

Comenzamos con la detección de nuestra dirección ip

```
File Actions Edit View Help
zsh: suspended nmap -v -sn 192.160.100.0/24

(juanc@kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:12:c4:4b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 84850sec preferred_lft 84850sec
    inet6 fe80::a00:27ff:fe12:c44b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8e:af:3f brd ff:ff:ff:ff:ff:ff

(juanc@kali)-[~]
$
```

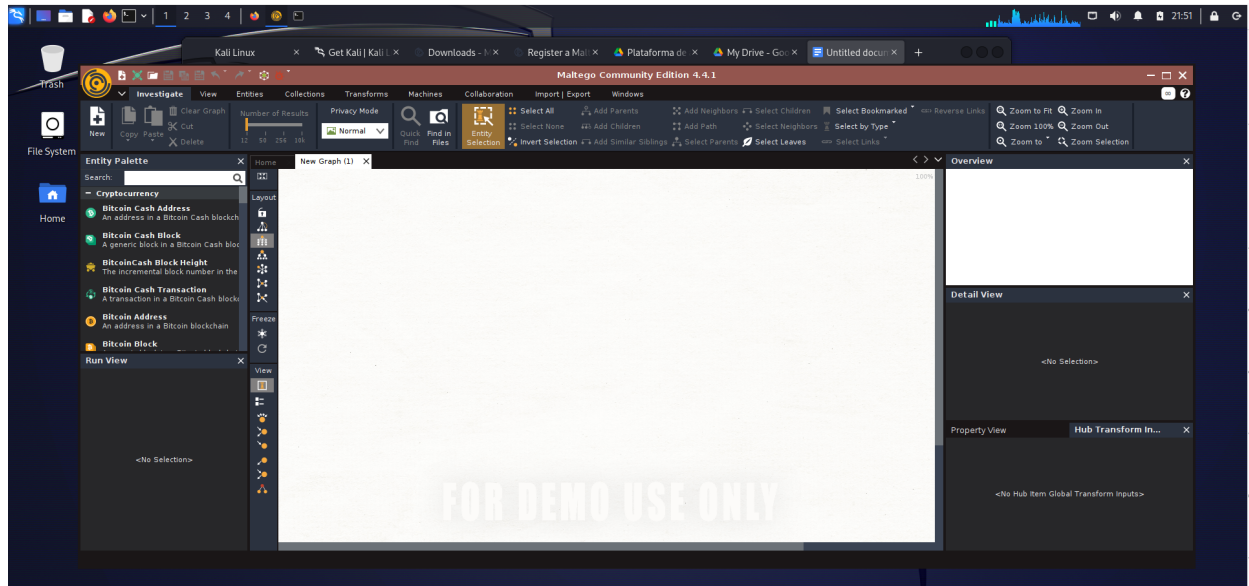
Detectamos los host que estén activos en la red

```
File Actions Edit View Help

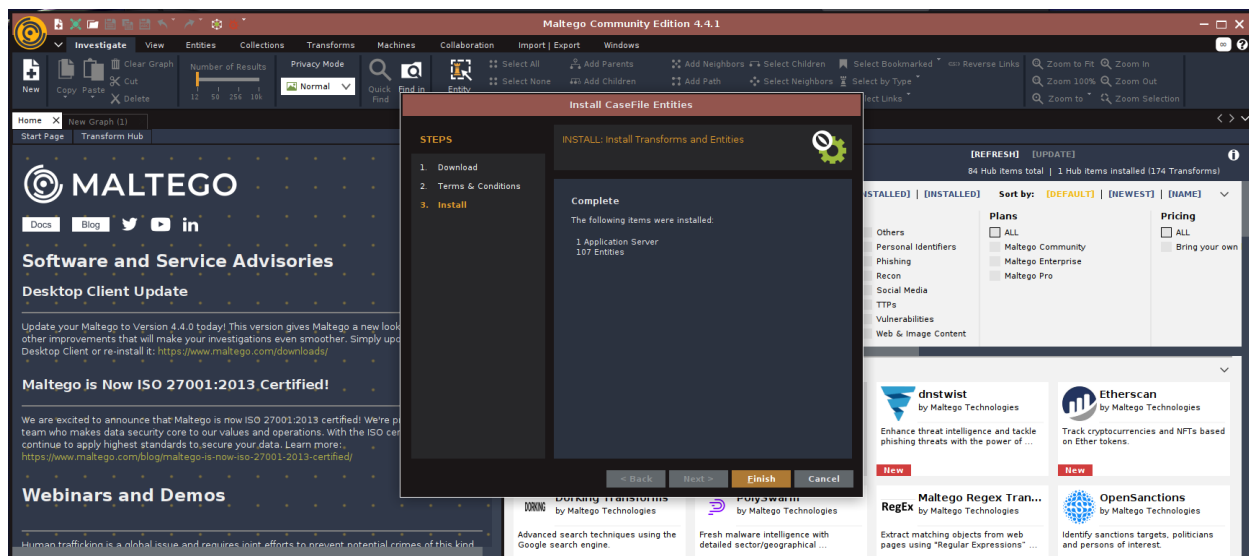
(juanc@kali)-[~]
$ nmap -v -sn 10.0.2.15/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-07 00:37 EDT
Initiating Ping Scan at 00:37
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 00:38, 3.31s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:38
Completed Parallel DNS resolution of 1 host. at 00:38, 0.02s elapsed
Nmap scan report for 10.0.2.0 [host down]
Nmap scan report for 10.0.2.1 [host down]
Nmap scan report for 10.0.2.2 [host down]
Nmap scan report for 10.0.2.3 [host down]
Nmap scan report for 10.0.2.4 [host down]
Nmap scan report for 10.0.2.5 [host down]
Nmap scan report for 10.0.2.6 [host down]
Nmap scan report for 10.0.2.7 [host down]
Nmap scan report for 10.0.2.8 [host down]
Nmap scan report for 10.0.2.9 [host down]
Nmap scan report for 10.0.2.10 [host down]
Nmap scan report for 10.0.2.11 [host down]
Nmap scan report for 10.0.2.12 [host down]
Nmap scan report for 10.0.2.13 [host down]
Nmap scan report for 10.0.2.14 [host down]
Nmap scan report for 10.0.2.15
```

