```php
<?php
session_start();
$db = new PDO("mysql:host=127.0.0.1;dbname=db00;charset=utf8", "root", "", null);

//如果還沒有身分，則指定身分為guest
if (empty($_SESSION['user'])) $_SESSION['user'] = "guest";

//如果do不是空的，開始進行事件類別之處理作業
if (!empty($_GET['do'])) switch ($_GET['do']) {
  case 'login':
    if ($_POST['ans'] != $_SESSION['rand']) echo '<script>alert("驗證碼錯誤！");location.href="index.php";</script>';
    elseif ($_POST['user'] == "admin" && $_POST['pwd'] == "1234") {
      $_SESSION['user'] = "admin";
      echo '<script>alert("歡迎管理者！");location.href="admin.php";</script>';
    } else {
      $sql = "SELECT * FROM msg WHERE user='" . $_POST['user'] . "' AND mail='" . $_POST['pwd'] . "'";
      $rows = $db->query($sql)->fetchAll();

      //如果有找到資料對象代表用戶存在
      if ($rows) {
        $_SESSION['user'] = $_POST['user'];
        $_SESSION['mail'] = $_POST['pwd'];
        echo '<script>alert("歡迎' . $_POST['user'] . '！");location.href="admin.php";</script>';
      }
      //反之，帳號不在資料表內
      else echo '<script>alert("查無此號！");location.href="index.php";</script>';
    }
    break;
  case 'logout':
    //刪除身分別
    unset($_SESSION['user']);
    echo '<script>alert("登出成功");location.href="index.php";</script>';
    break;
  case 'msgadd':
    //將表單資料轉換SQL之新增語法，且執行到資料庫
    $sql = "INSERT INTO `msg`(`id`, `user`, `info`, `mail`, `tel`, `date`, `del`) VALUES (null,'" . $_POST['user'] . "','" . $_POST['info'] . "','" . $_POST['mail'] . "','" . $_POST['tel'] . "',NOW(),0)";
    $db->query($sql);
    echo '<script>alert("留言完成");location.href="index.php";</script>';
    break;
  case 'msgmdy':
    echo $sql = "UPDATE `msg` SET `user`='" . $_POST['user'] . "',`info`='" . $_POST['info'] . "',`mail`='" . $_POST['mail'] . "',`tel`='" . $_POST['tel'] . "',`date`=NOW() WHERE id=" . $_POST['id'] . "";
    $db->query($sql);
    echo '<script>alert("修改完成");location.href="admin.php";</script>';
    break;
  case 'msgdel':
    echo $sql = "UPDATE `msg` SET del=1 WHERE id=" . $_GET['id'] . "";
    $db->query($sql);
    echo '<script>alert("刪除完成");location.href="admin.php";</script>';
    break;
  case 'pkadd':
    $newname = time() . "_" . $_FILES['img']['name'];
    copy($_FILES['img']['tmp_name'], "img/" . $newname);
```

```php
    $sql = "INSERT INTO `pk`(`id`, `user`, `info`, `mail`, `tel`, `date`, `del`) VALUES (null,'" . $_POST['user'] . "','" . $newname . "','" . $_POST['mail'] . "','" . $_POST['tel'] . "',NOW(),0)";
    $db->query($sql);
    echo '<script>alert("報名成功");location.href="index.php";</script>';
    break;
}
```