Dokumentáció

GypoWinery

konzulens tanár: Készítette:

Dobrocsi Róbertné Gábor Bence, Majzik Bence, Gellértfy Tamás Imre

Képek:

Bevezetés

A Gypo Winery egy modern és elegáns borászat, amely a legkiválóbb borok kínálatával várja a látogatókat. Az oldal letisztult dizájnnal és reszponzív megjelenítéssel készült, hogy minden eszközön kényelmes böngészést biztosítson. A felhasználók számára különleges funkciók, például egyedi menük és sötét mód teszik még élvezetesebbé az élményt.

A index.php fájl egy PHP-alapú weboldal kezdőlapja, amely a Gypo Winery nevű weboldal megjelenítéséért felelős. Az oldal betöltéséhez külső konfigurációs fájlt (index\_config.php) importál, majd HTML és CSS segítségével kialakítja a vizuális megjelenést.

**Főbb elemek:**

* **Fejléc (head)**:
  + A karakterkódolás UTF-8.
  + A reszponzivitás érdekében beállított viewport.
  + Az oldal címe: Gypo Winery.
  + Betölt több CSS fájlt, köztük a Bootstrap framework legújabb verzióját, egyedi stíluslapokat (style.css, user-menu.css, darkmode.css).
* **Külső fájlok használata**:
  + Az index\_config.php tartalmazhat konfigurációs beállításokat, például adatbáziskapcsolatokat vagy egyéb környezeti változókat.

## login.php

Ez a dokumentum a login.php fájl működését ismerteti. A szkript egy egyszerű bejelentkezési rendszert valósít meg, amely ellenőrzi a felhasználók hitelesítését egy MySQL adatbázisban.

## 2. Működés részletesen

### 2.1 Session indítás

A session segítségével a rendszer megjegyzi a bejelentkezett felhasználót:

session\_start();

### 2.2 Adatbázis kapcsolat

A szkript egy MySQL adatbázishoz csatlakozik a bejelentkezéshez:

$servername = "localhost";  
$username = "root";  
$password = "";  
$dbname = "gypowinery";  
$conn = new mysqli($servername, $username, $password, $dbname);  
  
if ($conn->connect\_error) {  
    die("Connection failed: " . $conn->connect\_error);  
}

* A mysqli osztály használatával csatlakozik az adatbázishoz.
* Ha a kapcsolat sikertelen, a szkript kilép egy hibaüzenettel.

### 2.3 Felhasználó adatainak ellenőrzése

A bejelentkezési adatok POST módszerrel érkeznek:

$email = $\_POST['email'];  
$jelszo = $\_POST['jelszo'];

A megadott email cím alapján a felhasználó adatait az adatbázisból lekéri:

$sql = "SELECT \* FROM login WHERE email = '$email'";  
$result = $conn->query($sql);

### 2.4 Jelszó ellenőrzés

Ha a felhasználó létezik, a megadott jelszót ellenőrizzük:

if ($result->num\_rows > 0) {  
    $row = $result->fetch\_assoc();  
    if (password\_verify($jelszo, $row['jelszo'])) {  
        $\_SESSION['user\_id'] = $row['id'];  
        echo "Sikeres bejelentkezés!";  
    } else {  
        echo "Hibás jelszó!";  
    }  
}

* **password\_verify()**: Ellenőrzi a titkosított jelszót.
* Ha helyes, a felhasználó ID-ja session-be kerül.
* Ha helytelen, hibaüzenet jelenik meg.

## 3. Hibakezelés

* **Session kezelés**: session\_start() biztosítja, hogy az adatok megőrzésre kerüljenek.
* **SQL injection elleni védelem**: Jelenleg nincs **prepared statement** használva, ami biztonsági kockázatot jelent.
* **Jelszóbiztonság**: A password\_hash() használata javasolt az adatbázisban történő tároláshoz.

boraink.php

A boraink.php fájl felelős a borok listázásáért és azok kosárba helyezéséért a Gypo Winery weboldalon. A fájl az adatbázisból lekérdezi a borokat és a hozzájuk tartozó képeket egy SQLJOIN művelet segítségével. Az adatokat egy PDO-alapú lekérdezés kezeli, amely az borok és bor\_kepek táblákból nyeri ki az információkat.

További funkcióként a fájl lehetőséget biztosít a borok kosárba helyezésére. Ha a felhasználó egy bort szeretne a kosarába tenni, a rendszer ellenőrzi, hogy az adott bor már szerepel-e benne. A vásárlási adatok kezelése PHP session változókon keresztül történik, amely lehetővé teszi a felhasználói élmény gördülékeny fenntartását.

