BRAC UNIVERSITY

Inspiring Excellence

CSE370 : Database Systems
Project Report
Project Title :Integrated Multi-Hospital Management System for District-Level Healthcare Coordination

Group No : 10, CSE370 Lab Section : 4, Summer 2025		
ID	**Name**	**Contribution**
19301102	Ibnul Ahsan Mayukh	Backend: Person, manages tables; Frontend+Backend: Patient registration + update, appointment management(CRUD), bill payment, view treatment; EER(partial); Schema + normalization;
20201089	Rezowana Mehjabin Lorel	Backend : Role based access control, Medical history and patient dashboard Frontend : CRUD (login and log out)

21301594	Mydul Islam Lisun	Frontend and backend of Inventory management and Analytics Dashboard for district health authority CRUD. EER (partial)

Table of Contents

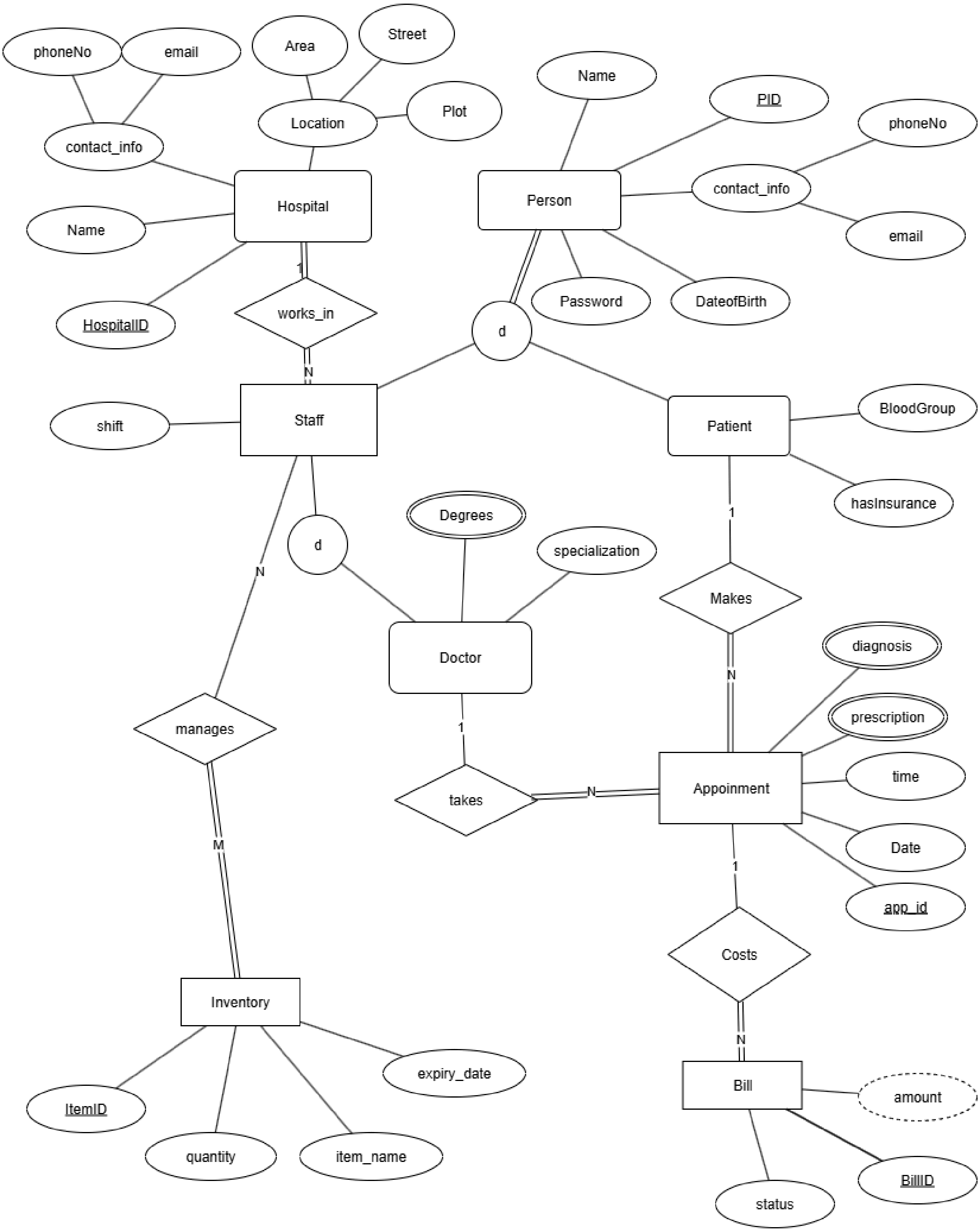
Introduction

In the current world, the health care sector faces a major challenge in managing patient data, appointments, medical records, and administrative duties for various reasons. Conventional hospital management systems most commonly function in silos, resulting in inefficiencies and communication breakdowns that can easily affect operational efficacy and patient care. Our project the Integrated Multi-Hospital Management System is a single platform which offers a complete solution created to optimize healthcare operations across several medical facilities. This system helps to connect patients, doctors, and administrative staff in a seamless network. Therefore, it also enables efficient information sharing, medical record management, appointment scheduling, and billing processes. This project aims to recover the bridge gap that healthcare systems fail to achieve by maintaining strict security and privacy standards for sensitive patient information.

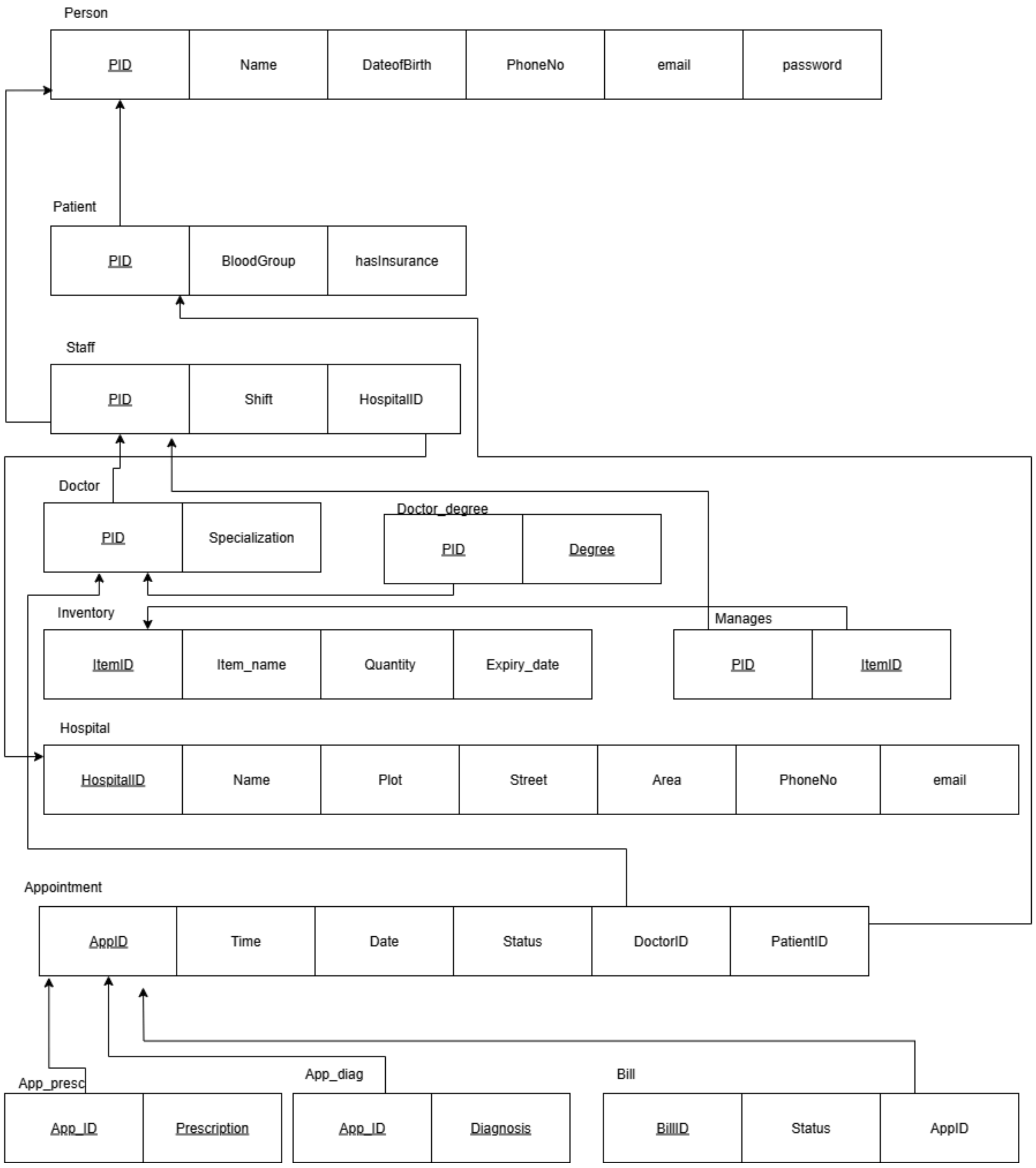
Project Features

ID, Name	Features [3 per member]	
19301102, Ibnul Ahsan Mayukh	Ft 1	Doctor Scheduling with conflict checks
	Ft 2	Billing System with insurance integration
	Ft 3	Patient CRUD and appointment CRUD
20201089, Rezowana Mehjabin Lorel	Ft 1	Role based access control
	Ft 2	Medical history and patient dashboard
	Ft 3	CRUD
21301594, Mydul Islam Lisun	Ft 1	Inventory Management
	Ft 2	Analytics Dashboard for district health authority
	Ft 3	Inventory and Hospital CRUD

ER/EER Diagram



Schema Diagram



Normalization

a. Explain if your converted Schema is in 1NF or not. If not, decompose it to 1NF.

Ans: Already in 1NF. No composite attributes, multivalued attributes or nested relations exist.

b. Explain if your converted Schema is in 2NF or not. If not, decompose it to 2NF. Can there be any partial functional dependencies in your relational schema?

Ans: Already in 2NF. No partial functional dependencies in the schema.

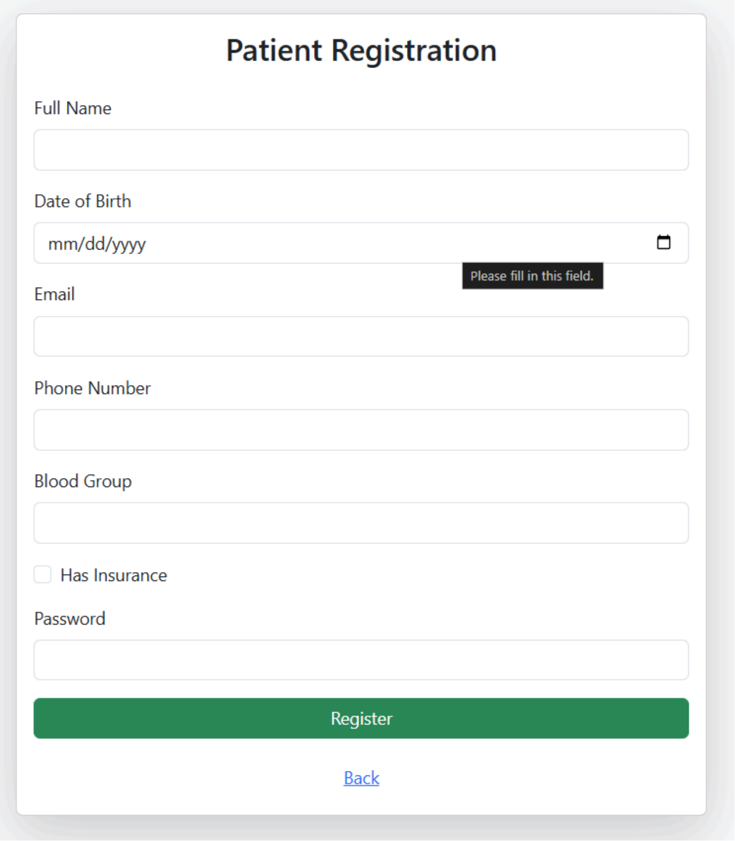
c. Explain if your converted Schema is in 3NF or not. If not, decompose it to 3NF. Can there be any transitive dependencies in your relational schema?

