UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Máster Universitario en Ingeniería de Software y Sistemas informáticos

Braulio Fernando Cusco Mejía

Jorge Patricio Santamaría

Priscila Elizabeth Uyaguari Cabrera

Juan Ramón Bermejo Higuera

Ciberseguridad Web

Actividad 3: Laboratorio: test de penetración a la aplicación BadStore utilizando un scanner de vulnerabilidades de aplicaciones web

Ambato – Ecuador

Contenido

1. Desarrollo:

Para esta actividad se desplegó una máquina virtual con la aplicación BadStore importando el archivo badstore.ova.

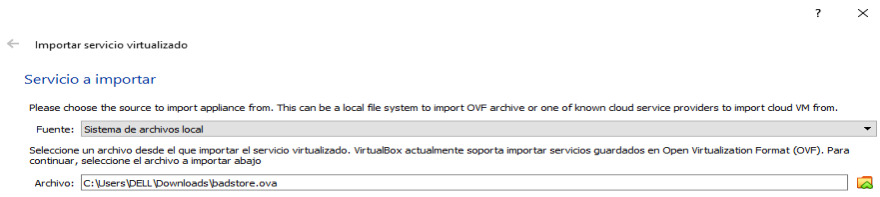


Figura. 1 Importar badstore.ova en Virtual Box.

Se cargó la Iso de Badstore asociándolo con un controlador Ide de tipo CD Rom.

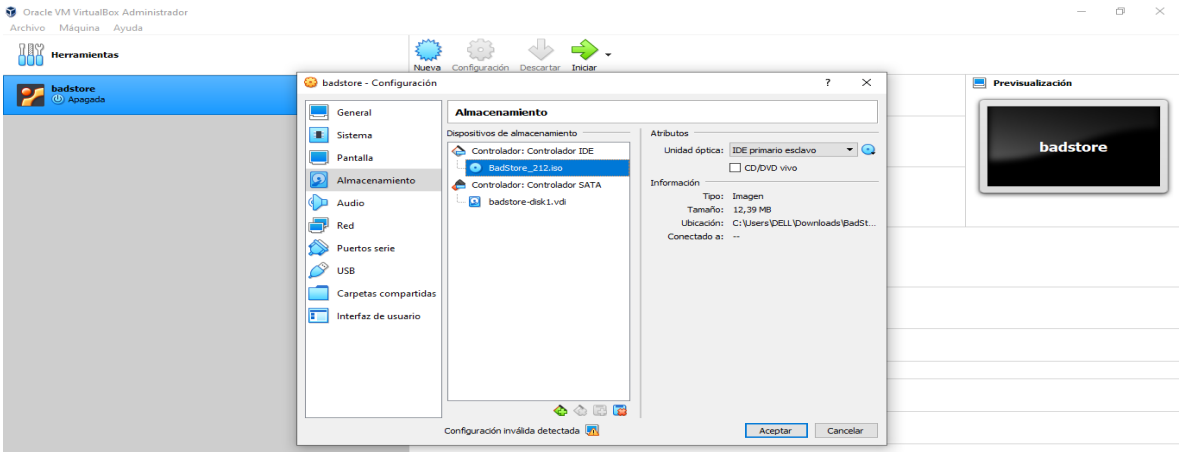


Figura. 2 Carga de iso en dispositivo de almacenamiento.

Después se configuró la red para que se comunique la maquina anfitrión con la máquina virtual que contiene Badstore, para ello se creó una red con las siguientes configuraciones:

En configurar adaptador manualmente se asignó la dirección IPv4: 192.168.100.1 y en servidor DCHP se asignó la dirección del servidor: 192.168.100.2 y se puso un límite inferior y superior de direcciones: 192.168.100.110 - 192.168.100.254.

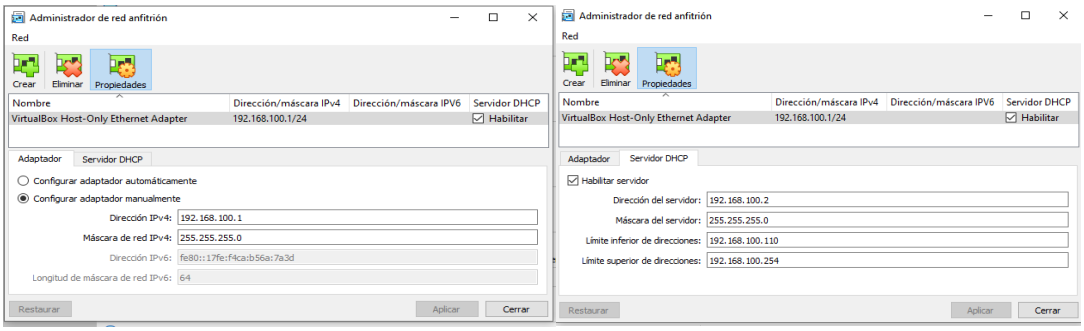


Figura. 3 Configuración de Red.

El siguiente paso fue configurar el adaptador de Red con Adaptador sólo-anfitrión que se había creado anteriormente y que permite comunicar a la maquina anfitrión con máquinas virtuales.

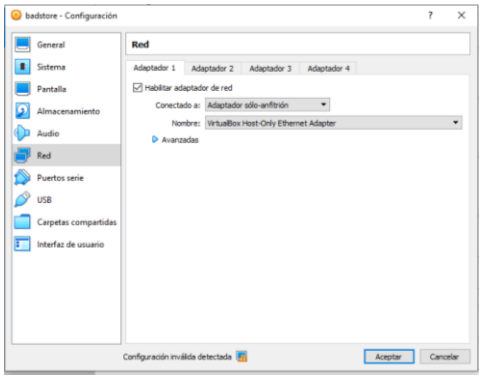


Figura. 4 Configuración de Red.

Se comprobó la dirección Ip de Badstore con ifconfig -a: 192.168.100.111

Para poder arrancar Badstore se configuró el Dns en el archivo host de la máquina en un bloc de notas como administrador agregando esta línea de código: 192.168.100.111 www.badstore.net

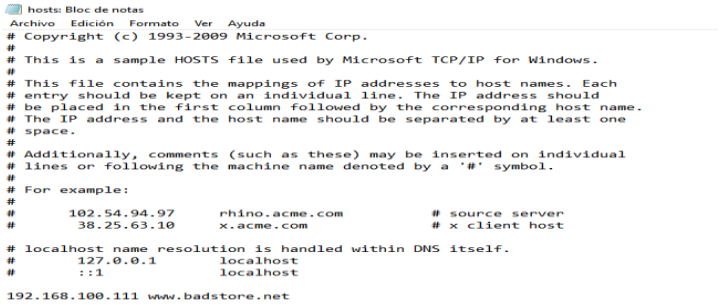


Figura. 5 Archivo hosts, configuración Dns.

En un navegador se pudo ingresar con éxito a la dirección www.badstore.net

Figura. 6 Página de prueba badstore.net

2. Reconocimiento

Para el reconocimiento se utilizó la herramienta Zenmap, en donde se especificó el objetivo y se creó un perfil de ataque.

