LE SESSIONI E L'ACCESSO AUTORIZZATO IN PHP

Il protocollo HTTP, utilizzato per la connessione e la trasmissione delle pagine Web, è un protocollo **senza memoria**. L'HTTP non ha quindi stato, ovvero, ogni richiesta è indipendente da tutte le altre fatte in precedenza, e non influenza quelle successive. Una volta che il server soddisfa tale richiesta, non è più in grado di **ricordare** nulla su di essa. Quando allora un utente presenterà una nuova richiesta, il Web Server non sarà in grado di rendersi conto che si tratta dello stesso utente della richiesta precedente, e la tratterà come tutte le altre.

Ci sono però situazioni in cui è importante stabilire una specie di **dialogo tra l'utente e il Web Server**, in quanto ogni operazione che l'utente compie può influenzare le successive ed essere influenzata dalle precedenti. Si pensi ad esempio a un sistema con un'**area riservata**: se un certo numero di pagine è visibile solo agli utenti registrati, questi dovranno loggarsi per poterle vedere, ma una volta effettuato il login dovranno essere messi nelle condizioni di vedere tutte le pagine dell'area riservata, senza, ovviamente, doversi ri-loggare per ciascuna pagina, e ciò sarà possibile solo se il server potrà ricordare che quell'utente si è già loggato.

NB Ricordiamo che possono esistere differenti tipi di utenti registrati con i relativi permessi per accedere o meno a determinate pagine o a determinati servizi offerti.

PHP permette di risolvere questo problema introducendo il meccanismo delle **sessioni**.

Dal punto di vista dell'utente, una **sessione di navigazione** sul Web è "*un periodo di tempo durante il quale l'utente naviga attraverso alcune pagine Web con il suo browser, per poi smettere di lavorare*".

Le pagine visitate sono generalmente (ma non necessariamente) in relazione tra di loro; possono ad esempio essere pagine visitate per la prenotazione di un volo di linea, quelle di un sito di vendita online, oppure quelle per gestire il conto-corrente online.

Durante la navigazione, per consentire un dialogo tra utente e Web Server occorre trovare un modo per ricordare i dati. Le sessioni, dal punto di vista di PHP "*sono file in ognuno dei quali vengono memorizzati i dati da ricordare (ad esempio quelli relativi all'utente)*".

Per aprire una nuova sessione in PHP esiste la funzione **session_start()**. In una pagina HTML questa funzione deve precedere qualsiasi altro codice.

Una volta aperta una sessione, PHP crea un array superglobale di nome **$_SESSION**, all'interno del quale vengono salvati tutti i dati che si ritiene di ricordare, per esempio la username e la password dell'utente che si sta per loggare.

Session_start();

$_SESSION

PROGETTO SITO WEB DINAMICO

1. **Reti di calcolatori**

- Ripasso di 4

2. **Database mySQL**
   - Ripasso di 3 → Database e Modello Relazionale
   - Connessione a un DB remoto
   - SQL: estrazione e inserimento dati

Creare un database contenente le seguenti tre tabelle in easyPHPmyAdmin (in associazione N:N):

`utenti(idUtente, nome, cognome, username, password, email, ruolo)`

`datiRilevati(idZona, idUtente, idZona, dato, data, ora)`

`dati(idZona, nome)`

3. **Struttura sito web – tabletless**
   - Fogli di stile CSS: sintassi
   - Utilizzo dei fogli di stile CSS per la realizzazione del layout:

     http://www.cssportal.com/layout-generator/

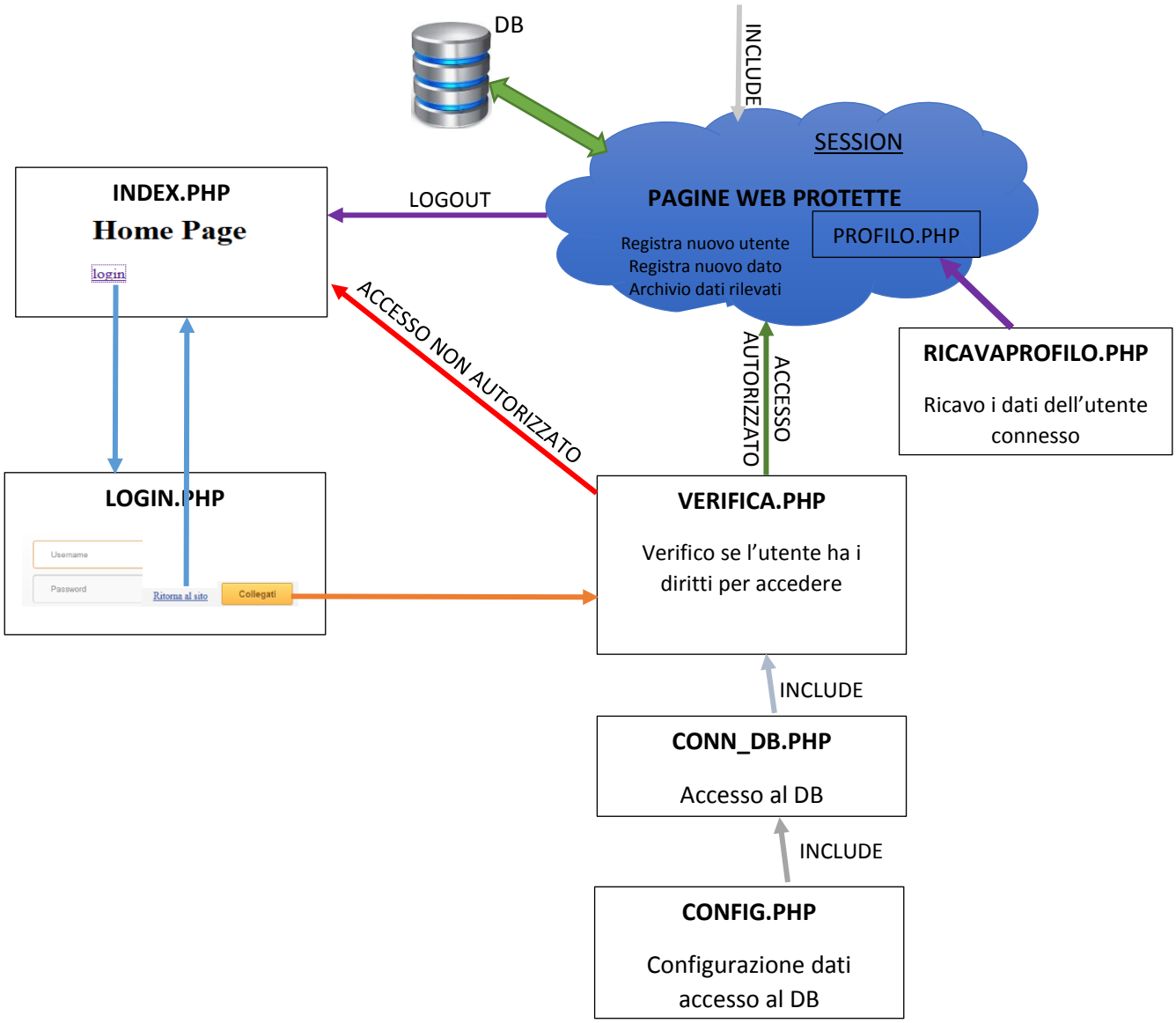
4. **Realizzazione pagine web dinamiche protette**
   - Linguaggio PHP
   - Variabili
   - Sequenza, selezione e iterazione
   - Funzioni standard
   - Accesso remoto al database attraverso PHP
   - Libreria PHP per la generazione di grafici 2D