Ans: Already in 3NF. No transitive functional dependencies in the schema.

Frontend Development

Contribution of ID : 19301102, Name : Ibnul Ahsan Mayukh

Patients can register by entering their information.



Patient Registration

Full Name

Date of Birth

mm/dd/yyyy

Please fill in this field.

Email

Phone Number

Blood Group

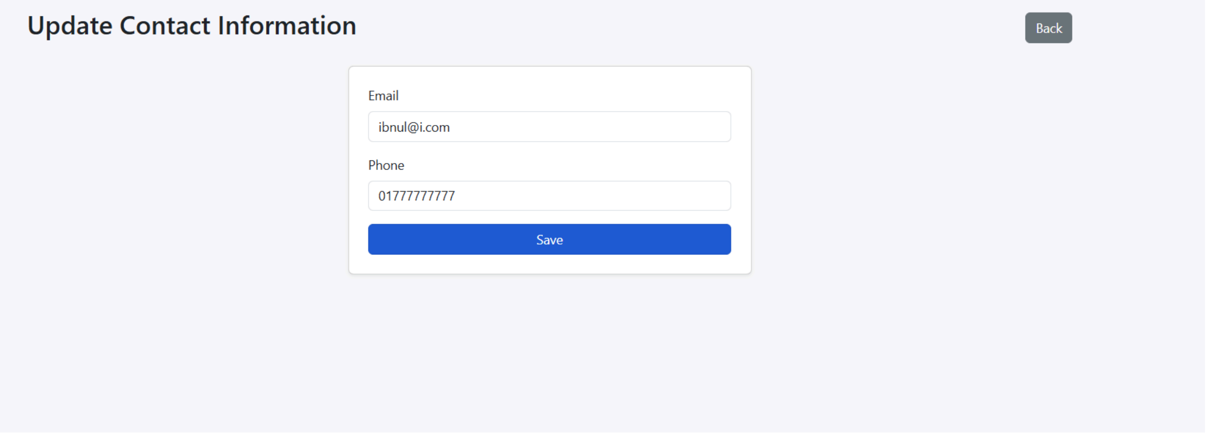
□ Has Insurance

Password

Register

Back

Patients can change their contact information later.



Update Contact Information

Back

Email

ibnul@i.com

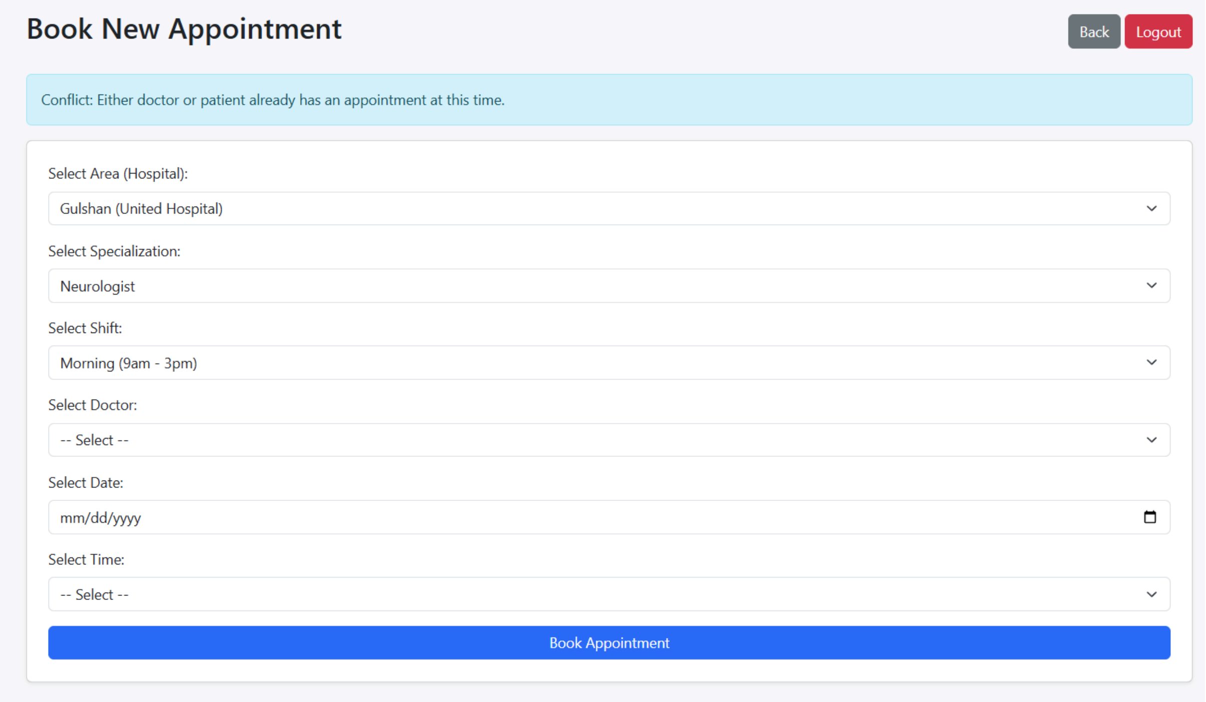
Phone

01777777777

Save

Doctor Scheduling with conflict checks

Created a form where patients can make appointments. Patients choose an area close to them and then a specialization they are listed in from a drop down list. Next the patient can choose either morning or evening. Next the patient picks the date and time and the doctor they are interested in. For dates the patient can only pick dates that are later than today, and not earlier or present day. The time is picked from half hour slots. There is a check to ensure that no doctor can have multiple appointments at the same time slot.



Book New Appointment

Conflict: Either doctor or patient already has an appointment at this time.

Select Area (Hospital): Gulshan (United Hospital)

Select Specialization: Neurologist

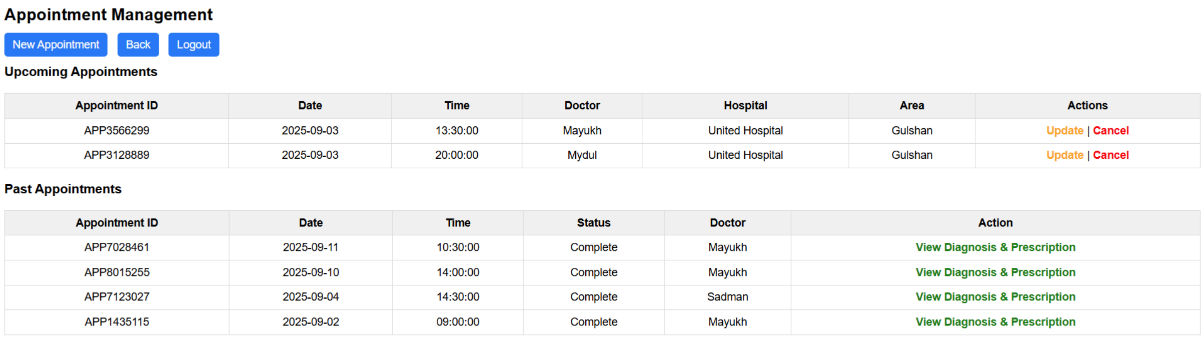
Select Shift: Morning (9am - 3pm)

Select Doctor: -- Select --

Select Date: mm/dd/yyyy

Select Time: -- Select --

Patients can reschedule or cancel upcoming appointments.



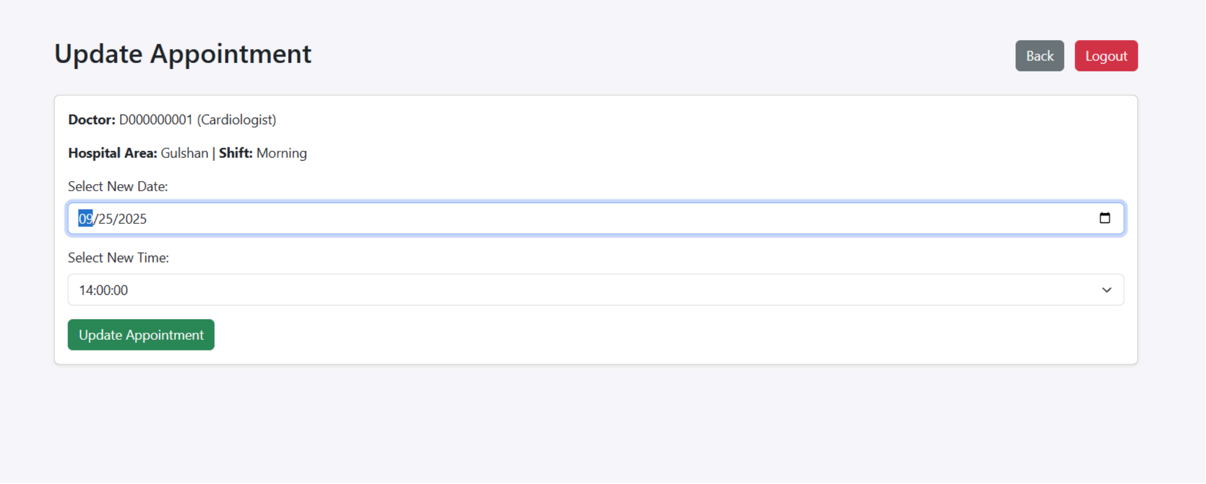
Appointment Management

Upcoming Appointments

Appointment ID	Date	Time	Doctor	Hospital	Area	Actions
APP3566299	2025-09-03	13:30:00	Mayukh	United Hospital	Gulshan	Update | Cancel
APP3128889	2025-09-03	20:00:00	Mydul	United Hospital	Gulshan	Update | Cancel

Past Appointments

Appointment ID	Date	Time	Status	Doctor	Action
APP7028461	2025-09-11	10:30:00	Complete	Mayukh	View Diagnosis & Prescription
APP8015255	2025-09-10	14:00:00	Complete	Mayukh	View Diagnosis & Prescription
APP7123027	2025-09-04	14:30:00	Complete	Sadman	View Diagnosis & Prescription
APP1435115	2025-09-02	09:00:00	Complete	Mayukh	View Diagnosis & Prescription



