**Dokumentace projektu**

**Wishlist**

**Stanislav Kovalchuk**

|  |  |
| --- | --- |
|  |  |

**Popis projektu**

Cílem je poskytnout registrovaným uživatelům možnost vytvořit si seznam přání, aby ostatní lidé věděli, jaký dárek mohou dát uživateli.

Stránky:

* Hlavní - seznámení s aplikací
* Přihlášení
* Registrace
* Seznam přání uživatele
* Stránka s formulářem pro přidání polohy
* Stránka s formulářem pro aktualizaci polohy
* Stránka s formulářem pro vyhledání uživatele podle jména
* Seznam přání vyhledávaného uživatele

Uživatelské role:

* Nepřihlášení uživatelé
* Přihlášení uživatelé

Funkce podle rolí:

* Nepřihlášení uživatelé mohou vyhledávat podle seznamů uživatelů, registrovat se, případně se přihlásit.
* Přihlášení uživatelé mohou přidávat položky do seznamu, upravovat, mazat položky, vyhledávat podle seznamů uživatelů a mohou označit dárek, který chtějí dát

**Standardní elementy stránek**

Záhlaví stránky

Header obsahuje:

* navigace
  + odkaz na hlavní stránku - “Home”
  + odkaz na přihlašovací stránku/ odkaz na odhlášení – “Log in/ Log out”
  + odkaz na seznam přání uživatele – “Wishlist”
* tlačítko pro změnu skina webu, jenom na hlavní stránce
* tlačítko pro vyhledávání uživatelů

## 

## Popis stránek

### Hlavní stránka

* Header
* Titulek
* Tlačítko s odkazem na stránku se seznamem přání:
* 3 uživatelské recenze
* Footer

### Stránka s seznamem přání uživatele

* Header
* Titulek
* Tlačítko pro přidání položky
* Tabulka obsahující přání - obsahuje sloupec s názvem, množství, datem, ke kterému uživatel chce dárek (uživatel nemusí nutně specifikovat datum). Každá položka obsahuje tlačítko pro úpravu a odstranění. Na každé stránce je celkem 5 řádků přání

**Stránka s formulářem pro přidání položky**

* Header
* Formulář pro přidání produktu

**Přihlášení**

* Header
* Přihlašovací formulář

**Registrace**

* Header
* Formulář pro registraci

**Stránka s formulářem pro vyhledání uživatele**

* Header
* Formulář pro vyhledání uživatele

**Seznamem přání vyhledávaného uživatele**

* Header
* Tabulka obsahující přání hledaného uživatele - obsahuje sloupec s uživatelským jménem, množstvím, datem, ke kterému chce uživatel dárek a sloupec pro rezervaci dárku. Bude možné označit dárek (pouze pro přihlášené uživatele), který chcete dát, aby uživatelé mohli vidět, který dárek je vybrán a který není). Na každé stránce je celkem 5 řádků přání.

**Formulary**

Tato část obsahuje informace o struktuře a funkčních vlastnostech formulářů.

**Přihlašovací formulář**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Element** | **Poznámka** | | Uživatelské jméno | Validace, minimálně 5 znaků | | Heslo | Validace, minimálně 8 znaků | | Tlačitko «Log in» |  | | Odkaz na registraci |  | |

Uživatel vyplní pole, klikne na tlačítko "Log in". Po kliknutí na tlačítko "Log in" jej přesměruji na stránku se seznamem.

**Formulář pro registraci**

|  |  |
| --- | --- |
| **Element** | **Poznámka** |
| Uživatelské jméno | Unikatní, minimálně 5 znaků |
| Heslo | Validace, minimálně 8 znaků |
| Potvrdit heslo | validace |
| Tlačitko «Sign up» |  |

**Formulář pro vyhledání uživatele**

|  |  |
| --- | --- |
| **Element** | **Poznámka** |
| Info | Jak najít seznam přání registrovaného uživatele |
| Uživatelské jméno |  |
| Tlačitko «Search» |  |

**Formulář pro přidání produktu**

|  |  |
| --- | --- |
| **Element** | **Poznámka** |
| Wish | Pole je povinné, maximálně 100 znaků |
| Count | Pole je povinné, minimální množství 1 |
| Date | Volitelné |
| Checkbox | Volitelné (splnit všechny požadavky) |
| Tlačitko «add item» |  |

**Akceptační podmínky**

Splnění všech podmínek technického zadání, správná práce ve všech prohlížečích (Chrome, Safari, Firefox), přizpůsobení mobilním telefonům.

