PHP Login System with Argon2id Security

A complete, enterprise-grade PHP login system with MySQL database integration, featuring the most advanced password hashing algorithm (Argon2id), secure authentication, user registration, and a modern responsive design.

Table of Contents

Features

Core Functionality

- ✅ **User Registration** - Complete registration system with comprehensive validation
- ✅ **Secure Login Authentication** - Multi-factor authentication with username or email
- ✅ **Session Management** - Database-backed session storage for enhanced security
- ✅ **Protected Dashboard** - Role-based access control for authenticated users
- ✅ **Profile Management** - Edit profile and change password functionality
- ✅ **Logout Functionality** - Secure session destruction

Security Features

- 🔐 **Argon2id Password Hashing** - Winner of the Password Hashing Competition (2015)
- 🛡️ **SQL Injection Protection** - Prepared statements with PDO
- 🔒 **XSS Protection** - Output escaping with htmlspecialchars()
- ✔️ **Input Validation** - Comprehensive server-side validation

- 📊 **Database Session Storage** - Enhanced session security and tracking
- 🎯 **CSRF Protection Ready** - Architecture supports token implementation

UI/UX Features

- 📱 **Responsive Design** - Mobile-first, works on all devices
- 🎨 **Modern UI** - Clean, professional interface with smooth transitions
- ⚡ **Client-side Validation** - JavaScript validation for better UX
- 🌈 **Consistent Styling** - Centralized CSS for easy theming

Security Highlights

Password Hashing - Argon2id

This system uses **Argon2id**, the most secure password hashing algorithm available today. Here's why it's the best choice:

Argon2id - The Best Password Hashing Algorithm

What is Argon2id?

Argon2id is a hybrid version of the Argon2 password hashing algorithm that combines the best features of both Argon2i and Argon2d variants. It was designed to be the most secure password hashing function in the world.

Competition Winner 🏆

Argon2 won the Password Hashing Competition (PHC) in 2015, competing against 24 other candidates from security researchers worldwide. The competition was organized to find the best password hashing algorithm to replace older, less secure methods.

Why Argon2id is the Best

1. Hybrid Security Approach

- Combines **data-dependent** (Argon2d) and **data-independent** (Argon2i) memory access
- Protects against both **GPU cracking attacks** and **side-channel attacks**
- Best of both worlds - maximum security

2. Memory-Hard Function

- Requires significant memory to compute
- Makes parallel attacks (GPU/ASIC) extremely expensive
- Adjustable memory cost parameter

3. Time-Cost Parameter

- Configurable computational cost
- Can increase difficulty as hardware improves
- Future-proof security

4. Parallelism Degree

- Supports parallel processing
- Optimized for modern multi-core processors
- Balanced performance and security

5. Resistance Against Attacks

- **GPU/ASIC Resistant** - Memory requirements make specialized hardware ineffective
- **Side-channel Resistant** - Argon2id variant protects against timing attacks
- **Brute-force Resistant** - Computationally expensive to attack
- **Rainbow Table Resistant** - Built-in salting mechanism

Comparison with Other Algorithms

Algorithm	Security Level	Speed	GPU Resistant	Side-channel Safe	Status
Argon2id	⭐⭐⭐⭐⭐	Medium	✅ Yes	✅ Yes	**BEST - PHC Winner 2015**
bcrypt	⭐⭐⭐⭐	Slow	⚠️ Partial	✅ Yes	Good
scrypt	⭐⭐⭐⭐	Slow	✅ Yes	⚠️ Partial	Good
PBKDF2	⭐⭐⭐	Fast	❌ No	✅ Yes	Acceptable
SHA-256	⭐⭐	Very Fast	❌ No	❌ No	Not Recommended
MD5	⭐	Very Fast	❌ No	❌ No	**NEVER USE**

Industry Adoption

Argon2id is recommended by:

- **OWASP** (Open Web Application Security Project)
- **NIST** (National Institute of Standards and Technology)
- **Libsodium** (Modern cryptography library)
- **RFC 9106** (Official IETF Standard)

Implementation in This Project

```
// User Registration - src/Auth/AuthService.php:40
$hashed = password_hash($password, PASSWORD_ARGON2ID);

// Password Change - controllers/change_password.php:37
$hashed_password = password_hash($new_password, PASSWORD_ARGON2ID);

// Password Verification (backward compatible)
password_verify($password, $hashed); // Works with any algorithm
```