Update Appointment

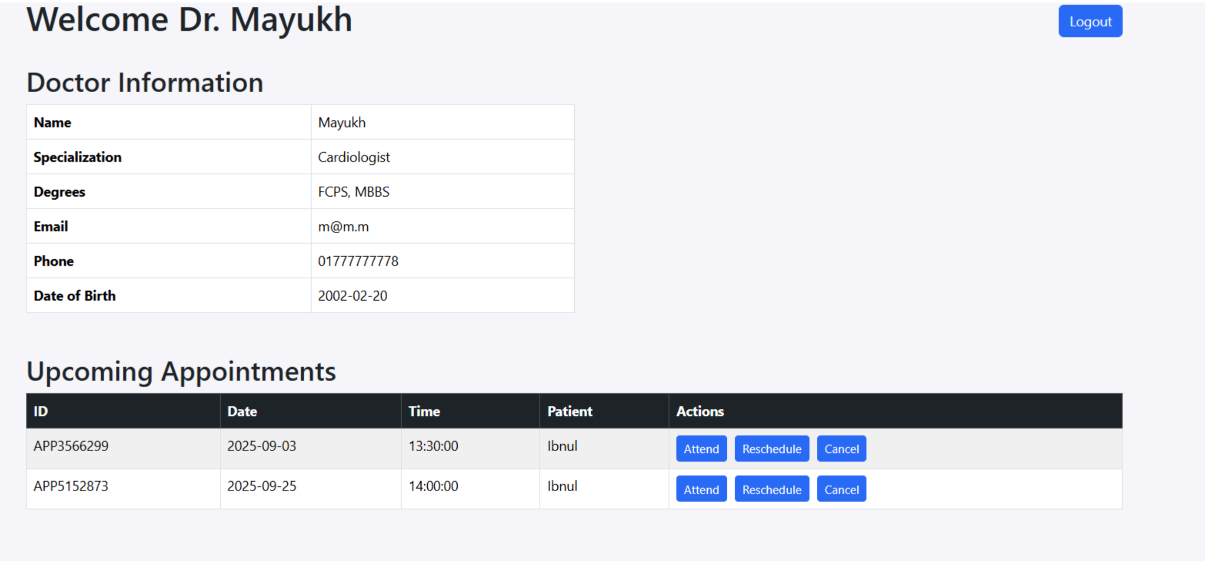
Doctor: D000000001 (Cardiologist)

Hospital Area: Gulshan | **Shift:** Morning

Select New Date: 09/25/2025

Select New Time: 14:00:00

Doctors can reschedule or cancel upcoming appointments.



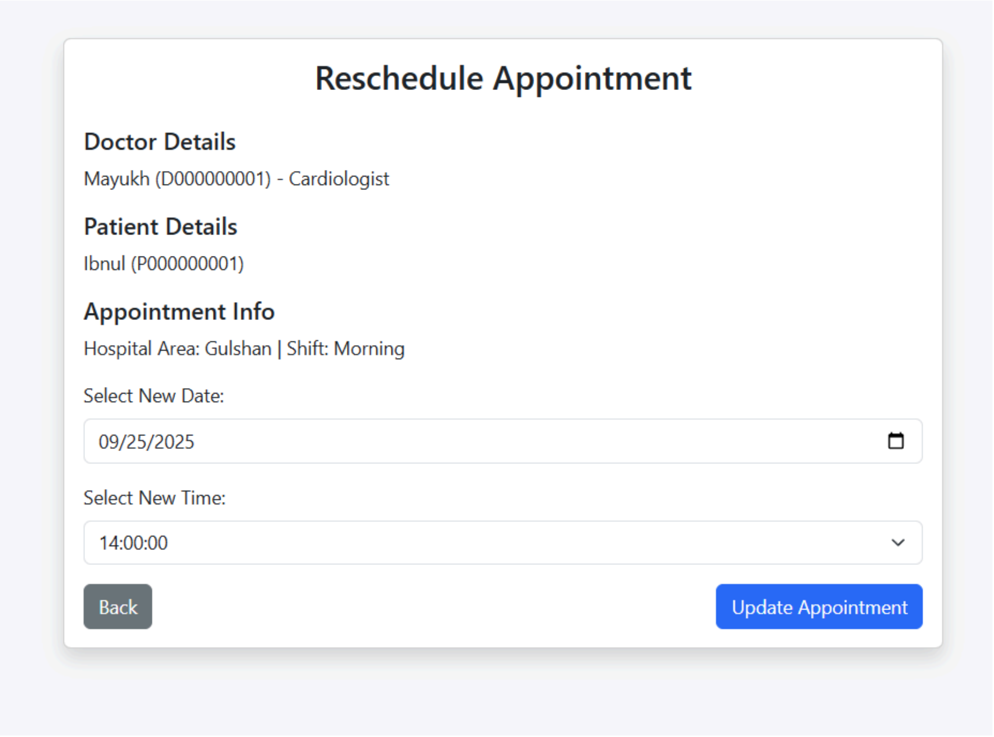
Welcome Dr. Mayukh

Doctor Information

Name	Mayukh
Specialization	Cardiologist
Degrees	FCPS, MBBS
Email	m@m.m
Phone	01777777778
Date of Birth	2002-02-20

Upcoming Appointments

ID	Date	Time	Patient	Actions
APP3566299	2025-09-03	13:30:00	Ibnul	Attend Reschedule Cancel
APP5152873	2025-09-25	14:00:00	Ibnul	Attend Reschedule Cancel



Reschedule Appointment

Doctor Details

Mayukh (D000000001) - Cardiologist

Patient Details

Ibnul (P000000001)

Appointment Info

Hospital Area: Gulshan | Shift: Morning

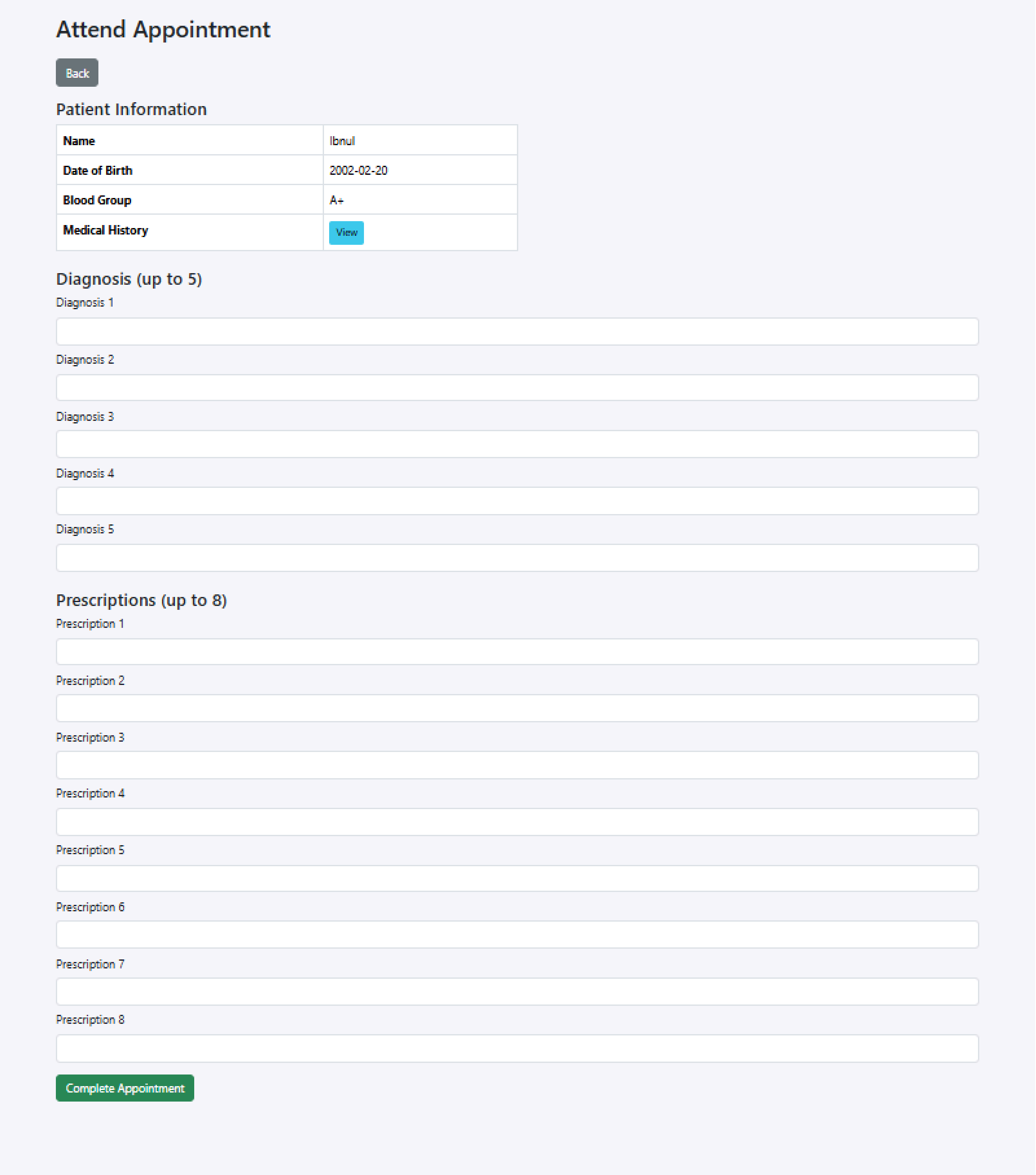
Select New Date:

09/25/2025

Select New Time:

14:00:00

Doctors can complete appointments by giving diagnosis and prescriptions in a form.



Attend Appointment

Patient Information

Name	Ibnul
Date of Birth	2002-02-20
Blood Group	A+
Medical History	View

Diagnosis (up to 5)

Diagnosis 1

Diagnosis 2

Diagnosis 3

Diagnosis 4

Diagnosis 5

Prescriptions (up to 8)

Prescription 1

Prescription 2

Prescription 3

Prescription 4

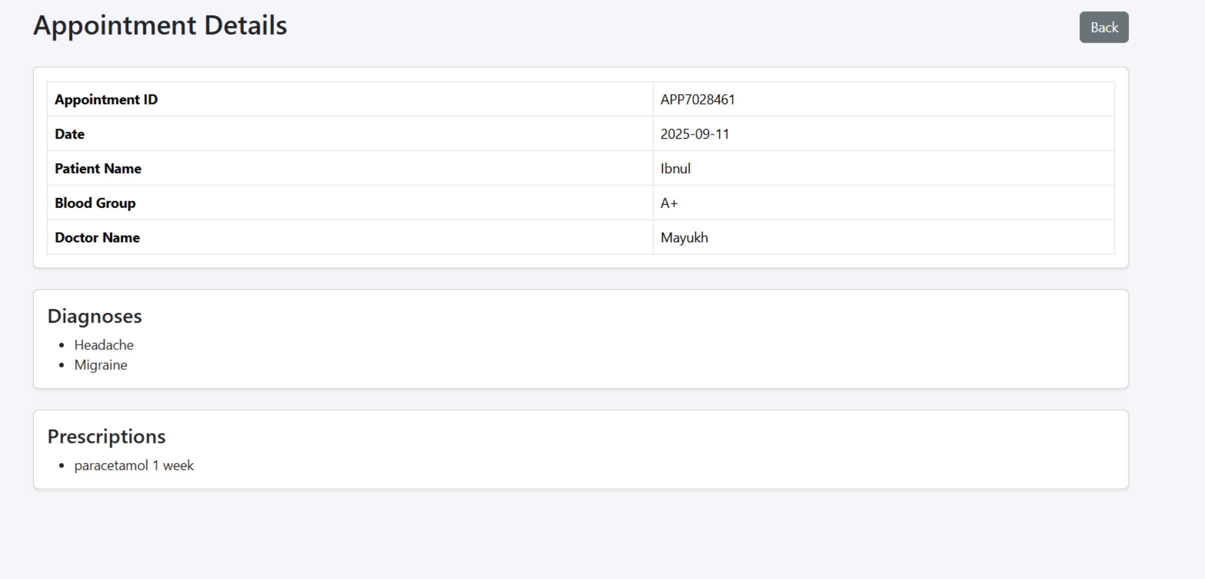
Prescription 5

Prescription 6

Prescription 7

Prescription 8

Patients can see what diagnosis and prescriptions were given by the doctor by going to the appointment management screen and pressing the button that shows all the diagnosis and prescription from a particular appointment.



