Aiken Tine Ahac, R4C, 10. 4. 2023

Spletne aplikacije Vaja 22_1

Teme:
Delo s PB – prepared statements:
Zaščita pred SQL vdori
Branje / filtriranje podatkov iz PB mySQL; prikaz podatkov
Obrazci, vnos podatkov, validacija podatkov
Testiranje

Prenesite in namestite PB `GeodetskaUprava`. Skripta je v datoteki `GeodetskaUprava.sql`. V bazi sta tabeli

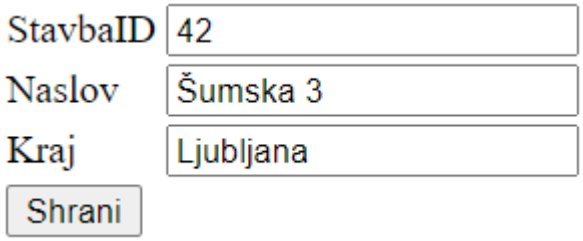
- Stavba(StavbaID:N, Naslov:A20, Kraj:A20, SteviloPrebivalcev:N) in
- Stanovanje(StavbaID:N-->Stavba, Zap_ST:N, Povrsina_kvadrati:N, Prijavljenih:N, VrednostStanovanja:N).

Pri realizaciji nalog uporabite

- API mysqli in prepared statements

Naloga 1

Napišite program, ki omogoča dodajanje podatkov o stavbi. Na obrazcu (glej sliko) uporabnik vnese le podatke StavbaID (celo število > 0), Naslov (niz vsaj 2, največ 30 znakov, prvi znak moram biti velika črka, sledi zaporedje velikih / malih črk, števk in presledkov) in Kraj (niz vsaj dve, največ tridesetih znakov, velika začetnica, ostali znaki so velike / male črke in presledki). V naslovu in kraju so lahko tudi šumniki. Veljavnost podatkov validirajte s atributom pattern. Očiščene podatke zapišite v tabelo Stavba. Skripto za dodajanje zapisa realizirajte z uporabo prepared statement. Vrednost podatka SteviloPrebivalcev ne vpisujete (defaut vrednost bo 0 – glej show create table Stavba). Po dodajanju zapisa, naj uporabnik dobi obvestilo: `zapis dodan` ali `napaka pri dodajanju, zapis NI dodan`.



Aiken Tine Ahac, R4C, 10. 4. 2023

Testirajte program z vnosom naslednjih podatkov:
1, Vegova 1, ljubljana // zapis mora biti zavrnjen
1, Vegova 1, Ljubljana
2, Vegova 4, Ljubljana
3, Šišenska 23a, Ljubljana
4, Dunajska 22, Ljubljana
5, Rateče 3, Rateče
6, Koroška 33, Kranjska Gora
6, Slovenska 2, Želimlje // zapis mora biti zavrnjen
7, Slovenska 2, Želimlje
8, Slovenska 33, Ljubljana
9, Ižanska 2, Ljubljana
10, Ljubljanska 1, Ig

Po izvedbi testiranja bo izpis iz mysql konzole:

```
MariaDB [geodetskauprava]> select * from stavba;
+----------+----------------+---------------+---------------------+
| StavbaID | Naslov         | Kraj          | SteviloPrebivalcev |
+----------+----------------+---------------+---------------------+
|        1 | Vegova 1       | Ljubljana     |                   0 |
|        2 | Vegova 4       | Ljubljana     |                   0 |
|        3 | Šišenska 23a   | Ljubljana     |                   0 |
|        4 | Dunajska 22    | Ljubljana     |                   0 |
|        5 | Rateče 3       | Rateče        |                   0 |
|        6 | Koroška 33     | Kranjska Gora |                   0 |
|        7 | Slovenska 2    | Želimlje      |                   0 |
|        8 | Slovenska 3    | Ljubljana     |                   0 |
|        9 | Ižanska 2      | Ljubljana     |                   0 |
|       10 | Ljubljanska 1  | Ig            |                   0 |
+----------+----------------+---------------+---------------------+
10 rows in set (0.00 sec)
```

index.php

```
<form action="skripta.php" method="GET">
  StavbaID: <input type="number" name="stavbaID" min="0" required
/><br />
  Naslov: <input type="text" name="naslov" minlength="2"
maxlength="30" required pattern="[A-ZČŠŽ][A-ZČŠŽa-zčšž\s0-9]+" /><br
/>
  Kraj: <input type="text" name="kraj" minlength="2" maxlength="30"
required pattern="[A-ZČŠŽ][A-ZČŠŽa-zčšž\s0-9]+" /><br />

  <input type="submit" value="Shrani">
```

```
</form>
```

skripta.php

```php
<?php

$conn = mysqli_connect("localhost", "root", "", "geodetskaUprava") or
die("error");
$stmt = mysqli_stmt_init($conn);

if (isset($_GET["stavbaID"])) $stavbaID = $_GET["stavbaID"];
else return;

if (isset($_GET["naslov"])) $naslov = $_GET["naslov"];
else return;

if (isset($_GET["kraj"])) $kraj = $_GET["kraj"];
else return;

if (!preg_match("/^[1-9][0-9]*$/", $_GET["stavbaID"])) {
  echo 'Prišlo je do napake, zapis NI dodan';
  return;
}

if (!preg_match("/^[A-ZČŠŽ][A-ZČŠŽa-zčšž\s0-9]+$/", $_GET["naslov"]))
{
  echo 'Prišlo je do napake, zapis NI dodan';
  return;
}

if (!preg_match("/^[A-ZČŠŽ][A-ZČŠŽa-zčšž\s0-9]+$/", $_GET["kraj"])) {
  echo 'Prišlo je do napake, zapis NI dodan';
  return;
}

$q = 'INSERT INTO Stavba VALUES (?, ?, ?, DEFAULT)';

mysqli_stmt_prepare($stmt, $q);
mysqli_stmt_bind_param($stmt, "iss", $_GET["stavbaID"],
$_GET["naslov"], $_GET["kraj"]);
mysqli_stmt_execute($stmt);

if (mysqli_stmt_affected_rows($stmt) > 0) {
```

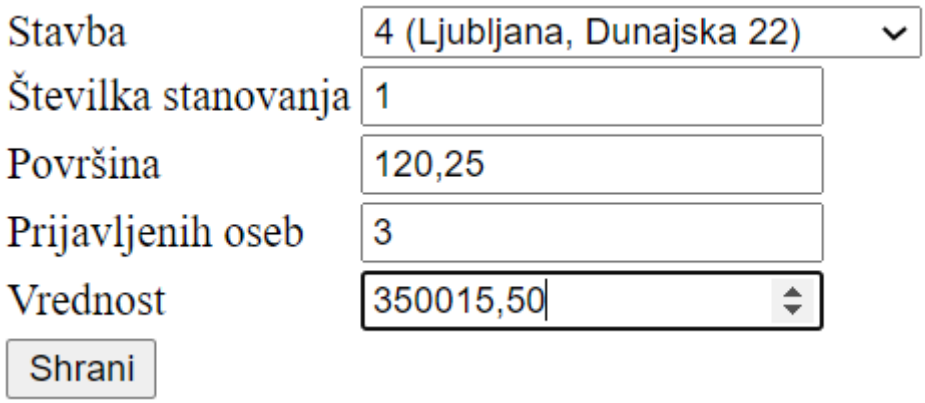
```
  echo 'Zapis je dodan';
} else {
  echo 'Prišlo je do napake, zapis NI dodan';
}

mysqli_close($conn);
```

```
MariaDB [geodetskauprava]> select * from stavba;
+----------+---------------+--------------+--------------------+
| StavbaID | Naslov        | Kraj         | SteviloPrebivalcev |
+----------+---------------+--------------+--------------------+
|        1 | Vegova 1      | Ljubljana    |                  0 |
|        2 | Vegova 4      | Ljubljana    |                  0 |
|        3 | Šišenska 23a  | Ljubljana    |                  0 |
|        4 | Dunajska 22   | Ljubljana    |                  0 |
|        5 | Rateče 3      | Rateče       |                  0 |
|        6 | Koroška 33    | Kranjska Gora |                  0 |
|        7 | Slovenska 2   | Želimlje     |                  0 |
|        8 | Slovenska 33  | Ljubljana    |                  0 |
|        9 | Ižanska 2     | Ljubljana    |                  0 |
|       10 | Ljubljanska 1 | Ig           |                  0 |
+----------+---------------+--------------+--------------------+
10 rows in set (0.000 sec)
```