El objetivo fue www.badstore.net

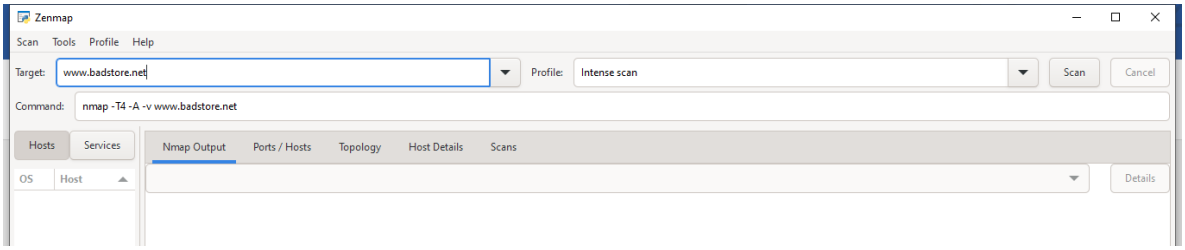


Figura. 7 Herramienta Zenmap

Se asignó un nombre al perfil en este caso “badstore”.

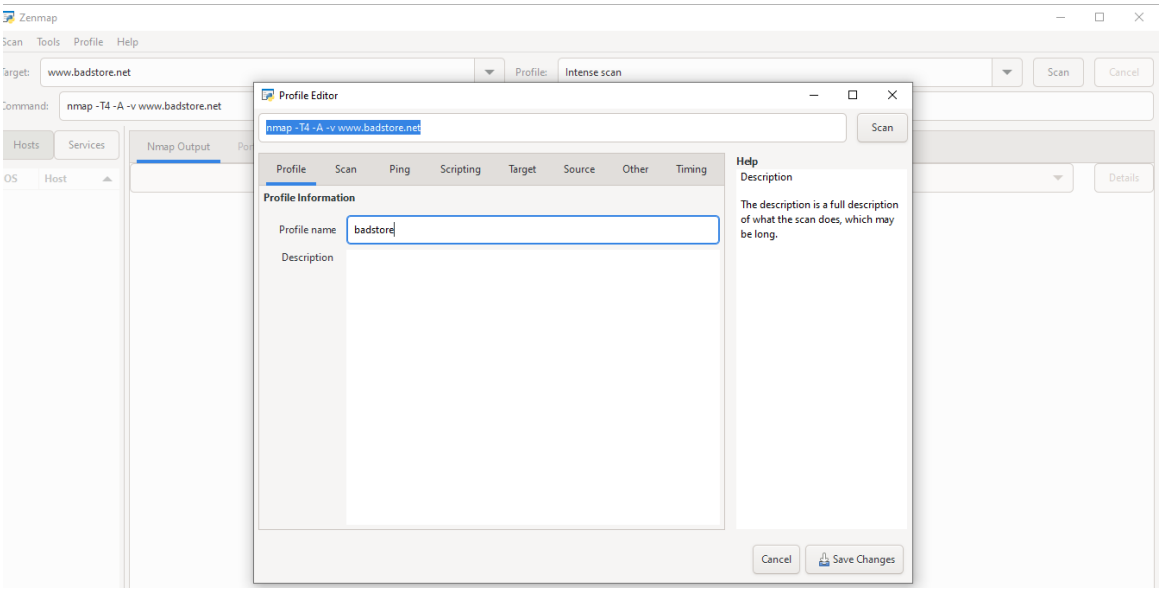


Figura. 8 Creación de Perfil badstore.

En escaneo en la parte de TCP Scan se seleccionó la opción de (TCP connect scan (-sT)) y en Timing template la opción (Aggressive (-T4)).

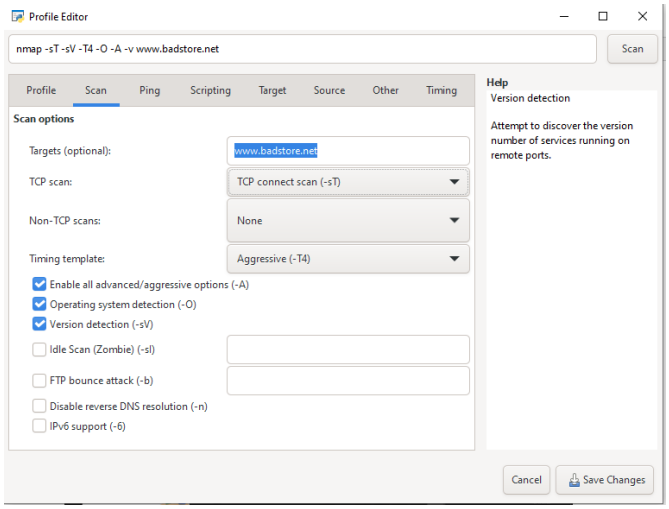


Figura. 9 Configuración del perfil badstore.

Se marcaron los siguientes scripts más importantes de tipo http y se procedió al escaneo; http auth, http backup finder, http cors, http cookies flags, http config backup, http comment displayer, http enum, http errors, http headers, http methods, http ntlm info. http open proxy, http robots.txt, http server header, http trace, http userdim enum, http waf detect, http waf fingerprint.

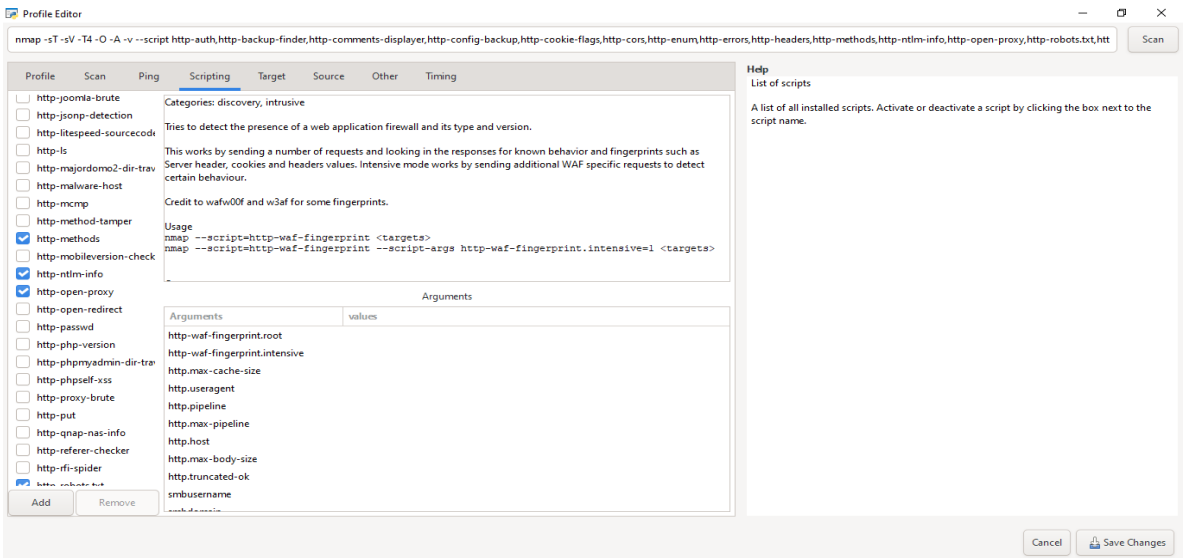


Figura. 10 Selección Scripts.

