Alexandria National University

Faculty of Computers and Data Science

Information Security management Course

Secure Medical System

Team Participants

Omar Magdy Abdulla 2205221

Kareem Ahmed Helmy 2205069

Adham Ahmed Reda 2205087

Ibrahim Hassan Ibrahim 2205001

Mohamed Ahmed Aly Mobarak 2205249

Amr Khaled Abdelwahab 2205220

Mariam Waleed Bassiouny 2205184

Introduction

This report provides an overview of the key functionalities implemented in the Medical System project. The system is designed to manage medical information with a strong emphasis on security and access control.

Link → https://github.com/omar-elkhazendar/Secure-Medical-System

User Roles and Access Control:

The system incorporates a robust Role-Based Access Control (RBAC) mechanism with four distinct user roles:

- Admin: Full administrative privileges over the system.
- Doctor: Access to manage appointments, view and update medical records.
- Patient: Access to view their own profile, appointments, and medical records.

Access control is enforced at both the application and database levels to ensure data security and prevent unauthorized access.

Authentication and Security:

The system employs multiple layers of security for user authentication:

- JWT-based Authentication: Securely verifies user identity using JSON Web Tokens.
- Two-Factor Authentication (2FA): Provides an extra layer of security for Doctor and Admin roles.
- Secure Password Hashing: Protects user passwords using the bcrypt algorithm.
- Social Login: Supports authentication via GitHub, Google, and Okta OAuth providers.
- Secure Session Management: Ensures secure handling of user sessions.

Core Functional Modules:

The system includes several key modules to manage medical operations:

- **Appointment Management:** **Allows scheduling, viewing, and managing appointments for patients and doctors.**
- **Medical Records Management:** **Facilitates the creation, viewing, and updating of patient medical records.**
- **User Profile Management:** **Enables users to manage their personal information.**

Security Measures:

Beyond authentication, the system incorporates several security practices to protect against common web vulnerabilities:

- **SQL Injection Prevention:** **Utilizes prepared statements to prevent malicious SQL injection attacks.**
- **XSS Protection:** **Implements output escaping to mitigate Cross-Site Scripting vulnerabilities.**
- **CSRF Protection:** **Includes measures to protect against Cross-Site Request Forgery attacks.**
- **Activity Logging:** **Maintains logs of user activities for auditing and security monitoring.**

Technology Stack:

The project is built using standard web technologies:

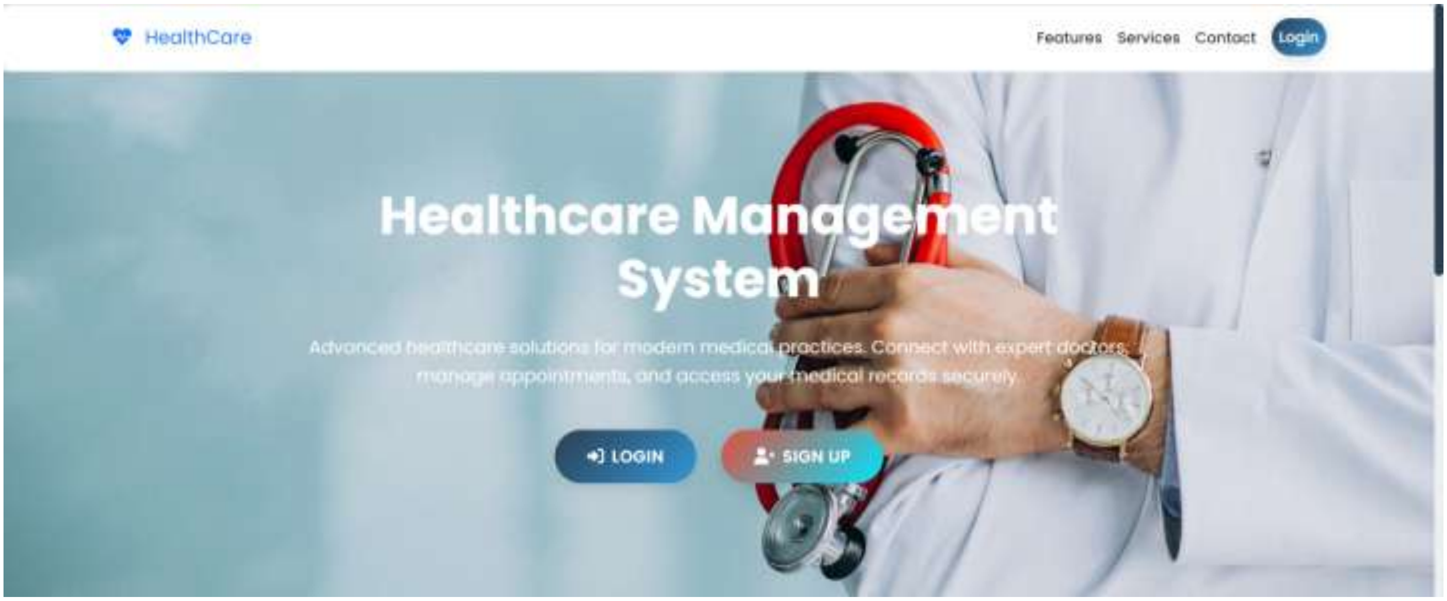
- **Backend:** **PHP**
- **Database:** **MySQL**
- **Frontend:** **HTML, CSS, JavaScript**

Conclusion

The Medical System is a comprehensive application featuring a strong RBAC model, multi-layered authentication including 2FA and social login, and core functionalities for managing appointments and medical records. The implementation includes key security measures to protect against common web vulnerabilities, making it a robust and secure platform for managing medical information.

Our System Home page:

We rnter from it to Signup page or Login Page

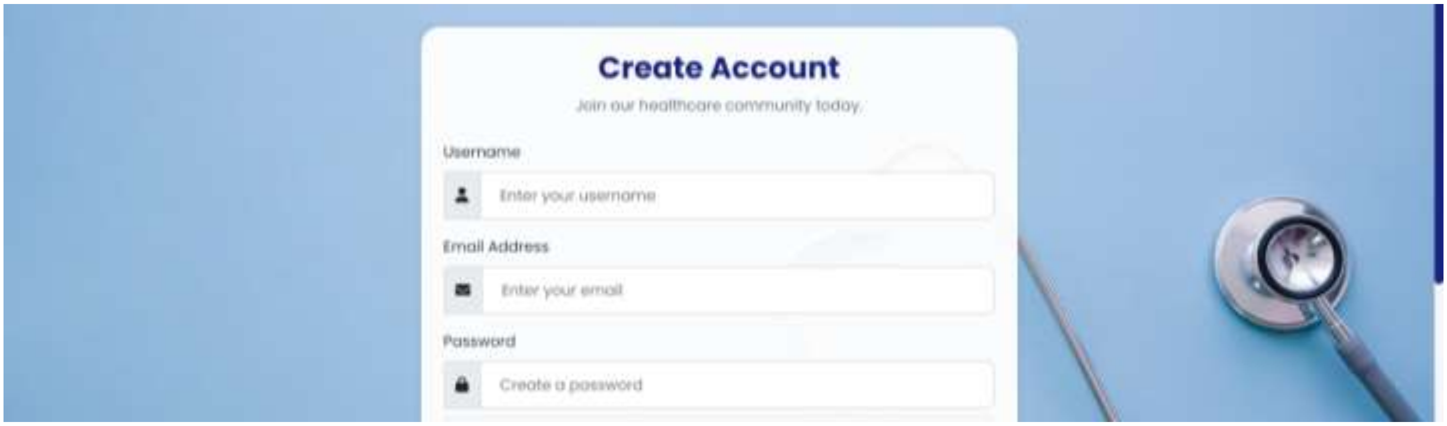


Healthcare Management System

Advanced healthcare solutions for modern medical practices. Connect with expert doctors, manage appointments, and access your medical records securely.