Sección 2

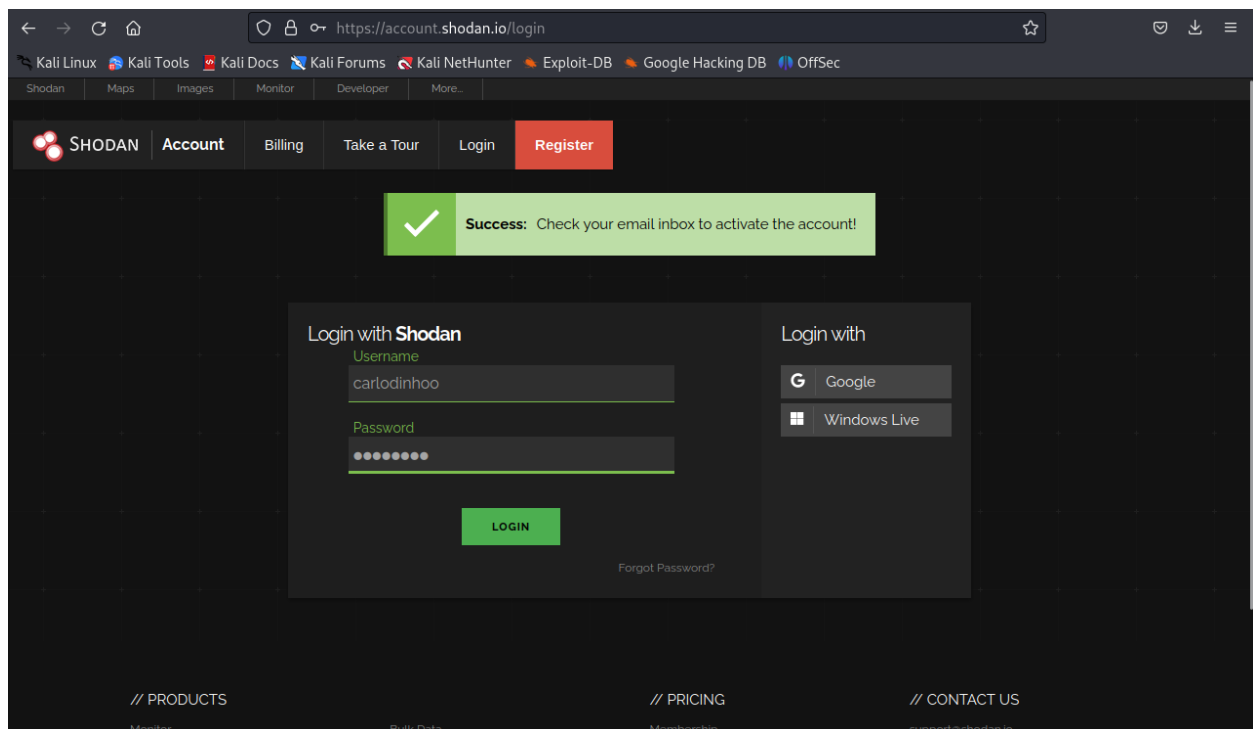
Hacemos el uso de la herramienta Maltego, para esto pasamos a hacer la instalación dentro de la maquina virtual y abrimos el programa.



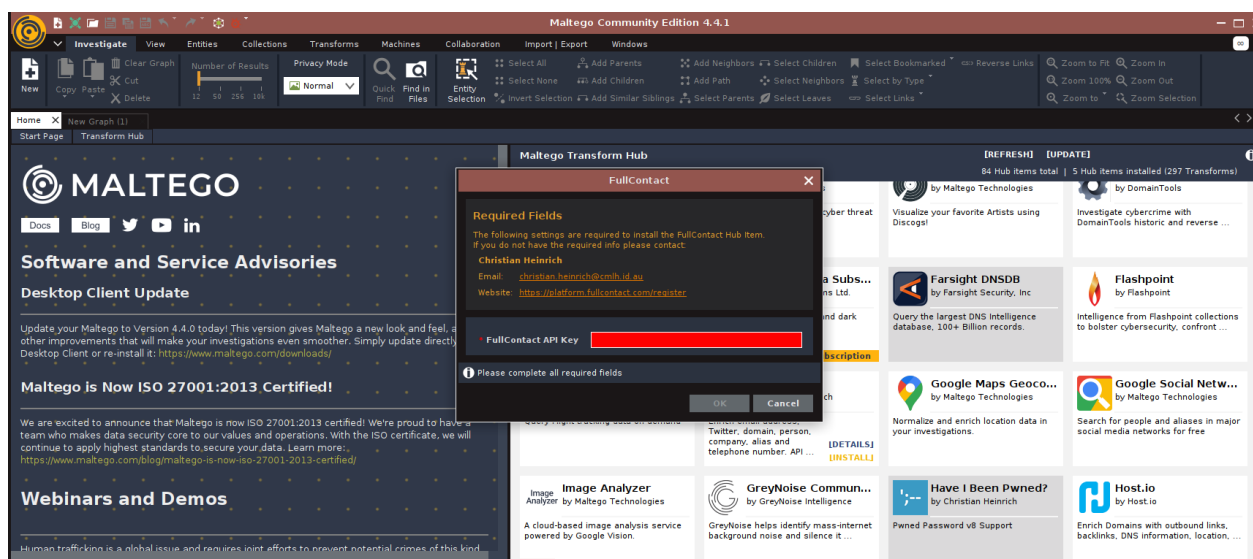
Instalamos las paqueterias que usaremos como CaseFile Entities, Shodan, Full contact, etc.