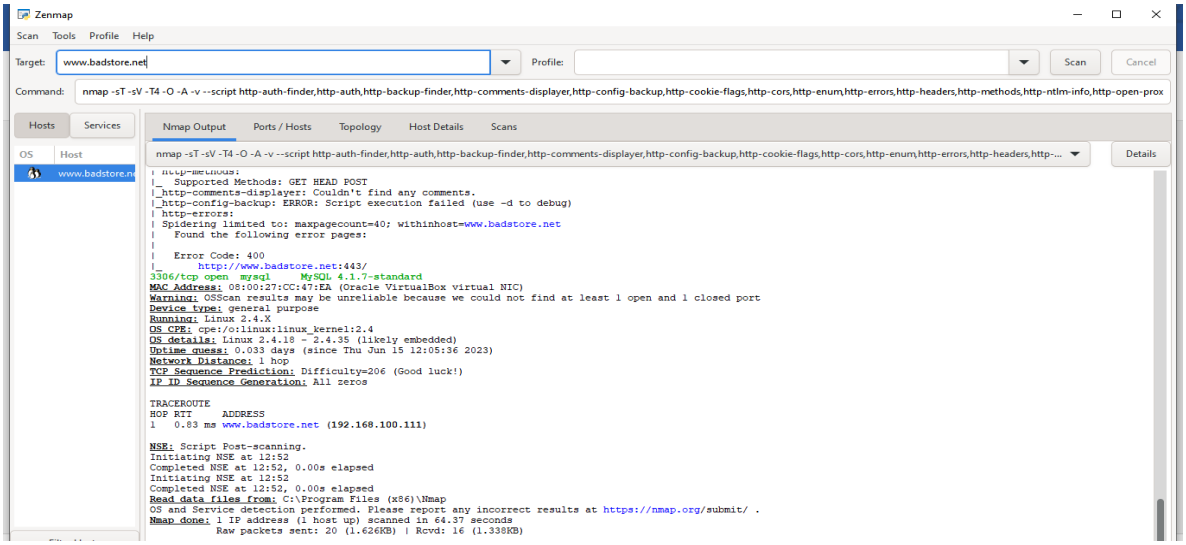


Figura. 11 Resultado de escaneo.

3. Crawling Manual y Análisis Pasivo

Para realizar el Crawling manual ingresamos en la dirección www.badstore.net en el navegador y se configuró el servidor proxy con la Ip en la que se encuentra instalado Owasp Zap, en este caso está en la máquina local.

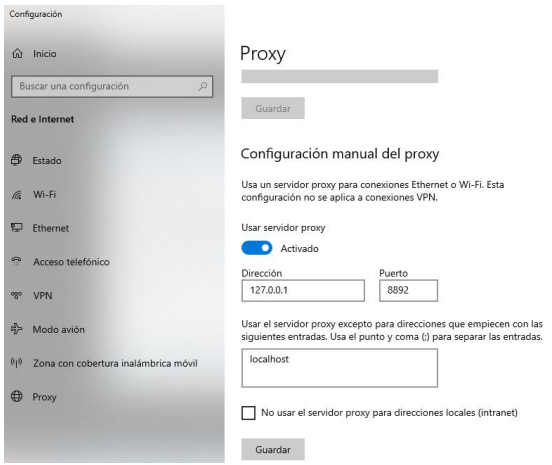


Figura. 12 Configuración de Proxy.

En la herramienta Owasp Zap se hizo la configuración del proxy para interceptar peticiones y respuestas.

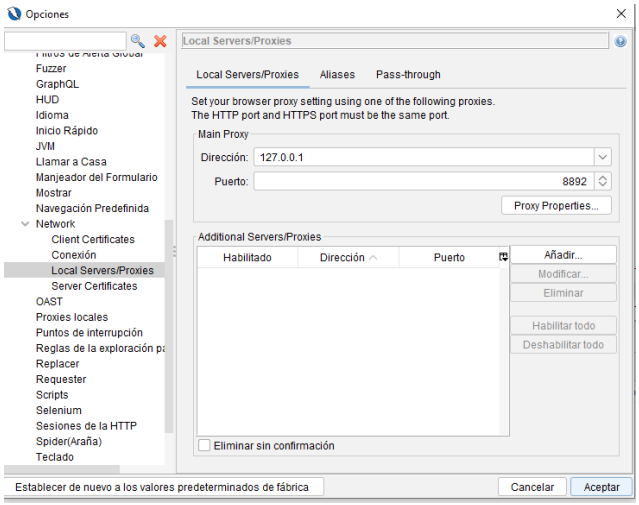


Figura. 13 Configuración del Proxy en Owasp Zap.

Se procedió a instalar los siguientes complementos dentro de Owasp Zap; Advance Sqlinjection Scanner y Pasive Scanner Ruler.

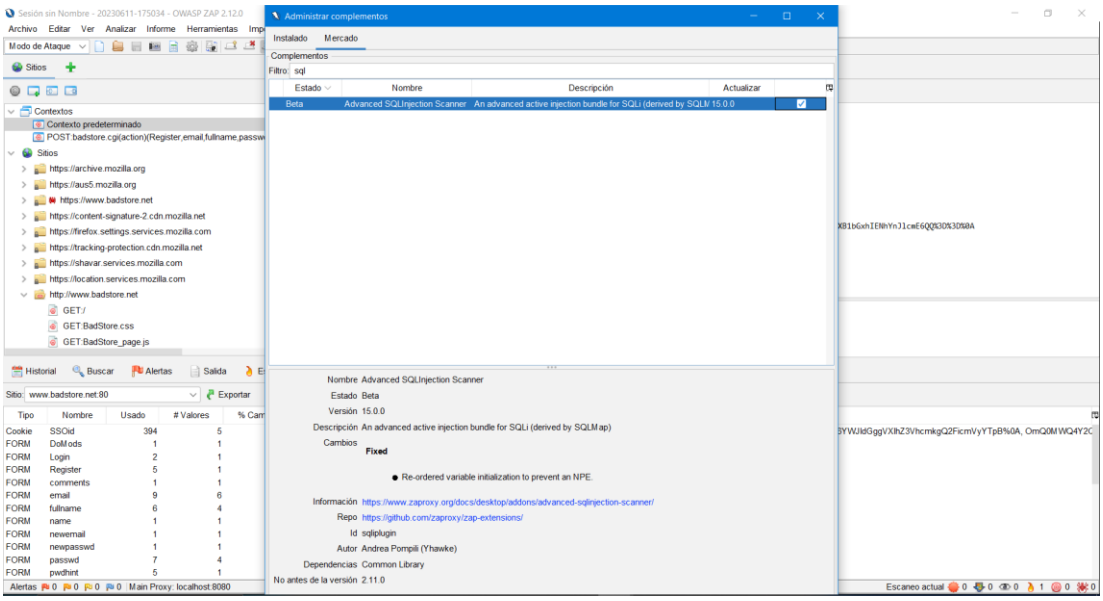


Figura. 14 Instalación de complementos

Se ingresó a www.badstore.net, se realizó toda la navegación posible, incluyendo el registro y login de un usuario nuevo para completar el Crawling manual y la herramienta capturó todas las peticiones que se hicieron con los parámetros ingresados.

Figura. 15 Página principal de perfil de usuario.

