

```

1  <?
2
3  session_start();
4
5  require "include/template.inc.php";
6  require "include/dbms.inc.php";
7  require "include/functions.inc.php";
8  require "include/auth.inc.php";
9
10 define(UPLOAD_DESTINATION_DIR,"upload/");
11
12 $main = new Template("dtml/cms_layout.html");
13 $menu = new Template("dtml/cms_menu_admin.html");
14 $content = new Template("dtml/cms_form_file.html");
15 $main->setContent("utente", getResult("SELECT nome,cognome FROM utente
16 WHERE username = '{$_SESSION['user']['username']}'"));
17 $main->setContent("username", $_SESSION['user']['username']);
18 $menu->setContent("pubblicati", getResult("SELECT * FROM contenuto
19 WHERE (pubblicato = 'Y') AND (username =
20 '{$_SESSION['user']['username']}'"));
21 $menu->setContent("bozze", getResult("SELECT * FROM contenuto WHERE
22 (pubblicato = 'N') AND (username =
23 '{$_SESSION['user']['username']}'"));
24 $menu->setContent("presenti", getResult("SELECT * FROM sezione"));
25 $menu->setContent("segnalati", getResult("SELECT * FROM link"));
26 $menu->setContent("archivio", getResult("SELECT * FROM file WHERE
27 username = '{$_SESSION['user']['username']}'"));
28 $main->setContent("menu", $menu->get() );
29
30 switch ($_REQUEST['page']) {
31     case 0:
32         $main->setContent("content", $content->get() );
33         break;
34     case 1:
35         /* UPLOAD FILE */
36         $message = "&nbsp;&nbsp;&nbsp;&nbsp;&File caricato con successo.";
37         $esito = "ok";
38         $type = explode("/",$_FILES['userfile']['type']);
39         do {
40             /* Controllo tipo file */
41             if (!is_uploadable_file($_FILES['userfile']['type'])) {
42                 $message = "&nbsp;&nbsp;&nbsp;&Tipo di file non accettato.";
43                 $esito = "ko";
44                 break;
45             }
46
47             /* Controllo dimensioni file */
48             /* IMMAGINI */
49             if (($_FILES['userfile']['size'] > 409600) && ($type[0] ==
50 "image")) {
51                 $message = "&nbsp;&nbsp;&L'immagine ha dimensioni

```

```

45     maggiori di quelle consentite (400 KB).";
46         $esito = "ko";
47         break;
48     }
49     /* DOCUMENTI RICH TEXT */
50     if (($FILES['userfile']['size'] > 2097152) && ($type[0] ==
"application")) {
51         $message = "&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&Il documento ha dimensioni
maggiori di quelle consentite (2 MB).";
52         $esito = "ko";
53         break;
54     }
55
56     /* DOCUMENTI PLAIN/HTML */
57     if (($FILES['userfile']['size'] > 524288) && ($type[0] ==
"text")) {
58         $message = "&nbsp;&nbsp;&nbsp;&nbsp;&Il file ha dimensioni maggiori
di quelle consentite (500 KB).";
59         $esito = "ko";
60         break;
61     }
62
63     if (!move_uploaded_file($FILES['userfile']['tmp_name'],
UPLOAD_DESTINATION_DIR.$FILES['userfile']['name'])) {
64         $message = "&nbsp;&nbsp;&nbsp;&nbsp;&File non caricato.";
65         $esito = "ko";
66         break;
67     }
68
69     /* MEMORIZZAZIONE NEL DATABASE. */
70     $oid = mysql_query("INSERT INTO file
71         VALUES ('{$SESSION['user']['username']}',
72         '".addslashes($FILES['userfile']['name'])."',
73         'upload/',
74         '{$FILES['userfile']['type']}',
75         '{$FILES['userfile']['size']}',
76         '{$REQUEST['descrizione']}',
77         '".date('H:i:s')."',
78         '".date('Y-m-d')."'");
79     if (!$oid) {
80         $message = "&nbsp;&nbsp;&nbsp;&nbsp;&File non caricato.";
81         $esito = "ko";
82         break;
83     }
84     } while (false);
85
86     $main = new Template("dtml/cms_layout.html");
87     $menu = new Template("dtml/cms_menu_admin.html");
88     $content = new Template("dtml/cms_form_file.html");

```

```

89     $main->setContent("utente", getResult("SELECT nome,cognome FROM
utente WHERE username = '{$_SESSION['user']['username']}'"));
90     $main->setContent("username", $_SESSION['user']['username']);
91     $menu->setContent("pubblicati", getResult("SELECT * FROM
contenuto WHERE (pubblicato = 'Y') AND (username =
'{$_SESSION['user']['username']}'"));
92     $menu->setContent("bozze", getResult("SELECT * FROM contenuto
WHERE (pubblicato = 'N') AND (username =
'{$_SESSION['user']['username']}'"));
93     $menu->setContent("presenti", getResult("SELECT * FROM
sezione"));
94     $menu->setContent("segnalati", getResult("SELECT * FROM
link"));
95     $menu->setContent("archivio", getResult("SELECT * FROM file
WHERE username = '{$_SESSION['user']['username']}'"));
96     $main->setContent("menu", $menu->get() );
97     $content->setContent("message", $message, "esito=\"$esito\"");
98     $main->setContent("content", $content->get() );
99     break;
100 }
101
102 $main->close();
103
104 ?>

```