

Asignatura	Datos del alumno	Fecha
<b>Seguridad en Aplicaciones Online</b>	Apellidos: Paz López	18/06/2022
	Nombre: Angel Ramon	

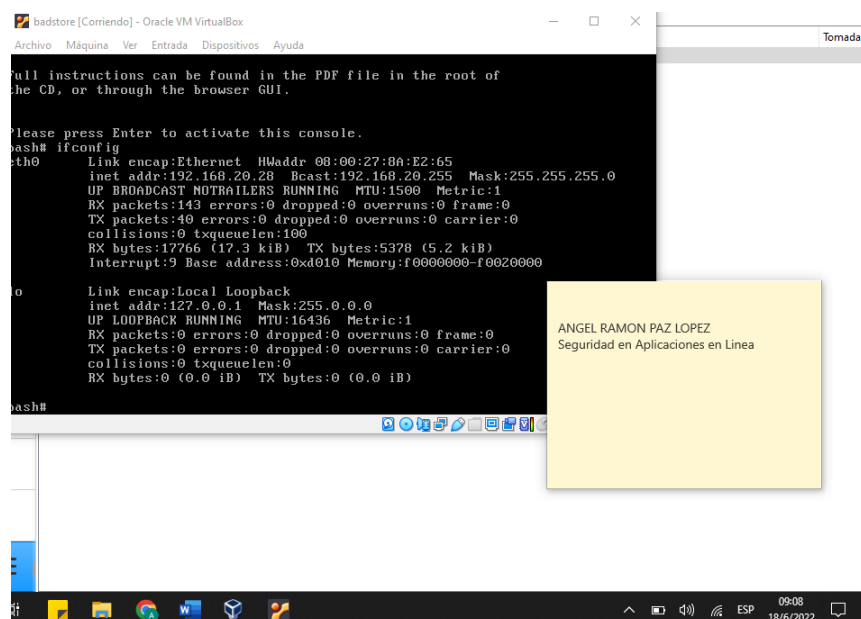
## Contenido

VERIFICACION DE FUNCIONAMIENTO DEL BADSTORE .....	2
VULNERABILIDADES ENCONTRADAS .....	6
1) Application Error Disclosure (Divulgación de error de aplicación) .....	7
Solución.....	8
2) Exploración de Directorios .....	8
Solución: .....	10
3) X-Content-Type-Options Header Missing (Falta el encabezado X-Content- Type-Options) .....	10
CONCLUSIONES.....	12

# VERIFICACION DE FUNCIONAMIENTO DEL BADSTORE

Teniendo ya listo la máquina virtual con el BADSTORE lo primero que tenemos que hacer es saber las direcciones IP de la computadora.

## Dirección IP BADSTORE



```
Full instructions can be found in the PDF file in the root of the CD, or through the browser GUI.

Please press Enter to activate this console.
bash# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8A:E2:65
          inet addr:192.168.20.28  Bcast:192.168.20.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING  MTU:1500  Metric:1
          RX packets:143 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17766 (17.3 KiB)  TX bytes:5378 (5.2 KiB)
          Interrupt:9 Base address:0xd010 Memory:f0000000-f0020000

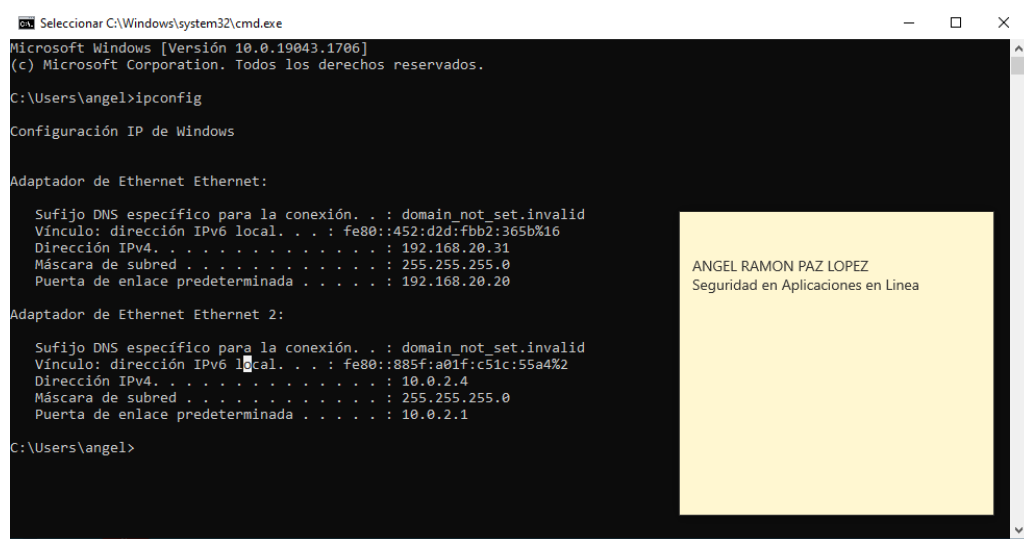
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
       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

bash#
```

ANGEL RAMON PAZ LOPEZ  
Seguridad en Aplicaciones en Linea

En la maquina Windows debemos realizar lo siguiente

### 1. Verificar la dirección IP



```
Microsoft Windows [Versión 10.0.19043.1706]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\angel>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufixo DNS específico para la conexión. . . : domain_not_set.invalid
    Vínculo: dirección IPv6 local. . . : fe80::452:d2d:fb2:365b%16
    Dirección IPv4. . . . . : 192.168.20.31
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.20.20

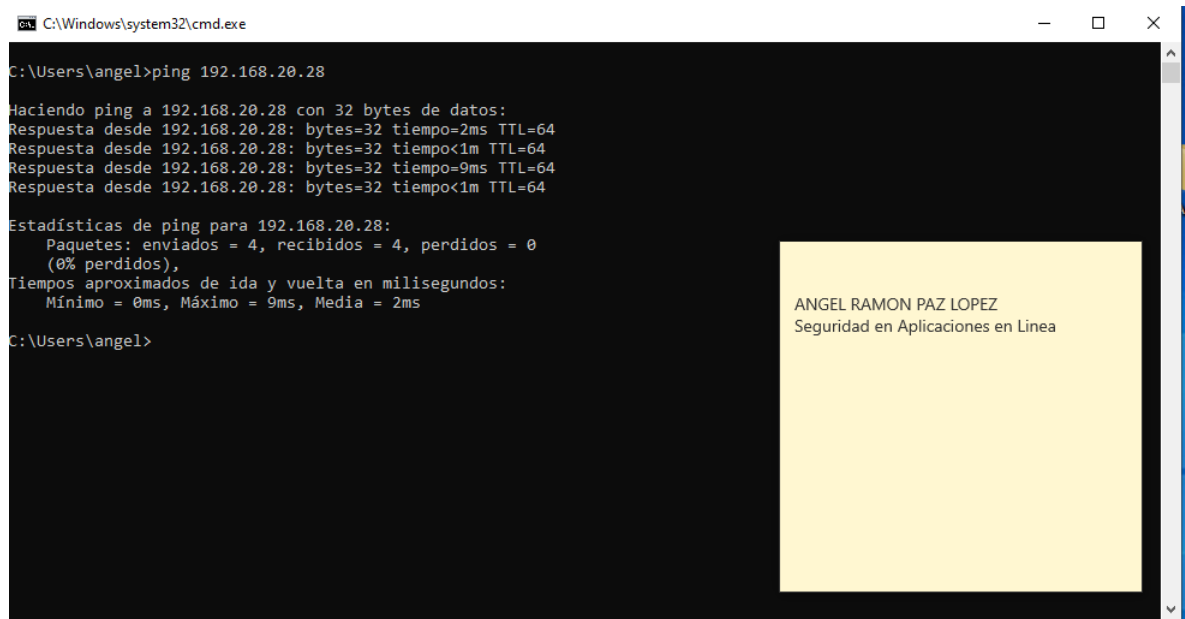
Adaptador de Ethernet Ethernet 2:

    Sufixo DNS específico para la conexión. . . : domain_not_set.invalid
    Vínculo: dirección IPv6 local. . . : fe80::885f:a01f:c51c:55a4%2
    Dirección IPv4. . . . . : 10.0.2.4
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 10.0.2.1

C:\Users\angel>
```

