

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:	2
2.	Reconocimiento	4
3.	Crawling Manual y Análisis Pasivo	6
4.	Crawling automático	9
5.	Scan activo	13
6.	Auditoria	16
7.	Conclusiones	19
8.	Referencias Bibliográficas	19

1. Desarrollo:

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

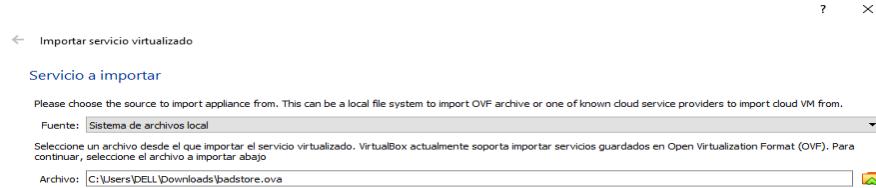


Figura. 1 Importar badstore.ova en Virtual Box.

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

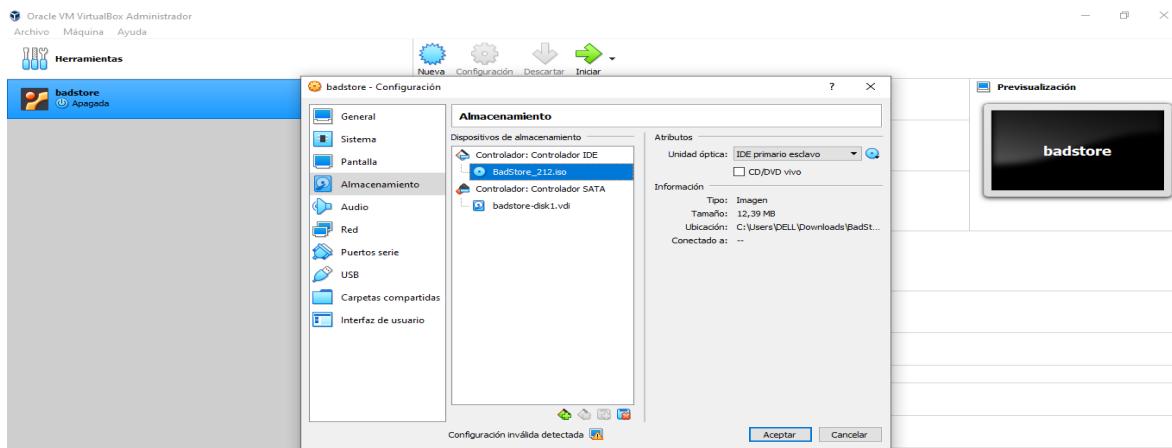


Figura. 2 Carga de iso en dispositivo de almacenamiento.

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.

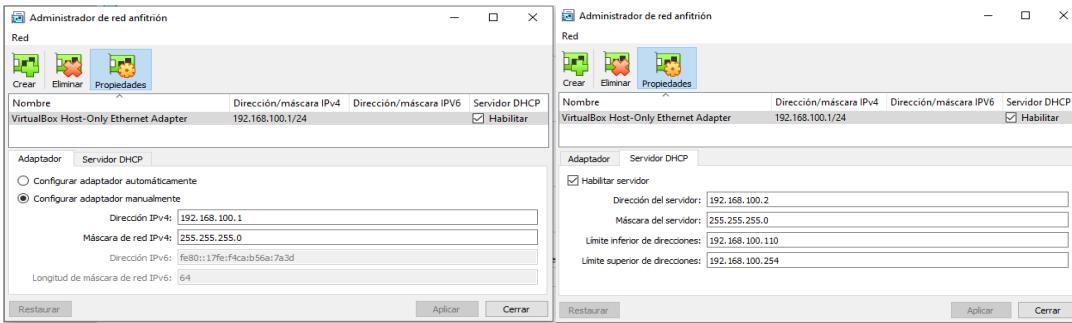


Figura. 3 Configuración de Red.

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.

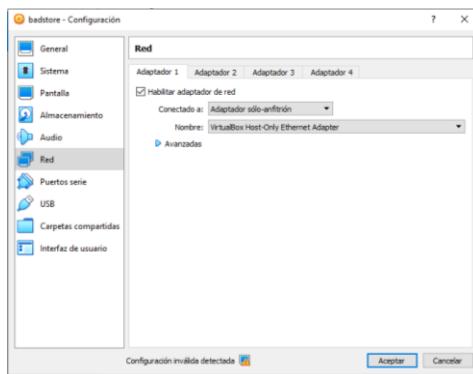


Figura. 4 Configuración de Red.

