TAREA 4 – TEST DE PENETRACION

JHON SEBASTIAN ZUÑIGA LOPEZ

TUTOR SERGIO LUIS LUDO ARGUMEDO

GRUPO 55

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA
INGENIERIA EN SISTEMAS
Argelia – Cauca
febrero 2022

Objetivo

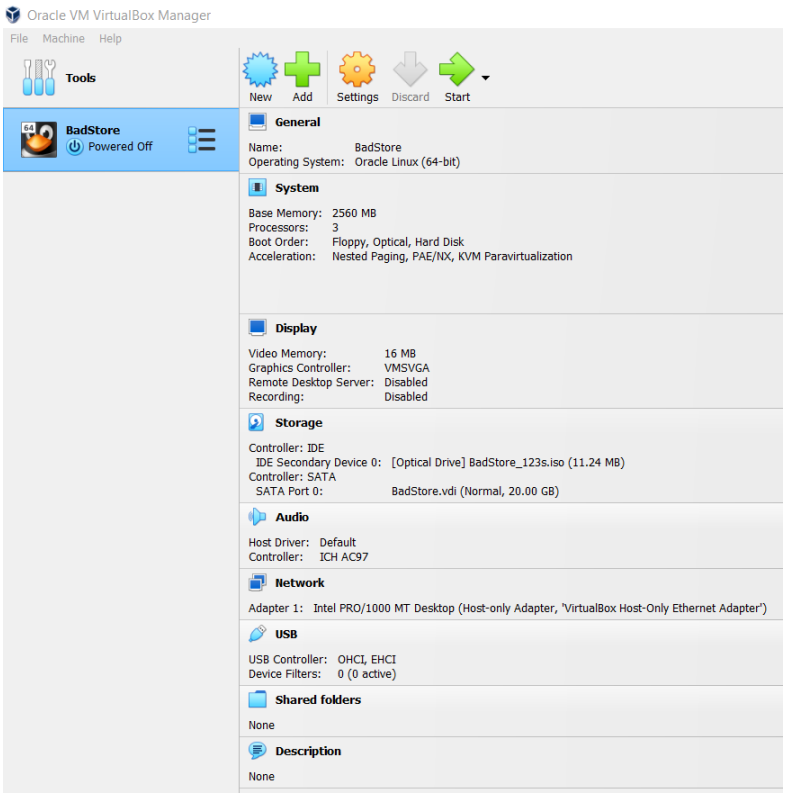
El objetivo es realizar un exhaustivo análisis de seguridad en la aplicación web alojada en la máquina virtual "badstore", utilizando la herramienta de prueba de penetración OWASP ZAP. Este análisis buscará identificar y evaluar posibles vulnerabilidades de seguridad, incluyendo, inyecciones SQL, vulnerabilidades XSS y otras amenazas comunes. A través de este proceso, se pretende mejorar la resistencia y la integridad de la aplicación web al identificar y corregir posibles brechas de seguridad, garantizando así un entorno en línea más seguro y confiable para los usuarios finales.

Link de la presentación: https://www.canva.com/design/DAGFCz7olLA/wGTl9-lP8lhjMPfuUDmFUg/edit?utm_content=DAGFCz7olLA&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

