**# `01` Broken Access Control - Insecure DOR (Change Secret)**

**\*\*Broken Access Control\*\*** son vulnerabilidades en las aplicaciones web que ocurre cuando los controles que restringen el acceso a recursos o funcionalidades no están implementados correctamente. Esto permite a los atacantes eludir las restricciones de acceso, lo que les da la capacidad de ver, modificar o interactuar con datos o funcionalidades a los que no deberían tener acceso. Para este ejercicio intentaremos explotar el hack **\*\*Insecure DOR\*\***, para intentar modificar el valor del parámetro de usuario en la solicitud para cambiar el secreto de otra cuenta.

**### \*\*Crear un nuevo usuario\*\***

A screenshot of a computer

Description automatically generated

1. Inicia la máquina virtual beebox.

2. Accede a la interfaz web de bWAPP desde tu navegador usando la dirección IP de la máquina beebox.

3. **\*\*Crea un nuevo usuario\*\***:

    - Crea un usuario llamado geeks con el secret: secret test.

    ![imagen 1](../../.learn/assets/usergeeks.png)

A screenshot of a login form

Description automatically generated

4. Inicia sesión en bWAPP:

```bash

    - Usuario: bee

    - Contraseña: bug

A screenshot of a login screen

Description automatically generated

**### \*\*Verificación en MySQL\*\***

1. Abre la terminal en la VM Beebox.

2. Accede a MySQL usando el siguiente comando:

```bash

mysql -u root -p

```

> 💡 La contraseña predeterminada: `bug`

A screenshot of a computer program

Description automatically generated

3. Selecciona la base de datos de bWAPP:

```sql

USE bWAPP;

A close-up of a computer screen

Description automatically generated

4. Verifica que el usuario `geeks` y su "secret" hayan sido creados:

A close-up of a document

Description automatically generated

**### \*\*Modificación del secreto de otro usuario\*\***

1. Vuelve a iniciar sesión como el usuario predeterminado `bee`.

2. Selecciona la vulnerabilidad **\*\*Insecure DOR (Change Secret)\*\*** y "Hack".

A screenshot of a computer

Description automatically generated

3. Inspeccionar el Formulario HTML.

- Una vez en la página de cambio de "secret", haz clic derecho en el campo donde se ingresa el nuevo "secret" y selecciona "Inspeccionar" (o usa las herramientas de desarrollo del navegador).

A screenshot of a computer

Description automatically generated

4. Modificar el Valor del Formulario.

- En el código HTML inspeccionado, localiza el valor del campo oculto (input) que contiene el valor "bee".

- Cambia este valor por "geeks" para que, al enviar el formulario, se modifique el "secret" del usuario geeks en lugar del usuario bee.

A black text on a white background

Description automatically generated

5. Enviar el Formulario: