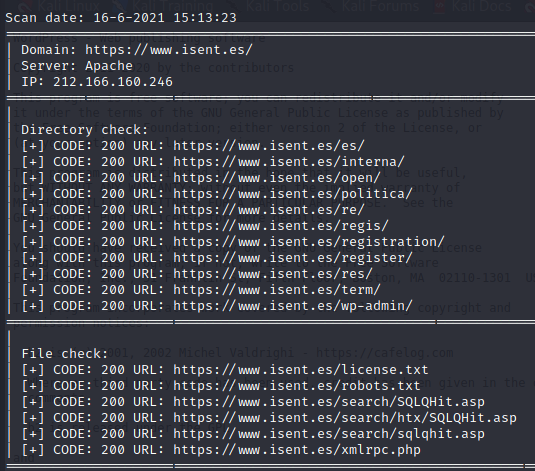
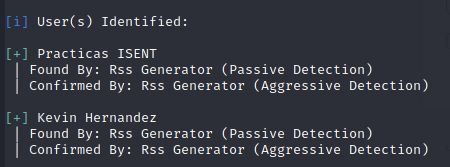
Durante los escaneos a la web ***isent.es*** que he realizado utilizando diversas herramientas (uniscan, wpscan, owasp) no he encontrado ninguna vulnerabilidad grave, pero sí algunas leves que sería adecuado solventar para garantizar la seguridad de los datos de la web y de los usuarios que accedan a ella.

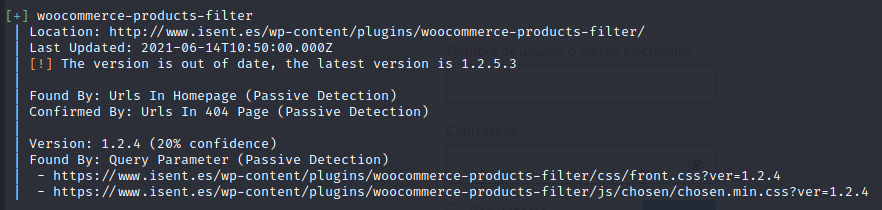
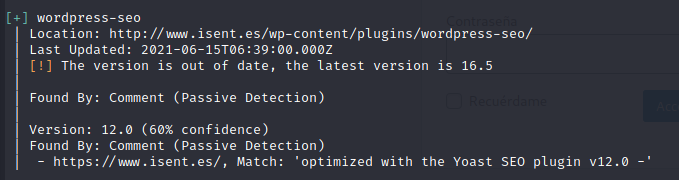
He detectado que los siguientes directorios son públicos, siendo de especial relevancia el de *wp-admin/* , ya que al tener tan fácil acceso a este directorio se puede hacer un intento forzado de login. También son visibles los archivos *license.txt* y *robots.txt .*

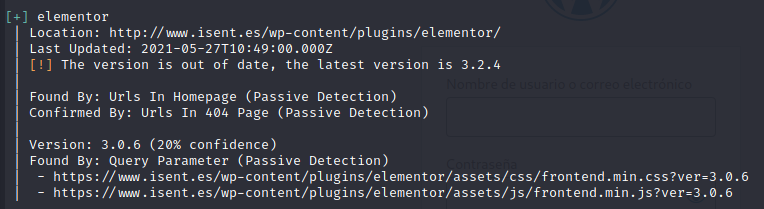
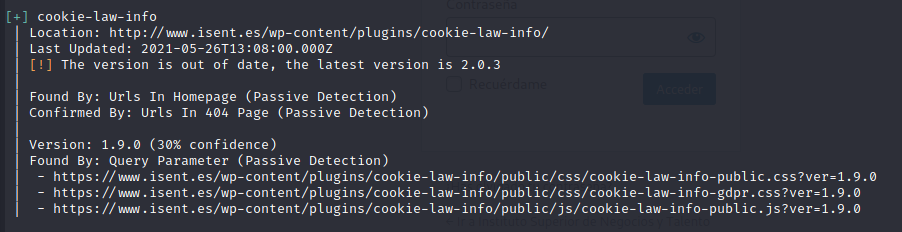
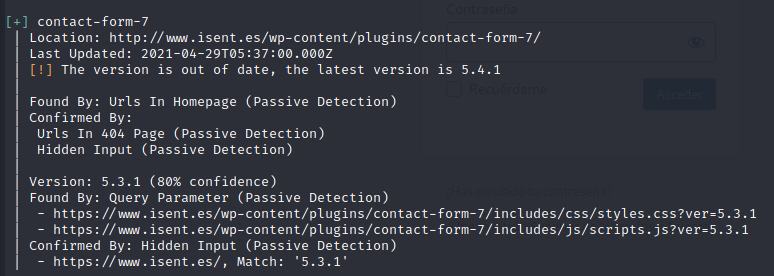


He detectado también el listado de usuarios de la web, facilitando así todavía más el acceso forzado.

