🔐 Complete Authentication System

Key Features Delivered:

- ✅ **1-Factor Authentication (1FA)** - Secure login with username/email
- ✅ **Role-Based Access Control** - Admin & User roles with different permissions
- ✅ **30-Minute Session Timeout** - Auto-logout with inactivity detection
- ✅ **User Management System** - Full CRUD operations for admin users
- ✅ **Secure Password Hashing** - All passwords encrypted in database
- ✅ **Session Tracking** - Real-time session monitoring and management
- ✅ **Dynamic Sidebar** - Username display changes, role-based menu items
- ✅ **Security Features** - Login attempt monitoring, IP lockout protection

What's Included:

1. **Enhanced Database Setup** - Creates users, sessions, and login tracking tables
2. **Functional Login Page** - Complete authentication with error handling
3. **Protected Dashboard** - Session validation on all pages
4. **Dynamic Sidebar Navigation** - Shows username, role-based menu items
5. **User Management Interface** - Add, edit, activate/deactivate users (Admin only)
6. **Profile Management** - Users can update their info and change passwords
7. **Session Management** - Real-time timeout display, activity tracking
8. **Security Features** - Password hashing, login attempt monitoring, IP lockout

Session Management Features:

- **Visual Timer** - Shows remaining session time in navbar (working)
- **Activity Detection** - Tracks mouse movement, clicks, keyboard input (working)
- **5-Minute Warning** - Alerts user before session expires (medyo buggy)
- **Auto-Logout** - Redirects to login page after 10 minutes of inactivity (working)
- **Session Database Tracking** - Stores all active sessions with IP/browser info

User Management (Admin Only):

- **Add Users** - Create accounts with email, username, password, role (working)

- **Edit Users** - Modify user details, optionally change passwords (buggy, di pa naaayos)
- **Activate/Deactivate** - Control account access without deletion (working)
- **Delete Users** - Remove accounts (with self-protection) (working)
- **Role Assignment** - Set users as Admin or regular User (working)
- **Status Monitoring** - View user creation dates and current status

Security Implementations:

- **Password Hashing** - Uses PHP `password_hash()` with salt
- **Login Attempt Tracking** - 5 failed attempts = 15-minute IP lockout
- **Session Regeneration** - Prevents session fixation attacks
- **CSRF Protection** - Server-side validation on all forms
- **Role Validation** - Checks permissions on every protected page

🔒 Current System (IP-Based Lockout):

- **Locks the entire IP address** after 5 failed attempts from ANY username
- **All accounts from that IP** are locked out together
- **Timer applies to the IP**, not individual accounts
- **Any successful login from that IP** clears all failed attempts

☑️ What I Fixed:

- **Prevented timer reset** during active lockout
- **No new failed attempts logged** during lockout period
- **Timer continues counting down** without interruption
- **Real-time countdown display** shows exact time remaining

🎯 The behavior I wanted that is now working:

- Make 5 failed attempts → IP gets locked for 15 minutes
- Wait 6 minutes → 9 minutes remaining on countdown
- Try to login again → Still shows 9 minutes (doesn't reset to 15!)
- Timer continues counting down normally
- After 15 minutes total → IP lockout expires

Admin User
Username: admin
Password: admin@123

User
Username: testuser
Password: user@123