Our Signup Page:

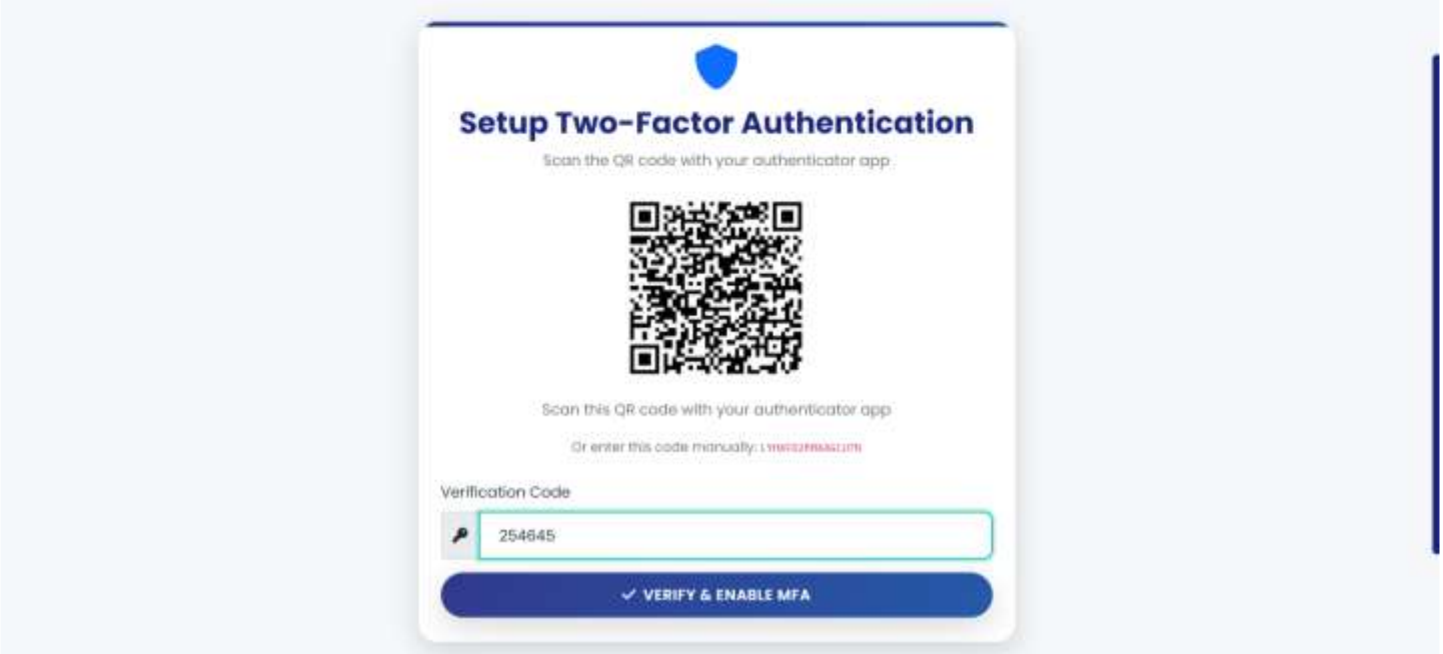
We can Signup a new user to our system by The Manual Method



Create Account

Join our healthcare community today.

After Register my Credentials it takes me to Do Two-Factor Authentication:


Setup Two-Factor Authentication

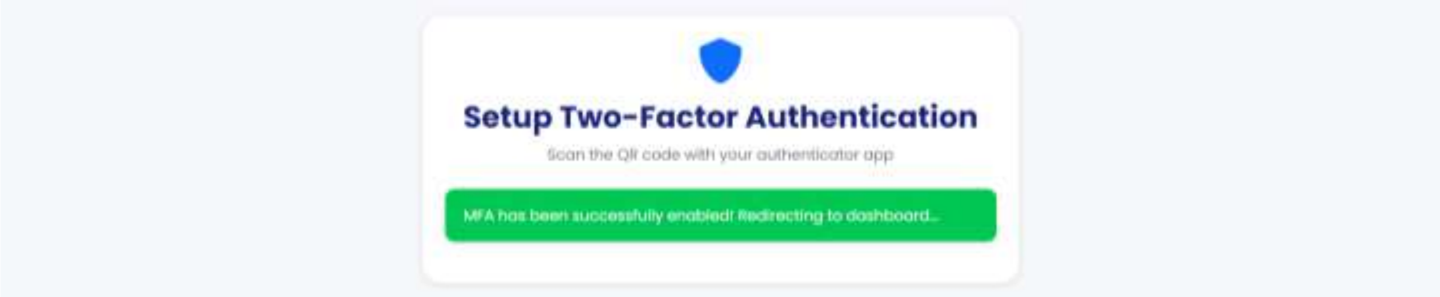
Scan the QR code with your authenticator app

Scan this QR code with your authenticator app

Or enter this code manually: [illegible]

Verification Code: 254645

Then it Notifies Me that 2FA has been Successfully Enabled

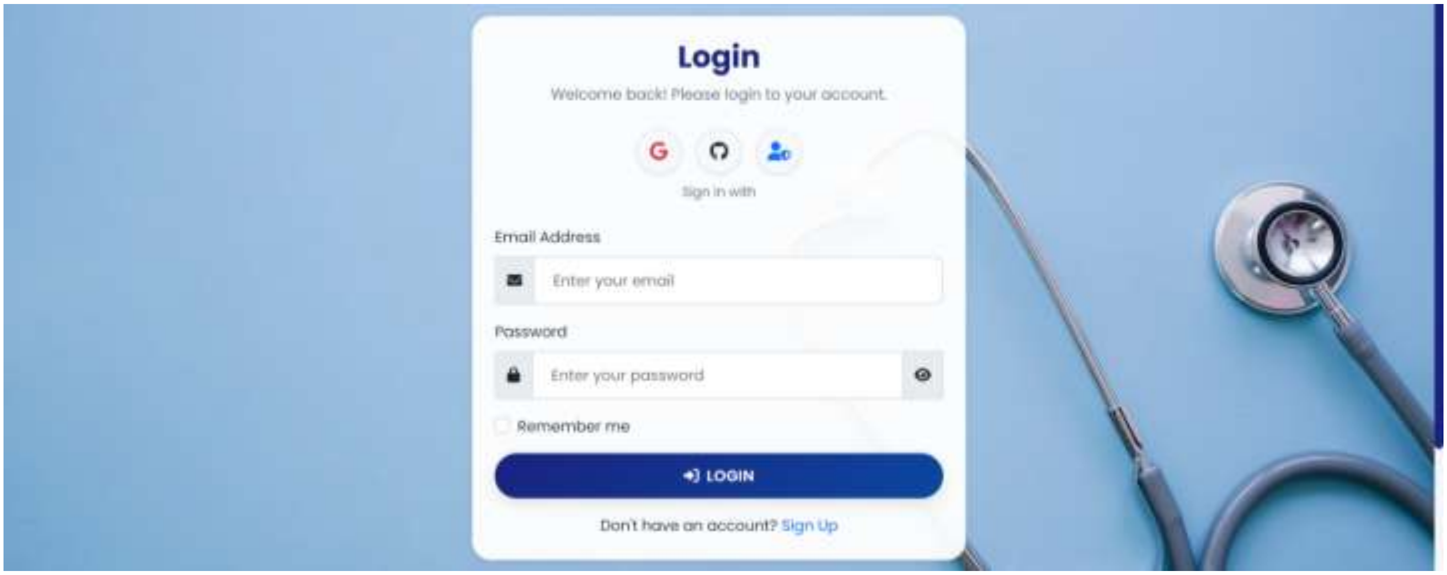

Setup Two-Factor Authentication

Scan the QR code with your authenticator app

MFA has been successfully enabled! Redirecting to dashboard...

Our Login Page:

The system implements a dual authentication approach featuring both traditional username/password login and GitHub OAuth 2.0 integration, with robust security measures including bcrypt password hashing, session management with anti-fixation protection, comprehensive login activity logging, and prevention of back navigation after logout, all wrapped in a clean and responsive user interface.



Login

Welcome back! Please login to your account.

Email Address: Enter your email

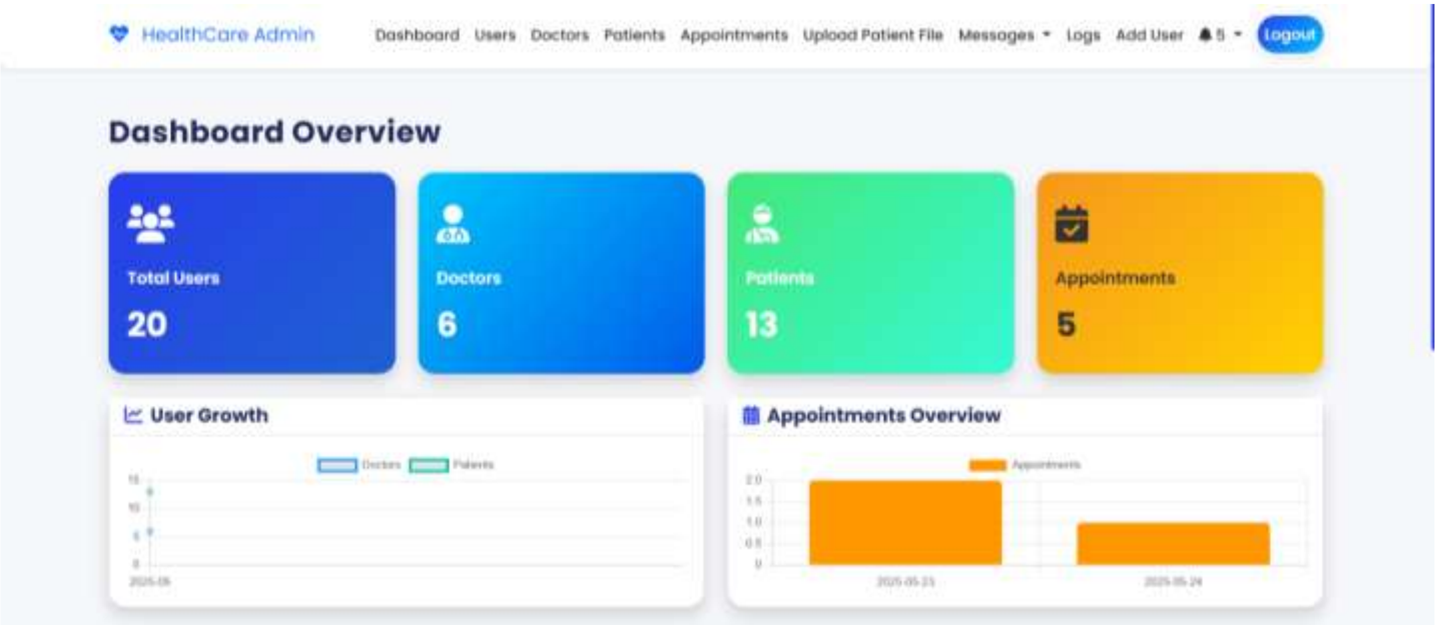
Password: Enter your password

□ Remember me

Don't have an account? Sign Up

Our Admin Dashboard Page:

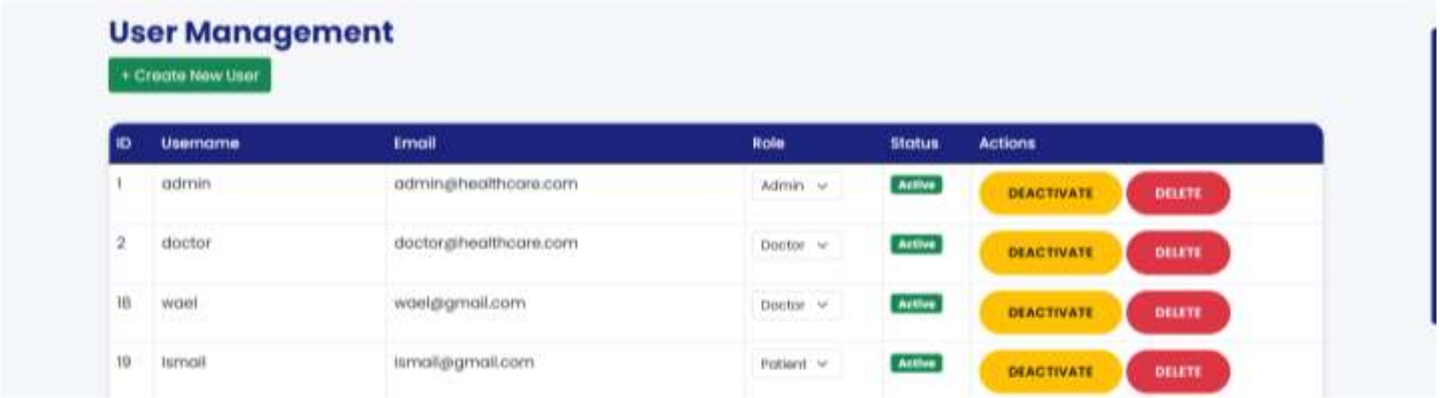
I Can Manage All Users, Doctors, Patients & Appointments in The System



Dashboard Overview

Total Users	Doctors	Patients	Appointments
20	6	13	5

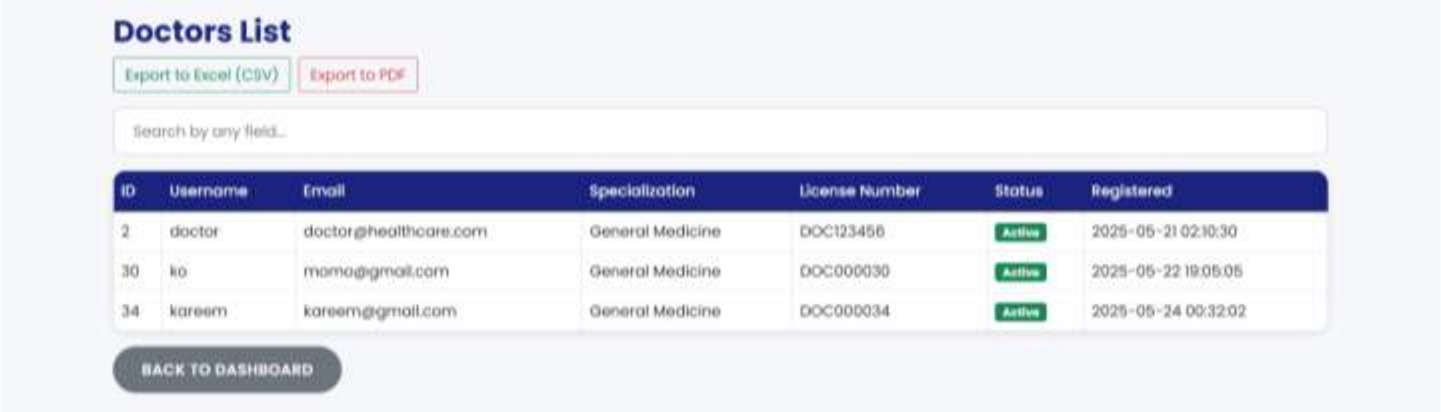
I Can Manage Users:



User Management

ID	Username	Email	Role	Status	Actions
1	admin	admin@healthcare.com	Admin	Active	DEACTIVATE DELETE
2	doctor	doctor@healthcare.com	Doctor	Active	DEACTIVATE DELETE
18	wael	wael@gmail.com	Doctor	Active	DEACTIVATE DELETE
19	Ismail	ismail@gmail.com	Patient	Active	DEACTIVATE DELETE

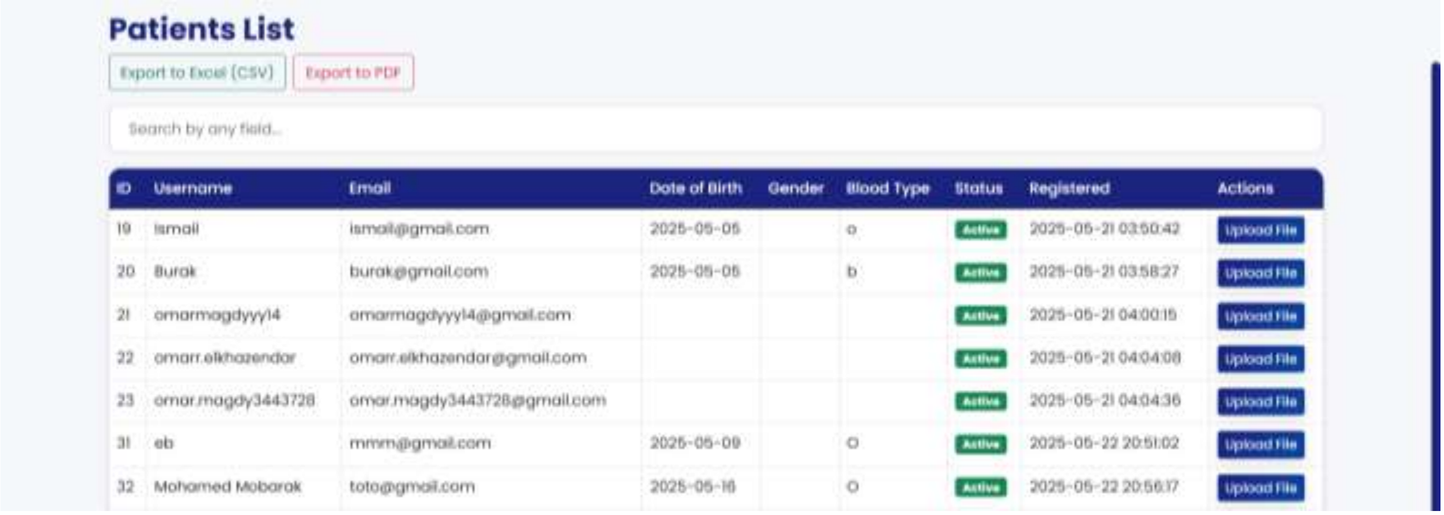
I Can Manage Doctors:



Doctors List

ID	Username	Email	Specialization	License Number	Status	Registered
2	doctor	doctor@healthcare.com	General Medicine	DOC123456	Active	2025-05-21 02:10:30
30	ko	momo@gmail.com	General Medicine	DOC000030	Active	2025-05-22 19:05:05
34	kareem	kareem@gmail.com	General Medicine	DOC000034	Active	2025-05-24 00:32:02

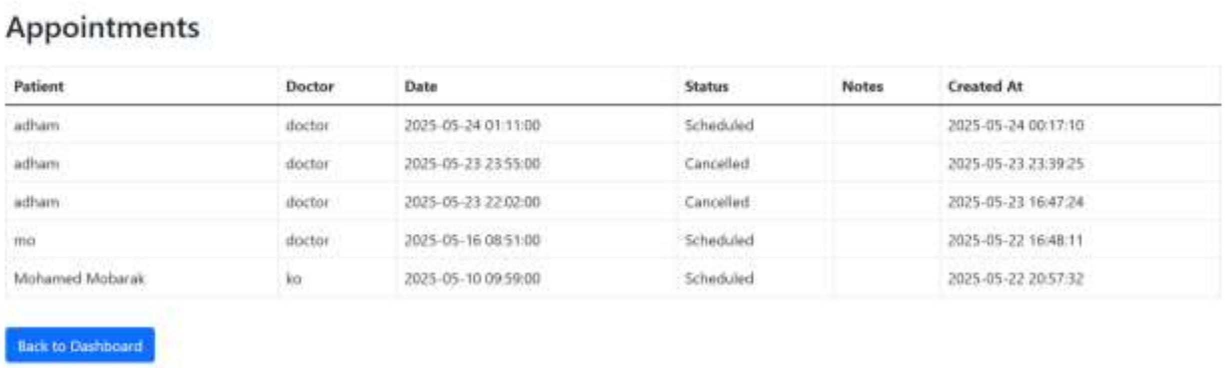
I Can Manage Patients:



Patients List

ID	Username	Email	Date of Birth	Gender	Blood Type	Status	Registered	Actions
19	ismail	ismail@gmail.com	2025-05-05		o	Active	2025-05-21 03:50:42	Upload File
20	Burak	burak@gmail.com	2025-05-05		b	Active	2025-05-21 03:58:27	Upload File
21	omarmagdyyy14	omarmagdyyy14@gmail.com				Active	2025-05-21 04:00:15	Upload File
22	omarr.elkhazendar	omarr.elkhazendar@gmail.com				Active	2025-05-21 04:04:08	Upload File
23	omar.magdy3443728	omar.magdy3443728@gmail.com				Active	2025-05-21 04:04:36	Upload File
31	eb	mmm@gmail.com	2025-05-09		O	Active	2025-05-22 20:51:02	Upload File
32	Mohamed Mobarak	toto@gmail.com	2025-05-16		O	Active	2025-05-22 20:56:17	Upload File

I Can Manage Appointments:

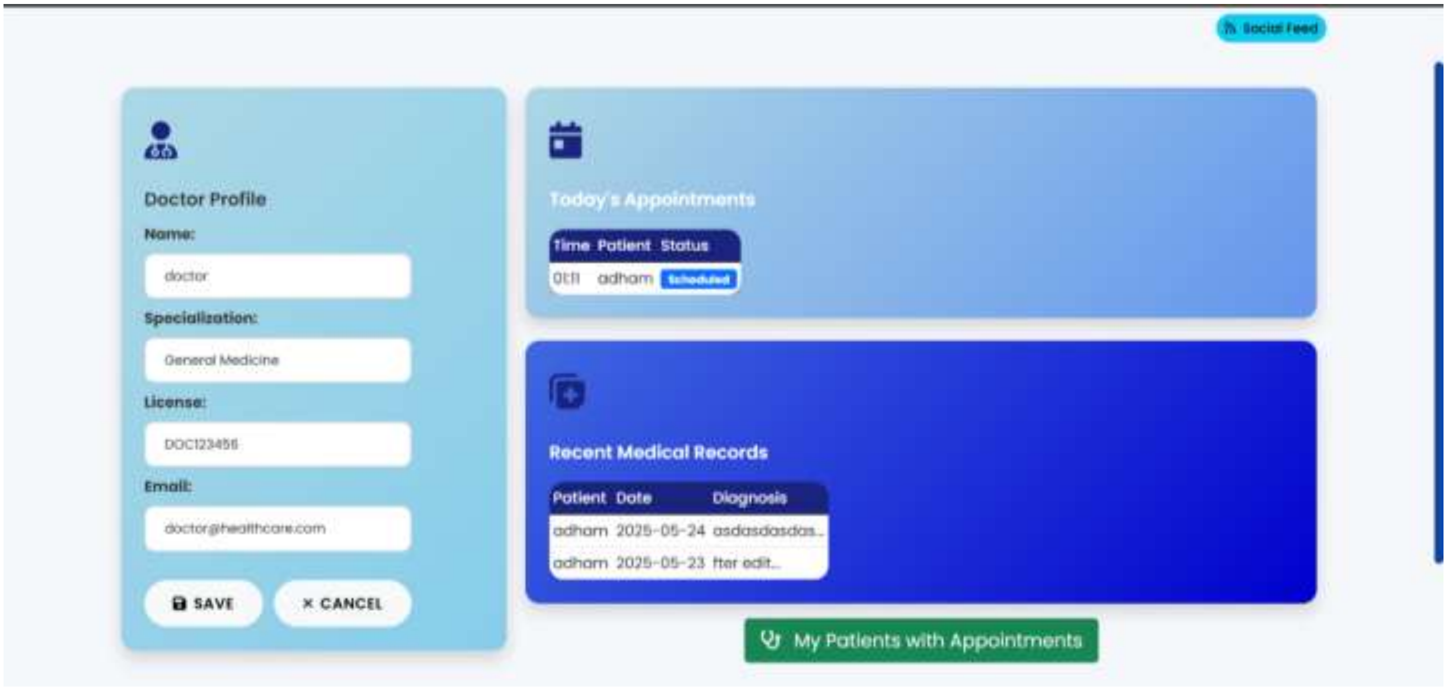


Appointments

Patient	Doctor	Date	Status	Notes	Created At
adham	doctor	2025-05-24 01:11:00	Scheduled		2025-05-24 00:17:10
adham	doctor	2025-05-23 23:55:00	Cancelled		2025-05-23 23:39:25
adham	doctor	2025-05-23 22:02:00	Cancelled		2025-05-23 16:47:24
mo	doctor	2025-05-16 08:51:00	Scheduled		2025-05-22 16:48:11
Mohamed Mobarak	ko	2025-05-10 09:59:00	Scheduled		2025-05-22 20:57:32

Registering as a Doctor:

The Doctor Can Update his profile, See Todays Appointements, Recent Medical Records



Doctor Profile

Name: doctor

Specialization: General Medicine

License: DOC123456

Email: doctor@healthcare.com

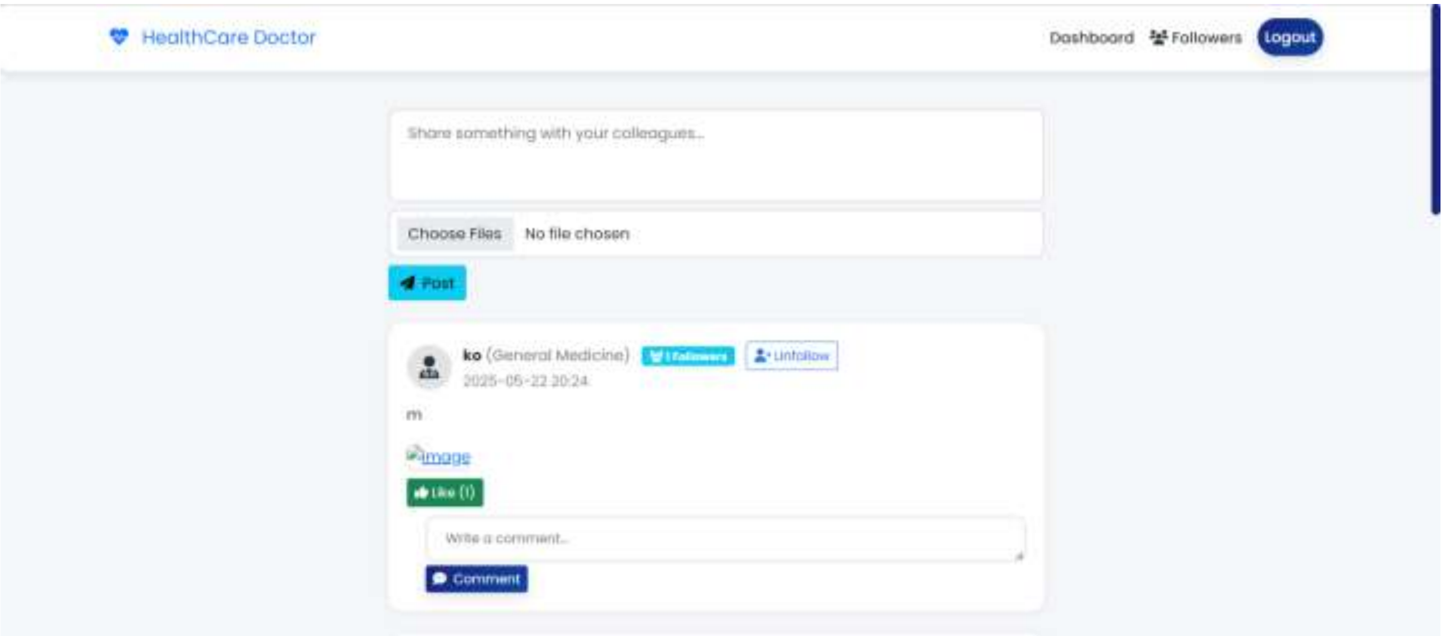
Today's Appointments

Time	Patient	Status
01:11	adham	Scheduled

Recent Medical Records

Patient	Date	Diagnosis
adham	2025-05-24	asdasdasdas...
adham	2025-05-23	fter edit...

And He Can also Enter the Social Feed as He can post, comment & like Other Posts with Doctors to Share Experiences with Other Doctors



Share something with your colleagues...