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

```

hosts: Bloc de notas
Archivo Edición Formato Ver Ayuda
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com          # source server
#      38.25.63.10          x.acme.com            # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1          localhost
#      ::1                 localhost
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

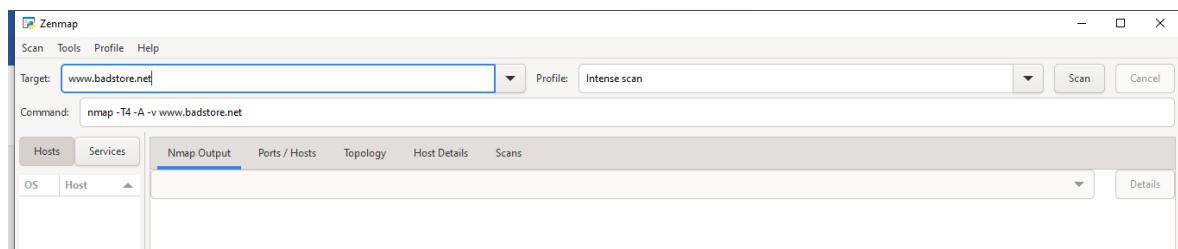


Figura. 7 Herramienta Zenmap

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

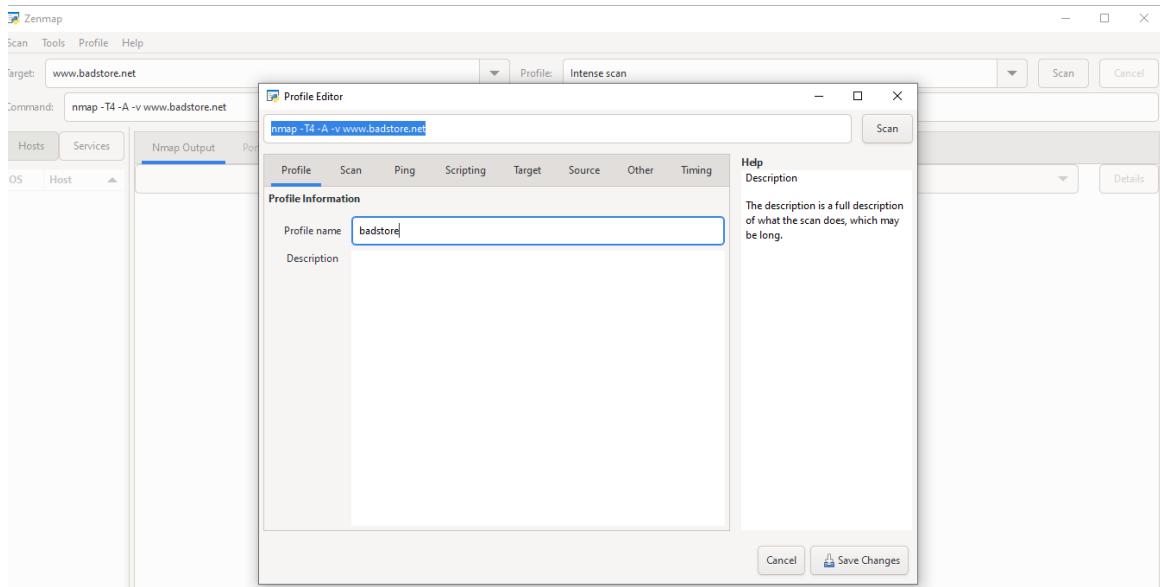


Figura. 8 Creación de Perfil badstore.

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)).

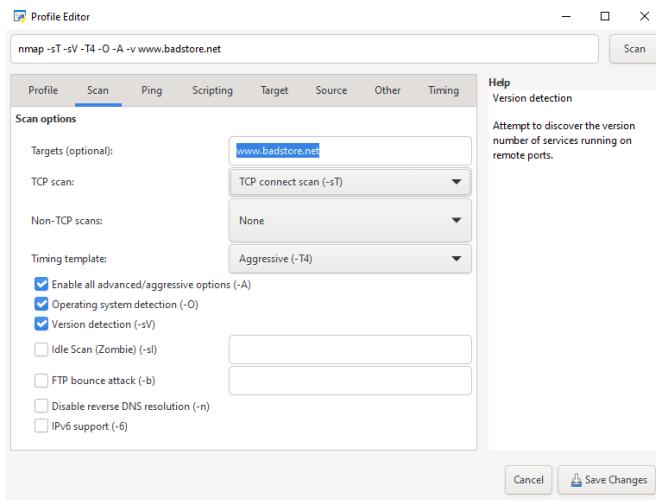


Figura. 9 Configuración del perfil badstore.

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.

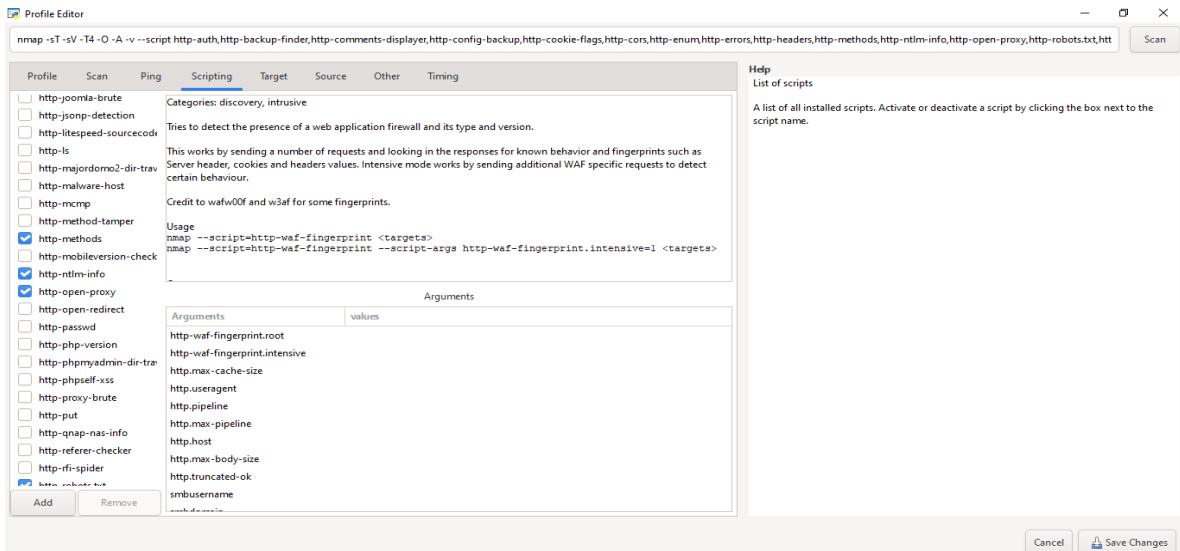


Figura. 10 Selección Scripts.