ANGEL RAMON PAZ LOPEZ  
Seguridad en Aplicaciones en Linea

## 2. Realizar ping a la maquina BADSTORE



```
C:\Windows\system32\cmd.exe

C:\Users\angel>ping 192.168.20.28

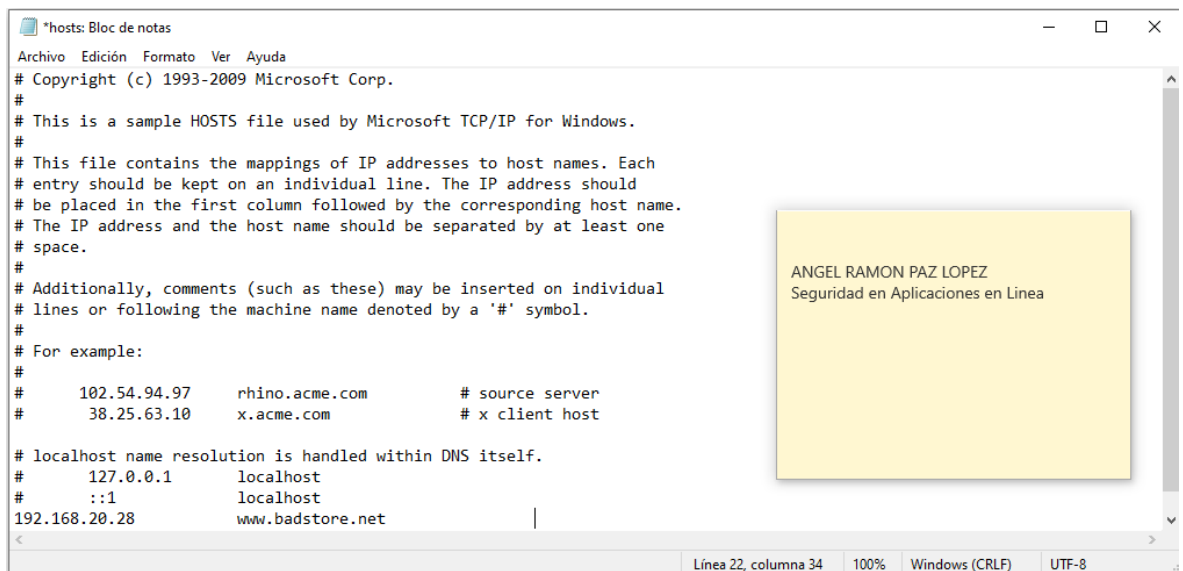
Haciendo ping a 192.168.20.28 con 32 bytes de datos:
Respuesta desde 192.168.20.28: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.20.28: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.20.28: bytes=32 tiempo=9ms TTL=64
Respuesta desde 192.168.20.28: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.20.28:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 9ms, Media = 2ms

C:\Users\angel>
```

## 3. Abrir un bloc de notas como Administrador y en el archivo de host que está en la ubicación C:\Windows\System32\drivers\etc\hosts colocamos la siguiente linea

**192.168.20.28                      www.badstore.net**



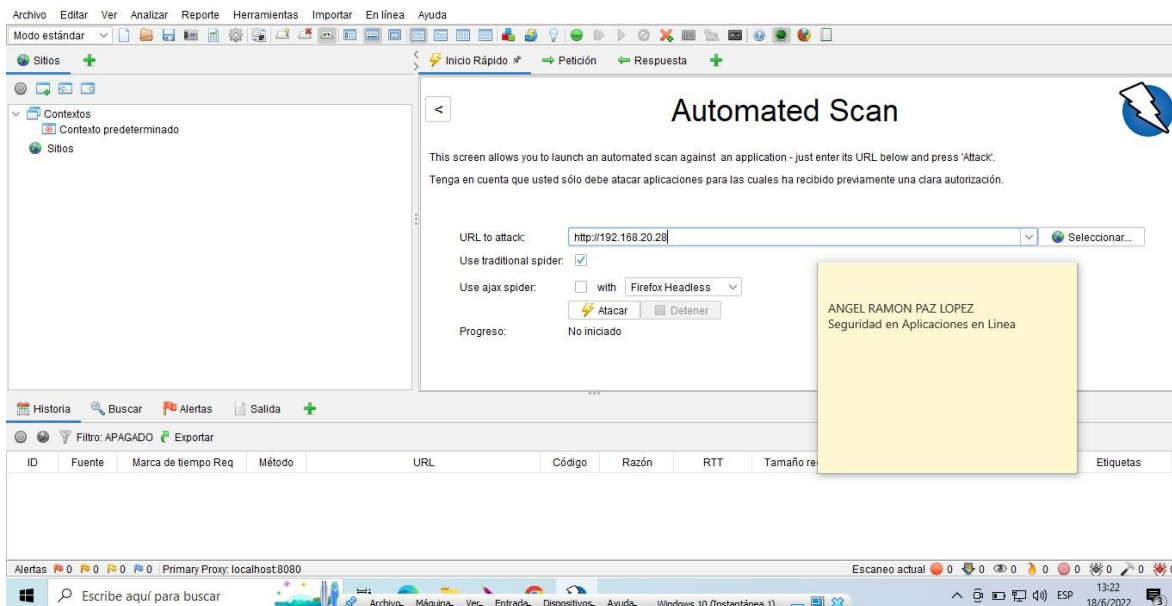
```
*hosts: Bloc de notas
Archivo Edición Formato Ver Ayuda
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address 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
192.168.20.28            www.badstore.net
```

## 4. Abrimos el navegador y escribimos [www.badstore.net](http://www.badstore.net) o 192.168.20.28 y tendremos visualizada la página web de BADSTORE.