Procedimiento de prueba

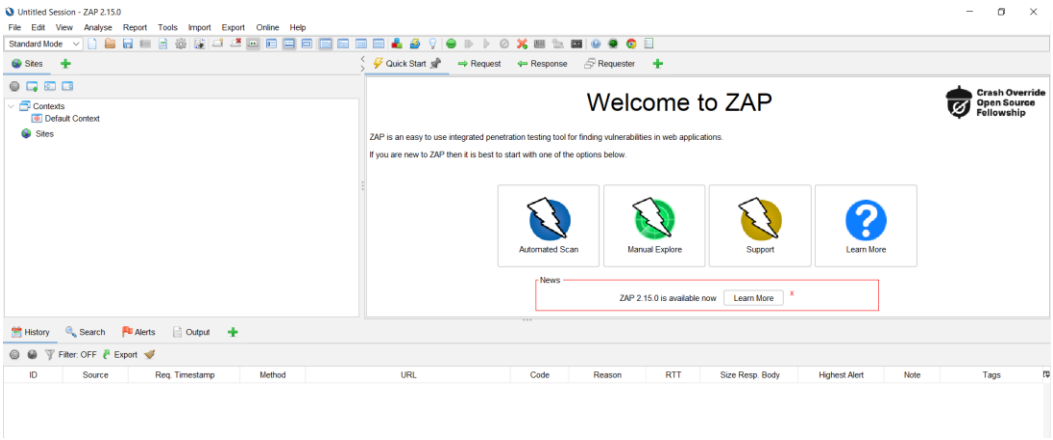
configuración de la máquina virtual

Una vez descargada la imagen ISO de la badStore se procede a crear la máquina virtual especificando cantidad de memoria RAM, capacidad de disco entre otras cosas.



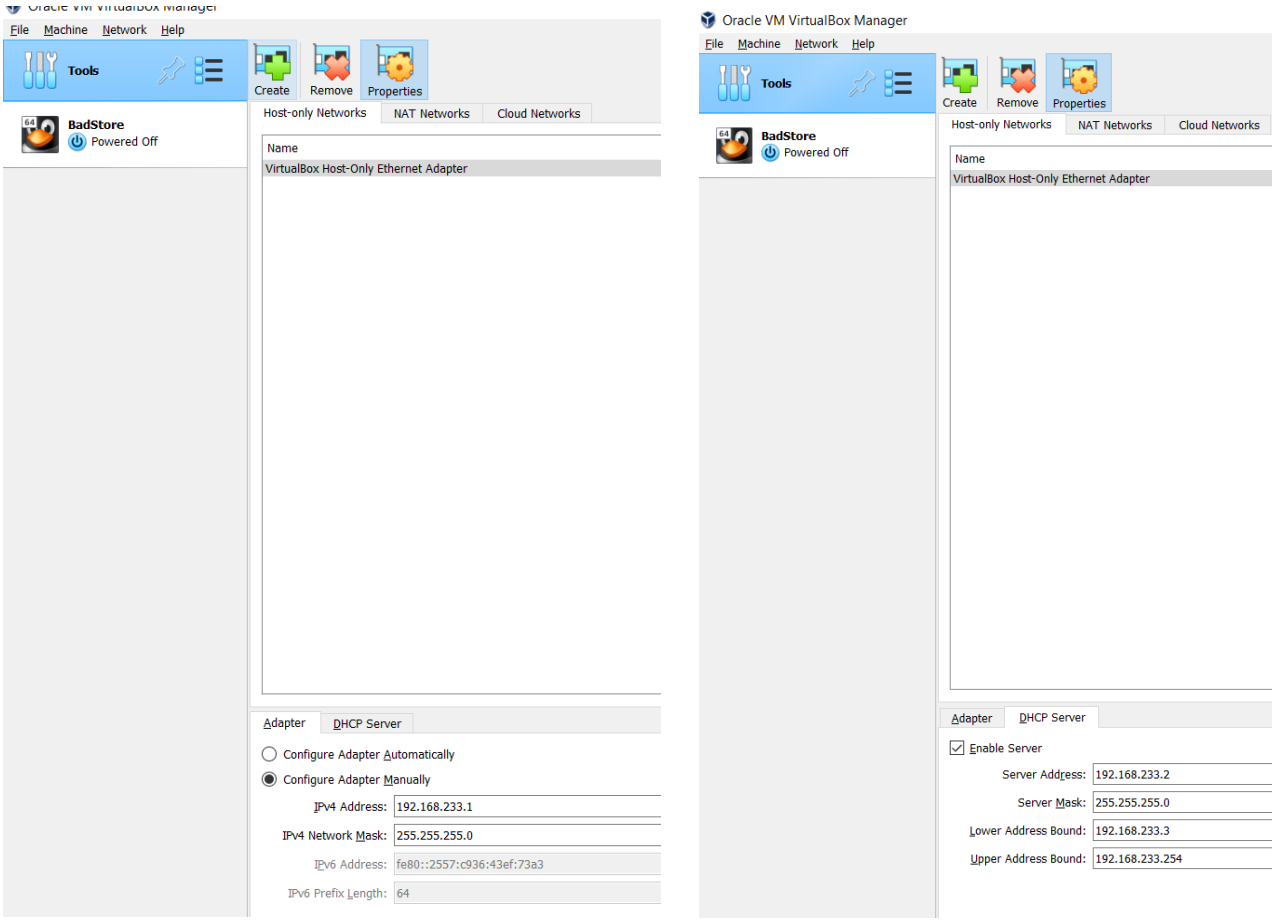
Instalación de la herramienta OWASP ZAP.