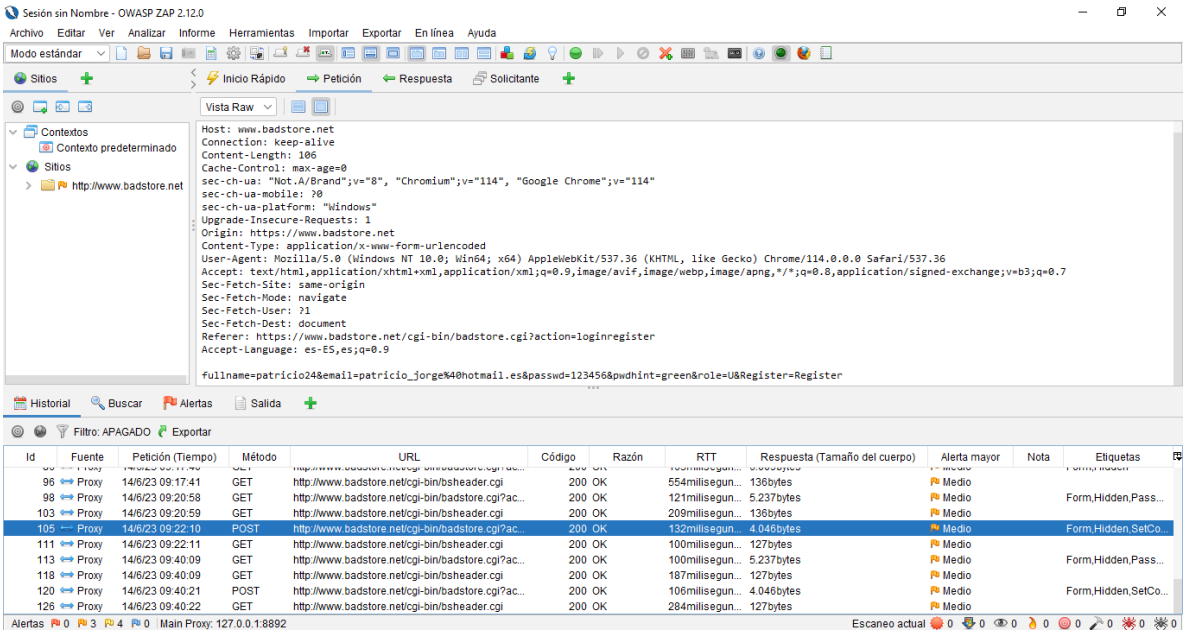


Figura. 16 Capturas de las peticiones obtenidas de la página badstore.net en Owasp Zap.

4. Crawling automático

Para hacer el Crawling automático nos situamos en la aplicación, dimos clic derecho y escogimos la opción incluir la aplicación en el contexto

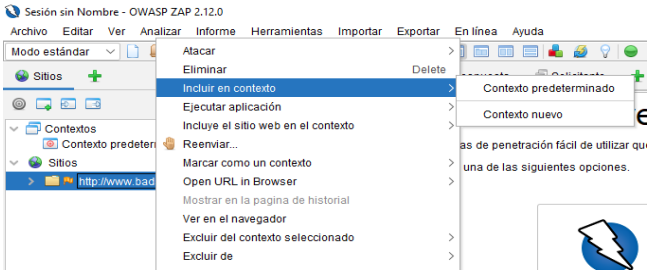


Figura. 17 Ruta para Crawling automático.

En la opción de tecnología escogimos el servidor, la base de datos, el lenguaje y el sistema operativo de badstore. En autenticación elegimos el método de autenticación basado en formularios y seleccionamos la url de login.

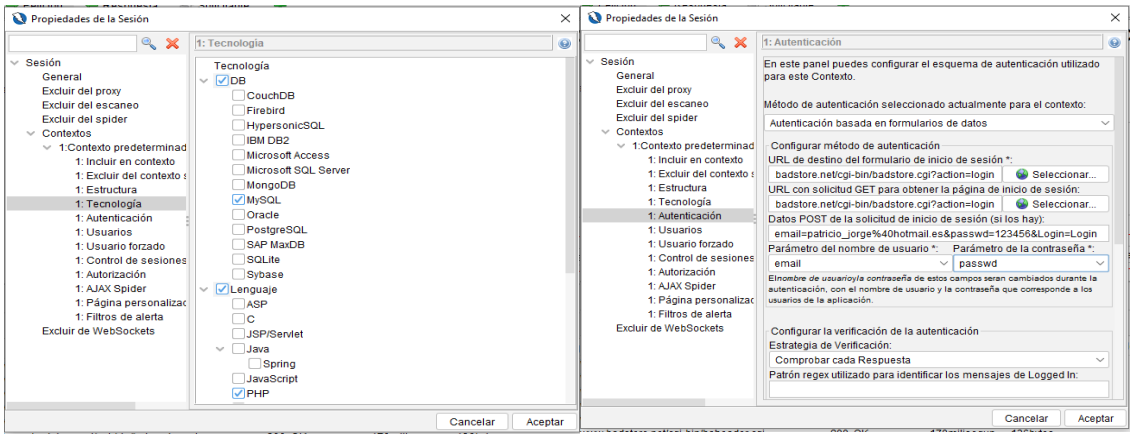


Figura. 18 Propiedades de tecnología de la sesión.

En usuario se configuró el usuario administrador y en autorización se configuró el código 401 para las respuestas q no llevan información cabecera de autentificación correcta.

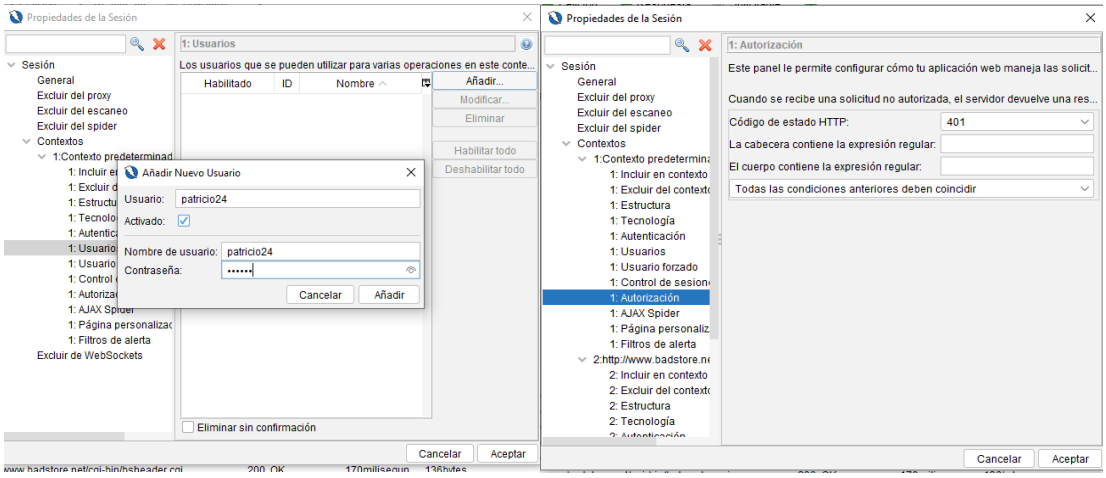


Figura. 19 Contexto Usuarios e ingreso de código 401 en contexto de Autorización.

Después dimos clic derecho en la aplicación, se seleccionó atacar y después spider

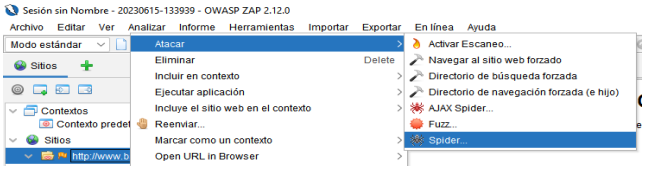


Figura. 20 Ruta para configurar Spider.

Seleccionamos el usuario y la profundidad del Crawling.

