



“Universidad Internacional de La Rioja en México”

Seguridad en Sistemas, Aplicaciones y Datos Masivos

Proyecto:

Actividad 3: Test de penetración a la aplicación web
Badstore utilizando una herramienta de análisis
dinámico.

Profesor:

Dra. María Teresa Pérez Morales

Autor:

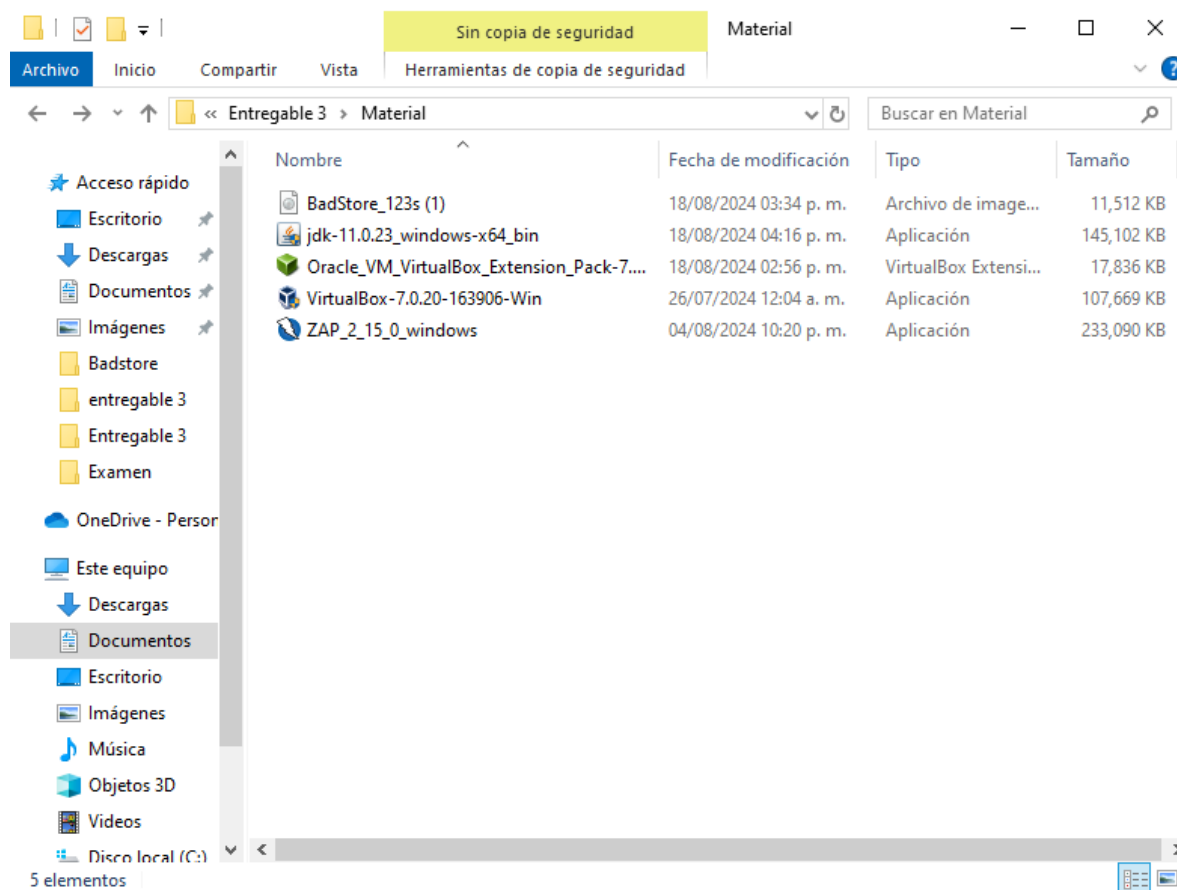
Ing. Juan Luis Cruz Aristeo.

