```php
<?

Class Auth {

    function doLogin() {

        if (!$_SESSION['user']) {

            $oid = mysql_query("SELECT *
                                  FROM utente
                                 WHERE username = '{$_POST['username']}'
                                   AND password =
MD5('{$_POST['password']}')");

            if (!$oid) {
                echo "Error in database!<hr>";
                echo mysql_error();
                    exit;
            }
            if (mysql_num_rows($oid) == 0) {
                Header("Location: error.php?id=1");
                exit;

            } else {

                $_SESSION['user'] = mysql_fetch_assoc($oid);

                $oid = mysql_query("SELECT utente.username,
                                           gruppo.nome,
                                           servizio.script,
                                           servizio.tableName,
                                           servizio.keyName,
                                           servizio.paramName
                                      FROM utente
                                 LEFT JOIN utente_gruppo
                                        ON utente_gruppo.id_utente =
utente.username
                                 LEFT JOIN gruppo
                                        ON gruppo.id =
utente_gruppo.id_gruppo
                                 LEFT JOIN gruppo_servizio
                                        ON gruppo_servizio.id_gruppo =
gruppo.id
                                 LEFT JOIN servizio
                                        ON servizio.id =
gruppo_servizio.id_servizio
                                     WHERE utente.username =
'{$_SESSION['user']['username']}'");
                if (!$oid) {
                    echo "Error in database! (services)";
                    exit;
```

```
46                  }
47
48                  do {
49                      $data = mysql_fetch_assoc($oid);
50                      if ($data) {
51                          $_SESSION['user']['services'][] = $data;
52
53                      }
54
55                  } while ($data);
56              }
57          }
58
59          $trovato = false;
60          foreach ($_SESSION['user']['services'] as $k => $v) {
61              if ($v['script'] == basename($_SERVER['SCRIPT_NAME'])) {
62                  $trovato = true;
63                  $currentService = $v;
64              }
65          }
66
67          if (!$trovato) {
68              Header("Location: error.php?id=2");
69              exit;
70          }
71
72          if ($currentService['tableName']) { // Data Filtering Check
73
74              $oid = mysql_query("SELECT username
75                                    FROM {$currentService['tableName']}
76                                   WHERE {$currentService['keyName']} =
    '".addslashes($_REQUEST[$currentService['paramName']])."'");
77              if (!$oid) {
78                  echo "Error in database! (df)";
79                  exit;
80              }
81
82              $data = mysql_fetch_assoc($oid);
83
84              if ($data['username'] != $_SESSION['user']['username']) {
85
86                  Header("Location: error.php?id=3");
87                  exit;
88              }
89
90          }
91
92      }
93
94
95  }
```

```
96
97
98  Auth::doLogin();
99
100 ?>
```