SQL Injection

...

SISI - LabSis - UTN FRC

Agenda

- ¿Qué es SQL Injection?
- Funcionamiento
- SQL Injection ciego
- Demo
- Amenazas
- Defensa
- Recomendaciones

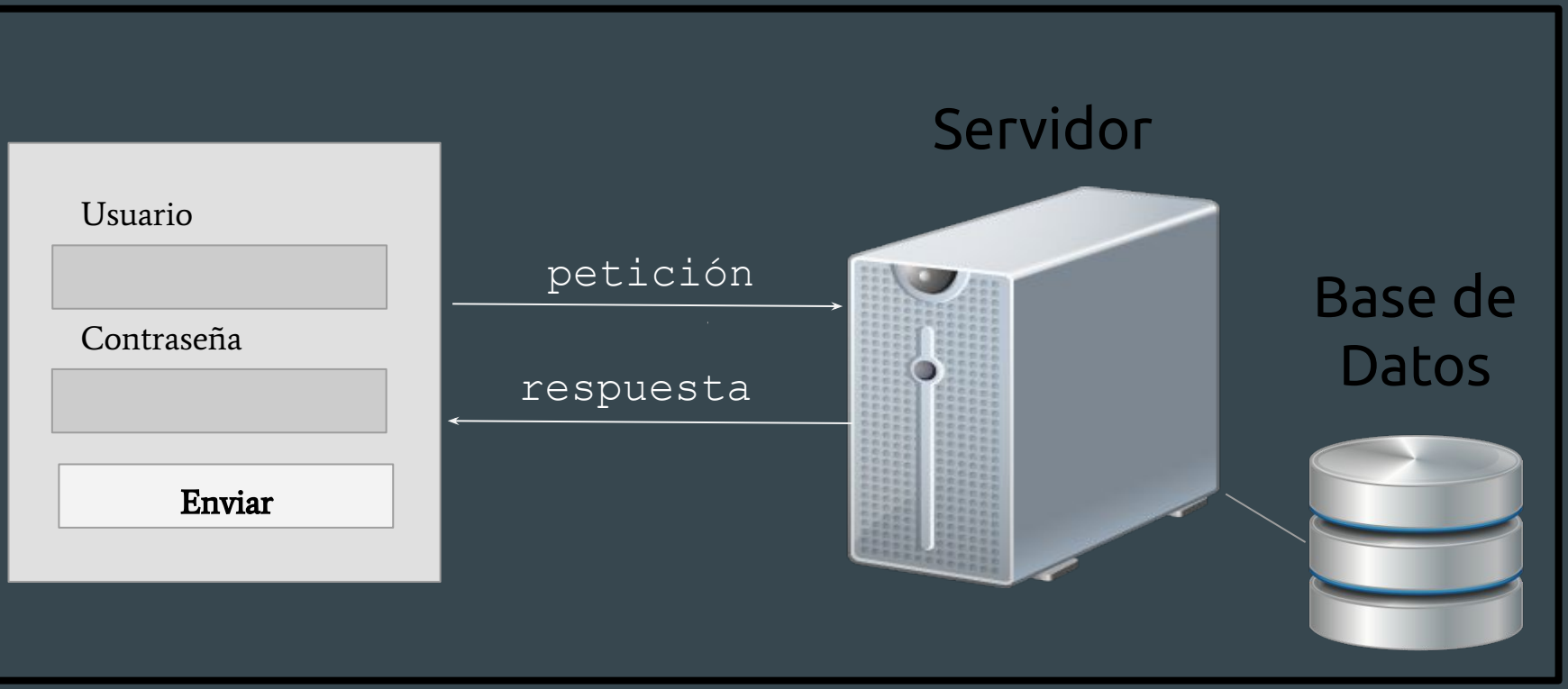
¿Qué es SQL injection?

SQL Injection

- **Ataque de inyección**
- Potencialmente puede realizarse sobre cualquier aplicación que tenga una base de datos SQL
- OWASP TOP 10
  - De fácil explotación
  - De impacto severo

Funcionamiento

Paso a paso - Caso de prueba - Login



Paso a paso - Caso de prueba - Login

Podemos imaginar que la consulta es algo similar a

SELECT id

FROM usuarios

WHERE username = '*&username*' AND password = '*&password*'

Si la consulta retorna el id, entonces el usuario existe y se loguea en la aplicación.