```

Nmap 7.7.0 (https://nmap.org)
Starting Nmap 7.7.0 (https://nmap.org) at 2023-06-15 12:05 CEST
NSE: Script Post-scanning.
Initiating NSE at 12:52
Completed NSE at 12:52. 0.00s elapsed
Initiating NSE at 12:52
Completed NSE at 12:52. 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap\os and service detection performance team report any incorrect results at https://nmap.org/submit/
OS and Service detection performed against www.badstore.net
Nmap done: 1 IP address (1 host up) scanned in 54.37 seconds
Raw packets sent: 20 (1.62KB) | Rcvd: 16 (1.33KB)

```

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.

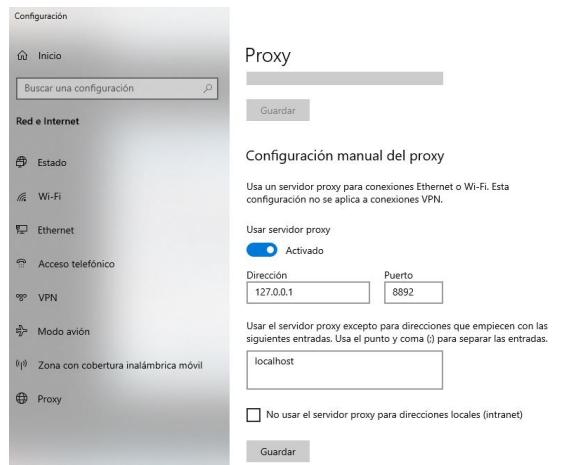


Figura. 12 Configuración de Proxy.

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

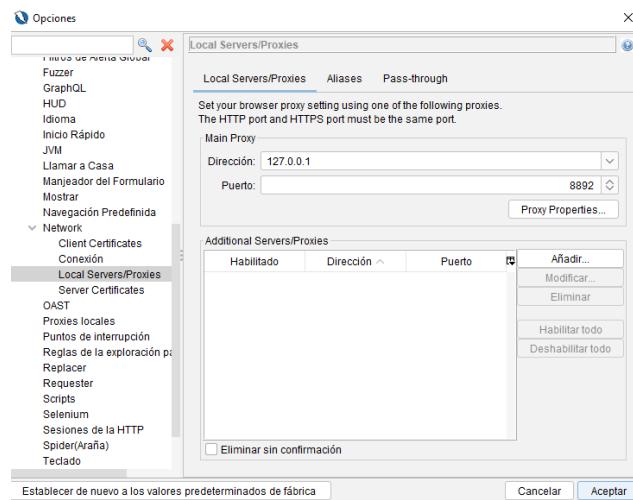


Figura. 13 Configuración del Proxy en Owasp Zap.

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

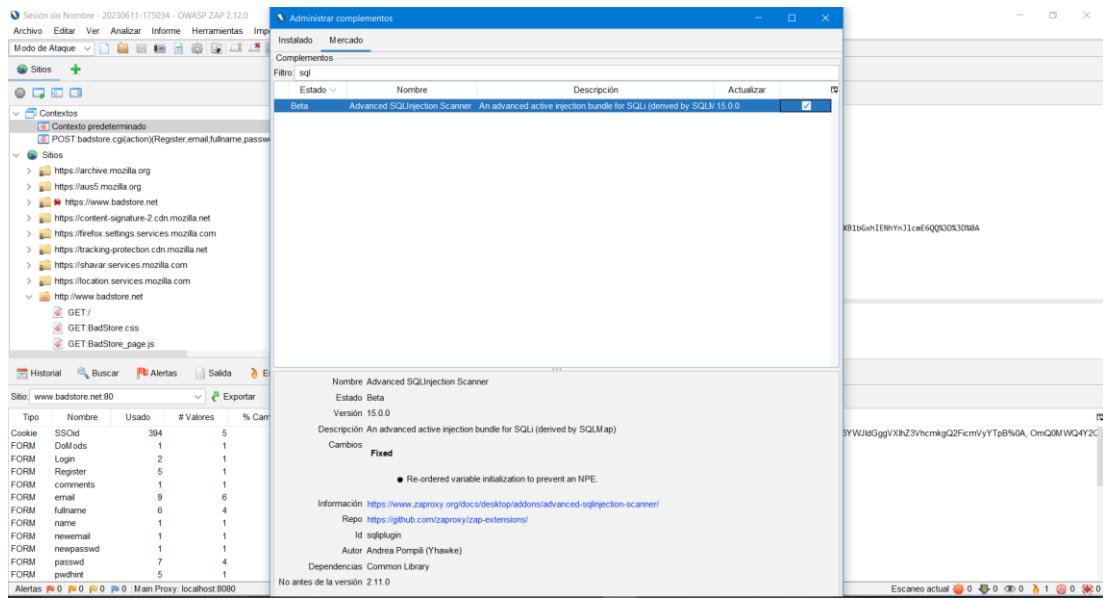


Figura. 14 Instalación de complementos

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.

Id	Fuente	Petición (Tiempo)	Método	URL	Código	Razón	RTT	Respuesta (Tamaño del cuerpo)	Alerta mayor	Nota	Etiquetas
95	Proxy	14/6/23 09:17:41	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=loginregister	200	OK	554millisegun...	136bytes	⚠️ Medio		Form,Hidden,Pass...
