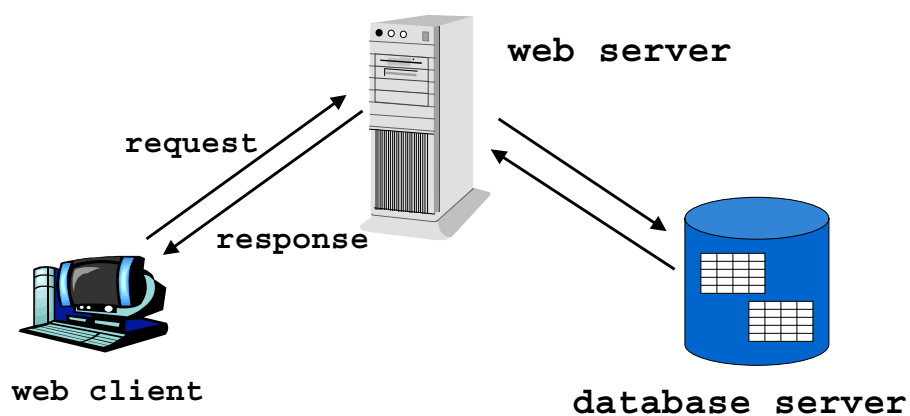

Programmazione lato server

PHP + MySQL

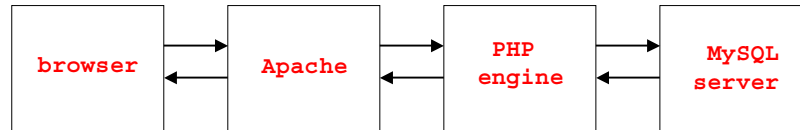
Applicazioni di Rete - M. Ribaudo - DISI

Cosa vediamo ...



Applicazioni di Rete - M. Ribaudo - DISI

Cosa vediamo ...



Applicazioni di Rete - M. Ribaudo - DISI

MySQL

" ... MySQL is a very fast, robust, relational database management system. The MySQL server controls access to your data to ensure that multiple users can work with it concurrently ... MySQL has been publicly available since 1996, but has a development history going back to 1979 ... "

Applicazioni di Rete - M. Ribaudo - DISI

MySQL: accesso al server

- Digitando

```
> mysql -h hostname -u username -p
Enter password: *****
```

si invoca il monitor MySQL, un client che permette di utilizzare il server MySQL

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 26944 to server version: 3.23.49-log
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql>
```

Applicazioni di Rete - M. Ribaudo - DISI

MySQL: comandi utili

```
mysql> show databases;
mysql> use <nomedb>;
mysql> show tables;
mysql> describe <nometable>;
```

Applicazioni di Rete - M. Ribaudo - DISI

MySQL: comandi utili

```
> mysql -h localhost -u ribaudo -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 27328 to server version: 3.23.49-log

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> use mysql;
ERROR 1044: Access denied for user: 'ribaudo@localhost' to
database 'mysql'

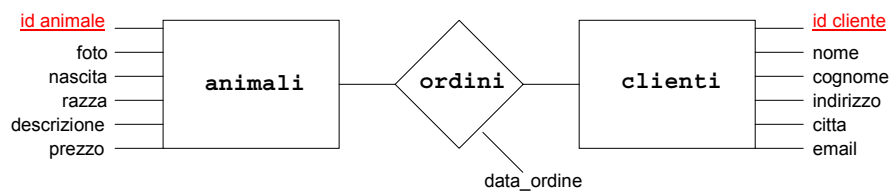
mysql> use negozio;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

Applicazioni di Rete - M. Ribaudo - DISI

MySQL: creazione di un database

▪ Database dell'esempio



Applicazioni di Rete - M. Ribaudo - DISI

MySQL: creazione di un database

```
mysql> CREATE DATABASE negozio;
```

```
mysql> CREATE TABLE animali (  
    id_animale INT NOT NULL AUTO_INCREMENT,  
    foto CHAR(255) NOT NULL ,  
    razza CHAR(100) NOT NULL ,  
    nascita DATE NOT NULL ,  
    descrizione TEXT,  
    prezzo FLOAT(4,2),  
    PRIMARY KEY (id_animale) );
```

NB: tutte le istruzioni devono sempre terminare con ;

