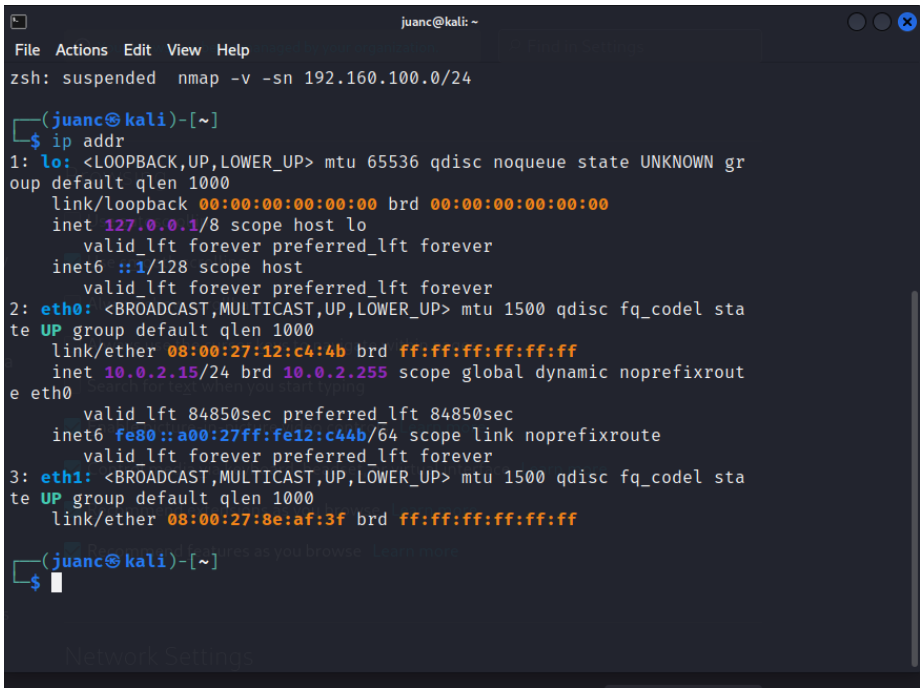
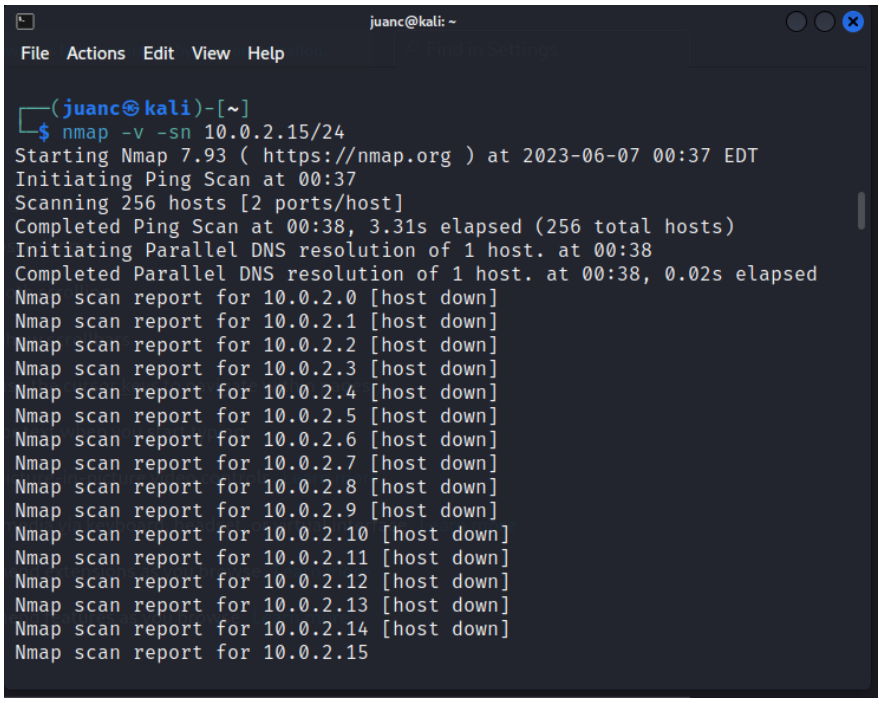
Garguño Vargas Juan Carlos **Reto 1**