98	Proxy	14/6/23 09:20:58	GET	http://www.badstore.net/cgi-bin/badstore.cgi?ac...	200	OK	121millisegun...	5,237bytes	⚠️ Medio		Form,Hidden,Pass...
103	Proxy	14/6/23 09:20:59	GET	http://www.badstore.net/cgi-bin/badstore.cgi	200	OK	209millisegun...	136bytes	⚠️ Medio		Form,Hidden,Pass...
105	Proxy	14/6/23 09:22:10	POST	http://www.badstore.net/cgi-bin/badstore.cgi?ac...	200	OK	132millisegun...	4,046bytes	⚠️ Medio		Form,Hidden,SetCo...
111	Proxy	14/6/23 09:22:11	GET	http://www.badstore.net/cgi-bin/badstore.cgi	200	OK	100millisegun...	127bytes	⚠️ Medio		Form,Hidden,Pass...
113	Proxy	14/6/23 09:40:09	GET	http://www.badstore.net/cgi-bin/badstore.cgi?ac...	200	OK	100millisegun...	5,237bytes	⚠️ Medio		Form,Hidden,Pass...
118	Proxy	14/6/23 09:40:09	GET	http://www.badstore.net/cgi-bin/badstore.cgi	200	OK	187millisegun...	127bytes	⚠️ Medio		Form,Hidden,Pass...
120	Proxy	14/6/23 09:40:21	POST	http://www.badstore.net/cgi-bin/badstore.cgi?ac...	200	OK	106millisegun...	4,046bytes	⚠️ Medio		Form,Hidden,SetCo...
126	Proxy	14/6/23 09:40:22	GET	http://www.badstore.net/cgi-bin/badstore.cgi	200	OK	284millisegun...	127bytes	⚠️ Medio		Form,Hidden,SetCo...

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

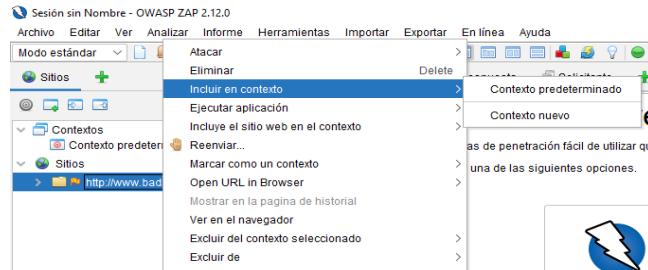


Figura. 17 Ruta para Crawling automático.

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.

