9. Databázy

Používatelia

Obsah

- Heslá a používatelia
- Potlačenie nežiaduceho výstupu

Používatelia

- Doteraz sa mohol prihlásiť len používateľ uwa.
- **Zmena**: Vytvoríme tabuľku používateľov, ktorí budú môcť pracovať so systémom TWD tour. Každý používateľ bude mať nastavené, či patrí/nepatrí medzi administrátorov.
- Tabuľka používateľov – podobná iným tabuľkám.
- **Používatelia existujú len v tabuľke – nemajú nič spoločné s používateľmi databázy MySQL alebo webového servera.**

Heslá

- Autentifikácia používateľov
- Ako ukladať heslá v databáze?
  - **Ako čistý text** (pri zabudnutí hesla sa dá odoslať, ale pri hacknutí databázy ich hacker vidí – riešenie sa neodporúča)
  - **Šifrované** (PASSWORD, **MD5**, SHA1, ...)
    - Pri šifrovaní **MD5** sa z hesla vytvorí hexadecimálny reťazec dĺžky 32 znakov.
    - Ide o jednosmerné šifrovanie (nedá sa zistiť pôvodné heslo).

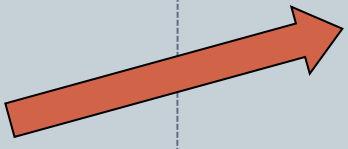
Úprava prihlasovania

- Vytvoríme tabuľku používateľov, ktorí môžu pracovať v systéme (**tour_pouzivatelia**)
- V pôvodnej tabuľke tour_objednavky **zrušíme stĺpec meno**, ktorý presunieme do novej tabuľky tour_pouzivatelia.
- Pôvodný stĺpec meno (v tabuľke tour_objednavky) nahradíme položkou ID používateľa (**id_pouz**).
- Pri prihlasovaní budeme kontrolovať používateľov podľa novo vytvorenej tabuľky.

Vzťahy medzi tabuľkami

tabuľka tour_objednavky

Stĺpce	Typ
id	smallint(6)
id_pouz	smallint(6)
dospeli	tinyint(4)
deti	tinyint(4)
id_zajazdu	smallint(6)
poistenie	tinyint(1)
izba_more	tinyint(1)
kurz_potapania	tinyint(1)

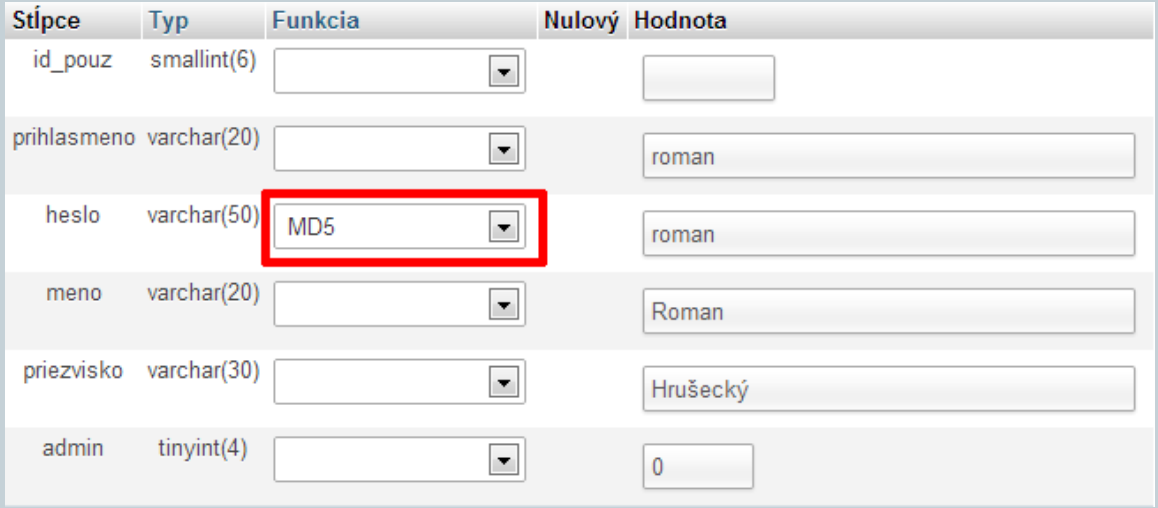


tabuľka tour_pouzivatelia

Stĺpce	Typ
id_pouz	smallint(6)
prihlasmeno	varchar(20)
heslo	varchar(50)
meno	varchar(20)
priezvisko	varchar(30)
admin	tinyint(4)

Nové definície tabuliek: `tour.sql`

Vytváranie používateľov



Stĺpce	Typ	Funkcia	Nulový	Hodnota
id_pouz	smallint(6)			
prihlasmeno	varchar(20)			roman
heslo	varchar(50)	MD5		roman
meno	varchar(20)			Roman
priezvisko	varchar(30)			Hrušecký
admin	tinyint(4)			0

- Vytváranie používateľov bude zatiaľ realizované len cez prostredie phpMyAdmin.
- INSERT INTO tour_pouzivatelia (prihlasmeno, heslo) VALUES ('roman', **MD5**('roman'));