Comenzamos con la detección de nuestra dirección ip

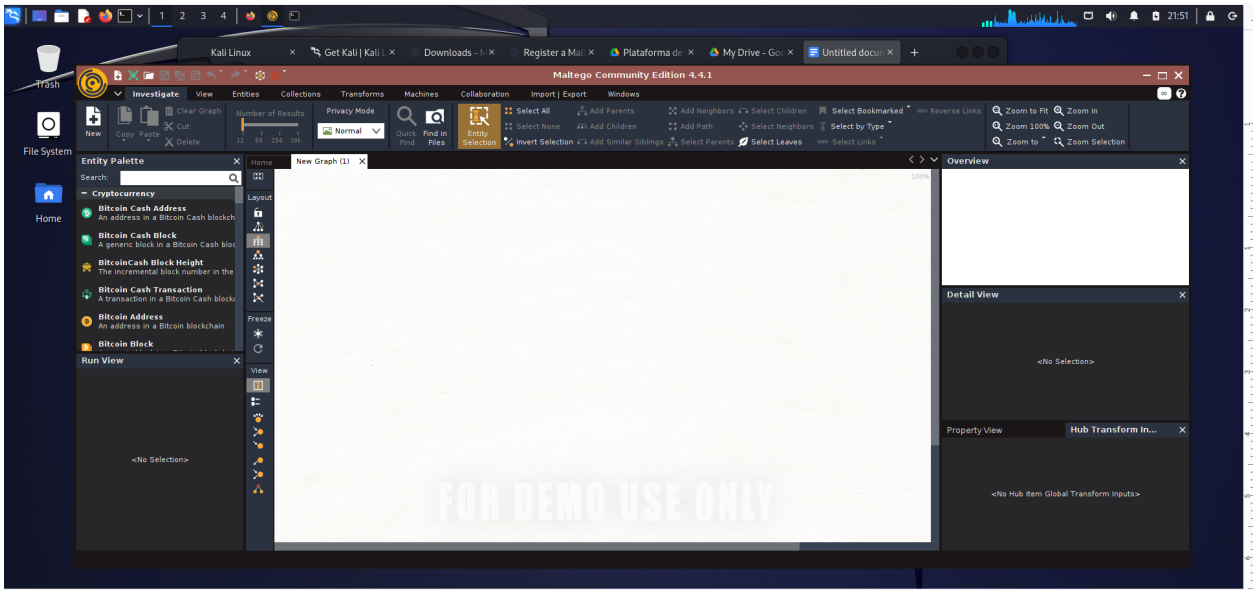


Detectamos los host que estén activos en la red

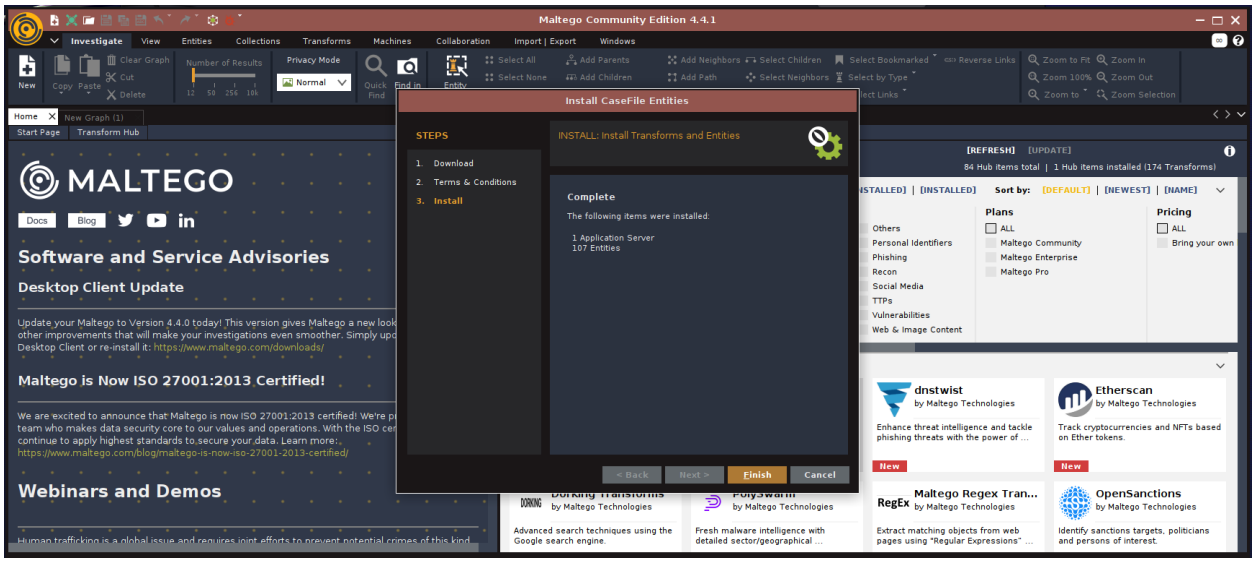


