# 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.

**//register.php**

<?php

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

function register()

{

*if* (!isset($\_POST["username"]) || !isset($\_POST["password"]))

*return*;

$mysqli = connect();

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

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

$stmt->bind\_param("ss", $\_POST["username"], sha1($\_POST["password"]));

$stmt->execute();

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

echo "registration failed";

*return*;

}

header("location: login.php");

}

?>

<form *action*="register.php" *method*="post">

<input *type*="text" *name*="username" *placeholder*="Username" *minlenght*="3" *required* /><br />

<input *type*="password" *name*="password" *placeholder*="Password" *minlenght*="3" *required* /><br />

<?php echo register() ?>

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

</form>

**//login.php**

<?php

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

function login()

{

*if* (!isset($\_POST["username"]) || !isset($\_POST["password"]))

*return*;

$mysqli = connect();

$query = "SELECT geslo status FROM Uporabnik WHERE uime = ?;";

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

$stmt->bind\_param("s", $\_POST["username"]);

$stmt->execute();

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

$user = $res->fetch\_row();

*if* (!$user || sha1($\_POST["password"]) !== $user["geslo"]) {

*return* ("wrong username or password");

}

session\_start();

$\_SESSION["username"] = $user["username"];

header("location: menu.php");

}

?>

<form *action*="login.php" *method*="post">

<input *type*="text" *name*="username" *placeholder*="Username" *minlenght*="3" *required* /><br />

<input *type*="password" *name*="password" *placeholder*="Password" *minlenght*="3" *required* /><br />

<?php echo login() ?>

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

</form>

**//logout.php**

<?php

session\_unset();

session\_destroy();

header("location: login.php");

**Naloga 0 – 1**

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

**// utils.php**

<?php

function connect() {

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

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

*exit*("prišlo je do napake pri povezavi do baze");

}

*return* $mysqli;

}

function check\_login() {

*if* (session\_status() === PHP\_SESSION\_NONE) {

header("location: login.php");

*exit*();

}

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

header("location: login.php");

*exit*();

}

echo '<a href="menu.php">Menu</a><br/>';

}

**Naloga 1-0**

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

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

**//menu.php**

<?php

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

check\_login();

?>

<ul>

<li><a *href*="iskanje.php">iskanje</a></li>

<li><a *href*="vnos.php">vnos</a></li>

<li><a *href*="izpis.php">izpis</a></li>

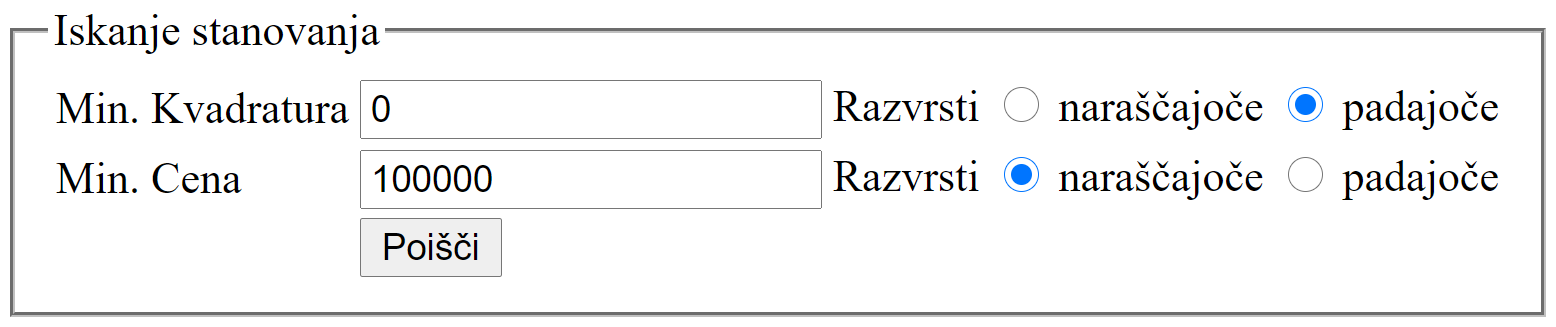
</ul><br />

<a *href*="logout.php">odjava</a>

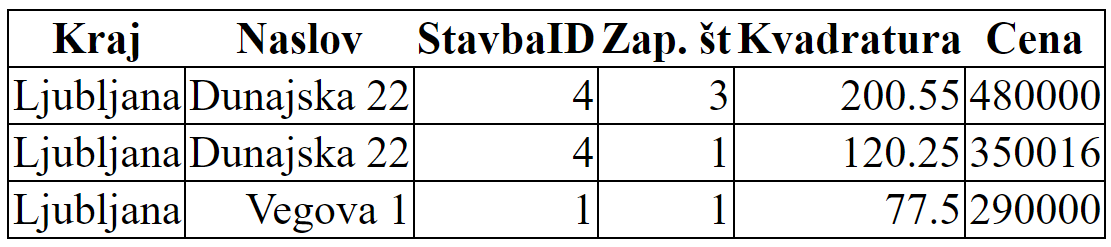
**Naloga 1-1**

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

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

check\_login();

function search()

{

*if* (!isset($\_GET["kvadratura"]) && !isset($\_GET["cena"]))

*return* null;

$mysqli = connect();

*if* (isset($\_GET["kvadratura"]) && isset($\_GET["cena"])) {

$where = "stan.kvadratura >= ? AND stan.cena >= ?";

} *else* *if* (isset($\_GET["kvadratura"])) {

$where = "stan.kvadratura >= ?";