Aiken Tine Ahac, R4C, 10. 4. 2023

Naloga 2

Napišite program PHP, ki omogoča dodajanje podatkov o enem stanovanju. Vnos podatka StavbaID naj bo realizirana s pomočjo elementa select, ostale podatke uporabnik vpiše v navadne elemente input. Za prenos podatkov uporabite metodo **get**. Pri vnosu vrednosti in površine omogočite vnos realnih števil z 2 decimalki. Najmanjša dovoljene vrednosti so: za podatek Številka stanovanja 1; za podatek Površina 1; za podatke Prijavljenih oseb 0 in za podatek Vrednost 1000. Po dodajanju uporabnik mora dobiti obvestilo 'podatki so uspešno dodani' ali 'podatki niso dodani'. Po uspešno dodanem stanovanju je potrebno poskrbeti za ustrezno posodobitev podatka SteviloPrebivalvec v tabeli Stavba. Pričakovana oblika uporabniškega vmesnika za vnos podatkov:



Skripto testirajte s podatki:
4; 1; 120,25; 3; 350015,15
4; 2; 32,25; 1; 50015,50
4; 3; 200,55; 2; 48000,00
1; 1; 77,50; 2; 290000,50
Po izvedbi testiranja mora biti vsebina tabele `Stanovanje`:

```
MariaDB [geodetskauprava]> select * from stanovanje;
+----------+--------+-------------------+-------------+--------------------+
| StavbaID | Zap_ST | Povrsina_kvadrati | Prijavljenih | VrednostStanovanja |
+----------+--------+-------------------+-------------+--------------------+
|        1 |      1 |              77.5 |           2 |             290000 |
|        4 |      1 |            120.25 |           3 |             350016 |
|        4 |      2 |             32.25 |           1 |            50015.5 |
|        4 |      3 |            200.55 |           2 |             480000 |
+----------+--------+-------------------+-------------+--------------------+
4 rows in set (0.00 sec)
```

in vsebina tabele `Stavba`:

```
MariaDB [geodetskauprava]> select * from stavba;
+----------+----------------+---------------+---------------------+
| StavbaID | Naslov         | Kraj          | SteviloPrebivalcev |
+----------+----------------+---------------+---------------------+
|        1 | Vegova 1       | Ljubljana     |                   2 |
|        2 | Vegova 4       | Ljubljana     |                   0 |
|        3 | Šišenska 23a   | Ljubljana     |                   0 |
|        4 | Dunajska 22    | Ljubljana     |                   6 |
|        5 | Rateče 3       | Rateče        |                   0 |
|        6 | Koroška 33     | Kranjska Gora |                   0 |
|        7 | Slovenska 2    | Želimlje      |                   0 |
|        8 | Slovenska 3    | Ljubljana     |                   0 |
|        9 | Ižanska 2      | Ljubljana     |                   0 |
|       10 | Ljubljanska 1  | Ig            |                   0 |
+----------+----------------+---------------+---------------------+
10 rows in set (0.00 sec)
```