Sección 2

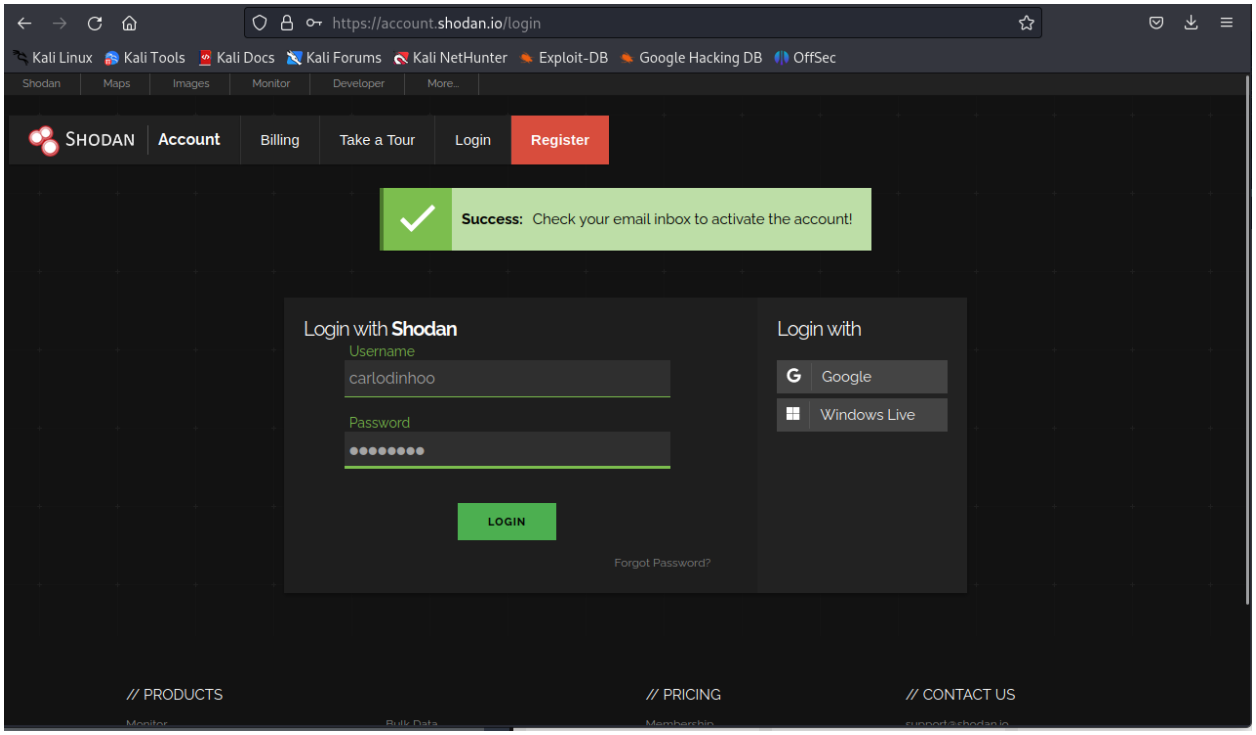
Hacemos el uso de la herramienta Maltego, para esto pasamos a hacer la instalación dentro de la maquina virtual y abrimos el programa.



