# 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

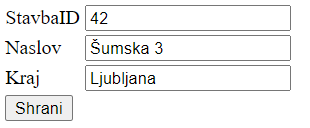
* Stavba(StavbaID:N, Naslov:A20, Kraj:A20, SteviloPrebivalcev:N) in
* Stanovanje(StavbaID:N-->Stavba, Zap\_ST:N, Povrsina\_kvadrati:N, Prijavljenih:N, VrednostStanovanja:N).

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.



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

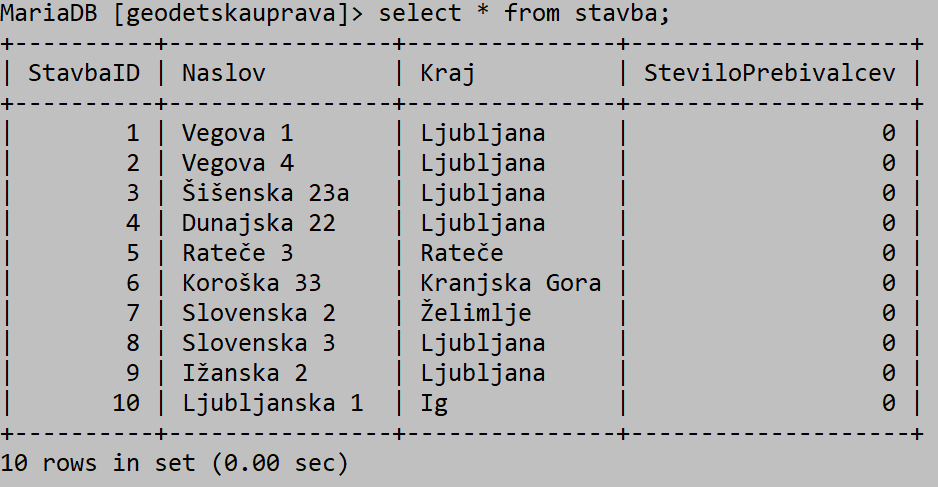
7, Slovenska 2, Želimlje

8, Slovenska 33, Ljubljana

9, Ižanska 2, Ljubljana

10, Ljubljanska 1, Ig

Po izvedbi testiranja bo izpis iz mysql konzole:



**// index.php**

<form *action*="shrani.php" *method*="GET">

<label *for*="stavbaid">StavbaID</label>

<input *type*="number" *min*="0" *name*="stavbaid" *id*="stavbaid" *required* /> <br />

<label *for*="naslov">Naslov</label>

<input *type*="text" *minlength*="2" *maxlength*="30" *name*="naslov" *id*="naslov" *pattern*="[A-ZČŠŽ][A-ZČŠŽa-zčšž]{2,30}" *required* /> <br />

<label *for*="kraj">Kraj</label>

<input *type*="text" *minlength*="2" *maxlength*="30" *name*="kraj" *id*="kraj" *pattern*="[A-ZČŠŽ][A-ZČŠŽa-zčšž]{2,30}" *required* /> <br />

<input *type*="submit" *value*="shrani" />

</form>

**// shrani.php**

<?php

*require\_once*("index.php");

$data = $\_GET;

*if* (!isset($data["stavbaid"]) || $data["stavbaid"] <= 0) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

}

*if* (!isset($data["naslov"]) || !preg\_match("/^[A-ZČŠŽ][A-ZČŠŽa-zčšž]{2,30}$/", $data["naslov"])) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

}

*if* (!isset($data["kraj"]) || !preg\_match("/^[A-ZČŠŽ][A-ZČŠŽa-zčšž]{2,30}$/", $data["kraj"])) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

}

$mysqli = new mysqli("localhost", "root", "", "GeodetskaUprava");

*if* ($mysqli->connect\_errno) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

}

$query = "INSERT INTO stavba VALUES (?, ?, ?, 0);";

$stmt = $mysqli->prepare($query);

$stmt->bind\_param("iss", $data["stavbaid"], $data["kraj"], $data["naslov"]);

$stmt->execute();

*if* (!$stmt->fetch()) {

echo "napaka pri dodajanju, zapis NI dodan";

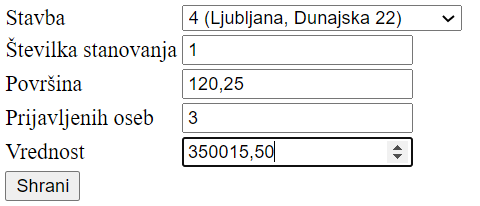
*exit*();

}

echo "zapis dodan";

**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:

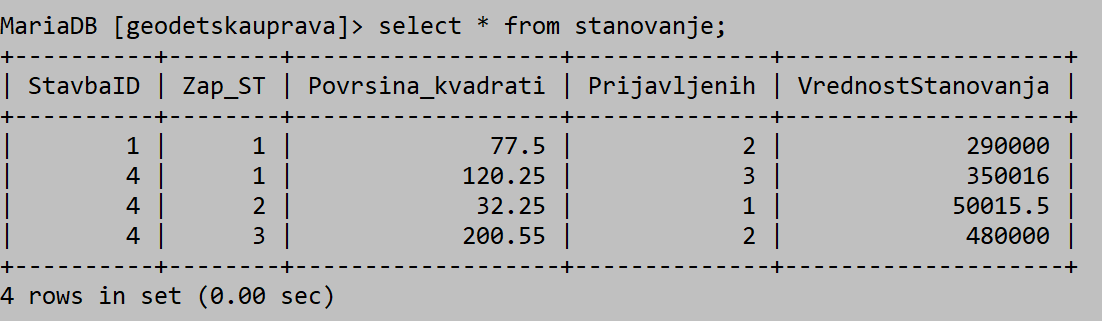
4; 1; 120,25; 3; 350015,15

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:



in vsebina tabele Stavba:



//index.php

<form *action*="shrani.php" *method*="GET">

<label *for*="stavba">Stavba</label>

<select *name*="stavba">

<?php

$mysqli = new mysqli("localhost", "root", "", "GeodetskaUprava");

*if* ($mysqli->connect\_errno) {

*exit*();

}

$res = $mysqli->query("SELECT \* FROM stavba");

*while* ($row = $res->fetch\_assoc()) {

$label = $res["StavbaID"] . " (" . $row["Kraj"] . ", " . $row["naslov"] . ")";

echo '<option value="' . $row["StavbaID"] . '">' . $label . '</option>';

}

$res->close();

$mysqli->close();

?>

</select></br>

<label *for*="st\_stanovanja">Številka stanovanja</label>

<input *type*="number" *min*="1" *step*="1" *name*="st\_stanovanja" *id*="st\_stanovanja" *required* /> <br />

<label *for*="povrsina">Površina</label>

<input *type*="number" *min*="1" *step*=".01" *name*="povrsina" *id*="povrsina" *required* /> <br />

<label *for*="osebe">Prijavljenih oseb</label>

<input *type*="number" *min*="0" *step*="1" *name*="osebe" *id*="osebe" *required* /> <br />

<label *for*="vrednost">Vrednost</label>

<input *type*="number" *min*="1000" *step*=".01" *name*="vrednost" *id*="vrednost" *required* /> <br />

<input *type*="submit" *value*="shrani" />

</form>

//shrani.php

<?php

*require\_once*("index.php");

$data = $\_GET;

*if* (!isset($data["stavba"])) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

}

*if* (!isset($data["st\_stanovanja"]) || $data["st\_stanovanja"] <= 1) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

}

*if* (!isset($data["povrsina"]) || $data["povrsina"] <= 1) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

}

*if* (!isset($data["osebe"]) || $data["osebe"] <= 0) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

}

*if* (!isset($data["vrednost"]) || $data["vrednost"] <= 1000) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

}

$mysqli = new $mysqli("localhost", "root", "", "GeodetskaUprava");

*if* ($mysqli->connect\_errno) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

}

$query = "INSERT INTO stanovanje VALUES (?, ?, ?, ?, ?);";

$stmt = $mysqli->prepare($query);

$stmt->bind\_param(

"iiiii",

$data["stavba"],

$data["st\_stanovanja"],

$data["povrsina"],

$data["osebe"],

$data["vrednost"]

);

$stmt->execute();

*if* ($stmt->fetch()) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

}

$update\_query = "UPDATE stavba SET steviloprebivalcev = steviloprebivalcev + ? WHERE stavbaid = ?";

$update\_stmt = $mysqli->prepare($update\_query);

$update\_stmt->bind\_param("ii", $data["osebe"], $data["stavba"]);

$udpate\_stmt->execute();

*if* ($update\_stmt->fetch()) {

echo "napaka pri dodajanju, zapis NI dodan";

*exit*();

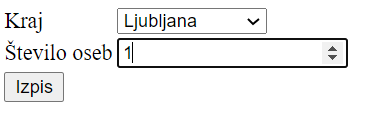
}

echo "zapis dodan";

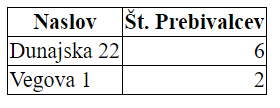
**Naloga 3**

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.



// index.php

<style>

table, tr, td {

border-collapse: collapse;

border: 1px solid black;

}

</style>

<form *action*="izpis.php" *method*="GET">

<label *for*="kraj">Kraj</label>

<select *name*="kraj">

<?php

$mysqli = new mysqli("localhost", "root", "", "GeodetskaUprava");

*if* ($mysqli->connect\_errno) {

*exit*();

}

$res = $mysqli->query("SELECT DISTINCT kraj FROM stavba ORDER BY kraj ASC");

*while* ($row = $res->fetch\_assoc()) {

echo '<option value="' . $row["kraj"] . '">' . $row["kraj"] . '</option>';

}

$res->close();

$mysqli->close();

?>

</select></br>

<label *for*="osebe">Število oseb</label>

<input *type*="number" *min*="0" *step*="1" *name*="osebe" *id*="osebe" *required* /> <br />

<input *type*="submit" *value*="izpis" />

</form>

// izpis.php

<?php

*require\_once*("index.php");

*if* (!isset($data["kraj"])) {

*exit*("napaka pri izpisu");

}

*if* (!isset($data["osebe"]) || $data["osebe"] <= 0) {

*exit*("napaka pri izpisu");

}

$mysqli = new mysqli("localhost", "root", "", "localhost");

*if* ($mysqli->connect\_error) {

*exit*("napaka pri izpisu");

}

$query = "SELECT naslov, steviloprebivalcev FROM stavba WHERE kraj = ? AND steviloprebivalcev > ?ORDER BY kraj DESC";

$stmt = $mysqli->prepare($query);

$stmt->bind\_param("si", $data["kraj"], $data["osebe"]);

$stmt->execute();

echo "<table><tr><th>Naslov</th><th>Št. Prebivalcev</th></tr>";

$res = $stmt->get\_result();

*while* ($row = $res->fetch\_assoc()) {

echo "<tr>";

echo '<td>' . $row["naslov"] . '</td>';

echo '<td>' . $row["steviloprebivalcev"] . '</td>';

echo "</tr>";

}

$stmt->close();

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.*