Applicazioni di Rete - M. Ribaudò - DISI

MySQL: creazione di un database

```
mysql> CREATE TABLE clienti (  
    id_cliente INT NOT NULL AUTO_INCREMENT,  
    nome CHAR(100) ,  
    cognome CHAR(100) NOT NULL ,  
    indirizzo CHAR(255) NOT NULL ,  
    citta CHAR(100) NOT NULL ,  
    email CHAR(100) NOT NULL ,  
    PRIMARY KEY (id_cliente) );
```

```
mysql> CREATE TABLE ordini (  
    id_cliente INT NOT NULL ,  
    id_animale INT NOT NULL ,  
    data DATE NOT NULL ,  
    PRIMARY KEY (id_cliente , id_animale) );
```

Applicazioni di Rete - M. Ribaudò - DISI

MySQL: popolare il database

```
mysql> INSERT INTO animali
(id_animale,foto,razza,nascita,descrizione,prezzo)
VALUES
(NULL,'images/pappagalli.jpg', 'Pappagallus
giallus', '2002-12-21', 'Coppia di pappagalli
(maschio e femmina) bla bla ...');
```

Poichè `id_animale` è di tipo `AUTO_INCREMENT` si può specificare il valore `NULL` (oppure nessun valore), lasciando a MySQL il compito di creare il valore per questo campo

Applicazioni di Rete - M. Ribaudo - DISI

MySQL: comandi utili

Si può salvare il codice SQL che serve per creare e popolare un database in un file di testo, es. `negozio.sql`, e poi usare il comando

```
$ mysql -u username -p < negozio.sql;
```

Applicazioni di Rete - M. Ribaudo - DISI

MySQL: comandi utili

```
mysql> show databases;
mysql> use <nomedb>;
mysql> show tables;
mysql> describe <nometable>;
```

```
mysql> describe animali;
```

Field	Type	Null	Key	Default	Extra
id_animale	int(11)		PRI	NULL	auto_increment
foto	varchar(255)				
razza	varchar(100)				
nascita	date			0000-00-00	
descrizione	text	YES		NULL	
prezzo	float(4,2)			0	

```
6 rows in set (0.00 sec)
```

```
mysql>
```

Applicazioni di Rete - M. Ribaudò - DISI

MySQL: select

Una volta creato e popolato un database lo si può interrogare e/o modificare usando il linguaggio SQL

```
$ mysql -u username -p
$ Enter password: ****;
```

```
mysql> use negozio;
```

```
mysql> select id_animale,foto,razza, prezzo from animali;
```

id_animale	foto	razza	prezzo
1	images/gatti.jpg	Persiano fulgidus	50
2	images/pesci.jpg	Pesce rosso cunilicus	20
3	images/pappagalli.jpg	Pappagallus giallus	100
4	images/cane.jpg	Lupus tuscanus	100

```
4 rows in set (0.00 sec)
```

```
mysql>
```

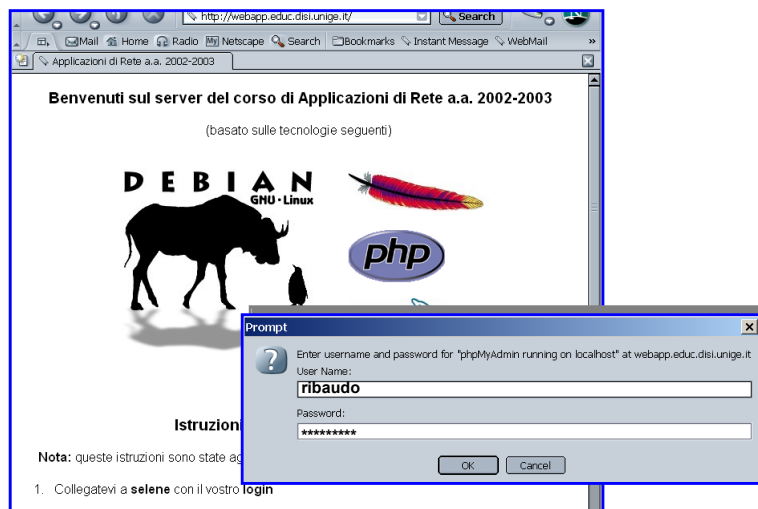
Applicazioni di Rete - M. Ribaudò - DISI

MySQL: front-end

- Per fortuna esistono dei pacchetti software (open source) che forniscono l'accesso ad un server MySQL mediante un'interfaccia grafica più o meno user-friendly ...
- Useremo phpMyAdmin

