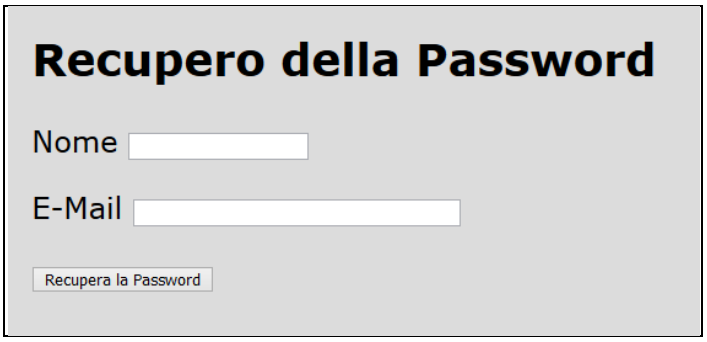
31. Il recupero della password

E’ utile prevedere anche la possibilità per l’utente di recuperare la password nel caso in cui non riesca più a ricordarla.

Una possibilità è quella di chiedere all’utente di rispondere ad una o più domande segrete per poter poi ricevere, tramite mail, la password che si aveva dimenticato oppure una nuova password temporanea generata automaticamente dal sistema. Le domande segrete e le relative risposte devono essere preventivamente acquisite dall’utente in fase di registrazione dello stesso; si tratta di domande del tipo “qual è il cognome da nubile di tua mamma?”.

Se non sono state previste domande segrete da porre all’utente, per recuperare la password l’utente dovrà semplicemente specificare la mail che ha usato in fase di registrazione. Questa mail verrà utilizzata come canale sicuro per ricevere la password.



Il form della pagina per il recupero della password

A questo punto il sistema potrà inviare direttamente all’utente la password memorizzata in chiaro nel database.

Qualora, invece, nel database vi fosse memorizzata l’impronta hash della password, ovvero **md5($password)**, risulta necessario generare una nuova password, in quanto quella originaria non risulta recuperabile.

Per evitare azioni indesiderate di estranei, il sistema, prima di generare una nuova password, invia all’utente una mail per chiedergli di confermare le intenzioni di rigenerare la password.

Questa mail conterrà un link che attiverà la funzione di rigenerazione della password e il conseguente suo invio alla mail dell'utente.

Da: xxxxx@tiscali.it <Admin>
A: pippo@gmail.com
Oggetto: Conferma richiesta di recupero password
sab 15 dic 2018 01:14

clicca sul seguente link per confermare la richiesta di recupero della password

La mail inviata all'utente per confermare
la richiesta di recupero della password

Il link di attivazione della suddetta funzione deve riportare anche l'impronta hash della vecchia password, per evitare che chiunque possa attivare tale funzione:

```
site_url("go/rigeneraPassword/$nome/".urlencode($email)."/$hash")
```

se ad esempio si hanno i seguenti valori:

```
$nome = 'alfa'

$email = 'alfa@tiscali.it'

$password = 'alfa'

md5($password) =  '7bd5c568f0f11d49a1527478c148cbcd'
```

si ottiene il seguente url

```
http://www.azienda.it/bici/index.php/go/rigeneraPassword/alfa/alfa%40tiscali.it/7bd5c568f0f11d49a1527478c148cbcd
```

La funzione urlencode() viene usata per produrre url validi, sostituendo i caratteri non alfabetici con codici numerici esadecimali di due cifre.
Gli spazi vengono sostituiti dal simbolo +.
In particolare il simbolo @ corrisponde a %40

La nuova password viene generata dal sistema e inviata all'utente tramite mail. Il sistema prontamente ne memorizza l'impronta hash (md5) nel database.