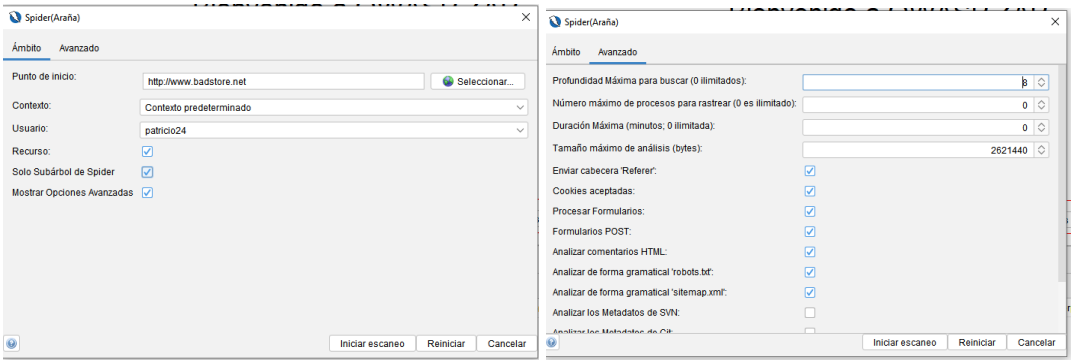


Figura. 21 Configuración Spider.

Después de este proceso se inició el escaneo y se pudieron visualizar las Url que va descubriendo la herramienta.

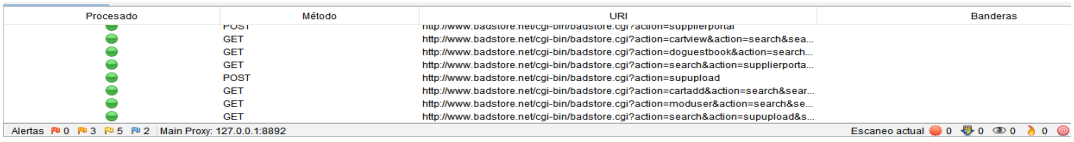


Figura. 22 Métodos obtenidos como resultado.

También se realizó un Crawling Ajax Spider para investigar ficheros código javascript en el navegador. Arrancamos el Ajax spider y seleccionamos la aplicación, el contexto, el usuario y el navegador para este caso Firefox y se inició el escaneo.

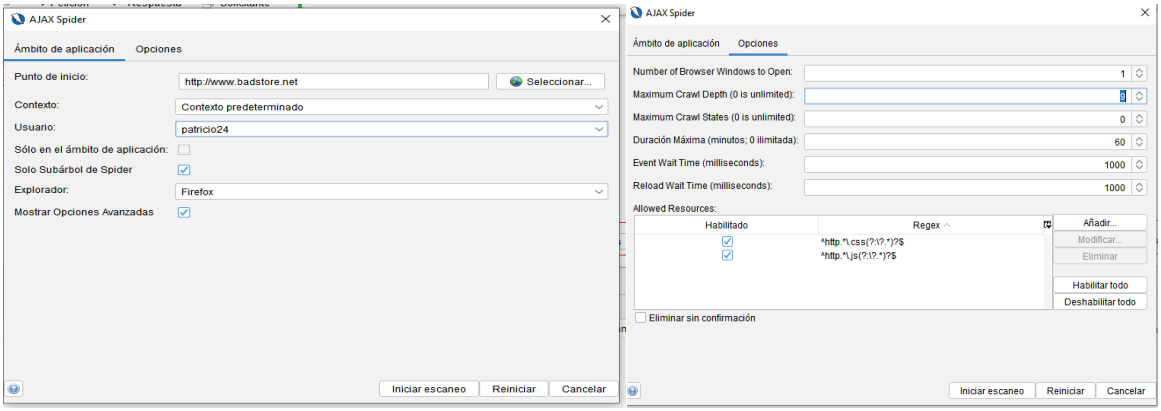


Figura. 23 Configuración Ajax Spider.

La herramienta abre el navegador Firefox y lanza peticiones a través de Firefox automáticamente, y la herramienta se encarga de todo este proceso.

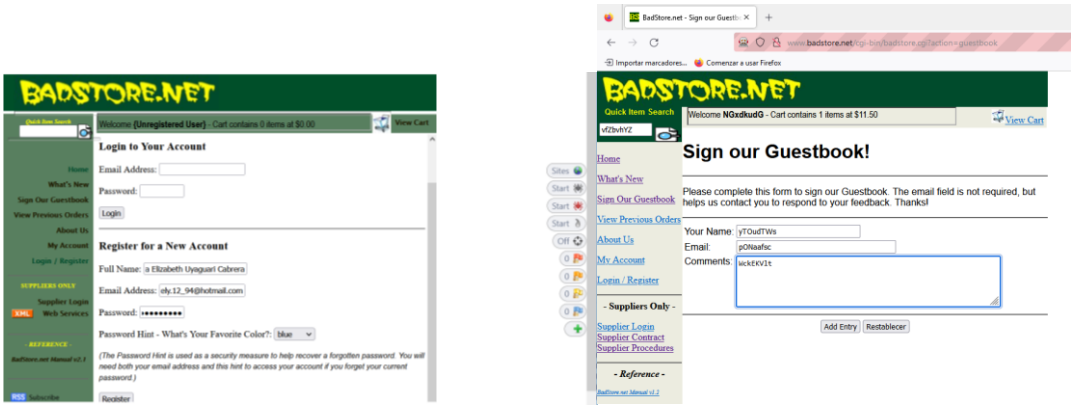


Figura. 24 Crawling manual.

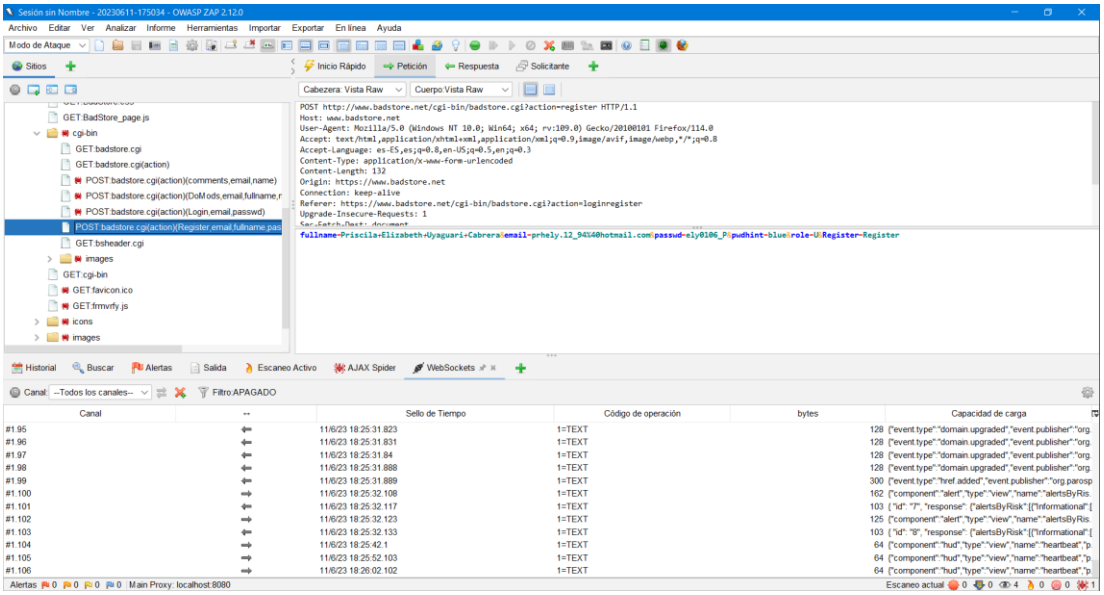


Figura. 25 Captura de registro de usuario.

Se capturó el registro y se notó que por defecto el usuario se crea con un role U, que hace referencia a un usuario común.