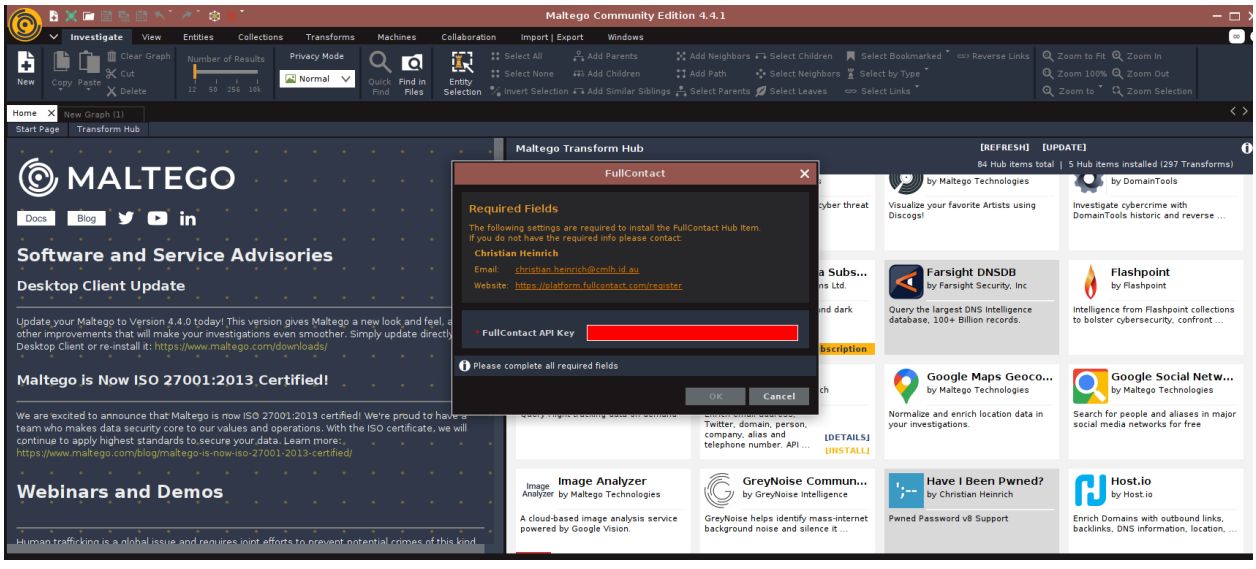
Instalamos las paqueterias que usaremos como CaseFile Entities, Shodan, Full contact, etc.



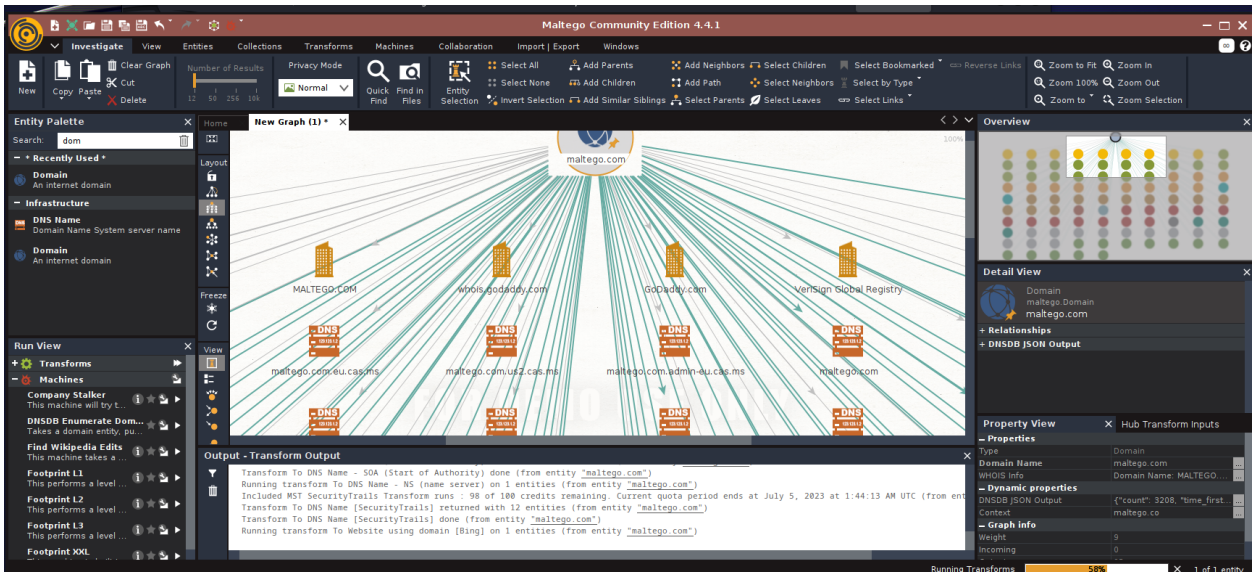
Instalamos shodan y nos registramos para obtener una API key y poder continuar con la instalación.