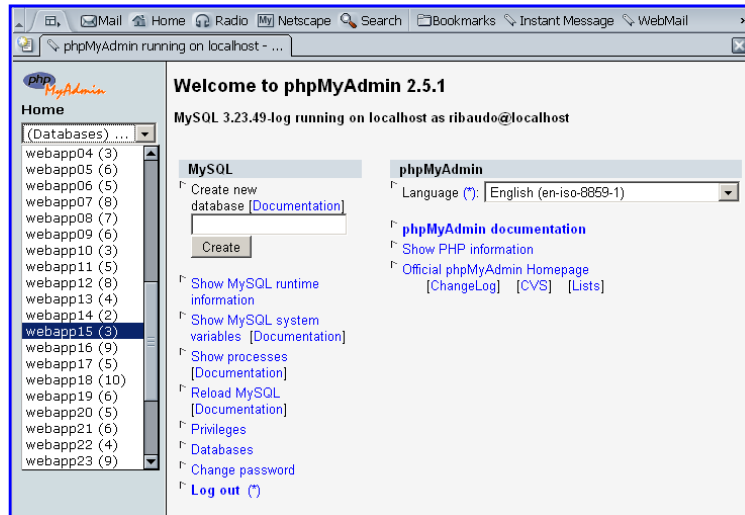
Applicazioni di Rete - M. Ribaldo - DISI

MySQL: phpMyAdmin su webapp



Applicazioni di Rete - M. Ribaldo - DISI

MySQL: phpMyAdmin su webapp



Applicazioni di Rete - M. Ribaudo - DISI

MySQL: utenti

- Un server MySQL può gestire più utenti
 - ✓ L'utente **root** deve essere usato solo per l'amministrazione del DBMS
 - ✓ Per ogni utente che deve usare il sistema (ancor meglio, per ogni applicazione web) si dovrebbero definire
 - 1) **username** e 2) **password**
- Per il progetto di laboratorio ogni gruppo avrà un suo username (webappx1, webappx2, webappx3, ...)

Applicazioni di Rete - M. Ribaudo - DISI

MySQL: privilegi

" ... A **privilege** is the right to perform a particular action on a particular object, and is associated with a particular user. You can create a user within MySQL, you grant her a set of privileges to specify what she can and cannot do within the system ..."

" ... principle of **Least Privilege**: a user (or process) should have the lowest level of privilege required in order to perform his task assigned ..."

Applicazioni di Rete - M. Ribaudò - DISI

MySQL: privilegi

- MySQL fornisce 4 livelli di privilegi
 - ✓ Global, Database, Table, Column
- Per assegnare (cancellare) un privilegio ad un utente si usa il comando GRANT (REVOKE)

```
mysql> GRANT <privileges> [columns]
      ON <item>
      TO <username> [IDENTIFIED BY '<password>']
      [WITH GRANT OPTION];
```

Applicazioni di Rete - M. Ribaudò - DISI

MySQL: privilegi

- I privilegi sono espressi mediante un elenco di nomi separati dalla virgola
- MySQL permette di definire privilegi per l'utente generico, privilegi per l'amministratore, e dei privilegi speciali
- Per l'utente generico si possono specificare i seguenti privilegi (che corrispondono alle operazioni che si possono fare su un database con SQL)
SELECT, INSERT, UPDATE, DELETE, INDEX, ALTER, CREATE, DROP

Applicazioni di Rete - M. Ribaudò - DISI

MySQL: privilegi

- Esempio

```
mysql> GRANT select, insert, update, delete,  
        index, alter, create, drop
```

```
ON webappxy.*  
TO webappxy  
IDENTIFIED BY '*****';
```

Applicazioni di Rete - M. Ribaudò - DISI

MySQL: privilegi

- I privilegi sono memorizzati in alcune tabelle del database di sistema mysql
 - ✓ mysql.user
 - ✓ mysql.db
 - ✓ mysql.tables_priv
 - ✓ mysql.column_priv

- Invece di usare il comando GRANT si possono modificare direttamente queste tabelle

- Perchè il server MySQL "senta" le modifiche sui privilegi ci vuole il comando

```
mysql> FLUSH PRIVILEGES;
```

Applicazioni di Rete - M. Ribaudo - DISI

Accesso a MySQL mediante PHP

- I passi fondamentali sono
 1. Controllare e filtrare i dati in arrivo dell'utente
 2. Stabilire una connessione con il database
 3. Interrogare il database
 4. Ottenere il risultato
 5. Formattare il risultato per l'utente

Applicazioni di Rete - M. Ribaudo - DISI

Accesso a MySQL mediante PHP

- Esistono molte funzioni di libreria che permettono di portare a termine i passi 2, 3, 4
- Tutte queste funzioni iniziano con il prefisso `mysql_`

