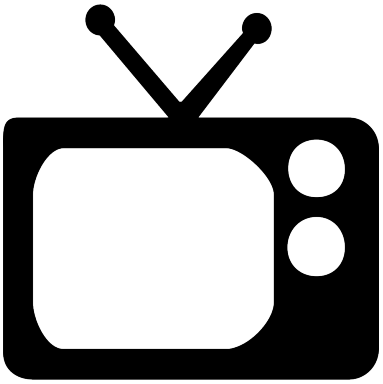

Proyecto Final

Keter Vulnerability

Índice

1. Introducción Teórica

Keter Vulnerability es una página web diseñada para representar algunos errores de configuración a la hora de crear aplicaciones web. El objetivo es disponer a los usuarios de diferentes **retos** donde deberán usar sus conocimientos y su capacidad de búsqueda a través de Internet para explotar dichas vulnerabilidades.

Figura 1: Fuente whiteknightit.com

El objetivo es ser capaces de concienciar a jóvenes **desarrolladores** del peligro que puede llevar realizar páginas web sin conciencia sobre los errores. Al final veremos como el usuario es un factor bastante peligroso para los desarrolladores y como nunca podemos confiar plenamente en sus intenciones.

Es por ello que debemos protegernos con las últimas tecnologías. Mantenernos **actualizados y activos** será la clave para evitar cualquier error.

El objetivo de esta página es su escalabilidad. Una vez terminado el proyecto la página pasará a ser código abierto, con el objetivo de que la comunidad pueda aportar sus propios retos y módulos desde GitHub. Es por ello que gran parte de los contenidos serán en inglés.

Haremos uso de las últimas tecnologías para la realización de este proyecto:

- **LaTex**: haremos uso de esta herramienta de texto mediante código para la creación de esta misma documentación.
- **NodeJS**: utilizaremos este paquete de recurso para la creación de la página web.
- **Mongo Atlas**: nos prooverá una base de datos principal para retos de NoSQL Injection.
- **HerokuApps**: será la página que hosteará nuestra aplicación.
- **GitHub**: allí subiremos el código y utilizaremos la función de GitHub Pages para crear una pequeña página web que muestre un breve resumen.
- **Docker**: crearemos un proyecto adicional con un contenedor en Docker para poder montar y utilizar nuestra aplicación en local.

2. Introducción Técnica

3. Vulnerabilidades utilizadas

4. API

5. Código

6. Explotaciones

7. Soluciones

8. Conclusión