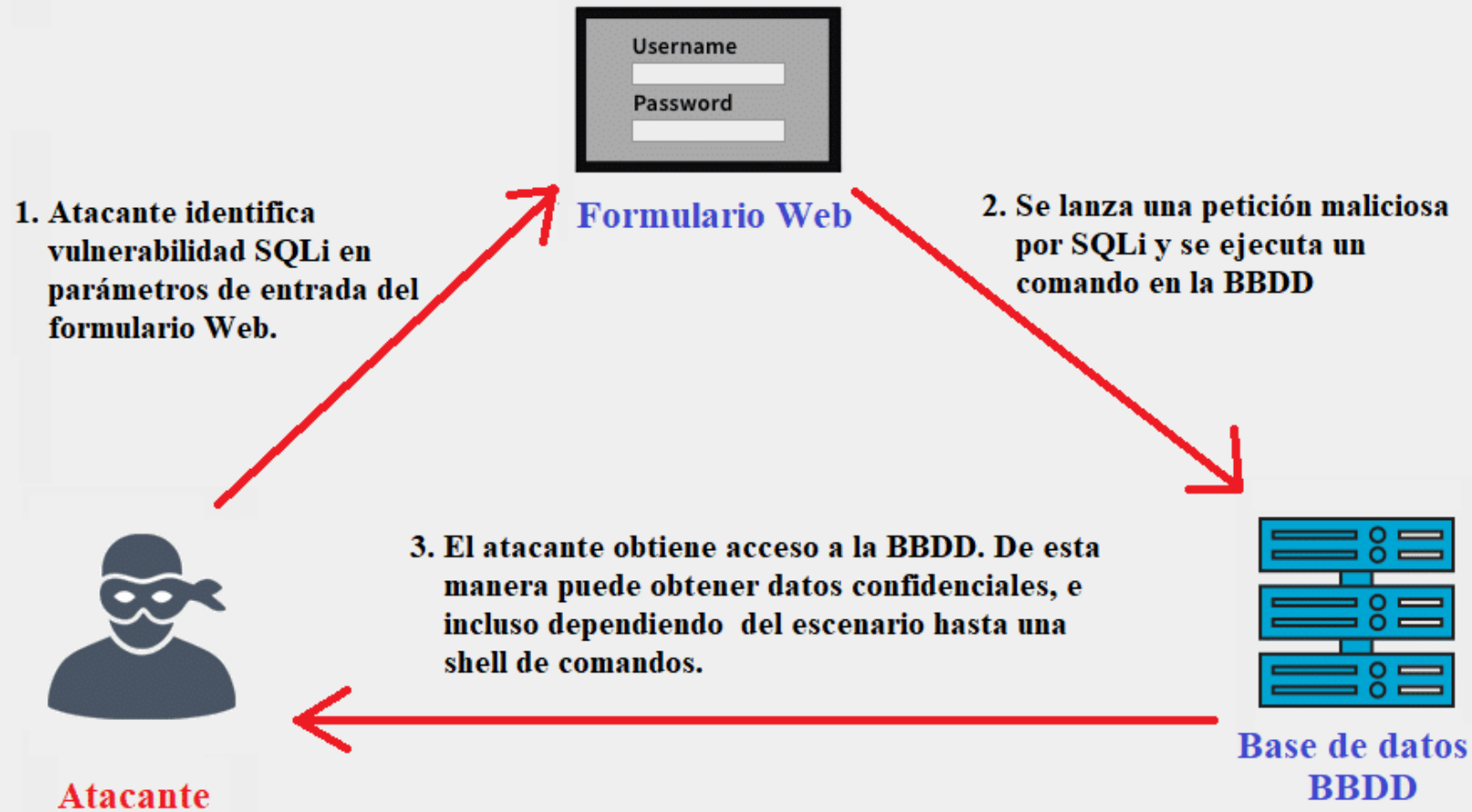




Inyecciones SQL

ATAQUE INYECCIÓN SQL (SQLi)