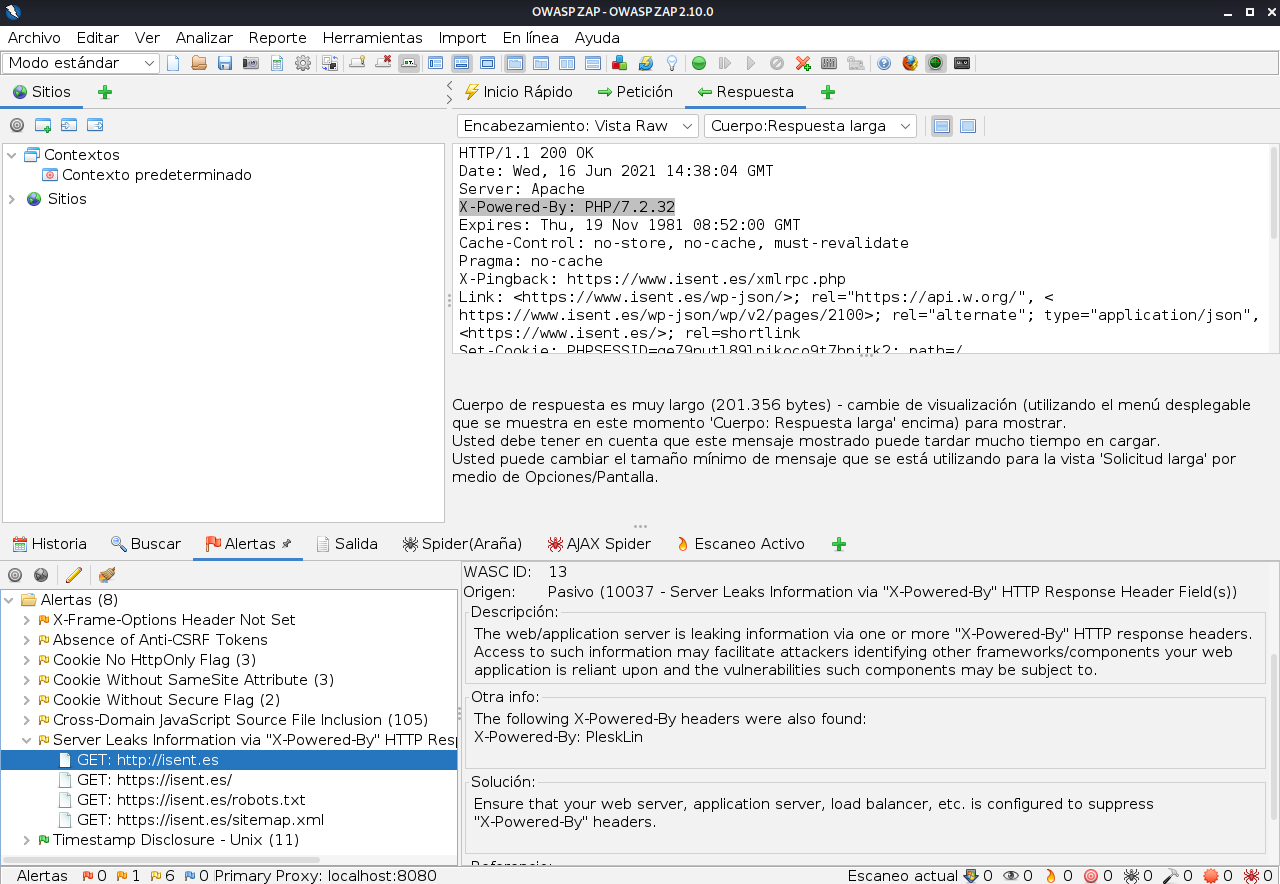


También he identificado algunos plugins que necesitan actualizarse:  
- contact-form-7  
- cookie-law-info  
- elementor  
-woocomerce-products-filter  
-wordpress-seo

