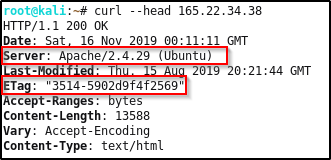
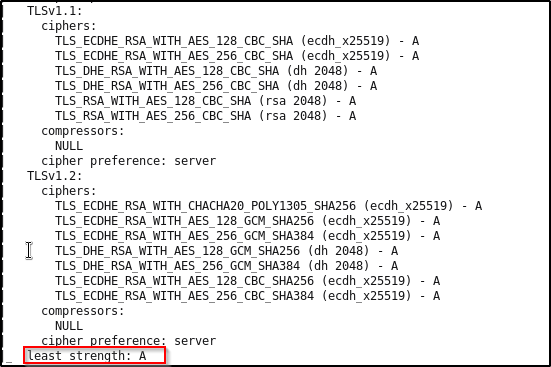
Server Header Info Disclosure (Low)



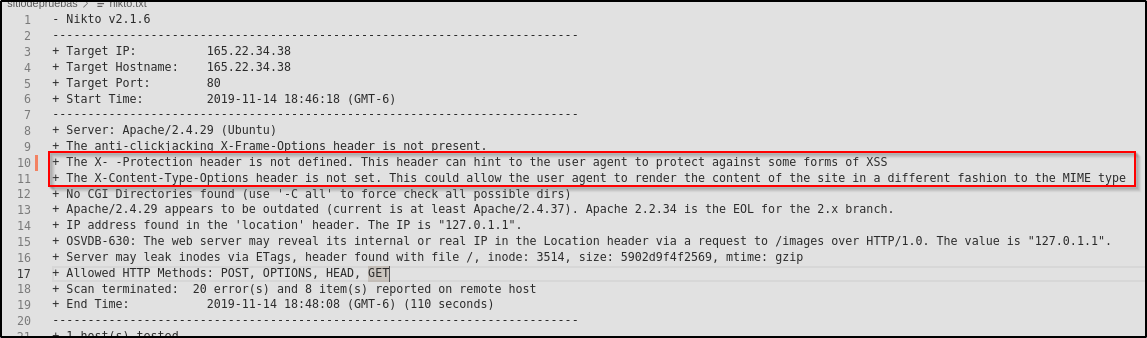
Default 404 Info Disclosure (Low)



Strong ciphers



Cross Site Scripting

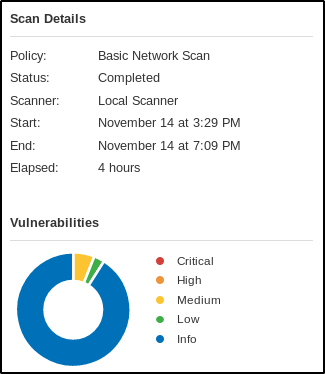


Possible vulnerable formulary:



# Nessus

La herramienta encontró diversas posibles vulnerabilidades en la página. Lo que se resume como:



## Directorios Navegables

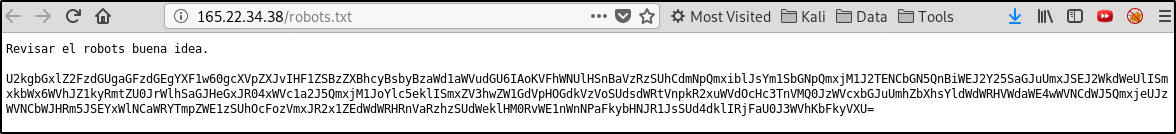


Se refiere a la falta de indexación o direccionamiento de rutas de los archivos montados en el sitio, lo que por consecuencia deriva en la indexación automática de estos por medio de la interfaz que ofrece por defecto la plataforma Apache.

El riesgo radica en la exposición de todo los directorios y archivos contenidos en esos directorios utilizados por el sitio web, lo que puede implicar la exposición de información sensible.

### Robots.txt

Este archivo se encuentra disponible para su acceso de forma pública. El archivo expone información privada respecto a una llave de acceso.