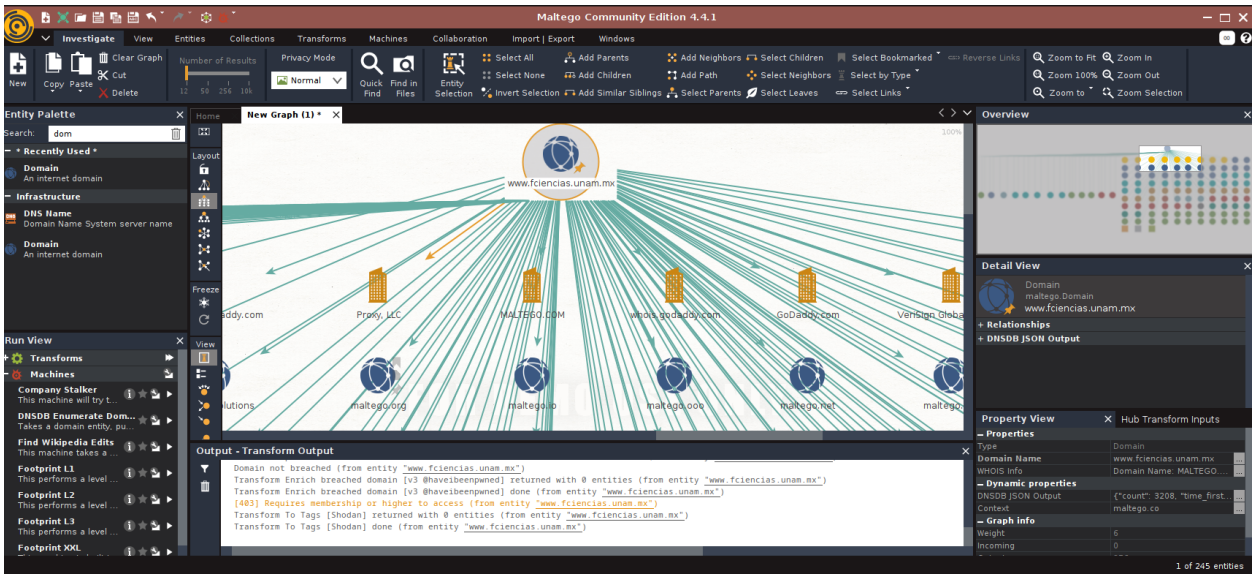
Instalamos Full contact y hacemos los mismos pasos que en Shodan, nos registramos y obtenemos una API Key gratuita para continuar.



