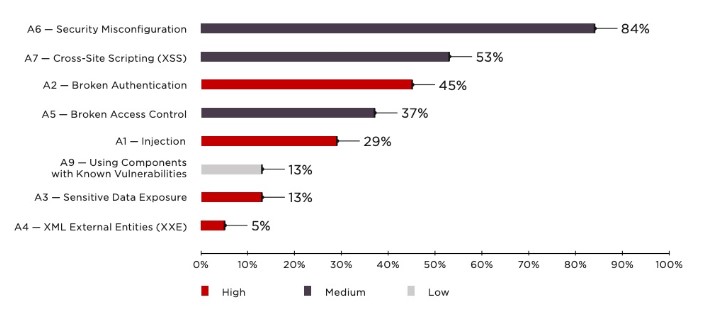
**Porcentaje de aplicaciones web que contienen vulnerabilidades de alto riesgo.**



**Número promedio de vulnerabilidades por aplicación.**



**Vulnerabilidades más comunes según el proyecto OWASP y su porcentaje en aplicaciones web.**



# 

# 5.- Justificación

Esta investigación servirá para que los programadores web que estén comenzando a trabajar con el framework Django tengan una guía de apoyo con información accesible sobre las buenas prácticas de desarrollo y despliegue de aplicaciones web; y para que a la vez puedan combinar estas prácticas con un buen código estandarizado como lo es el caso del estándar PEP8 en Python y así logren construir aplicaciones web más sólidas, confiables y seguras.

Entre los principales beneficios esta contrarrestar y minimizar el top 10 de vulnerabilidades y riesgos que nos menciona el proyecto OWASP, asi como lograr que los programadores web que están iniciando a trabajar con Django mejoren su esfuerzo de desarrollo y disminuyan su tiempo de desarrollo; y también que logren crear aplicaciones web de calidad con una buena seguridad e integridad en los datos. Lo que se pretende principalmente con esta guía es minimizar los altos riesgos de seguridad en los datos a los que se enfrentan las aplicaciones web actualmente.

# 6.- Objetivos

Objetivo General: Identificar cuáles son las buenas prácticas al desarrollar y desplegar aplicaciones web en la actualidad usando el framework web Django; para minimizar los errores y vulnerabilidades de seguridad en los datos, que se generan en estas etapas, asi como los principales riesgos de seguridad que presentan las aplicaciones web actualmente, según como lo indica el proyecto OWASP.

Objetivos Específicos:

* Investigar sobre las principales vulnerabilidades o amenazas de seguridad que presentan las aplicaciones web en la actualidad.
* Buscar y recopilar las buenas prácticas de desarrollar una aplicación web con Django y que a la vez logran contrarrestar los principales riesgos de seguridad que nos indica el proyecto OWASP.
* Buscar y recopilar las buenas prácticas de desplegar una aplicación web con Django para minimizar los riesgos de seguridad que nos indica el proyecto OWASP.

# 

# 7.- Antecedentes

El proyecto OWASP ha desarrollado durante varios años una guía completa para probar la seguridad de las aplicaciones web. La Guía de pruebas describe en detalle tanto el framework de prueba general como las técnicas necesarias para implementar el framework en la práctica. El objetivo de la guía es ayudar a las personas a comprender el qué, por qué, cuándo, dónde y cómo probar aplicaciones web. Este framework o guía ayuda a las organizaciones a probar sus aplicaciones web para construir software confiable y seguro. Esta guía de pruebas está enfocada a todas las posibles funcionalidades que contiene una aplicación web y a diferencia de lo que nosotros planteamos conseguir; es que nosotros nos enfocamos en abordar las buenas prácticas de desarrollo y despliegue en un framework específico para contrarrestar o minimizar las vulnerabilidades más comunes que presenta una aplicación web actualmente.

(Sönmez, 2019) provee una lista personalizada de elementos relacionados con el desarrollo de aplicaciones web que facilitarán las comprobaciones de análisis de cumplimiento de OWASP.

(Salas-Zárate et al., 2015) proporciona una comparación de ocho frameworks web en términos de sus mejores prácticas. El uso de las mejores prácticas permite el desarrollo de aplicaciones web mejores y más eficientes. Y dice que las aplicaciones web se desarrollaron de manera interactiva, intuitiva y segura, mejorando el esfuerzo de desarrollo y reduciendo el tiempo de desarrollo. Por lo tanto, las mejores prácticas son esenciales para la comunidad de ingenieros de software, ya que ayudan a disminuir los errores en la fase de implementación.

# 8.- Hipótesis

Algunas de las preguntas que resolveremos son las siguientes:

Q1: ¿Cuáles son los principales riesgos de seguridad en una aplicación web en la actualidad?

Q2: ¿Cuáles son las buenas prácticas en el desarrollo de una aplicación web para minimizar o prevenir los principales riesgos de seguridad?

Q3: ¿Cuáles son las buenas prácticas en el despliegue de una aplicación web para minimizar o prevenir los principales riesgos de seguridad?

