CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

Nombre	La base de los datos
Categoría	WEB
Dificultad	MUY FÁCIL
Puntos	100

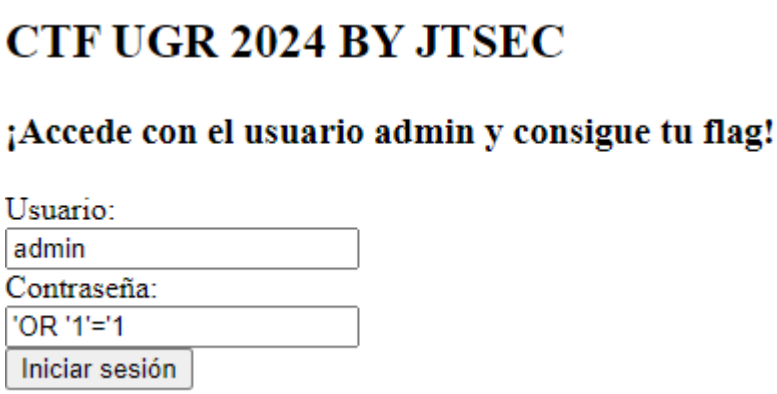
DESCRIPCIÓN DEL RETO (CTFD)

Parece que el desarrollador que ha creado esta página web no tiene mucho conocimiento de desarrollar aplicaciones con bases de datos. ¿Podrás encontrar el fallo de esta página para acceder con el usuario admin?

WRITEUP

1. Al acceder a la página solo vemos un formulario, el cuál nos confirma que si accedemos como administrador podremos conseguir la flag.

2. En este tipo de retos, donde tenemos un input para meter datos se suelen intentar ataques de Inyección.
3. En este caso, al tratarse de un formulario de login, probablemente tengamos por detrás una base de datos que se encargue de almacenar estos usuarios y sus credenciales.
4. Para ello cuando el usuario pulsa el botón de Iniciar sesión, la aplicación realiza una consulta a la base de datos, añadiendo los parámetros que nosotros hemos añadimos previamente en el formulario.
5. Como sabemos el usuario con el que queremos acceder, introduciremos como usuario “admin” y como contraseña, al no saberla, un payload de inyección SQL. Por ejemplo, **'OR '1'='1:**



6. Con el payload 'OR '1'='1 lo que hemos conseguido es decirle a la base de datos lo siguiente:

---

*SELECT * FROM users WHERE username='admin' AND password=''OR '1'='1'*

Selecciónname todo de la tabla usuario donde el usuario sea ADMIN y la contraseña sea ‘’ (es decir este vacía, que sería falso) OR 1=1 (Como 1 es igual a 1, se cumple una de las condiciones).

Como 1=1, hemos podido acceder con el usuario admin.

7. Pulsar “Iniciar sesión” para obtener la flag.