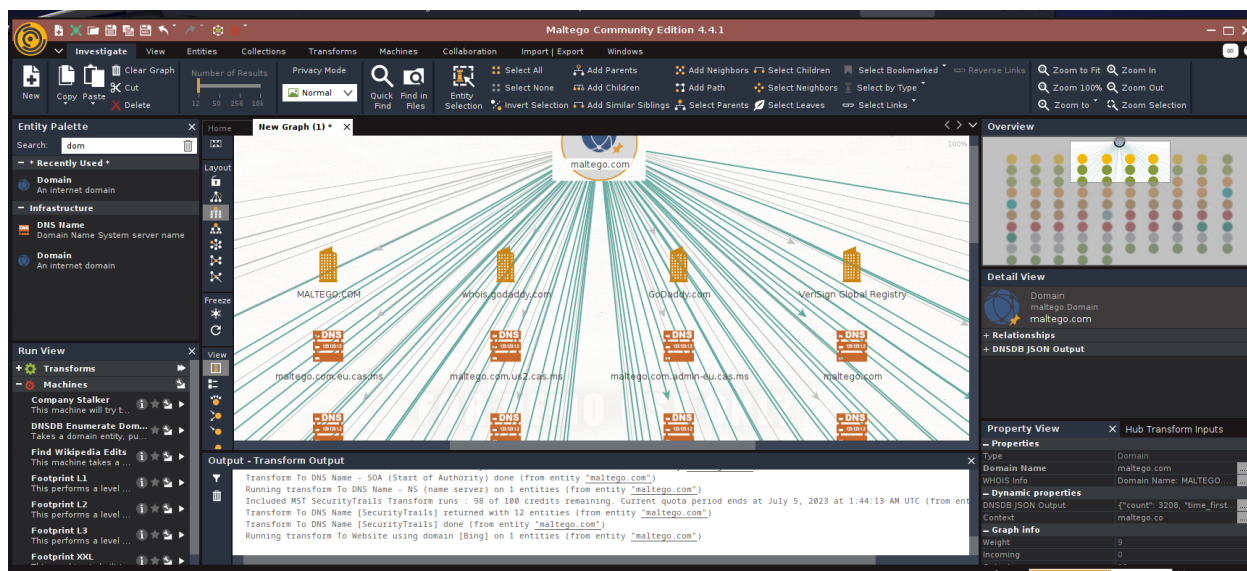
Instalamos shodan y nos registramos para obtener una API key y poder continuar con la instalación.



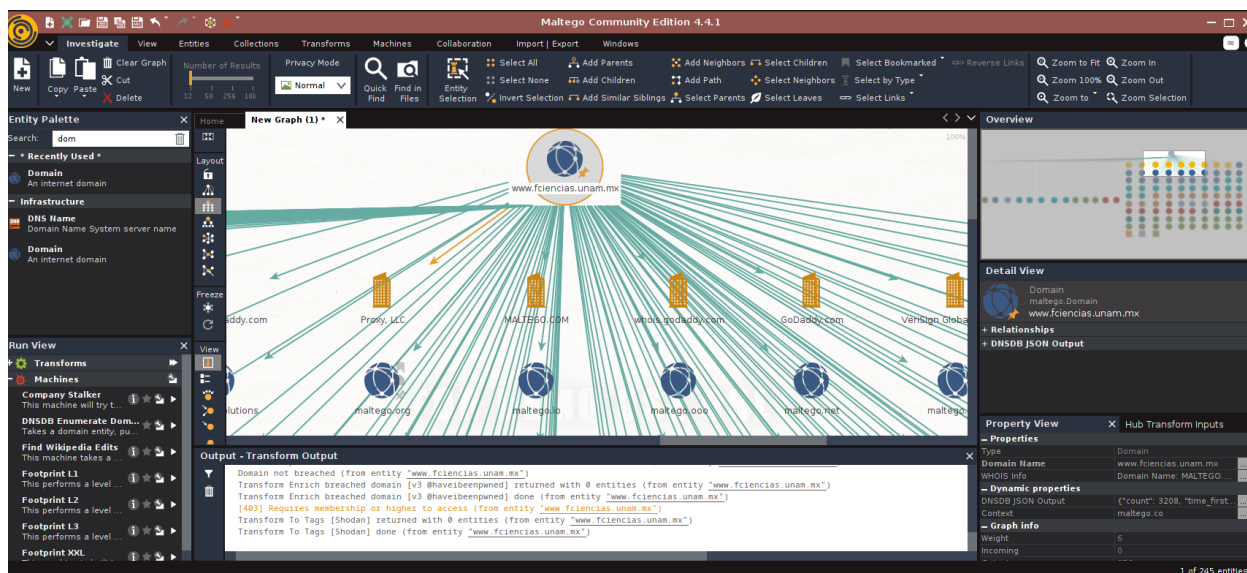
Instalamos Full contact y hacemos los mismos pasos que en Shodan, nos registramos y obtenemos una API Key gratuita para continuar.