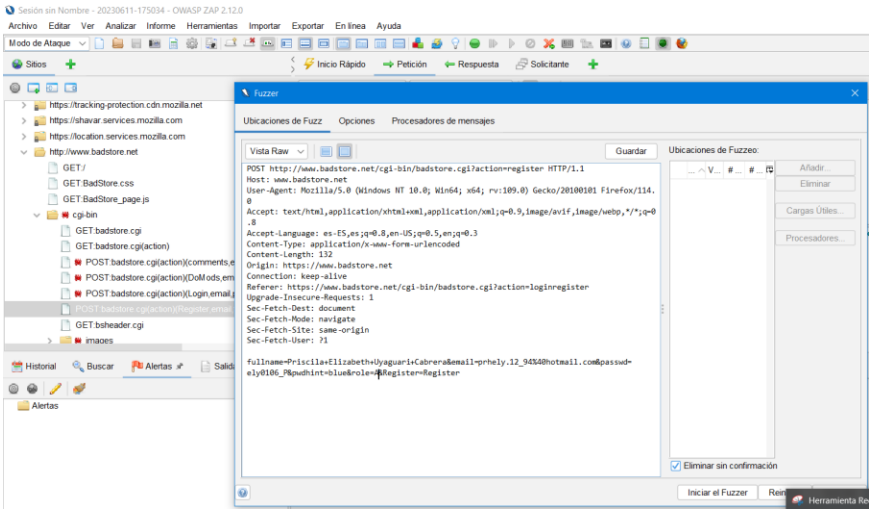


Figura. 26 Se capturó el registro notando que por

A continuación, se aplicó un fuzzer para modificar la petición de registro, y se cambió por un usuario con rol de administrador; A. En donde, se logró ingresar a la base de datos y se puedo verificar que el usuario fue identificado con un rol de administrador.

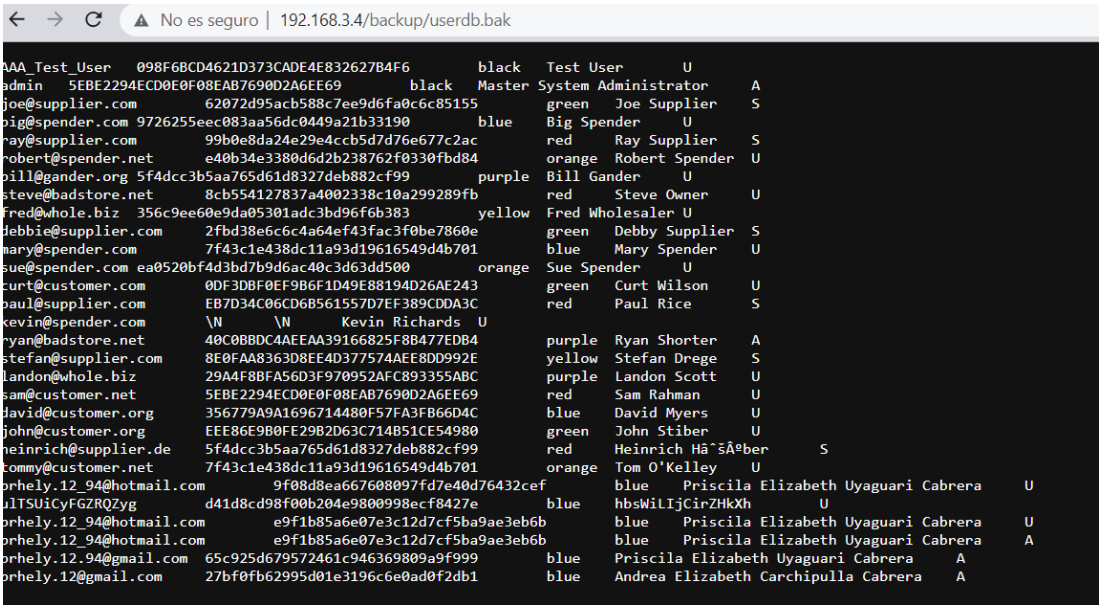
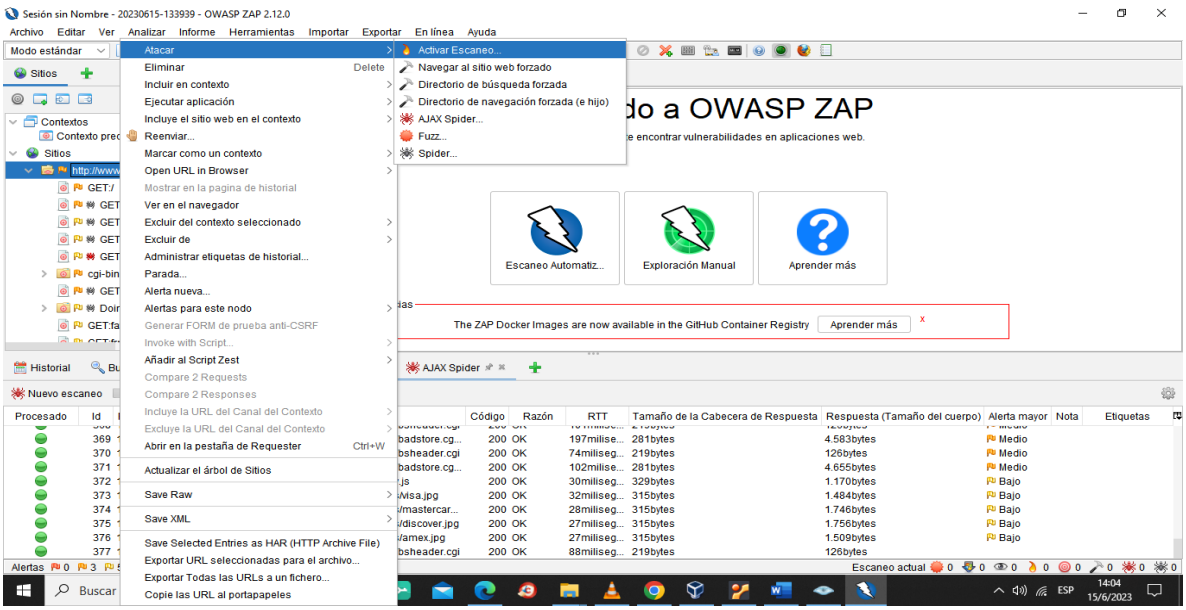


Figura. 27

5. Scan activo

Para realizar el Scan activo nos situamos en Badstore dimos clic derecho, seleccionamos atacar y después activar escaneo.



Elegimos el usuario, el contexto, la aplicación, la tecnología y definimos los vectores de entrada.