Architecture & Code Explanation

Project Structure

This project follows a modern MVC-inspired architecture with dependency injection and separation of concerns:

```
design_p/
├── controllers/              # Request handlers and business logic
│   ├── index.php            # Welcome page controller
│   ├── login.php            # Login controller
│   ├── register.php         # Registration controller
│   ├── dashboard.php        # Dashboard controller
│   ├── logout.php           # Logout handler
│   ├── edit_profile.php     # Profile edit controller
│   └── change_password.php  # Password change controller
├── templates/               # View layer (presentation)
│   ├── index.php           # Welcome page template
│   ├── login.php           # Login form template
│   ├── register.php        # Registration form template
│   └── dashboard.php       # Dashboard template
├── src/                    # Core application classes
```

```
│   ├── Core/
│   │   ├── Container.php   # Dependency injection container
│   │   └── Renderer.php    # Template rendering engine
│   ├── Auth/
│   │   └── AuthService.php # Authentication service
│   └── Security/
│       └── Validator.php   # Input validation utilities
├── config/                 # Configuration files
│   └── database.php       # Database connection settings
├── includes/              # Legacy helper functions
│   └── auth.php          # Authentication helpers
├── assets/               # Static resources
│   ├── styles.css       # Application stylesheet
│   └── validation.js    # Client-side validation
├── bootstrap.php        # Application bootstrap
├── index.php           # Entry point (redirects to login)
├── database_schema.sql # Database schema
└── README.md          # This file
```

Core Components Explained

1. Bootstrap System (`bootstrap.php`)

```
// Initializes the application
- Starts PHP session
- Loads autoloader for PSR-4 class loading
- Sets up dependency injection container
- Initializes database connection (PDO)
```

Purpose: Centralized initialization ensures consistent setup across all entry points.

2. Dependency Injection Container (`src/Core/Container.php`)

```
// Manages application dependencies
- Stores and retrieves services (like PDO)
- Enables loose coupling between components
- Facilitates testing and maintenance
```

Purpose: Promotes SOLID principles and makes code more maintainable.

3. Template Renderer (`src/Core/Renderer.php`)

```
// Separates presentation from logic
- Loads template files
- Passes variables to views
- Maintains MVC pattern
```

Purpose: Clean separation between business logic and presentation.

4. Authentication Service (`src/Auth/AuthService.php`)

The heart of the security system:

```
// Core Methods:

1. findUserByUsernameOrEmail($identifier)
   - Searches for user by username OR email
   - Returns user data including hashed password
   - Used during login authentication

2. register($username, $email, $password)
   - Validates input using Validator class
   - Checks for existing users
   - Hashes password with Argon2id
   - Creates new user in database
   - Returns success/error status

3. createSession($userId)
   - Generates secure random token (64 characters)
   - Stores session in database with expiration
   - Sets PHP session variables
   - Returns session token

4. destroySession()
   - Removes session from database
   - Unsets all session variables
   - Destroys PHP session
   - Ensures complete logout

5. getCurrentUser()
   - Retrieves logged-in user data
   - Used for displaying user info
   - Returns null if not logged in
```

```
6. isLoggedIn()
   - Checks if user has active session
   - Verifies both user_id and session_token
   - Used for access control
```

5. Validator Class (`src/Security/Validator.php`)

Comprehensive input validation:

```
// Validation Methods:

1. isValidUsername($username)
   - Length: 3-50 characters
   - Allowed: letters, numbers, underscore, dot, hyphen
   - Prevents SQL injection and XSS

2. isValidEmail($email)
   - Uses PHP's FILTER_VALIDATE_EMAIL
   - RFC 5322 compliant
   - Prevents invalid email formats

3. isStrongPassword($password)
   - Minimum 8 characters
   - Requires: uppercase, lowercase, number, special char
   - Ensures strong password policy
```

6. Database Schema (`database_schema.sql`)

Two main tables:

Users Table:

```
- id: Primary key (AUTO_INCREMENT)
- username: Unique user identifier (VARCHAR 50)
- email: Unique email address (VARCHAR 100)
- password: Argon2id hashed password (VARCHAR 255)
- created_at: Account creation timestamp
- updated_at: Last update timestamp
```

User Sessions Table:

```
- id: Primary key (AUTO_INCREMENT)
- user_id: Foreign key to users table
- session_token: Unique 64-char token (VARCHAR 255)
- created_at: Session creation time
- expires_at: Session expiration time (24 hours)
- Indexes on user_id and session_token for performance
```

