Aiken Tine Ahac, R4C, 12. 4. 2023

Spletne aplikacije Vaja 24

Teme:
Delo s PB:
- ***Zaščita pred SQL vdori***
- ***Obrazci, vnos podatkov, validacija podatkov***
- ***Razprševanje/preverjanje razpršene vrednosti***
- ***Povezovanje strani in zaščita dostopa***
- ***Testiranje***

Prenesite in namestite PB `GeodetskaUprava`, ki ste jo ustvarili z izvedbo 23. vaje. Baza ima nekaj testnih podatkov (če je prazna, ponovno izvedite vnose iz prejšnje vaje). 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, regularne izraze in seje

Naloga 1

V PB ustvarite še tabelo

`Uporabnik (imeUporabnika:A20, geslo:A100, datumRegistracije:D, ime:A10, priimek:A20, eMail:A20, datumZadnjegDostopa:D, stNeuspesnihPrijav:N)`

```sql
CREATE TABLE Uporabnik (
  imeUporabnika VARCHAR(20) PRIMARY KEY,
  geslo VARCHAR(100) NOT NULL,
  datumRegistracije DATE NOT NULL,
  ime VARCHAR(10) NOT NULL,
  priimek VARCHAR(20) NOT NULL,
  eMail VARCHAR(20) NOT NULL UNIQUE,
  datumZadnjegaDostopa DATE NOT NULL,
  stNeuspesnihPrijav INT NOT NULL
);
```

Napišite program PHP, ki omogoča registracijo uporabnika. Pri registraciji mora uporabnik upoštevati naslednje omejitve:

- dolžina gesla je vsaj 8 znakov, med znaki mora biti vsaj 1 mala črka, vsaj 1 velika črka in vsaj 1 števka;
- v imenu in priimku se lahko pojavijo le črke, ime in priimek morata imeti veliko začetnico.

Veljavnost podatkov preverite v brskalniku in v PHP skripti.

Geslo shranite v razpršeni obliki (lahko uporabite katerikoli razpršilni algoritem, priporoča se bcrypt, ki je obenem tudi default algoritem za razpršitev).

Datum registracije in datum zadnjeg dostopa nastavite na sistemski datum. Podatek stNeuspesnihPrijav naj bo 0. Podatek eMail je enoličen (2 uporabnika ne moreta imeti enak mail naslov).

Po uspešni registraciji izvedite preusmeritev uporabnika na prijavno stran.

registracija.php

```
<form method="POST" action="registracijaSkripta.php">
  Uporabniško ime: <input type="text" name="uime" required /><br />
  Ime: <input type="text" name="ime" pattern="[A-Z][a-zA-Z]+" required
/><br />
  Priimek: <input type="text" name="priimek" pattern="[A-Z][a-zA-Z]+"
required /><br />
  E-mail: <input type="email" name="email" required /><br />
  Geslo: <input type="password" name="geslo" minlength="8"
pattern="(?=.*[0-9])(?=.*[a-z])(?=.*[A-Z])([a-zA-Z0-9]+)*" required
/><br />

  <input type="submit" value="Registriraj se" />
</form>
```

registracijaSkripta.php

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

if (!preg_match("/^(?=.*[0-9])(?=.*[a-z])(?=.*[A-Z])([a-zA-Z0-
9]+)*$/", $_POST["geslo"]) || strlen($_POST["geslo"]) < 8) {
    echo 'Geslo mora vsebovati vsaj eno števko, eno veliko črko, eno
malo črko, dolžine vsaj 8 znakov';
    return;
}

if (!preg_match("/^[A-Z][a-zA-Z]+$/", $_POST["ime"])) {
```

```
    echo 'Ime lahko vsebuje le črke z veliko začetnico';
    return;
}

if (!preg_match("/^[A-Z][a-zA-Z]+$/", $_POST["priimek"])) {
    echo 'Priimek lahko vsebuje le črke z veliko začetnico';
    return;
}

$q = 'INSERT INTO Uporabnik VALUES (?, ?, ?, ?, ?, ?, ?, 0)';

$g = password_hash($_POST["geslo"], PASSWORD_BCRYPT);
$datum = date("Y-m-d");

try {
    mysqli_stmt_prepare($stmt, $q);
    mysqli_stmt_bind_param($stmt, "sssssss", $_POST["uime"], $g,
$datum, $_POST["ime"], $_POST["priimek"],  $_POST["email"], $datum);
    mysqli_stmt_execute($stmt);
} catch (mysqli_sql_exception $e) {
    echo 'Uporabniško ime ali email že obstaja<br/>';
}

