Indice

**Autore : Mohamed Hassan**

|  |
| --- |
|  |
| Usare MYSQL in PHP |
|  |
| Approfondimento Tecnico |

* Che Cos’è il PHP
* PHP e Database
* Che Cos’è MYSQL
* PHPMyAdmin
* PHP e MYSQL
* Sequenza dei passi per interagire con MySQL da PHP

Fonti

* <http://galdusmaffi.tk/Galdus/documenti/dispensa-php.pdfPHP>
* <http://galdusmaffi.tk/Galdus/documenti/php_e_mysql.pdf>
* Ringrazio il professore Pietro Maffi per collaborazzione

Che cos’èil PHP:

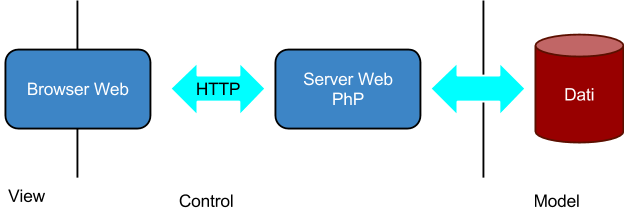
PHP:**Hypertext Preprocessor**, ed è un **linguaggio di scripting** dal lato del server immerso nel codice **Html**, **sofisticato e flessibile**, che può girare praticamente su qualsiasi **server Web,** su qualsiasi sistema operativo (Windows o Unix/Linux, ma anche Mac e altri), e consente di **interagire** praticamente con qualsiasi tipo di **database** (SQLite, MySQL, PostgreSQL, SQL Server, Oracle, SyBase, Access e altri).

PHP è un linguaggio molto semplice da utilizzare, a cominciare dalla sintassi derivata direttamente da veri l**inguaggi di programmazione** come C/C++, Perl, Java.

La vera forza del PHP sta nella gestione dei **database**, con poche righe di codice è possibileaccedere qualsiasi database, estrapolare **i dati** che ci interessano e inserirli nella **pagina Web.**

PHP è un linguaggio la cui funzione fondamentale è quella di produrre codice HTML, il linguaggio col quale si compongono le pagine Web. Ma, poichè PHP è un linguaggio di programmazione, abbiamo la possibilità di analizzare diverse situazioni (l’input degli utenti, i dati contenuti in un database) e di decidere, di conseguenza, di produrre codice HTML condizionato ai risultati dell’elaborazione. Questo è, in parole povere, il Web dinamico.