**Főbb funkciók:**

* Borok adatbázisból történő lekérdezése és megjelenítése
* Borokhoz tartozó képek betöltése
* Kosárba helyezési funkció session alapú kezeléssel
* Adatbáziskapcsolat a config2.php fájlon keresztül

Kviz.php

A Kviz.php fájl egy kvízoldalt biztosít a Gypo Winery weboldal számára, amely interaktív módon teszteli a felhasználók borokkal kapcsolatos tudását. Az oldal a config2.php fájlon keresztül kapcsolódik az adatbázishoz, és Bootstrap-alapú stílusokat használ a reszponzív megjelenítéshez.

A kvíz működéséhez egy külső JavaScript fájl (kviz.js) is betöltődik, amely valószínűleg az interaktív kérdés-válasz logikát kezeli. A felhasználói élmény fokozására az oldal támogatja a sötét módot, és tartalmaz egyedi stílusokat a user-menu.css és style.css fájlokból.

**Főbb funkciók:**

* Kvízkérdések megjelenítése a felhasználók számára
* Bootstrap és egyedi CSS segítségével reszponzív dizájn
* Külső JavaScript fájl biztosítja az interaktív funkciókat
* Adatbáziskapcsolat a config2.php fájlon keresztül

# add\_to\_cart.php

## Áttekintés

Ez a fájl egy PHP szkript, amely egy webshop kosárkezelő funkcióját biztosítja. A felhasználók hozzáadhatnak termékeket a kosarukhoz, és ha a termék már szerepel benne, akkor frissíti annak mennyiségét.

## Főbb Funkciók

### 1. Konfiguráció Betöltése

A fájl betölti a **config.php** fájlt, amely feltételezhetően az adatbázis-kapcsolatot és egyéb beállításokat tartalmazza:

include 'config.php';

### 2. Felhasználói Bejelentkezés Ellenőrzése

A szkript ellenőrzi, hogy a felhasználó be van-e jelentkezve. Ha nem, akkor JSON formátumban egy hibát ad vissza és kilép a végrehajtásból:

if (!isset($\_SESSION['user\_id'])) {

echo json\_encode(["error" => "Nincs bejelentkezve."]);

exit;

}

### 3. Bejövő Adatok Feldolgozása

A következő változók a **POST kéréssel érkeznek**, és a felhasználó azonosítóját, a kiválasztott termék azonosítóját és a hozzáadni kívánt mennyiséget tárolják:

$user\_id = $\_SESSION['user\_id'];

$bor\_id = $\_POST['bor\_id']; // Termék ID

$quantity = $\_POST['quantity']; // Mennyiség

### 4. Kosár Ellenőrzése

A rendszer ellenőrzi, hogy az adott termék már szerepel-e a kosárban:

$stmt = $pdo->prepare("SELECT \* FROM cart WHERE user\_id = :user\_id AND bor\_id = :bor\_id");

$stmt->execute(['user\_id' => $user\_id, 'bor\_id' => $bor\_id]);

$item = $stmt->fetch();

### 5. Termék Hozzáadása vagy Frissítése

* **Ha a termék már létezik**, akkor az új mennyiséget a meglévő mennyiséghez adja hozzá:

if ($item) {

$stmt = $pdo->prepare("UPDATE cart SET quantity = quantity + :quantity WHERE user\_id = :user\_id AND bor\_id = :bor\_id");

$stmt->execute(['quantity' => $quantity, 'user\_id' => $user\_id, 'bor\_id' => $bor\_id]);

* **Ha a termék még nincs a kosárban**, akkor egy új bejegyzést hoz létre az adatbázisban:

} else {

$stmt = $pdo->prepare("INSERT INTO cart (user\_id, bor\_id, quantity) VALUES (:user\_id, :bor\_id, :quantity)");

$stmt->execute(['user\_id' => $user\_id, 'bor\_id' => $bor\_id, 'quantity' => $quantity]);

}

### 6. Válasz Küldése a Kliensnek

A szkript végül egy JSON választ küld vissza a frontend számára:

echo json\_encode(["success" => "Termék sikeresen hozzáadva a kosárhoz."]);

## Használati Útmutató

* A szkript **AJAX POST kéréseket** vár a kosárkezeléshez.
* A felhasználónak be kell jelentkeznie, ellenkező esetben a művelet sikertelen lesz.
* Az adatbázisnak tartalmaznia kell egy **cart** nevű táblát a következő oszlopokkal:
  + id (elsődleges kulcs)
  + user\_id (felhasználó azonosító)
  + bor\_id (termék azonosító)
  + quantity (darabszám)

## Fejlesztési Javaslatok

* **Hibakezelés fejlesztése**: Érdemes részletesebb hibaüzeneteket küldeni és naplózni a hibákat.
* **SQL injekció elleni védelem**: Bár a **PDO prepared statement** használata már biztonságos, érdemes további validálásokat végezni a bemeneti adatokon.
* **Kosár összegző funkció**: Egy külön endpoint implementálható a kosár tartalmának lekérdezésére és összegzésére.

