# Spletne aplikacije Vaja 23\_1

***Teme:***

***Delo s PB – prepared statements:***

***Zaščita pred SQL vdori***

***Branje / filtriranje podatkov iz PB mySQL; prikaz podatkov***

***Obrazci, vnos podatkov, validacija podatkov***

***Razprševanje/preverjanje razpršene vrednosti***

***Testiranje***

Prenesite in namestite PB GeodetskaUprava, ki ste jo ustvarili z izvedbo 23. vaje. V skripti so še shranjeni testni podatki. 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 0 - 0**

V PB GeodetskaUprava ustvarite tabelo Uporabnik(uIme:A20, uGeslo:A200).

Naredite program (obrazec in skripto), ki omogoča registracijo uporabnika. Za razprševanje gesla uporabite algoritem sha1. V geslu mora biti vsaj 1 števka in vsaj 1 črka.

CREATE TABLE Uporabnik (

uIme VARCHAR(20) NOT NULL UNIQUE,

uGeslo VARCHAR(200) NOT NULL

);

index.php

<form action="registriraj.php" method="POST">

Uporabniško ime: <input type="text" name="uime" required /> <br>

Geslo: <input type="password" name="geslo" pattern="(?=.\*[0-9])(?=.\*[a-zA-Z])([a-zA-Z0-9]+)\*" required /> <br>

<input type="submit" value="Registracija" />

</form>

registriraj.php

<?php

$conn = mysqli\_connect("localhost", "root", "", "geodetskaUprava") or die("error");

$stmt = mysqli\_stmt\_init($conn);

if (!preg\_match("/^(?=.\*[0-9])(?=.\*[a-zA-Z])([a-zA-Z0-9]+)$/", $\_POST["geslo"])) {

echo 'Geslo mora vsebovati vsaj eno števko in eno črko';

}

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

$g = sha1($\_POST["geslo"]);

mysqli\_stmt\_prepare($stmt, $q);

mysqli\_stmt\_bind\_param($stmt, "ss", $\_POST["uime"], $g);

mysqli\_stmt\_execute($stmt);

if (mysqli\_stmt\_affected\_rows($stmt) > 0) {

echo 'Zapis je dodan';

} else {

echo 'Prišlo je do napake, zapis NI dodan';

}

**Naloga 0 – 1**

Dostop do skript, ostalih nalog vaje mora biti zaščiten 🡺 ustvarite obrazec za prijavo in preverjanje podatkov o uporabniku.

prijava.php

<form action="preveriPrijavo.php" method="POST">

Uporabniško ime: <input type="text" name="uime" required /> <br>

Geslo: <input type="password" name="geslo" pattern="(?=.\*[0-9])(?=.\*[a-zA-Z])([a-zA-Z0-9]+)\*" required /> <br>

<input type="submit" value="Prijava" />

</form>

preveriPrijavo.php

<?php

session\_start();

$conn = mysqli\_connect("localhost", "root", "", "geodetskaUprava") or die("error");

$stmt = mysqli\_stmt\_init($conn);

if (!preg\_match("/^(?=.\*[0-9])(?=.\*[a-zA-Z])([a-zA-Z0-9]+)$/", $\_POST["geslo"])) {

echo 'Geslo mora vsebovati vsaj eno števko in eno črko';

}

$q = 'SELECT uIme FROM Uporabnik WHERE uIme = ? AND uGeslo = ?';

$g = sha1($\_POST["geslo"]);

mysqli\_stmt\_prepare($stmt, $q);

mysqli\_stmt\_bind\_param($stmt, "ss", $\_POST["uime"], $g);

mysqli\_stmt\_execute($stmt);

$rs = mysqli\_stmt\_get\_result($stmt);

$x = mysqli\_fetch\_all($rs);

if (count($x) > 0) {

$\_SESSION["uime"] = $\_POST["uime"];

header("location: glavna.php");

}

**Naloga 1-0**

Ustvarite program (skripto), ki bo omogočala dostop do naslednjih funkcij programa:

* Iskanje (Naloga1)
* Vnos stanovanja (Naloga2)
* Izpis (Naloga3)
* Odjava (logout)

glavna.php

<?php

session\_start();

if (!isset($\_SESSION["uime"])) {

header("location: prijava.php");