5. **Grafica**
   - Temi grafici

STRUTTURA SITO WEB DINAMICO

PRIVATO.PHP

Controllo che l'utente sia ancora connesso e sia lo stesso
(come prima istruzione della pagina protetta)



config.php

```
<?php
	//dati generali
	$sitoweb = "Dani Blog";
	$data =(date("d-m-y"));
	$vers = "1.0";

	//URL PER HTACCESS
```

```
      $base_url = "http://localhost/appweb";


      //par connessione al DB
      $nomehost = "localhost"; //hostname
    $nomeuser = "root"; //nome utente per la connessione a MySQL
    $password = "admin"; //password per la connessione a MySQL
    $nomedb = "appweb"; //nome del DB MySQL
?>
```

conn_db.php

```
<?php
      include("config.php"); //includo file configurazione per recupero
variabili


    //connessione al Server tramite mysql_connect
    $conn = mysql_connect($nomehost,$nomeuser,$password) or die
("Impossibile connettersi al Server ...");


      //connessione al DB
      $db_selected=mysql_select_db($nomedb, $conn) or die ("Errore nella
selezione del database ...");
?>
```

verifica.php

```
      //includo i file necessari a collegarmi al db
      include("config.php");


      //mi collego al db
      include("conn_db.php");


      //variabili POST con anti sql Injection
      $username=mysql_real_escape_string($_POST['username']); //faccio
l'escape dei caratteri dannosi
      $password=mysql_real_escape_string(sha1($_POST['password']));
//sha1 cifra la password
```

```
      $query = "SELECT * FROM utenti WHERE username = '$username' AND
password = '$password' ";
      $ris = mysql_query($query, $conn) or die (mysql_error());
      $riga=mysql_fetch_array($ris);

      /*Prelevo l'identificativo dell'utente */
      $cod=$riga['username'];

      /* Effettuo il controllo */
      if ($cod == NULL) $trovato = 0 ;
      else $trovato = 1;

      /* Username e password corrette */
      if($trovato === 1) {
       /*Registro la sessione*/
       //funzione deprecata
        ///session_register('autorizzato');
        //come descritto in
        //http://php.net/manual/it/function.session-is-registered.php

        $_SESSION["autorizzato"] = 1;
        /*Registro il codice dell'utente ... poco sicuro salvare cod*/
        $_SESSION['cod'] = $cod;

       /*Redirect alla pagina riservata, per esempio profilo.php*/
         echo '<script
language=javascript>document.location.href="profilo.php"</script>';

      }
      else {

      /*Username e password errati, redirect alla pagina di login*/
```

```
      echo '<script
language=javascript>document.location.href="index.php"</script>';


     }
?>
```

profilo.php

```
<?php
        include("privato.php");
?>


<!DOCTYPE html>
<html>
<head>
    <title>Profilo</title>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-
8" />
</head>
<body>
        <h1>PROFILO</h1>
        <a href="registraNuovoUtente.php">Registra nuovo utente</a><br
/>
        <a href="logout.php">logout</a>
</body>
</html>
```

ricavoProfilo.php

```
<?php
        include("config.php");
        include("conn_db.php");
        $cod=$_SESSION['cod']; //username
        $query = "SELECT * FROM utenti WHERE username = '$cod' ";
        $ris = mysql_query($query, $conn) or die (mysql_error());
        $riga=mysql_fetch_array($ris);
```

```
?>
```

registraNuovoUtente.php

```
<!DOCTYPE html>
<html lang="it">
<head>
    <title>Registrazione nuovo utente</title>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-
8" />
</head>
<body>
        <h1>DATI UTENTE</h1>
        <form action="inserisciNuovoUtente.php" method="post">
        Nome: <input type="text" name="nome" size="30"
maxlength="30"><br />
        Cognome: <input type="text" name="cognome" size="30"
maxlength="30"><br />
        Username: <input type="text" name="username" size="20"
maxlength="20"><br />
        Password: <input type="password" name="password" size="20"
maxlength="20"><br />
        Email: <input type="text" name="email" size="20"
maxlength="30"><br />
        Ruolo:  <input type="radio" name="ruolo" value="finale"
/>Finale<br />
                <input type="radio" name="ruolo" value="collaboratore"
/>Collaboratore<br /><br />
        <input type="submit" value="REGISTRA">
        </form>
        <a href="logout.php">logout</a>
</body>
</html>
```