No file chosen

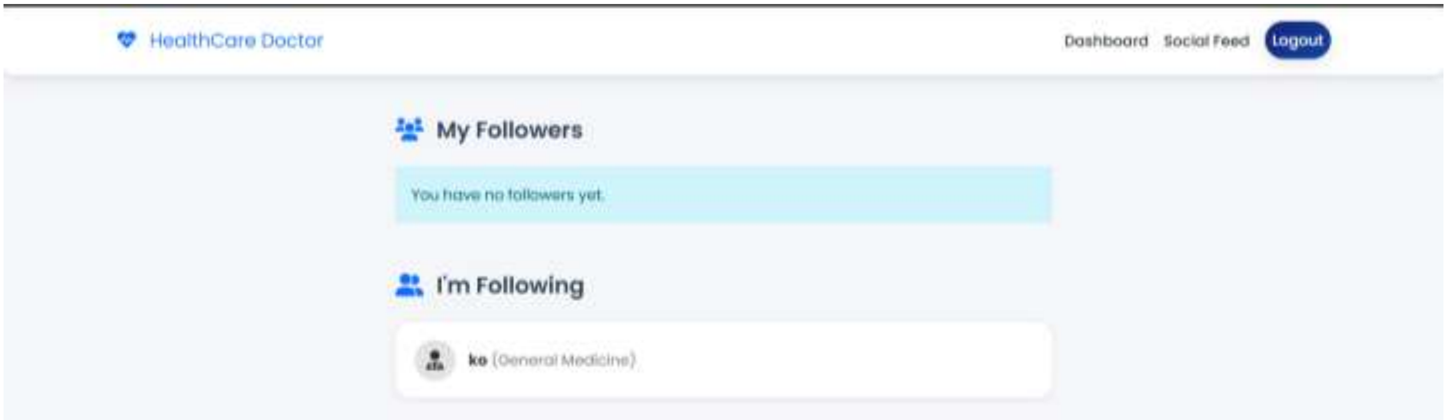
ko (General Medicine)
2025-05-22 20:24

m

image

Write a comment...

Doctor Can See Both the Following & the Followers Lists



My Followers

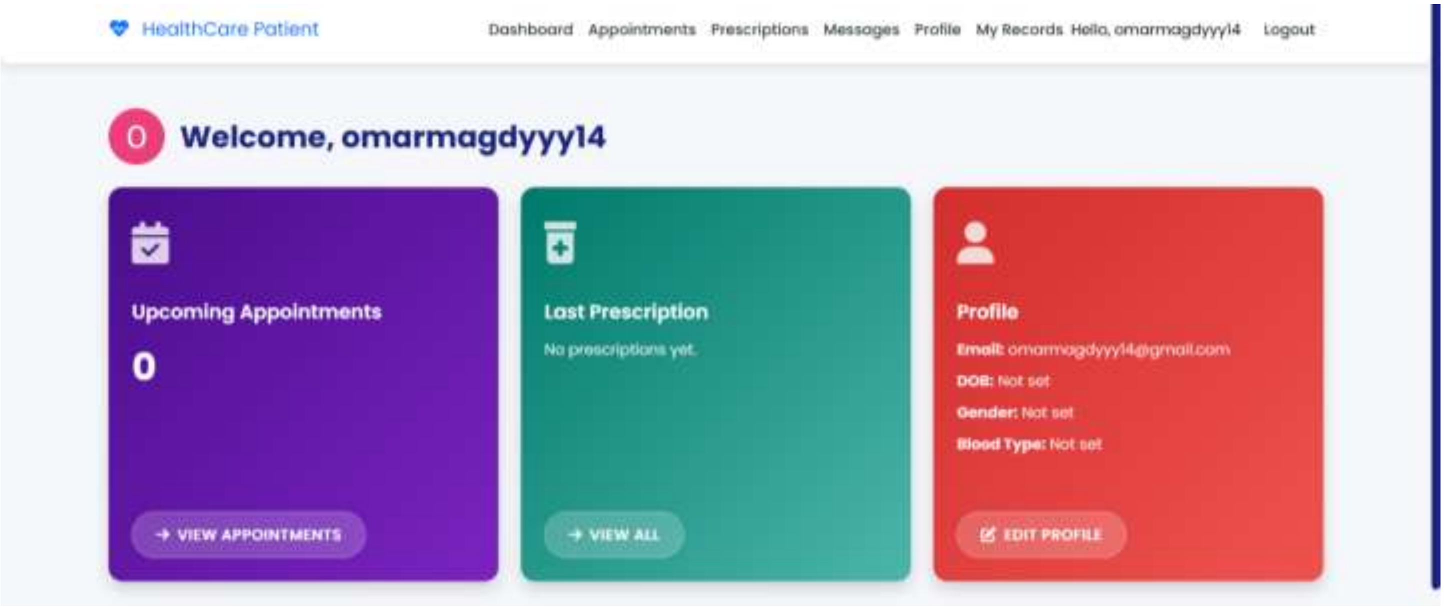
You have no followers yet.

I'm Following

ko (General Medicine)

Registering as a Normal User Page:

User can See Appointments, Lasr Prescription, & can Update his Profile



Welcome, omarmagdyyy14

Upcoming Appointments

0

Last Prescription

No prescriptions yet.