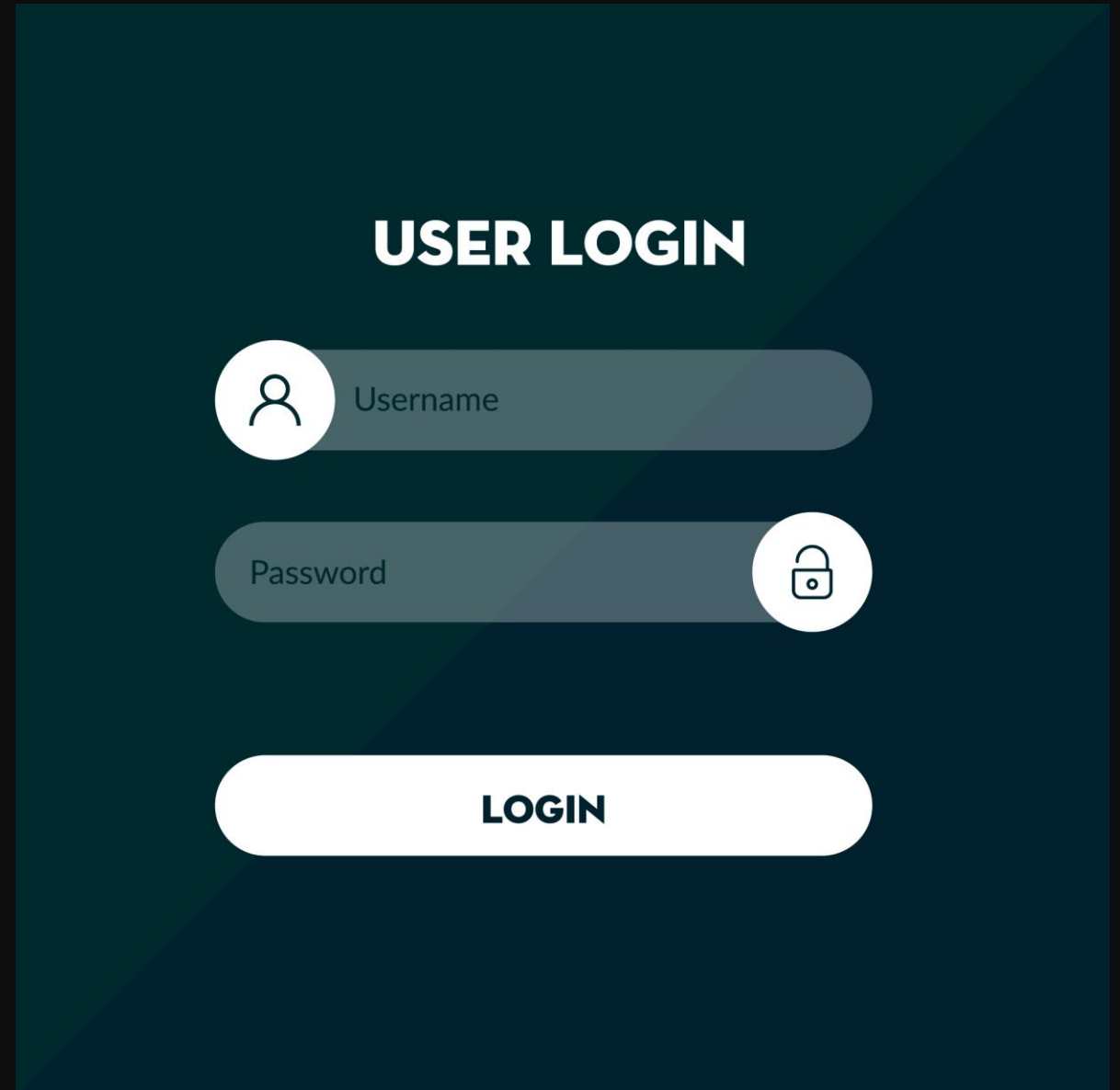
¿Cómo funcionan los ataques de inyección de SQL?

Antes de ver como funcionan los ataques SQL, debemos saber que es el lenguaje SQL




Problemas SQL: Formularios Web


- Muchas veces esos no tienen forma de frenar el ingreso de información adicional
 - Los atacantes utilizan los campos de entrada para enviar sus solicitudes a la BD.
-



A mockup of a user login form on a dark teal background. The form consists of three main elements: a title, two input fields, and a submit button. The title 'USER LOGIN' is in bold white text. The first input field is for the 'Username', indicated by a person icon in a circle and the text 'Username'. The second input field is for the 'Password', indicated by a padlock icon in a circle and the text 'Password'. Below these fields is a large white rounded rectangle containing the word 'LOGIN' in bold black text.

USER LOGIN

 Username

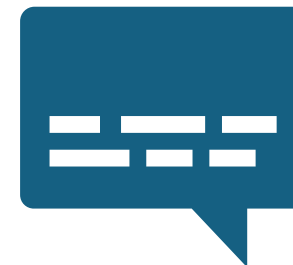
Password 

LOGIN

Signos de SQLi



Recepción de una cantidad excesiva de solicitudes en un plazo breve.



Ventanas emergentes desconocidas y mensajes de error.

Tipos de inyección de SQL

**SQLi en
banda**

**SQLi
inferencial**

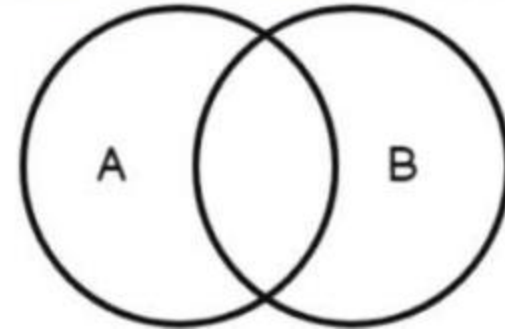
**SQLi fuera
de banda**

SQLi en Banda



Basado en Errores

La BD genera un mensaje de error, el atacante obtiene información de la infraestructura de la BD en función de los datos que generaron el error



Basado en Unión

Usan el operador de UNION para obtener todos los datos deseados en una única respuesta.

SQLi Inferencial

Aquí se buscan patrones de respuesta y comportamiento.

Los datos no se transfieren al atacante (osea que este no ve información sobre su ataque). Se clasifica en dos tipos

SQLi basado en el tiempo

Se estudia el tiempo de respuesta de un resultado de consulta, se espera determinar si esta fue True o False

SQLi booleana

Se envia consulta SQL, permite que la aplicación atacada responda mediante la generacion de un True o False

SQLi fuera de banda:

- Solo se pueden llevar a cabo en dos situaciones:
 1. Cuando los atacantes no pueden usar el mismo canal y compartir información.
 2. Cuando el servidor es demasiado lento o inestable para realizar acciones.