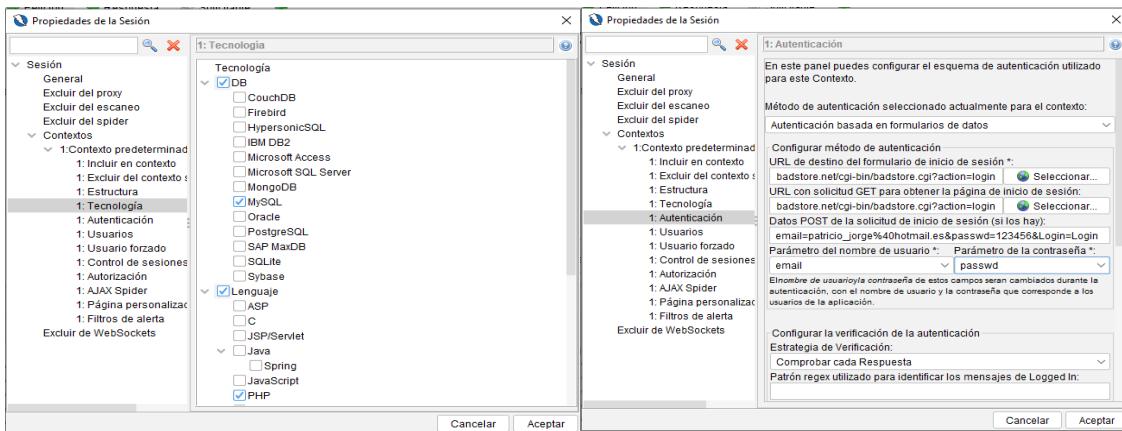


Figura. 18 Propiedades de tecnología de la sesión.

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

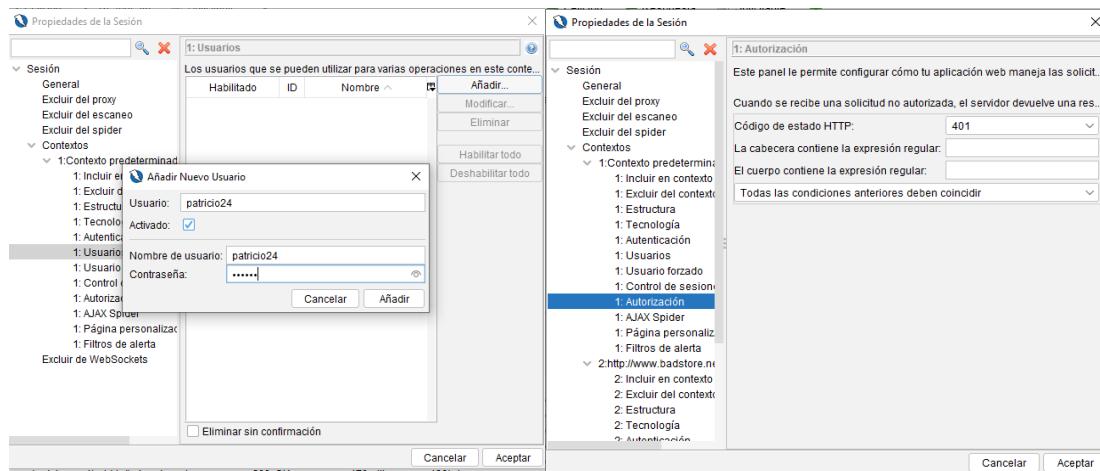


Figura. 19 Contexto Usuarios e ingreso de código 401 en contexto de Autorización.

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.

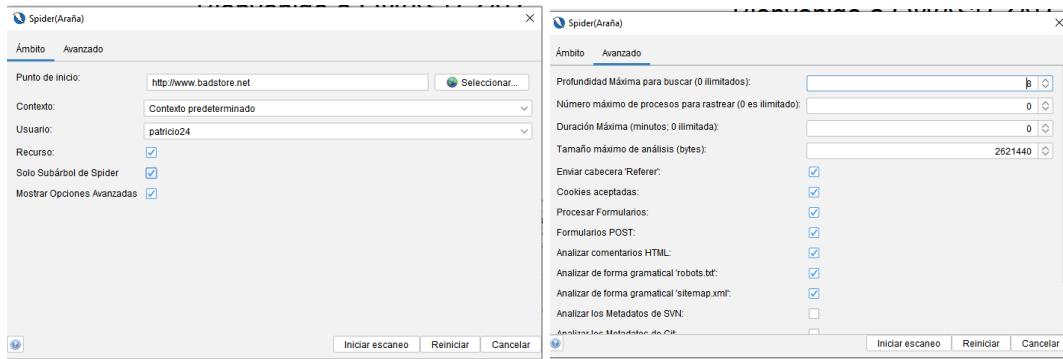


Figura. 21 Configuración Spider.

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

Procesado	Método	URI	Banderas
0	POST	http://www.badstore.net/cgi-bin/badstore.cgi?action=search&sea...	
1	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=cartview&action=search&sea...	
2	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=doguestbook&action=search...	
3	POST	http://www.badstore.net/cgi-bin/badstore.cgi?action=search&action=supplierport...	
4	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=supplierport...	
5	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=supupload...	
6	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=cartadd&action=search&sear...	
7	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=moduser&action=search&sear...	
8	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=search&action=supupload&se...	

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.