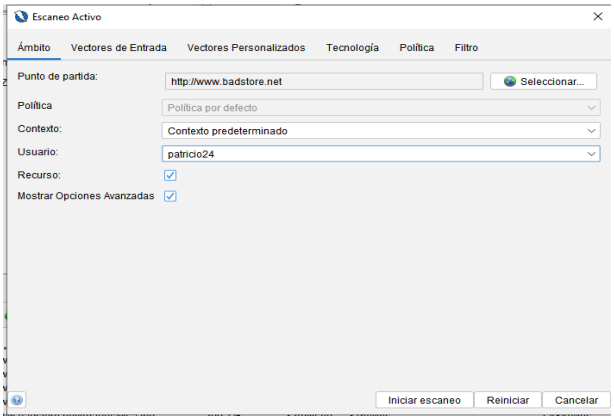


Figura. 28 Escaneo activo

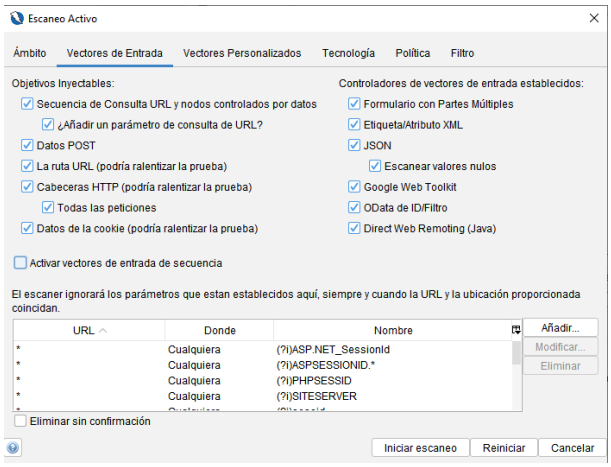


Figura. 29 Vectores de entrada

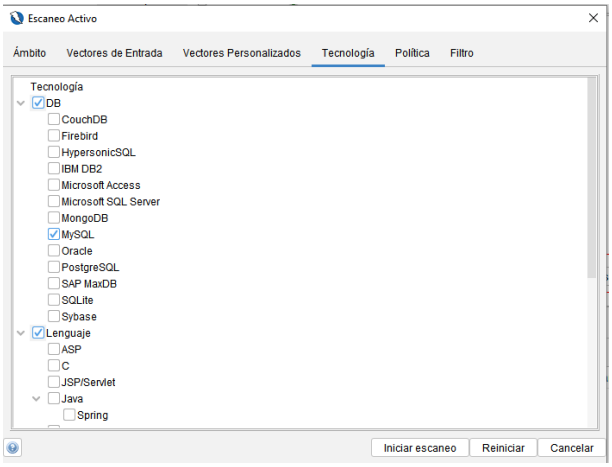


Figura. 30 Tecnología

Después de realizar todas estas configuraciones se inició el escaneo.

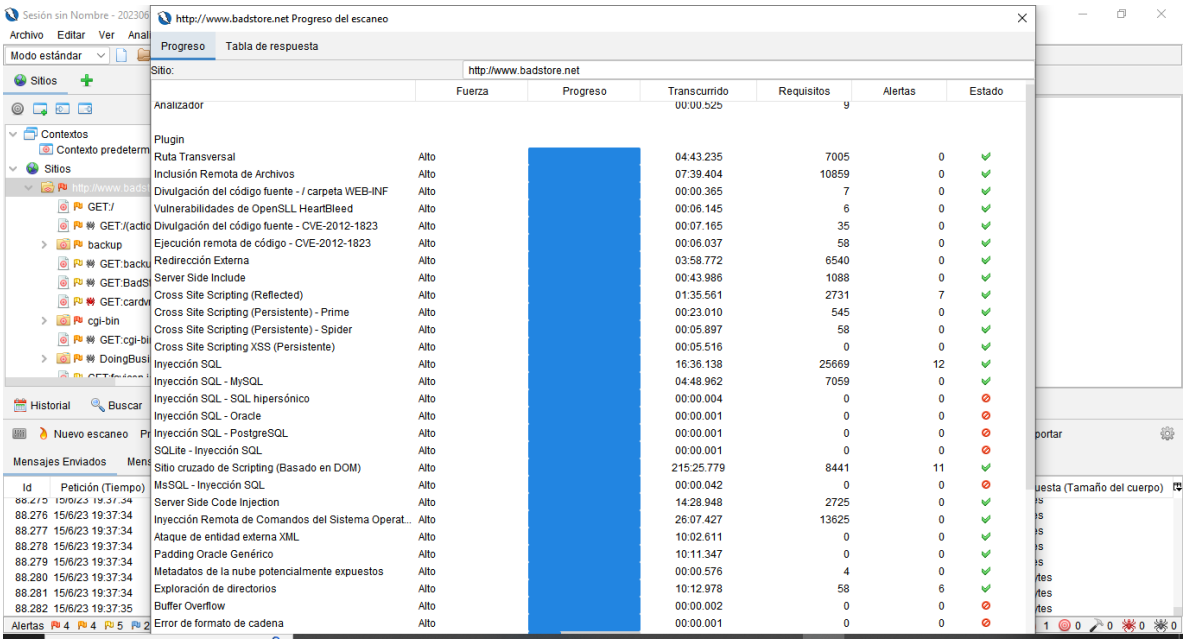


Figura. 31 Proceso escaneo

6. Auditoria

Después de haber realizado todos estos procesos se genera un fichero con extensión session, se abrió este archivo y se obtuvo el reporte del Crawling Manual, Ajax Spider y Scan Activo.

Se descubrieron las siguientes vulnerabilidades:

1. Cross_site Scripting (XSS):

Es una técnica de ataque que comprende hacer eco del código que fue proporcionado por el atacante en la instancia del navegador de un usuario