inserisciNuovoUtente.php

```
<?php
        include("privato.php");
```

```
    $nome = $_POST["nome"];
    $cognome = $_POST["cognome"];
    $username = $_POST["username"];
         $password = $_POST["password"];
         $password = sha1($password);
         $email = $_POST["email"];
         $ruolo = $_POST["ruolo"];
    //creo e salvo la query nella variabile stringa $query
    $query = "INSERT INTO utenti(nome, cognome, username, password,
email, ruolo)";
    $query .= "VALUES ('$nome', '$cognome', '$username', '$password',
'$email', '$ruolo')";
    $result = mysql_query($query) or die ("Error Query..."); //eseguo la
query
    echo("<br />" . "Utente aggiunto correttamente.");
    mysql_close($con); //chiudo la connessione
?>
```

CERCA.PHP CONTROLLA

```
<?php
    //http://it2.php.net/ (manuale)
    // parametri per la connessione al database
    $nomehost = "localhost"; //hostname
    $nomeuser = "root"; //nome utente per la connessione a MySQL
    $password = "admin"; //password per la connessione a MySQL
    $nomedb = "rubrica"; //nome delE database MySQL
    //connessione al Server tramite mysql_connect
    $con = mysql_connect($nomehost,$nomeuser,$password) or die
("Impossibile connettersi al Server ...");
    /*if (!$con) //$con==0
        die('Could not connect: ' . mysql_error());
    echo "You are connected to the Web Server!";
    */
```

```
    //connessione al DB

    mysql_select_db($nomedb, $con) or die ("Impossibile connettersi al DB
...");

    echo("<br />Access to DB" . $nomedb);

    $cognome = $_POST["cognome"]; //recupero il valore del parametro di
ricerca cognome passato con metodo POST

    //creo e salvo la query nella variabile stringa $query

    $query = "SELECT * FROM utenti WHERE Cognome = '$cognome'";

    echo $query . "<br /";

    $result = mysql_query($query) or die ("Error Query..."); //eseguo la
query

    $num_row = mysql_num_rows($result); //numero di righe restituite
dalla query

    $num_col = mysql_num_fields($result); //numero di campi restituiti
dalla query

    print("<br />" . "Numero di righe che corrispondono al criterio di
ricerca: " . $num_row);

    echo("<br />" . "Numero di campi restituiti dalla query: " .
$num_col);

    printf("<h2>Dati trovati</h2>");


    $irow = 0;

    while($row = mysql_fetch_array($result)) //carico in row una riga del
vettore associativo usando i nomi dei campi restituiti dalla query

    {

        $recordset[$irow] = $row; //salvo le righe nel oggetto (matrice)
recordset - tabella virtuale antropomorfa

        echo("<p>");

        echo("Cognome = " . $row["Cognome"]);

        echo(" - ");

        echo("Nome = ".$row["Nome"]);

        echo(" " . "-" . " ");

        echo("Tel = ".$row["Tel"]);

        echo("</p>");

        $irow++;

    }

    //visualizzazione tabellare dei dati
```

```
    echo("<table border=\"1\">");
    echo("<tr>");
    for($icol=0; $icol < $num_col; $icol++)
    {
        echo("<td>" . mysql_field_name($result, $icol) . "</td>");
    }
    echo("</tr>");
    for($irow=0; $irow < $num_row; $irow++)
    {
        echo("<tr>");
        for($icol=0; $icol < $num_col; $icol++)
        {
            echo("<td>" . $recordset[$irow][$icol] . "</td>");
        }
        echo("</tr>");
    }
    echo("</table>");
    mysql_close($con); //chiudo la connessione
?>
```