Realizamos una prueba y corremos el analisis en maltego.com

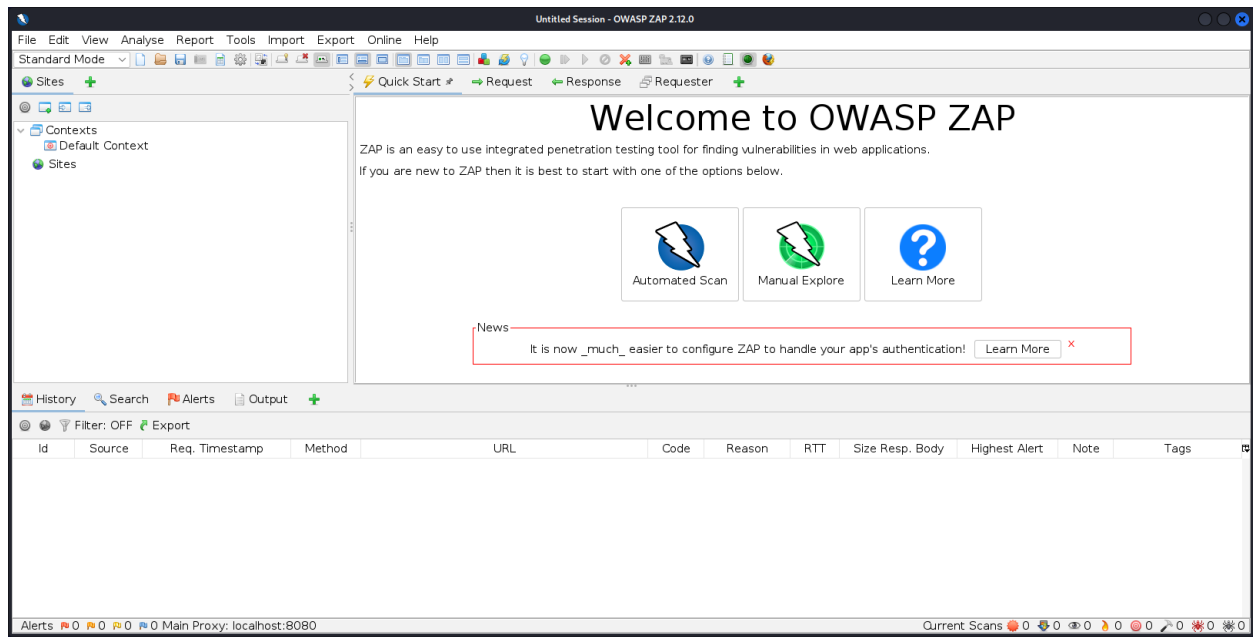


Procedemos a realizar un escaneo a la página de la Facultad de Ciencias de la UNAM y verificar que podamos obtener alguna información que nos pueda servir.