Appointment Details

Appointment ID	APP7028461
Date	2025-09-11
Patient Name	Ibnul
Blood Group	A+
Doctor Name	Mayukh

Diagnoses

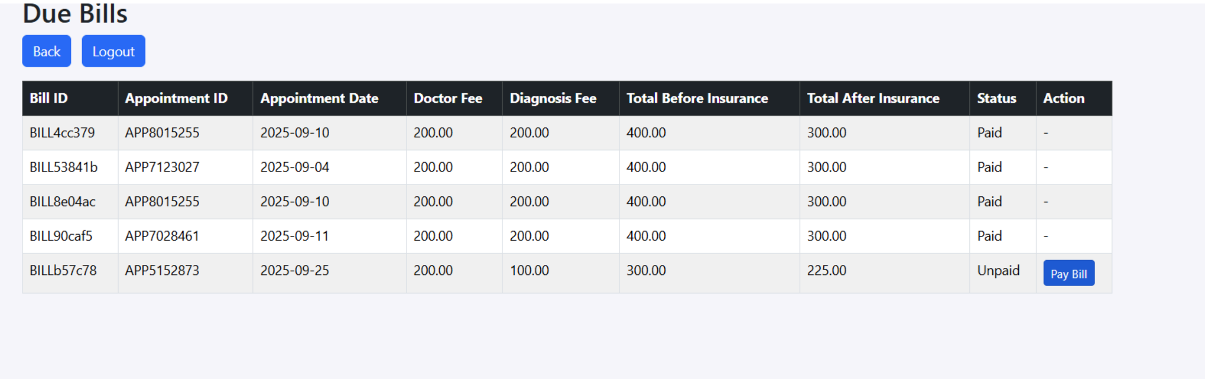
- Headache
- Migraine

Prescriptions

- paracetamol 1 week

Billing System with insurance integration

Patients can check their bill by going to the view bills screen. If an appointment has been completed by a doctor, a bill is generated. If the patient has hasinsurance = 1, the patient gets a 25% discount on their total bill. Patients can pay their bill by pressing the pay button.

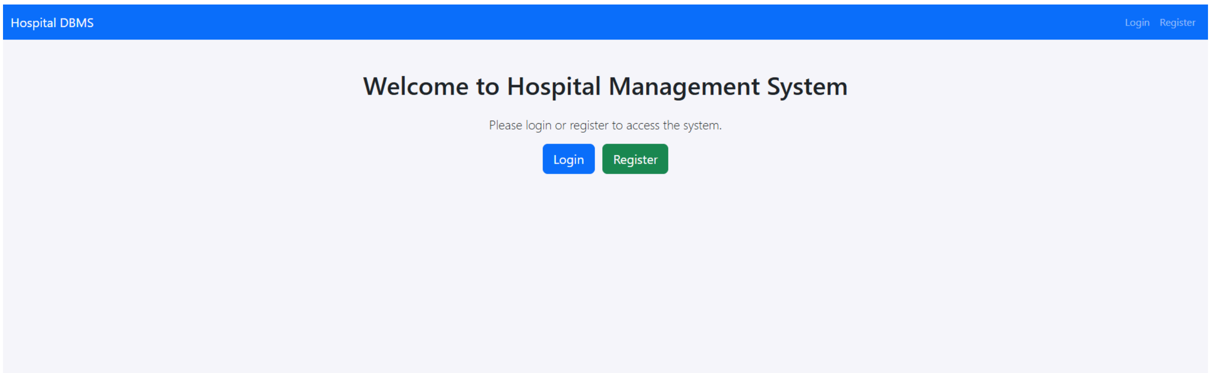


Due Bills

Bill ID	Appointment ID	Appointment Date	Doctor Fee	Diagnosis Fee	Total Before Insurance	Total After Insurance	Status	Action
BILL4cc379	APP8015255	2025-09-10	200.00	200.00	400.00	300.00	Paid	-
BILL53841b	APP7123027	2025-09-04	200.00	200.00	400.00	300.00	Paid	-
BILL8e04ac	APP8015255	2025-09-10	200.00	200.00	400.00	300.00	Paid	-
BILL90caf5	APP7028461	2025-09-11	200.00	200.00	400.00	300.00	Paid	-
BILLb57c78	APP5152873	2025-09-25	200.00	100.00	300.00	225.00	Unpaid	Pay Bill

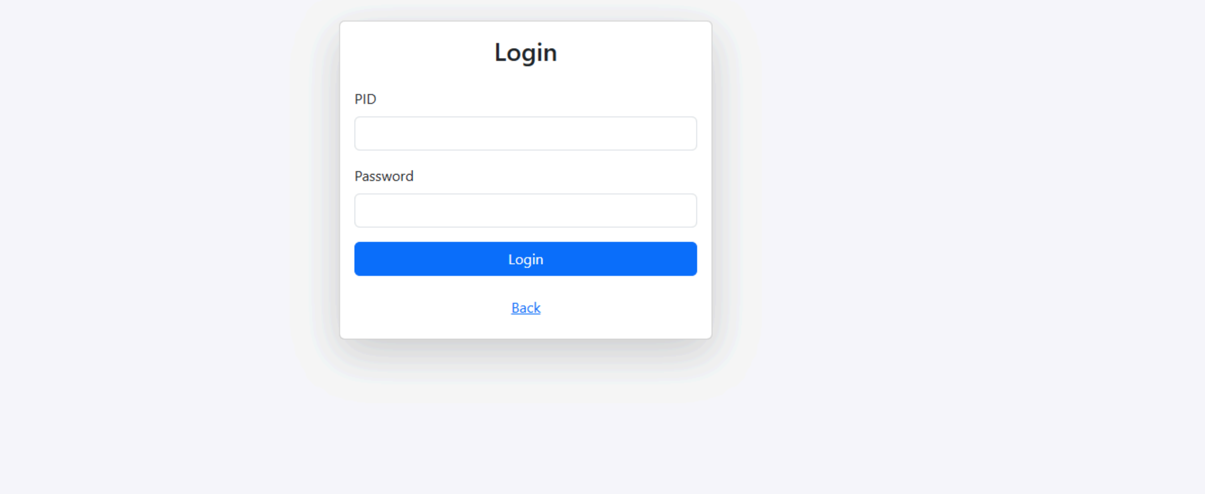
Contribution of ID : 20201089, Name : Rezowana Mehjabin Lorel

Login and logout :



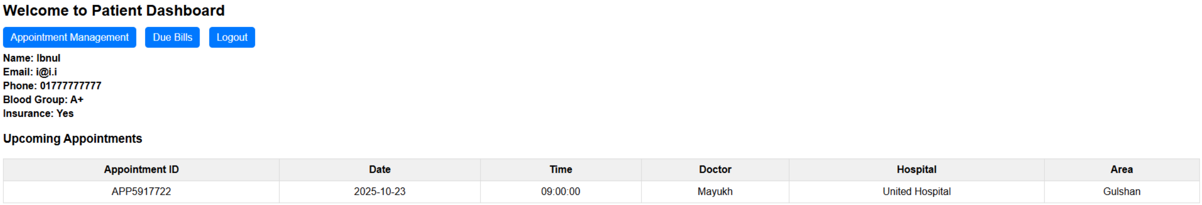
Welcome to Hospital Management System

Please login or register to access the system.



In this part, patients, doctors and admin can login and logout from their designated page. Here, the authentication method uses direct password comparison and after completing successful login the session starts. By checking existence in role-specific tables it determines the user role.

Patient Dashboard :



Welcome to Patient Dashboard

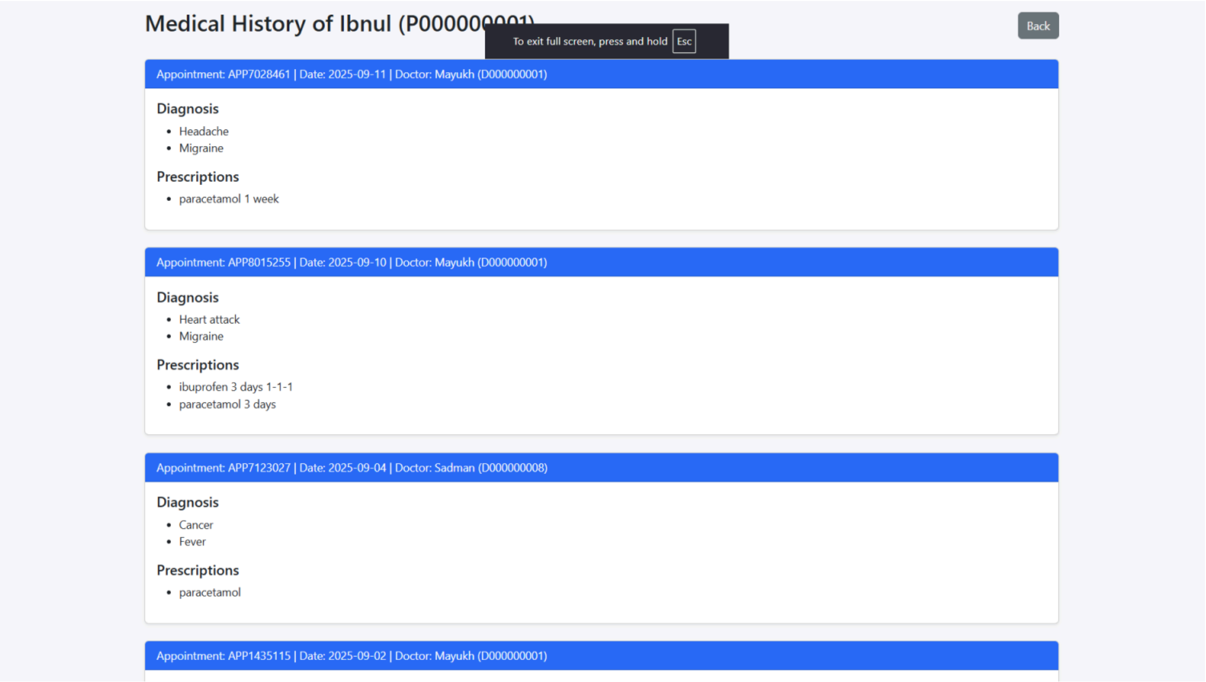
Name: Ibnul
Email: i@i.i
Phone: 01777777777
Blood Group: A+
Insurance: Yes

Upcoming Appointments

Appointment ID	Date	Time	Doctor	Hospital	Area
APP5917722	2025-10-23	09:00:00	Mayukh	United Hospital	Gulshan

Here, the upcoming appointments list can be seen by the patient only. The doctor and admin will have no access to the patient dashboard.