Después de descargar la aplicación se procede a realizar la instalación. La instalación se realiza mediante el sistema de instalación de Windows lo que hace que sea sencilla. Una vez terminada la instalación se obtiene la interfaz del aplicativo.

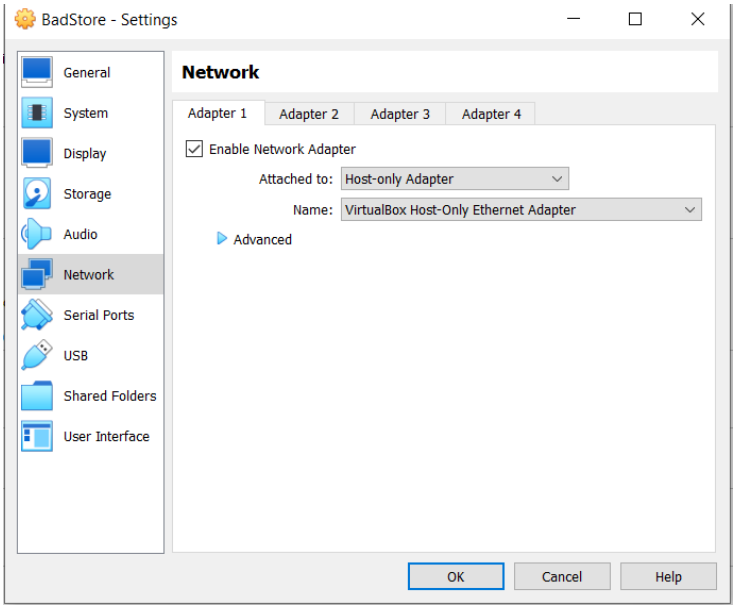


Configuración de la maquina badstore.

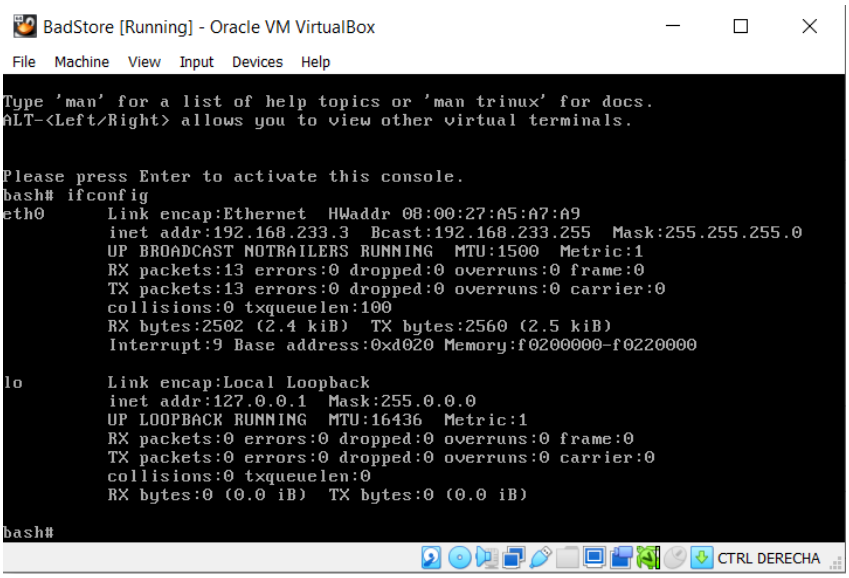
A continuación, se configura la red virtual teniendo en cuenta la dirección IP de la máquina virtual creada anteriormente. Se configura el adaptador y el servidor DHCP.