Request Flow

Registration Flow:

```
1. User submits form → controllers/register.php
2. POST data extracted and validated
3. AuthService→register() called
4. Validator checks username, email, password
5. Password hashed with Argon2id
6. User inserted into database
7. Success message shown → templates/register.php
```

Login Flow:

```
1. User submits credentials → controllers/login.php
2. AuthService→findUserByUsernameOrEmail() searches user
3. password_verify() checks password against Argon2id hash
4. AuthService→createSession() creates session
5. Session stored in database + PHP session
6. Redirect to dashboard → controllers/dashboard.php
```

Dashboard Access Flow:

```
1. Request to dashboard → controllers/dashboard.php
2. AuthService→isLoggedIn() checks session
3. If not logged in → redirect to login
4. If logged in → AuthService→getCurrentUser() fetches data
5. Render dashboard with user data → templates/dashboard.php
```

Logout Flow:

```
1. User clicks logout → controllers/logout.php
2. AuthService→destroySession() called
3. Session removed from database
```

```
4. PHP session destroyed
5. Redirect to login page
```

Security Measures Implemented

1. Password Security

- Argon2id hashing (PHC winner 2015)
- Automatic salting
- Hash length: 255 characters
- Backward compatible verification

2. SQL Injection Prevention

```
// Prepared Statements with PDO
$stmt = $pdo->prepare("SELECT * FROM users WHERE username = ?");
$stmt->execute([$username]);
// Never concatenates user input into SQL
```

3. XSS Prevention

```
// All output is escaped
<?php echo htmlspecialchars($user['username']); ?>
// Prevents malicious script injection
```

4. Session Security

- Database-backed sessions
- 24-hour expiration
- Secure random tokens (bin2hex + random_bytes)
- Proper session destruction

5. Input Validation

- Server-side validation (primary)
- Client-side validation (UX enhancement)
- Type checking and sanitization
- Length and format validation

Requirements

Minimum Requirements

- **PHP**: 7.2 or higher (for PASSWORD_ARGON2ID support)
- **MySQL**: 5.7 or higher
- **Web Server**: Apache 2.4+ or Nginx 1.18+
- **PHP Extensions**:
  - PDO
  - pdo_mysql
  - sodium (for Argon2id)
  - session

Recommended Requirements

- **PHP**: 8.0 or higher
- **MySQL**: 8.0 or higher
- **HTTPS**: SSL/TLS certificate for production
- **PHP Settings**:
  - `session.cookie_secure = On` (production)
  - `session.cookie_httponly = On`
  - `session.cookie_samesite = Strict`

Installation

Step 1: Clone or Download

```
# Clone the repository
git clone https://github.com/shadrack-ss/login_system

# Or download and extract to your web server directory
# Example: C:\xampp\htdocs\design_p\
```

Step 2: Database Setup

1. **Create the database:**

```
CREATE DATABASE IF NOT EXISTS login_system CHARACTER SET utf8mb4 COLI
```

2. **Import the schema:**

```
mysql -u root -p login_system < database_schema.sql
```

Or manually run the SQL from `database_schema.sql` :

```
USE login_system;

-- Create users table
CREATE TABLE users (
    id INT AUTO_INCREMENT PRIMARY KEY,
    username VARCHAR(50) UNIQUE NOT NULL,
    email VARCHAR(100) UNIQUE NOT NULL,
    password VARCHAR(255) NOT NULL,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_
);

-- Create sessions table
CREATE TABLE user_sessions (
    id INT AUTO_INCREMENT PRIMARY KEY,
    user_id INT NOT NULL,
    session_token VARCHAR(255) UNIQUE NOT NULL,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    expires_at TIMESTAMP NOT NULL,
    FOREIGN KEY (user_id) REFERENCES users(id) ON DELETE CASCADE,
    INDEX idx_user_id (user_id),
    INDEX idx_session_token (session_token)
);
```

Step 3: Configure Database Connection

1. Open `config/database.php`
2. Update credentials:

```
$host = 'localhost';
$dbname = 'login_system';
$username = 'root';  // Your MySQL username
$password = '';      // Your MySQL password
```

Step 4: Web Server Configuration

For Apache (XAMPP/WAMP):

1. Place project in `htdocs/` directory
2. Ensure mod_rewrite is enabled
3. Start Apache and MySQL

For Nginx:

```
server {
    listen 80;
    server_name localhost;
    root /var/www/design_p;
    index index.php;

    location / {
        try_files $uri $uri/ /index.php?$query_string;
    }

    location ~ \.php$ {
        fastcgi_pass unix:/var/run/php/php8.0-fpm.sock;
        fastcgi_index index.php;
        include fastcgi_params;
    }
}
```