Medical History :



Medical History of Ibnul (P000000001)

To exit full screen, press and hold Esc

Appointment: APP7028461 | Date: 2025-09-11 | Doctor: Mayukh (D000000001)

Diagnosis

- Headache
- Migraine

Prescriptions

- paracetamol 1 week

Appointment: APP8015255 | Date: 2025-09-10 | Doctor: Mayukh (D000000001)

Diagnosis

- Heart attack
- Migraine

Prescriptions

- ibuprofen 3 days 1-1-1
- paracetamol 3 days

Appointment: APP7123027 | Date: 2025-09-04 | Doctor: Sadman (D000000008)

Diagnosis

- Cancer
- Fever

Prescriptions

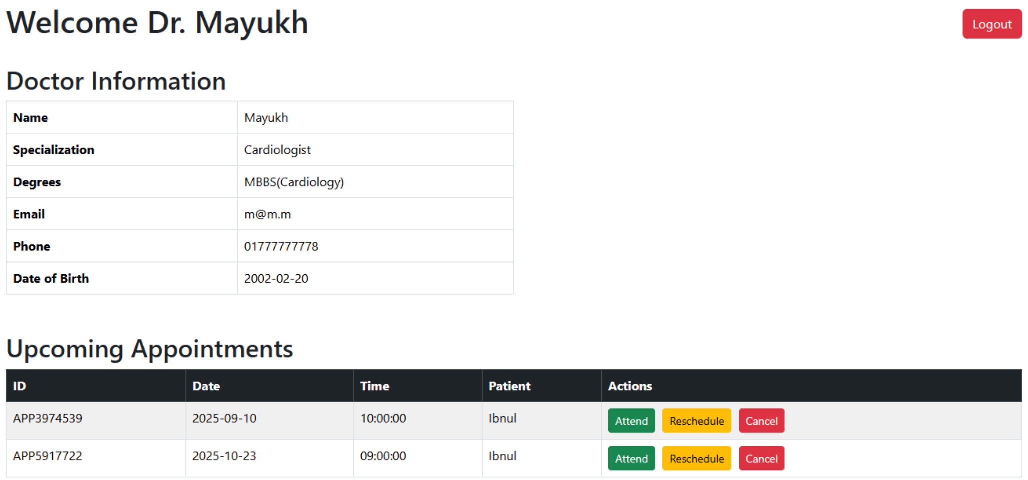
- paracetamol

Appointment: APP1435115 | Date: 2025-09-02 | Doctor: Mayukh (D000000001)

In this part of the project , prescriptions ,diagnosis, appointed doctors name and hospital name is visible. Doctors can access this page . Therefore, doctors can easily review diagnoses and prescriptions from previous consultations and understand the patient's treatment history across multiple visits.

Role based access control :

This feature will help the users to protect a page and ensures that only authorized users can view it .



Welcome Dr. Mayukh

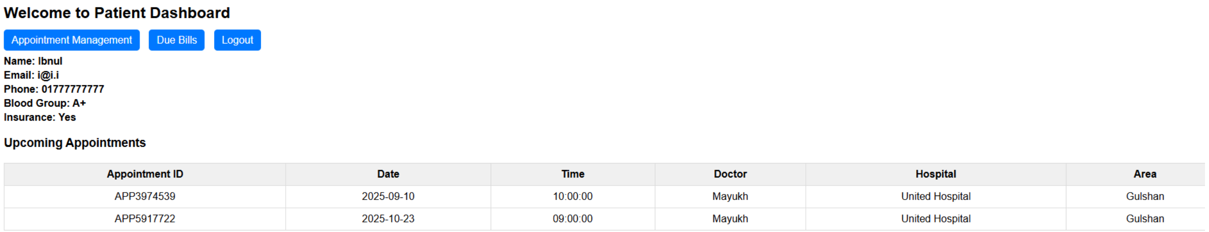
Doctor Information

Name	Mayukh
Specialization	Cardiologist
Degrees	MBBS(Cardiology)
Email	m@m.m
Phone	01777777778
Date of Birth	2002-02-20

Upcoming Appointments

ID	Date	Time	Patient	Actions
APP3974539	2025-09-10	10:00:00	Ibnul	Attend Reschedule Cancel
APP5917722	2025-10-23	09:00:00	Ibnul	Attend Reschedule Cancel

Doctors can see this page after logging in as a doctor.



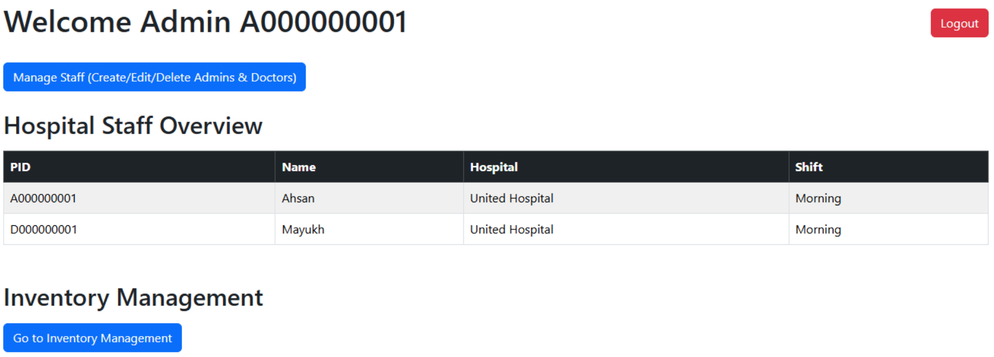
Welcome to Patient Dashboard

Name: Ibnul
Email: i@i.i
Phone: 01777777777
Blood Group: A+
Insurance: Yes

Upcoming Appointments

Appointment ID	Date	Time	Doctor	Hospital	Area
APP3974539	2025-09-10	10:00:00	Mayukh	United Hospital	Gulshan
APP5917722	2025-10-23	09:00:00	Mayukh	United Hospital	Gulshan

Only patients will get to see this page which represents their personal information and appointment schedule.


Logout
Manage Staff (Create/Edit/Delete Admins & Doctors)
Go to Inventory Management

Welcome Admin A000000001

Hospital Staff Overview

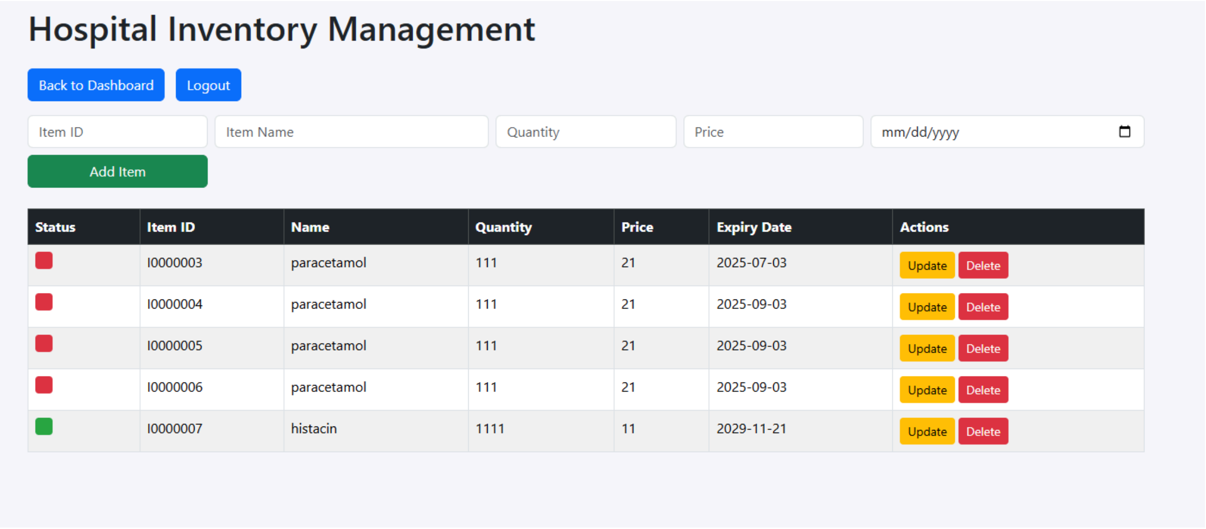
PID	Name	Hospital	Shift
A000000001	Ahsan	United Hospital	Morning
D000000001	Mayukh	United Hospital	Morning

Inventory Management

Admin can see this page only.

Contribution of ID : 21301594, Name : Mydul Islam Lisun

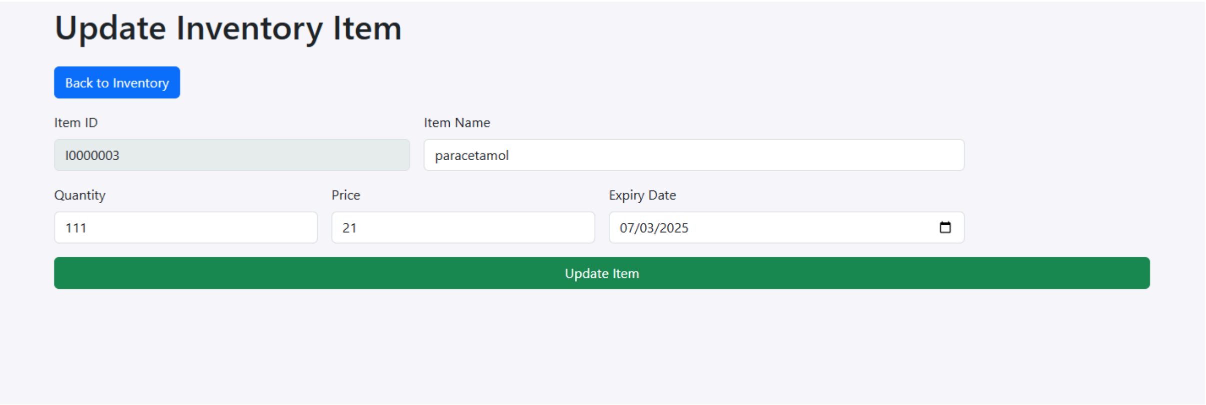
Here the admin has the ability to add a new item see the quantity of the item, delete item if necessary, and also the expiration date. The expiration date is shown directly and also as status. The status bar of a particular item stays green, if the expiry date is within the next seven days, it turns yellow, and if it is expired, then the status turned into red.



Hospital Inventory Management

Status	Item ID	Name	Quantity	Price	Expiry Date	Actions
🟥	I0000003	paracetamol	111	21	2025-07-03	Update Delete
🟥	I0000004	paracetamol	111	21	2025-09-03	Update Delete
🟥	I0000005	paracetamol	111	21	2025-09-03	Update Delete
🟥	I0000006	paracetamol	111	21	2025-09-03	Update Delete
🟩	I0000007	histacin	1111	11	2029-11-21	Update Delete

If the admin wants to update something, he can do it on the update page.



Update Inventory Item

Item ID: I0000003

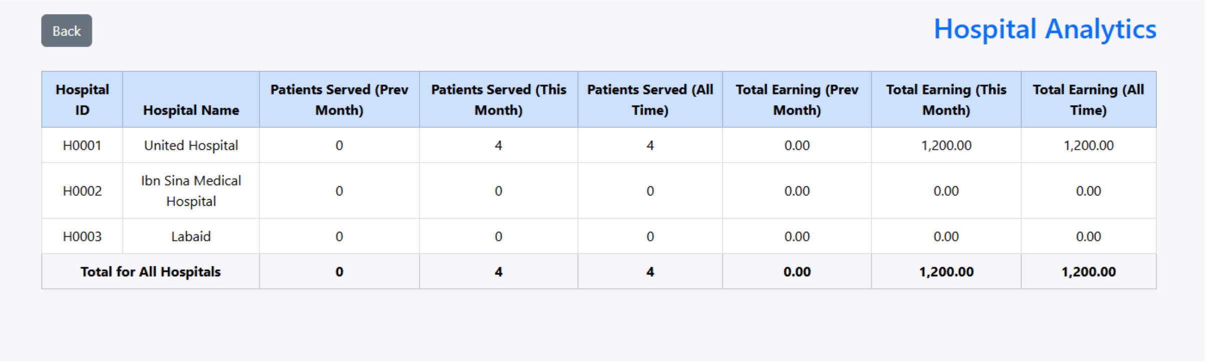
Item Name: paracetamol

Quantity: 111

Price: 21

Expiry Date: 07/03/2025

This is the analytics dashboard for the district health authority. this is an automated report for the health officials. It includes how many patients have the particular hospital have served in a month, how many it did in the previous month and the total number of patients, it has served in lifetime And the total number of patient, it has served in lifetime . it also includes the earning of current month, the previous month and all-time earning. earning of current month the previous month and all-time earning.



