```php
1   <?
2
3   session_start();
4
5   require "include/template.inc.php";
6   require "include/dbms.inc.php";
7   require "include/auth.inc.php";
8   require "include/functions.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_contenuto_html.html");
15  $main->setContent("utente", getResult("SELECT nome,cognome FROM utente
    WHERE username = '{$_SESSION['user']['username']}'"));
16  $main->setContent("username", $_SESSION['user']['username']);
17  $menu->setContent("pubblicati", getResult("SELECT * FROM contenuto
    WHERE (pubblicato = 'Y') AND (username =
    '{$_SESSION['user']['username']}')"));
18  $menu->setContent("bozze", getResult("SELECT * FROM contenuto WHERE
    (pubblicato = 'N') AND (username =
    '{$_SESSION['user']['username']}')"));
19  $menu->setContent("presenti", getResult("SELECT * FROM sezione"));
20  $menu->setContent("segnalati", getResult("SELECT * FROM link"));
21  $menu->setContent("archivio", getResult("SELECT * FROM file WHERE
    username = '{$_SESSION['user']['username']}'"));
22  $main->setContent("menu", $menu->get() );
23  $content->setContent("sezioni", getResult("SELECT id,nome FROM sezione
    ORDER BY nome"));
24
25  // Contenuto
26
27  switch($_REQUEST['page']) {
28      case 0:
29          $main->setContent("content", $content->get() );
30          break;
31      case 1:
32
33          foreach ($_REQUEST as $k=>$value) {
34              $_REQUEST[$k] = addslashes($value);
35          }
36
37          $message = "  Articolo inserito con successo.";
38          $esito = "ok";
39          do {
40
41              if($_FILES['userfile']['type'] != "text/html") {
42                  $message = "  Tipo file non accettato";
43                  $esito = "ko";
44                  break;
```

```php
45                    }
46
47            if($_FILES['userfile']['size'] > 204800) {
48                    $message = "  Il file supera le dimensioni
consentite. (Max 200 KB)";
49                    $esito = "ko";
50                    break;
51            }
52
53            if(!move_uploaded_file($_FILES['userfile']['tmp_name'],
UPLOAD_DESTINATION_DIR.$_FILES['userfile']['name'])) {
54                    $message = "  File non caricato.";
55                    $esito = "ko";
56                    break;
57            }
58
59            $subsections = explode("|", $_REQUEST['sezioni']);
60
61            $today = date('Y-m-d');
62            $now = date('H:i:s');
63
64            $fid = mysql_query("INSERT INTO file
65                            VALUES ('{$_SESSION['user']['username']}',
66
'".addslashes($_FILES['userfile']['name'])."',
67                                    '".UPLOAD_DESTINATION_DIR."',
68                                    '{$_FILES['userfile']['type']}',
69                                    '{$_FILES['userfile']['size']}',
70                                    '{$_REQUEST['descrizione']}',
71                                    '".date('H:i:s')."',
72                                    '".date('Y-m-d')."')");
73
74            if (!$fid) {
75                    $message = "  File non caricato." .
mysql_error();
76                    $esito = "ko";
77                    break;
78            }
79
80            /* Estrazione dell'HTML dal file */
81            $testo =
extract_html(UPLOAD_DESTINATION_DIR.$_FILES['userfile']['name']);
82            $testo = ($_REQUEST['note'] != '' ? $testo . "<br>" .
$_REQUEST['note'] : $testo);
83
84            $oid = mysql_query("INSERT INTO contenuto
85                                    VALUES (NULL,
86
'{$_SESSION['user']['username']}',
87                                            '{$_REQUEST['titolo']}',
88                                            '{$testo}',
```

```php
89                                              '{$now}',
90                                              '{$today}',
91                                              '{$now}',
92                                              '{$today}',
93
    '{$_REQUEST['pubblicato']}',
94                                              1)");
95
96              if (!$oid) {
97                  $message = "  Articolo non inserito." .
    mysql_error();
98                  $esito = "ko";
99                  break;
100             }
101
102             $hid = mysql_query("SELECT id FROM contenuto
103                                 WHERE (titolo =
    '{$_REQUEST['titolo']}')
104                                 AND (ora_creazione = '$now')
105                                 AND (data_creazione = '$today')");
106
107             $aux = mysql_fetch_assoc($hid);
108
109             /* Inserimento SOTTOSEZIONI */
110             foreach ($subsections as $key => $value) {
111                 $suid = mysql_query("INSERT INTO contenuto_sottosezione
112                                      VALUES ({$aux['id']},
    {$value}) ");
113             }
114
115             $cfid = mysql_query("INSERT INTO contenuto_file VALUES
    ({$aux['id']},'{$_FILES['userfile']['name']}')");
116
117         } while(false);
118
119         if($esito == "ok") {
120             $main = new Template("dtml/cms_layout.html");
121             $main->setContent("utente", getResult("SELECT nome,cognome
    FROM utente WHERE username = '{$_SESSION['user']['username']}'"));
122             $main->setContent("username",
    $_SESSION['user']['username']);
123             $menu = new Template("dtml/cms_menu_admin.html");
124             $content = new Template("dtml/cms_form_contenuto.html");
125             $menu->setContent("pubblicati", getResult("SELECT * FROM
    contenuto WHERE (pubblicato = 'Y') AND (username =
    '{$_SESSION['user']['username']}')"));
126             $menu->setContent("bozze", getResult("SELECT * FROM
    contenuto WHERE (pubblicato = 'N') AND (username =
    '{$_SESSION['user']['username']}')"));
127             $menu->setContent("presenti", getResult("SELECT * FROM
    sezione"));
```

```php
128            $menu->setContent("segnalati", getResult("SELECT * FROM
    link"));
129            $menu->setContent("archivio", getResult("SELECT * FROM file
    WHERE username = '{$_SESSION['user']['username']}'"));
130            $main->setContent("menu", $menu->get() );
131            $content->setContent("sezioni", getResult("SELECT id,nome
    FROM sezione ORDER BY nome"));
132            $content->setContent("message", $message,
    "esito=\"$esito\"");
133        } else {
134            $content->setContent("message", $message,
    "esito=\"$esito\"");
135        }
136
137        $main->setContent("content", $content->get() );
138        break;
139 }
140
141 $main->close();
142
143 ?>
```