**Uživatelská příručka**

Uživatelé, kteří nejsou přihlášeni, mohou najít seznam přání jiného uživatele kliknutím na tlačítko „Search“, budete přesměrováni na stránku s vyhledáváním, musíte vyplnit formulář. Pokud takový uživatel existuje, budete přesměrováni na stránku se seznamem přání:

 🡪 Изображение выглядит как текст

Автоматически созданное описание🡪 Изображение выглядит как стол

Автоматически созданное описание

Chcete-li se přihlásit, klikněte na tlačítko “Log in”, budete přesměrováni na přihlašovací stránku, pokud již nemáte účet, pomocí odkazu “Sign up”, budete přesměrováni na registrační stránku:

Изображение выглядит как текст

Автоматически созданное описание 🡪 Изображение выглядит как текст

Автоматически созданное описание

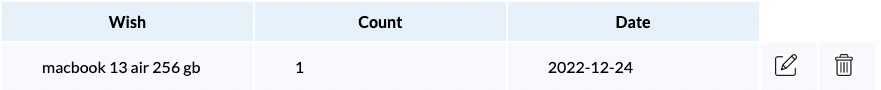
Při správném vyplnění vstupního pole se barva rámečku změní na zelenou. Jakmile se přihlásíte nebo se zaregistrujete, budete přesměrováni na stránku se seznamem přání. Chcete-li do seznamu přidat přání, klikněte na zelené tlačítko “add another item”, poté vyplňte formulář, nezapomeňte zadat název položky, množství, volitelně můžete určit datum, ke kterému chcete dárek:

Изображение выглядит как текст

Автоматически созданное описание 🡪 Изображение выглядит как текст

Автоматически созданное описание

Takto vypadá seznam přání. Na pravé straně má každá položka dvě tlačítka pro úpravy a odstranění:





Chcete-li položku upravit, klikněte na tlačítko - 

Chcete-li položku smazat, klikněte na tlačítko - 

Přihlášeni uživatelé mohou najít seznam přání jiného uživatele a mohou také označit položku, kterou by chtěli dát uživateli, za tímto účelem klikněte na odkaz "Click to reserve". Pro zrušení rezervace dárku klikněte na odkaz se svým uživatelským jménem:

Изображение выглядит как стол

Автоматически созданное описание

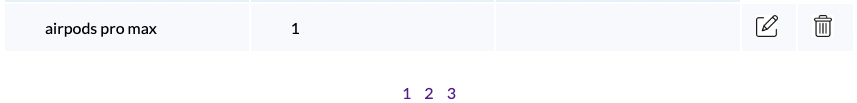
Изображение выглядит как стол

Автоматически созданное описание

Chcete-li změnit barevné téma webu, klikněte na tlačítko - .

Ve výchozím nastavení je barevné téma webu modrá, můžete ji také změnit na růžový

**Stránkování** - každá stránka může mít maximálně 5 řádků se zbožím, pod tabulkou je číslování stránek. Chcete-li přejít na požadovanou stránku, klikněte na její číslo





**Popis implementace**

Všechny formuláře jsou zpracovány v souborech ležících ve složce **main.**

**Registrace**

Při registraci jsou data z formuláře odeslána metodou POST do souboru main/registration.php. Pomocí funkce clean() ze souboru main/validation.php je pole s uživatelským jménem vymazáno ze značek html a php, speciální znaky jsou převedeny na entity HTML. Po ověření všech úvodních parametrů je heslo hashováno spolu s automaticky generovanou solí pomocí funkce password \_hash(). Pokud uživatel při registraci zadal již existující jméno, bude předán zpět na registrační stránku a požádán o výběr jiného jména. Pokud jsou všechny kontroly úspěšné, uživatel bude přidán do databáze, jeho uživatelské jméno a id jsou uloženy v Cookies a $\_SESSION[„session“] nastavuje hodnotu „active“. Jinak se zobrazí chybová zpráva.