Da: xxxxx@tiscali.it <Admin>
A: pippo@gmail.com
Oggetto: Invio nuova password
sab 15 dic 2018 01:20

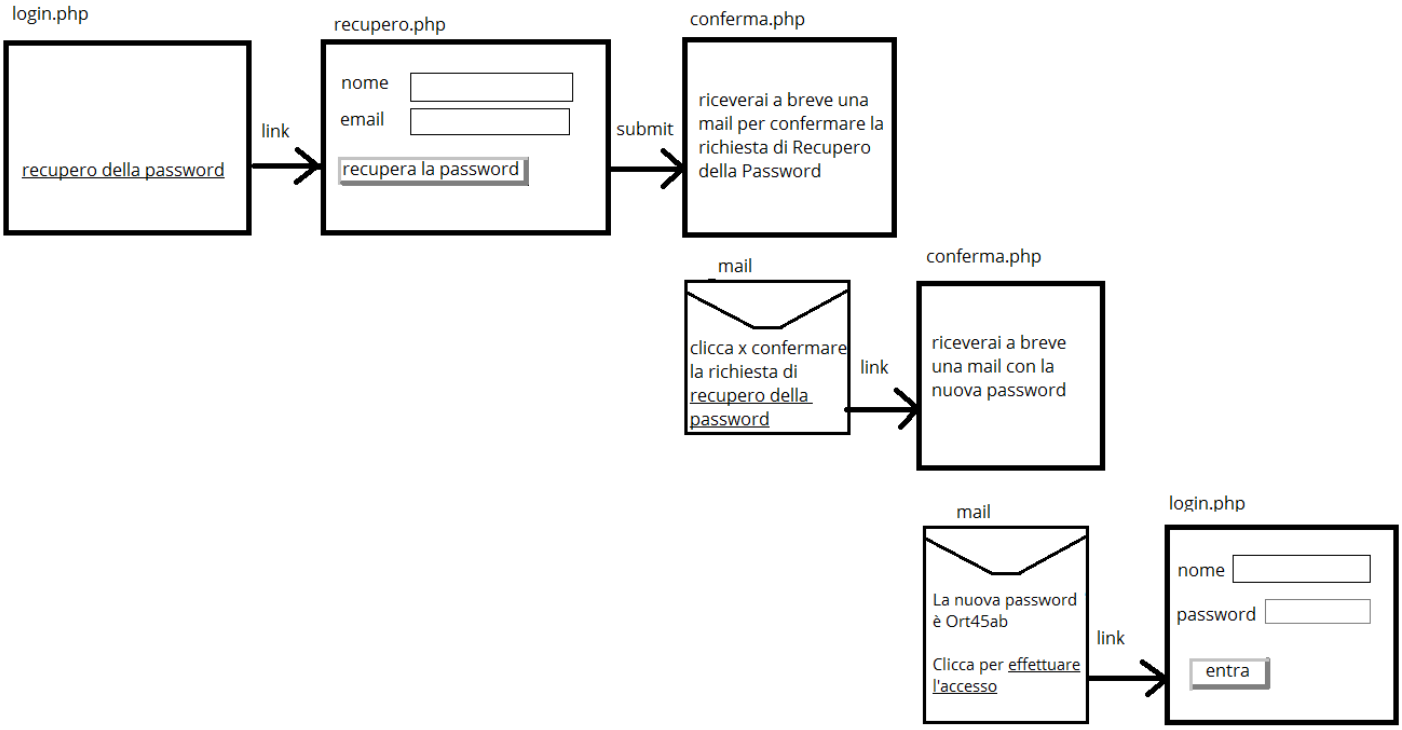
La nuova password è Ort45ab
Clicca sul seguente link per effettuare l'accesso

La mail con la nuova password

Il link per effettuare l'accesso è `site_url('go/entra')`

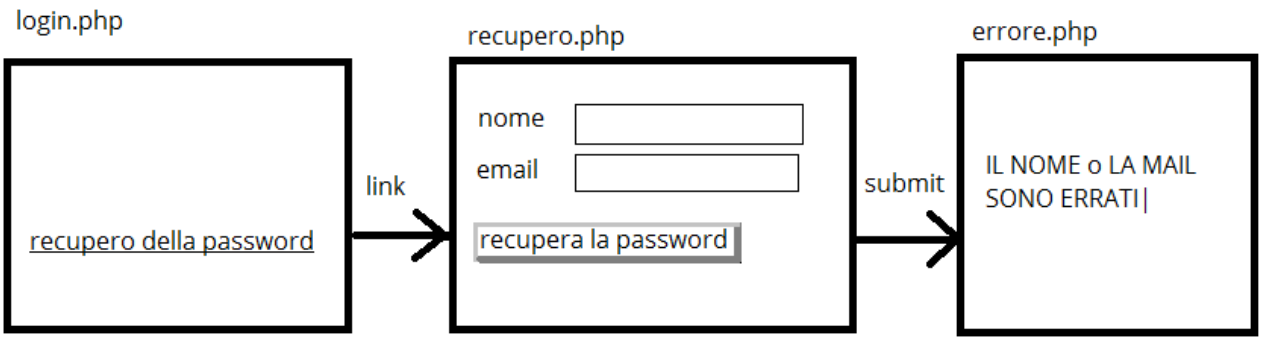
ovvero `http://www.azienda.it/bici/index.php/go/entra`