Step 5: Verify Installation

1. Open browser: `http://localhost/design_p/`
2. Should redirect to login page
3. Click "Register" to create first account
4. Login with new credentials

Usage

User Registration

1. Navigate to the registration page
2. Provide:
    - **Username**: 3-50 characters, letters, numbers, `_`, `.`, `-`
    - **Email**: Valid email format
    - **Password**: 8+ chars, uppercase, lowercase, number, special char

    - **Confirm Password**: Must match password
3. Submit form
4. On success, you can login immediately

Login

1. Navigate to login page (automatic from root)
2. Enter username **OR** email
3. Enter password
4. Click "Login"
5. Redirects to dashboard on success

Dashboard

- View your profile information:
    - Username
    - Email address
    - Member since date
    - User ID
- Access profile management:
    - Edit Profile
    - Change Password
- Logout securely

Edit Profile

1. Click "Edit Profile" from dashboard
2. Update username or email
3. System checks for duplicates
4. Submit to save changes

Change Password

1. Click "Change Password" from dashboard
2. Enter current password
3. Enter new password (must meet strength requirements)
4. Confirm new password
5. Submit to update (hashed with Argon2id)

File Structure

Detailed File Overview

Controllers Layer

File	Purpose	Key Features
`controllers/index.php`	Welcome page	Redirects logged-in users to dashboard
`controllers/login.php`	Login handler	Username/email login, password verification
`controllers/register.php`	Registration handler	Validation, Argon2id hashing, duplicate check
`controllers/dashboard.php`	User dashboard	Authentication check, user data display
`controllers/logout.php`	Logout handler	Session destruction, database cleanup
`controllers/edit_profile.php`	Profile editor	Username/email update, duplicate check
`controllers/change_password.php`	Password changer	Current password verification, Argon2id hashing

Templates Layer

File	Purpose	Styling
`templates/index.php`	Welcome view	Centered layout, feature list
`templates/login.php`	Login form	Clean form, error display
`templates/register.php`	Registration form	Multi-step validation
`templates/dashboard.php`	Dashboard view	User info cards, action buttons

Core Classes

File	Class	Responsibility
`src/Core/Container.php`	Container	Dependency injection, service location
`src/Core/Renderer.php`	Renderer	Template rendering, variable passing
`src/Auth/AuthService.php`	AuthService	Authentication, session management
`src/Security/Validator.php`	Validator	Input validation, security checks

Configuration

File	Purpose

File	Purpose
`config/database.php`	PDO connection, credentials
`bootstrap.php`	App initialization, autoloader

Assets

File	Purpose
`assets/styles.css`	Global styles, responsive design
`assets/validation.js`	Client-side validation

Customization

Changing Password Policy

Edit `src/Security/Validator.php`:

```
public static function isStrongPassword(string $password): bool {
    // Customize minimum length
    if (strlen($password) < 12) {  // Changed from 8 to 12
        return false;
    }
    // Add custom requirements
    return preg_match('/[A-Z]/', $password)     // Uppercase
        && preg_match('/[a-z]/', $password)     // Lowercase
        && preg_match('/[0-9]/', $password)     // Number
        && preg_match('/[^A-Za-z0-9]/', $password); // Special char
}
```

Changing Session Expiration

Edit `src/Auth/AuthService.php`:

```
public function createSession(int $userId): string {
    $token = bin2hex(random_bytes(32));
    // Change from 24 hours to 7 days
    $expiresAt = date('Y-m-d H:i:s', strtotime('+7 days'));
    // ... rest of code
}
```

Customizing Argon2id Parameters

```
// For even stronger hashing (slower but more secure)
$options = [
    'memory_cost' => 65536,  // 64 MB (default: 65536)
    'time_cost' => 4,        // 4 iterations (default: 4)
    'threads' => 3           // 3 parallel threads (default: 1)
];
$hashed = password_hash($password, PASSWORD_ARGON2ID, $options);
```

Styling Customization

Edit `assets/styles.css`:

```
/* Change primary color */
.btn {
    background: #your-color;
}

/* Change background */
body {
    background: #ffffff;  /* Already white */
}
```