Una vez comprobado que tenemos lista el BADSTORE, procedemos a ejecutar OWASP ZAP



Colocamos en la URL la IP de la dirección del BADSTORE en nuestro caso 192.168.20.28 y activamos usar el spider y damos en el botón atacar

Owasp ZAP - OWASP ZAP 2.11.1

Archivo Editar Ver Analizar Reporte Herramientas Importar En línea Ayuda

Modo estándar

Sitios

Sitios

- http://192.168.20.28
  - GET /
  - backup
  - GET.backup
  - GET.cgi-bin
  - Icons
  - GET.robots.txt
  - GET.scanbot
  - scanbot

Inicio Rápido Petición Respuesta

Encabezamiento: Vista Raw Cuerpo: Vista Raw

HTTP/1.1 200 OK  
Date: Sat, 18 Jun 2022 18:30:05 GMT  
Server: Apache/1.3.28 (Unix) mod\_ssl/2.8.15 OpenSSL/0.9.7c  
Content-Type: text/html

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<HTML>
<HEAD>
<TITLE>Index of /backup/</TITLE>
</HEAD>
<BODY>
<H1>Index of /backup/</H1>
```

ANGEL RAMON PAZ LOPEZ  
Seguridad en Aplicaciones en Línea

Historia Buscar Alertas Salida Spider(Araña) Escaneo Activo

Nuevo escaneo Progreso: 0. http://192.168.20.28 100% Escaneo actual: 0 Num Requests: 1673 Alertas Nuevas: 6 Exportar

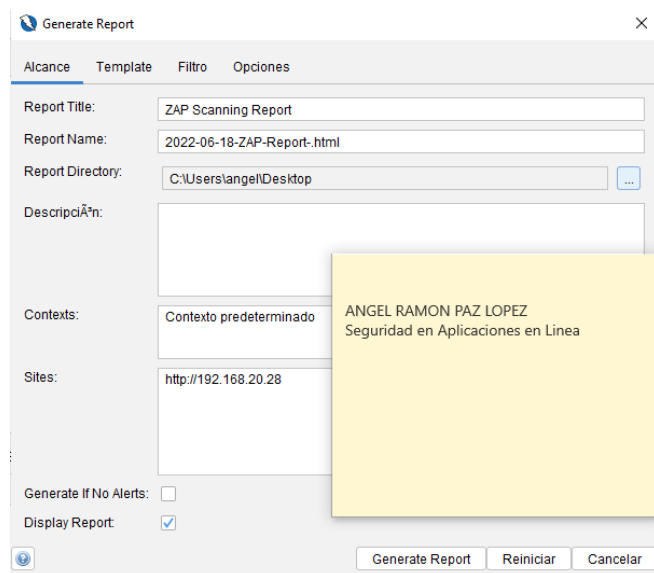
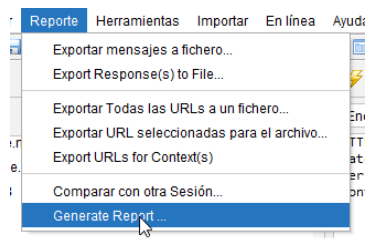
Mensajes Enviados Mensajes Filtrados

ID	Marca de tiempo Req	Marca de tiempo Resp	Método	URL	Código	Razón	RTT	Tamaño que se r...	Tamaño requerid...
771	06-18-22 01:23:57 PM	06-18-22 01:23:57 PM	GET	http://192.168.20.28/backup/?N=A%27-UNION+ALL+select+NULL+--+	200	OK	32milisegun...	141bytes	535bytes
772	06-18-22 01:23:57 PM	06-18-22 01:23:57 PM	GET	http://192.168.20.28/backup/?N=A%22-UNION+ALL+select+NULL+--+	200	OK	21milisegun...	141bytes	535bytes
773	06-18-22 01:23:57 PM	06-18-22 01:23:57 PM	GET	http://192.168.20.28/backup/?S=D%27-UNION+ALL+select+NULL+--+	200	OK	21milisegun...	141bytes	535bytes