En las configuraciones de red se debe asegurar que este seleccionada la opción Host-only adapter.

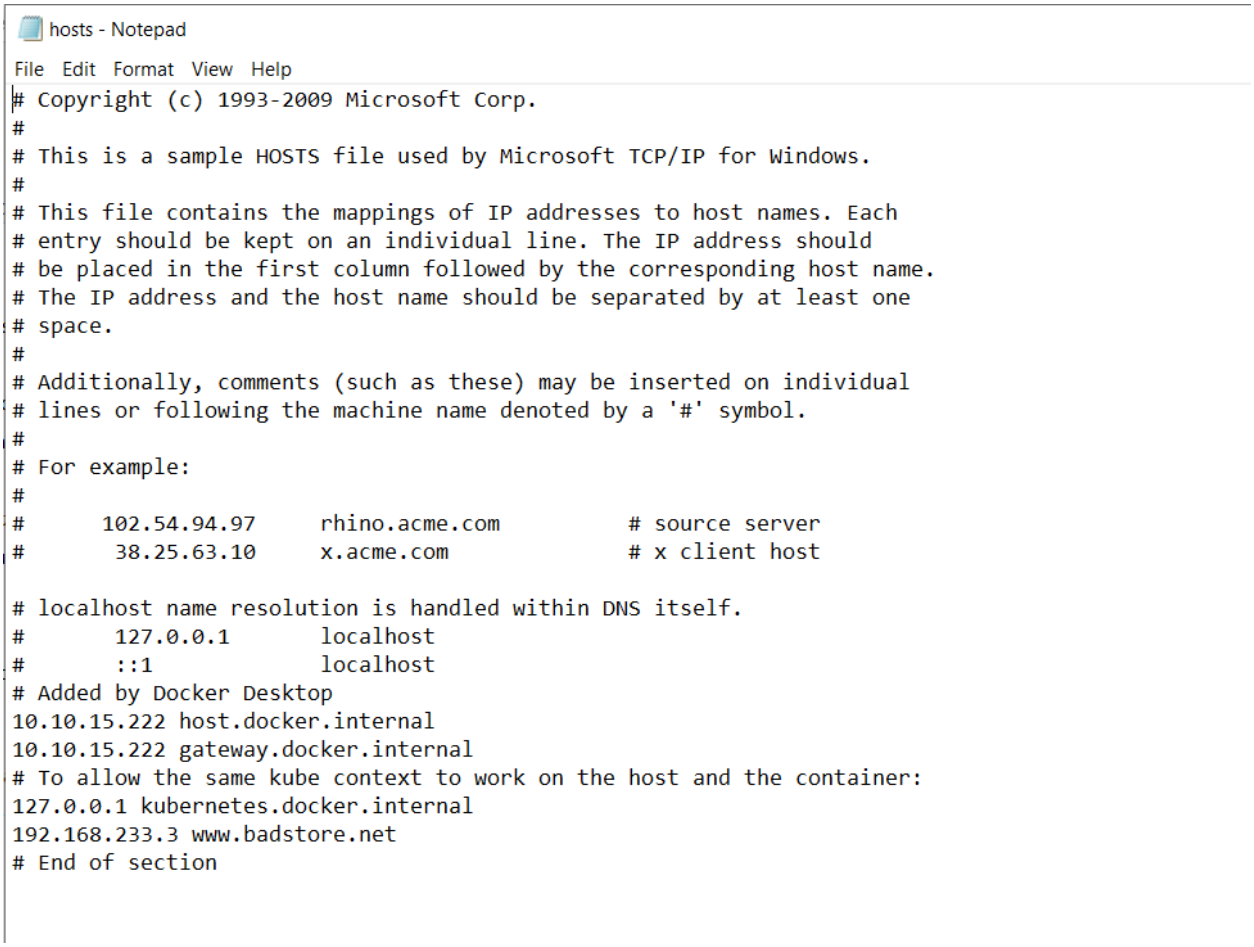


Para obtener la dirección IP de la maquina se inicializa la misma y en consola se ejecuta el comando **ifconfig.**