In definitiva lo storyboard del caso d'uso "Recupera la password" è il seguente:



Scenario principale del caso d'uso "Recupera la password"

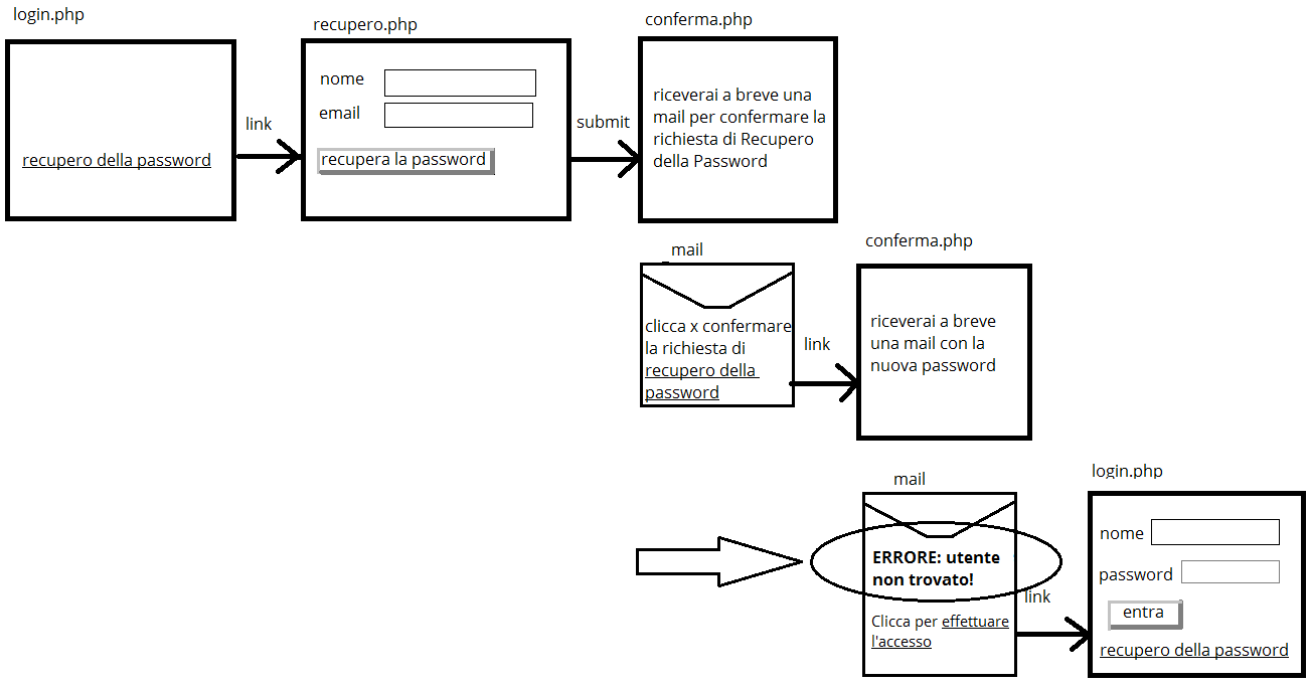
C'è uno scenario alternativo che comporta la visualizzazione di una pagina con un messaggio di errore nel caso di inserimento di credenziali errate (nome e mail) nel form della pagina recupero.php:



Scenario alternativo con credenziali errate

e un altro scenario alternativo nel caso di problemi nell'accesso al database o nelle credenziali inserite nel link presente nella mail.