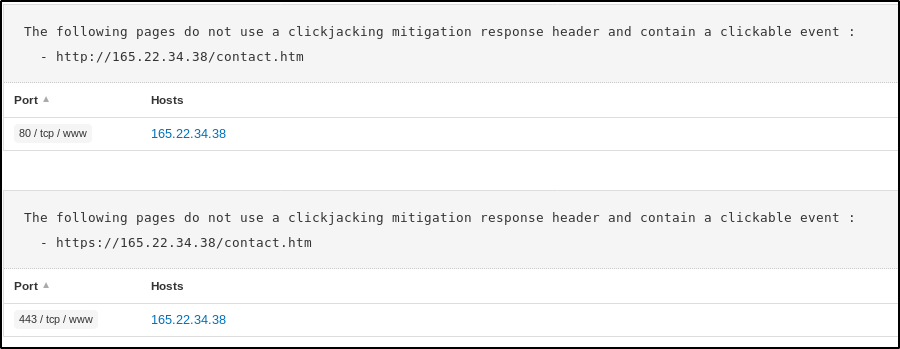


´

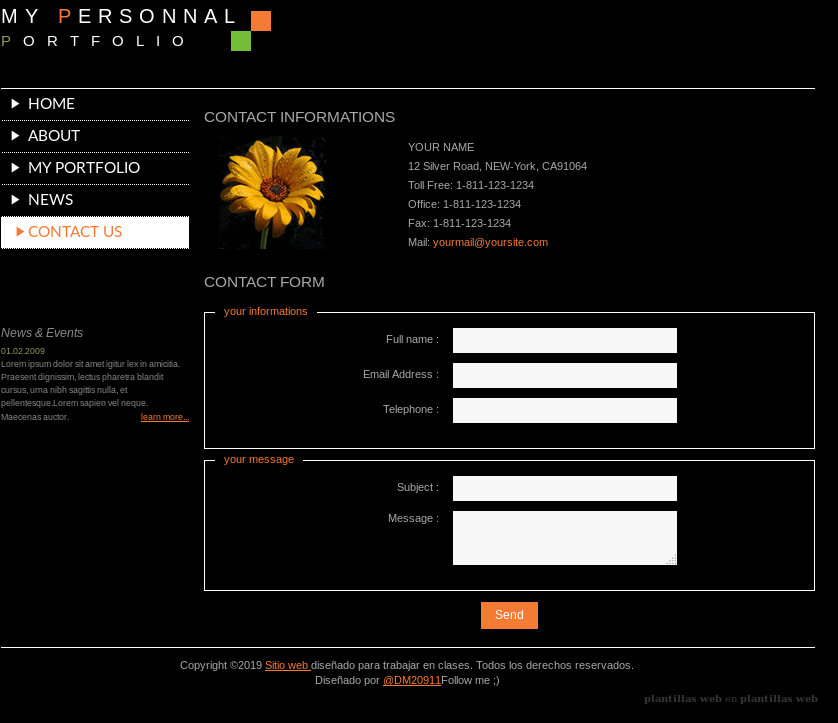
## Vulnerabilidades contra Clickjacking



Consiste en una validación que realizan los sitios web al ser cargados, que se encarga de verificar si el sitio esta siendo cargado dentro de un frame o no. Esto implica la posibilidad de poder llamar al sitio desde otro sitio utilizando un elemento de tipo frame, el cual puede configurarse para ser imperceptible para el usuario. Esto es especialmente peligroso para sitios contenedores de formularios de cualquier tipo, como el que tenemos a continuación (indicado por el análisis de Nessus):



Al intentar acceder a esta página <https://sitiodepruebas.org/contact.htm> obtenemos:

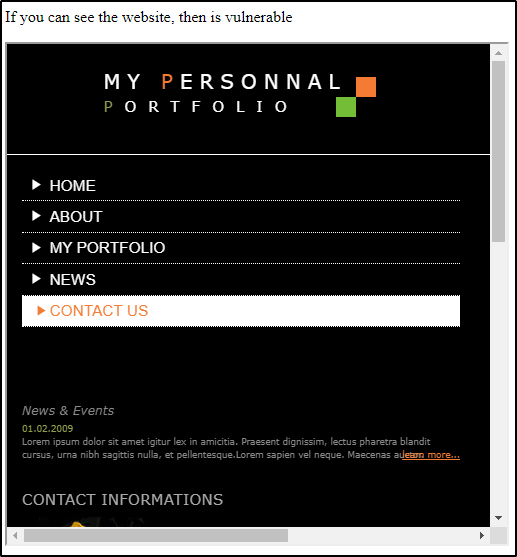


Como vemos el sitio contiene un formulario que luego es enviado por POST utilizando los datos ingresados.

Utilizando el siguiente código HTML seremos capaces de ver si la página es vulnerable o no:



Al ejecutar el código obtenemos:



Lo que implica una posible vulnerabilidad respecto a que un tercero pueda obtener los datos ingresados en el formulario vía Clickjacking.

Un ejemplo de una página que cuenta con defensas contra esta vulnerabilidad es Facebook:

