Escenario3

https://hub.docker.com/r/vulnerables/web-dvwa

Lanzamos la herramienta DVWA

```
docker run --rm -it -p 80:80 vulnerables/web-dvwa
```

**La podemos ver en el navegador "localhost:80"

Credenciales

```
Username: admin
Password: password
```

Creamos base de datos

Vamos a `Setup DWVA` y le damos a `Create / Reset Database`.

Una vez creada cerrará sesión y debemos entrar de nuevo con el mismo ususario y contraseña (admin/password)

Seguridad de la estructura frente al ataque

Vamos al apartado `DVWA Security` donde podremos escoger el nivel de seguridad que tendrá el sistema frente al ataque que tenemos que realizar.

Cabe recordar que cuanto más alto el nivel más difícil será atacarlo y tenemos los siguientes:

> Low
>
> Medium
>
> High
>
> Impossible

Escenarios

Tenemos varios escenarios de prueba para practicar múltiples vulnerabilidades. Algunos son:

> Brute Force
>
> SQL Injection
>
> XSS
>
> Javascript

Añadir que cada escenarios también tiene un apartado de *más información* donde tendremos información de las distintas vulnerabilidades y algunas pistas.

Ademas, tenemos dos botones *View Source* y *View Help*. El primero muestra el código de la página a atacar y el segundo ofrece ayuda sobre el nivel (las partes en negro se desbloquean arrastrando el ratón sobre ellas).

Ejemplos

SQL Injection

En el apartado SQL Injection, podemos probar a atacar la base de datos del sistema. En el formulario tendríamos que meter el ID del usuario pero con el comando siguiente veremos que tiene una vulnerabilidad de configuración que nos dará todos los usuarios de la base de datos con la contraseña.

```
%' and 1=0 union select null, concat(user,':',password) from users #
```