Applicazioni di Rete - M. Ribaudò - DISI

1) Controllare i dati in arrivo

```
$nomevar = trim($nomevar)
```

```
$nomevar = addslashes($nomevar)
```

```
$nomevar = stripslashes($nomevar)
```

In alternativa, nel file `php.ini`

```
magic_quotes_gpc On
```

```
magic_quotes_runtime On
```

```
$nomevar = htmlspecialchars($nomevar)
```

Applicazioni di Rete - M. Ribaudò - DISI

2) Stabilire una connessione con il database

```
<?php
$db = mysql_pconnect("localhost","username","password");

if (!$db) {
    echo "*** Attenzione, non riesco a creare la
    connessione";
    exit;
}

mysql_select_db("nomedb") or
    die ("*** Attenzione, non trovo il database");

?>
```

Applicazioni di Rete - M. Ribaudò - DISI

2) Stabilire una connessione con il database

```
mysql_pconnect(): crea una connessione persistente
mysql_connect(): la connessione viene chiusa quando
termina lo script
```

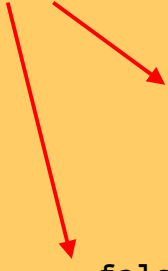
La funzione die() permette di terminare l'esecuzione di uno script fornendo un messaggio di errore. Si può anche richiamare una funzione, es.

```
function err_msg(){
    echo "Si è verificato il seguente errore:";
    echo mysql_error();
}
die(err_msg());
```

Applicazioni di Rete - M. Ribaudò - DISI

3) Interrogare il database

```
$query="select attr1,..., attrn from ... where ...";  
$res = mysql_query($query);
```



attr1	attr2		attrn

false


Applicazioni di Rete - M. Ribaudo - DISI

4) Ottenere il risultato

attr1	attr2		attrn

```
$num_res = mysql_num_rows($res);
```

```
$row = mysql_fetch_array($res);
```

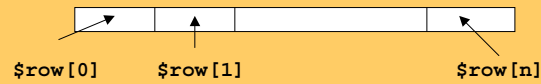


```
$row["attr1"] $row["attr2"] $row["attrn"]
```

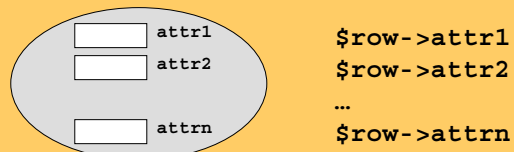
Applicazioni di Rete - M. Ribaudo - DISI

4) Ottenere il risultato

```
$row = mysql_fetch_row($res);
```



```
$row = mysql_fetch_object($res);
```



Applicazioni di Rete - M. Ribaudo - DISI

5) Formattare il risultato per l'utente

```
...
echo "<tr>";
echo "<td>" . $row["attr1"] . "</td>\n";
echo "<td>" . $row["attr2"] . "</td>\n";
...
echo "<td>" . $row["attrn"] . "</td>\n";
echo "</tr>"
...

```

Applicazioni di Rete - M. Ribaudo - DISI

Esempio: negozio virtuale

The screenshot shows the 'spesa CLICK' website interface. At the top, it says 'spesa CLICK' and 'Reparto Animali'. Below this, there is a navigation instruction: 'Segui il link "dettagli" a fianco dell'animale che ti interessa'. There are three animal images: a cat, a goldfish, and two parrots. Each image has a 'dettagli' link next to it. A red arrow points from the 'dettagli' link for the cat to a separate window titled 'Dettagli - Netscape'. This window displays the following information: 'Razza: Persiano fulgidus', 'Data di nascita: 2003-01-18', 'Descrizione: Persiano tradizionale, colore grigio bianco; su richiesta si redige il pedigree', and 'Prezzo: 50 euro'. At the bottom of the window, there is a link: 'Per procedere all'ordine, segui il link [ordina adesso](#)'.

Codice sorgente degli esempi sulle pagine della lezione

Applicazioni di Rete - M. Ribaudò - DISI

Esempio: negozio virtuale

The screenshot shows two parts of the 'spesa CLICK' website. The top part is a registration form with the following fields: 'Nome' (Gianni), 'Cognome' (Verduci), 'Indirizzo' (Via Dodecaneso 35), 'Città' (Bologna), and 'E-mail' (verduci@disi.unige.it). There are 'Continua' and 'Cancella' buttons. A red arrow points from the 'Continua' button to the bottom part of the screenshot. The bottom part shows a confirmation message: 'Gianni Verduci, il tuo ordine è stato ricevuto. Provvederemo alla consegna entro 48 ore. Grazie, lo staff di spesaClick'. At the bottom of this message, there is contact information: 'spesa CLICK, sede legale: Torino, Via Po 1' and 'Scrivi a webmaster@spesaclick.it'.

