```
<?

session_start();

require "include/template.inc.php";
require "include/dbms.inc.php";
require "include/functions.inc.php";
require "include/auth.inc.php";

define(UPLOAD_DESTINATION_DIR,"upload/");

$main = new Template("dtml/cms_layout.html");
$menu = new Template("dtml/cms_menu_admin.html");
$content = new Template("dtml/cms_form_file.html");
$main->setContent("utente", getResult("SELECT nome,cognome FROM utente WHERE username = '{$_SESSION['user']['username']}'"));
$main->setContent("username", $_SESSION['user']['username']);
$menu->setContent("pubblicati", getResult("SELECT * FROM contenuto WHERE (pubblicato = 'Y') AND (username = '{$_SESSION['user']['username']}')"));
$menu->setContent("bozze", getResult("SELECT * FROM contenuto WHERE (pubblicato = 'N') AND (username = '{$_SESSION['user']['username']}')"));
$menu->setContent("presenti", getResult("SELECT * FROM sezione"));
$menu->setContent("segnalati", getResult("SELECT * FROM link"));
$menu->setContent("archivio", getResult("SELECT * FROM file WHERE username = '{$_SESSION['user']['username']}'"));
$main->setContent("menu", $menu->get() );

switch ($_REQUEST['page']) {
    case 0:
        $main->setContent("content", $content->get() );
        break;
    case 1:
        /* UPLOAD FILE */
        $message = "&nbsp;&nbsp;File caricato con successo.";
        $esito = "ok";
        $type = explode("/",$_FILES['userfile']['type']);
        do {
                /* Controllo tipo file */
            if (!is_uploadable_file($_FILES['userfile']['type'])) {
                $message = "&nbsp;&nbsp;Tipo di file non accettato.";
                $esito = "ko";
                break;
            }

            /* Controllo dimensioni file */
            /* IMMAGINI */
            if (($_FILES['userfile']['size'] > 409600) && ($type[0] == "image")) {
                $message = "&nbsp;&nbsp;L'immagine ha dimensioni
maggiori di quelle consentite (400 KB).";
                $esito = "ko";
                break;
            }

            /* DOCUMENTI RICH TEXT */
            if (($_FILES['userfile']['size'] > 2097152) && ($type[0] == "application")) {
                $message = "&nbsp;&nbsp;Il documento ha dimensioni maggiori di quelle consentite (2 MB).";
                $esito = "ko";
                break;
            }

            /* DOCUMENTI PLAIN/HTML */
            if (($_FILES['userfile']['size'] > 524288) && ($type[0] == "text")) {
                $message = "&nbsp;&nbsp;Il file ha dimensioni maggiori di quelle consentite (500 KB).";
                $esito = "ko";
                break;
            }

            if(!move_uploaded_file($_FILES['userfile']['tmp_name'], UPLOAD_DESTINATION_DIR.$_FILES['userfile']['name'])) {
                $message = "&nbsp;&nbsp;File non caricato.";
                $esito = "ko";
                break;
            }

            /* MEMORIZZAZIONE NEL DATABASE. */
            $oid = mysql_query("INSERT INTO file
                             VALUES ('{$_SESSION['user']['username']}',
                                     '".addslashes($_FILES['userfile']['name'])."',
                                     'upload/',
                                     '{$_FILES['userfile']['type']}',
                                     '{$_FILES['userfile']['size']}',
                                     '{$_REQUEST['descrizione']}',
                                     '".date('H:i:s')."',
                                     '".date('Y-m-d')."')");
            if (!$oid) {
                $message = "&nbsp;&nbsp;File non caricato.";
                $esito = "ko";
                break;
            }
        } while (false);

        $main = new Template("dtml/cms_layout.html");
        $menu = new Template("dtml/cms_menu_admin.html");
        $content = new Template("dtml/cms_form_file.html");
```

```php
        $main->setContent("utente", getResult("SELECT nome,cognome FROM utente WHERE username = '{$_SESSION['user']['username']}'"));
        $main->setContent("username", $_SESSION['user']['username']);
        $menu->setContent("pubblicati", getResult("SELECT * FROM contenuto WHERE (pubblicato = 'Y') AND (username = '{$_SESSION['user']['username']}')"));
        $menu->setContent("bozze", getResult("SELECT * FROM contenuto WHERE (pubblicato = 'N') AND (username = '{$_SESSION['user']['username']}')"));
        $menu->setContent("presenti", getResult("SELECT * FROM sezione"));
        $menu->setContent("segnalati", getResult("SELECT * FROM link"));
        $menu->setContent("archivio", getResult("SELECT * FROM file WHERE username = '{$_SESSION['user']['username']}'"));
        $main->setContent("menu", $menu->get() );
        $content->setContent("message", $message, "esito=\"$esito\"");
        $main->setContent("content", $content->get() );
        break;
}

$main->close();

?>
```