

12. PHP, MySQL

1

Čo ďalej s tvorbou webových aplikácií

Obsah

2

- Možné problémy pri funkcii `include()`
- Využitie adresy prehliadača
- Porovnávanie reťazcov
- Funkcie `header()`, `die()`
- Regulárne výrazy
- Informácie o skúškovom príklade

Možné problémy pri include()

3

- Majme nasledujúci kód, ktorý očakáva súbor ako parameter:

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

- index.php?str=uvod.html
- V čom je problém?

- Ak napr. zadáme hodnotu parametra uvod.html, tak je všetko v poriadku.
- Ale ak zadáme hodnotu parametra <http://zlyserver.sk/skodlivykod.php>, tak kód na inom serveri nám môže spôsobiť problémy.

include() – možné riešenia

4

- Ak očakávame na vstupe lokálny súbor, ale nekontrolujeme ho (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, stačilo by len uvedenie priečinka, čím dáme jasne najavo, že očakávame lokálny súbor (napr. `include('./' . $_GET['str'])`).

Využitie adresy prehliadača

5

- Posielanie údajov cez adresu prehliadača
 - Pomocou formulára odoslaného metódou GET
 - Priamym zadaním parametrov do odkazu
- Posielanie formulára nie je vždy možné alebo efektívne. Napr. môžeme odosielať formulár metódou POST, ale aj tak dokážeme preniesť do adresy rôzne parametre
- Adresu môžeme využiť napr. pri usporadúvaní údajov (podobne ako v phpMyAdmin)

Usporiadanie údajov v objednávkach

6

- Pri zobrazení objednávok umožníme používateľovi, aby si údaje usporiadal podľa niektorého stĺpca (názov stĺpca bude odkazom)

meno a priezvisko	<u>počet dospelých</u>	<u>počet detí</u>	
Jana Pekárová	2	0	Grécko-K
Jana Pekárová	2	0	Grécko-R
predmet UWA	4	0	Grécko-K
predmet UWA	1	0	Bulharsko
Roman Hrušecký	2	1	Grécko-K
Roman Hrušecký	2	0	Bulharsko (€)

Usporiadanie – riešenie

7

- Zmeníme funkciu **vypis_objednavky()**
- 1. zmena: doplníme nadpisy stĺpcov o odkazy s parametrom
 - `počet dospelých`
- 2. zmena: upravíme dopyt podľa parametra
=>

Zmena dopytu na výpis objednávok

8

- `$sql = "SELECT * FROM tour_objednavky, tour_destinacie, tour_pouzivatelia WHERE tour_objednavky.id_zajazdu = tour_destinacie.id_zajazdu AND tour_objednavky.id_pouz = tour_pouzivatelia.id_pouz"; // definuj dopyt`

```
if ($_GET['usporiadaj'] == 'dospeli')
```

```
    $sql .= "ORDER BY tour_objednavky.dospeli DESC,  
tour_pouzivatelia.meno ASC";
```

```
elseif ($_GET['usporiadaj'] == 'deti')
```

```
    $sql .= "ORDER BY tour_objednavky.deti DESC,  
tour_pouzivatelia.meno ASC";
```

```
else
```

```
    $sql .= "ORDER BY tour_pouzivatelia.meno ASC";
```


Porovnávanie reťazcov

9

- Na porovnanie stringov slúžia operátory rovnosti a nerovnosti a príkaz **LIKE**.
- Porovnanie 'jana' < 'janka' je pravdivé pretože štvrtý znak v 'jana' predchádza v abecede štvrtému znaku v 'janka'.
- Príkaz **LIKE** definuje vzor vyhľadávaného textového reťazca pomocou špeciálnych znakov '%' a '_'. Znak '_' zastupuje jeden znak v reťazci, znak '%' zastupuje textový reťazec ľubovoľnej dĺžky.
- `SELECT * FROM tour_pouzivatelia WHERE priezvisko LIKE '%ová'`
 - vyhľadá všetky priezviská končiace na **ová**.

Funkcia header()

10

- Odošle prehliadaču HTTP hlavičku (typ výstupného súboru, presmerovanie...).
- Funkcia by mala byť volaná pred ľubovoľným výpisom (HTML alebo PHP).
- **header("Location: login.php")** – presmerovanie
- Môžeme ňou eliminovať viacnásobné odoslanie formulára, ale môžeme tiež zabudnúť riešiť spätnú väzbu k používateľovi.

Funkcia die()

- Ukončí vykonávanie skriptu (prípadne s výpisom chybovej správy).
- Veľmi dobre zvážiť jej použitie.
- Často sa vyskytuje v konštrukcii
`$link = mysql_connect('localhost', 'user', 'heslo') or die('Nedá sa spojiť s mysql serverom.')`;
- Problém pri použití tejto funkcie – nevykoná sa žiadny príkaz za ním, teda napr. v našich skriptoch by sa nedokončil HTML zdrojový kód a stránka by vyzerala trochu inak.

Regulárne výrazy

12

- Regulárny výraz je vzorka (sada znakov), ktorá popisuje hľadaný reťazec alebo porovnáva reťazce.
- Vo vzorke môžeme použiť bežné, ale aj špeciálne znaky.
- Využívajú sa najmä pri kontrole reťazcových a číselných hodnôt (aj kombinovane), napr. PSČ, tel. číslo, e-mail, značka auta atď.
- Napr. funkcie `preg_grep()`, `preg_match()`...
- `if(preg_match('/^[0-9]{3}\s[0-9]{2}$/', $psc)) ...`
 - Či `$psc` obsahuje PSČ s medzerou

Čo ďalej s tvorbou webových aplikácií

13

- Vylepšenia PHP (aj objektové), MySQL
- HTML5 – Canvas, Drag and Drop, Web Storage, Audio, Video...
- JavaScript
- JQuery
- AJAX

Informácie o skúškovom príklade

14

- **Skoro určite bude súčasťou skúšky:**
 - Spracovanie formulára
 - Využitie SESSION
 - Vyberanie dát z tabuliek
 - Práca s heslami v MySQL
 - Vkladanie alebo aktualizácia alebo mazanie dát tabuliek

Ďakujem za pozornosť 😊

15

Priestor na vaše otázky