Dokumentacija

Autor: Jovan Sekulic 298/16

Visoka ICT Skola

Sadrzaj

<head>

```
    <head>
        <title>TechStore</title>
        <meta charset="utf-8">
        <meta name="author" content="Jovan Sekulic">
        <meta name="keywords" content="" />
        <meta name="description" content="Online store for PC parts (not in
function, this is for show)" />
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width = device-width, initial-scale = 1">
        <link rel="icon" href="images/icon.png">
        <link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css"
integrity="sha384-
BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u"
crossorigin="anonymous">
        <link rel="stylesheet" type="text/css" href="css/style.css">
        <link rel="stylesheet" type="text/css" href="css/modal.css">
        <script src="https://code.jquery.com/jquery-3.3.1.min.js"
integrity="sha256-FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8="
crossorigin="anonymous"></script>
        <script
src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"
integrity="sha384-
Tc5IQib027qvyjSMfHjOMaLkfuWVxZxUPnCJA7l2mCWNIpG9mGCD8wGNIcPD7Txa"
crossorigin="anonymous"></script>
        <script src="js/functions.js"></script>
        <script src="js/modal.js"></script>
    </head>
```

Strana index.php

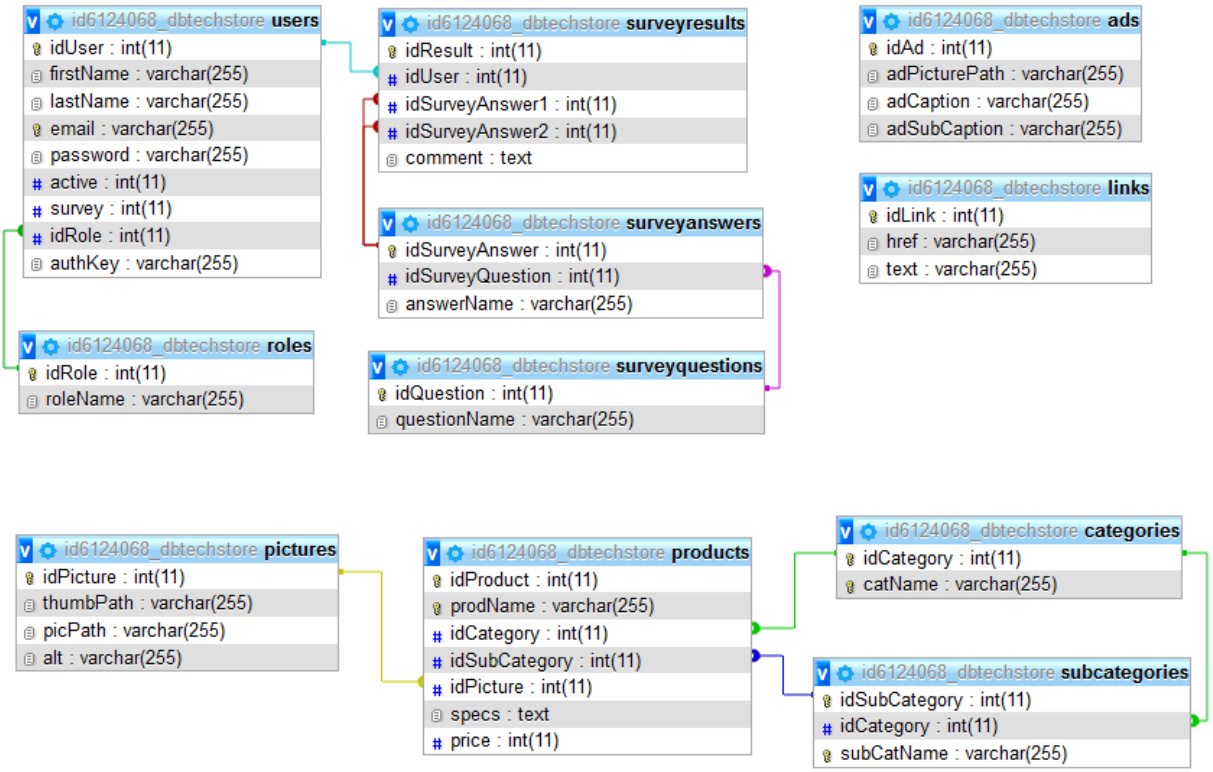
```
<?php

session_start();
if (isset($_GET['action'])&& $_GET['action']=="logout"){
    unset($_SESSION['user']);
}
include "php/connection.php";
include "php/functions.php";
include "php/login.php";
```

```php
include "php/validateKey.php";
include "php/contactAdmin.php";
if(isset($_SESSION['user']) && $_SESSION['user']->idRole == 1){
    include "php/adminTools.php";
}
include "php/cart.php";

include "views/header.php";
include "views/navigation.php";
include "views/ads.php";
if(isset($_GET['page'])){
    $page = $_GET['page'];
    if(isset($_SESSION['user'])){
        if($_SESSION['user']->idRole == 1){
            switch($page){
                case "list" : include "views/adminViews/list.php"; goto end;
                case "insert" : include "views/adminViews/insert.php"; goto end;
                case "surveyStats" : include "views/adminViews/surveyStats.php";
goto end;
                case "editProduct" : if(isset($_GET['id'])) {include
"views/adminViews/editProduct.php"; goto end;}
            }
        }
        switch($page){
            case "editUser": include "views/userViews/editUser.php"; goto end;
            case "survey" : if($_SESSION['user']->survey==0){include
"views/userViews/survey.php"; goto end;}
            case "cart" : if(isset($_SESSION['cart'])) {include
"views/userViews/cart.php"; goto end;}
        }
    }
    switch($page){
        case "register" : include "views/register.php"; goto end;
        case "contact" : include "views/contact.php"; goto end;
        case "about" : include "views/about.php"; goto end;
        case "productView" : if(isset($_GET['prodId'])) {include
"views/product.php"; goto end;}
        case "validation": if(isset($_SESSION['validateKey'])) {include
"views/validation.php"; goto end;}
        default: include_once "views/store.php";
    }
}
else include_once "views/store.php";
end: include "views/footer.php";
```

Struktura baze podataka



Login

```php
<?php

if(isset($_POST['btnLogin'])){
    $email=$_POST['tbEmail'];
    $password=$_POST['tbPasswd'];

    $errors = 0;

    if(!filter_var($email,FILTER_VALIDATE_EMAIL)){
        $_SESSION['emailerr']="Invalid e-mail address";
        $errors++;
    }
    else{
        unset($_SESSION['emailerr']);
    }

    $passwdTest = "/^(?=.*[a-z])(?=.*[A-Z])(?=.*[0-
9])(?=.*[!@#\$%\^&\*])(?=.{8,})/";

    if(!preg_match($passwdTest,$password)){
        $_SESSION['passwderr']="Invalid password";
        $errors++;
    }
    else{
        unset($_SESSION['passwderr']);
    }

    if($errors == 0){
        $query = "SELECT idUser, firstName, lastName, email, survey, idRole FROM
users WHERE email = :email AND password = SHA1(:password) AND active=1";
        $stmt = $con->prepare($query);
        $stmt->bindParam(":email",$email);
        $stmt->bindParam(":password",$password);
        try{
            $result = $stmt->execute();
            $user = $stmt->fetch();
            if($user){
                $_SESSION['user']=$user;
                unset($_SESSION['usrerr']);
            }
            else{
                $_SESSION['usrerr']="User doesn't exist.";
```

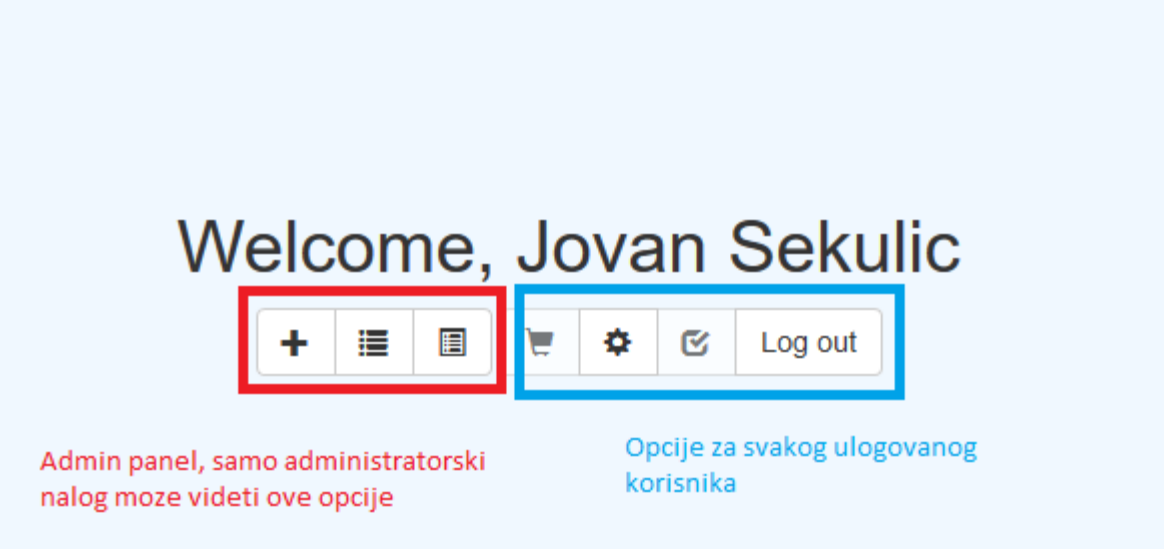
```
            }
        }
        catch(PDOException $ex){
            echo $ex->getMessage();
        }
    }
}
```

Logout

Nalazi se na pocetku koda index.php stranice

Prikaz sekcije za korisnika

Vizuelni prikaz



HTML kod za prikaz elemenata u zavisnosti da li je korisnik ulogovan ili ne

```
<div class="container">
            <div id="header" class="row">
                <div class="col-lg-6 col-md-6 col-sm-6 col-xs-12 text-center">
                    <img src="images/logo.png" alt="Site logo"></img>
                </div>
                <div id="userPanel" class="col-lg-6 col-md-6 col-sm-6 col-xs-12
text-center">
                    <?php
```

```
                        if(isset($_SESSION['user'])){
                            $user = $_SESSION['user'];
                            include "headerViews/userPanel.php";
                        }
                        else include "headerViews/loginForm.php";
                    ?>
                </div>
            </div>
```

