Injecția SQL (SQL Injection)

Injecția SQL (SQL Injection) este o tehnică de injecție de cod (**code injection**) care ar putea distruge **baza de date**.
Injecția SQL (SQL Injection) este una dintre cele mai frecvente **tehnici de hacking web**.
Injecția SQL (SQL Injection) este plasarea codului rău intenționat în **declarațiile SQL**, prin introducerea **paginii web**.

SQL în paginile web

Injecția SQL (SQL Injection) are loc de obicei atunci când ceri utilizatorului o introducere, cum ar fi numele său de utilizator/userid (**username/userid**), iar în loc de nume/id (**name/id**), utilizatorul vă oferă o **declarație SQL** pe care o veți rula în mod neștiut pe **baza de date**.
Uitați-vă la următorul exemplu care creează o **instrucțiune SELECT** adăugând o variabilă (**txtUserId**) la un șir selectat. Variabila este preluată din intrarea utilizatorului (**getRequestString**):

Exemplu:

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

Restul acestui capitol descrie pericolele potențiale ale utilizării intrării utilizatorului în **declarațiile SQL**.