Por lo tanto, una vez terminada la investigación resolveremos las preguntas anteriores y proporcionaremos una guía con las buenas prácticas, la cual nos servirá para minimizar las vulnerabilidades y ataques que presentan las aplicaciones web actualmente.

# 9.- Metodología

BUENAS PRÁCTICAS EN EL DESARROLLO Y DESPLIEGUE DE APLICACIONES WEB, CON UN ENFOQUE EN SEGURIDAD.

|  |  |  |
| --- | --- | --- |
| **OBJETIVO GENERAL** | **OBJETIVOS ESPECÍFICOS** | **OBJETIVOS METODOLÓGICOS** |
| : Identificar cuáles son las buenas prácticas al desarrollar y desplegar aplicaciones web en la actualidad usando el framework web Django; para minimizar los errores y vulnerabilidades de seguridad en los datos, que se generan en estas etapas, asi como los principales riesgos de seguridad que presentan las aplicaciones web actualmente, según como lo indica el proyecto OWASP. | 1.- Investigar sobre las principales vulnerabilidades o amenazas de seguridad que presentan las aplicaciones web en la actualidad.  2.- Buscar y recopilar las buenas prácticas de desarrollar una aplicación web con Django y que a la vez logran contrarrestar los principales riesgos de seguridad que nos indica el proyecto OWASP.  3.- Buscar y recopilar las buenas prácticas de desplegar una aplicación web con Django para minimizar los riesgos de seguridad que nos indica el proyecto OWASP. | * 1. revisar el top 10 de los riesgos de seguridad en el proyecto OWASP.   2. leer artículos especializados en seguridad de aplicaciones web de 2013 a 2020.   1.3 resumir la información relevante de los artículos de seguridad y del proyecto OWASP.   * 1. almacenar la información de las vulnerabilidades y/o amenazas más comunes y las referencias en un reporte.   2.1 leer artículos de 2013 a 2020 relacionados con las buenas prácticas en desarrollo web.  2.2 almacenar en un reporte información relevante de las buenas prácticas.  3.1 leer artículos de 2013 a 2020 sobre la seguridad en el despliegue de aplicaciones web.  3.2 almacenar en un reporte información relevante sobre las buenas prácticas de deployment. |
|  |  |  |

# 10.- Recursos materiales y humanos

Se estarán revisando artículos de revista, capítulos de libros, reportes, etc. especializados en la seguridad de aplicaciones web y sus buenas practicas; y a la vez se estará consultando información con un programador web que tiene bastante experiencia en el área de desarrollo y despliegue de software.

# 11.- Alcances o metas

Al término de la investigación se tendrá un reporte o guía con las buenas prácticas de desarrollo y despliegue de aplicaciones web usando el framework Django, estas buenas practicas podrán contrarrestar o minimizar los vulnerabilidades y amenazas que presentan las aplicaciones web actualmente y también les ayudará a los programadores web que estén trabajando con Django a crear aplicaciones web más seguras y confiables.

Que los programadores que están empezando a desarrollar app en Django tengan una buena guía de referencia para mitigar las principales vulnerabilidades de seguridad más comunes.

# 12.- Cronograma



# 13.- Bibliografías

Marashdih, A. W., Zaaba, Z. F., Suwais, K., & Mohd, N. A. (2019). Web Application Security: An Investigation on Static Analysis with other Algorithms to Detect Cross Site Scripting. *Procedia Computer Science*, *161*, 1173–1181. https://doi.org/https://doi.org/10.1016/j.procs.2019.11.230

Michael Felderer. (2019). *Knowledge-based security testing of web applications by logic programming*.

Mouli, V. R., & Jevitha, K. P. (2016). Web Services Attacks and Security- A Systematic Literature Review. *Procedia Computer Science*, *93*, 870–877. https://doi.org/https://doi.org/10.1016/j.procs.2016.07.265

Salas-Zárate, M. del P., Alor-Hernández, G., Valencia-García, R., Rodríguez-Mazahua, L., Rodríguez-González, A., & López Cuadrado, J. L. (2015). Analyzing best practices on Web development frameworks: The lift approach. *Science of Computer Programming*, *102*, 1–19. https://doi.org/https://doi.org/10.1016/j.scico.2014.12.004

Sönmez, F. Ö. (2019). Security Qualitative Metrics for Open Web Application Security Project Compliance. *Procedia Computer Science*, *151*, 998–1003. https://doi.org/https://doi.org/10.1016/j.procs.2019.04.140

Suppan, M. B. K. (2014). Modeling Security Features of Web Applications. *Springer, Cham*. https://link.springer.com/chapter/10.1007/978-3-319-07452-8\_5

OWASP, T.: Top 10–2019–the ten most critical web application security risks. The Open Web Application Security Project (2019).

web-security-testing-guide/stable/4-Web\_Application\_Security\_Testing/02-Configuration\_and\_Deployment\_Management\_Testing/03Test\_File\_Extensions\_Handling\_for\_Sensitive\_Information.html

<https://owasp.org/www-project-top-ten/>

<https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/>