Fecha de entrega:

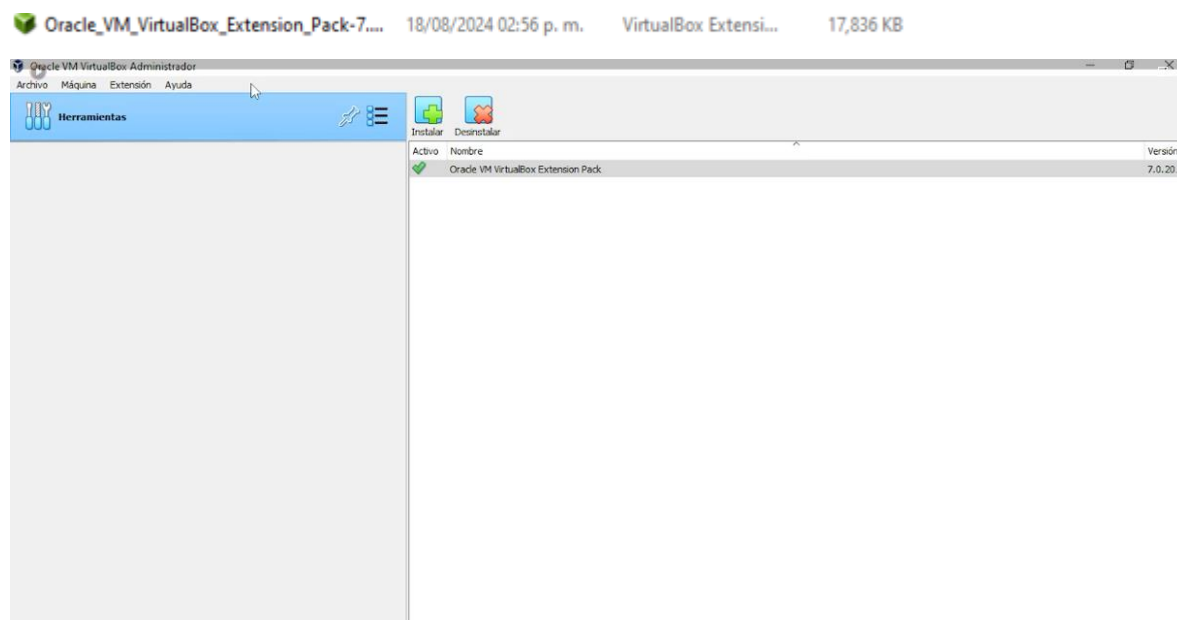
19/08/2024

Confección de memoria.