HTML kod kada je korisnik ulogovan (userPanel.php)

```
<h1>Welcome, <?=$user->firstName?> <?=$user->lastName?></h1>
<?php if($user->idRole == 1): ?>
    <div class="btn-group" role="group">
        <a href="index.php?page=insert" data-toggle="tooltip" title="Add new
product, category or sub-category" class="btn btn-default glyphicon glyphicon
glyphicon-plus"></a>
        <a href="index.php?page=list" data-toggle="tooltip" title="List all
items" class="btn btn-default glyphicon glyphicon glyphicon glyphicon-list"></a>
        <a href="index.php?page=surveyStats" data-toggle="tooltip" title="List
survey results" class="btn btn-default glyphicon glyphicon glyphicon glyphicon-
list-alt"></a>
    </div>
<?php endif;?>
<div class="btn-group" role="group">
    <a href="index.php?page=cart" data-toggle="tooltip" title="View shopping
cart" class="btn btn-default glyphicon glyphicon-shopping-cart <?php
if(!isset($_SESSION['cart'])) echo "disabled"; ?>"></a>
    <a href="index.php?page=editUser" data-toggle="tooltip" title="Change
password" class="btn btn-default glyphicon glyphicon-cog"></a>
    <a href="index.php?page=survey" data-toggle="tooltip" title="Take survey"
class="btn btn-default glyphicon glyphicon-check <?php if($user->survey == 1)
echo "disabled";?>"></a>
    <a href="index.php?action=logout" class="btn btn-default" value="Log out">Log
out</a>
</div>
```

Navigacija

```
<div id="navigation">
    <ul class="nav nav-justified">
        <?php
            $resultSet = $con->query("SELECT * FROM links")->fetchAll();
            foreach($resultSet as $result):
        ?>
        <li class="nav-item">
            <a class="nav-link" href="<?=$result->href?>"><?=$result->text?></a>
        </li>
        <?php endforeach;?>
    </ul>
</div>
```

Dinamicka galerija

```
<div id="ads" class="carousel slide" data-ride="carousel">
    <?php
        $query="SELECT * FROM ads";
        $stmt=$con->prepare($query);
        try{
            $stmt->execute();
            $resultSet = $stmt->fetchAll();
            echo "<ol class='carousel-indicators'>";
            for($i=0; $i<count($resultSet); $i++){
                echo "<li data-target='#ads' data-slide-to='".$i."' ";
                if($i==0) echo "class='active'></li>";
                else echo "></li>";
            }
            echo "</ol>";
            echo "<div class='carousel-inner'>";
            for($i=0; $i<count($resultSet); $i++){
                if($i==0) echo "<div class='item active'>";
                else echo "<div class='item'>";
                echo "<div class='slide".$i."' style=\"background-image:
url('".$resultSet[$i]->adPicturePath."');\"></div>";
                echo "<div class='carousel-caption'><h1>".$resultSet[$i]-
>adCaption."</h1><p>".$resultSet[$i]->adSubCaption."</p></div>";
                echo "</div>";
            }
            echo "</div>";
        }
        catch(PDOException $ex){
            echo $ex->getMessage();
```

```
        }
    ?>
    <a class='left carousel-control' href='#ads' data-slide='prev'>
        <span class='glyphicon glyphicon-chevron-left'></span>
    </a>
    <a class='right carousel-control' href='#ads' data-slide='next'>
        <span class='glyphicon glyphicon-chevron-right'></span>
    </a>
</div>
```

CSS

```
[class*='slide']{
    height: 500px;
    background-repeat: no-repeat;
    background-position: center;
    background-size: cover;
}
.carousel-caption h1{
    font-size: 40px;
    font-family: Arial, Helvetica, sans-serif;
    padding-bottom: .4em;
}
.carousel-caption p{
    font-size: 2em;
}
```

Prodavnica

```
<div class="row">
    <div class="col-lg-12 col-md-12 col-sm-12 col-xs-12">
        <form action="index.php?page=store" method="POST" id="storeSearch">
            <div class="col-lg-3 col-md-3 col-sm-6 col-xs-6">
                <input type="text" id="tbSearchName" name="tbSearchName"
placeholder="Search by name" class="form-control"/>
            </div>
            <div class="col-lg-3 col-md-3 col-sm-6 col-xs-6">
                <select name="sCategory1" id="sCategory1" class="form-control">
                    <option value="0">Select category...</option>
                </select>
            </div>
            <div class="col-lg-3 col-md-3 col-sm-6 col-xs-6">
                <select name="sSubCategory1" id="sSubCategory1" class="form-
control"/>
                    <option value="0">Select sub-category...</option>
                </select>
```

```
            </div>
            <div class="col-lg-2 col-md-2 col-sm-6 col-xs-6">
                <select name="sSort" id="sSort" class="form-control">
                    <option value="prodName ASC">Name A-Z</option>
                    <option value="prodName DESC">Name Z-A</option>
                    <option value="price ASC">Price ascending</option>
                    <option value="price DESC">Price descending</option>
                </select>
            </div>
            <div class="col-lg-1 col-md-1 col-sm-2 col-xs-2">
                <input type="submit" class="btn btn-default" id="btnSearch"
name="btnSearch" value="Search"/>
            </div>
        </form>
    </div>
</div>
<div class="row" id="productView"></div>
```

Dinamicki prikaz proizvoda putem AJAX-a

```
if(!($("#productView").length === 0)){
    $.ajax({
        url: "php/storeSearch.php",
        method: "POST",
        dataType: "json",
        data: {
            storeSearch: 1,
        },
        success: function(data){
            fillStoreData(data);
        },
        error: function(xhr,statusText,error){
            alert(error);
            location.reload(true);
        }
    });
}
function fillStoreData(x){
    var products = "";
    for(var i=0; i<x.length; i++){
        products+="<div class='col-lg-4 col-md-4 col-sm-6 col-xs-12 text-center'
id='product'>";
        products+="<h1>"+x[i].prodName+"</h1>";
        products+="<h2>"+x[i].catName+" - "+x[i].subCatName+"</h2>";
        products+="<img src="+x[i].thumbPath+" alt="+x[i].alt+"/>";
        products+="<h3>$"+x[i].price+"</h3>";
```

```
        products+="<a href='index.php?page=productView&prodId="+x[i].idProduct+"'
class='btn btn-default'>View More</a>";
        products+="</div>";
    }
    $("#productView").html("");
    $("#productView").html(products);
}
```

Pretraga u zavisnosti od parametara

```
$("#storeSearch").submit(function(e){
    e.preventDefault();
    storeSearch();
});
function storeSearch(){
    var prodName=$("#tbSearchName").val();
    var idCategory=$("#sCategory1").val();
    var idSubCategory=$("#sSubCategory1").val();
    var sort=$("#sSort").val();
    $.ajax({
        url: "php/storeSearch.php",
        method: "POST",
        dataType: "json",
        data: {
            storeSearch: 1,
            searchFilters: 1,
            prodName: prodName,
            idCategory: idCategory,
            idSubCategory: idSubCategory,
            sort: sort,
        },
        success: function(data){
            if(!($("#productView").length === 0)) fillStoreData(data);
            else if(!($("#productTable").length === 0)) fillStoreDataTable(data);
        },
        error: function(xhr,statusText,error){
            alert("SQL Injection detected. The page will refresh.");
            location.reload(true);
        }
    });
}
```

storeSearch.php – Uzimanje proizvoda iz baze

```
if(isset($_POST['storeSearch'])){
```

```
    $query= "SELECT * FROM products INNER JOIN pictures ON
products.idPicture=pictures.idPicture INNER JOIN categories ON
products.idCategory=categories.idCategory INNER JOIN subcategories ON
products.idSubCategory=subcategories.idSubCategory";
    if(isset($_POST['searchFilters'])){
        if($_POST['prodName'] != "" || $_POST['idCategory'] != "0" ||
$_POST['idSubCategory'] != "0"){
            $query .= " WHERE ";
            $conditions = [];
            if($_POST['prodName'] != "") array_push($conditions,"prodName LIKE
(:prodName)");
            if($_POST['idCategory'] != "0") array_push($conditions,
"products.idCategory=(:idCategory)");
            if($_POST['idSubCategory'] != "0") array_push($conditions,
"products.idSubCategory=(:idSubCategory)");
            for($i=0;$i<count($conditions);$i++){
                $query .= $conditions[$i];
                if($i != count($conditions)-1) $query.=" AND ";
            }
        }
        switch($_POST['sort']){
            case "prodName ASC": $query.=" ORDER BY prodName ASC"; break;
            case "prodName DESC": $query.=" ORDER BY prodName DESC"; break;
            case "price ASC": $query.=" ORDER BY price ASC"; break;
            case "price DESC": $query.=" ORDER BY price DESC"; break;
            default: http_response_code(400); return;
        }
        $stmt = $con->prepare($query);
        if($_POST['prodName'] != ""){
            $prodName = "%".$_POST['prodName']."%";
            $stmt->bindParam(":prodName", $prodName);
        }
        if($_POST['idCategory'] != "0") $stmt->bindParam(":idCategory",
$_POST['idCategory']);
        if($_POST['idSubCategory'] != "0") $stmt->bindParam(":idSubCategory",
$_POST['idSubCategory']);
    }
    else {
        $stmt = $con->prepare($query);
    }
    try{
        $stmt->execute();
        $data = $stmt->fetchAll();
        echo json_encode($data);
    }
```

```
    catch(PDOException $ex){
        echo $ex->getMessage();
    }
}
```

