PHP MySQL Declarații pregătite

Declarațiile pregătite (prepared statements) sunt foarte utile împotriva injecțiilor SQL (SQL injections).

Declarații pregătite și parametri legați (Prepared Statements and Bound Parameters)

O **declarație pregătită (prepared statements)** este o caracteristică utilizată pentru a executa aceleași (sau similare) **instrucțiuni SQL** cu o eficiență ridicată.

Declarațiile pregătite (prepared statements) funcționează astfel:

1. **Pregătire:** Un **șablon de instrucțiuni SQL (SQL statement template)** este creat și trimis în **baza de date**. Anumite valori sunt lăsate nespecificate, numite parametri (etichetat (labeled) "?"). **Exemplu: INSERT INTO MyGuests VALUES(?, ?, ?)**.
2. **Baza de date** analizează, compilează și efectuează **optimizarea interogării** (**query**) pe **șablonul de instrucțiuni SQL (SQL statement template)** și stochează rezultatul fără a-l executa.
3. **Executare:** ulterior, aplicația leagă valorile la parametrii, iar **baza de date** execută **instrucțiunea**. Aplicația poate executa **instrucțiunea** ori de câte ori dorește cu valori diferite.

Față de executarea directă a **instrucțiunilor SQL**, **instrucțiunile pregătite (prepared statements)** au trei avantaje principale:

- **Instrucțiunile pregătite (prepared statements)** reduc **timpul de analiză (parsing time)**, deoarece pregătirea pe **interogare (query)** se face o singură dată (deși instrucțiunea este executată de mai multe ori).
- **Parametrii legați (bound parameters)** minimizează **lățimea de bandă (bandwidth)** către server, deoarece trebuie să trimiteți de fiecare dată doar **parametrii** și nu întreaga **interogare (query)**.
- **Instrucțiunile pregătite (prepared statements)** sunt foarte utile împotriva **injecțiilor SQL (SQL injections)**, deoarece **valorile parametrilor**, care sunt transmise ulterior folosind un protocol diferit, nu trebuie eliberate corect (correctly escaped). Dacă **șablonul de instrucțiune originală (original statement template)** nu este derivat de la **intrarea externă (external input)**, nu poate apărea **injecția SQL (SQL injection)**.