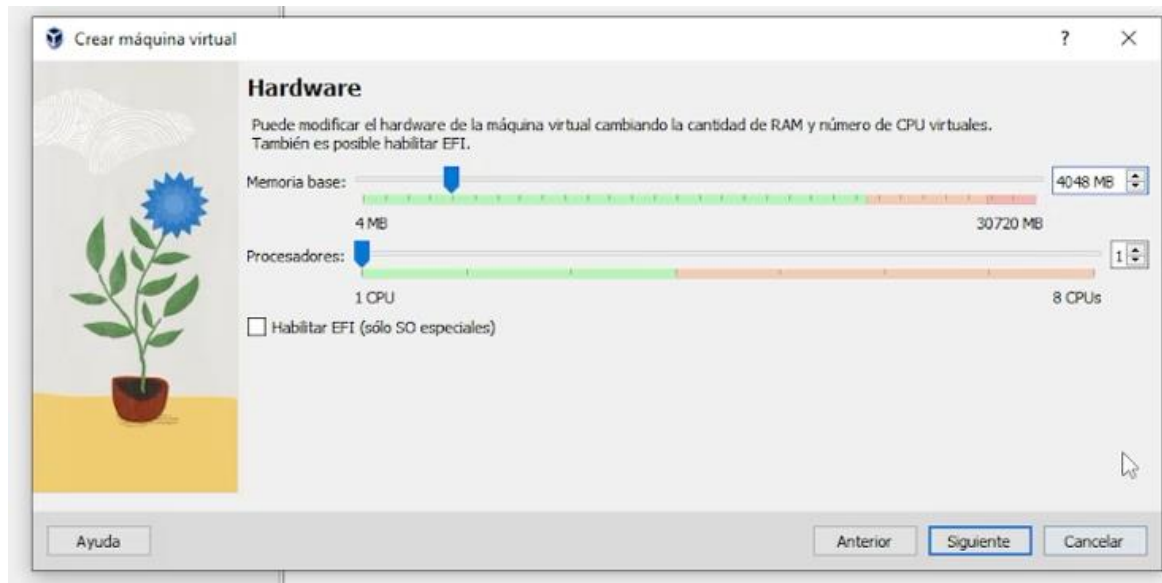
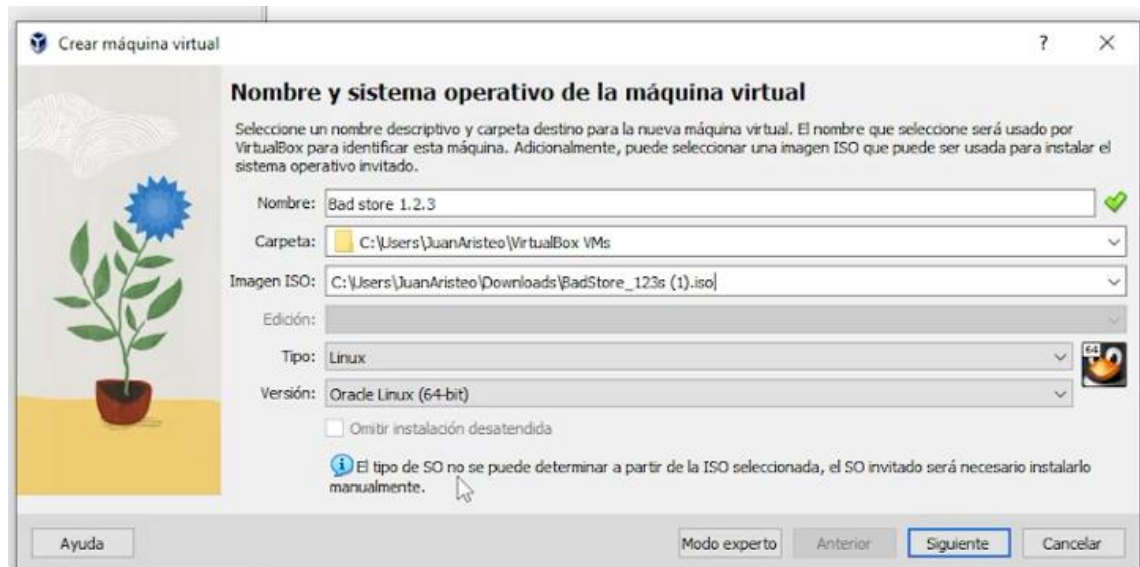
1. Descarga de archivos necesarios para la prueba.




2. Se instala VirtualBox, se ejecuta y se instala la extensión.



3. Se realiza la instalación de la imagen.



Crear máquina virtual



Disco duro virtual

Si lo desea puede añadir un nuevo disco duro virtual a la nueva máquina. Puede crear un nuevo archivo de disco duro o seleccionar uno existente. De forma alternativa puede crear una máquina virtual sin un disco duro virtual.

☒ Crear un disco duro virtual ahora

Tamaño de disco: 10.00 GB

4.00 MB 2.00 TB

☐ Reservar tamaño completo

☐ Usar un archivo de disco duro virtual existente

Vacio

☐ No añadir un disco duro virtual


Ayuda

Anterior

Siguiente

Cancelar

Crear máquina virtual



Resumen

La siguiente tabla resume la configuración que ha elegido para la nueva máquina virtual. Cuando esté conforme con la configuración presione Finalizar para crear la máquina virtual. También puede volver atrás y modificar la configuración.

Nombre y tipo de SO de la máquina	
Nombre de máquina	Bad Store 1.2.3
Carpeta de la máquina	C:/Users/JuanAristeo/VirtualBox VMs/Bad Store 1.2.3
Imagen ISO	C:/Users/JuanAristeo/Downloads/BadStore_123s (1).iso
Tipo de SO invitado	Oracle Linux (64-bit)
Omitir instalación desatendida	false