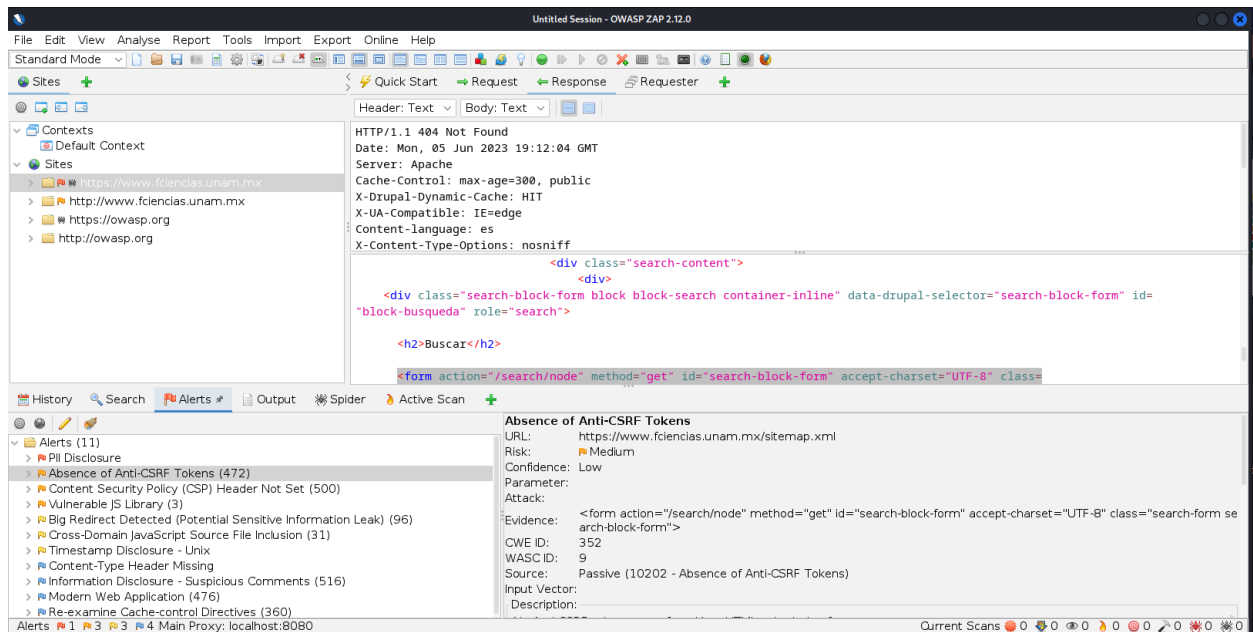
Del analisis notamos que el sitio interactua con GoDaddy.com, nos devuelve correos y teléfonos de contacto.

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



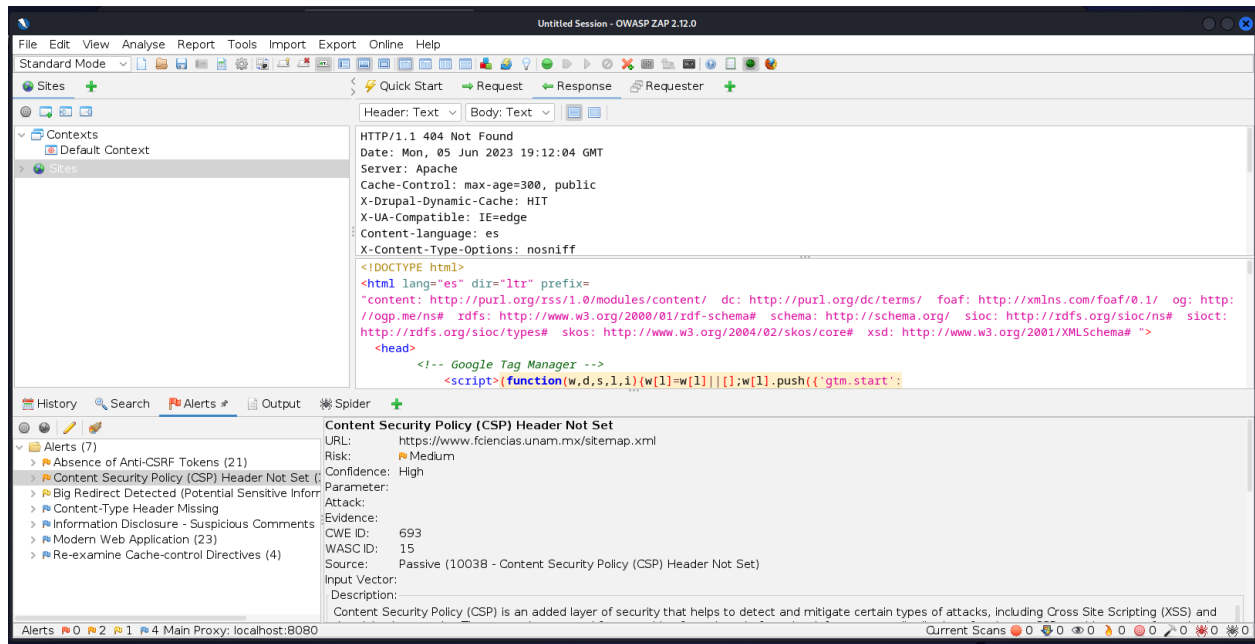
Hacemos el análisis al mismo sitio de la Facultad de Ciencias y encontramos con un total de 11 alertas