Dinamicko popunjavanje kategorija i podkategorija preko AJAX-a

```
function fillCatOptions(x){
    $.ajax({
        url: "php/storeSearch.php",
        method: "POST",
        dataType: "json",
        data : {
            fillCategories : 1,
        },
        success: function(data){
            var options="<option value='0'>Select category...</option>";
            for(var i=0; i<data.length; i++){
                options+="<option
value="+data[i].idCategory+">"+data[i].catName+"</option>";
            }
            $(x).html(options);
        },
        error: function(xhr,statusText,error){
            alert(error);
        }
    });
}
```

```
$("#sCategory1").change(function(){
      fillSubCatOptions("#sSubCategory1");
});
function fillSubCatOptions(x){
    $.ajax({
        url: "php/storeSearch.php",
        method: "POST",
        dataType: "json",
        data : {
            idCategory: $("#sCategory1").val(),
            fillSubCategories : 1,
        },
        success: function(data){
            var options="<option value='0'>Select sub-category...</option>";
            for(var i=0; i<data.length; i++){
```

```
                options+="<option
value="+data[i].idSubCategory+">"+data[i].subCatName+"</option>";
            }
            $(x).html(options);
        },
        error: function(xhr,statusText,error){
            alert(error);
        }
    });
}
```

Dinamicko popunjavanje kategorija i podkategorija – storeSearch.php

```
if(isset($_POST['fillCategories'])){
    $query = "SELECT * FROM categories";
    $stmt = $con->prepare($query);
    try{
        $stmt->execute();
        $resultSet = $stmt->fetchAll();
        echo json_encode($resultSet);
    }
    catch(PDOException $ex){
        echo $ex->getMessage();
    }
}

if(isset($_POST['fillSubCategories'])){
    $idCategory=$_POST['idCategory'];

    $query = "SELECT * FROM subcategories WHERE idCategory=:idCategory";
    $stmt = $con->prepare($query);
    $stmt->bindParam(":idCategory",$idCategory);
    try{
        $stmt->execute();
        $resultSet = $stmt->fetchAll();
        echo json_encode($resultSet);
    }
    catch(PDOException $ex){
        echo $ex->getMessage();
    }
}
```

CSS za karticu proizvoda

```
#product{
    border: 1px solid aliceblue;
    box-shadow: 10px 10px 15px 0px aliceblue;
    height: 450px;
}
#product h2{
    font-size: 17px;
}
#product h3{
    position: absolute;
    bottom: 0;
    left: 0;
    margin: 20px;
}
#product a{
    position: absolute;
    bottom: 0;
    right: 0;
    margin: 20px;
}
```

Detaljan prikaz jednog proizvoda

```
<div class="row" id="productPage">
    <?php
        $idProduct= $_GET['prodId'];
        if(!is_nan($idProduct)){
            $query= "SELECT * FROM products INNER JOIN pictures ON
products.idPicture=pictures.idPicture INNER JOIN categories ON
products.idCategory=categories.idCategory INNER JOIN subcategories ON
products.idSubCategory=subcategories.idSubCategory WHERE idProduct = :idProduct";
            $stmt = $con->prepare($query);
            $stmt->bindParam(":idProduct", $idProduct);
            try{
                $stmt->execute();
                $product = $stmt->fetch();
                http_response_code(200);
            }
            catch(PDOException $ex){
                echo $ex->getMessage();
                http_response_code(400);
            }
        }
```

```
        else{
            echo "Invalid id";
            http_response_code(400);
        }
    ?>
    <div class="col-lg-4 col-md-4 col-s-12 col-xs-12">
        <img id="productImage" src="<?=$product->picPath?>" alt="<?=$product-
>alt?>">
    </div>
    <div class="col-lg-2 col-md-2 hidden-sm hidden-xs"></div>
    <div class="col-lg-6 col-md-6 col-s-12 col-xs-12">
        <table class="table table-striped table-hover">
            <tbody>
                <tr>
                    <td>Product ID:</td>
                    <th><?=$product->idProduct?></td>
                </tr>
                <tr>
                    <td>Product name:</td>
                    <th><?=$product->prodName?></td>
                </tr>
                <tr>
                    <td>Category:</td>
                    <th><?=$product->catName?></td>
                </tr>
                <tr>
                    <td>Sub-category:</td>
                    <th><?=$product->subCatName?></td>
                </tr>
                <tr>
                    <td>Specs:</td>
                    <th><p><?=$product->specs?></p></th>
                </tr>
                <tr>
                    <td>Price:</td>
                    <th>$ <?=$product->price?></th>
                </tr>
                <?php if(isset($_SESSION['user'])):?>
                <tr>
                    <td></td>
                    <td id="cartForm">
                        <?php
                            if(isset($_POST['btnAddToCart']))
array_push($_SESSION['cart'], $product);
```

```
                            if(!(isset($_SESSION['cart']) &&
in_array($product,$_SESSION['cart']))):
                        ?>
                        <form action="#" method='POST'>
                            <input type="submit" name="btnAddToCart" class="btn
btn-default" value="Add to cart"/>
                        </form>
                        <?php
                            endif;
                            if(isset($_SESSION['cart']) &&
in_array($product,$_SESSION['cart'])) echo "(Item in cart)";
                        ?>
                    </td>
                </tr>
                <?php endif; ?>
            </tbody>
        </table>
    </div>
    <div id="myModal" class="modal">
        <span class="close">&times;</span>
        <img class="modal-content" id="img01">
        <div id="caption"></div>
    </div>
</div>
```

Korpa

```
<div class="row">

    <div class="col-lg-12 col-md-12 col-s-12 col-xs-12">

        <table class="table table-striped table-hover" id="cartTable">

            <thead>

                <tr>

                    <th scope='col'>ID</th>

                    <th scope='col'>Product name</th>

                    <th scope='col'>Category</th>

                    <th scope='col'>Sub-category</th>

                    <th scope='col'>Price</th>

                    <th scope='col'>Options</th>
```

```
                </tr>
            </thead>
            <tbody>
                <?php foreach($_SESSION['cart'] as $product): ?>
                <tr>
                    <td><?=$product->idProduct?></td>
                    <td><?=$product->prodName?></td>
                    <td><?=$product->catName?></td>
                    <td><?=$product->subCatName?></td>
                    <td>$ <?=$product->price?></td>
                    <td>
                        <form action="#" method='POST'>
                            <input type="hidden" name="hiddenID"
value="<?=array_search($product,$_SESSION['cart'])?>">
                            <input type="submit" name="btnRemoveFromCart"
class="btn btn-default" value="Remove from cart"/>
                        </form>
                    </td>
                </tr>
                <?php endforeach; ?>
            </tbody>
        </table>
    </div>
</div>
```

Dodavanje i brisanje proizvoda iz korpe

```
<?php


if(isset($_POST['btnRemoveFromCart'])){
```

```php
    $id = $_POST['hiddenID'];

    unset($_SESSION['cart'][$id]);

    if(count($_SESSION['cart'])==0){

        unset($_SESSION['cart']);

    }

}



if(isset($_POST['btnAddToCart'])){

    if(!isset($_SESSION['cart'])) $_SESSION['cart'] = [];

//Sama dodaja proizvoda u korpu se vrsi u prikazu, posto su vec sve informacije o proizvodu ucitane


}
```

Registracija preko AJAX-a

```
<div class="row">
    <div class="col-lg-3 col-md-2 hidden-sm hidden-xs"></div>
    <div id="center" class="col-lg-6 col-md-8 col-sm-12 col-xs-12">
        <?php if(!isset($_SESSION['user'])):?>
        <form action="index.php?page=register" method="POST" id="register">
            <div class="input-group">
                <label for="firstName">First name:</label>
                <input type="text" name="tbFirstName" id="tbFirstName"
class="form-control"/>
            </div>
            <div class="input-group">
                <label for="lastName">Last name:</label>
                <input type="text" name="tbLastName" id="tbLastName" class="form-
control"/>
            </div>
            <div class="input-group">
                <label for="eMail">E-Mail address:</label>
                <input type="text" name="tbeMail" id="tbeMail" class="form-
control"/>
            </div>
            <div class="input-group">
                <label for="password">Password:</label>
                <input type="password" name="tbPassword" id="tbPassword"
class="form-control"/>
                <label for="password" id="warning"><span class="glyphicon
glyphicon-exclamation-sign"></span>Password must be at least 8 characters long
and have one upper and lower case letter, number and special sign</span>
            </div>
            <div class="input-group">
                <label for="password">Confirm password:</label>
                <input type="password" name="tbConfirm" id="tbConfirm"
class="form-control"/>
            </div>
            <div class="input-group buttons">
                <input type="reset" name="btnReset" id="btnReset" class="btn btn-
default" value="Reset fields"/>
                <input type="submit" name="btnRegister" id="btnRegister"
class="btn btn-default" value="Register"/>
            </div>
        </form>
        <?php
            endif;
            if(isset($_SESSION['user'])) echo "<h1>You are already registered and
logged in on this website.</h1>";
```

```
        ?>
    </div>
    <div class="col-lg-3 col-md-2 hidden-sm hidden-xs"></div>
</div>
```