Paso a paso - Caso de prueba - Login

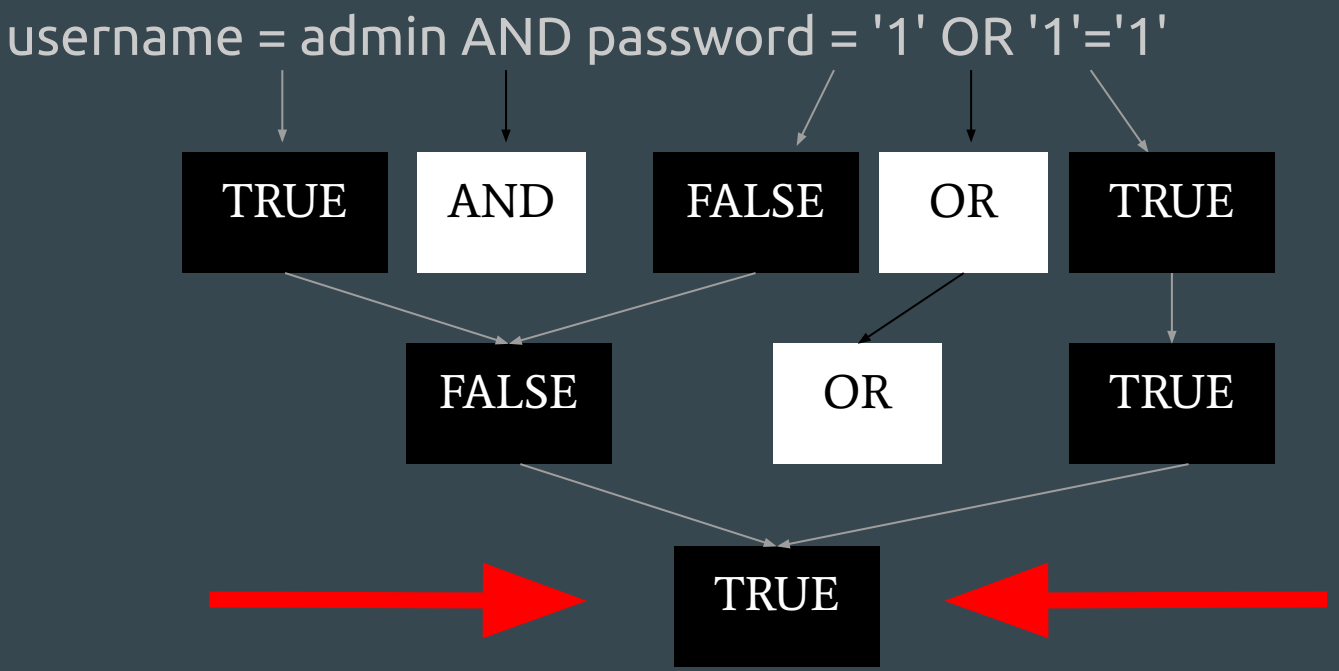
$username = admin ; $pass = 1' OR '1'='1


```
SELECT id

FROM usuarios

WHERE username = admin

AND password = '1' OR '1'='1'
```

¿?

Paso a paso - Caso de prueba - Login

Analicemos lógicamente la cláusula WHERE:



SQL Injection ciego

SQL Injection ciego

Es inyección SQL como cualquiera con la particularidad de que la misma no devuelve mensajes de error al ejecutar una sentencia SQL. Sino que retorna un TRUE o un FALSE.

La idea es ir probando valores y analizar si los mismos retornan un verdadero o false

Dos tipos de SQL injection a ciegas:

- Basados en contenido
- Basados en tiempo

Demo

Amenazas

Según el nivel de permisos que un atacante obtenga sobre el servidor y la base de datos, podría:

- Suplantar a usuarios específicos.
- Obtener toda la información almacenada en la base.
- Modificar o eliminar cualquiera de los datos almacenados.
- Ejecutar comandos del sistema operativo, si el servidor lo permite.

Defensa

...

Defensa

- Validar cualquier entrada de datos:
  - Todo lo que vaya a ser interpretado por el DBMS debe ser lo esperado. Deben filtrarse caracteres inválidos, llamadas a funciones, procedimientos almacenados, etc.
  - Realizar validaciones del lado del cliente (opcional) y del servidor (obligatorio).
- Limitar el acceso a los recursos:
  - Creación de perfiles de usuario que limiten el uso de la base de datos según roles.
  - Utilización de vistas que muestren sólo las columnas necesarias.

Recomendaciones

- Validar el formato de las entradas.
- Respetar el mínimo privilegio.
- Almacenar la información sensible en un formato secreto.
- Realizar backups periódicamente.
- Registrar las acciones de los usuarios mediante logs.
- Ocultar los mensajes de error que brinden información relevante.

¡¡Muchas gracias!!

¿Preguntas?