Codice sorgente degli esempi sulle pagine della lezione

Applicazioni di Rete - M. Ribaudò - DISI

Invio di e-mail

```
$to=$email;  
  
$subject="Grazie per aver scelto spesaClik";  
  
$msg="$nome $cognome, abbiamo ricevuto ...";  
$msg = $msg . "Grazie, lo staff di spesaClick";  
  
$from="ribaudo@disi.unige.it";  
  
mail($to, $subject, $msg, $from);
```

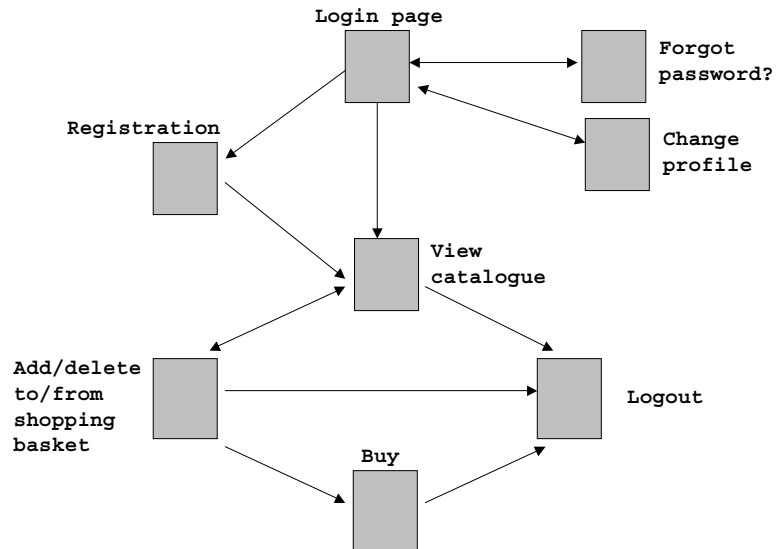
Applicazioni di Rete - M. Ribaudo - DISI

Problemi dell'esempio

- Tanti ...
 - ✓ Ogni volta un cliente deve inserire i propri dati per effettuare un nuovo ordine
 - ✓ Il catalogo è lo stesso per tutti gli utenti
 - ✓ Si può effettuare un solo ordine alla volta
 - ✓ Non aggiornare il database dopo ogni ordine!

Applicazioni di Rete - M. Ribaudo - DISI

Una esempio di struttura più complessa



Applicazioni di Rete - M. Ribaudo - DISI

Problemi

- Tanti ... ma soprattutto

HTTP è stateless e quindi richieste successive non sono "associate" tra loro

- Non possiamo chiedere all'utente di digitare login e password ogni volta che visita una nuova pagina

Applicazioni di Rete - M. Ribaudo - DISI

Alcune soluzioni possibili

- **Usare campi nascosti**
- **Farsi aiutare dal web server mediante il meccanismo di autenticazione fornito da .htaccess**
(bisogna avere accesso al web server come amministratori)
- **Usare cookies e sessioni**

Applicazioni di Rete - M. Ribaudo - DISI

Campi nascosti

- **Al momento della registrazione si crea un valore che identifica l'utente, per esempio una stringa generata in modo casuale**
- **Si memorizza questo dato nel database insieme ai dati dell'utente**

Applicazioni di Rete - M. Ribaudo - DISI

Campi nascosti

- In tutte le pagine successive,
 - ✓ se c'è un modulo, si deve introdurre un campo nascosto

```
<input type="hidden"
      name="pin"
      value="*****">
```

- ✓ se non c'è un modulo, si deve associare ai link una stringa di interrogazione

```
<a href="file.php?pin=*****">next</a>
```

Applicazioni di Rete - M. Ribaudò - DISI

Campi nascosti

- In tutti i file PHP, prima di tutto si legge dalla variabile \$pin il valore del campo nascosto
- Si "riconosce" l'utente e si prosegue
- Problema
 - ✓ Il campo nascosto è nel sorgente HTML (quindi modificabile !!!)
 - ✓ ... inoltre è un po' "macchinoso"

Applicazioni di Rete - M. Ribaudò - DISI