Client-side validacija

```
$("#register").submit(function(e){
    e.preventDefault();
    register();
});
function register(){
    var firstName = $("#tbFirstName").val();
    var lastName = $("#tbLastName").val();
    var eMail = $("#tbeMail").val();
    var passwd = $("#tbPassword").val();
    var confirmPasswd = $("#tbConfirm").val();

    var errors = 0;

    var fnTest = new RegExp(/^[a-zčćđšž,.'-]+$/i);
    var lnTest = new RegExp(/^[a-zčćđšž ,.'-]+$/i);
    var emTest = new
RegExp(/^(([^<>()\[\]\\.,;:\s@"]+(\.[^<>()\[\]\\.,;:\s@"]+)*)|(".+"))@((\[[0-
9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}])|(([a-zA-Z\-0-9]+\.)+[a-zA-
Z]{2,}))$/);
    var pTest = new RegExp(/^(?=.*[a-z])(?=.*[A-Z])(?=.*[0-
9])(?=.*[!@#\$%\^&\*])(?=.{8,})/);

    if(!fnTest.test(firstName)){
        $("#tbFirstName").addClass("errField");
        $("#tbFirstName").val("");
        $("#tbFirstName").attr("placeholder", "Invalid first name");
        errors++;
    }
    else{
        $("#tbFirstName").removeClass("errField");
        $("#tbFirstName").attr("placeholder", "");
    }

    if(!lnTest.test(lastName)){
        $("#tbLastName").addClass("errField");
        $("#tbLastName").val("");
        $("#tbLastName").attr("placeholder", "Invalid last name");
        errors++;
    }
```

```
    else{
        $("#tbLastName").removeClass("errField");
        $("#tbLastName").attr("placeholder", "");
    }

    if(!emTest.test(eMail)){
        $("#tbeMail").addClass("errField");
        $("#tbeMail").val("");
        $("#tbeMail").attr("placeholder", "Invalid email");
        errors++;
    }
    else{
        $("#tbeMail").removeClass("errField");
        $("#tbeMail").attr("placeholder", "");
    }

    if(!pTest.test(passwd)){
        $("#tbPassword").addClass("errField");
        $("#tbPassword").val("");
        $("#tbConfirm").val("");
        $("#tbPassword").attr("placeholder", "Invalid password");
        errors++;
    }
    else{
        $("#tbPassword").removeClass("errField");
        $("#tbPassword").attr("placeholder", "");
    }

    if(passwd != confirmPasswd){
        $("#tbConfirm").addClass("errField");
        $("#tbPassword").val("");
        $("#tbConfirm").val("");
        $("#tbConfirm").attr("placeholder", "The passwords don't match");
        errors++;
    }
    else{
        $("#tbConfirm").removeClass("errField");
        $("#tbConfirm").attr("placeholder", "");
    }

    if(errors == 0){
        $.ajax({
            method : "POST",
            url : "php/register.php",
            data: {
```

```
                firstName: firstName,
                lastName: lastName,
                eMail: eMail,
                passwd : passwd,
                register : 1,
            },
            success: function(data){
                var success = "<h1>You have successfully regisered on this
website. Please cheek your e-mail to activate this account.</h1>";
                $("#center").html(success);
            },
            error: function(xhr, statusText, error){
                var status = xhr.status;
                switch(status){
                    case 409: {
                        $("#tbeMail").addClass("errField");
                        $("#tbeMail").val("");
                        $("#tbeMail").attr("placeholder", "An account is already
registered with this e-mail address");
                        break;
                    }
                    case 400: {
                        alert("Invalid user input. The page will refresh to start
again.");
                        location.reload(true);
                        break;
                    }
                }
            }
        });
    }
}
```

Server-side validacija i unos u bazu – register.php

```
<?php

if(isset($_POST['register'])){
    $firstName= $_POST['firstName'];
    $lastName = $_POST['lastName'];
    $eMail = $_POST['eMail'];
    $password = $_POST['passwd'];

    $fnTest = "/^[a-zčćđšž,.'-]+$/i";
    $lnTest = "/^[a-zčćđšž ,.'-]+$/i";
```

```
    $pTest = "/^(?=.*[a-z])(?=.*[A-Z])(?=.*[0-9])(?=.*[!@#\$%\^&\*])(?=.{8,})/";

    $errors = [];

    if(!preg_match($fnTest,$firstName)){
        array_push($errors, "Invalid first name.");
    }
    if(!preg_match($lnTest,$lastName)){
        array_push($errors, "Invalid last name.");
    }
    if(!filter_var($eMail,FILTER_VALIDATE_EMAIL)){
        array_push($errors, "Invalid e-mail address");
    }
    if(!preg_match($pTest,$password)){
        array_push($errors, "Invalid password.");
    }

    if(count($errors) == 0){
        include "connection.php";
        $query = "INSERT INTO users VALUES
('',:firstName,:lastName,:email,SHA1(:password),0,0,2,:authKey)";
        $stmt = $con->prepare($query);
        $stmt->bindParam(":firstName", $firstName);
        $stmt->bindParam(":lastName", $lastName);
        $stmt->bindParam(":email", $eMail);
        $stmt->bindParam(":password",$password);
        $key = md5(uniqid());
        $stmt->bindParam(":authKey",$key);

        try{
            $result = $stmt->execute();

            $subject = "TechStore - Activate account";
            $message =
"
Thanks for registering on TechStore website, ".$firstName."
Your account has been created, you can log in with the e-mail address and
password listed below:

Your e-mail: ".$eMail."
Your password: ".$password."

Please click the following link to activate your account.
http://localhost/TechStore/index.php?page=validation&key=".$key."
```

```
Admin of TechStore
";
            mail($eMail,$subject,$message);

            http_response_code(201);
        }
        catch(PDOException $ex){
            http_response_code(409);
        }
    }
    else{
        echo json_encode($errors);
        http_response_code(400);
    }
}
```

Promena lozinke preko AJAX-a

```
<div class="row">
    <div class="col-lg-3 col-md-2 hidden-sm hidden-xs"></div>
    <div id="center" class="col-lg-6 col-md-8 col-sm-12 col-xs-12">
        <form action="index.php?page=editUser" method="POST" id="editUser">
            <input type="hidden" id="email" name="email"
value="<?=$_SESSION['user']->email;?>">
            <div class="input-group">
                <label for="password">Old password:</label>
                <input type="password" name="tbOldPassword" id="tbOldPassword"
class="form-control"/>
            </div>
            <div class="input-group">
                <label for="password">New password:</label>
                <input type="password" name="tbPassword" id="tbPassword"
class="form-control"/>
                <label for="password" id="warning"><span class="glyphicon
glyphicon-exclamation-sign"></span>Password must be at least 8 characters long
and have one upper and lower case letter, number and special sign</span>
            </div>
            <div class="input-group">
                <label for="password">Confirm new password:</label>
                <input type="password" name="tbConfirm" id="tbConfirm"
class="form-control"/>
            </div>
            <div class="input-group buttons">
                <input type="reset" name="btnReset" id="btnReset" class="btn btn-
default" value="Reset fields"/>
```

```
                <input type="submit" name="btnUpdate" id="btnUpdate" class="btn
btn-default" value="Change password"/>
            </div>
        </form>
    </div>
    <div class="col-lg-3 col-md-2 hidden-sm hidden-xs"></div>
</div>
```

Client-side validacija

```
$("#editUser").submit(function(e){
    e.preventDefault();
    editUser();
});
function editUser(){
    var email = $("#email").val();
    var oldPasswd = $("#tbOldPassword").val();
    var newPasswd = $("#tbPassword").val();
    var confirmNewPasswd = $("#tbConfirm").val();

    var errors=0;

    var pTest = new RegExp(/^(?=.*[a-z])(?=.*[A-Z])(?=.*[0-
9])(?=.*[!@#\$%\^&\*])(?=.{8,})/);

    if(!pTest.test(oldPasswd)){
        $("#tbOldPassword").addClass("errField");
        $("#tbOldPassword").val("");
        $("#tbOldPassword").attr("placeholder", "Invalid password");
        errors++;
    }
    else{
        $("#tbOldPassword").removeClass("errField");
        $("#tbOldPassword").attr("placeholder", "");
    }

    if(!pTest.test(newPasswd)){
        $("#tbPassword").addClass("errField");
        $("#tbPassword").val("");
        $("#tbConfirm").val("");
        $("#tbPassword").attr("placeholder", "Invalid password");
        errors++;
    }
    else{
        $("#tbPassword").removeClass("errField");
        $("#tbPassword").attr("placeholder", "");
```

```
    }

    if(newPasswd != confirmNewPasswd){
        $("#tbConfirm").addClass("errField");
        $("#tbPassword").val("");
        $("#tbConfirm").val("");
        $("#tbConfirm").attr("placeholder", "The passwords don't match");
        errors++;
    }
    else{
        $("#tbConfirm").removeClass("errField");
        $("#tbConfirm").attr("placeholder", "");
    }

    if(errors == 0){
        $.ajax({
            url: "php/editUser.php",
            method: "POST",
            data: {
                email: email,
                oldPasswd: oldPasswd,
                newPasswd: newPasswd,
                editUser: 1,
            },
            success: function(data){
                var success = "<h1>You have successfully changed your password.
Please check your email to activate this account.</h1>";
                $("#center").html(success);
            },
            error: function(xhr, statusText, error){
                var status = xhr.status;
                switch(status){
                    case 409: {
                        $("#tbOldPassword").addClass("errField");
                        $("#tbOldPassword").val("");
                        $("#tbOldPassword").attr("placeholder", "Wrong
password");
                        break;
                    }
                    case 400: {
                        alert("Invalid user input. The page will refresh to start
again.");
                        location.reload(true);
                        break;
                    }
```

```
                }
            }
        });
    }
}
```

Server side promena lozinke

```
<?php

if(isset($_POST['editUser'])){
    $eMail= $_POST['email'];
    $oldPasswd= $_POST['oldPasswd'];
    $newPasswd= $_POST['newPasswd'];

    $pTest = "/^(?=.*[a-z])(?=.*[A-Z])(?=.*[0-9])(?=.*[!@#\$%\^&\*])(?=.{8,})/";

    $errors = [];

    if(!preg_match($pTest,$oldPasswd)){
        array_push($errors, "Invalid old password.");
    }
    if(!preg_match($pTest,$newPasswd)){
        array_push($errors, "Invalid new password.");
    }

    if(count($errors) == 0){
        include "connection.php";
        $query = "UPDATE users SET password=SHA1(:newPassword), active=0,
authKey=:authKey WHERE email=:eMail AND password=SHA1(:oldPassword)";
        $stmt = $con->prepare($query);
        $stmt->bindParam(":newPassword", $newPasswd);
        $key = md5(uniqid());
        $stmt->bindParam(":authKey",$key);
        $stmt->bindParam(":eMail", $eMail);
        $stmt->bindParam(":oldPassword", $oldPasswd);
        try{
            $res = $stmt->execute();
            if($stmt->rowCount()){
                $subject = "TechStore - Changed Password";
                $message =
"
You have succesfully changed your password,

Your new password is: ".$newPasswd.",
```

```
Please click the following link to activate your account:
http://localhost/TechStore/index.php?page=validation&key=".$key."

Admin of TechStore
";
                mail($eMail,$subject,$message);
                http_response_code(202);
            }
            else http_response_code(409);
        }
        catch(PDOException $ex){
            http_response_code(409);
        }
    }
    else{
        echo json_encode($errors);
        http_response_code(400);
    }
}
```

