INYECCIÓN SQL

HACKING

CONCEPTOS

DB: Almacén de datos simples o estructurados.

Motor de DB: Programa que implementa acceso a data.

SQL: Lenguaje de consulta (para DB).

CONCEPTOS

Inyección: Interceptar una transacción.

Transacción: Consulta (o grupo) hecha a una DB.

Tabla, columna, registro: Componentes de DB.

INTRODUCCIÓN A SQL

MANIPULACIÓN: SELECT

```
SELECT * FROM users;
```

INTRODUCCIÓN A SQL

MANIPULACIÓN: INSERT

```
INSERT INTO users VALUES ('bryanjhv', 'password');
```

INTRODUCCIÓN A SQL

MANIPULACIÓN: UPDATE

```
UPDATE users SET username = 'bryan' WHERE id = 1;
```

INTRODUCCIÓN A SQL

MANIPULACIÓN: DELETE

```
DELETE FROM users;
```

INTRODUCCIÓN A SQL

FILTRADO: WHERE

```
SELECT * FROM users WHERE id >= 5;
```

INTRODUCCIÓN A SQL

FILTRADO: ORDER BY

```
SELECT * FROM personas ORDER BY nombre;
```

INTRODUCCIÓN A SQL

FILTRADO: LIMIT

```
SELECT * FROM personas ORDER BY pago LIMIT 3;
```

INTRODUCCIÓN A SQL

OPERADORES: BETWEEN

```sql
SELECT * FROM personas WHERE edad BETWEEN (18, 30);
```

INTRODUCCIÓN A SQL

OPERADORES: AND/OR

```
SELECT * FROM users WHERE id >= 5 AND id <= 30;
```

MYSQL

Motor de DB opensource, gratis. Muy usado con PHP.

ESCENARIOS

FORMULARIOS

Se pide un usuario y se ingresa una consulta.

ESCENARIOS

CONCATENACIÓN

Al leer el usuario, se lo adjunta a la consulta.

ESCENARIOS

NO VALIDACIÓN

El usuario contiene símbolos, o tiene 1000 caracteres.

IMPLICACIONES

OBTENER DB DESIGN

"Atar cabos" lleva a esto.

IMPLICACIONES

FILTRADO

Los muy conocidos "leaks", se filtra información.

IMPLICACIONES

DESCONFIANZA

¿Confiarías en un sitio si deja libre tus datos?

No los datos que piensas, los comunes.

IMPLICACIONES

DATA LOSS

Si puede ejecutar algo, ¿por qué no un ...?

```
DELETE FROM payments;
```

SOLUCIONES

ESCAPAR CARACTERES

Una consulta no debe tener " o ' .

Reemplazar " por \" .

SOLUCIONES

VALIDACIÓN

Un nombre de usuario debe:

- Tener entre 6 y 30 caracteres.
- Hacer match a `[A-Za-z][A-Za-z0-9._]+`.

SOLUCIONES

GUARDS

Por cada consulta, preguntar si el usuario está autorizado.

Poner un campo oculto y verificarlo en cada petición.

SOLUCIONES

LIBRERÍAS

Éstas han pasado por esto y son mantenidas. Ejemplos para PHP:

- `illuminate/database`
- `Zend ORM`

FIN