In particolare, se vengono contraffatte le credenziali inserite nel link della mail di conferma si ottiene il seguente scenario:



Vedi anche http://www.manuelmarangoni.it/sir-bit/678/php-creare-uno-strumento-sicuro-per-il-recupero-della-password-dell'utente-esempio-completo/.

Per quanto riguarda il codice delle pagine della vista utilizzate, nella pagina login.php viene inserito il link per attivare la funzione richiestaRecuperoPassword(), che si occuperà di visualizzare il form presentato dalla pagina recupero.php:

login.php

```
....
<p>
Se non ricordi la password puoi effettuare il
<?= anchor('go/richiestaRecuperoPassword', 'recupero della password') ?>
</p>
....
```

La pagina che realizza il form per il recupero della password è il seguente:

recupero.php

```
<main>
<?= form_open('go/recuperaPassword') ?>
<p> Nome  <input type="text" name="nome"></p>
<p> EMail  <input type="text" name="email"></p>
<p> <input type="submit" name="submit" value="Recupera la Password"></p>
</form>
</main>
```

La pagina di errore e quella di conferma mostrano all'utente appositi messaggi:

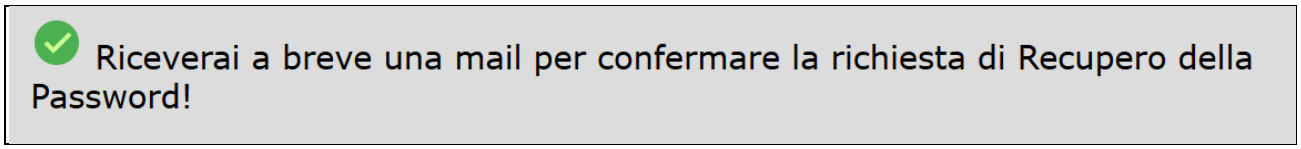
errore.php

```
<main>
<p id="errore"> <?= img('images/icona-errore.png') ?> <?= $messaggio ?>
</p>
</main>
```

Messaggio di errore per credenziali di recupero errate

conferma.php

```
<main>
<p id="messaggio"> <?= img('images/icona-ok.png') ?> <?= $messaggio ?>
</p>
</main>
```



Messaggio di conferma

Il Controller conterrà:

- la funzione richiestaRecuperoPassword() per visualizzare la pagina del form di richiesta
- la funzione recuperaPassword() per inviare all'utente la mail con il link per confermare la richiesta di rigenerazione della password
- la funzione rigeneraPassword() per rigenerare la password, memorizzarla nel database ed inviare all'utente la mail con la nuova password

Go.php

```
public function richiestaRecuperoPassword()
{
        $this->load->view('header');
        $this->load->view('recupero');
        $this->load->view('footer');
}


public function recuperaPassword()
{
   // acquisizione degli input dal form
   $nome = $this->input->post('nome');
   $email = $this->input->post('email');
   // leggo nel database i dati dell'utente, in particolare
   // mi interessa la sua password
   $utente = $this->negozio_model->get_password($nome, $email);
   if (isset($utente))
   {
     // scenario principale
```

```
     $hash = $utente->hash; // uso una variabile di appoggio
     // invio una mail per chiedere conferma
     $this->email->from('xxxxxx@tiscali.it','Admin');
     $this->email->to($email);
     $this->email->subject('Conferma richiesta di recupero password');
     $testo = '<p>clicca sul seguente link per <a href="'.
     site_url("go/rigeneraPassword/$nome/".urlencode($email)."/$hash").
     '">'.   // con urlencode() si va a sostituire @ con %40
     'confermare la richiesta di recupero della password</a></p>';
     $this->email->message($testo);
     $this->email->send();
     // debug
     //if ($this->email->send()) {
     //   echo 'Your email was sent';
     //   }
     //   else {
     //   //show_error($this->email->print_debugger(array('headers')));
     //   show_error($this->email->print_debugger());
     //}
     // fine debug

     $data['messaggio'] = 'Riceverai a breve una mail per confermare la
                           richiesta di Recupero della Password!';
     $this->load->view('header');
     $this->load->view('conferma', $data);
     $this->load->view('footer');
   }
   else  // scenario alternativo: dati errati
   {
     $data['messaggio'] = 'IL NOME o LA EMAIL SONO ERRATI!';
     $this->load->view('header');
     $this->load->view('errore', $data);
     $this->load->view('footer');
   }
}


public function rigeneraPassword($nome, $email, $hash)
{
    $email = urldecode($email);  // sostituisce %40 con @
    $messaggio = $this->negozio_model->genera_nuova_password($nome,
                 $email, $hash);
    // invio una mail con il messaggio contenente la nuova password
    // oppure un messaggio di errore
    $this->email->from('xxxxx@tiscali.it', 'Admin');
    $this->email->to($email);
    $this->email->subject('Invio nuova password');
    $testo = '<p>'.$messaggio.'</p><p>Clicca sul seguente link per '.
             '<a href="'. site_url('go/entra'). '">'.
             'effettuare l\'accesso</a></p>';
```

```
    $this->email->message($testo);
    $this->email->send();
    // debug
    //if ($this->email->send())
    //{
    //    echo 'Your email was sent';
    //}
    //else
    //{
    // //show_error($this->email->print_debugger(array('headers')));
    //   show_error($this->email->print_debugger());
    //}
    // fine debug
    $data['messaggio'] = 'Riceverai a breve una mail con la nuova
                          password!';
    $this->load->view('header');
    $this->load->view('conferma', $data);
    $this->load->view('footer');
}
```