Aktivacija naloga

Nakon uspesne registracije ili promene lozinke, korisniku se salje na e-mail da se aktivira nalog

```
<?php

if(isset($_GET['key'])){
    $key = $_GET['key'];
    $query = "UPDATE users SET authKey=0, active=1 WHERE authKey= :authkey";
    $stmt = $con->prepare($query);
    $stmt->bindParam(":authkey",$key);
    try{
        $res = $stmt->execute();
        if($stmt->rowCount()){
            $_SESSION['validateKey']="You have successfully activated your
accout. You can now log in to our website.";
        }
        else{
            $_SESSION['validateKey']="Wrong authentication key";
        }
    }
    catch(PDOException $ex){
        $_SESSION['validateKey']=$ex->getMessage();
    }
}
```

Kontakt forma

Nakon uspesno popunjene forme, e-mail se salje administratoru sajta na techstorers@gmail.com

```
<div class="row">
    <div class="col-lg-3 col-md-2 hidden-sm hidden-xs"></div>
    <div id="center" class="col-lg-6 col-md-8 col-sm-12 col-xs-12">
        <?php if(!isset($_SESSION['contactAdmin'])):?>
        <form action="index.php?page=contact" method="POST">
            <div class="input-group">
                <label for="fullName">Full name:</label>
                <input type="text" name="tbFullName" id="tbFullName" class="form-
control" value="<?php if(isset($_SESSION['user'])) echo $_SESSION['user']-
>firstName." ".$_SESSION['user']->lastName;?>"/>
            </div>
            <div class="input-group">
                <label for="eMail">E-mail address:</label>
                <input type="text" name="tbEmail" id="tbEmail" class="form-
control" value="<?php if(isset($_SESSION['user'])) echo $_SESSION['user']-
>email;?>"/>
            </div>
            <div class="input-group">
                <label for="title">Title:</label>
                <input type="text" name="tbTitle" id="tbTitle" class="form-
control"/>
            </div>
            <div class="input-group">
                <label for="message" style="width:100%">Message:</label>
                <textarea type="text" name="taMessage" id="taMessage"
class="form-control" rows="7"></textarea>
            </div>
            <div class="input-group buttons">
                <input type="reset" name="btnReset" id="btnReset" class="btn btn-
default" value="Reset fields"/>
                <input type="submit" name="btnSend" id="btnSend" class="btn btn-
default" value="Send Message"/>
            </div>
        </form>
        <?php
            endif;
            if(isset($_SESSION['contactAdmin'])){
                if(is_array($_SESSION['contactAdmin'])){
                    echo "<h1><ul>";
```

```
                    foreach($_SESSION['contactAdmin'] as $sessionError){
                        echo "<li>".$sessionError."</li>";
                    }
                    echo "</ul></h1>";
                }
                else echo "<h1>".$_SESSION['contactAdmin']."</h1>";
                unset($_SESSION['contactAdmin']);
            }
        ?>
    </div>
    <div class="col-lg-3 col-md-2 hidden-sm hidden-xs"></div>
</div>
```

contactAdmin.php

```
<?php

if(isset($_POST['btnSend'])){
    $fullname = $_POST['tbFullName'];
    $eMail = $_POST['tbEmail'];
    $subject = $_POST['tbTitle'];
    $message = $_POST['taMessage'];

    $fnTest = "/^[a-zčćđšž ,.'-]+$/i";

    $errors = [];

    if(!preg_match($fnTest,$fullname)){
        array_push($errors,"Invalid name");
    }
    if(!filter_var($eMail,FILTER_VALIDATE_EMAIL)){
        array_push($errors,"Invalid e-mail address");
    }
    if($subject == ""){
        array_push($errors,"Title field is empty");
    }
    if($message == ""){
        array_push($errors,"Message field is empty");
    }

    if(count($errors) == 0){
        $admEmail="techstorers@gmail.com";
        $admSubject = "TechStore | Contact form - ".$subject;
        $admMessage =
"
Full name: ".$fullname."
```

```
E-mail address: ".$eMail."

".$message;
        mail($admEmail,$admSubject,$admMessage);

        $_SESSION['contactAdmin']="Your message has been successfully sent to the
administrator.";
    }
    else{
        $_SESSION['contactAdmin'] = [];
        foreach($errors as $error){
            array_push($_SESSION['contactAdmin'],$error);
        }
        array_push($_SESSION['contactAdmin'],"Please <a
href='index.php?page=contact'>refesh this page</a> to start again.");
    }
}
```

Anketa

```
<div class="row">
    <div class="col-lg-3 col-md-3 hidden-sm hidden-xs"></div>
    <div class="col-lg-6 col-md-6 col-sm-12 col-xs-12">
        <form action="#" method="POST" id="surveyFrom">
            <?php
                $query="SELECT * FROM surveyquestions";
                $stmt=$con->prepare($query);
                $stmt->execute();
                $resultSet=$stmt->fetchAll();
                foreach($resultSet as $result):
            ?>
            <div class="input-group">
                <label><?=$result->questionName?></label>
                <select name="<?=$result->idQuestion?>" id="<?=$result-
>idQuestion?>" class="form-control">
                    <option value="0">Select answer...</option>
                    <?php
                        $query2="SELECT * FROM surveyanswers WHERE
idSurveyQuestion = :idSurveyQuestion";
                        $stmt2=$con->prepare($query2);
                        $stmt2->bindParam(":idSurveyQuestion",$result-
>idQuestion);
                        $stmt2->execute();
                        $resultSet2=$stmt2->fetchAll();
                        foreach($resultSet2 as $result2):
```

```
                    ?>
                    <option value="<?=$result2->idSurveyAnswer?>"><?=$result2->answerName?></option>
                    <?php endforeach;?>
                </select>
            </div>
            <?php endforeach; ?>
            <div class="input-group">
                <label for="taComment" style="width:100%">Comment about this website (optional):</label>
                <textarea name="taComment" id="taComment" rows="5" class="form-control"></textarea>
            </div>
            <div class="input-group buttons">
                <input type="reset" name="btnReset" id="btnReset" class="btn btn-default" value="Reset fields"/>
                <input type="submit" name="btnSubmitSurvey" id="btnSubmitSurvey" class="btn btn-default" value="Submit results"/>
            </div>
        </form>
    </div>
    <div class="col-lg-3 col-md-3 hidden-sm hidden-xs"></div>
</div>
```

Validacija forme i slanje u bazu preko AJAX-a

```
$("#surveyFrom").submit(function(e){
    e.preventDefault();
    var answer1 = $("#1").val();
    var answer2 = $("#2").val();
    var comment = $("#taComment").val();

    var errors = 0;

    if(answer1 == 0){
        $("#1").addClass("errField");
        errors++;
    }
    else $("#1").removeClass("errField");
    if(answer2 == 0){
        $("#2").addClass("errField");
        errors++;
    }
    else $("#2").removeClass("errField");

    if(errors == 0){
```

```
        $.ajax({
            url: "php/submitSurvey.php",
            method: "POST",
            data: {
                answer1: answer1,
                answer2: answer2,
                comment: comment,
                submitSurvey: 1,
            },
            success: function (data) {
                alert("Successfully submited survey.");
                location.reload(true);
            },
            error: function(xhr,statusText,error){
                alert(xhr.responseText);
            }
        });
    }
});
```

Ubacivanje u bazu – submitSurvey.php

```
<?php
session_start();

if(isset($_POST['submitSurvey'])){
    include "connection.php";

    $idUser = $_SESSION['user']->idUser;
    $idSurveyAnswer1 = $_POST['answer1'];
    $idSurveyAnswer2 = $_POST['answer2'];
    $comment = $_POST['comment'];

    $errors = [];

    if($idSurveyAnswer1 == 0){
        array_push($errors,"Invalid answer 1");
    }
    if($idSurveyAnswer2 == 0){
        array_push($errors,"Invalid answer 2");
    }

    if(count($errors) == 0){
        $query="INSERT INTO surveyresults VALUES ('', :idUser, :idSurveyAnswer1,
:idSurveyAnswer2, :comment)";
        $stmt=$con->prepare($query);
```

```
        $stmt->bindParam(":idUser",$idUser);
        $stmt->bindParam(":idSurveyAnswer1",$idSurveyAnswer1);
        $stmt->bindParam(":idSurveyAnswer2",$idSurveyAnswer2);
        $stmt->bindParam(":comment",$comment);
        try{
            $res = $stmt->execute();
            if($res){
                $query2="UPDATE users SET survey=1 WHERE idUser = :idUser";
                $stmt2=$con->prepare($query2);
                $stmt2->bindParam(":idUser",$idUser);
                $stmt2->execute();
                $_SESSION['user']->survey = 1;
                http_response_code(201);
            }
        }
        catch(PDOException $ex){
            echo $ex->getMessage();
            http_response_code(409);
        }
    }
    else{
        var_dump($errors);
        http_response_code(400);
    }
}
```

Admin panel – Prikaz statistike ankete

```
<div class="row">
    <div class="col-lg-12 col-md-12 col-sm-12 col-xs-12">
        <table class="table table-striped table-hover">
            <thead>
                <tr>
                    <th scope='col'>Result ID</th>
                    <th scope='col'>Full name</th>
                    <th scope='col'><?=$con->query("SELECT questionName FROM
surveyquestions WHERE idQuestion=1")->fetch()->questionName?></th>
                    <th scope='col'><?=$con->query("SELECT questionName FROM
surveyquestions WHERE idQuestion=2")->fetch()->questionName?></th>
                    <th scope='col'>Comment</th>
                </tr>
            </thead>
            <tbody>
                <?php
                    $resultSet = $con->query("SELECT * FROM surveyresults INNER
JOIN users ON surveyresults.idUser=users.idUser")->fetchAll();
                    foreach($resultSet as $result):
                ?>
                <tr>
                    <td><?=$result->idResult?></td>
                    <td><?=$result->firstName." ".$result->lastName?></td>
                    <td><?=$con->query("SELECT answerName FROM surveyanswers
WHERE idSurveyAnswer=".$result->idSurveyAnswer1)->fetch()->answerName?></td>
                    <td><?=$con->query("SELECT answerName FROM surveyanswers
WHERE idSurveyAnswer=".$result->idSurveyAnswer2)->fetch()->answerName?></td>
                    <td><?=$result->comment?></td>
                </tr>
                <?php endforeach;?>
            </tbody>
        </table>
    </div>
</div>
```