} *else* *if* (isset($\_GET["cena"])) {

$where = "stan.cena >= ?";

}

$order\_options = ["asc", "desc"];

*if* (!in\_array($\_GET["sort\_kvadratura"], $order\_options) || !in\_array($\_GET["sort\_cena"], $order\_options))

*return* null;

$query = 'SELECT stav.kraj AS kraj, stav.naslov AS naslov, stav.stavbaid AS stavbaid,

stan.zap\_st AS zapst, stan.kvadratura AS kvadratura, stan.cena AS cena

FROM stanovanje stan

INNER JOIN stavba stav ON stav.stavbaid = stan.stavbaid

WHERE ' . $where . ' ORDER BY stav.kvadratura ' . $\_GET["sort\_kvadratura"] . ', stav.cena ' . $\_GET["sort\_cena"] . ';';

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

*if* (isset($\_GET["kvadratura"]) && isset($\_GET["cena"])) {

$stmt->bind\_param("ii", isset($\_GET["kvadratura"]), isset($\_GET["cena"]));

} *else* *if* (isset($\_GET["kvadratura"])) {

$stmt->bind\_param("i", isset($\_GET["kvadratura"]));

} *else* *if* (isset($\_GET["cena"])) {

$stmt->bind\_param("i", isset($\_GET["cena"]));

}

$stmt->execute();

*return* $stmt->get\_result();

}

?>

<fieldset>

<legend>Iskanje stanovanja</legend>

<form *action*="iskanje.php" *method*="get">

<label *for*="kvadratura">Min. Kvadratura</label>

<input *type*="number" *min*="0" *name*="kvadratura">

<label *for*="sort\_kvadratura">Razvrsti</label>

<input *type*="radio" *name*="sort\_kvadratura" *value*="asc" *required* />

<label *for*="asc">naraščajoče</label>

<input *type*="radio" *name*="sort\_kvadratura" *value*="desc" *required* />

<label *for*="desc">padajoče</label>

<br />

<label *for*="cena">Min. Cena</label>

<input *type*="number" *min*="0" *name*="cena">

<label *for*="sort\_cena">Razvrsti</label>

<input *type*="radio" *name*="sort\_cena" *value*="asc" *required* />

<label *for*="asc">naraščajoče</label>

<input *type*="radio" *name*="sort\_cena" *value*="desc" *required* />

<label *for*="desc">padajoče</label>

<br />

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

</form>

</fieldset>

<?php

$res = search();

*if* (!$res) {

*exit*();

}

?>

<table>

<thead>

<tr>

<th>Kraj</th>

<th>Naslov</th>

<th>StavbaID</th>

<th>Zap. št.</th>

<th>Kvadratura</th>

<th>Cena</th>

</tr>

</thead>

<tbody>

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

<tr>

<td><?= $row["kraj"] ?></td>

<td><?= $row["naslov"] ?></td>

<td><?= $row["stavbaid"] ?></td>

<td><?= $row["zapst"] ?></td>

<td><?= $row["kvadratura"] ?></td>

<td><?= $row["cena"] ?></td>

</tr>

<?php } ?>

</tbody>

</table>

**Naloga 1-2**

V tabelo Stanovanje dodaj opcijski atribut 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; 2; 50,00; 2; 120000,00; vikend

1; 3; 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.php

<?php

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

check\_login();

?>

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

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

<select *name*="stavba">

<?php

$mysqli = connect();

$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();

?>

<option *value*="1">hello</option>

</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 />

<label *for*="zaupno">Zaupno</label>

<input *type*="text" *maxlength*="60" *name*="zaupno" /> <br />

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

</form>

//shrani\_vnos.php

<?php

*require\_once*("vnos.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(

"iiiiis",

$data["stavba"],

$data["st\_stanovanja"],

$data["povrsina"],

$data["osebe"],

$data["vrednost"],

$data["zaupno"] ? password\_hash($data["zaupno"], PASSWORD\_DEFAULT) : null

);

$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 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

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

check\_login();

function izpis()

{

$mysqli = connect();

$zaupno\_where = "";

*if* (isset($\_POST["zaupno"])) {

$zaupno\_where = "OR zaupno = ?";

}

$query = "SELECT stavbaid, zap\_st, povrsina\_kvadrati, prijavljenih, vrednoststanovanja

FROM stavba

WHERE zaupno IS NULL $zaupno\_where

ORDER BY zap\_st ASC";

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

$stmt->bind\_param("s", password\_hash($\_POST["zaupno"], PASSWORD\_DEFAULT));

$stmt->execute();

*return* $stmt->get\_result();

}

?>

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

<input *type*="text" *name*="zaupno" *placeholder*="zaupno" />

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

</form>

<table>

<thead>

<tr>

<th>Kraj</th>

<th>Naslov</th>

<th>StavbaID</th>

<th>Zap. št.</th>

<th>Kvadratura</th>

<th>Cena</th>

</tr>

</thead>

<tbody>

<?php

$res = izpis();

*if* (!$res) {

*exit*();

}

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

<tr>

<td><?= $row["kraj"] ?></td>

<td><?= $row["naslov"] ?></td>

<td><?= $row["stavbaid"] ?></td>

<td><?= $row["zapst"] ?></td>

<td><?= $row["kvadratura"] ?></td>

<td><?= $row["cena"] ?></td>

</tr>

<?php } ?>

</tbody>

</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 (do naloge 1-1) v nabiralnik spletne učilnice je takoj po izvedeni vaji, ostale naloge lahko oddate to naslednje vaje.*