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

built with Tools ▾ Features ▾ Plans Customers Resources ▾ Website, Tech, Keyword **Lookup**

Home / ciencias.unam.mx Technology Profile

FCIENCIAS.UNAM.MX

Technology Profile Detailed Technology Profile Meta Profile Relationship Redirect Recommendations Company

Misleading Technology Profile Warning

UNAM.MX is on our misleading profile site list. This means that various pages across unam.mx and its subdomains make it difficult for us to accurately tell you what this site is built with.

Profile Details [Change Layout](#)

[Link to this page](#). This profile will be updated 13th June 2023.

Widgets [View Global Trends](#)

Google Tag Manager

[Google Tag Manager Usage Statistics](#) · [Download List of All Websites using Google Tag Manager](#)

Tag management that lets you add and update website tags without changes to underlying website code.

Tag Management

COVID-19

[COVID-19 Usage Statistics](#) · [Download List of All Websites using COVID-19](#)

This website mentions COVID-19 / Novel Coronavirus.

Get a notification when unam.mx adds new technologies.
[Create Notification](#)

Recent Lookups

robotmea.com

usekai.com.br

mcelroylawoffice.com

cleaner.pl

azzadgourmet.com

szaluminumpipe.com

tranquility-spa.net

gozensecurity.com

...

differexvalue.com

mattshousechurch.org

awog.org

nomadderwhere.com

nicolettipphoto.com

fashionmakeschange.org

dalbertograham.com

orlandoyk.com

...

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

Language [View Global Trends](#)

Spanish

[Spanish Usage Statistics](#) · [Download List of All Websites using Spanish](#)

Website content is written in Spanish.

Mobile [View Global Trends](#)

Mobile Optimized

[Mobile Optimized Usage Statistics](#) · [Download List of All Websites using Mobile Optimized](#)

Microsoft invented the MobileOptimized META tag to control the layout width for mobile markup rendered in Internet Explorer Mobile.

Viewport Meta

[Viewport Meta Usage Statistics](#) · [Download List of All Websites using Viewport Meta](#)

This page uses the viewport meta tag which means the content may be optimized for mobile content.

iPhone / Mobile Compatible

[iPhone / Mobile Compatible Usage Statistics](#) · [Download List of All Websites using iPhone / Mobile Compatible](#)

The website contains code that allows the page to support iPhone / Mobile Content.

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

SSL Certificates

[View Global Trends](#)

HSTS

[HSTS Usage Statistics](#) · [Download List of All Websites using HSTS](#)

Forces browsers to only communicate with the site using HTTPS.

Web Servers

[View Global Trends](#)

Apache

[Apache Usage Statistics](#) · [Download List of All Websites using Apache](#)

Apache has been the most popular web server on the Internet since April 1996.