774	06-18-22 01:23:57 PM	06-18-22 01:23:57 PM	GET	http://192.168.20.28/backup/?S=D%27-UNION+ALL+select+NULL+--+	200	OK	16milisegun...	141bytes	535bytes
775	06-18-22 01:23:57 PM	06-18-22 01:23:57 PM	GET	http://192.168.20.28/backup/?N=A%29-UNION+ALL+select+NULL+--+	200	OK	16milisegun...	141bytes	535bytes
776	06-18-22 01:23:57 PM	06-18-22 01:23:57 PM	GET	http://192.168.20.28/backup/?N=D%22-UNION+ALL+select+NULL+--+	200	OK	16milisegun...	141bytes	535bytes
777	06-18-22 01:23:57 PM	06-18-22 01:23:57 PM	GET	http://192.168.20.28/backup/?N=A%27%29-UNION+ALL+select+NULL+--+	200	OK	16milisegun...	141bytes	535bytes
778	06-18-22 01:23:57 PM	06-18-22 01:23:57 PM	GET	http://192.168.20.28/backup/?N=A	200	OK	16milisegun...	141bytes	535bytes
779	06-18-22 01:23:57 PM	06-18-22 01:23:57 PM	GET	http://192.168.20.28/backup/?S=D%29-UNION+ALL+select+NULL+--+	200	OK	16milisegun...	141bytes	535bytes
780	06-18-22 01:23:57 PM	06-18-22 01:23:57 PM	GET	http://192.168.20.28/backup/?S=D%27%29-UNION+ALL+select+NULL+--+	200	OK	15milisegun...	141bytes	535bytes

Alertas 0 4 1 0 Primary Proxy: localhost8080

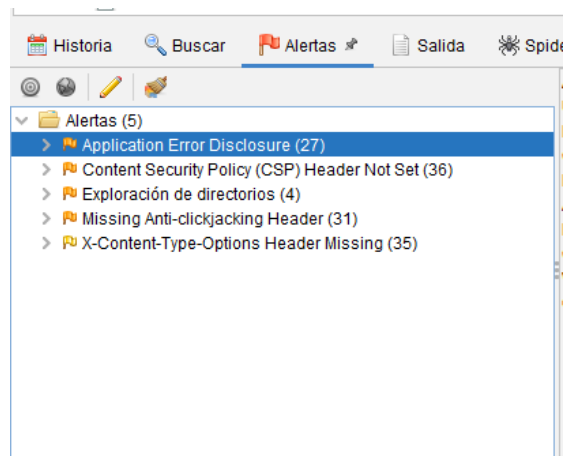
Escaneo actual

También tenemos la opción de generar reportes de los resultados del escaneo



Y damos en generar reporte

## VULNERABILIDADES ENCONTRADAS



La herramienta OWASP ZAP podemos encontrar 5 alertas en la cual explicaremos 3 vulnerabilidades.

## 1) Application Error Disclosure (Divulgación de error de aplicación)

Application Error Disclosure	
URL:	http://192.168.20.28/supplier/
Riesgo:	🔴 Medium
Confianza:	Medium
Parámetro:	
Ataque:	
Evidencia:	Parent Directory
CWE ID:	200
WASC ID:	13
Origen:	Pasivo (90022 - Application Error Disclosure)

### Descripción:

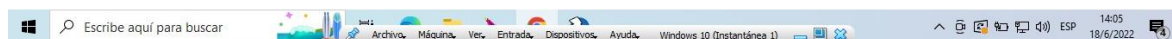