if (mysqli_stmt_affected_rows($stmt) > 0) {
    echo 'Zapis je dodan';
    header("location: prijava.php");
} else {
    echo 'Prišlo je do napake, zapis NI dodan';
}
```

Naloga 2

Napišite program PHP, ki omogoča prijavo. Po uspešno izvedeni prijavi, uporabnika preusmerite na stran `meni.php`, ki ponuja 3 povezave:

- Iskanje stanovanja, s tem da določimo minimalno kvadraturo oz. ceno (naloga 2-1 prejšnje vaje),
- Iskanje stanovanj po kraju (funkcionalnost je potrebno realizirati; izpis stanovanj naj bo deljen na več strani – po 5 zapisov na stran) in
- Odjavo.

Dostop do strain meni.php in strain za iskanje zagotovite le registriranim uporabnikom, vse druge poizkuse preusmerite na prijavno stran.

Aiken Tine Ahac, R4C, 12. 4. 2023

Če uporabnik pri prijavi vnese napačne podatke in uporabniško ime obstaja, povečajte števec neuspešnih prijav za 1. Če (ko) števec doseže vrednost 6, naj uporabnik dobi obvestilo 'Vaš račun je blokiran, obrnite se na skrbnika sistema'. Od takrat naprej uporabnik (kljub morebitni pravilni prijavi) nima več dostopa do aplikacije. Če pa se uporabnik pravočasno 'spomni' pravega gesla, njegov števec neuspešnih poskusov ponastavite na 0.

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-z])(?=.*[A-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 številko in eno črko';
}

$q = 'SELECT imeUporabnika, geslo, stNeuspesnihPrijav FROM Uporabnik
WHERE imeUporabnika = ?';

mysqli_stmt_prepare($stmt, $q);
mysqli_stmt_bind_param($stmt, "s", $_POST["uime"]);
mysqli_stmt_execute($stmt);

$rs = mysqli_stmt_get_result($stmt);
$x = mysqli_fetch_assoc($rs);

if (count($x) > 0) {
    // user obstaja
    if ($x["stNeuspesnihPrijav"] >= 6) {
        echo 'Vaš račun je blokiran, obrnite se na skrbnika sistema.';
        return;
```

```
    }

    if (password_verify($_POST["geslo"], $x["geslo"])) {
        $q = 'UPDATE Uporabnik SET stNeuspesnihPrijav = 0';
        mysqli_stmt_prepare($stmt, $q);
        mysqli_stmt_execute($stmt);

        $_SESSION["uime"] = $_POST["uime"];
        header("location: meni.php");
    } else {
        // napacno geslo, user obstaja
        $q = 'UPDATE Uporabnik SET stNeuspesnihPrijav =
stNeuspesnihPrijav + 1';
        mysqli_stmt_prepare($stmt, $q);
        mysqli_stmt_execute($stmt);
    }
}
```

meni.php

```
<?php
session_start();

if (!isset($_SESSION["uime"])) {
  header("location: prijava.php");
}
?>

<a href="iskanje1.php">Iskanje po kvadraturi/ceni</a><br>
<a href="iskanje2.php">Iskanje po kraju</a><br>
<a href="odjava.php">Odjava</a><br>
```

iskanje1.php

```
<?php
session_start();

if (!isset($_SESSION["uime"])) {
  header("location: prijava.php");
}
?>
```

```
<form action="iskanje1Skripta.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>
```

iskanje1Skripta.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["stavbaI
D"].
```

```
'</td><td>'.$x["Zap_st"].'</td><td>'.$x["Povrsina_kvadrati"].'</td><td
>'.$x["vrednostStanovanja"].'</td></tr>';
}
echo '</table>';
```

iskanje2.php

```
<?php
session_start();

if (!isset($_SESSION["uime"])) {
  header("location: prijava.php");
}
?>
<form action="iskanje2Skripta.php" method="GET">
  <fieldset style="display:inline-block">
    <legend>Izpis Stanovanj</legend>
    Kraj:
    <select name="kraj">
      <?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 />
    <input type="submit" value="Izpis" />
  </fieldset>
</form>
```

Aiken Tine Ahac, R4C, 12. 4. 2023

iskanje2Skripta.php

```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") or
die("error");
$stmt = mysqli_stmt_init($conn);

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

if (isset($_GET["stran"])) $stran = $_GET["stran"];
else $stran = 1;

if ($stran < 1) $stran = 1;

$q = 'SELECT s2.StavbaID FROM Stavba s1
INNER JOIN Stanovanje s2 ON s1.StavbaID = s2.StavbaID
WHERE s1.Kraj = ?';

mysqli_stmt_prepare($stmt, $q);
mysqli_stmt_bind_param($stmt, "s", $_GET["kraj"]);
```

```php
mysqli_stmt_execute($stmt);

$rs = mysqli_stmt_get_result($stmt);
$stVseh = mysqli_num_rows($rs);

$stStrani = ceil($stVseh / 5);

if ($stran > $stStrani) $stran = $stStrani;

$offset = ($stran - 1)*5;

// tabela
$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 s1.Kraj = ?
LIMIT ?, 5';

mysqli_stmt_prepare($stmt, $q);
mysqli_stmt_bind_param($stmt, "si", $_GET["kraj"], $offset);
mysqli_stmt_execute($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["stavbaI
D"].

'</td><td>'.$x["Zap_st"].'</td><td>'.$x["Povrsina_kvadrati"].'</td><td
>'.$x["vrednostStanovanja"].'</td></tr>';
}
echo '</table>';
// konec tabele

echo '<div style="display:flex; gap: 20px;">';
if ($stran != 1) {
    echo '<a href="' . $_SERVER["PHP_SELF"] . '?kraj=' .$kraj .'&'
.'stran=1">prva</a>';
    echo '<a href="' . $_SERVER["PHP_SELF"] . '?kraj=' .$kraj .'&'
.'stran=' . $stran-1 . '">prejsnja</a>';
```

```
}

if ($stran != $stStrani) {
    echo '<a href="' . $_SERVER["PHP_SELF"] . '?kraj=' .$kraj .'&'
.'stran=' . $stran+1 . '">naslednja</a>';
    echo '<a href="' . $_SERVER["PHP_SELF"] . '?kraj=' .$kraj .'&'
.'stran=' . $stStrani . '">zadnja</a>';
}
echo '</div>';
?>
```

Naloga 3

Napišite skripto za varno odjavo. Ko se uporabnik odjavi, ga preusmerite nazaj na prijavno stran.

odjava.php

```
<?php
session_start();

if (isset($_SESSION["uime"])) {
    unset($_SESSION);
    session_destroy();
    header("location: prijava.php");
}
```

Rok za oddajo vaje je takoj po izvedeni vaji.
V poročilo prekopirajte kodo (PHP, HTML) in sliko rezultata (zaslonska slika izpisa).