Realizamos una prueba y corremos el analisis en maltego.com

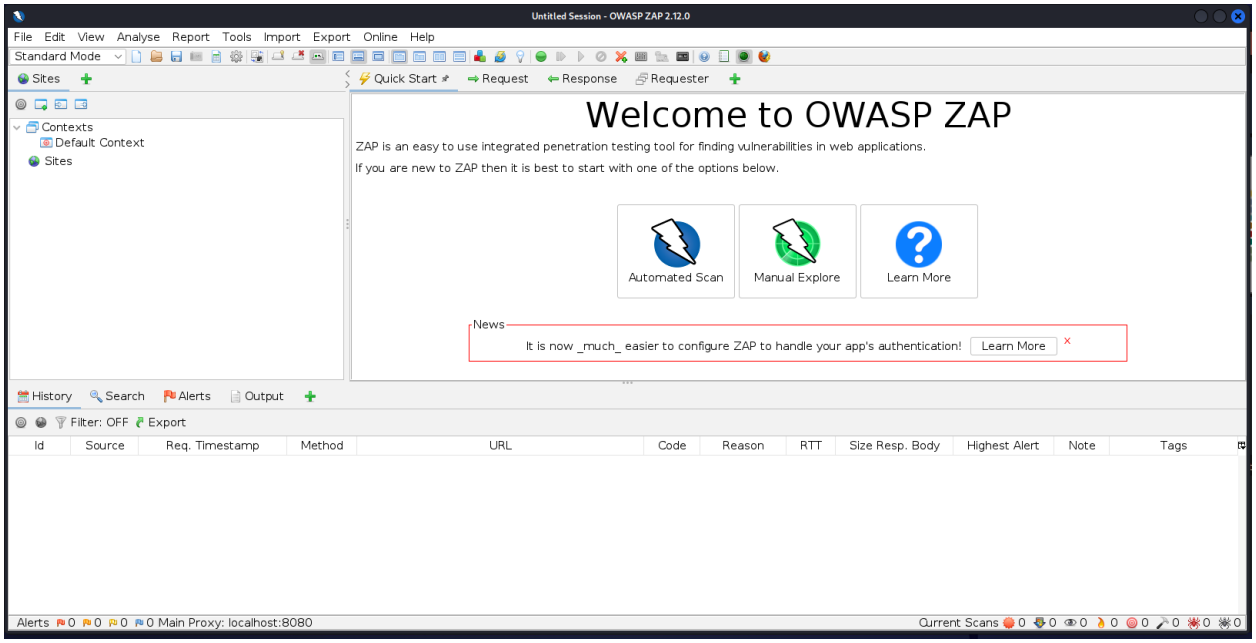


Procedemos a realizar un escaneo a la página de la Facultad de Ciencias de la UNAM y verificar que podamos obtener alguna información que nos pueda servir.



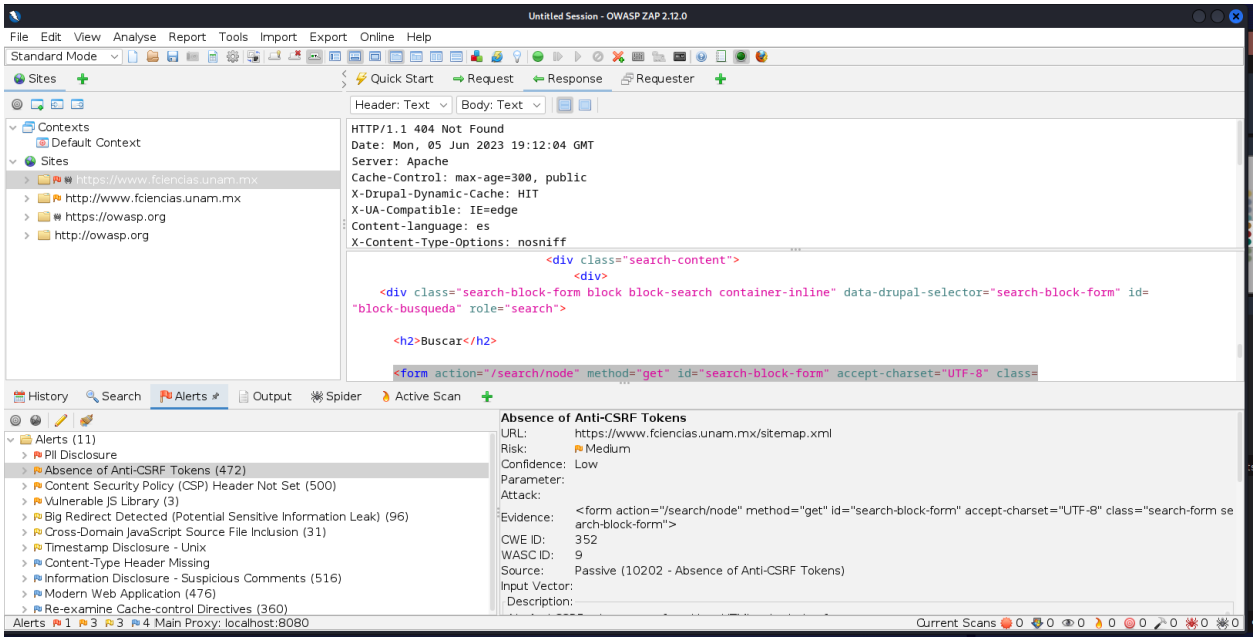
Del analisis notamos que el sitio interactua con GoDaddy.com, nos devuelve correos y teléfonos de contacto.