Hardware	
Memoria base	4048
Procesador(es)	1
Habilitar EFI	false

Disco	
Tamaño de disco	10.00 GB
Reservar tamaño completo	false

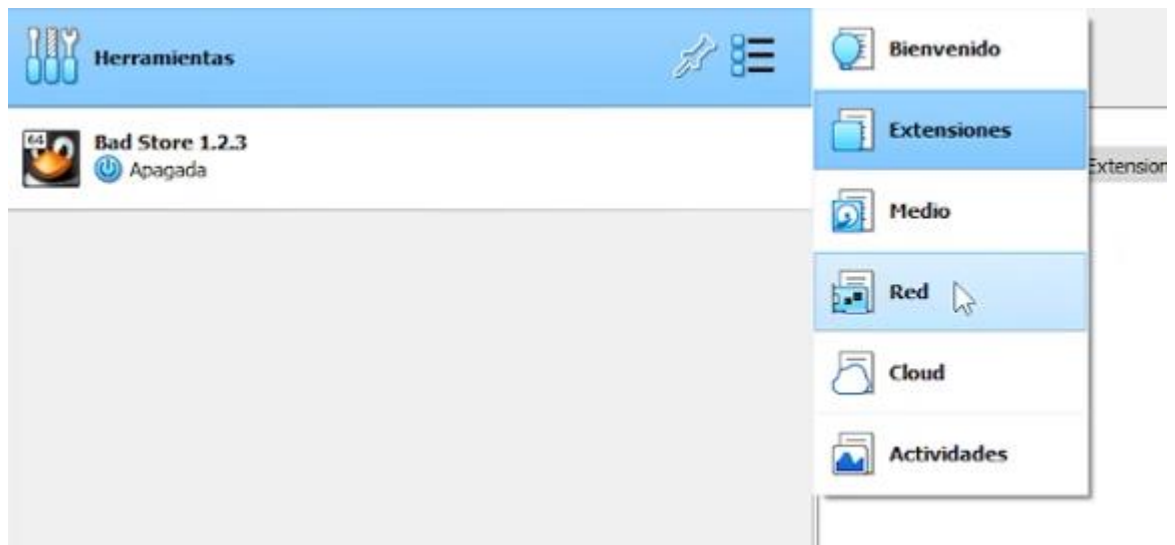
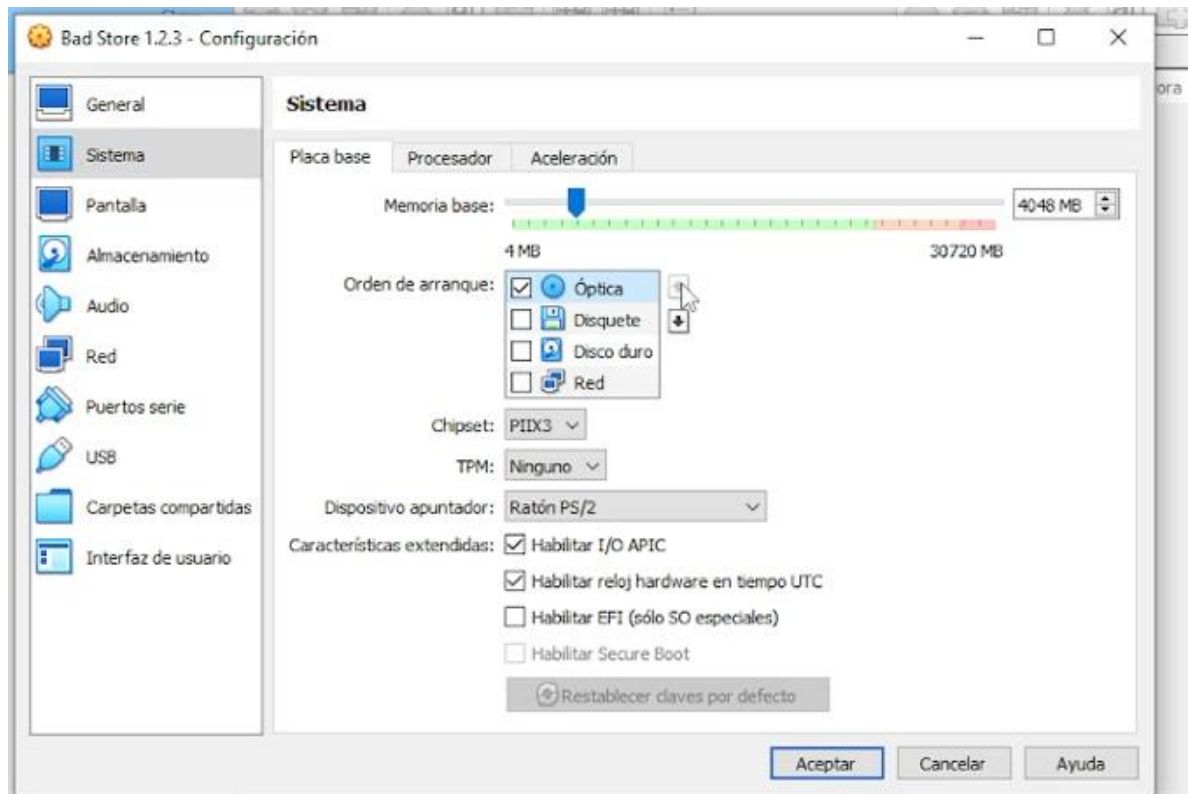
Ayuda