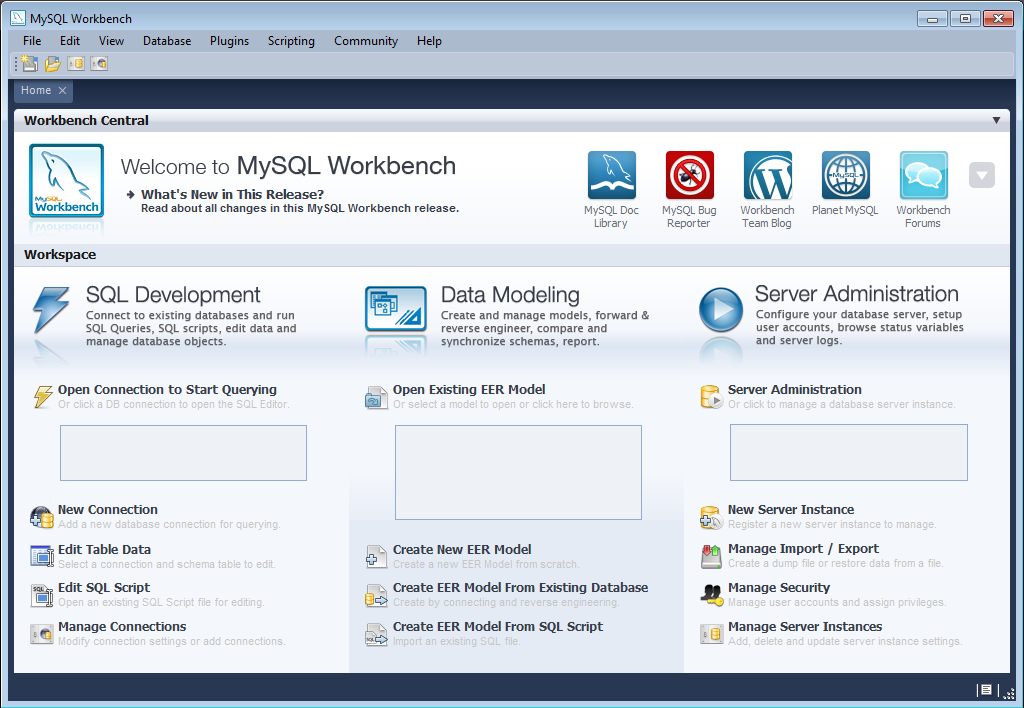
PHP e Database



Quando i dati sono molti e salvare i dati su filesystem risulta inefficiente conviene usare il supporto di una **base di dati**.PHP fornisce delle funzioni per **accedere ai database**, ma essenzialmente si usa lo script SQL per lavorare sui DB.

PHP è tipicamente usato con MySQL, un database free opensourceliberamente scaricabile da [www.mysql.org](http://www.mysql.org). E’ possibile accedere anche ad altri database (Postgres, access, oracleetc).

Che Cos’è MYSQL:

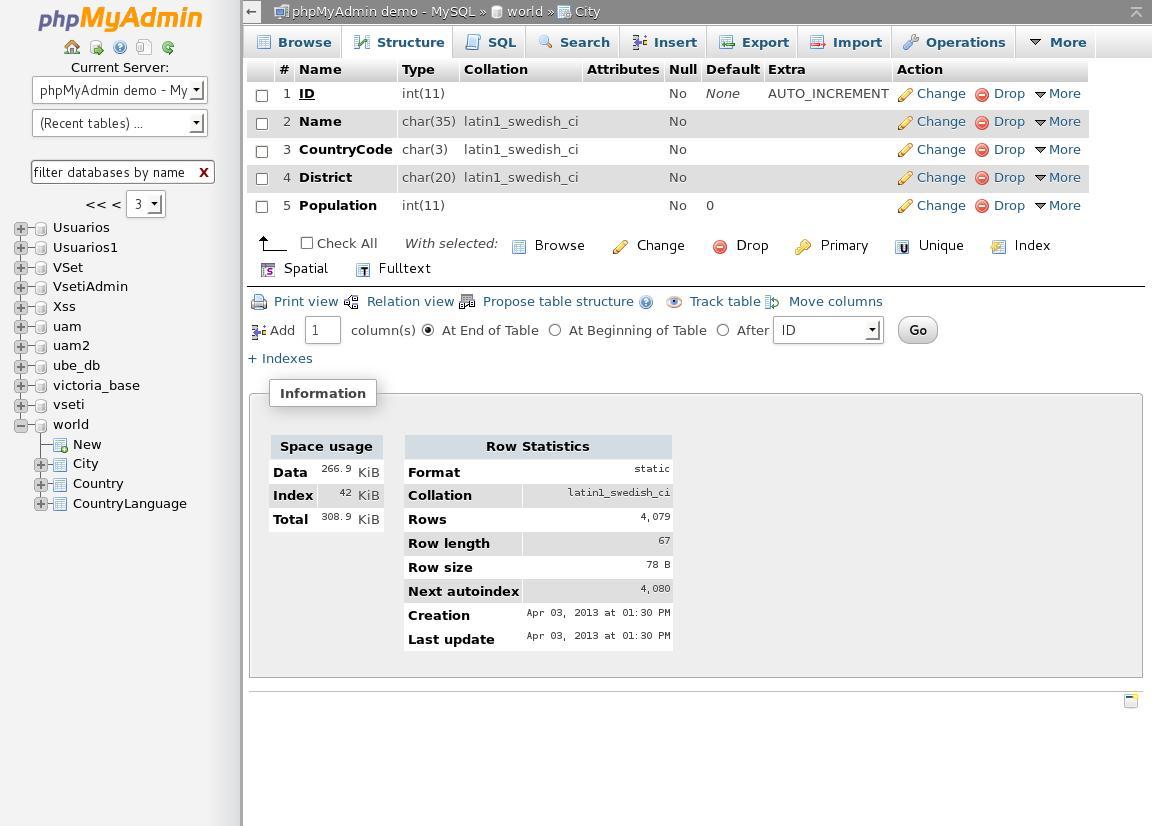


MySQL è disponibile su tutte le piattaforme ed è realizzato come un server (quindi un servizio attivo che risponde su una porta) .

Ogni **server MySQL** può essere configurato per gestire **database**, ognuno dei quali conterrà **tabelle** le quali potranno essere popolate con i **dati** (**record**).

L’interazione con il server MySQL può avvenire da riga di comando (shell) digitando i comandi, o le query SQL, per creare database, tabelle, inserire dati, fare ricerche etc. L’interazione può avvenire anche tramite interfaccia grafica, ad esempio PhpMyAdmin.

PHPMyAdmin



Un client molto usato basato su una grafica user-friendly è PHPMyAdmin, una **applicazione web** fatta in PHP che permette di gestire **MYSQL** server via interfaccia web.

Si può liberamente scaricare da <http://www.phpmyadmin.net/> si installa come applicazione PHP. E’ già incluso in EasyPHP, MAMP e XAMMP.

Se è installato sulla cartella di default del **server web** è tipicamente disponibile alla URL: <http://localhost/phpmyadmin/> Oppure <http://localhost/mysql> su Easyphp.

MySQL viene configurato di default con un utente “root” amministratore. Può essere configurato aggiungendo altri utenti e concedendo diritti sui database.

Con il login di root possiamo accedere all’interfaccia di phpmyadmin, da dove possiamo creare nuovi database, nuove tabelle, inserire dati, eseguire query e tante altre funzionalità più avanzate.

Occorre ricordarsi la password di "root". Se non è stata impostata sarà null.

PHP e MYSQL

Le basi di dati, chiamate anche **database** o banche dati, sono degli archivi che contengono dei dati e integrano informazioni relative alla struttura dei dati stessi; in particolare, è possibile affermare che un database viene strutturato in modo da permettere procedure per la **manipolazione** dei dati attraverso apposite applicazioni, in esso i dati sono suddivisi sulla base di argomenti disposti in ordine logico, chiamati **tabelle**, suddivisi a loro volta per categorie chiamate **campi**.

I campi sono destinati a definire le caratteristiche delle informazioni archiviate, conservate all’interno di **record**, per cui ogni tabella può essere rappresentata come un piano cartesiano in cui le colonne conservano le **proprietà** dei dati mentre le righe memorizzano i dati stessi.

La **SQL injection** è una tecnica dell’**hacking** mirata a colpire le applicazioni web che si appoggiano su un **database** di tipo SQL. Il metodo usato per forzare un sito sfrutta la mancata implementazione di controlli sui campi che si ricevono in input che arrivano tramite il **GET o il POST** al nostro sito.

Se non vengono fatti i dovuti controlli, il nostro malintenzionato può inviare codice maligno all’interno di una richiesta sfruttando il codice SQL e il nostro DB. Se il nostro sito è vittima di questo attacco le conseguenza possono essere **disastrose** in quanto il nostro intruso può autenticarsi con privilegi anche si root e cambiare o visualizzare dati sensibili.

Come tutte le cose efficienti il metodo usato per questo attacco è molto semplice e si basa sulla possibilità di inviare del codice SQL opportunamente creato in un form o in una query string in modo tale che il server interpreti il nostro codice nel DB ma un esempio è molto più esplicativo.

Sequenza dei passi per interagire con MySQL da PHP