Profile

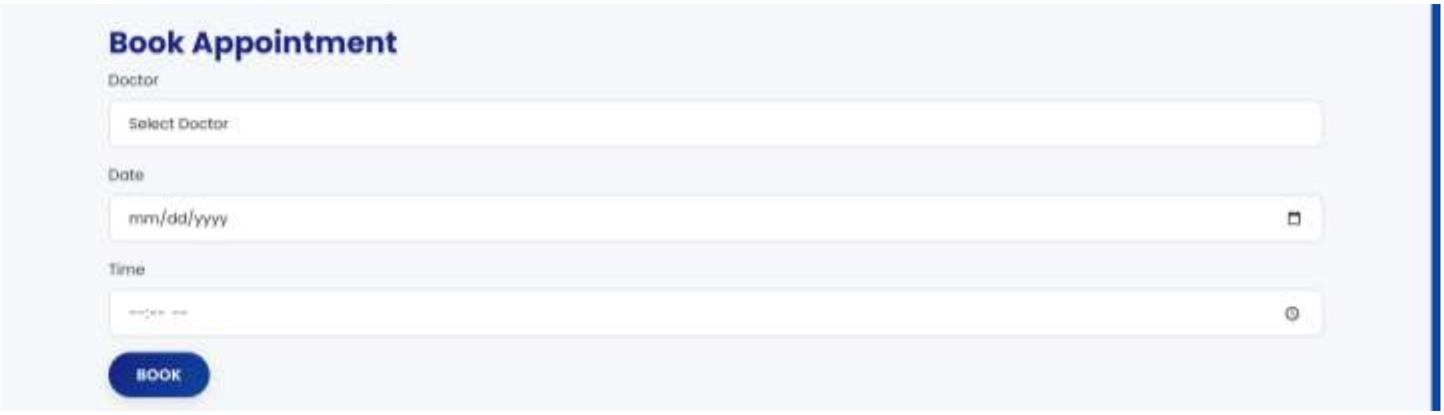
Email: omarmagdyyy14@gmail.com

DOB: Not set

Gender: Not set

Blood Type: Not set

He Can Book new Appointment with specific Doctor He wants



Book Appointment

Doctor

Select Doctor

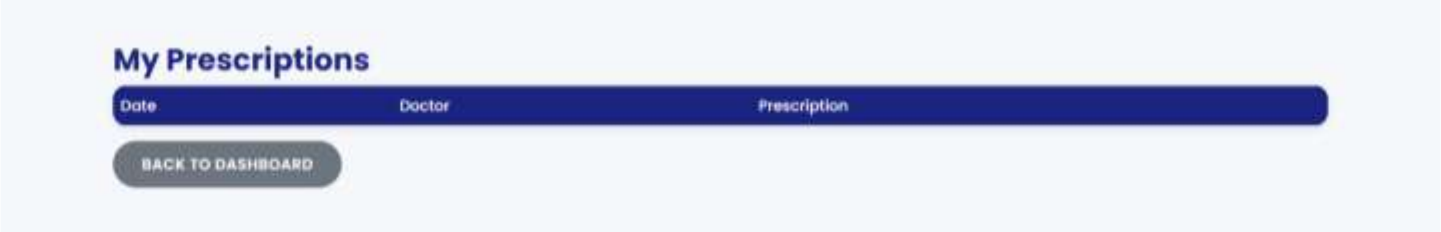
Date

mm/dd/yyyy

Time

--:-- --

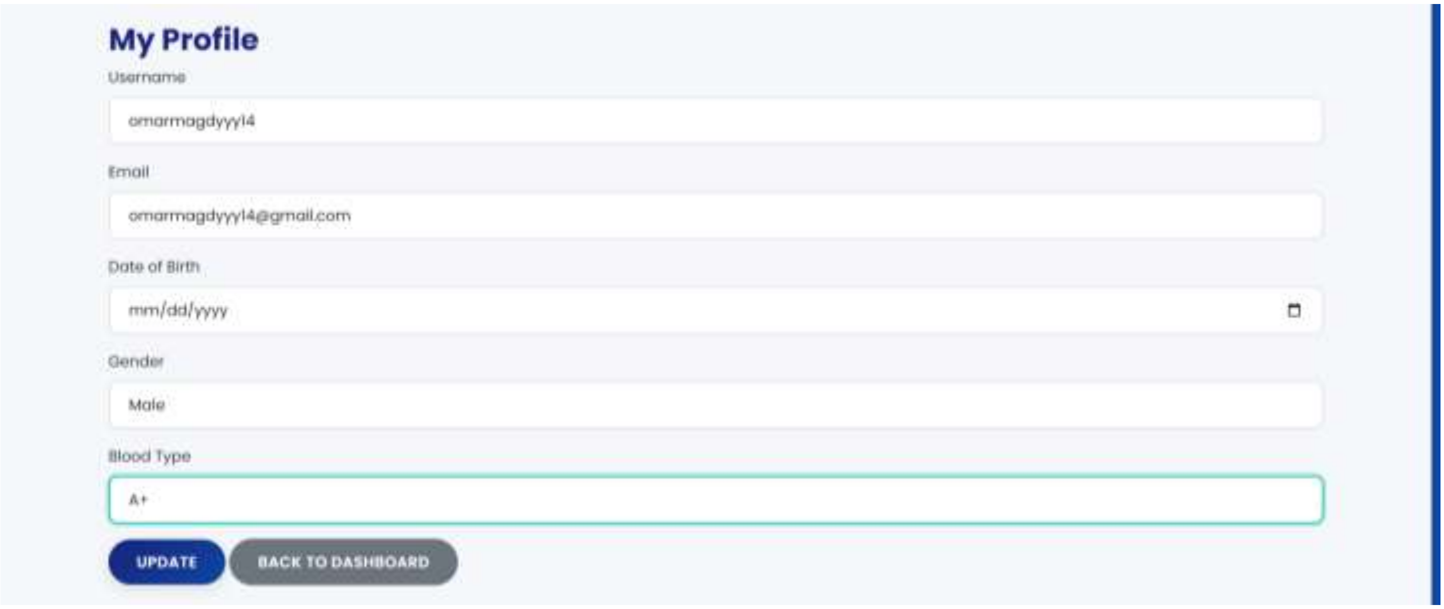
He Can See His Prescriptions



My Prescriptions

Date	Doctor	Prescription

He Can Update his Profile Information



My Profile

Username

omarmagdyyyl4

Email

omarmagdyyyl4@gmail.com

Date of Birth

mm/dd/yyyy

Gender

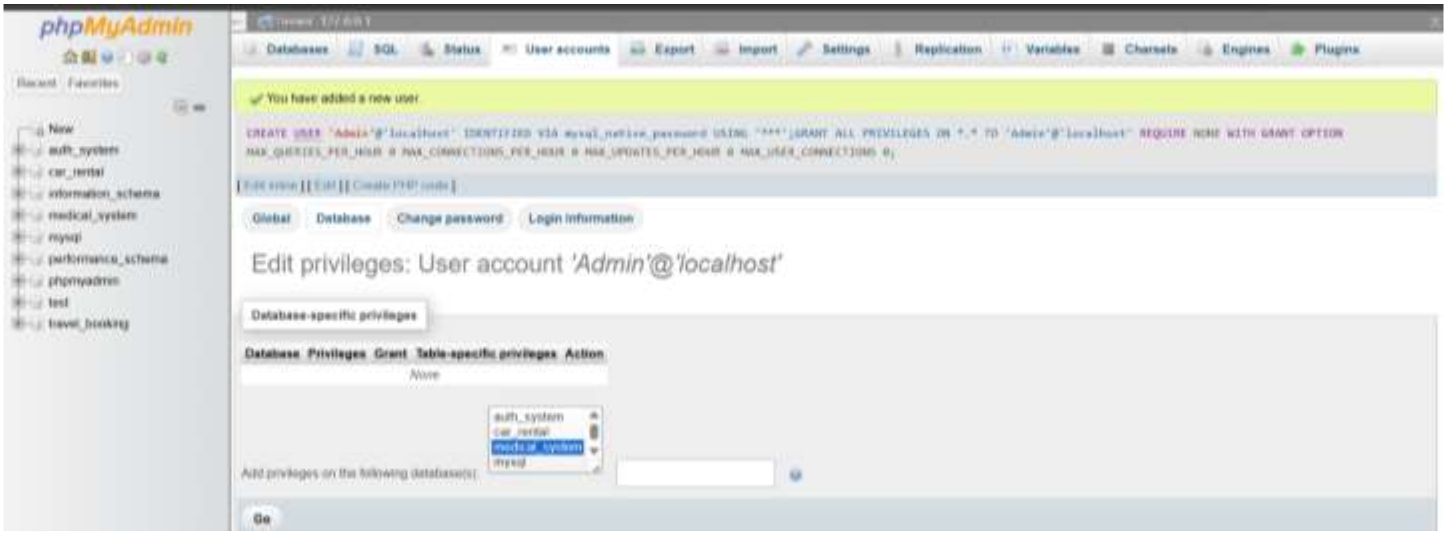
Male

Blood Type

A+

After That We Defined also The Access Control Over The Database

I Created new User as an Admin and Gave him the Privileges of Admin



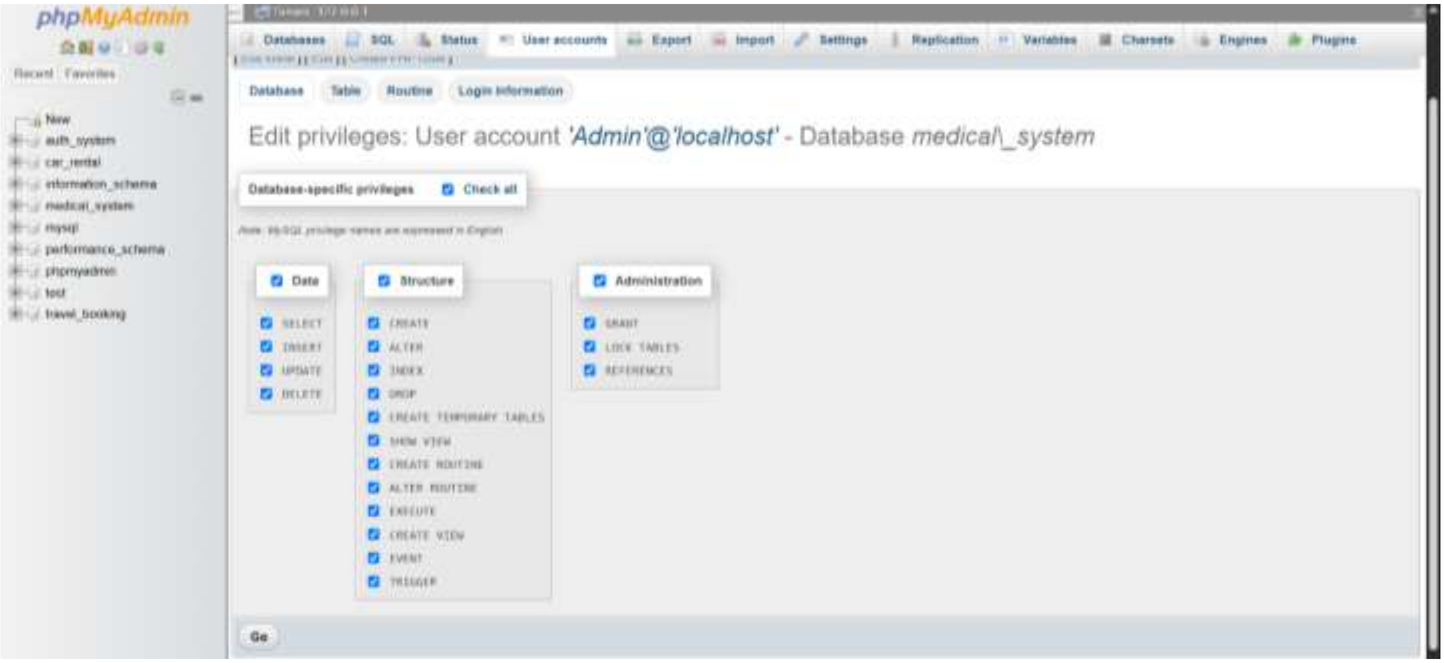
✓ You have added a new user

```
CREATE USER 'Admin'@'localhost' IDENTIFIED VIA mysql_native_password USING '***';GRANT ALL PRIVILEGES ON *.* TO 'Admin'@'localhost' REQUIRE NONE WITH GRANT OPTION
MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0;
```

Edit privileges: User account *'Admin'@'localhost'*

Database	Privileges	Grant	Table-specific privileges	Action
None				

Add privileges on the following database(s): auth_system, car_rental, medical_system, mysql