Ez a szkript egy alapvető, de jól használható kosárkezelő megoldás egy webshop számára.

# config2.php

## Áttekintés

Ez a fájl egy PHP konfigurációs szkript, amely adatbázis-kapcsolatot kezel, valamint felhasználói munkameneteket indít. Az adatbázis eléréséhez **PDO (PHP Data Objects)** interfészt használ, amely biztonságos és rugalmas módja az SQL adatbázisok kezelésének.

## Főbb Funkciók

### 1. Munkamenet Kezelés

A fájl elején található az alábbi kód:

session\_start();

Ez elindítja a **PHP munkamenetet (session)**, amely lehetővé teszi az adatok tárolását a felhasználók között történő navigáció során.

### 2. Adatbázis Kapcsolat Beállításai

Az adatbázis eléréséhez a következő változók vannak meghatározva:

$host = 'localhost';

$dbname = 'gypowinery';

$username = 'root';

$password = '';

Ezek a beállítások határozzák meg az adatbázis elérhetőségét.

### 3. Adatbázis Kapcsolódás PDO-val

A fájl egy **try-catch blokkot** használ a biztonságos adatbázis-kapcsolat létrehozásához és a hibák kezeléséhez:

try {

$pdo = new PDO("mysql:host=$host;dbname=$dbname;charset=utf8", $username, $password);

$pdo->setAttribute(PDO::ATTR\_ERRMODE, PDO::ERRMODE\_EXCEPTION);

$pdo->setAttribute(PDO::ATTR\_DEFAULT\_FETCH\_MODE, PDO::FETCH\_ASSOC);

} catch (PDOException $e) {

die("Kapcsolódási hiba: " . $e->getMessage());

}

* **PDO objektum létrehozása**: Az adatbázis kapcsolatot a **PDO** osztály kezeli.
* **Hibakezelés**: Ha a kapcsolat sikertelen, a szkript leáll és kiírja a hibát.
* **Attribútumok beállítása**:
  + ERRMODE\_EXCEPTION: Az esetleges hibák kivételt generálnak, amelyet kezelni lehet.
  + FETCH\_ASSOC: Az adatokat asszociatív tömbként adja vissza.

### 4. Bejelentkezés Ellenőrzése

A fájl egy bejelentkezési ellenőrzési részt is tartalmazhat, amely a munkamenetben tárolt felhasználói adatok alapján azonosítja a bejelentkezett felhasználót.

## Használati Útmutató

* Győződj meg róla, hogy a **MySQL adatbázis fut**, és a **beállított hitelesítő adatok helyesek**.
* Ha jelszót használ az adatbázishoz, állítsd be a megfelelő értéket a **$password** változóban.
* A kapcsolódási hibák elkerülése érdekében ellenőrizd, hogy a megfelelő **PHP PDO kiterjesztés** engedélyezve van a szerveren.

## 1. Bevezetés

Ez a dokumentum a boraink.php fájl funkcionalitását ismerteti. A szkript egy adatbázisból kinyeri a borokat, megjeleníti azokat a felhasználónak, valamint kezeli a kosárba helyezés funkciót.

## 2. Működés részletesen

### 2.1 Borok listázása

A szkript egy **SQL-lekérdezést** hajt végre a borok és a hozzájuk tartozó képek lekérdezésére:

$query = "SELECT borok.\*, bor\_kepek.kep\_url FROM borok LEFT JOIN bor\_kepek ON borok.ID = bor\_kepek.bor\_id";

$stmt = $pdo->query($query);

$borok = $stmt->fetchAll(PDO::FETCH\_ASSOC);

**borok.\***: A borok minden adatát lekéri.

**LEFT JOIN bor\_kepek**: A borokhoz tartozó képeket csatolja.

**fetchAll(PDO::FETCH\_ASSOC)**: Az eredményt asszociatív tömbként adja vissza.

### 2.2 Kosár kezelés

Amikor a felhasználó egy bort a kosárba helyez, a következő folyamat történik:

Az űrlapon keresztül elküldött **bor azonosító** és **mennyiség** lekérése:

$bor\_id = $\_POST['bor\_id'];

$quantity = $\_POST['quantity'];

Ellenőrzés, hogy a bor már a kosárban van-e:

$user\_id = $\_SESSION['user\_id'];

$check\_query = "SELECT \* FROM cart WHERE user\_id = :user\_id AND bor\_id = :bor\_id";

$check\_stmt = $pdo->prepare($check\_query);

$check\_stmt->execute(['user\_id' => $user\_id, 'bor\_id' => $bor\_id]);

$existing\_item = $check\_stmt->fetch(PDO::FETCH\_ASSOC);

**Ha a bor már benne van**, akkor a mennyiség frissítése történik:

$new\_quantity = $existing\_item['quantity'] + $quantity;

$update\_query = "UPDATE cart SET quantity = :quantity WHERE user\_id = :user\_id AND bor\_id = :bor\_id";

$update\_stmt = $pdo->prepare($update\_query);

$update\_stmt->execute(['quantity' => $new\_quantity, 'user\_id' => $user\_id, 'bor\_id' => $bor\_id]);

**Ha nincs még a kosárban**, akkor beszúrás történik:

$insert\_query = "INSERT INTO cart (user\_id, bor\_id, quantity) VALUES (:user\_id, :bor\_id, :quantity)";

$insert\_stmt = $pdo->prepare($insert\_query);

$insert\_stmt->execute(['user\_id' => $user\_id, 'bor\_id' => $bor\_id, 'quantity' => $quantity]);

## 3. Hibakezelés

**Session ellenőrzés**: A $\_SESSION['user\_id'] létezését ellenőrizni kell, hogy a felhasználó be van-e jelentkezve.

**SQL injection elleni védelem**: A prepare() és execute() metódusok használata biztosítja a védelmet.

**Hibakezelés**: A try-catch szerkezet alkalmazása segíthet a PDO hibák kezelésében.

## 4. Javaslatok a fejlesztésre

**Frontend fejlesztés**: A borok és a kosár felhasználóbarát megjelenítése.

**Kosár funkció bővítése**: Törlési lehetőség, rendelések kezelése.

**Biztonság növelése**: További ellenőrzések, pl. CSRF tokenek.

# admin\_login.php

## Áttekintés

Ez a fájl egy **PHP alapú adminisztrátori bejelentkezési rendszer**, amely ellenőrzi a felhasználó e-mail címét és jelszavát az adatbázisban. A hitelesítés sikeressége esetén munkamenetet indít az admin számára.

## Főbb Funkciók

### 1. Konfiguráció Betöltése

A fájl elején betölti a **config2.php** fájlt, amely feltételezhetően az adatbázis-kapcsolatot tartalmazza:

include('config2.php');

### 2. POST Adatok Fogadása

A szkript ellenőrzi, hogy az adatokat **POST** módszerrel küldték-e be:

if ($\_SERVER["REQUEST\_METHOD"] == "POST") {

$email = isset($\_POST["email"]) ? trim($\_POST["email"]) : '';

$password = isset($\_POST["password"]) ? trim($\_POST["password"]) : '';

### 3. Üres Mezők Ellenőrzése

Ha az e-mail vagy a jelszó mező üres, a szkript hibaüzenetet ad vissza, majd kilép:

if (empty($email) || empty($password)) {

echo "Email and password fields cannot be empty.";

exit;

}

### 4. Felhasználó Keresése az Adatbázisban

A rendszer ellenőrzi, hogy létezik-e az adott e-mail cím az **admin felhasználók adatbázisában**:

try {

$sql = "SELECT ID, jelszo, usertype FROM login WHERE email = :email";

$stmt = $pdo->prepare($sql);

$stmt->execute(['email' => $email]);

$row = $stmt->fetch(PDO::FETCH\_ASSOC);

### 5. Jelszó Ellenőrzése és Munkamenet Indítása

* **Ha az e-mail cím létezik**, a rendszer összehasonlítja a tárolt hash-elt jelszót a megadott jelszóval:

if ($row && password\_verify($password, $row["jelszo"])) {

$\_SESSION['user\_id'] = $row['ID'];

$\_SESSION['usertype'] = $row['usertype'];

echo "Login successful";

} else {

echo "Invalid email or password.";

}

* Ha a jelszó helyes, a rendszer beállítja a munkameneti változókat (user\_id és usertype).
* Ha a jelszó nem megfelelő, a rendszer hibaüzenetet küld vissza.