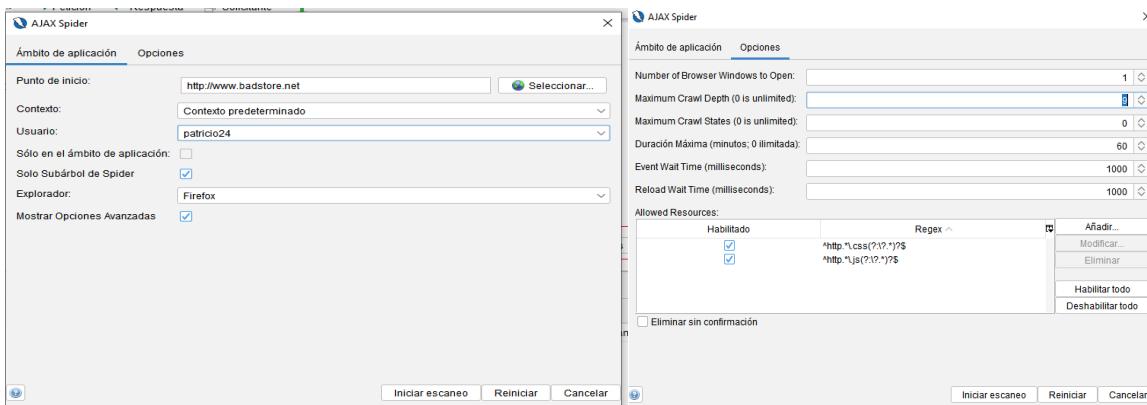


Figura. 23 Configuración Ajax Spider.

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

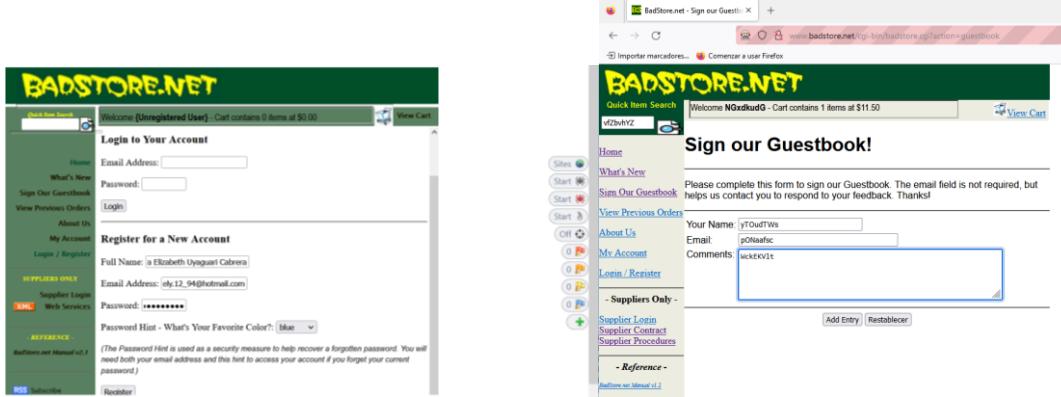


Figura. 24 Crawling manual.

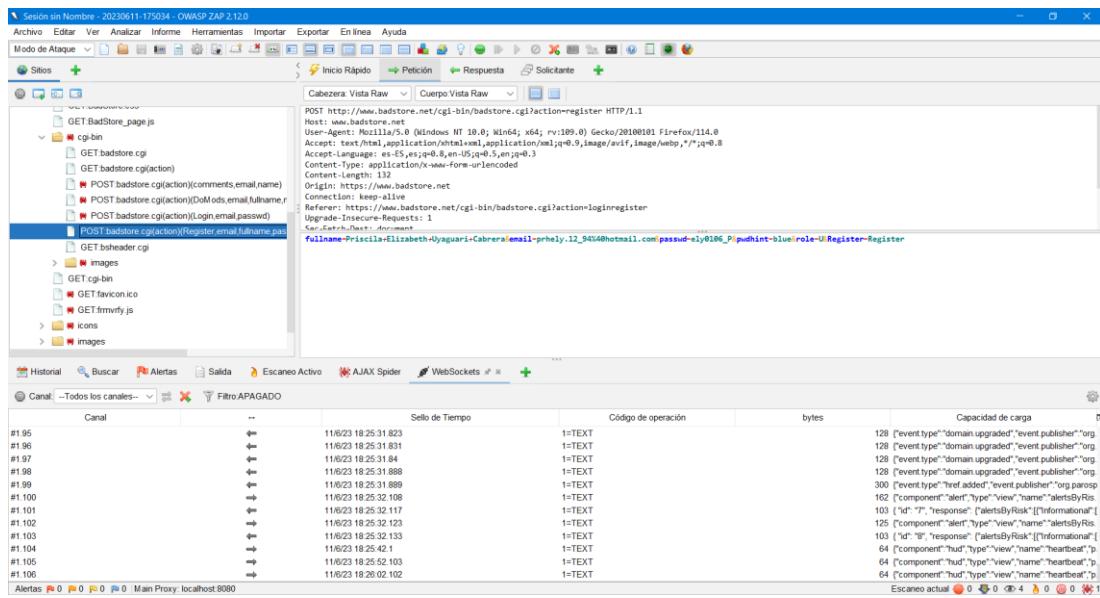


Figura. 25 Captura de registro de usuario.

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.

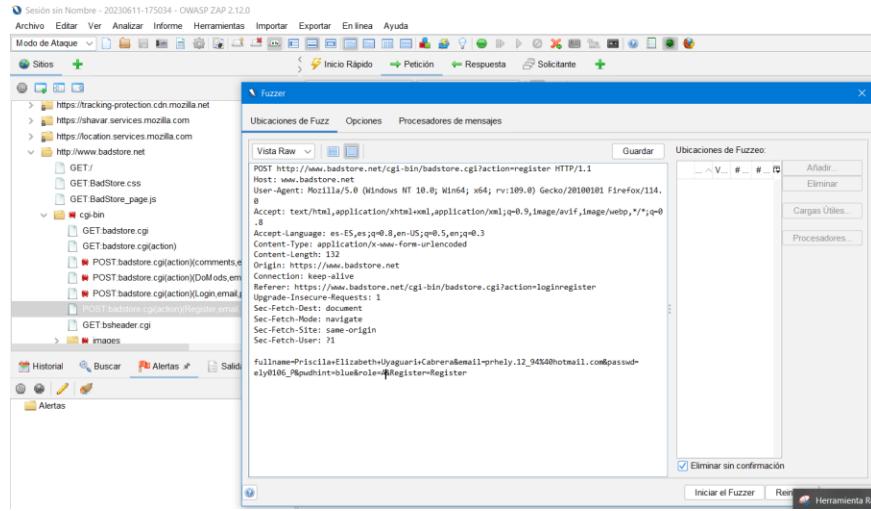


Figura. 26 Se capturó el registro notando que por

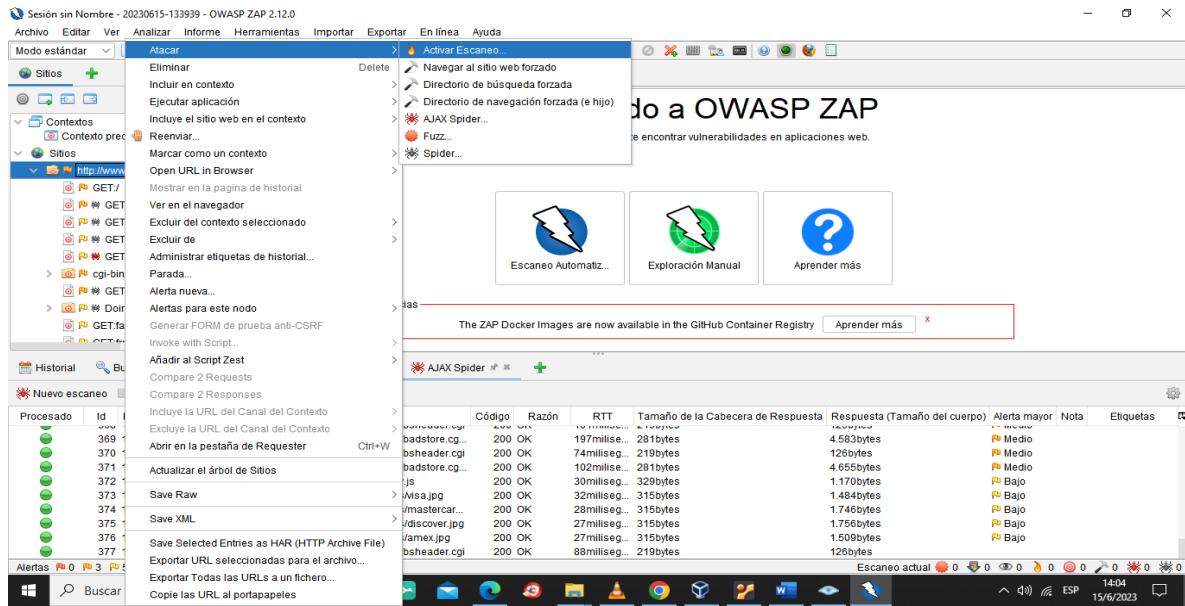
A continuación, se aplicó un fuzzer para modificar la petición de registro, y se cambió por un usuario con rol de administrador; A. En donde, se logró ingresar a la base de datos y se pudo verificar que el usuario fue identificado con un rol de administrador.

No es seguro 192.168.3.4/backup/userdb.bak						
AAA_Test_User	098F6BCD04621D373CADC4E832627B4F6	black	Test User	U		
admin	5EBE2294EC00E0F08EA87690D2A6EE69	black	Master System Administrator	A		
joe@supplier.com	62072d95acb588c7ee9d6fa0c6c85155	green	Joe Supplier	S		
bigspender.com	9726295eec083a56dc0449a21b31910	blue	Big Spender	U		
ray@supplier.com	99b0e8da24e29e4ccb5d7d76e677c2ac	red	Ray Supplier	S		
robert@spender.net	e40b34e3380dd62b238762f0330fb84	orange	Robert Spender	U		
bill@gander.org	5f4dcc3b765d61d8327deb882cf99	purple	Bill Gander	U		