Admin panel – ubacivanje kategorija, proizvoda i oglasa

```
<div class="row">
    <div class="col-lg-6 col-md-6 col-sm-12 col-xs-12">
        <h1>Insert category</h1>
        <form action="index.php?page=insert" method="POST" id="insertCat">
            <div class="input-group">
                <label for="tbCategory">Category name:</label>
                <input type="text" name="tbCategory" id="tbCategory" class="form-
control"/>
            </div>
            <div class="input-group buttons">
                <input type="reset" name="btnReset" id="btnReset" class="btn btn-
default" value="Reset fields"/>
                <input type="submit" name="btnInsertCat" id="btnInsertCat"
class="btn btn-default" value="Add category"/>
            </div>
        </form>
    </div>
    <div class="col-lg-6 col-md-6 col-sm-12 col-xs-12">
        <h1>Insert sub-category</h1>
        <form action="index.php?page=insert" method="POST" id="insertSubCat">
            <div class="input-group">
                <label for="sCategory">Category:</label>
                <select name="sCategory" id="sCategory" class="form-control">
                    <option value="0">Select...</option>
                </select>
            </div>
            <div class="input-group">
                <label for="tbSubCategory">Sub-category name:</label>
                <input type="text" name="tbSubCategory" id="tbSubCategory"
class="form-control"/>
            </div>
            <div class="input-group buttons">
                <input type="reset" name="btnReset" id="btnReset" class="btn btn-
default" value="Reset fields"/>
                <input type="submit" name="btnInsertSubCat" id="btnInsertSubCat"
class="btn btn-default" value="Add sub-category"/>
            </div>
        </form>
    </div>
</div>
<div class="row">
    <div class="col-lg-12 col-md-12 col-sm-12 col-xs-12">
        <h1>Insert product</h1>
```

```
        <form action="index.php?page=insert" method="POST" id="insertProduct"
enctype="multipart/form-data">
            <div class="input-group">
                <label for="tbProductName">Product name:</label>
                <input type="text" name="tbProductName" id="tbProductName"
class="form-control"/>
            </div>
            <div class="input-group">
                <label for="sCategory1">Category:</label>
                <select name="sCategory1" id="sCategory1" class="form-control">
                    <option value="0">Select category...</option>
                </select>
            </div>
            <div class="input-group">
                <label for="sSubCategory1">Sub-category:</label>
                <select name="sSubCategory1" id="sSubCategory1" class="form-
control"/>
                    <option value="0">Select sub-category...</option>
                </select>
            </div>
            <div class="input-group">
                <label for="tbPrice">Price:</label>
                <input type="text" name="tbPrice" id="tbPrice" class="form-
control"/>
            </div>
            <div class="input-group">
                <label for="taSpecs" style="width:100%">Specs:</label>
                <textarea name="taSpecs" id="taSpecs" rows="10" class="form-
control"></textarea>
            </div>
            <div class="input-group">
                <label for="fPicture">Picture:</label>
                <input type="file" id="fPicture" name="fPicture" class="form-
control-file"/>
            </div>
            <div class="input-group buttons">
                <input type="reset" name="btnReset" id="btnReset" class="btn btn-
default" value="Reset fields"/>
                <input type="submit" name="btnInsert" id="btnInsert" class="btn
btn-default" value="Add Product"/>
            </div>
        </form>
        <?php
            if(isset($_SESSION['insertProduct'])){
                echo "<h1>".$_SESSION['insertProduct']."</h1>";
```

```
                unset($_SESSION['insertProduct']);
            }
        ?>
    </div>
</div>
<div class="row">
    <div class="col-lg-12 col-md-12 col-sm-12 col-xs-12">
        <h1>Insert ad</h1>
        <form action="index.php?page=insert"  method="POST" id="insertAd"
enctype="multipart/form-data">
            <div class="input-group">
                <label for="tbCaption">Caption:</label>
                <input type="text" name="tbCaption" id="tbCaption" class="form-
control"/>
            </div>
            <div class="input-group">
                <label for="tbSubCaption">Sub-caption:</label>
                <input type="text" name="tbSubCaption" id="tbSubCaption"
class="form-control"/>
            </div>
            <div class="input-group">
                <label for="fPictureAd">Picture:</label>
                <input type="file" id="fPictureAd" name="fPictureAd" class="form-
control-file"/>
            </div>
            <div class="input-group buttons">
                <input type="reset" name="btnReset" id="btnReset" class="btn btn-
default" value="Reset fields"/>
                <input type="submit" name="btnInsertAd" id="btnInsertAd"
class="btn btn-default" value="Insert Ad"/>
            </div>
        </form>
        <?php
            if(isset($_SESSION['insertAd'])){
                echo "<h1>".$_SESSION['insertAd']."</h1>";
                unset($_SESSION['insertAd']);
            }
        ?>
    </div>
</div>
```

Ubacivanje kategorija i podkategorija preko AJAX-a

Client-side validacija i slanje serveru

```
$("#insertCat").submit(function(e){
    e.preventDefault();
    insertCategory();
});
$("#insertSubCat").submit(function(e){
    e.preventDefault();
    insertSubCategory();
});

function insertCategory(){
    var catName = $("#tbCategory").val();

    if(catName == ""){
        $("#tbCategory").addClass("errField");
        $("#tbCategory").attr("placeholder","This field is empty.");
    }
    else{
        $("#tbCategory").removeClass("errField");
        $("#tbCategory").attr("placeholder","");
        $.ajax({
            url: "php/adminTools.php",
            method: "POST",
            data: {
                catName: catName,
                insertCategory: 1,
            },
            success: function(data){
                alert("Category successfully added.");
                location.reload(true);
            },
            error: function(xhr,statusText,error){
                var status = xhr.status;
                $("#tbCategory").addClass("errField");
                switch(status){
                    case 400: $("#tbCategory").attr("placeholder","This field is
empty."); break;
                    case 409: $("#tbCategory").attr("placeholder","That category
already exists."); break;
                }
            }
        });
    }
```

```
}

function insertSubCategory(){
    var idCategory = $("#sCategory").val();
    var subCatName = $("#tbSubCategory").val();

    var errors=0;

    if(idCategory == "0"){
        $("#sCategory").addClass("errField");
        alert("Please select a category");
        errors++;
    }
    else{
        $("#sCategory").removeClass("errField");
    }

    if(subCatName == ""){
        $("#tbSubCategory").addClass("errField");
        $("#tbSubCategory").attr("placeholder","This field is empty.");
        errors++;
    }
    else{
        $("#tbSubCategory").removeClass("errField");
        $("#tbSubCategory").attr("placeholder","");
    }

    if(errors==0){
        $.ajax({
            url: "php/adminTools.php",
            method: "POST",
            data: {
                idCategory: idCategory,
                subCatName: subCatName,
                insertSubCategory: 1
            },
            success: function(data){
                alert("Sub-category successfully added.");
                location.reload(true);
            },
            error: function(xhr,statusText,error){
                var status = xhr.status;
                switch(status){
                    case 400: {
```

```
                        alert("Invalid user input, the page will refresh to start
again.");
                        location.reload(true);
                    }
                    case 409: {
                        $("#tbSubCategory").addClass("errField");
                        $("#tbSubCategory").val("");
                        $("#tbSubCategory").attr("placeholder","That sub-category
already exists.");
                        break;
                    }
                }
            }
        });
    }
}
```

Server-side validacija i ubacivanje u bazu

```
if(isset($_POST['insertCategory'])){
    $catName= $_POST['catName'];

    if($catName != ""){
        $query = "INSERT INTO categories VALUES ('',:catName)";
        $stmt = $con->prepare($query);
        $stmt->bindParam(":catName",$catName);

        try{
            $stmt->execute();
            http_response_code(201);
        }
        catch(PDOException $ex){
            http_response_code(409);
        }
    }
    else{
        http_response_code(400);
    }
}

if(isset($_POST['insertSubCategory'])){
    $idCategory = $_POST['idCategory'];
    $subCatName = $_POST['subCatName'];
```

```
    $errors=[];

    if(is_nan($idCategory)){
        array_push($errors, "Invalid category");
    }
    if($subCatName == ""){
        array_push($errors, "Field empty");
    }

    if(count($errors) == 0){
        $query = "INSERT INTO subcategories VALUES ('',:idCategory,:subCatName)";
        $stmt = $con->prepare($query);
        $stmt->bindParam(":idCategory",$idCategory);
        $stmt->bindParam(":subCatName",$subCatName);
        try{
            $stmt->execute();
            http_response_code(201);
        }
        catch(PDOException $ex){
            http_response_code(409);
        }
    }
    else{
        var_dump($errors);
        http_response_code(400);
    }
}
```

Validacija i ubacivanje proizvoda u bazu

```
if(isset($_POST['btnInsert'])){
    $prodName = $_POST['tbProductName'];
    $idCategory = $_POST['sCategory1'];
    $idSubCategory = $_POST['sSubCategory1'];
    $price = $_POST['tbPrice'];
    $specs = $_POST['taSpecs'];
    $picture = $_FILES['fPicture'];

    $fileName = $picture['name'];
    $fileType = $picture['type'];
    $tmpPath = $picture['tmp_name'];

    $errors = [];

    if($prodName == ""){
        array_push($errors,"<li>Invalid product name.</li>");
    }
    if($idCategory == 0){
        array_push($errors,"<li>Invalid category.</li>");
    }
    if($idSubCategory == ""){
        array_push($errors,"<li>Invalid sub-category</li>");
    }
    if(is_nan($price) || $price==""){
        array_push($errors,"<li>Invalid price.</li>");
    }
    if($specs == ""){
        array_push($errors,"<li>Specification field is empty.</li>");
    }
    $allowedFormats = array("image/jpg", "image/jpeg", "image/png", "image/gif");
    if(!in_array($fileType,$allowedFormats)){
        array_push($errors,"<li>The file is not an image</li>");
    }
    if(count($errors) == 0){
        $fileName=time().$fileName;
        $newPath="images/".$fileName;

        if(move_uploaded_file($tmpPath,$newPath)){
            $thumbPath="images/thumb_".$fileName;
            make_thumb($newPath,$thumbPath, 200);

            $picQuery = "INSERT INTO pictures VALUES
('',:thumbPath,:picPath,:alt)";
            $picStmt = $con->prepare($picQuery);
```

```
            $picStmt->bindParam(":thumbPath",$thumbPath);
            $picStmt->bindParam(":picPath",$newPath);
            $picStmt->bindParam(":alt",$prodName);

            try{
                $result = $picStmt->execute();
                if($result){
                    $idPicture=$con->lastInsertId();

                    $prodQuery= "INSERT INTO products VALUES
('',:prodName,:idCategory,:idSubCategory,:idPicture,:specs,:price)";
                    $prodStmt= $con->prepare($prodQuery);
                    $prodStmt->bindParam(":prodName",$prodName);
                    $prodStmt->bindParam(":idCategory",$idCategory);
                    $prodStmt->bindParam(":idSubCategory",$idSubCategory);
                    $prodStmt->bindParam(":idPicture",$idPicture);
                    $prodStmt->bindParam(":specs",$specs);
                    $prodStmt->bindParam(":price",$price);

                    try{
                        $prodStmt->execute();
                        $_SESSION['insertProduct']="You have successfully added a
product";
                    }
                    catch(PDOException $ex){
                        $_SESSION['insertProduct']=$ex->getMessage();
                    }
                }
            }
            catch(PDOException $ex){
                $_SESSION['insertProduct']=$ex->getMessage();
            }
        }
        else{
            $_SESSION['insertProduct']="Failed to upload image.";
        }
    }
    else{
        $_SESSION['insertProduct']="<ul>";
        foreach($errors as $error){
            $_SESSION['insertProduct'].=$error;
        }
        $_SESSION['insertProduct'].="</ul>";
        http_response_code(400);
    }
```

```
}
```