Edit privileges: User account *'Admin'@'localhost'* - Database *medical_system*

Database-specific privileges ☑ Check all

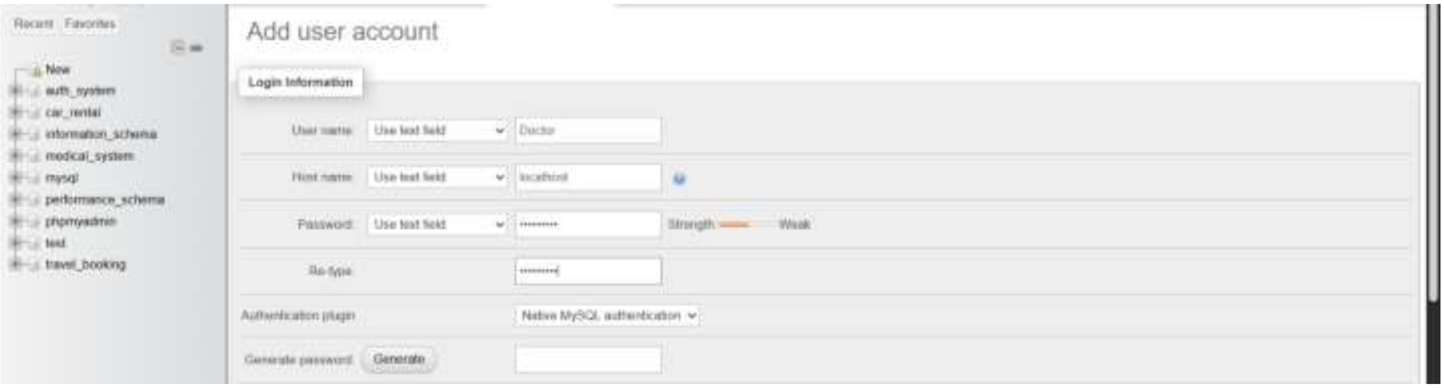
Note: MySQL privilege names are expressed in English

☑ Data
- ☑ SELECT
- ☑ INSERT
- ☑ UPDATE
- ☑ DELETE

☑ Structure
- ☑ CREATE
- ☑ ALTER
- ☑ INDEX
- ☑ DROP
- ☑ CREATE TEMPORARY TABLES
- ☑ SHOW VIEW
- ☑ CREATE ROUTINE
- ☑ ALTER ROUTINE
- ☑ EXECUTE
- ☑ CREATE VIEW
- ☑ EVENT
- ☑ TRIGGER

☑ Administration
- ☑ GRANT
- ☑ LOCK TABLES
- ☑ REFERENCES

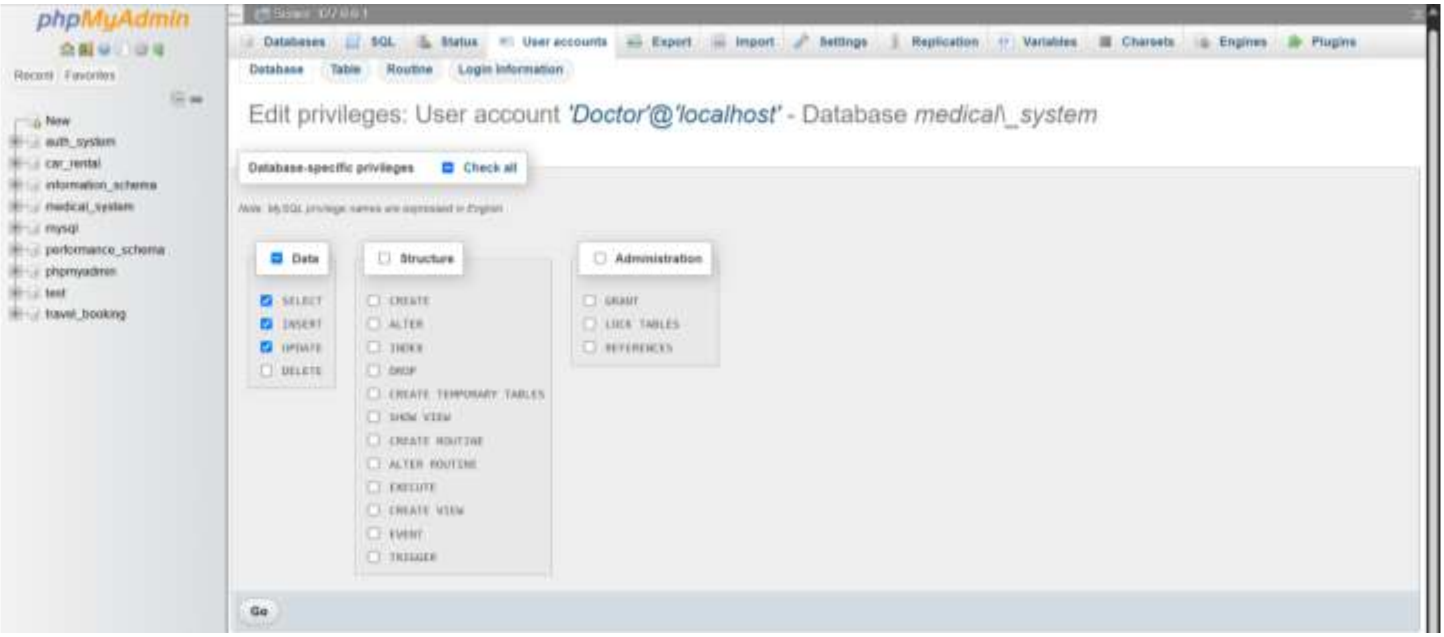
I Created new User as an Doctor and Gave him the Privileges of Doctor



Add user account

Login Information

User name:	Use text field	Doctor
Host name:	Use text field	localhost
Password:	Use text field	•••••••• Strength: Weak
Re-type:		••••••••
Authentication plugin		Native MySQL authentication
Generate password:	Generate	



Edit privileges: User account *'Doctor'@'localhost'* - Database *medical_system*

Database-specific privileges ☑ Check all

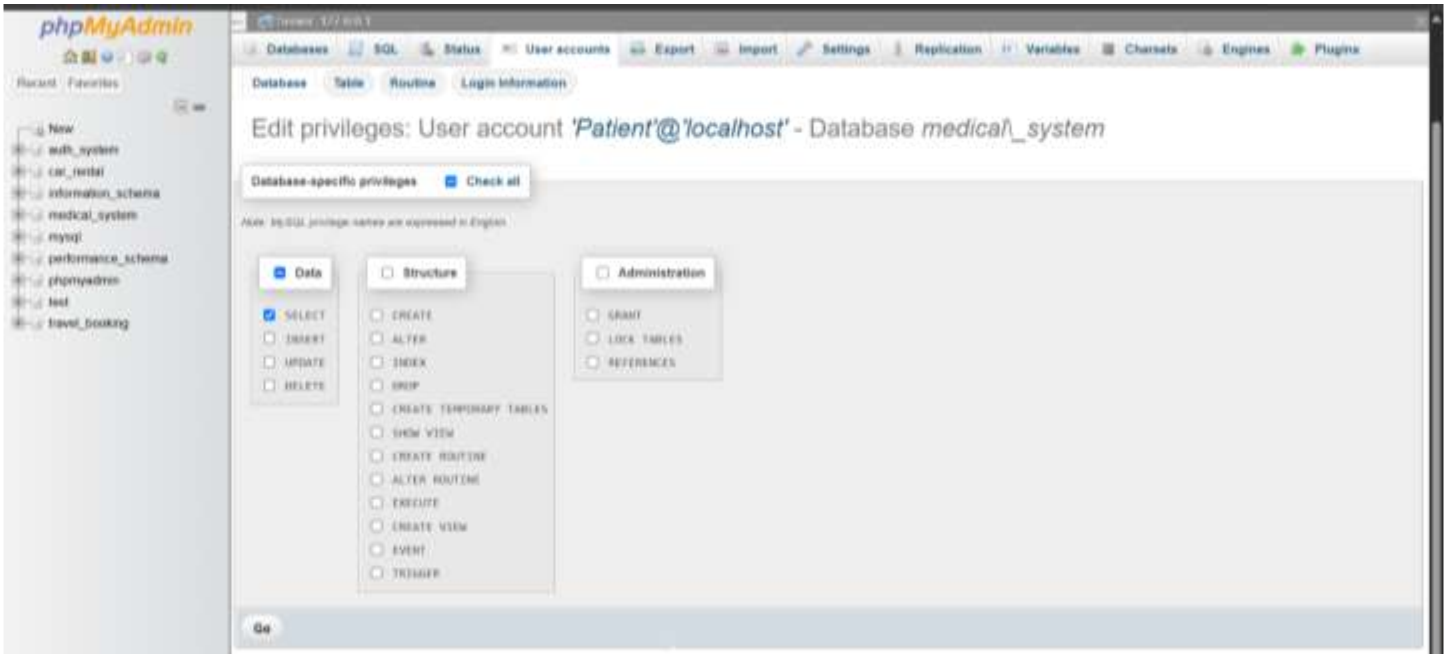
Note: MySQL privilege names are expressed in English

☑ Data
- ☑ SELECT
- ☑ INSERT
- ☑ UPDATE
- □ DELETE

□ Structure
- □ CREATE
- □ ALTER
- □ INDEX
- □ DROP
- □ CREATE TEMPORARY TABLES
- □ SHOW VIEW
- □ CREATE ROUTINE
- □ ALTER ROUTINE
- □ EXECUTE
- □ CREATE VIEW
- □ EVENT
- □ TRIGGER