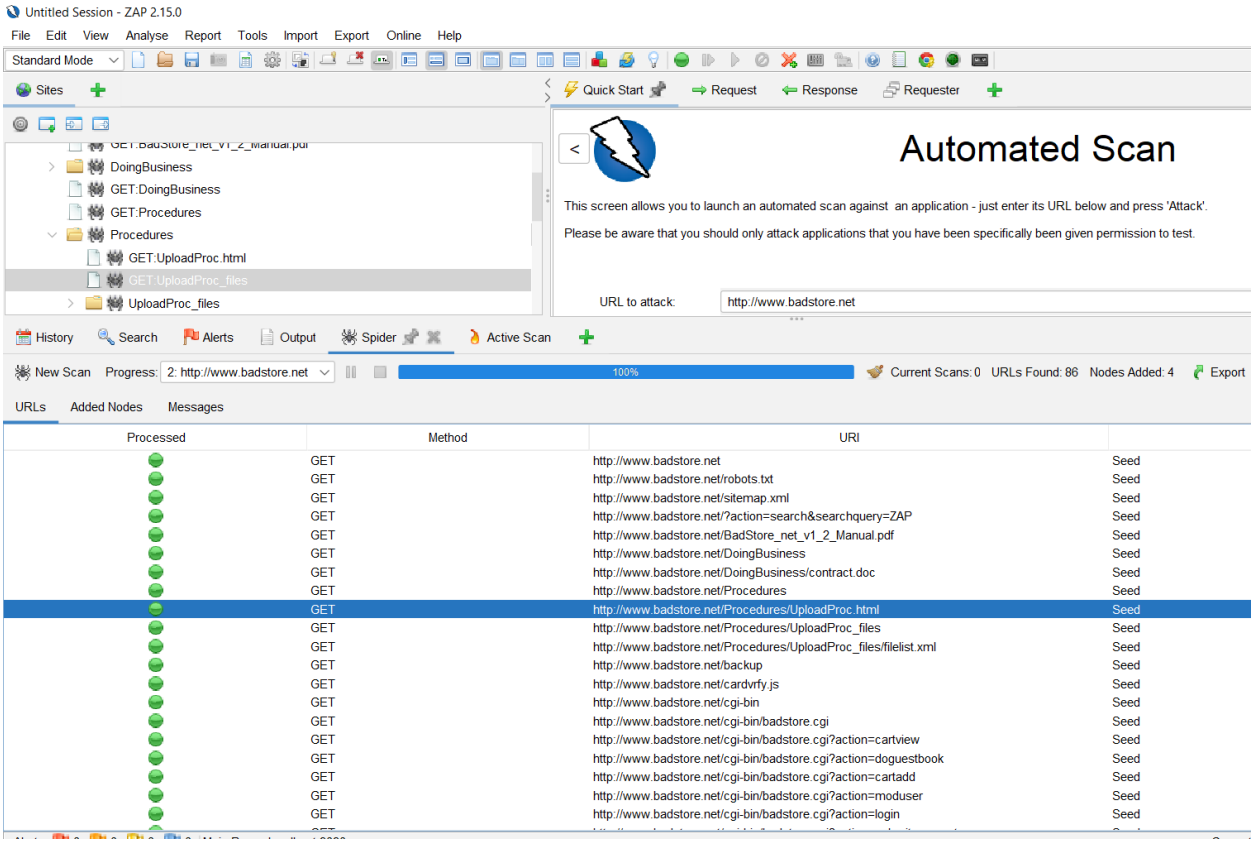


Configuración del proxi en el navegador

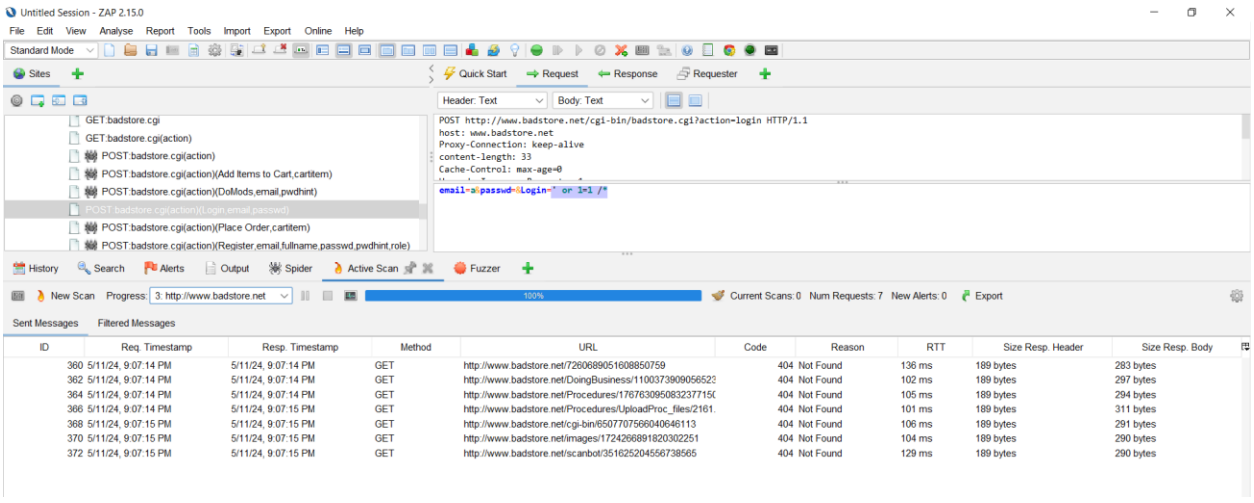
Para poder acceder a el badstore mediante un nombre de dominio y no directamente desde una IP se agrega la dirección IP de la máquina virtual a un archivo llamado **hosts** que se encuentra en la dirección C:\Windows\System32\drivers\etc\hosts