Ataque <script>alert(1);</script>

Riesgo: Alto

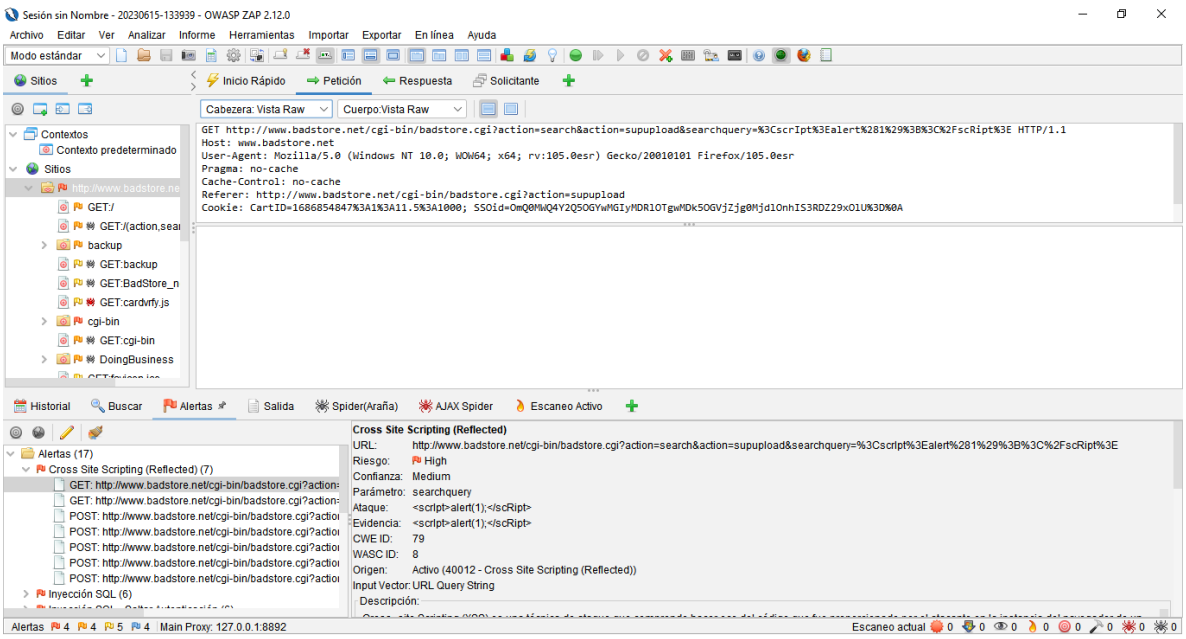


Figura. 32 Cross Site Scriptting

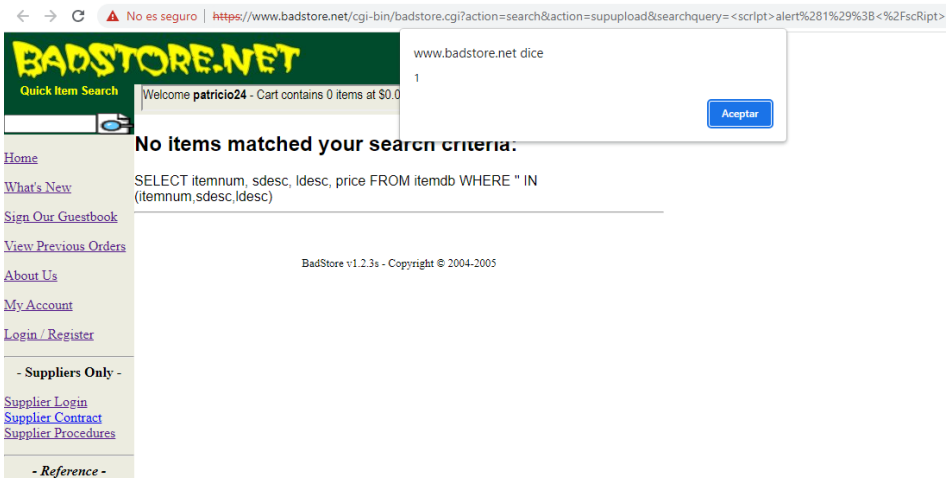


Figura. 33 Cross Site Scriptting

2. Sitio cruzado de Scripting (Basado en DOM)

Los ataques que no son persistentes y los basados en DOM necesitan que el usuario visite un enlace que fue diseñado con código maliciosos o visite alguna página web maliciosa que incluya un formulario web que, cuando se publique en el sitio que es vulnerable, originará el ataque. El uso de un formulario que es malicioso normalmente tendrá lugar cuando el recurso que es vulnerable solo acepte las solicitudes HTTP POST. En tal caso, el formulario

puede ser enviado de forma automática, sin el conocimiento de la víctima (por ejemplo, por medio de JavaScript).

Ataque #<script>alert(5397)</script>

Riesgo: Alto

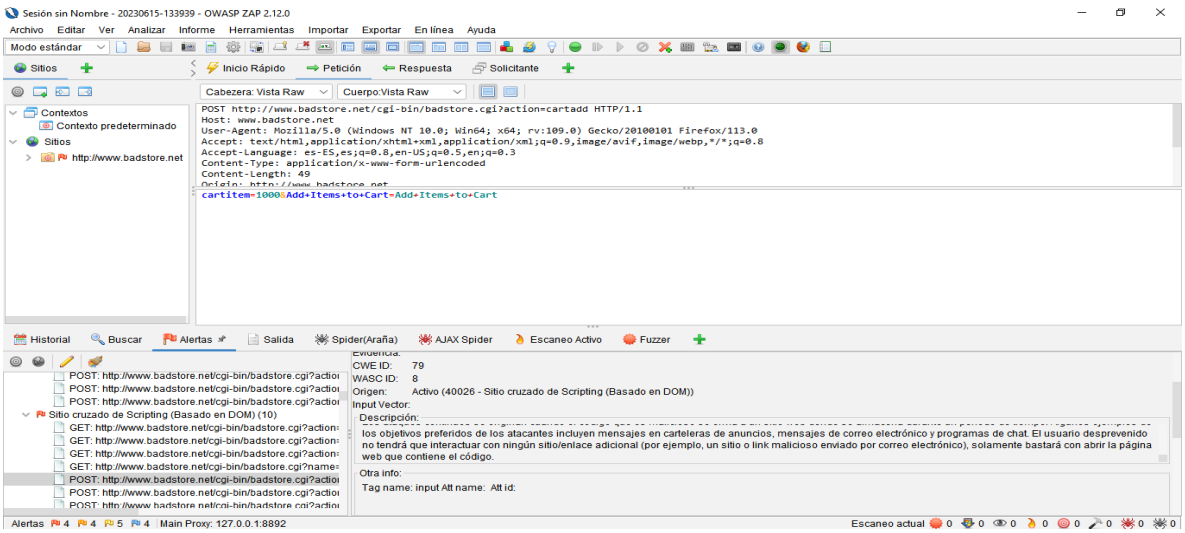


Figura. 34 Cross Site Scriptting DOM

3. Inyección Sql

La inyección SQL puede ser posible en una página de inicio de sesión, lo que potencialmente permite eludir el mecanismo de autenticación de la aplicación.

Ataque 1000' AND '1'='1' –

Riesgo: Alto

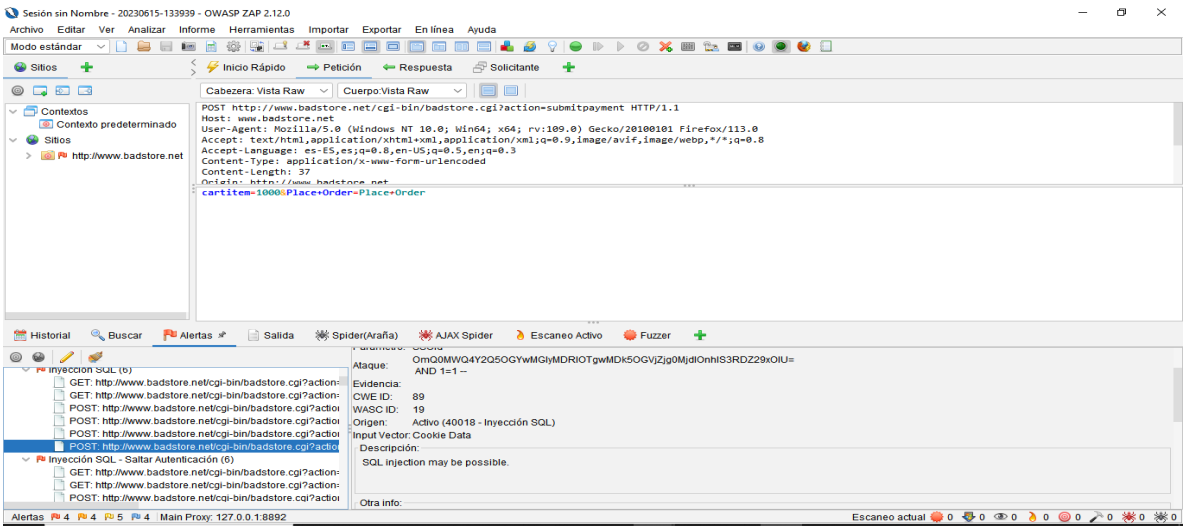


Figura. 35 Inyección Sql

7. Conclusiones

- Se realizó una descripción general de la aplicación web Badstore: (arquitectura, tecnologías utilizadas, funcionalidades principales e información relevante para comprender el contexto de la prueba de penetración)
- Se descubrieron hallazgos de crawling (identificación de páginas web, puntos de entrada, parámetros, formularios y otras áreas de interés en la aplicación)
- Se identificaron vulnerabilidades durante los procesos de Crawling y Escaneo Activo

8. Referencias Bibliográficas

Libro Electrónico:

Título: "Metasploit: The Penetration Tester's Guide"
Autores: David Kennedy, Jim O'Gorman, Devon Kearns y Mati Aharoni
Año de publicación: 2011