Anterior

Terminar

Cancelar

4. Realizamos las modificaciones de orden de arranque y de red en nuestra VM.



Adaptador Servidor DHCP

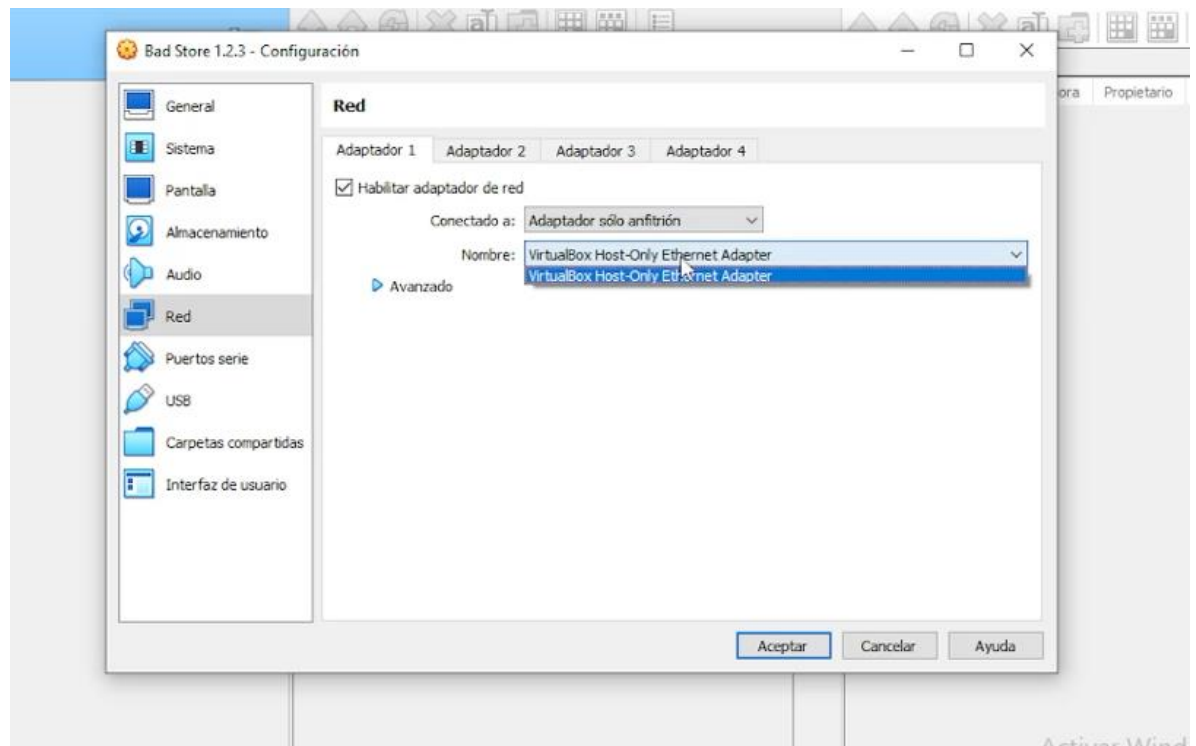
☒ Habilitar servidor

Dirección del servidor: 192.168.56.2

Máscara del servidor: 255.255.255.0

Límite inferior de direcciones: 192.168.56.110

Límite superior de direcciones: 192.168.56.254



5. Iniciamos la MV y ponemos el comando ifconfig.

```
ALT-Left/Right allows you to view other virtual terminals.

Please press Enter to activate this console.
bash# ipconfig
sh: ipconfig: command not found
bash# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:EC:65:BF