Ataque 1 – Spider

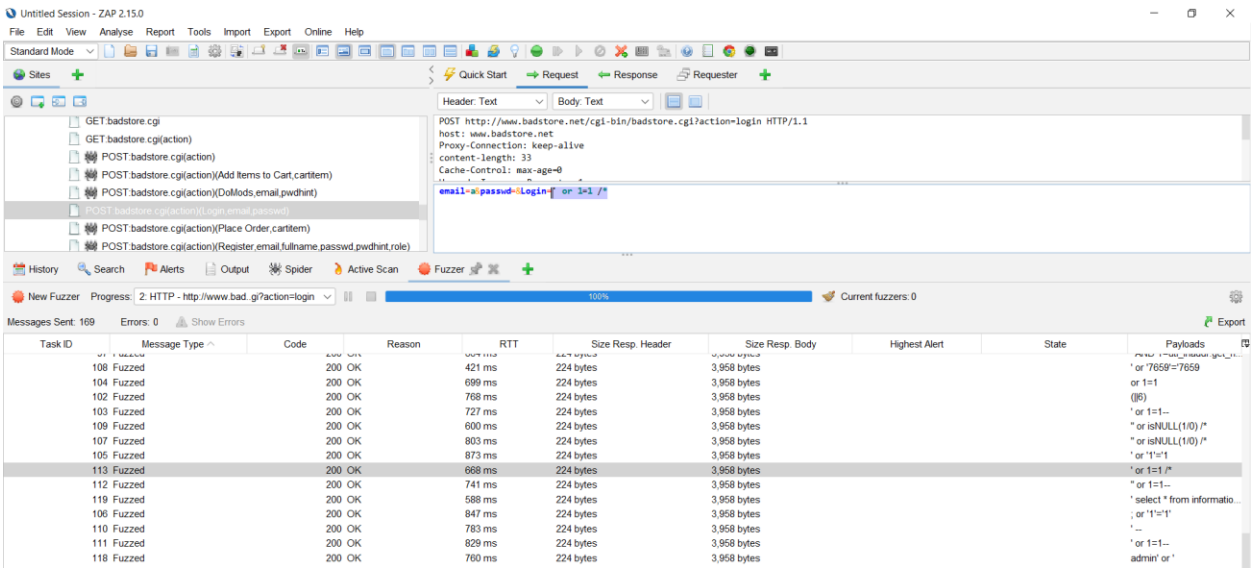


Ataque 2 – escaneo

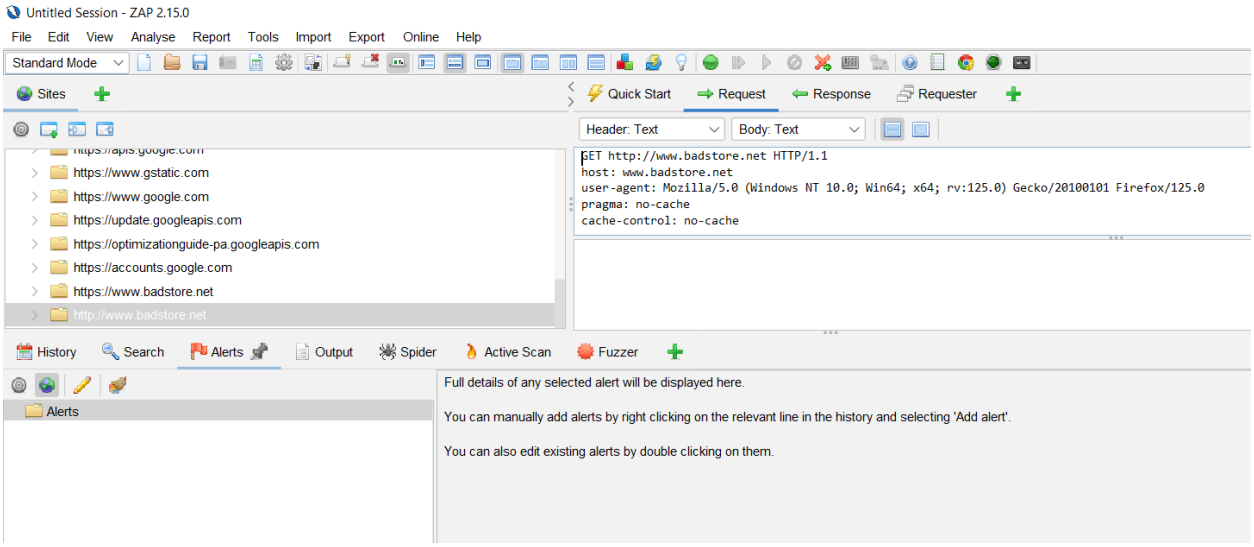


Ataque 3 - inyección SQL

Se realiza la prueba mediante inyección SQL y se identifica que la cláusula ' **or 1=1 /*** permite el ingreso a la aplicación.



Los escaneos no generan alertar, sin embargo, se debe tener en cuenta que mediante de inyección de código SQL se logró iniciar sesión, lo cual es un fallo de seguridad muy elevado. Para ello se deben tomar medidas correctivas y preventivas como lo son la validación de carácteres, el escape de caracteres especiales, actualización de los sistemas y directamente desde código separar los valores ingresados de la consulta SQL.



Referencias Bibliográficas

OWASP (2020). Web Application Penetration Testing. https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

OWASP (2021). TOP TEN. https://owasp.org/Top10/es/

Ramachandran, M. (2012). Software Security Testing. En Nova (Eds), Software Security Engineering : Design and Applications (pp. 151-164). Nova Science Publishers, Inc. https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=602994&lang=es&site=eds[1]live&scope=site&ebv=EB&ppid=pp_151