

**11. include() II.,
UPDATE II.,
uploadovanie súborov**

1.5.2006

Obsah

- Možné problémy pri vkladni súborov
- Dodatok ku UPDATE
- Uploadovanie súborov

Problémy pri include()

Majme nasledujúci kód, ktorý očakáva súbor ako parameter:

```
if ($_GET['str'] == "")
    include('home.htm');
else
    include($_GET['str']);
```

V čom je problém?

- Ak zadáme parameter **index.htm**, tak je všetko v poriadku.
- Ale ak zadáme napr. parameter http://zlyserver.sk/sko_dlivykod.php, tak kód na inom serveri nám môže spôsobiť problémy.

include() – možné riešenia

- Ak očakávame na vstupe lokálny súbor, ale ho nekontrolujeme (vôbec alebo nedostatočne), môže byť náš skript zdrojom rôznych útokov.
- Jednou z kontrol môže byť napr.
`if (file_exists($_GET['str'] . '.php'))`
- Keby sme aj netestovali existenciu súboru, možno by stačilo len uvedenie priečinku, čím dáme jasne najavo, že hľadáme lokálny súbor.

Rozšírenie prihlasovania

- Pre každého používateľa budeme evidovať počet prihlásení.
- Vytvoríme stránku s možnosťou aktualizácie svojho "profilu" ([11-pouzivatel-01.php](#)). Zatiaľ len s pridávaním fotografie (budú v priečinku [fotky](#)).
- V tabuľke `skuska_pouzivatelia` pridáme 2 položky:
 - `pocet_prihl` – počet prihlásení používateľa
 - `foto` – názov súboru fotografie používateľa

UPDATE – dodatok

- Po každom úspešnom prihlásení chceme zvýšiť počet prihlásení daného používateľa (nová položka `pocet_prihl`).
- Aby sme nemuseli zisťovať aktuálnu hodnotu danej položky, môžeme využiť nasledujúci zápis, v ktorom uvedieme výraz na zvýšenie danej položky: `pocet_prihl=pocet_prihl+1`.
- Výsledný dotaz: `"UPDATE skuska_pouzivatelia SET pocet_prihl=pocet_prihl+1 WHERE prihlasmeno=" . $_POST['prihlasmeno'] . "' LIMIT 1"`

Uploadovanie súborov

- Robíme cez formulár **len metódou POST.**
- Musíme nastaviť typ kódovania údajov na **multipart/form-data.**
- Vložíme prvok formulára typu **file**
`<input type="file" name="xyz" />`
- Pri prvku typu **file** sa nám automaticky zobrazí tlačidlo na nájdenie súboru v našom počítači.

Formulár na uploadovanie

```
<form enctype="multipart/form-data"  
  action="subor.php" method="post">
```

```
<input type="hidden"  
  name="MAX_FILE_SIZE" value="max" />
```

```
<input type="file" name="obr" />
```

```
</form>
```

MAX_FILE_SIZE

- Vo formulári môžeme vytvoriť špeciálny skrytý prvok **MAX_FILE_SIZE**, v ktorom nastavíme maximálnu prípustnú veľkosť uploadovaného súboru (v **bytoch**).
- `<input type="hidden" name="MAX_FILE_SIZE" value="30000" />`
- Nemusí fungovať vo všetkých prehliadačoch – mal by fungovať v IE.
- Netreba sa na neho spoliehať.

Akceptované typy súborov

- Pri prvku typu **file** môžeme definovať atribút **accept**, ktorým definujeme akceptované typy súborov (viac typov oddeľujeme čiarkou).
- `<input type="file" accept="typ_súboru" name="obr" />`
- **Napr.** `<input type="file" accept="image/gif,image/jpeg" name="obr" />`
- Atribút **accept** nemusí fungovať vo všetkých prehliadačoch.

Čo sa deje po odoslaní formulára so súborom?

- Všetky klasické prvky formulára sa správajú ako doteraz, teda sú v poliach `$_POST`, resp. `$_GET`.
- **Uploadované súbory sa správajú inak.**
- Nie sú dostupné z polí `$_POST`, resp. `$_GET`, ale vytvorí sa pole `$_FILES['xyz']`, kde **xyz** je názov prvku typu `file` (`<input type="file" name="xyz"/>`).