## Használati Útmutató

* Az admin felhasználók **e-mail címükkel és jelszavukkal** jelentkezhetnek be.
* A jelszavakat **hash-elt formában kell tárolni** az adatbázisban password\_hash() függvénnyel.
* Az usertype mező használható különböző jogosultsági szintek megkülönböztetésére.

Checkout.php:

Ez a PHP script kezeli a felhasználók kosarát és a rendelés leadását a Gypo Winery weboldalon. A rendszer az alábbi funkciókat tartalmazza:

* Kosár adatainak betöltése az adatbázisból
* Végösszeg kiszámítása szállítási díjjal és esetleges kedvezményekkel
* Rendelés adatok mentése az adatbázisba
* Raktárkészlet frissítése a rendelés alapján
* Kosár törlése a rendelés leadása után
* Rendelés visszaigazolása e-mailben a Web3Forms API segítségével
* Felhasználói felület a fizetési módok kiválasztására

## Adatbázis lekérdezések

### Kosár lekérdezése

SELECT cart.ID as cart\_id, borok.ID as bor\_id, borok.ar, borok.nev, cart.quantity

FROM cart

JOIN borok ON cart.bor\_id = borok.ID

WHERE cart.user\_id = :user\_id

**Leírás:** Betölti a felhasználó kosarában levő termékeket, azok árait és mennyiségeit.

### Rendelés rögzítése

INSERT INTO rendelesek (user\_id, statusz) VALUES (:user\_id, 'pending')

**Leírás:** Létrehozza az új rendelést "pending" állapottal.

### Rendelés tételek mentése

INSERT INTO rendeles\_tetelek (rendeles\_id, bor\_id, quantity) VALUES (:order\_id, :bor\_id, :quantity)

**Leírás:** Elmenti a rendelés termékeit a rendeles\_tetelek táblába.

### Készlet frissítése

UPDATE borok SET keszlet = keszlet - :quantity WHERE ID = :bor\_id

**Leírás:** Frissíti a raktárkészletet a rendelés mennyisége alapján.

### Kosár törlése

DELETE FROM cart WHERE user\_id = :user\_id

**Leírás:** Törli a felhasználó kosarát a rendelés leadása után.

### Felhasználó e-mail lekérdezése

SELECT email FROM login WHERE ID = :user\_id

**Leírás:** Lekéri a felhasználó regisztrált e-mail címét a visszaigazolás küldéséhez.

## Rendelés visszaigazolás e-mailben

A Web3Forms API segítségével a rendszer e-mailt küld a felhasználónak a rendelésről. Az e-mail tartalmazza a rendelési azonosítót, a tételeket és az összes fizetendő összeget.

A kérést cURL-lel hajtja végre:

$ch = curl\_init("https://api.web3forms.com/submit");

curl\_setopt($ch, CURLOPT\_RETURNTRANSFER, true);

curl\_setopt($ch, CURLOPT\_POST, true);

curl\_setopt($ch, CURLOPT\_POSTFIELDS, $post\_fields);

$response = curl\_exec($ch);

curl\_close($ch);

## Frontend: Checkout oldal

Az oldal egy Bootstrap alapú felület, amely lehetőséget biztosít a felhasználónak a fizetési mód kiválasztására:

* **Készpénz**
* **Bankkártya** (rejtett mezők a kártyaadatoknak)
* **PayPal** (e-mail megadásával)

A JavaScript biztosítja, hogy a megfelelő fizetési mezők jelenjenek meg:

function togglePaymentDetails() {

var paymentMethod = document.getElementById("payment\_method").value;

var cardDetails = document.getElementById("card-details");

var paypalDetails = document.getElementById("paypal-details");

if (paymentMethod === "Bankkártya") {

cardDetails.style.display = "block";

paypalDetails.style.display = "none";

} else if (paymentMethod === "PayPal") {

cardDetails.style.display = "none";

paypalDetails.style.display = "block";

} else {

cardDetails.style.display = "none";

paypalDetails.style.display = "none";

}

}

## Biztonsági megfontolások

* **Adatbázis lekérdezések**: A PDO prepared statement-ek védettek SQL injection ellen.
* **Bankkártya adatok kezelése**: A kártyaadatok bevitele jelenleg nincs titkosítva, ezért valódi fizetési rendszert (pl. Stripe, PayPal API) kellene integrálni.
* **Session védelem**: A felhasználó azonosítása session változókon keresztül történik.

## Összegzés

Ez a checkout rendszer biztosítja a rendeléskezelés alapvető funkcionalitásait, beleértve a termékek betöltését, rendelés leadását és visszaigazolás küldését. Javasolt a további fejlesztés biztonsági és fizetési integrációs szempontból.