}

?>

<a href="iskanje.php">Iskanje</a><br>

<a href="vnos\_stan.php">Vnos stanovanja</a><br>

<a href="izpis.php">Izpis</a><br>

<a href="odjava.php">Odjava</a><br>

odjava.php

<?php

session\_start();

if (isset($\_SESSION["uime"])) {

unset($\_SESSION);

session\_destroy();

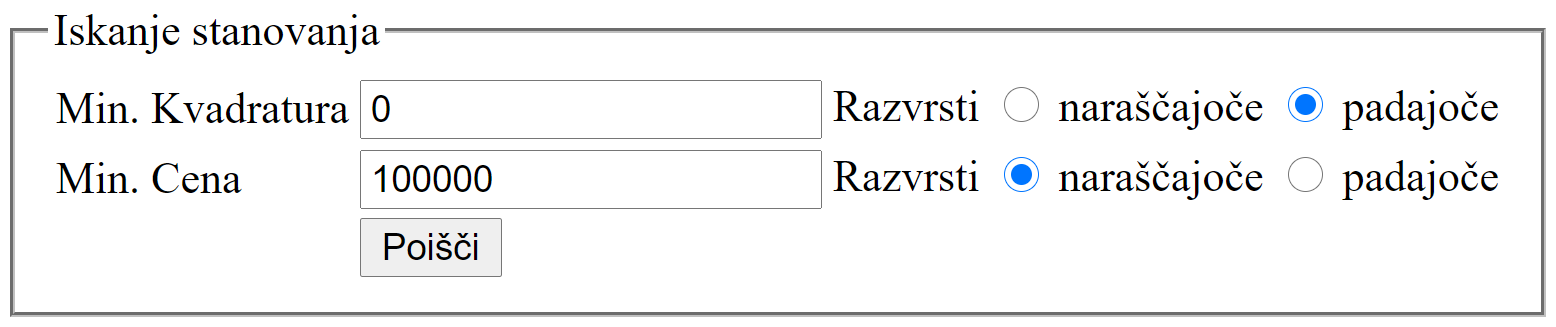
header("location: prijava.php");

}

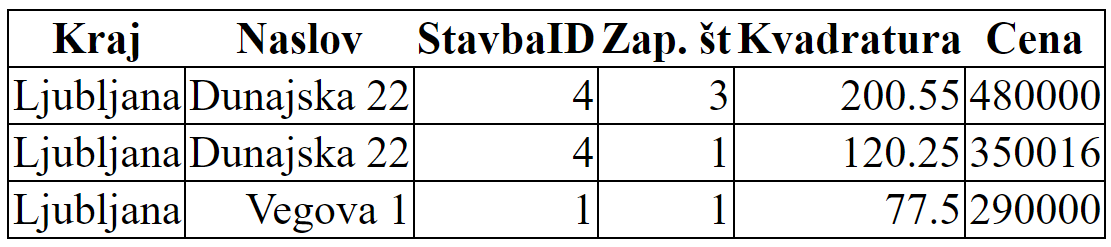
**Naloga 1-1**

Napišite program PHP, ki omogoča iskanje podatkov o stanovanjih. Kriterija za iskanje sta najmanjša zahtevana kvadratura in/ali najmanjša zahtevana vrednost. Hkrati uporabnik izbere smer sortiranja (naraščajoše/padajoče) posameznega kriterija. Prvi kriterij razvrščanja je kvadratura, drugi je cena stanovanja.

Zahtevana oblika vmesnika:



Nato se podatki izpišejo v tabelarični obliki, primer izpisa:



Testni PODATKI:

1. Min. kvadratura=0; min. cena =1; sortiranje naraščajoče
2. Min. kvadratura=100; min. cena=1; sortiranje padajoče po kvadraturi
3. V url dopiši SQL injection: select user,host,password,4,5,6 from mysql.user

iskanje.php

<?php

session\_start();

if (!isset($\_SESSION["uime"])) {

header("location: prijava.php");

}

?>

<form action="iskanjeRez.php" method="GET">

<fieldset style="display:inline-block">

<legend>Iskanje stanovanja</legend>

<div class="forma">

Min. kvadratura <input type="number" name="kvad" step="0.1" /> Razvrsti

<input type="radio" name="raz1" value="nar" checked /> naraščajoče

<input type="radio" name="raz1" value="pad" />

<div>padajoče</div>

Min. cena <input type="number" name="cena" step="0.1" /> Razvrsti

<input type="radio" name="raz2" value="nar" checked /> naraščajoče

<input type="radio" name="raz2" value="pad" /> padajoče

<input type="submit" value="Poišči" />

</div>

</fieldset>

</form>

<style>

.forma {

display: grid;

grid-template-columns: auto auto auto auto auto auto auto;

gap: 5px 10px;