Údaje po odeslání formulára

PHP Variables

Variable	Value
<code>_POST["MAX_FILE_SIZE"]</code>	30000
<code>_POST["submit"]</code>	Aktualizuj
<code>_FILES["obr"]</code>	<pre>Array ([name] => test1-obr_sachovnica.gif [type] => image/gif [tmp_name] => C:\WINDOWS\TEMP\php2A2.tmp [error] => 0 [size] => 1715)</pre>

Pole `$_FILES['xyz']`

- Je to asociatívne pole (dvojrozmerné) s presne definovanými prvkami (pozri ďalej).
- Existuje len počas behu skriptu.
- Po úspešnom uploade sa vytvorí dočasný súbor na serveri, ktorý treba presunúť na vhodné miesto. Po skončení skriptu sa dočasný súbor zmaže.

`$_FILES['xyz']` – prvky (1)

- `['name']` – meno pôvodného súboru s cestou
- `['tmp_name']` – dočasné meno súboru s cestou na strane servera
- `['type']` – mime type súboru (nastavené klientom – prehliadačom). Napr. Windows nepoznajú formát ogg tak mime nenastavia. PHP to neopraví, aj keď daný formát pozná.

`$_FILES['xyz']` – prvky (2)

- `['size']` – veľkosť súboru v bytoch
- `['error']` – "chybový" stav prenosu. Všetky možné hodnoty sú uvedené ďalej.
- Napr.

```
if ($_FILES['obr']['error'] ==  
    UPLOAD_ERR_OK)  
    echo 'Súbor bol úspešne uploadovaný.';
```

`$_FILES['xyz']['error']`

- `UPLOAD_ERR_OK (0)`: žiadna chyba, súbor bol úspešne uploadovaný
- `UPLOAD_ERR_INI_SIZE (1)`: uploadovaný súbor je väčší ako hodnota `upload_max_filesize` definovaná v `php.ini`
- `UPLOAD_ERR_FORM_SIZE (2)`: uploadovaný súbor je väčší ako hodnota `MAX_FILE_SIZE` definovaná vo formulári
- `UPLOAD_ERR_PARTIAL (3)`: uploadovaný súbor nebol prenesený celý (nastal problém počas uploadovania)
- `UPLOAD_ERR_NO_FILE (4)`: nebol uploadovaný žiadny súbor

Funkcie pri uploadovaní (1)

- `move_uploaded_file`(dočasný_súbor, nový_súbor) – presunie dočasný uploadovaný súbor na zadané miesto
- `move_uploaded_file($_FILES['xyz']['tmp_name'], "nova_cesta/novy_subor.pripona")`
- Používateľ, pod ktorým sa vykonávajú php skripty, musí mať právo zápisu do priečinka `nova_cesta`.
- Ak súbor na serveri už existuje, prepíše sa!

Funkcie pri uploadovaní (2)

- **is_uploaded_file**(dočasný_súbor) – vráti TRUE, ak bol zadaný súbor naozaj uploadovaný pomocou formulára metódou POST
- **is_uploaded_file**(\$_FILES['xy']['tmp_name'])
- **basename**(\$_FILES['xyz']['name']) – pôvodný názov súboru bez cesty a bez prípony

Dôležité premenné v súbore php.ini

- **file_uploads** – či je možný upload
- **upload_max_filesize** – max. veľkosť jedného uploadovaného súboru
- **upload_tmp_dir** – kde sa umiestňujú uploadované súbory
- **post_max_size** – max. veľkosť POST sekcie (teda všetkých súčastí formulára odosielaného metódou POST)
- **memory_limit** – max. veľkosť pamäte, ktorú vie PHP alokovať

Čo musí platiť pri uploadovaní

- Ak napr. uploadujeme 3 súbory naraz, potom musí platiť:
 $3 * \text{upload_max_filesize} < \text{post_max_size}$
- Ďalej musí platiť:
 $\text{post_max_size} < \text{memory_limit}$
- $\text{MAX_FILE_SIZE} \leq \text{upload_max_filesize}$
(dodržiavanie MAX_FILE_SIZE je na prehliadači => nespoliehať sa na to)

Ďalšie dôležité premenné v súbore php.ini

- **max_execution_time** – max. čas vykonávania PHP skriptu (regulovanie vytáženía servera)
- **max_input_time** – max. čas strávený prenosom "PHP" údajov (POST, GET, upload, ...)
 - Upozornenie: klienti so slabším pripojením môžu na tomto "stroskotat".

Premenná v Apache (httpd.conf)

- **LimitRequestBody** – veľkosť "balíka", ktorú Apache akceptuje. (vrátane POST, GET, ...)
- V hierarchii predchádzajúcich (obmedzujúcich) premenných má táto najvyššiu prioritu, lebo je definovaná priamo v Apache (webovom serveri).

**Ďakujem za
pozornosť 😊**

Vaše otázky môžete posielat' do
diskusného fóra.