Ubacivanje oglasa u bazu

```
if(isset($_POST['btnInsertAd'])){
    $caption = $_POST['tbCaption'];
    $subCaption = $_POST['tbSubCaption'];
    $picture = $_FILES['fPictureAd'];

    $fileName = $picture['name'];
    $fileType = $picture['type'];
    $tmpPath = $picture['tmp_name'];

    $errors = [];

    if($fileName == ''){
        array_push($errors,"<li>File not selected</li>");
    }
    $allowedFormats = array("image/jpg", "image/jpeg", "image/png", "image/gif");
    if(!in_array($fileType,$allowedFormats)){
        array_push($errors,"<li>The file is not an image</li>");
    }
    if(count($errors) == 0){
        $fileName=time().$fileName;
        $newPath="images/".$fileName;

        if(move_uploaded_file($tmpPath,$newPath)){
            $query = "INSERT INTO ads VALUES
('',:adPicturePath,:adCaption,:adSubCaption)";
            $stmt=$con->prepare($query);
            $stmt->bindParam(":adPicturePath",$newPath);
            $stmt->bindParam(":adCaption",$caption);
            $stmt->bindParam(":adSubCaption",$subCaption);
            try{
                $stmt->execute();
                $_SESSION['insertAd']="Successfully inserted ad.";
            }
            catch(PDOException $ex){
                $_SESSION['insertAd']=$ex->getMessage();
            }
        }
        else{
            $_SESSION['insertAd']="Failed to upload image.";
        }
    }
    else{
```

```
        $_SESSION['insertAd']="<ul>";
        foreach($errors as $error){
            $_SESSION['insertAd'].=$error;
        }
        $_SESSION['insertAd'].="</ul>";
        http_response_code(400);
    }
}
```

Admin panel – listanje proizvoda i oglasa za brisanje i izmenu

```
<div class="row">
    <div class="col-lg-12 col-md-12 col-sm-12 col-xs-12">
        <form action="index.php?page=list" method="POST" id="storeSearch">
            <div class="col-lg-3 col-md-3 col-sm-6 col-xs-6">
                <input type="text" id="tbSearchName" name="tbSearchName"
placeholder="Search by name" class="form-control"/>
            </div>
            <div class="col-lg-3 col-md-3 col-sm-6 col-xs-6">
                <select name="sCategory1" id="sCategory1" class="form-control">
                    <option value="0">Select category...</option>
                </select>
            </div>
            <div class="col-lg-3 col-md-3 col-sm-6 col-xs-6">
                <select name="sSubCategory1" id="sSubCategory1" class="form-
control"/>
                    <option value="0">Select sub-category...</option>
                </select>
            </div>
            <div class="col-lg-2 col-md-2 col-sm-6 col-xs-6">
                <select name="sSort" id="sSort" class="form-control">
                    <option value="prodName ASC">Name A-Z</option>
                    <option value="prodName DESC">Name Z-A</option>
                    <option value="price ASC">Price ascending</option>
                    <option value="price DESC">Price descending</option>
                </select>
            </div>
            <div class="col-lg-1 col-md-1 col-sm-2 col-xs-2">
                <input type="submit" class="btn btn-default" id="btnSearch"
name="btnSearch" value="Search"/>
            </div>
        </form>
    </div>
</div>
<div id="productTable"></div>
```

```
<div id="adsTable"></div>
```

Popunjavanje tablele za proizvode i oglase putem AJAX-a

```
if(!($("#productTable").length === 0)){
    $.ajax({
        url: "php/storeSearch.php",
        method: "POST",
        dataType: "json",
        data: {
            storeSearch: 1,
        },
        success: function(data){
            fillStoreDataTable(data);
        },
        error: function(xhr,statusText,error){
            alert(error);
            location.reload(true);
        }
    });
}

if(!($("#adsTable").length === 0)){
    $.ajax({
        url: "php/storeSearch.php",
        method: "POST",
        dataType: "json",
        data: {
            searchAds: 1,
        },
        success: function(data){
            fillAdsTable(data);
        },
        error: function(xhr,statusText,error){
            alert(error);
            location.reload(true);
        }
    });
}

function fillStoreDataTable(x){
    var table="<table class='table table-striped table-hover'>";
    table+="<thead><tr>";
    table+="<th scope='col'>ID</th>";
    table+="<th scope='col'>Name</th>";
    table+="<th scope='col'>Category</th>";
```

```
    table+="<th scope='col'>Sub-category</th>";
    table+="<th scope='col'>Price</th>";
    table+="<th scope='col'>Options</th>";
    table+="</tr></thead>";
    table+="<tbody>";
    for(var i=0; i<x.length; i++){
        table+="<tr>";
        table+="<td scope='row' style='vertical-align:
middle;'>"+x[i].idProduct+"</td>";
        table+="<td style='vertical-align: middle;'>"+x[i].prodName+"</td>";
        table+="<td style='vertical-align: middle;'>"+x[i].catName+"</td>";
        table+="<td style='vertical-align: middle;'>"+x[i].subCatName+"</td>";
        table+="<td style='vertical-align: middle;'>"+x[i].price+"</td>";
        table+="<td>";
        table+="<div class='btn-group' role='group'>";
        table+="<a href='index.php?page=editProduct&id="+x[i].idProduct+"' data-
toggle='tooltip' title='Edit Product' class='btn btn-default glyphicon glyphicon-
pencil edit'></a>";
        table+="<button type='button' data-toggle='tooltip' title='Delete
Product' class='btn btn-default glyphicon glyphicon-trash delete'></button>";
        table+="</div>";
        table+="</td>";
        table+="</tr>";
    }
    table+="</tbody>";
    table+="</table>";
    $("#productTable").html("");
    $("#productTable").html("<h1>Products</h1>"+table);
}

function fillAdsTable(x){
    var table="<table class='table table-striped table-hover'>";
    table+="<thead><tr>";
    table+="<th scope='col'>ID</th>";
    table+="<th scope='col'>Caption</th>";
    table+="<th scope='col'>Sub-caption</th>";
    table+="<th scope='col'>Options</th>";
    table+="</tr></thead>";
    table+="<tbody>";
    for(var i=0; i<x.length; i++){
        table+="<tr>";
        table+="<td scope='row' style='vertical-align:
middle;'>"+x[i].idAd+"</td>";
        table+="<td style='vertical-align: middle;'>"+x[i].adCaption+"</td>";
        table+="<td style='vertical-align: middle;'>"+x[i].adSubCaption+"</td>";
```

```
        table+="<td>";
        table+="<button type='button' data-toggle='tooltip' title='Delete Ad'
class='btn btn-default glyphicon glyphicon-trash deleteAd'></button>";
        table+="</td>";
        table+="</tr>";
    }
    table+="</tbody>";
    table+="</table>";
    $("#adsTable").html("");
    $("#adsTable").html("<h1>Ads</h1>"+table);
}
```

storeSearch.php – Uzimanje oglasa iz baze

Funkcija za uzimanje proizvoda iz baze je vec definisana u dokumentaciji

```
if(isset($_POST['searchAds'])){
    $query="SELECT * FROM ads";
    $stmt=$con->prepare($query);
    try{
        $stmt->execute();
        $resultSet = $stmt->fetchAll();
        echo json_encode($resultSet);
    }
    catch(PDOException $ex){
        echo $ex->getMessage();
    }
}
```

Brisanje proizvoda i oglasa iz baze putem AJAX-a – client-side

```
$("body").on("click", ".delete", function(){
    var idProduct = $(this).parent().parent().parent().find(":first-
child").html();

    if(isNaN(idProduct)){
        alert("SQL injection detected. The page will reload.");
        location.reload(true);
    }
    else{
        $.ajax({
            url: "php/adminTools.php",
            method: "POST",
            data:{
                deleteProduct: 1,
                idProduct: idProduct,
            },
```

```
            success: function(data){
                alert("Successfully deleted product. The page will reload.");
                location.reload(true);
            },
            error: function(xhr,statusText,error){
                alert(error);
                location.reload(true);
            }
        });
    }
});
$("body").on("click", ".deleteAd", function(){
    var idAd = $(this).parent().parent().find(":first-child").html();
    console.log(idAd);

    if(isNaN(idAd)){
        alert("SQL injection detected. The page will reload.");
        location.reload(true);
    }
    else{
        $.ajax({
            url: "php/adminTools.php",
            method: "POST",
            data:{
                deleteAd: 1,
                idAd: idAd,
            },
            success: function(data){
                alert("Successfully deleted Ad. The page will reload.");
                location.reload(true);
            },
            error: function(xhr,statusText,error){
                alert(error);
                location.reload(true);
            }
        });
    }
});
```