Procedemos a identificar vulnerabilidades en un sitio web a través de la herramienta OWASP Zap



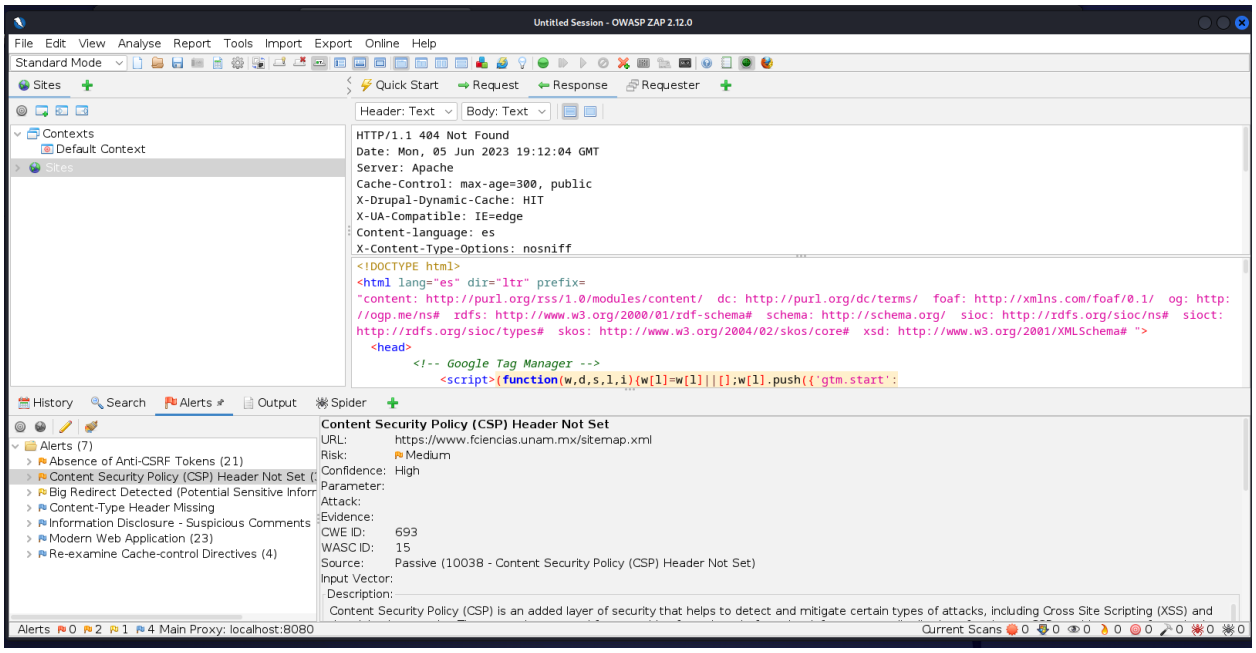
Hacemos el análisis al mismo sitio de la Facultad de Ciencias y encontramos con un total de 11 alertas

La alerta relacionada con Absence of Anti-CSRF notamos que tiene un riesgo bajo pero que sin embargo tiene una posibilidad de realizar un ataque a través de la etiqueta form, la solución que se sugiere es realizar un rediseño en la arquitectura y evitar estas debilidades.



La siguiente alerta está relacionada a Content Security Policy, la cual tiene que ver con los ataques de inyección, los cuales pueden servir para robar información sensible o distribuir algún malware en los sistemas.