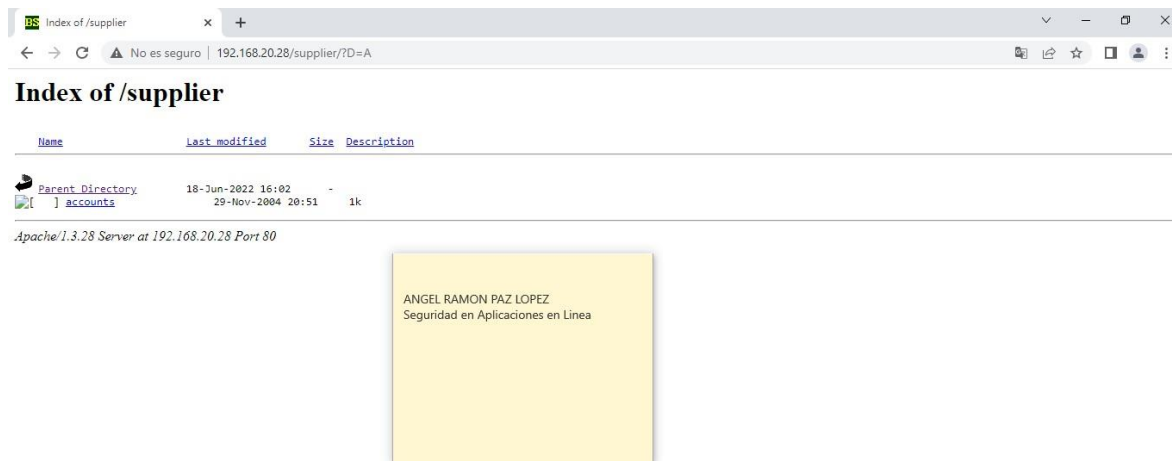
Esta página contiene un mensaje de error/advertencia que puede revelar información confidencial, como la ubicación del archivo que produjo la excepción no controlada. Esta información se puede utilizar para lanzar más. Dentro de esta vulnerabilidad tenemos 27 casos o alertas

Application Error Disclosure (27)
<input type="checkbox"/> GET: http://192.168.20.28/backup/
<input type="checkbox"/> GET: http://192.168.20.28/backup/?D=A
<input type="checkbox"/> GET: http://192.168.20.28/backup/?D=D
<input type="checkbox"/> GET: http://192.168.20.28/backup/?M=A
<input type="checkbox"/> GET: http://192.168.20.28/backup/?M=D
<input type="checkbox"/> GET: http://192.168.20.28/backup/?N=A
<input type="checkbox"/> GET: http://192.168.20.28/backup/?N=D
<input type="checkbox"/> GET: http://192.168.20.28/backup/?S=A
<input type="checkbox"/> GET: http://192.168.20.28/backup/?S=D
<input type="checkbox"/> GET: http://192.168.20.28/scanbot/
<input type="checkbox"/> GET: http://192.168.20.28/scanbot/?D=A
<input type="checkbox"/> GET: http://192.168.20.28/scanbot/?D=D
<input type="checkbox"/> GET: http://192.168.20.28/scanbot/?M=A
<input type="checkbox"/> GET: http://192.168.20.28/scanbot/?M=D
<input type="checkbox"/> GET: http://192.168.20.28/scanbot/?N=A
<input type="checkbox"/> GET: http://192.168.20.28/scanbot/?N=D
<input type="checkbox"/> GET: http://192.168.20.28/scanbot/?S=A
<input type="checkbox"/> GET: http://192.168.20.28/scanbot/?S=D

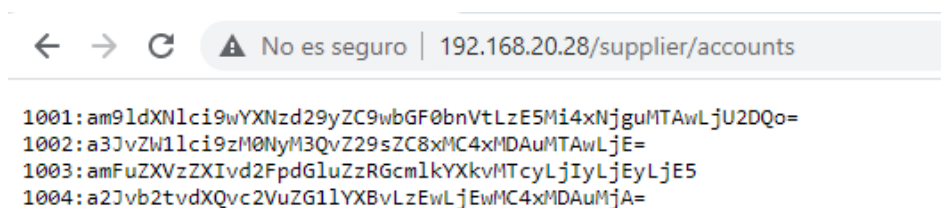
Viendo con más detalle la vulnerabilidad damos clic en un caso

Application Error Disclosure	▼
URL:	http://192.168.20.28/supplier/?D=A
Riesgo:	Medium ▼
Confianza:	Medium ▼
Parámetro:	▼
Ataque:	
Evidencia:	Parent Directory