Le funzioni che vengono aggiunte al modello sono

- get_password() che consente di recuperare i dati dell'utente dati il suo nome e la sua mail
- random() che genera una stringa casuale da usare come password temporanea
- genera_nuova_password() che dopo aver fatto generare la nuova password ne memorizza l'impronta hash nella tabella utenti del database

negozio.utenti: 7 righe totali

nome	password	ruolo	email	confermato	hash
admin	admin	admin	admin@negozio.it	si	21232F297A57A5A743894A0E4A801FC3
alfa	mu66rkk2	utente	alfa@tiscali.it	si	7bd5c568f0f11d49a1527478c148cbcd
elena	elena	utente	elena@tiscali.it	si	FADF17141F3F9C3389D10D09DB99F757
gianni	gianni	utente	gianni@libero.it	si	1BC42179CC24BCC5EEFF1B1B2D03657C
pietro	pietro	utente	pietro@yahoo.it	no	7189DFEAC32CEA348F25D63EB1F07276
pippo	pippo	utente	pippo@gmail.com	si	0C88028BF3AA6A6A143ED846F2BE1EA4
pollo	gqjeOvZJ	utente	admin@azienda.it	si	7bc376ed3680781350096b0b02f15e989

La tabella utenti – è preferibile evitare di memorizzare la password in chiaro e registrarne solo l'impronta hash

Il codice del modello è il seguente:

Negozio_model.php

```
// funzione usata per il recupero della password
public function get_password($nome, $email)
{
   $query = $this->db->query("select *
                         from utenti
                         where nome = ? and email = ?",
                         array($nome, $email));
   return $query->row();  // oggetto o null
}


// funzione di servizio per generare una password casuale
// della lunghezza specificata
private function random($lunghezza)
{
 $caratteri = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz1234567890";
 $stringa = "";
 for($i=0; $i<$lunghezza; $i++)
 {
   $stringa = $stringa. substr($caratteri, rand(0,strlen($caratteri)-1), 1);
 }
 return $stringa;
}


// effettua la generazione di una nuova password e la registra nel database
public function genera_nuova_password($nome, $email, $hash)
{
     $messaggio = '';
     $nuovaPassword = $this->random(8);  // di 8 caratteri
     $nuovoHash = md5($nuovaPassword);
     $sql = 'update utenti
             set password = ?, hash = ?
             where nome = ? and email = ? and hash = ?';
     $this->db->query($sql, array($nuovaPassword, $nuovoHash, $nome, $email,
                                  $hash));
     $e = $this->db->error();  // array 'code' 'message'
     if ($e['code'] != 0)
     {
        $messaggio = 'ERRORE: '. $e['message'];
     }
     else if ($this->db->affected_rows() == 0)
     {
        $messaggio = 'ERRORE: utente non trovato!';
     }
     else
     {
        $messaggio = "La nuova password è " . $nuovaPassword;
```

```
        }
        return $messaggio;
}
```