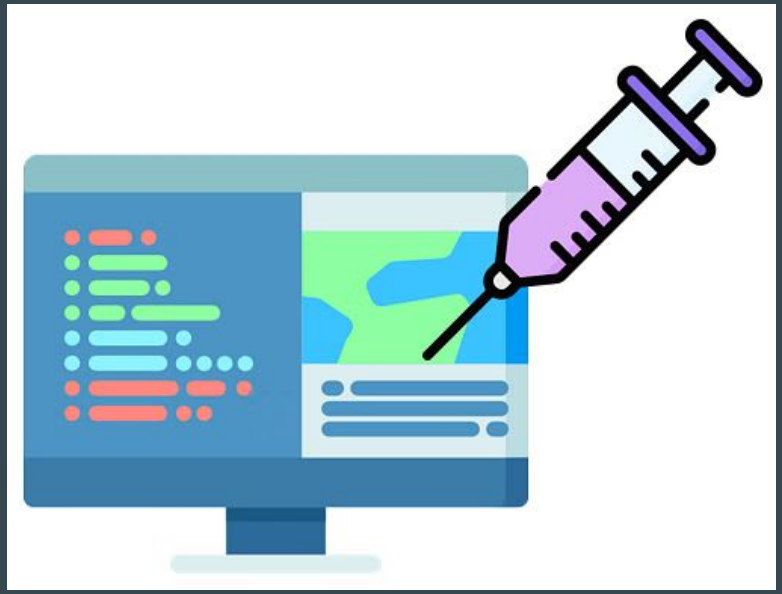
SQL INJECTION

Seguridad e Integridad de Sistemas



¿Qué es un SQL Injection?

SQL injection (SQLi) es un tipo de vulnerabilidad que ocurre cuando un usuario puede modificar las consultas que la aplicación realiza sobre su base de datos.

Se da cuando las consultas SQL son armadas de forma insegura, por ejemplo, concatenando entradas del usuario.

EJEMPLO

```go
func loginUserVulnerable(db *sql.DB, username, password string) bool {
    query := "SELECT * FROM users WHERE username='" + username +
    "' AND password='" + password + "'"
    rows, err := db.Query(query)
    if err != nil {
        log.Fatal(err)
    }
    defer rows.Close()

    return rows.Next()
}
```

```go
func loginUserSafe(db *sql.DB, username, password string) bool {
    query := "SELECT * FROM users WHERE username=? AND password=?"
    rows, err := db.Query(query, username, password)
    if err != nil {
        log.Fatal(err)
    }
    defer rows.Close()

    return rows.Next()
}
```

Técnicas de explotación

- Recuperación de datos ocultos.
- Login bypass.
- Recuperar datos de otras tablas.

Técnicas de explotación

- Recuperación de datos ocultos

https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

Técnicas de explotación

- Login bypass.

https://portswigger.net/web-security/sql-injection/lab-login-bypass

Técnicas de explotación

- Recuperar datos de otras tablas.

https://portswigger.net/web-security/sql-injection/union-attacks

```
' UNION SELECT username, password FROM users--
```