# Introducción

## Resumen

El objetivo de este proyecto es desarrollar un escáner de vulnerabilidades para aplicaciones web que pueda, de manera automática y con mínima intervención del usuario, escanear una aplicación web y generar un informe detallando las vulnerabilidades encontradas así como recomendaciones generales para mitigarlas.

El programa será tan minimalista y sencillo de utilizar como sea posible, de tal forma que una persona que carezca de conocimientos técnicos pudiera utilizarlo.

## Motivación

Una prueba de penetración, o pen-test, es un ataque controlado a un sistema con el propósito de encontrar vulnerabilidades de la manera que lo haría un atacante, para así poder neutralizarlas. Aunque es un método efectivo para encontrar fallos de seguridad, muchas compañías evitan utilizarlo debido a su alto coste, que oscila aproximadamente entre los 3500€ y 18000€.

Estudios exponen que casi la mitad de los fallos de seguridad encontrados en 2015 superaban los 450000€ en pérdidas. Una encuesta enviada a profesionales de la seguridad revela que el 24% de los encuestados había sufrido un filtrado de datos en el último año, y sin embargo el 8% de los mismos nunca realiza pruebas de penetración.

Por tanto, si bien las pruebas de penetración son costosas, las pérdidas provocadas debido a aplicaciones web inseguras son mucho más graves. El relativamente escaso presupuesto que se invierte en testeo de aplicaciones web comparado con otros tipos de prácticas de seguridad podría denotar una insuficiente concienciación acerca de la severidad de los fallos de seguridad relacionados con aplicaciones web.

El propósito de este proyecto no es tanto crear un escáner de vulnerabilidades exhaustivo de alta gama, sino concienciar acerca de la importancia de las pruebas de seguridad. Si una herramienta tan sencilla y barata es capaz de detectar vulnerabilidades en una aplicación web, un atacante habilidoso con herramientas sofisticadas podría ponerlo en peligro con mucha mayor facilidad.

## Objetivos

Este proyecto automatizará una auditoría de seguridad sencilla y generará un informe, con la ayuda del escáner de vulnerabilidades OWASP ZAP. El dispositivo probará diferentes ataques o “payloads” de manera automatizada para buscar vulnerabilidades en una aplicación web objetivo. Las aplicaciones web son susceptibles a diversos tipos de ataques, como XSS (cross-site scripting) o inyección SQL, y esto las convierte en objetivos comunes para los atacantes. Los resultados se guardarán en un documento de formato portátil (pdf) para su posterior análisis.

Si bien los resultados no serán comparables a aquellos obtenidos mediante un pen-test manual de un profesional, debería al menos ser capaz de encontrar vulnerabilidades comunes, y por un bajo precio. Si una herramienta tan simple y económica es capaz de poner en peligro un sistema, entonces debería resultar inmediatamente evidente que cualquier atacante malicioso también sería capaz de explotar esas vulnerabilidades, y tal sistema debería considerarse inseguro y poco fiable.

Además del informe, el programa ofrecerá una serie de recomendaciones generales para proteger una infraestructura pyme típica contra el tipo de ataques que realiza el programa, basándose en los tipos de vulnerabilidades encontradas en el objetivo.

Este tipo de dispositivo no está ideado para resolver los problemas encontrados, sino meramente informar sobre los mismos. De esta forma, está diseñado de tal manera que cualquier comercial debería poder utilizarlo sin requerir conocimientos técnicos previos.

Este tipo de escaneo de vulnerabilidades sencillo podría usarse para alentar a las compañías a contratar los servicios de un pen-tester profesional que pudiera remediar los problemas encontrados, así como otros problemas que un escaneo automatizado sea incapaz de encontrar, para así evitar daños financieros o el robo de datos confidenciales.