□ Administration
- □ GRANT
- □ LOCK TABLES
- □ REFERENCES

I Created new User as an Patient and Gave him the Privileges of Patient



Edit privileges: User account *'Patient'@'localhost'* - Database *medical_system*

Database-specific privileges ☑ Check all

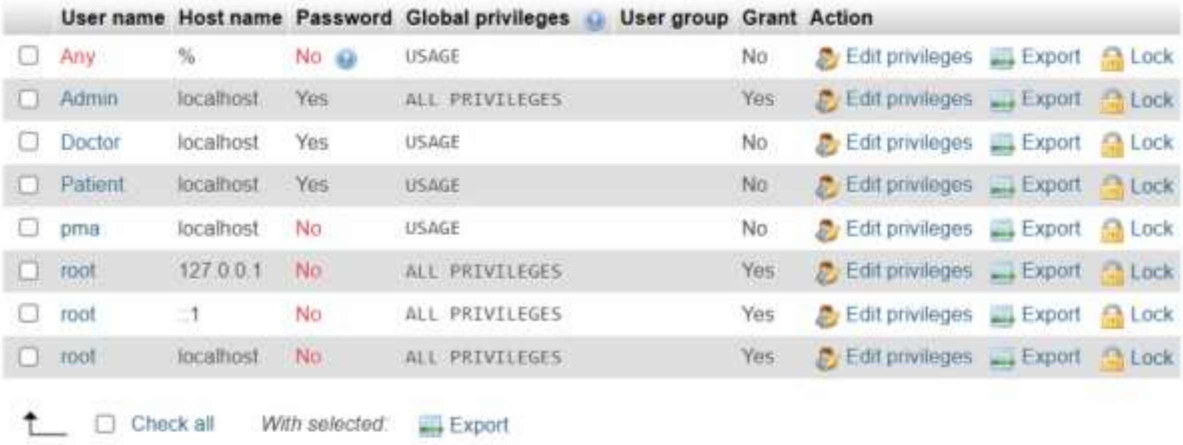
Note: MySQL privilege names are expressed in English

☑ Data
- ☑ SELECT
- ☐ INSERT
- ☐ UPDATE
- ☐ DELETE

☐ Structure
- ☐ CREATE
- ☐ ALTER
- ☐ INDEX
- ☐ DROP
- ☐ CREATE TEMPORARY TABLES
- ☐ SHOW VIEW
- ☐ CREATE ROUTINE
- ☐ ALTER ROUTINE
- ☐ EXECUTE
- ☐ CREATE VIEW
- ☐ EVENT
- ☐ TRIGGER

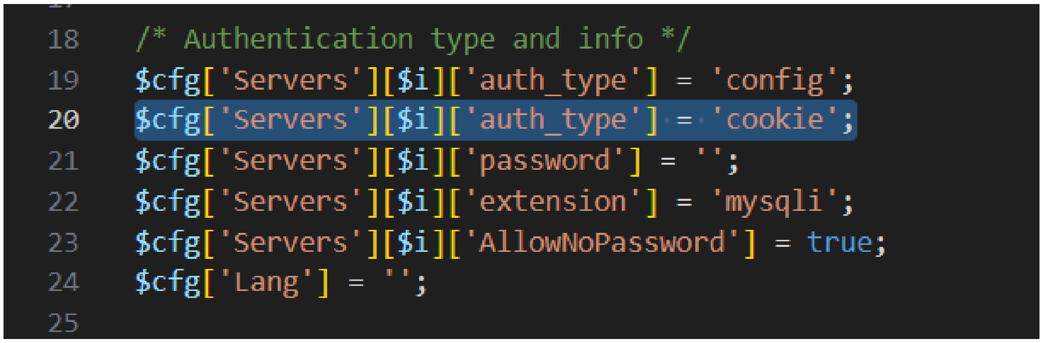
☐ Administration
- ☐ GRANT
- ☐ LOCK TABLES
- ☐ REFERENCES

Now We have Created 3 Users With Different Roles On Database



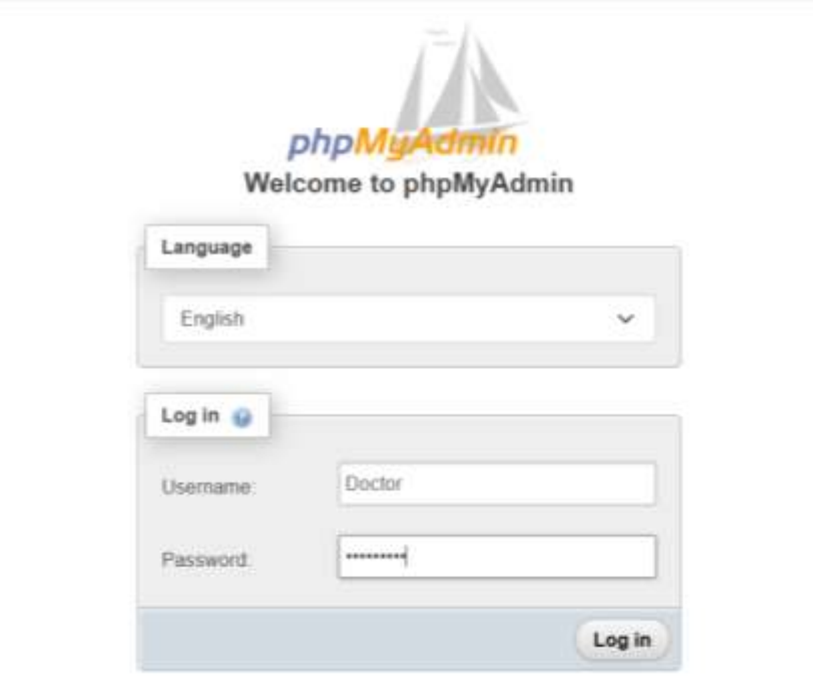
	User name	Host name	Password	Global privileges	User group	Grant	Action		
☐	Any	%	No	USAGE		No	Edit privileges	Export	Lock
☐	Admin	localhost	Yes	ALL PRIVILEGES		Yes	Edit privileges	Export	Lock
☐	Doctor	localhost	Yes	USAGE		No	Edit privileges	Export	Lock
☐	Patient	localhost	Yes	USAGE		No	Edit privileges	Export	Lock
☐	pma	localhost	No	USAGE		No	Edit privileges	Export	Lock
☐	root	127.0.0.1	No	ALL PRIVILEGES		Yes	Edit privileges	Export	Lock
☐	root	::1	No	ALL PRIVILEGES		Yes	Edit privileges	Export	Lock
☐	root	localhost	No	ALL PRIVILEGES		Yes	Edit privileges	Export	Lock

After that I go to this file to Update this line in The File C:\xamppp\phpMyAdmin\config.inc.php to make the server request From me my Credentials to login and not login as a root directly



```
/* Authentication type and info */
$cfg['Servers'][$i]['auth_type'] = 'config';
$cfg['Servers'][$i]['auth_type'] = 'cookie';
$cfg['Servers'][$i]['password'] = '';
$cfg['Servers'][$i]['extension'] = 'mysqli';
$cfg['Servers'][$i]['AllowNoPassword'] = true;
$cfg['Lang'] = '';
```

Now it Requests my Credentials to Login so I logged in as a Doctor:



Welcome to phpMyAdmin

Language

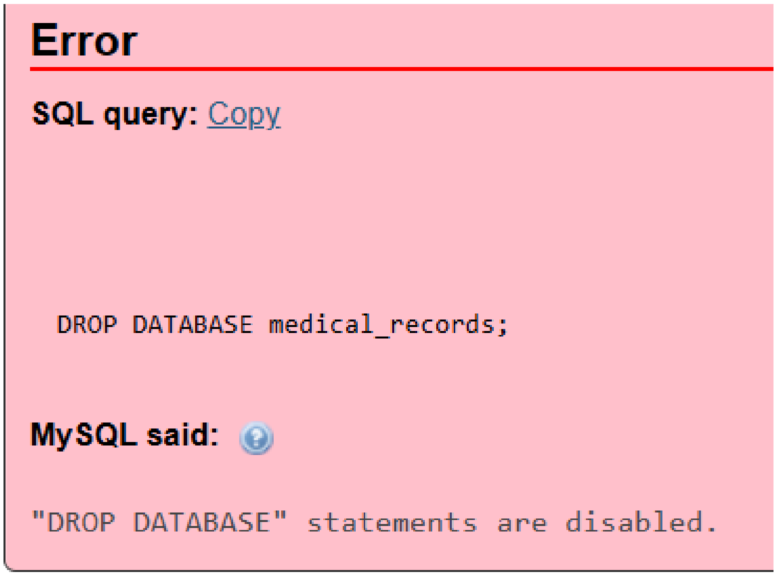
English

Log in

Username: Doctor

Password: ••••••••••

I tried to Drop the medical_records by the privileges of the Doctor but it Refused:



Error

SQL query: Copy

```
DROP DATABASE medical_records;
```

MySQL said:

```
"DROP DATABASE" statements are disabled.
```

So Everything Works Well