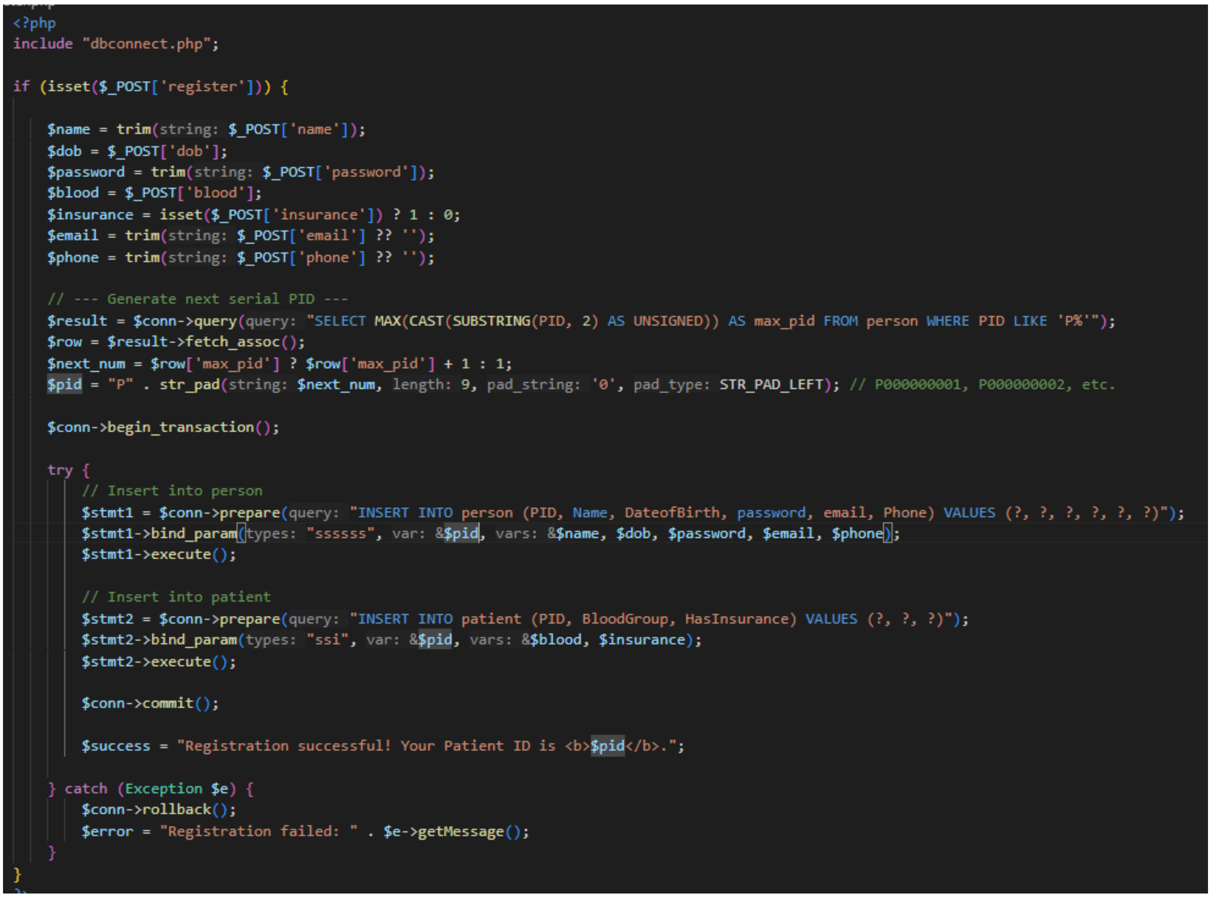
Hospital Analytics

Hospital ID	Hospital Name	Patients Served (Prev Month)	Patients Served (This Month)	Patients Served (All Time)	Total Earning (Prev Month)	Total Earning (This Month)	Total Earning (All Time)
H0001	United Hospital	0	4	4	0.00	1,200.00	1,200.00
H0002	Ibn Sina Medical Hospital	0	0	0	0.00	0.00	0.00
H0003	Labaid	0	0	0	0.00	0.00	0.00
Total for All Hospitals		**0**	**4**	**4**	**0.00**	**1,200.00**	**1,200.00**

Backend Development

Contribution of ID : 19301102, Name : Ibnul Ahsan Mayukh

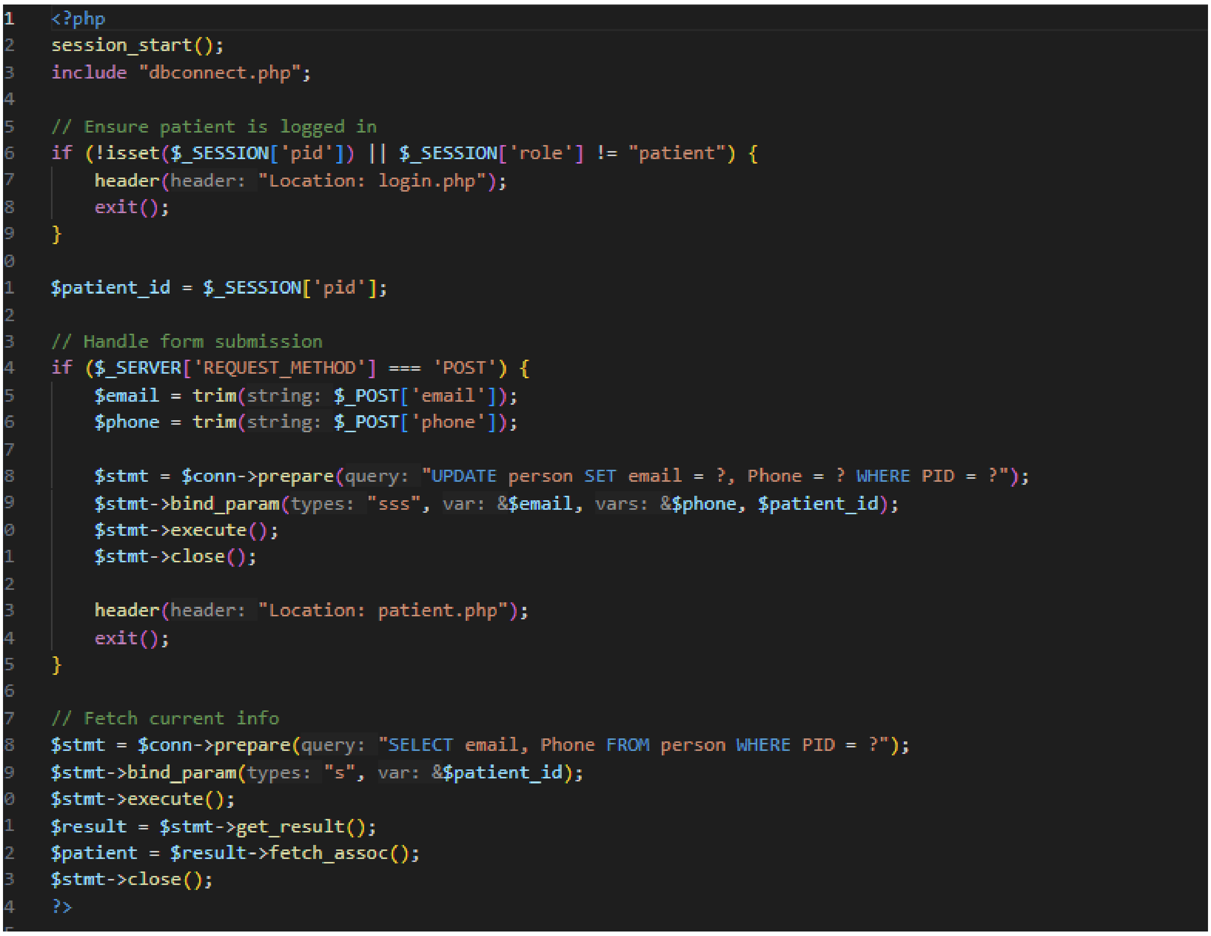
Patient Registration: Patient enters necessary information. Bloodgroup is verified with constraints in db that checks if bloodgroup is valid. PID is autogenerated as PXXXXXXXXX by incrementing it in the php not in mysql server.



```php
<?php
include "dbconnect.php";

if (isset($_POST['register'])) {

    $name = trim(string: $_POST['name']);
    $dob = $_POST['dob'];
    $password = trim(string: $_POST['password']);
    $blood = $_POST['blood'];
    $insurance = isset($_POST['insurance']) ? 1 : 0;
    $email = trim(string: $_POST['email'] ?? '');
    $phone = trim(string: $_POST['phone'] ?? '');

    // --- Generate next serial PID ---
    $result = $conn->query(query: "SELECT MAX(CAST(SUBSTRING(PID, 2) AS UNSIGNED)) AS max_pid FROM person WHERE PID LIKE 'P%'");
    $row = $result->fetch_assoc();
    $next_num = $row['max_pid'] ? $row['max_pid'] + 1 : 1;
    $pid = "P" . str_pad(string: $next_num, length: 9, pad_string: '0', pad_type: STR_PAD_LEFT); // P000000001, P000000002, etc.

    $conn->begin_transaction();

    try {
        // Insert into person
        $stmt1 = $conn->prepare(query: "INSERT INTO person (PID, Name, DateofBirth, password, email, Phone) VALUES (?, ?, ?, ?, ?, ?)");
        $stmt1->bind_param(types: "ssssss", var: &$pid, vars: &$name, $dob, $password, $email, $phone);
        $stmt1->execute();

        // Insert into patient
        $stmt2 = $conn->prepare(query: "INSERT INTO patient (PID, BloodGroup, HasInsurance) VALUES (?, ?, ?)");
        $stmt2->bind_param(types: "ssi", var: &$pid, vars: &$blood, $insurance);
        $stmt2->execute();

        $conn->commit();

        $success = "Registration successful! Your Patient ID is <b>$pid</b>.";

    } catch (Exception $e) {
        $conn->rollback();
        $error = "Registration failed: " . $e->getMessage();
    }
}
```