          inet addr:192.168.56.110 Bcast:192.168.56.255 Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2502 (2.4 kiB) TX bytes:2560 (2.5 kiB)
          Interrupt:9 Base address:0xd020 Memory:f0200000-f0220000

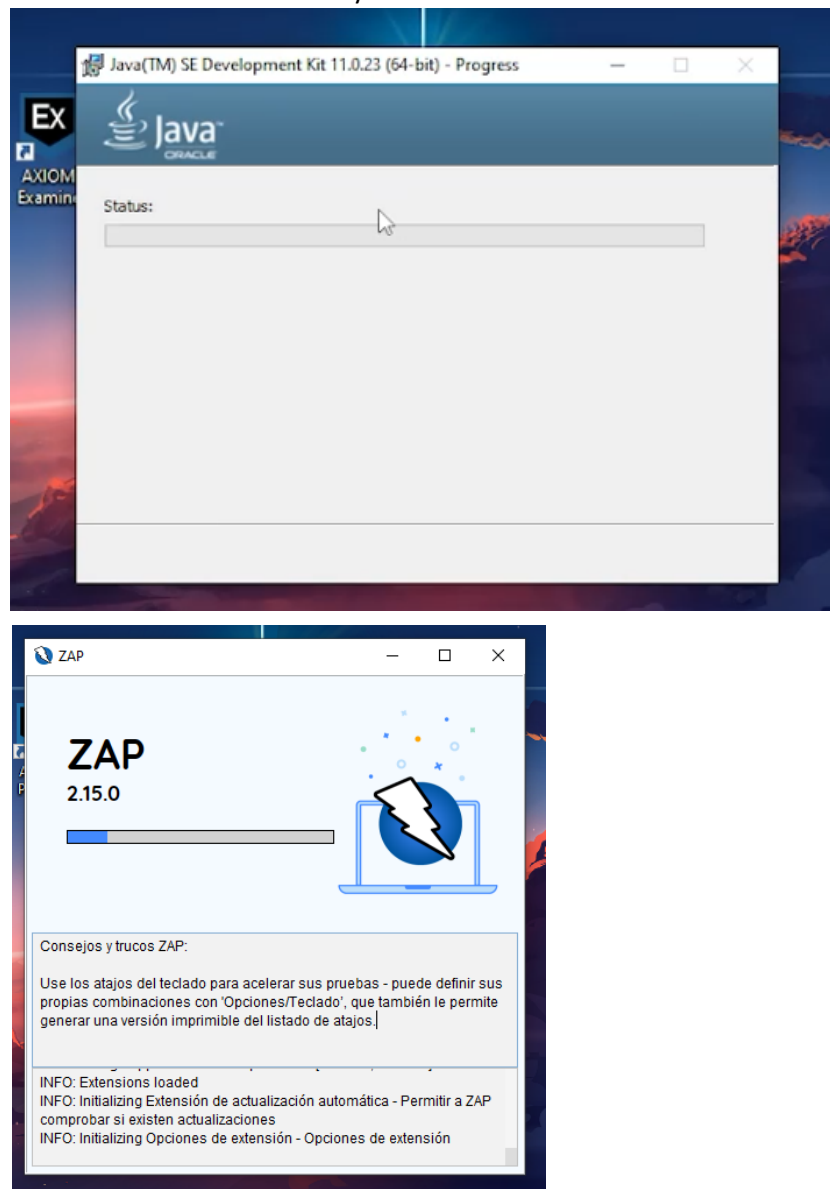
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 iB) TX bytes:0 (0.0 iB)

bash#
```

6. Abrimos la BadStore.net



7. Instalamos la versión de JAV y ZAP.



8. Realizamos el ataque a la BadStore.net

Escaneo automatizado

Esta pantalla le permite iniciar un escaneo automático contra una aplicación: simplemente ingrese su URL a continuación y presione 'Atacar'.

Tenga en cuenta que solo debe atacar aplicaciones para las cuales ha recibido previamente una clara autorización.