Overovanie používateľov

id_pouz	prihlasmeno	heslo	meno	priezvisko	admin
1	admin	21232f297a57a5a743894a0e4a801fc3	Administrátor	systému	1
2	uwa	78f0f32c08873cfdba57f17c855943c0	predmet	UWA	0
3	roman	b179a9ec0777eae19382c14319872e1b	Roman	Hrušecký	0
4	marek	e061c9aea5026301e7b3ff09e9aca2cf	Marek	Nagy	1
5	jozko	256f035bd7cf72238fad007fb9199c66	Jožko	Púčik	0
6	mrkva	bfd7d9c62540ed72de0f32932077bef7	Janko	Mrkvička	0

- Keďže nevieme zistiť pôvodné heslo, musíme zadané heslo zašifrovať funkciou **MD5()** a porovnať s reťazcom v tabuľke.
- SELECT * FROM tour_pouzivatelia WHERE prihlasmeno='**meno**' AND heslo=**MD5**('**heslo**');
- $sql = "SELECT * FROM tour_pouzivatelia WHERE prihlasmeno='" . $_POST['meno'] . "' AND heslo=**MD5**('" . $_POST['heslo'] . "')";

Zmena prihlasovania

- Overovanie cez databázu
- Výpis celého mena prihláseného používateľa (pri každom zobrazení stránky s prihlásením/odhlásením)
- Zapamätáme si nielen prihlasovacie meno, ale takmer kompletné údaje o používateľovi (nie heslo) do SESSION, aby sme ich nemuseli vždy zisťovať z databázy.
- **Musíme zmeniť**: výpis a odoslanie objednávky, úprava a zmazanie objednávky

Zmena pri výpise objednávok

- Zmena dopytu – údaje budeme vyberať už z **3 tabuliek**
- 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** ORDER BY tour_pouzivatelia.meno ASC

Zmena pri odoslaní objednávky

- Objednávku môže odoslať len prihlásený používateľ.
- Meno a priezvisko sa nebudú zadávať (zrušíme z formulára objednávky), ale sa vypíšu podľa údajov v SESSION.
- Meno a priezvisko sa nemusia vkladať do tabuľky. Vkladá sa len **ID prihláseného používateľa**.
- INSERT INTO tour_objednavky SET **id_pouz="" . $_SESSION['id_pouz']** ...

Zrušenie objednávky

- V prvom kroku netreba nič meniť – dopyt sa nemení.
- **Problém**: Prihlásený používateľ môže zmazať objednávky iných používateľov (**ak zmení parameter id v adrese**)
- **Zmena**: pri výpise sa odkaz na zrušenie objednávky zobrazí len pri objednávke, ktorá patrí prihlásenému používateľovi (**+kontrola** podľa **$_SESSION['id_pouz']** – či zadané **id** objednávky v adrese patrí prihlásenému používateľovi – využijeme funkciu daj_udaje_objednavky())

```
$udaje = daj_udaje_objednavky($_GET['id']);
 if ($udaje['id_pouz'] == $_SESSION['id_pouz']) {
...
```

Zmena objednávky

- V prvom kroku: drobná zmena kontroly, dopytu a formulára (vyplýva z predchádzajúcich zmien)
- **Skrytý problém**: Prihlásený používateľ môže upravovať objednávky iných používateľov (**ak zmení parameter id v adrese**)
- **Zmena**: pri výpise sa odkaz na úpravu objednávky zobrazí len pri objednávke, ktorá patrí prihlásenému používateľovi (**+kontrola** podľa **$_SESSION['id_pouz']**) – ako pri zrušení objednávky, využijeme daj_udaje_objednavky()

```
$udaje = daj_udaje_objednavky($_GET['id']);
if ($udaje['id_pouz'] == $_SESSION['id_pouz'])
  $zobraz_form = true; ...
```

Námet na zmenu (1)

- Každý používateľ môže odoslať viac objednávok.
- Čo ak by sme chceli obmedziť, že používateľ môže odoslať len 1 objednávku?

- **Riešenie 1**: zistíme, či existuje v databáze záznam (objednávka) pre prihláseného používateľa
- **Riešenie 2**: položku **id_pouz** v tabuľke **tour_objednavky** nastavíme ako **unikátny kľúč**

- Vyberte si jedno z riešení a vyskúšajte si ho naprogramovať.

Námet na zmenu (2)

- Momentálne sa vypisujú všetkým používateľom všetky objednávky. Pri objednávkach to nie je úplne logické, skôr by sa im mali zobrazovať len ich objednávky (administrátorom by sa mali zobrazovať všetky).
- Spôsob zobrazovanie všetkých „objednávok“ s možnosťou úpravy/zmazania len vlastných sa dá aplikovať napr. na fórum, rezervácie lístkov, spravovanie článkov.

Ako zabrániť nežiadúcim výpisom/výstupom?

- Ľubovoľný príkaz v PHP môže vygenerovať chybovú správu, ktorú nechceme vypísať.
- Potlačíme ju znakom @ – zadávame pred príkaz (bez medzery).
- **Napr.**: vyskúšajte si vypnúť MySQL server (pred alebo po prihlásení) a následne spustiť niektorý php skript.
- $link = @mysql_connect('localhost', 'uwa', 'uwa');

- Neodporúča sa používať pri tvorbe a testovaní aplikácie.

Ďakujem za pozornosť ☺

Priestor na vaše otázky