index.php

```
<form action="skripta.php" method="GET">
  Stavba:
  <select name="stavbaID" required>
    <?php
    $conn = mysqli_connect("localhost", "root", "",
"geodetskauprava");

    $q = "SELECT * FROM stavba";

    $rs = mysqli_query($conn, $q);

    while ($x = mysqli_fetch_assoc($rs))
      echo '<option value="' . $x["StavbaID"] . '">' .
        $x["StavbaID"] . ' (' . $x["Kraj"] . ', ' . $x["Naslov"] . ')'
        . '</option>';

    mysqli_close($conn);
    ?>
  </select><br />

  Številka stanovanja: <input type="number" name="stStan" min="1"
required /><br />
  Površina: <input type="number" name="povrsina" min="1" step="0.01"
required /><br />
  Prijavljenih oseb: <input type="number" name="stOseb" min="0"
required /><br />
```

```
  Vrednost: <input type="number" name="vrednost" min="1000"
step="0.01" required /><br />

  <input type="submit" value="Shrani">
</form>
```

skripta.php

```
<?php

$conn = mysqli_connect("localhost", "root", "", "geodetskaUprava") or
die("error");
$stmt = mysqli_stmt_init($conn);

if (!preg_match("/^[1-9][0-9]*$/", $_GET["stavbaID"])) {
  echo 'Prišlo je do napake, zapis NI dodan';
  return;
}

if ($_GET["stStan"] < 1) {
  echo 'Prišlo je do napake, zapis NI dodan';
  return;
}

if ($_GET["povrsina"] < 1) {
  echo 'Prišlo je do napake, zapis NI dodan';
  return;
}

if ($_GET["stOseb"] < 0) {
  echo 'Prišlo je do napake, zapis NI dodan';
  return;
}

if ($_GET["vrednost"] < 1000) {
  echo 'Prišlo je do napake, zapis NI dodan';
  return;
}

$q = 'INSERT INTO Stanovanje VALUES (?, ?, ?, ?, ?)';

mysqli_stmt_prepare($stmt, $q);
```

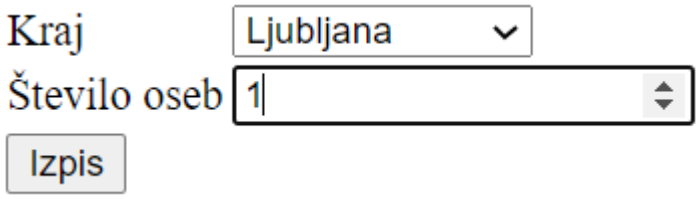
```php
mysqli_stmt_bind_param($stmt, "iidid", $_GET["stavbaID"],
$_GET["stStan"], $_GET["povrsina"], $_GET["stOseb"],
$_GET["vrednost"]);
mysqli_stmt_execute($stmt);

$q = 'UPDATE Stavba SET SteviloPrebivalcev = SteviloPrebivalcev + ?
WHERE StavbaID = ?';
mysqli_stmt_prepare($stmt, $q);
mysqli_stmt_bind_param($stmt, "ii", $_GET["stOseb"],
$_GET["stavbaID"]);
mysqli_stmt_execute($stmt);

if (mysqli_stmt_affected_rows($stmt) > 0) {
  echo 'Zapis je dodan';
} else {
  echo 'Prišlo je do napake, zapis NI dodan';
}

mysqli_close($conn);
```

```
MariaDB [geodetskauprava]> select * from stanovanje;
+----------+--------+-------------------+-------------+--------------------+
| StavbaID | Zap_ST | Povrsina_kvadrati | Prijavljenih | VrednostStanovanja |
+----------+--------+-------------------+-------------+--------------------+
|        1 |      1 |              77.5 |           2 |             290000 |
|        4 |      1 |            120.25 |           3 |             350015 |
|        4 |      2 |             32.25 |           1 |            50015.5 |
|        4 |      3 |            200.55 |           2 |              48000 |
+----------+--------+-------------------+-------------+--------------------+
4 rows in set (0.000 sec)

MariaDB [geodetskauprava]> select * from stavba;
+----------+----------------+--------------+--------------------+
| StavbaID | Naslov         | Kraj         | SteviloPrebivalcev |
+----------+----------------+--------------+--------------------+
|        1 | Vegova 1       | Ljubljana    |                  2 |
|        2 | Vegova 4       | Ljubljana    |                  0 |
|        3 | Šišenska 23a   | Ljubljana    |                  0 |
|        4 | Dunajska 22    | Ljubljana    |                  6 |
|        5 | Rateče 3       | Rateče       |                  0 |
|        6 | Koroška 33     | Kranjska Gora |                 0 |
|        7 | Slovenska 2    | Želimlje     |                  0 |
|        8 | Slovenska 33   | Ljubljana    |                  0 |
|        9 | Ižanska 2      | Ljubljana    |                  0 |
|       10 | Ljubljanska 1  | Ig           |                  0 |
+----------+----------------+--------------+--------------------+
10 rows in set (0.001 sec)
```