steve@badstore.net	8cb554127837a4002338c10a299289fb	red	Steve Owner	U		
Fred@whole.biz	356c9ee60e9da05301adc3bd96f6b383	yellow	Fred Wholesaler	U		
debbie@supplier.com	2fb38e6c6c4a64ef43fac3f0be7860e	green	Debby Supplier	S		
mary@spender.com	7f43c1e438dc11a93d19616549d4b701	blue	Mary Spender	U		
sue@spender.com	ea0520bf4d3bd7b9d6ac40c3d63dd500	orange	Sue Spender	U		
curt@customer.com	0DF3DBF0EF8B6F1D49E88194D26AE243	green	Curt Wilson	U		
paul@supplier.com	EB7D34C06CD6B561557D7EF389CDDA3C	red	Paul Rice	S		
kevin@spender.com	\N \N Kevin Richards	U				
ryan@badstore.net	40C0BBDC4AEAA39166825F8B477EDB4	purple	Ryan Shorter	A		
stefan@supplier.com	8E0FAA8363D8EE4D377574AE8DD992E	yellow	Stefan Drege	S		
landon@whole.biz	29A4F8BF8A56D3F970952AFC893355ABC	purple	Landon Scott	U		
san@customer.net	5EBE2294EC00E0F08EA87690D2A6EE69	red	San Rahman	U		
david@customer.org	356779A91696714480F57FA3FB66D4C	blue	David Myers	U		
john@customer.org	EEE86E9B0FE29B2D63C714851CE54980	green	John Stiber	U		
heinrich@supplier.de	5f4dcc3b5aa765d61d8327deb882cf99	red	Heinrich H��ber	S		
tommy@customer.net	7f43c1e438dc11a93d19616549d4b701	orange	Tom O'Kelley	U		
prhely.12_94@hotmail.com	9f08d8ea667608097fd7e40d76432cef	blue	Priscila Elizabeth Uyaguari Cabrera	U		
ulTSUiYfGZRQZyg	d41d8cd98f0b204e9800998ecfb427e	blue	hb5wIjCirZhXh	U		