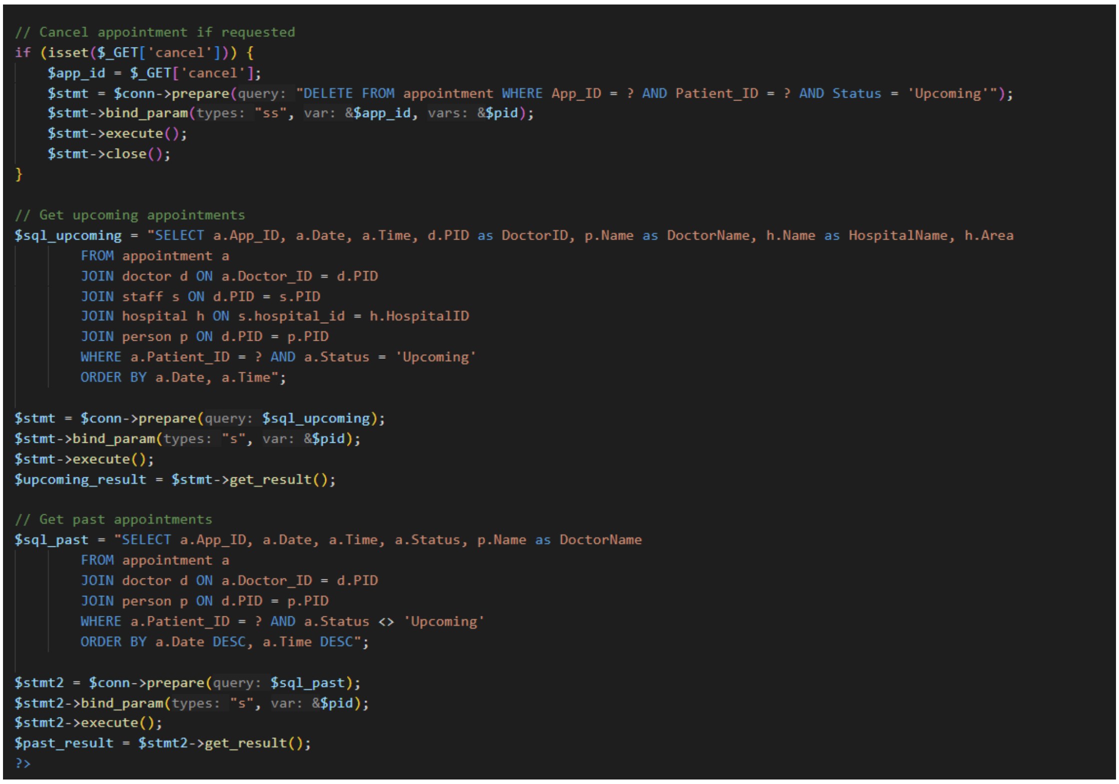
Patient Contact info update:

Patients are only allowed to update contact info.



```php
<?php
session_start();
include "dbconnect.php";

// Ensure patient is logged in
if (!isset($_SESSION['pid']) || $_SESSION['role'] != "patient") {
    header(header: "Location: login.php");
    exit();
}

$patient_id = $_SESSION['pid'];

// Handle form submission
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $email = trim(string: $_POST['email']);
    $phone = trim(string: $_POST['phone']);

    $stmt = $conn->prepare(query: "UPDATE person SET email = ?, Phone = ? WHERE PID = ?");
    $stmt->bind_param(types: "sss", var: &$email, vars: &$phone, $patient_id);
    $stmt->execute();
    $stmt->close();

    header(header: "Location: patient.php");
    exit();
}

// Fetch current info
$stmt = $conn->prepare(query: "SELECT email, Phone FROM person WHERE PID = ?");
$stmt->bind_param(types: "s", var: &$patient_id);
$stmt->execute();
$result = $stmt->get_result();
$patient = $result->fetch_assoc();
$stmt->close();
?>
```

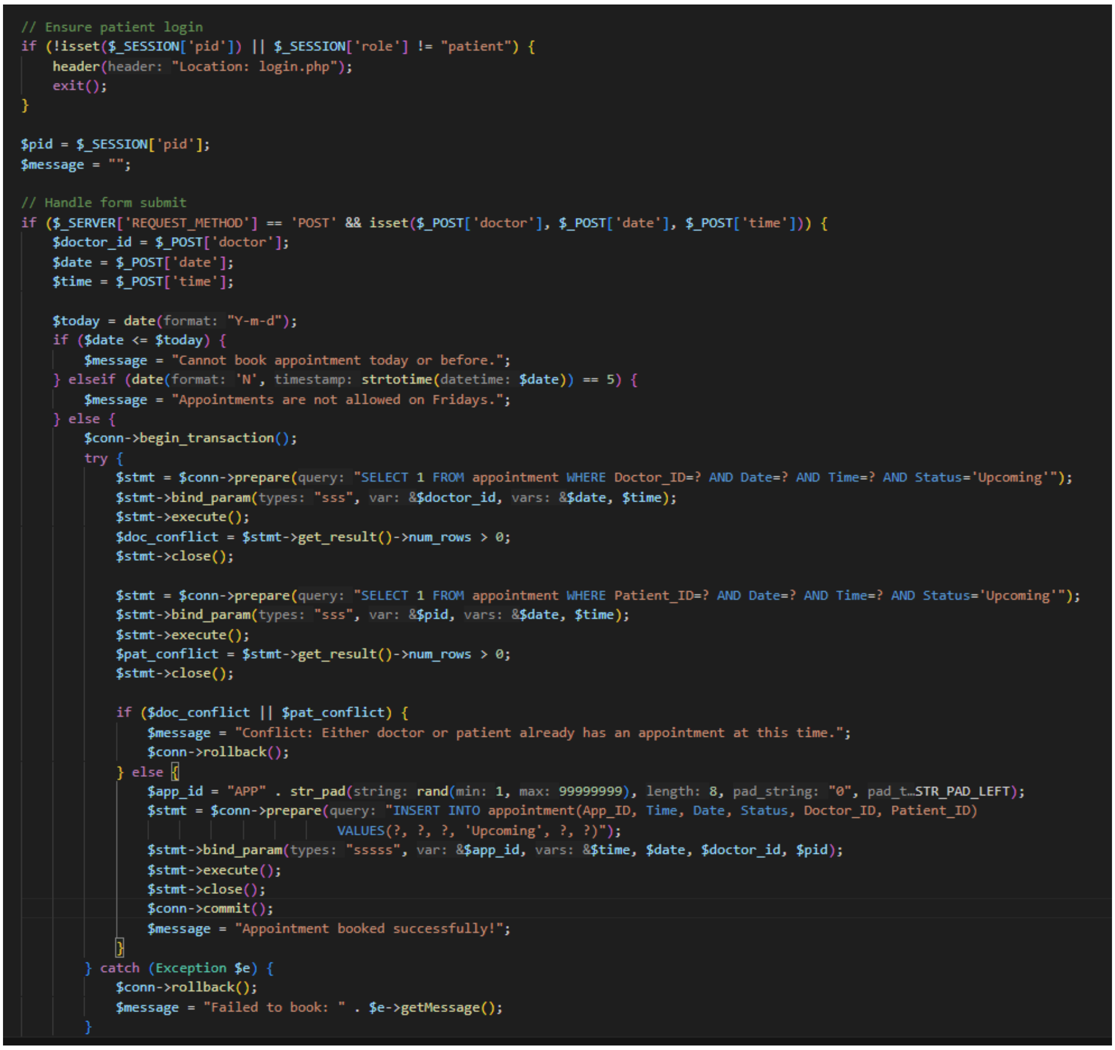
Appointment management: Patients can cancel or update their appointment as well as create new appointments. Can also check the diagnosis screen from here. Cancel is instantaneous but modifying requires going to a different page. Can only modify upcoming appointments.



```
// Cancel appointment if requested
if (isset($_GET['cancel'])) {
    $app_id = $_GET['cancel'];
    $stmt = $conn->prepare(query: "DELETE FROM appointment WHERE App_ID = ? AND Patient_ID = ? AND Status = 'Upcoming'");
    $stmt->bind_param(types: "ss", var: &$app_id, vars: &$pid);
    $stmt->execute();
    $stmt->close();
}

// Get upcoming appointments
$sql_upcoming = "SELECT a.App_ID, a.Date, a.Time, d.PID as DoctorID, p.Name as DoctorName, h.Name as HospitalName, h.Area
        FROM appointment a
        JOIN doctor d ON a.Doctor_ID = d.PID
        JOIN staff s ON d.PID = s.PID
        JOIN hospital h ON s.hospital_id = h.HospitalID
        JOIN person p ON d.PID = p.PID
        WHERE a.Patient_ID = ? AND a.Status = 'Upcoming'
        ORDER BY a.Date, a.Time";

$stmt = $conn->prepare(query: $sql_upcoming);
$stmt->bind_param(types: "s", var: &$pid);
$stmt->execute();
$upcoming_result = $stmt->get_result();

// Get past appointments
$sql_past = "SELECT a.App_ID, a.Date, a.Time, a.Status, p.Name as DoctorName
        FROM appointment a
        JOIN doctor d ON a.Doctor_ID = d.PID
        JOIN person p ON d.PID = p.PID
        WHERE a.Patient_ID = ? AND a.Status <> 'Upcoming'
        ORDER BY a.Date DESC, a.Time DESC";

$stmt2 = $conn->prepare(query: $sql_past);
$stmt2->bind_param(types: "s", var: &$pid);
$stmt2->execute();
$past_result = $stmt2->get_result();
?>
```

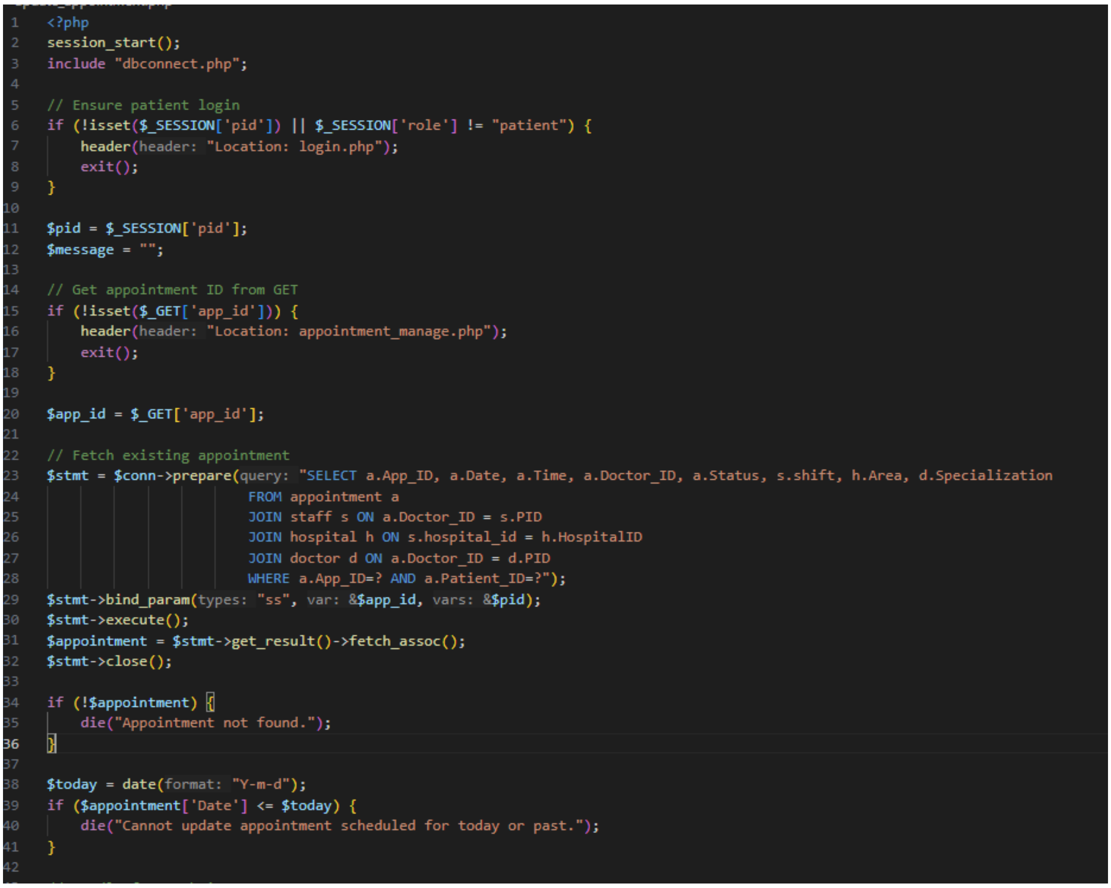
Patient can make new appointments:

Patient can make appointments later than today. Patient choses from granular options.