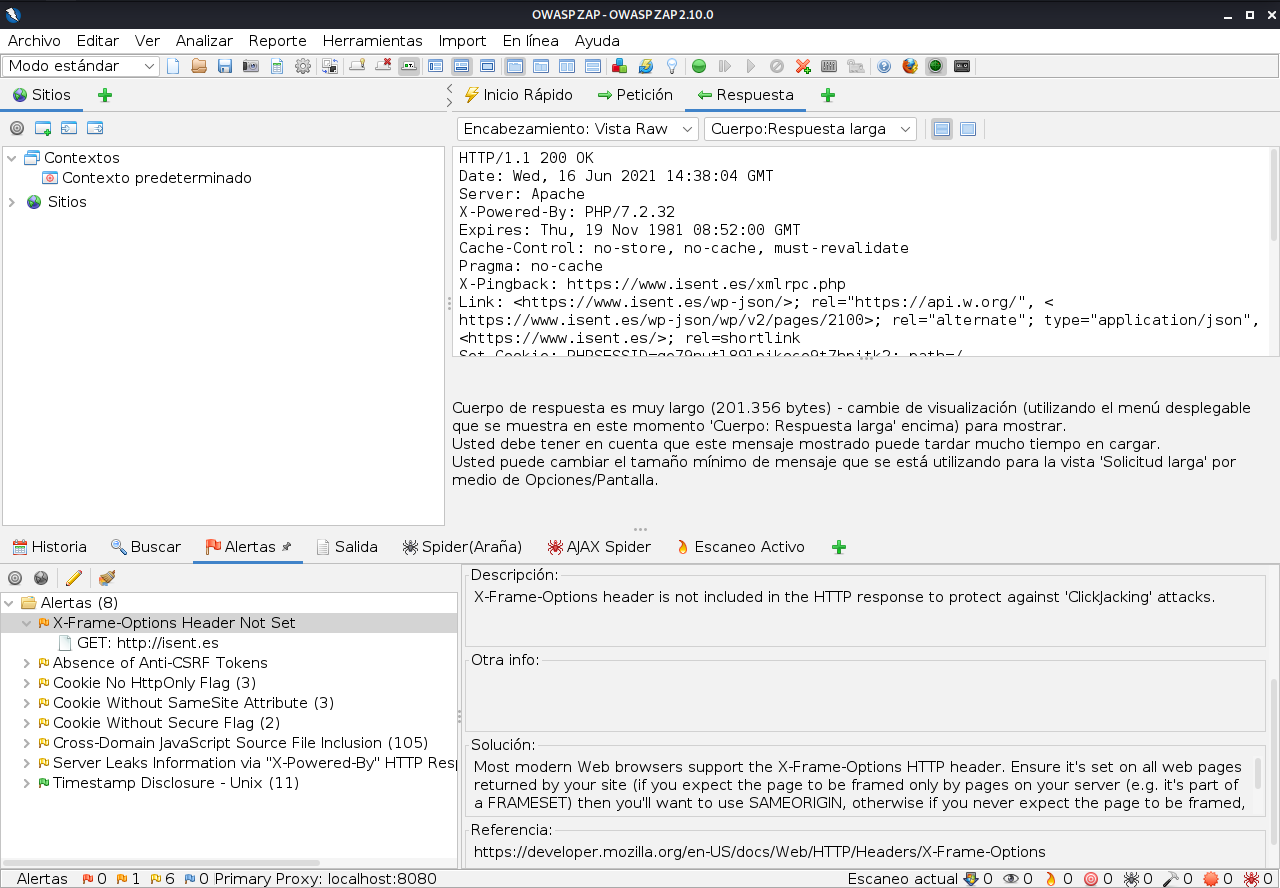




He detectado que la versión utilizada de PHP es visible. Conocer esta información facilita el uso de frameworks específicos para atacar la web.



También he notado la ausencia del header X-Frame-Options en el código, que evitarían posibles ataques de clickjacking dirigidos al usuario.



Por último, algunas cookies del sitio web no han sido del todo aseguradas.