CWE ID:	200 ↕
WASC ID:	13 ↕
Descripción:	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further
Otra info:	
Solución:	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the
Referencia:	

Vamos al navegador y colocamos el enlace de la URL y obtenemos lo siguiente:



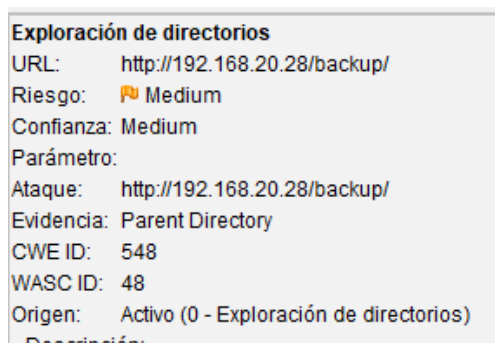
Podemos observar que hay un archivo al que podemos acceder “accounts” y al abrirlo tenemos la siguiente información



## Solución

Revisa el código fuente de esta página. Implementar páginas de error personalizadas. Considere implementar un mecanismo para proporcionar una referencia/identificador de error único al cliente (navegador) mientras registra los detalles en el.

## 2) Exploración de Directorios





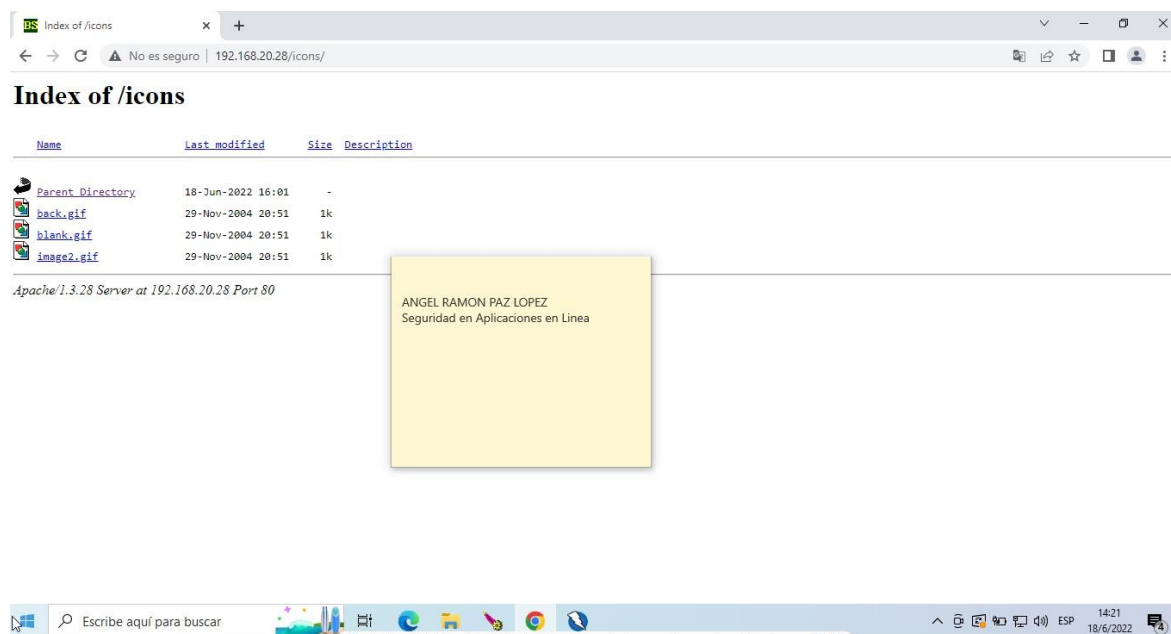
## Descripción:

La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.

Dentro de esta vulnerabilidad tenemos los casos de:



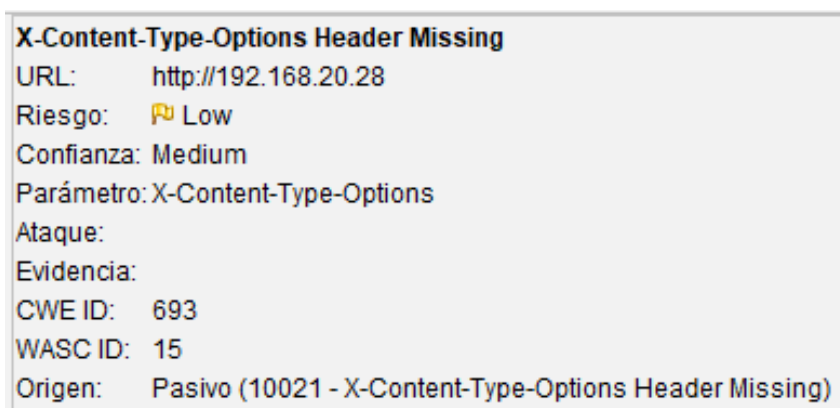
En la cual se puede ingresar en el navegador cada URL para poder buscar información como, por ejemplo:



### **Solución:**

Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer el encabezado Política de seguridad de contenido, para lograr un soporte óptimo del navegador: "Política de seguridad de contenido" para Chrome 25+, Firefox 23+ y Safari 7 +, "X-Content-Security-Policy" para Firefox 4.0+ e Internet Explorer 10+, y "X-WebKit-CSP" para Chrome 14+ y Safari 6+.

### 3) X-Content-Type-Options Header Missing (Falta el encabezado X-Content-Type-Options)

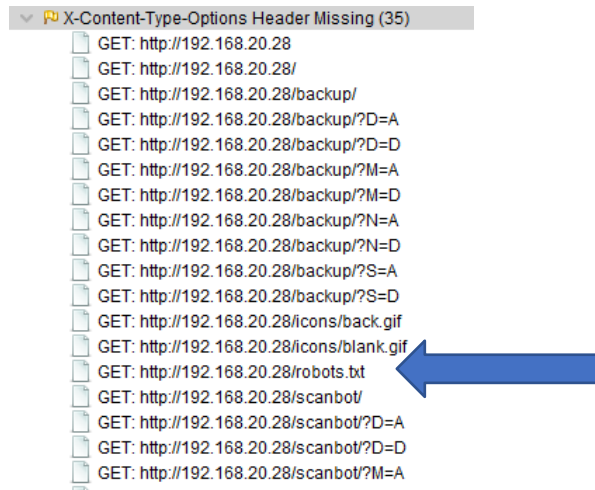


### **Descripción:**

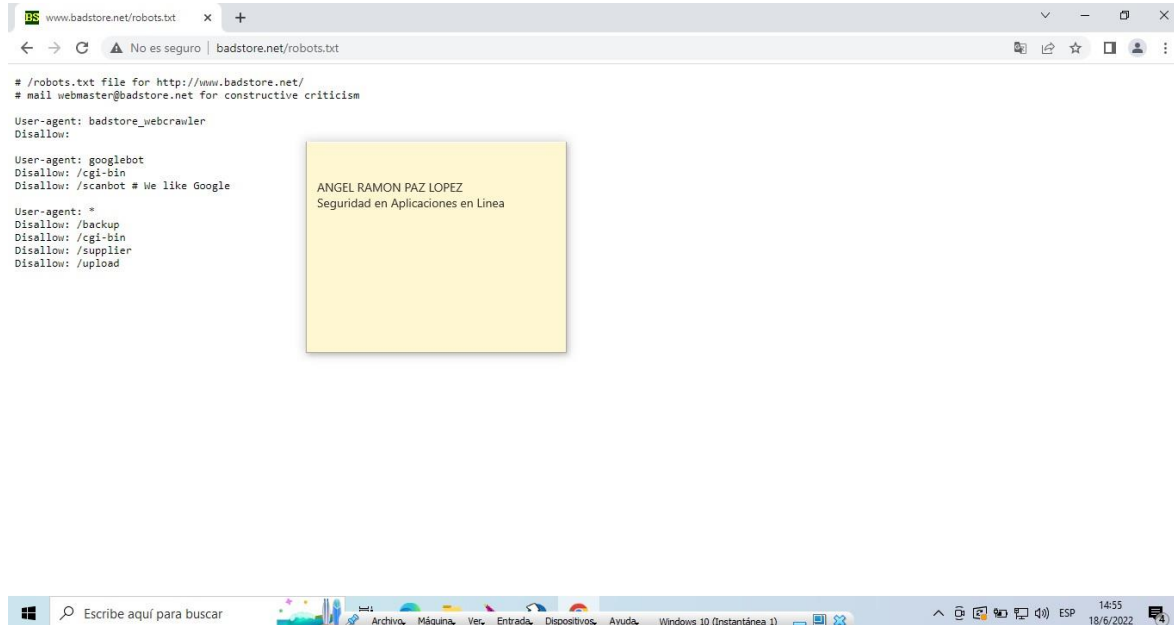