URL a atacar:

Usar el spider tradicional: ☒

Usar el spider ajax: con

Progreso:

Progreso: No iniciado

ID	Fuente	Petición (Tiempo)	Método	URL	Código	Razón	RTT	Respuesta (Tamaño del cuerpo)	Alerta mayor	Nota	Etiquetas
870	18/08/24, 16:31:28	18/08/24, 16:31:28	GET	http://192.168.56.110/cgi-bin/badstore.cgi?~s	200	OK	141ms	1020bytes			
871	18/08/24, 16:31:28	18/08/24, 16:31:28	GET	http://192.168.56.110/cgi-bin/badstore.cgi?~s	200	OK	203ms	224bytes			
872	18/08/24, 16:31:28	18/08/24, 16:31:28	GET	http://192.168.56.110/cgi-bin/badstore.cgi?~s	200	OK	229ms	224bytes			
873	18/08/24, 16:31:28	18/08/24, 16:31:28	GET	http://192.168.56.110/cgi-bin/badstore.cgi?~s	200	OK	226ms	224bytes			

9. Obtenemos los resultados.

Respuesta

Cabecera: Vista Raw

HTTP/1.1 200 OK
Date: Tue, 20 Aug 2024 01:43:04 GMT
Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Cache-Control: no-cache
ETag: CPE1704TK5
Pragma: no-cache
Content-Type: text/html
Content-Length: 3991

HTML content: `<TD class=normal width=120>View Cart</TD></TR><TR bgColor=#333333></TR></BODY></TABLE><DOCTYPE HTML PUBLIC "-//IETF//DTD HTML//EN"><HTML><HEAD><TITLE>BadStore.net - Reset Password for User</TITLE></HEAD><BODY><H2>The password for user: </H2><script>alert(1)</script><h2><P>...has been reset to: Welcome</H2><HR><P>
<Center>BadStore v1.2.3s - Copyright 8#169; 2004-2005</Center></BODY></HTML>`

ID	Petición (Tiempo)	Marca de tiempo Respuesta	Método	URL	Código	Razón	RTT	Tamaño de la Cabecera de Respuesta	Respuesta (Tamaño del cuerpo)
870	18/08/24, 16:31:28	18/08/24, 16:31:28	GET	http://192.168.56.110/cgi-bin/badstore.cgi?~s	200	OK	141ms	1020bytes	1020bytes
871	18/08/24, 16:31:28	18/08/24, 16:31:28	GET	http://192.168.56.110/cgi-bin/badstore.cgi?~s	200	OK	203ms	224bytes	4,046bytes
872	18/08/24, 16:31:28	18/08/24, 16:31:28	GET	http://192.168.56.110/cgi-bin/badstore.cgi?~s	200	OK	229ms	224bytes	4,046bytes
873	18/08/24, 16:31:28	18/08/24, 16:31:28	GET	http://192.168.56.110/cgi-bin/badstore.cgi?~s	200	OK	226ms	224bytes	4,046bytes

10. Generamos el informe.

<< Entregable 3 > Informe ZAP		Buscar en Informe ZAP		
	Nombre	Fecha de modificación	Tipo	Tamaño
do	2024-08-18-ZAP-Report-	18/08/2024 04:29 p. m.	Carpeta de archivos	
	2024-08-18-ZAP-Report-	18/08/2024 04:41 p. m.	Microsoft Edge H...	69 KB

Auditoría de las vulnerabilidades encontradas

Cross-Site Scripting (XSS):

Mediante el análisis se identificaron vulnerabilidades de tipo Cross-Site Scripting (XSS). Esto significa que un atacante es capaz de inyectar scripts maliciosos en paginas web que son visualizadas por otros usuarios. Esta vulnerabilidad permite ejecutar scripts en el contexto de la sesión del usuario afectado, robando credenciales y cookies.

Es recomendable utilizar métodos como la codificación correcta de los datos en las respuestas HTML y la validación del lado del servidor para evitar ejecución de scripts maliciosos.

SQL inyección:

DE igual forma se detectaron puntos vulnerables que podrían permitir inyecciones SQL. Este tipo de vulnerabilidad permite a un atacante manipular las consultas SQL que se realizan por la aplicación., esto podría conducir a la exposición o manipulación de datos sensibles.

Se recomienda implementar consultas preparadas y validar correctamente las entradas de los usuarios para mitigar este riesgo.