Brisanje proizvoda i oglasa iz baze – server-side

```php
if(isset($_POST['deleteProduct'])){
    $idProduct = $_POST['idProduct'];

    if(is_nan($idProduct)){
        echo "SQL injection detected.";
        http_response_code(400);
    }
    else{
        $query1 = "SELECT * FROM pictures WHERE idPicture=(SELECT idPicture FROM
products WHERE idProduct = :idProduct)";
        $query2 = "DELETE FROM products WHERE idProduct = :idProduct";
        $stmt1=$con->prepare($query1);
        $stmt2=$con->prepare($query2);
        $stmt1->bindParam(":idProduct",$idProduct);
        $stmt2->bindParam(":idProduct",$idProduct);
        try{
            $stmt1->execute();
            $stmt2->execute();

            $pictureObj = $stmt1->fetch();
            $idPicture=$pictureObj->idPicture;
            $picPath="../".$pictureObj->picPath;
            $thumbPath="../".$pictureObj->thumbPath;
            unlink($picPath);
            unlink($thumbPath);
            $query3= "DELETE FROM pictures WHERE idPicture=:idPicture";
            $stmt3=$con->prepare($query3);
            $stmt3->bindParam(":idPicture",$idPicture);
            $stmt3->execute();

            http_response_code(200);
        }
        catch(PDOException $ex){
            echo $ex->getMessage();
            http_response_code(422);
        }
    }
}

if(isset($_POST['deleteAd'])){
    $idAd = $_POST['idAd'];

    if(is_nan($idAd)){
        echo "SQL injection detected.";
```

```
        http_response_code(400);
    }
    else{
        $query1="SELECT adPicturePath FROM ads WHERE idAd = :idAd";
        $stmt1=$con->prepare($query1);
        $stmt1->bindParam(":idAd",$idAd);
        try{
            $stmt1->execute();
            $path = $stmt1->fetch();
            $path = "../".$path->adPicturePath;
            $query2="DELETE FROM ads WHERE idAd = :idAd";
            $stmt2=$con->prepare($query2);
            $stmt2->bindParam(":idAd",$idAd);
            $stmt2->execute();
            unlink($path);
        }
        catch(PDOException $ex){
            echo $ex->getMessage();
            http_response_code(422);
        }
    }
}
```

Admin-panel izmena oglasa

```
<div class="row">
    <div class="col-lg-12 col-md-12 col-sm-12 col-xs-12">
        <form action="index.php?page=editProduct&id=<?=$_GET['id']?>"
method="POST" id="editProduct" enctype="multipart/form-data">
            <input type="hidden" id="hIdProduct" name="hIdProduct" value="">
            <div class="input-group">
                <label for="tbProductName">Product name:</label>
                <input type="text" name="tbProductName" id="tbProductName"
class="form-control"/>
            </div>
            <div class="input-group">
                <label for="sCategory1">Category:</label>
                <select name="sCategory1" id="sCategory1" class="form-control">
                    <option value="0">Select category...</option>
                </select>
            </div>
            <div class="input-group">
                <label for="sSubCategory1">Sub-category:</label>
                <select name="sSubCategory1" id="sSubCategory1" class="form-
control"/>
```

```
                    <option value="0">Select sub-category...</option>
                </select>
            </div>
            <div class="input-group">
                <label for="tbPrice">Price:</label>
                <input type="text" name="tbPrice" id="tbPrice" class="form-
control"/>
            </div>
            <div class="input-group">
                <label for="taSpecs" style="width:100%">Specs:</label>
                <textarea name="taSpecs" id="taSpecs" rows="10" class="form-
control"></textarea>
            </div>
            <div class="input-group">
                <label for="fPicture">Picture:</label>
                <input type="file" id="fPicture" name="fPicture" class="form-
control-file"/>
            </div>
            <div class="input-group buttons">
                <input type="reset" name="btnReset" id="btnReset" class="btn btn-
default" value="Reset fields"/>
                <input type="submit" name="btnUpdateProduct"
id="btnUpdateProduct" class="btn btn-default" value="Update Product"/>
            </div>
        </form>
        <?php
            if(isset($_SESSION['updateProduct'])){
                echo "<h1>".$_SESSION['updateProduct']."</h1>";
                unset($_SESSION['updateProduct']);
            }
        ?>
    </div>
</div>
```

Dinamicko popunjavanje forme putem AJAX-a – client-side

```
if(!($("#editProduct").length === 0)){
    var idProduct = window.location.href.split("id=")[1];

    if(!isNaN(idProduct)){
        $.ajax({
            url: "php/storeSearch.php",
            method: "POST",
            dataType: "json",
            data: {
                searchProductById: 1,
```

```
                idProduct: idProduct,
            },
            success: function(data){
                $("#hIdProduct").val(data.idProduct);
                $("#tbProductName").val(data.prodName);
                $("#sCategory1").val(data.idCategory);
                fillSubCatOptions("#sSubCategory1");
                $("#tbPrice").val(data.price);
                $("#taSpecs").val(data.specs);
            },
            error: function(xhr,statusText,error){
                alert(error);
            }
        });
    }
}
```

Dinamicko popunjavanje forme putem AJAX-a – server-side

```
if(isset($_POST['searchProductById'])){
    $idProduct= $_POST['idProduct'];
    if(!is_nan($idProduct)){
        $query= "SELECT * FROM products INNER JOIN pictures ON
products.idPicture=pictures.idPicture INNER JOIN categories ON
products.idCategory=categories.idCategory INNER JOIN subcategories ON
products.idSubCategory=subcategories.idSubCategory WHERE idProduct = :idProduct";
        $stmt = $con->prepare($query);
        $stmt->bindParam(":idProduct", $idProduct);
        try{
            $stmt->execute();
            $product = $stmt->fetch();
            echo json_encode($product);
            http_response_code(200);
        }
        catch(PDOException $ex){
            echo $ex->getMessage();
            http_response_code(400);
        }
    }
    else{
        echo "Invalid id";
        http_response_code(400);
    }
}
```

Izmena proizvoda – izvrsavanje promene u bazi

```
if(isset($_POST['btnUpdateProduct'])){
    $idProduct = $_POST['hIdProduct'];
    $prodName = $_POST['tbProductName'];
    $idCategory = $_POST['sCategory1'];
    $idSubCategory = $_POST['sSubCategory1'];
    $price = $_POST['tbPrice'];
    $specs = $_POST['taSpecs'];

    $errors = [];

    if($prodName == ""){
        array_push($errors,"<li>Invalid product name.</li>");
    }
    if($idCategory == 0){
        array_push($errors,"<li>Invalid category.</li>");
    }
    if($idSubCategory == ""){
        array_push($errors,"<li>Invalid sub-category.</li>");
    }
    if(is_nan($price) || $price==""){
        array_push($errors,"<li>Invalid price.</li>");
    }
    if($specs == ""){
        array_push($errors,"<li>Specification field is empty.</li>");
    }

    if(count($errors)==0){
        $query = "UPDATE products SET prodName=:prodName, idCategory=:idCategory,
idSubCategory=:idSubCategory, specs=:specs, price=:price WHERE
idProduct=:idProduct";
        $stmt = $con->prepare($query);
        $stmt->bindParam(":prodName",$prodName);
        $stmt->bindParam(":idCategory",$idCategory);
        $stmt->bindParam(":idSubCategory",$idSubCategory);
        $stmt->bindParam(":specs",$specs);
        $stmt->bindParam(":price",$price);
        $stmt->bindParam(":idProduct",$idProduct);
        try{
            $stmt->execute();
            if($stmt->rowCount()) $_SESSION['updateProduct']="Product update
successful.<br/>";
            else $_SESSION['updateProduct']="Product update failed - Nothing was
changed.<br/>";
        }
```

```
        catch(PDOException $ex){
            $_SESSION['updateProduct']=$ex->getMessage();
        }
    }
    else{
        $_SESSION['updateProduct']="<ul>";
        foreach($errors as $error){
            $_SESSION['updateProduct'].=$error;
        }
        $_SESSION['updateProduct'].="</ul>";
    }
    if($_FILES['fPicture']['name'] !=''){
        $picture = $_FILES['fPicture'];

        $fileName = $picture['name'];
        $fileType = $picture['type'];
        $tmpPath = $picture['tmp_name'];

        $allowedFormats = array("image/jpg", "image/jpeg", "image/png",
"image/gif");
        if(in_array($fileType,$allowedFormats)){
            $query1 = "SELECT * FROM pictures WHERE idPicture=(SELECT idPicture
FROM products WHERE idProduct=:idProduct)";
            $stmt1 = $con->prepare($query1);
            $stmt1->bindParam(":idProduct",$idProduct);
            try{
                $stmt1->execute();
                $pictureObj=$stmt1->fetch();

                $idPicture=$pictureObj->idPicture;
                $oldPicPath=$pictureObj->picPath;
                $oldThumbPath=$pictureObj->thumbPath;
                unlink($oldPicPath);
                unlink($oldThumbPath);

                $fileName=time().$fileName;
                $newPath="images/".$fileName;

                if(move_uploaded_file($tmpPath,$newPath)){
                    $thumbPath="images/thumb_".$fileName;
                    make_thumb($newPath,$thumbPath, 200);

                    $picQuery = "UPDATE pictures SET thumbPath=:thumbPath,
picPath=:picPath, alt=:alt WHERE idPicture=:idPicture";
                    $picStmt = $con->prepare($picQuery);
```

```
                    $picStmt->bindParam(":thumbPath",$thumbPath);
                    $picStmt->bindParam(":picPath",$newPath);
                    $picStmt->bindParam(":alt",$prodName);
                    $picStmt->bindParam(":idPicture",$idPicture);

                    $picStmt->execute();
                    if($picStmt->rowCount()){
                        $_SESSION['updateProduct'].="Image update
successful.<br/>";
                    }
                    else $_SESSION['updateProduct'].="Failed to change
image.<br/>";
                }
                else $_SESSION['updateProduct'].="Failed to upload image.<br/>";
            }
            catch(PDOException $ex){
                $_SESSION['updateProduct'].=$ex->getMessage();
            }
        }
        else $_SESSION['updateProduct'].="Invalid picture type.<br/>";
    }
}
```