}

</style>

iskanjeRez.php

<?php

session\_start();

if (!isset($\_SESSION["uime"])) {

header("location: prijava.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>';

if (!isset($\_GET["kvad"]) || !isset($\_GET["raz1"]) || !isset($\_GET["cena"]) || !isset($\_GET["raz2"])) return;

$conn = mysqli\_connect("localhost", "root", "", "geodetskaUprava") or die("error");

$stmt = mysqli\_stmt\_init($conn);

$q = 'SELECT s1.kraj, s1.naslov, s1.stavbaID, s2.Zap\_st, s2.Povrsina\_kvadrati, s2.vrednostStanovanja FROM stavba s1

INNER JOIN stanovanje s2 ON s1.StavbaID = s2.StavbaID

WHERE s2.VrednostStanovanja >= ? AND s2.Povrsina\_kvadrati >= ?

ORDER BY s2.Povrsina\_kvadrati';

if ($\_GET["raz1"] == "pad") $q = $q . ' DESC';

$q = $q . ', s2.VrednostStanovanja';

if ($\_GET["raz2"] == "pad") $q = $q . ' DESC';

mysqli\_stmt\_prepare($stmt, $q);

mysqli\_stmt\_bind\_param($stmt, "dd", $\_GET["cena"], $\_GET["kvad"]);

mysqli\_stmt\_execute($stmt);

$rs = mysqli\_stmt\_get\_result($stmt);

echo '<table>';

echo '<thead><td>Kraj</td><td>Naslov</td><td>StavbaID</td><td>Zap. št</td><td>Kvadratura</td><td>Cena</td></thead>';

while ($x = mysqli\_fetch\_assoc($rs)) {

echo '<tr><td>' . $x["kraj"] . '</td><td>' . $x["naslov"] . '</td><td>' . $x["stavbaID"] .

'</td><td>' . $x["Zap\_st"] . '</td><td>' . $x["Povrsina\_kvadrati"] . '</td><td>' . $x["vrednostStanovanja"] . '</td></tr>';

}

echo '</table>';

**Naloga 1-2**

V tabelo Stanovanje dodaj opcijski atribut zaupno varchar(60).

ALTER TABLE Stanovanje ADD zaupno VARCHAR(60);

Dopolni program za vnos podatkov o stanovanju ( 2. nalogo prejšnje vaje). Uporabnik lahko vnese tudi podatek zaupno (input type text). Če je podatek vpisan, ga je potrebno razpršiti z algoritmom bcrypt in razpršenega zapisati v bazo.

Vnesite testne podatke

1; 2; 30,00; 1; 100000,00; studio

1; 3; 50,00; 2; 120000,00; vikend

1; 4; 77,50; 0; 130000,00;

4; 5; 150,00; 0; 210000,00; vikend

Izpišite mysql shell zaslonsko sliko po izvedbi Stavka select \* from stanovanje;

vnos\_stan.php

<?php

session\_start();

if (!isset($\_SESSION["uime"])) {

header("location: prijava.php");

}

?>

<form action="vnos\_skripta.php" method="POST">

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 />

Zaupno: <input type="text" name="zaupno"><br />

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

</form>

vnos\_skripta.php

<?php

session\_start();

if (!isset($\_SESSION["uime"])) {

header("location: prijava.php");

}

$conn = mysqli\_connect("localhost", "root", "", "geodetskaUprava") or die("error");

$stmt = mysqli\_stmt\_init($conn);

if (!preg\_match("/^[1-9][0-9]\*$/", $\_POST["stavbaID"])) {

echo 'Prišlo je do napake, zapis NI dodan';

return;

}

if ($\_POST["stStan"] < 1) {

echo 'Prišlo je do napake, zapis NI dodan';

return;

}

if ($\_POST["povrsina"] < 1) {

echo 'Prišlo je do napake, zapis NI dodan';

return;

}

if ($\_POST["stOseb"] < 0) {

echo 'Prišlo je do napake, zapis NI dodan';

return;

}

if ($\_POST["vrednost"] < 1000) {

echo 'Prišlo je do napake, zapis NI dodan';

return;

}

if (isset($\_POST["zaupno"]) && $\_POST["zaupno"] != "") {

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

$zaupno = password\_hash($\_POST["zaupno"], PASSWORD\_BCRYPT);

mysqli\_stmt\_prepare($stmt, $q);

mysqli\_stmt\_bind\_param($stmt, "iidids", $\_POST["stavbaID"], $\_POST["stStan"], $\_POST["povrsina"], $\_POST["stOseb"], $\_POST["vrednost"], $zaupno);

mysqli\_stmt\_execute($stmt);

} else {

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

mysqli\_stmt\_prepare($stmt, $q);

mysqli\_stmt\_bind\_param($stmt, "iidid", $\_POST["stavbaID"], $\_POST["stStan"], $\_POST["povrsina"], $\_POST["stOseb"], $\_POST["vrednost"]);

mysqli\_stmt\_execute($stmt);

}

if (mysqli\_stmt\_affected\_rows($stmt) > 0) {

echo 'Zapis je dodan';

} else {

echo 'Prišlo je do napake, zapis NI dodan';

}

$q = 'UPDATE Stavba SET SteviloPrebivalcev = SteviloPrebivalcev + ? WHERE StavbaID = ?';

mysqli\_stmt\_prepare($stmt, $q);

mysqli\_stmt\_bind\_param($stmt, "ii", $\_POST["stOseb"], $\_POST["stavbaID"]);

mysqli\_stmt\_execute($stmt);

mysqli\_close($conn);

**Naloga 1-3**

Napišite program za izpis podatkov o stanovanjih. Uporabnik lahko (vendar ne nujno) vpiše vrednost atributa zaupno. Skripta izpiše podatke o stanovanjih, pri katerih je vrednost podatka zaupno bodisi NULL ali je enaka vpisani vrednosti na formi.

*Primeri*

Če uporabnik vpiše studio, dobi izpisane vrednosti vseh stanovanj, pri katerih je vrednost atributa zaupno studio ali NULL (od testnih podatkov dobi vse, razen vikend).

Če uporabnik ne vpiše vrednosti zaupno, dobi izpisane podatke le za tista stanovanja, pri katerih je vrednost podatka zaupno NULL.

izpis.php

<?php

session\_start();

if (!isset($\_SESSION["uime"])) {

header("location: prijava.php");

}

?>

<form action="izpisSkripta.php" method="post">

<fieldset style="display:inline-block">

<legend>Izpis Stanovanja</legend>

Zaupno: <input type="text" name="zaupno"><br />

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

</fieldset>

</form>

izpisSkripta.php

<?php

session\_start();

if (!isset($\_SESSION["uime"])) {

header("location: prijava.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");

$stmt = mysqli\_stmt\_init($conn);

$q = "SELECT \* FROM stanovanje";

mysqli\_stmt\_prepare($stmt, $q);

mysqli\_stmt\_execute($stmt);

$rs = mysqli\_stmt\_get\_result($stmt);

echo '<table><tr><td>StavbaID</td><td>Zap\_ST</td><td>Povrsina\_kvadrati</td><td>Prijavljenih</td><td>VrednostStanovanja</td></tr>';

while ($x = mysqli\_fetch\_assoc($rs)) {

if (!isset($x["zaupno"])) {

echo '<tr><td>' . $x["StavbaID"] . '</td><td>' . $x["Zap\_ST"] . '</td><td>' . $x["Povrsina\_kvadrati"] . '</td><td>' . $x["Prijavljenih"] . '</td><td>' . $x["VrednostStanovanja"] . '</td></tr>';

} else {

if (strlen($\_POST["zaupno"]) > 0 && password\_verify($\_POST["zaupno"], $x["zaupno"])) {

echo '<tr><td>' . $x["StavbaID"] . '</td><td>' . $x["Zap\_ST"] . '</td><td>' . $x["Povrsina\_kvadrati"] . '</td><td>' . $x["Prijavljenih"] . '</td><td>' . $x["VrednostStanovanja"] . '</td></tr>';

}

}

}

echo '</table>';

mysqli\_stmt\_close($stmt);

mysqli\_close($conn);

*Programe prekopirajte pod navodila posamezne naloge. V glavo poročila zapišite ime, priimek, razred in datum. Poročilo oddajte v nabiralnik. Skrajnji rok za oddajo poročila (do naloge 1-1) v nabiralnik spletne učilnice je takoj po izvedeni vaji, ostale naloge lahko oddate to naslednje vaje.*