**Přihlášení**

Při přihlášeníjsou data z formuláře odeslána metodou POST do souboru main/authorization.php. Pomocí funkce clean() ze souboru main/validation.php je pole s uživatelským jménem vymazáno ze značek html a php, speciální znaky jsou převedeny na entity HTML. Nejprve se zkontroluje, zda je uživatel se zadaným uživatelským jménem v databázi, poté zkontrolujte heslo pomocí funkce password\_verify(), která zkontroluje, zda heslo odpovídá hash v databázi. Pokud jsou všechny kontroly úspěšné, uživatel bude přesměrován na stránku se seznamem přání, jeho uživatelské jméno a id jsou uloženy v Cookies a $\_SESSION[„session“] nastavuje hodnotu „active“. Jinak se zobrazí chybová zpráva.

**Přidání položky**

Při přidání položky jsou data z formuláře odeslána metodou POST do souboru main/add.php. Pomocí funkce clean() ze souboru main/validation.php je pole s názvem položky vymazáno ze značek html a php, speciální znaky jsou převedeny na entity HTML. Pomocí dotazu sql zkontrolujeme jedinečnost položky, pokud je taková položka již v seznamu, zobrazí se chybová zpráva, pokud ne, pak po ověření správnosti tokenu CSRF se data přidají do databáze.

**Aktualizace položky**

Při aktualizacipoložky odešle id uživatele get parametrem do souboru update.php. Pomocí funkce clean() ze souboru main/validation.php je pole s názvem položky vymazáno ze značek html a php, speciální znaky jsou převedeny na entity HTML. Po ověření správnosti CSRF tokenu se zobrazí formulář pro aktualizaci položky. Dále jsou data z tohoto formuláře odesílána metodou POST do souboru main/update.php, ve kterém jsou aktualizovány v databázi. Jinak se zobrazí chybová zpráva.

**Odstranění položky**

Při odstraněnípoložky odešle id uživatele get parametrem do souboru main/delete.php. Po ověření správnosti CSRF tokenu odstraní položku z databáze. Jinak se zobrazí chybová zpráva.

**Vyhledání uživatele**

Při přidání položky jsou data z formuláře odeslána metodou POST do souboru main/search.php. Pomocí funkce clean() ze souboru main/validation.php je pole se jménem vymazáno ze značek html a php, speciální znaky jsou převedeny na entity HTML. Pokud je uživatel se zadaným uživatelským jménem v databázi, jeho jméno se uloží do Cookie a předá se do souboru searchPage.php, který vytiskne tabulku s přáním uživatele. Jinak se zobrazí chybová zpráva. Přihlášený uživatel nemůže hledat svůj seznam.

**Rezervace položky**

Kliknutím na odkaz “Click to reserve“ get parametrem předán do souboru main/book\_gift.рһр **id** položky, kterou chce uživatel označit, pokud není uživatel zaregistrován nebo přihlášen, bude mu nabídnuto přihlášení, jinak bude do databáze zadáno uživatelské jméno a zobrazeno ve sloupci

“Reserved by“.

**Zrušení rezervace zboží**

Chcete-li zrušit rezervaci dárku, klikněte na své jméno v tabulce ve sloupci „Reserved by“ naproti požadované položce. Kliknutím na odkaz get parametrem předán do souboru main/cancelReservation.рһр **id** položky, rezervace kterou chce uživatel zrušit. Poté bude jméno odstraněno z pole databázové tabulky

**Zabezpečení**

Heslo je hashováno spolu se solí pomocí funkce password\_hash(). Proti útokům XSS se používají funkce trim(), stripslashes(), strip\_tags(), htmlspecialchars(). Ochrana proti CSRF se provádí pomocí CSRF tokenu.

**Zpracování dat**

Při přihlášení je **id** uživatele a jeho **uživatelské jméno** přidáno do Сookies. Kliknutím na tlačítko se změnou motivu "Switch" se nová hodnota motivu uloží do Cookies. Při provádění formuláře pro vyhledání seznamu uživatelů, jméno hledaného uživatele je uložen do Cookies. Hodnota sezení „aktivní“ a „neaktivní“ uloženo do session. Uživatelské jméno, jeho heslo a jeho položky, rezervace dárků pro ostatní uživatele jsou uloženy v databázi MySQL. Veškerá práce s daty se provádí pomocí dotazů s příkazy select, insert, update, delete.