Troubleshooting

Common Issues

1. Argon2id Not Available

Error: `PASSWORD_ARGON2ID` constant not defined

Solution:

```
# Check PHP version (need 7.2+)
php -v

# Check if sodium extension is installed
```

```
php -m | grep sodium

# Install sodium (Ubuntu/Debian)
sudo apt-get install php-sodium

# Restart web server
sudo service apache2 restart
```

2. Database Connection Failed

Error: SQLSTATE[HY000][1045] Access denied

Solution:

- Verify credentials in `config/database.php`
- Check MySQL is running: `sudo service mysql status`
- Test connection: `mysql -u root -p`

3. CSS Not Loading

Error: Styles not applied

Solution:

- Check file paths in templates (should be `../assets/styles.css`)
- Verify `assets/styles.css` exists
- Clear browser cache (Ctrl+F5)

4. Session Issues

Error: Cannot start session

Solution:

```
// Check session directory permissions
<?php
echo session_save_path();
// Ensure directory is writable
?>
```

5. Registration/Login Not Working

Checklist:

- ☐ Database tables created
- ☐ Database credentials correct
- ☐ PHP version 7.2+
- ☐ Sodium extension installed
- ☐ No PHP errors in logs

Debug Mode

Enable error display (development only):

```
// Add to top of bootstrap.php
ini_set('display_errors', 1);
ini_set('display_startup_errors', 1);
error_reporting(E_ALL);
```

WARNING: Never enable in production!

Performance Optimization

Database Indexing

Already implemented:

- `users.username` (UNIQUE)
- `users.email` (UNIQUE)
- `user_sessions.user_id` (INDEX)
- `user_sessions.session_token` (INDEX)

Caching Recommendations

- Use opcache for PHP code caching
- Implement Redis/Memcached for session storage (high-traffic sites)
- Enable browser caching for static assets

Argon2id Performance

Argon2id is intentionally slow for security. For high-traffic sites:

- Use default parameters (already optimized)
- Consider dedicated authentication server

- Implement rate limiting for login attempts

Production Deployment Checklist

- [ ] Use HTTPS (SSL/TLS certificate)
- [ ] Disable error display (`display_errors = Off`)
- [ ] Enable error logging
- [ ] Set secure session cookies
- [ ] Implement rate limiting
- [ ] Add CSRF tokens
- [ ] Set up regular database backups
- [ ] Configure firewall rules
- [ ] Use environment variables for credentials
- [ ] Enable audit logging
- [ ] Implement 2FA (optional but recommended)

Security Best Practices

1. **Always use HTTPS in production**
2. **Keep PHP and dependencies updated**
3. **Regular security audits**
4. **Monitor failed login attempts**
5. **Implement account lockout after X failed attempts**
6. **Use Content Security Policy (CSP) headers**
7. **Regular database backups**
8. **Sanitize all user inputs**
9. **Use prepared statements (already implemented)**
10. **Keep Argon2id parameters up-to-date**

Why This System is Secure

1. Industry-Leading Hashing

- **Argon2id**: Winner of Password Hashing Competition 2015
- Recommended by OWASP, NIST, and security experts worldwide
- GPU/ASIC resistant
- Side-channel attack resistant

2. Defense in Depth

- Multiple layers of security
- Input validation + output escaping
- SQL injection prevention
- Session security

3. Modern Architecture

- Separation of concerns
- Dependency injection
- PSR-4 autoloading
- Clean code principles

4. Battle-Tested Patterns

- MVC-inspired architecture
- Service layer pattern
- Repository pattern (via PDO)
- Secure session management

License

This project is open-source and available for educational and commercial use.

Credits

- **Password Hashing:** Argon2id (PHC Winner 2015)
- **Framework:** Custom PHP 8+ architecture
- **Database:** MySQL/MariaDB
- **Security Standards:** OWASP, NIST guidelines

Support

For issues, questions, or contributions:

1. Check this documentation
2. Review code comments
3. Check PHP error logs
4. Verify configuration settings

Changelog

Version 2.0 (Current)

- ✅ Upgraded to Argon2id password hashing
- ✅ Reorganized controllers into dedicated folder
- ✅ Fixed CSS paths for proper asset loading
- ✅ Added comprehensive documentation
- ✅ Implemented dependency injection
- ✅ Enhanced security validation

Version 1.0

- Initial release with bcrypt hashing
- Basic authentication system
- Simple session management

Built with security, performance, and maintainability in mind.

Powered by Argon2id - The World's Most Secure Password Hashing Algorithm 🏆