prhely.12_94@hotmail.com	e9f1b85a6e07e3c12d7cf5ba9ae3eb6b	blue	Priscila Elizabeth Uyaguari Cabrera	U		
prhely.12_94@hotmail.com	e9f1b85a6e07e3c12d7cf5ba9ae3eb6b	blue	Priscila Elizabeth Uyaguari Cabrera	A		
prhely.12_94@gmail.com	65c925d679572461c946369809a9f999	blue	Priscila Elizabeth Uyaguari Cabrera	A		
prhely.12@gmail.com	27bf0fb62995d01e3196c6e0ad0f2db1	blue	Andrea Elizabeth Carchipulla Cabrera	A		

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.

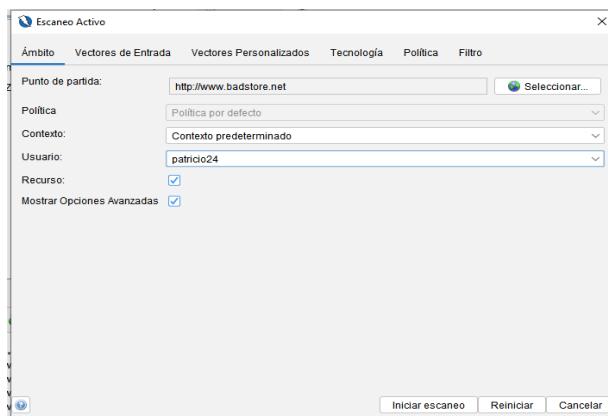


Figura. 28 Escaneo activo

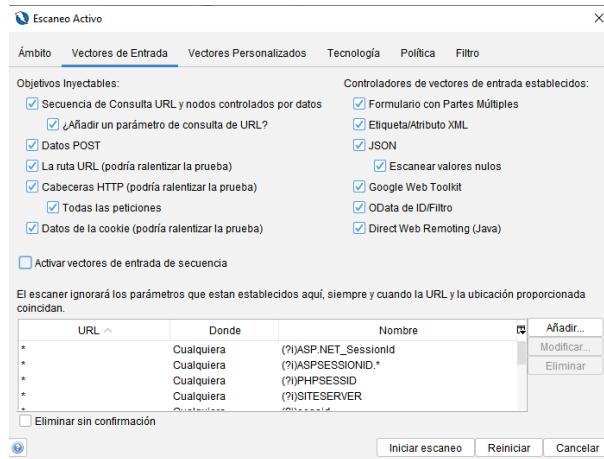


Figura. 29 Vectores de entrada

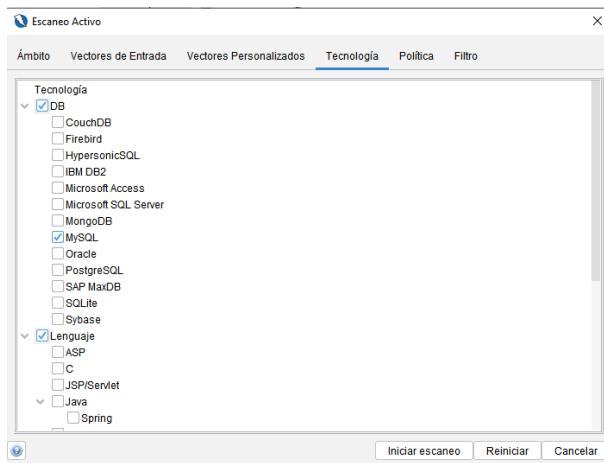


Figura. 30 Tecnología

Después de realizar todas estas configuraciones se inició el escaneo.

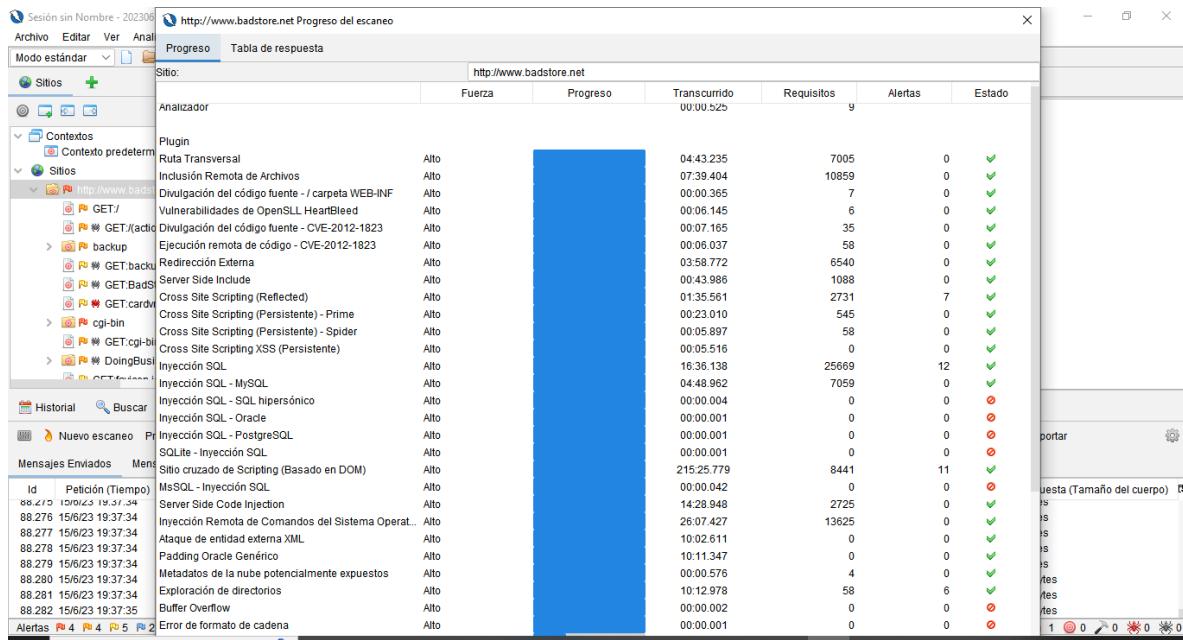


Figura. 31 Proceso escaneo

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

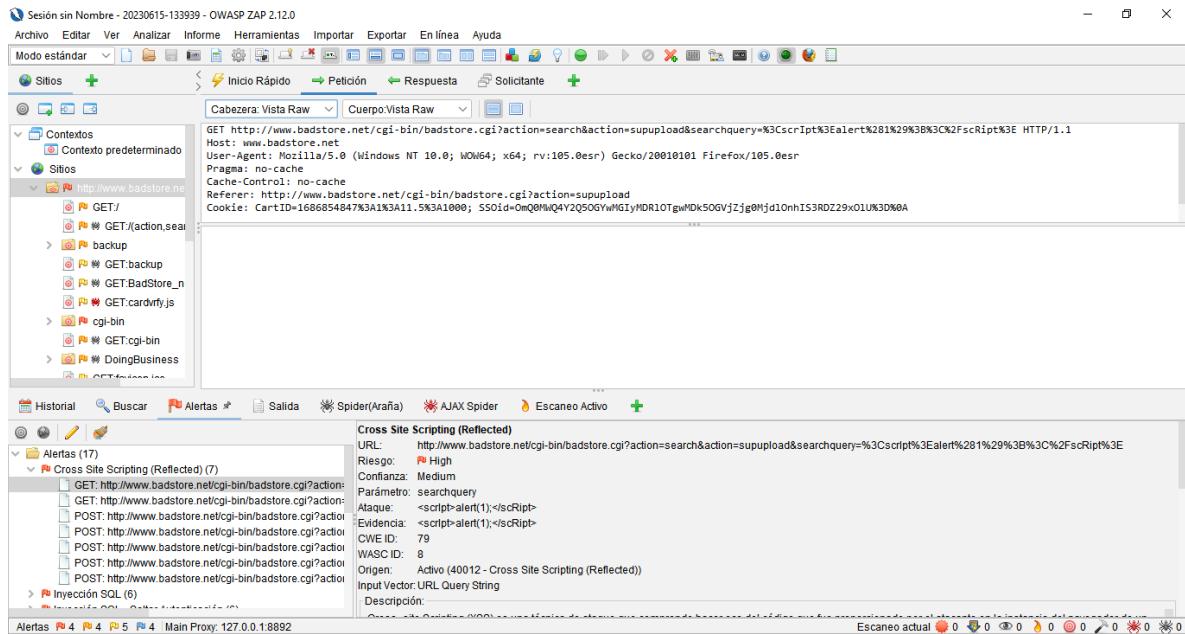


Figura. 32 Cross Site Scriptting

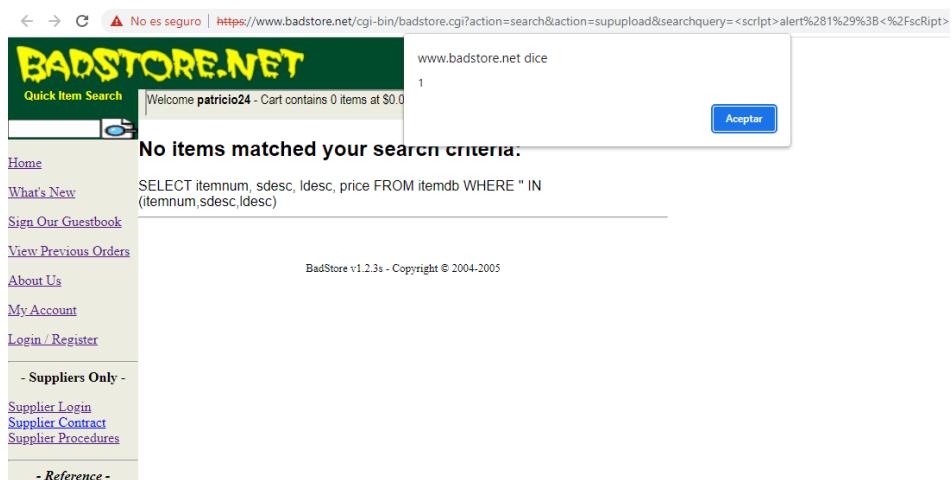


Figura. 33 Cross Site Scriptting

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

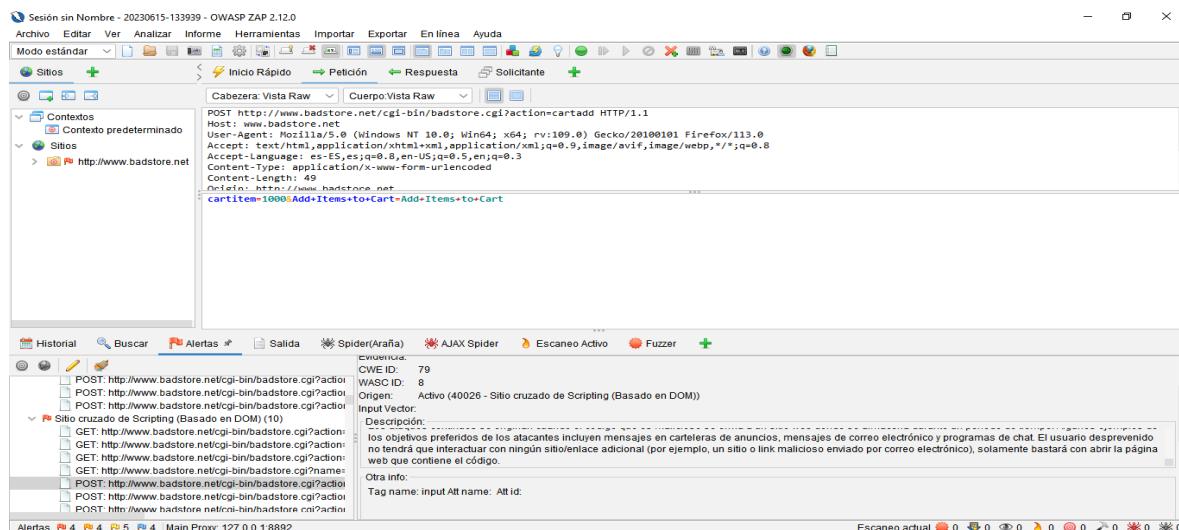


Figura. 34 Cross Site Scriptting DOM

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

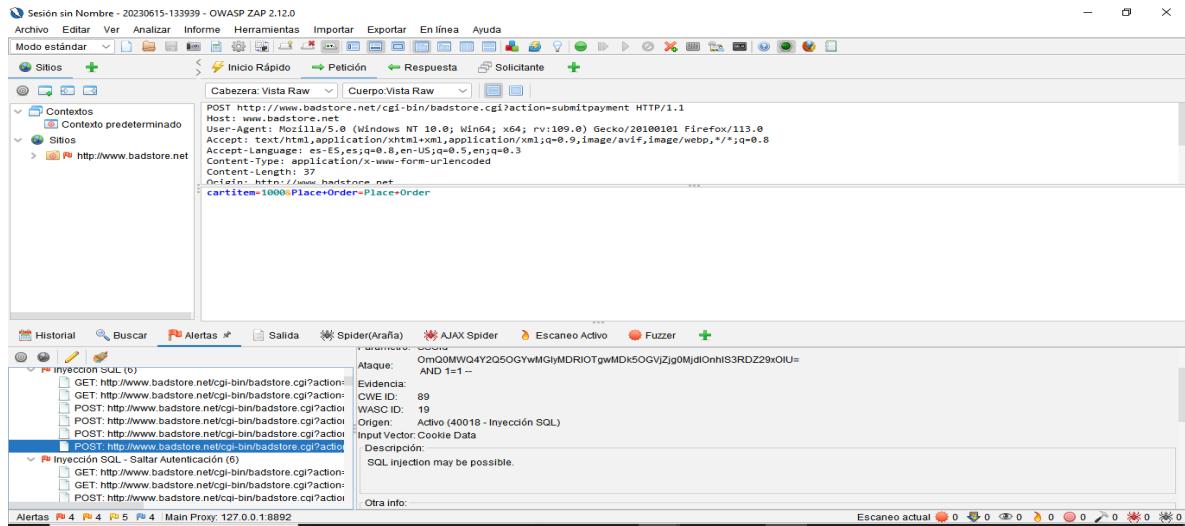


Figura. 35 Inyección Sql

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