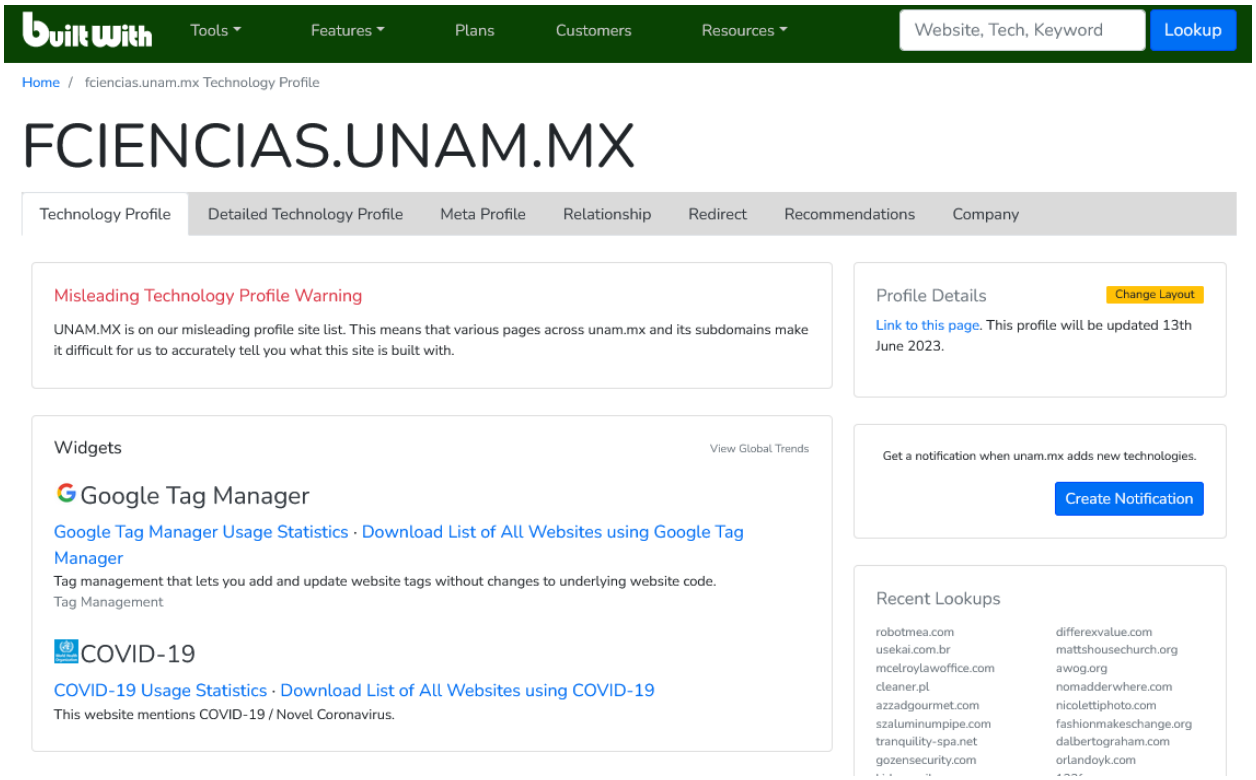
La solución sugerida para este caso es habilitar las configuraciones de seguridad y privacidad en los Headers.



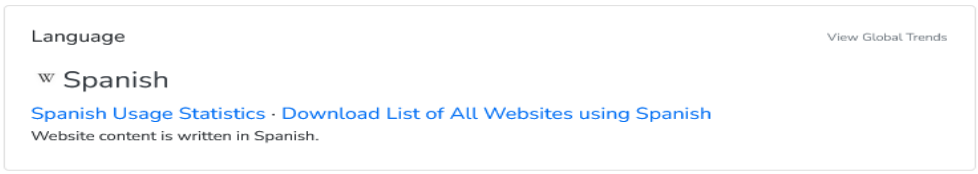
Por último usando la herramienta de BuiltWith hacemos otro análisis sobre la misma página de la Facultad de Ciencias

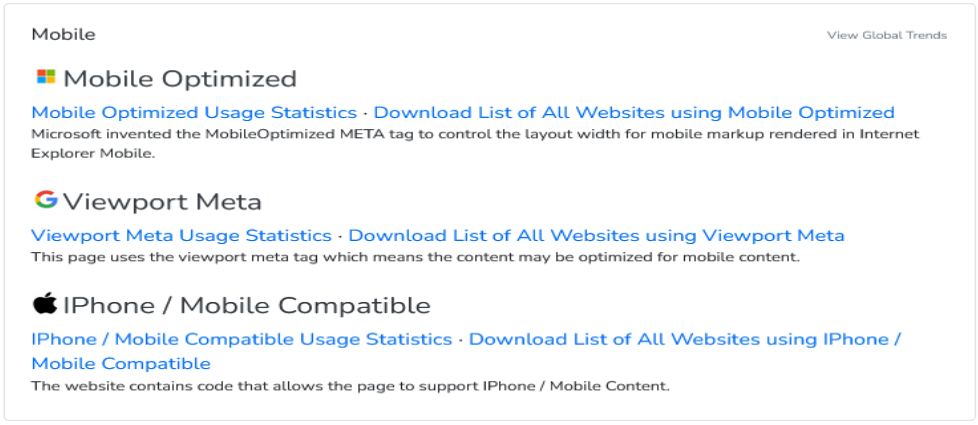
Los widgets que usa el sitio de la Facultad son

- Google Tag Manager
- Covid 19



Observamos también que solo manejan el lenguaje en español y que tambien es compatible si se quiere visitar el sitio desde un dispositivo Android o IOS





Podemos también obtener el tipo de servidor donde esta ubicado el sitio, así como sus certificados SSL