El encabezado Anti-MIME-Sniffing X-Content-Type-Options no se configuró en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen un rastreo MIME en el cuerpo de la respuesta, lo que podría causar que el cuerpo de la respuesta se interprete y muestre como un tipo de contenido diferente al tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si se ha configurado uno), en lugar de realizar un análisis MIME.

Este problema aún se aplica a las páginas de tipo de error (401, 403, 500, etc.) ya que esas páginas a menudo aún se ven afectadas por problemas de inyección, en cuyo caso todavía existe la preocupación de que los navegadores detecten páginas de su tipo de contenido real. En el umbral "Alto", esta regla de exploración no alertará sobre las respuestas de error del cliente o del servidor.

Dentro de esta vulnerabilidad tenemos los casos de:



Probamos en el navegador a utilizar robots.txt para obtener información



## Solución:

Asegúrese de que la aplicación/servidor web establezca el encabezado de tipo de contenido correctamente y que establezca el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.

Si es posible, asegúrese de que el usuario final utilice un navegador web moderno y compatible con los estándares que no realice ningún tipo de detección de MIME, o que la aplicación web o el servidor web puedan indicarle que no realice la detección de MIME.

## **CONCLUSIONES**

Aprendimos a configurar una máquina virtual vulnerable como lo es BADSTORE y auditar la página web con la herramienta OWASP ZAP lo cual nos da detalles importantes de las vulnerabilidades que pueda tener una aplicación Web en nuestro caso BADSTORE dándonos a mostrar el nivel y valoración de riesgo de cada vulnerabilidad encontrada, el ataque que realizo para encontrar la vulnerabilidad, el código CWE y el WASC de cada vulnerabilidad, así como la posible solución a dicha vulnerabilidad.