Aiken Tine Ahac, R4C, 10. 4. 2023

Naloga 3

Napišite program PHP, ki v tabelarični obliki izpiše naslove stavb v kraju X, ki imajo več kot N prebivalcev. Ime kraja uporabnik izbere iz elementa select (napolnite ga tako, da vnesete kraje iz tabele Stavba), število prebivalcev N pa vpiše (minimalno število je 0). Izpis realizirajte s funkcijo in naj bo urejen po padajočem številu prebivalcev.
Pričakovana oblika uporabniškega vmesnika:



Primer izpisa za kraj Ljubljana in število prebivalcev > 1.

Naslov	Št. Prebivalcev
Dunajska 22	6
Vegova 1	2

index.php

```
<form action="skripta.php" method="GET">
  Kraj:
  <select name="kraj" required>
    <?php
    $conn = mysqli_connect("localhost", "root", "",
"geodetskauprava");

    $q = "SELECT DISTINCT Kraj FROM stavba";

    $rs = mysqli_query($conn, $q);

    while ($x = mysqli_fetch_assoc($rs))
      echo '<option value="' . $x["Kraj"] . '">' . $x["Kraj"] .
'</option>';

    mysqli_close($conn);
    ?>
  </select><br />
```

```
  Število oseb: <input type="number" name="stOseb" min="0" required
/><br />

  <input type="submit" value="Izpis">
</form>
```

Aiken Tine Ahac, R4C, 10. 4. 2023

skripta.php

```php
<?php
echo '<style>
table, tr, td {
    border-collapse: collapse;
    border: 1px solid black;
  text-align: center;
}

td {
    padding: 0 10px;
}

thead {
    background: #dbdbdb;
    font-weight: bold;
}
</style>';


$conn = mysqli_connect("localhost", "root", "", "geodetskaUprava") or
die("error");
$stmt = mysqli_stmt_init($conn);

if (!preg_match("/^[A-ZČŠŽ][A-ZČŠŽa-zčšž\s0-9]+$/", $_GET["kraj"])) {
  echo 'Prišlo je do napake, zapis NI dodan';
  return;
}

if ($_GET["stOseb"] < 0) {
  echo 'Prišlo je do napake, zapis NI dodan';
  return;
}

$q = 'SELECT * FROM Stavba WHERE Kraj = ? AND SteviloPrebivalcev > ?
ORDER BY SteviloPrebivalcev DESC';

mysqli_stmt_prepare($stmt, $q);
mysqli_stmt_bind_param($stmt, "si", $_GET["kraj"], $_GET["stOseb"]);
mysqli_stmt_execute($stmt);


$rs = mysqli_stmt_get_result($stmt);
```

```php
izpis($rs);

mysqli_close($conn);

function izpis($rs)
{
  echo '<table><thead>
    <td>Naslov</td>
    <td>Št. prebivalcev</td>
    </thead>';

  while ($x = mysqli_fetch_assoc($rs)) {
    echo '<tr>';
    echo '<td>' . $x["Naslov"] . '</td>';
    echo '<td>' . $x["SteviloPrebivalcev"] . '</td>';
    echo '</tr>';
  }

  echo '</table>';
}
```

Programe prekopirajte pod navodila posamezne naloge. V glavo poročila zapišite ime, priimek, razred in datum. Poročilo oddajte v nabiralnik. Skrajnji rok za oddajo poročila v nabiralnik spletne učilnice je takoj po izvedeni vaji.