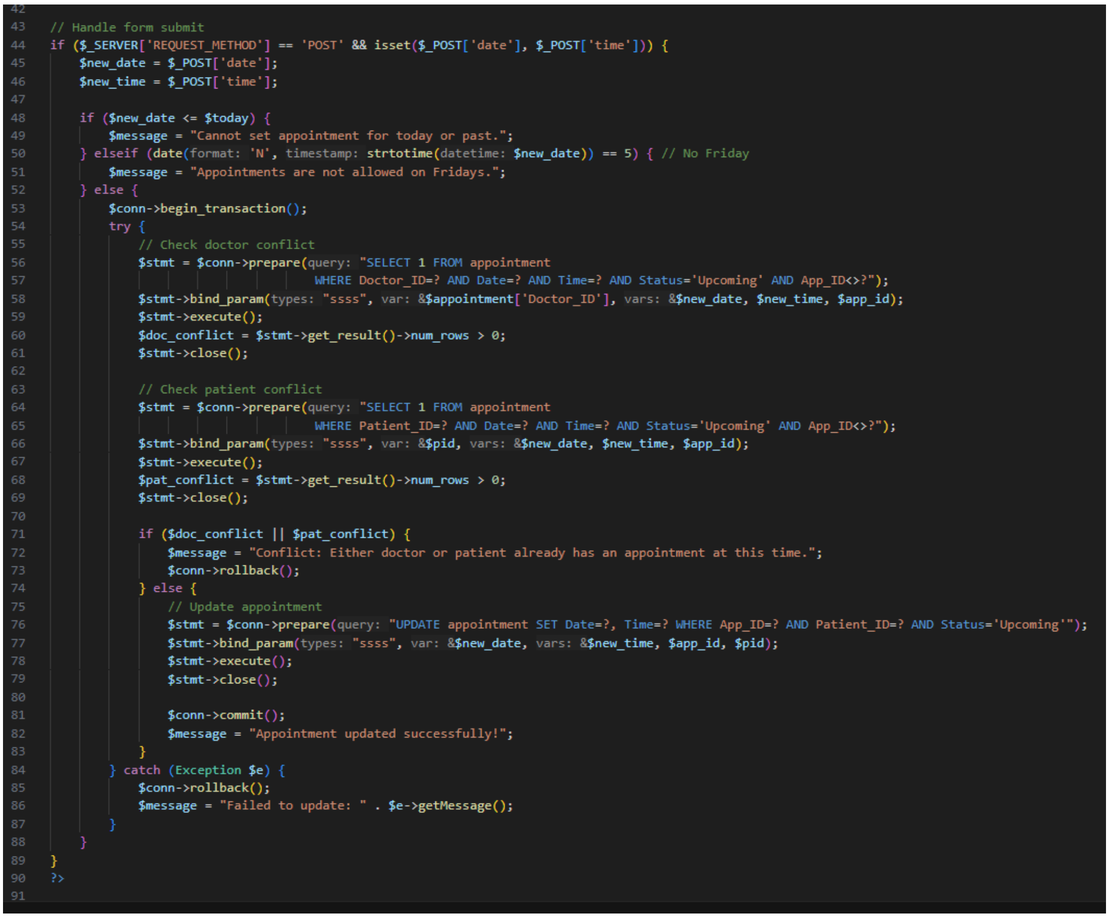


```php
// Ensure patient login
if (!isset($_SESSION['pid']) || $_SESSION['role'] != "patient") {
    header(header: "Location: login.php");
    exit();
}

$pid = $_SESSION['pid'];
$message = "";

// Handle form submit
if ($_SERVER['REQUEST_METHOD'] == 'POST' && isset($_POST['doctor'], $_POST['date'], $_POST['time'])) {
    $doctor_id = $_POST['doctor'];
    $date = $_POST['date'];
    $time = $_POST['time'];

    $today = date(format: "Y-m-d");
    if ($date <= $today) {
        $message = "Cannot book appointment today or before.";
    } elseif (date(format: 'N', timestamp: strtotime(datetime: $date)) == 5) {
        $message = "Appointments are not allowed on Fridays.";
    } else {
        $conn->begin_transaction();
        try {
            $stmt = $conn->prepare(query: "SELECT 1 FROM appointment WHERE Doctor_ID=? AND Date=? AND Time=? AND Status='Upcoming'");
            $stmt->bind_param(types: "sss", var: &$doctor_id, vars: &$date, $time);
            $stmt->execute();
            $doc_conflict = $stmt->get_result()->num_rows > 0;
            $stmt->close();

            $stmt = $conn->prepare(query: "SELECT 1 FROM appointment WHERE Patient_ID=? AND Date=? AND Time=? AND Status='Upcoming'");
            $stmt->bind_param(types: "sss", var: &$pid, vars: &$date, $time);
            $stmt->execute();
            $pat_conflict = $stmt->get_result()->num_rows > 0;
            $stmt->close();

            if ($doc_conflict || $pat_conflict) {
                $message = "Conflict: Either doctor or patient already has an appointment at this time.";
                $conn->rollback();
            } else {
                $app_id = "APP" . str_pad(string: rand(min: 1, max: 99999999), length: 8, pad_string: "0", pad_t…STR_PAD_LEFT);
                $stmt = $conn->prepare(query: "INSERT INTO appointment(App_ID, Time, Date, Status, Doctor_ID, Patient_ID)
                                        VALUES(?, ?, ?, 'Upcoming', ?, ?)");
                $stmt->bind_param(types: "sssss", var: &$app_id, vars: &$time, $date, $doctor_id, $pid);
                $stmt->execute();
                $stmt->close();
                $conn->commit();
                $message = "Appointment booked successfully!";
            }
        } catch (Exception $e) {
            $conn->rollback();
            $message = "Failed to book: " . $e->getMessage();
        }
```

Patient can delay their appointment:

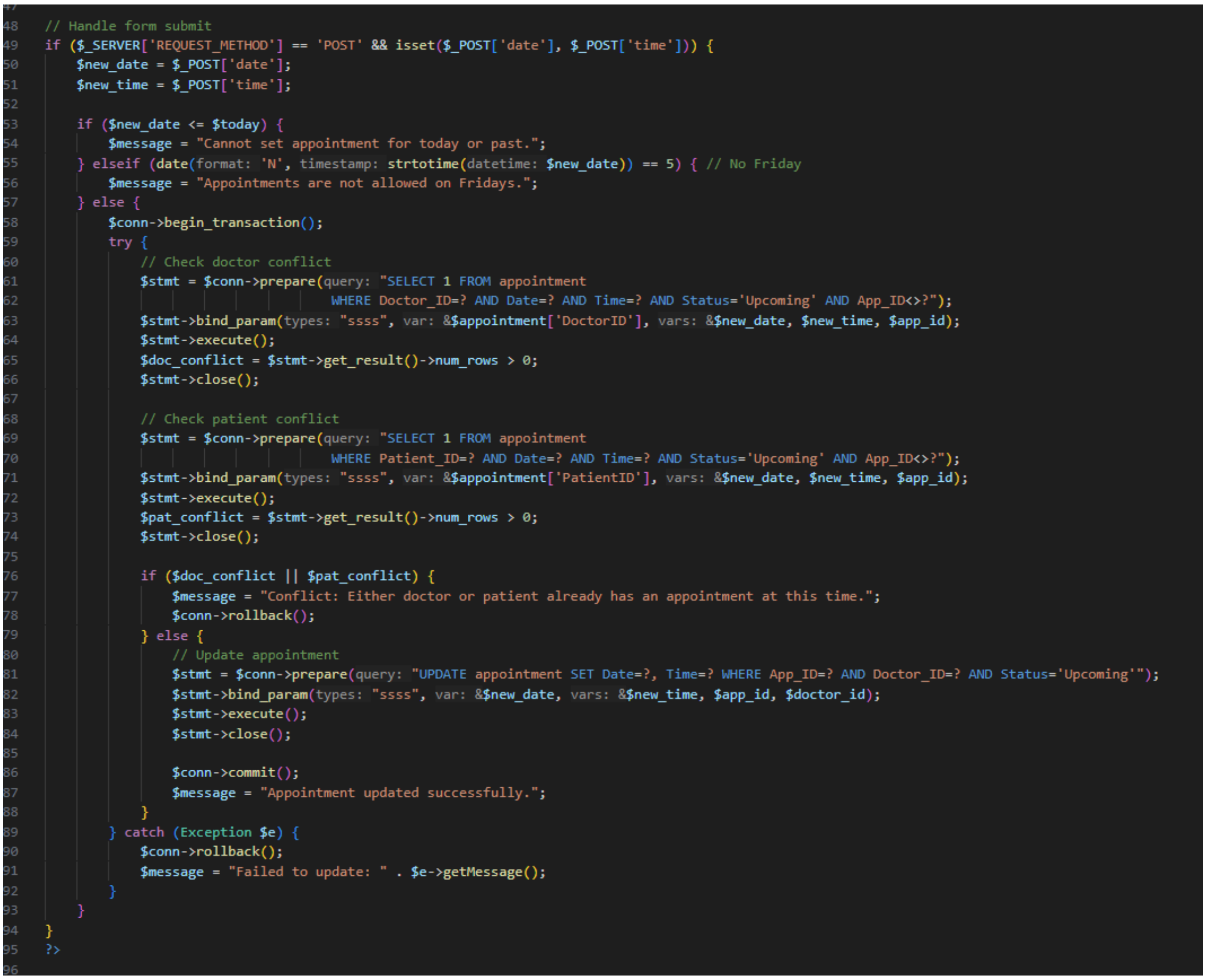


```php
<?php
session_start();
include "dbconnect.php";

// Ensure patient login
if (!isset($_SESSION['pid']) || $_SESSION['role'] != "patient") {
    header(header: "Location: login.php");
    exit();
}

$pid = $_SESSION['pid'];
$message = "";

// Get appointment ID from GET
if (!isset($_GET['app_id'])) {
    header(header: "Location: appointment_manage.php");
    exit();
}

$app_id = $_GET['app_id'];

// Fetch existing appointment
$stmt = $conn->prepare(query: "SELECT a.App_ID, a.Date, a.Time, a.Doctor_ID, a.Status, s.shift, h.Area, d.Specialization
                        FROM appointment a
                        JOIN staff s ON a.Doctor_ID = s.PID
                        JOIN hospital h ON s.hospital_id = h.HospitalID
                        JOIN doctor d ON a.Doctor_ID = d.PID
                        WHERE a.App_ID=? AND a.Patient_ID=?");
$stmt->bind_param(types: "ss", var: &$app_id, vars: &$pid);
$stmt->execute();
$appointment = $stmt->get_result()->fetch_assoc();
$stmt->close();

if (!$appointment) {
    die("Appointment not found.");
}

$today = date(format: "Y-m-d");
if ($appointment['Date'] <= $today) {
    die("Cannot update appointment scheduled for today or past.");
}

```



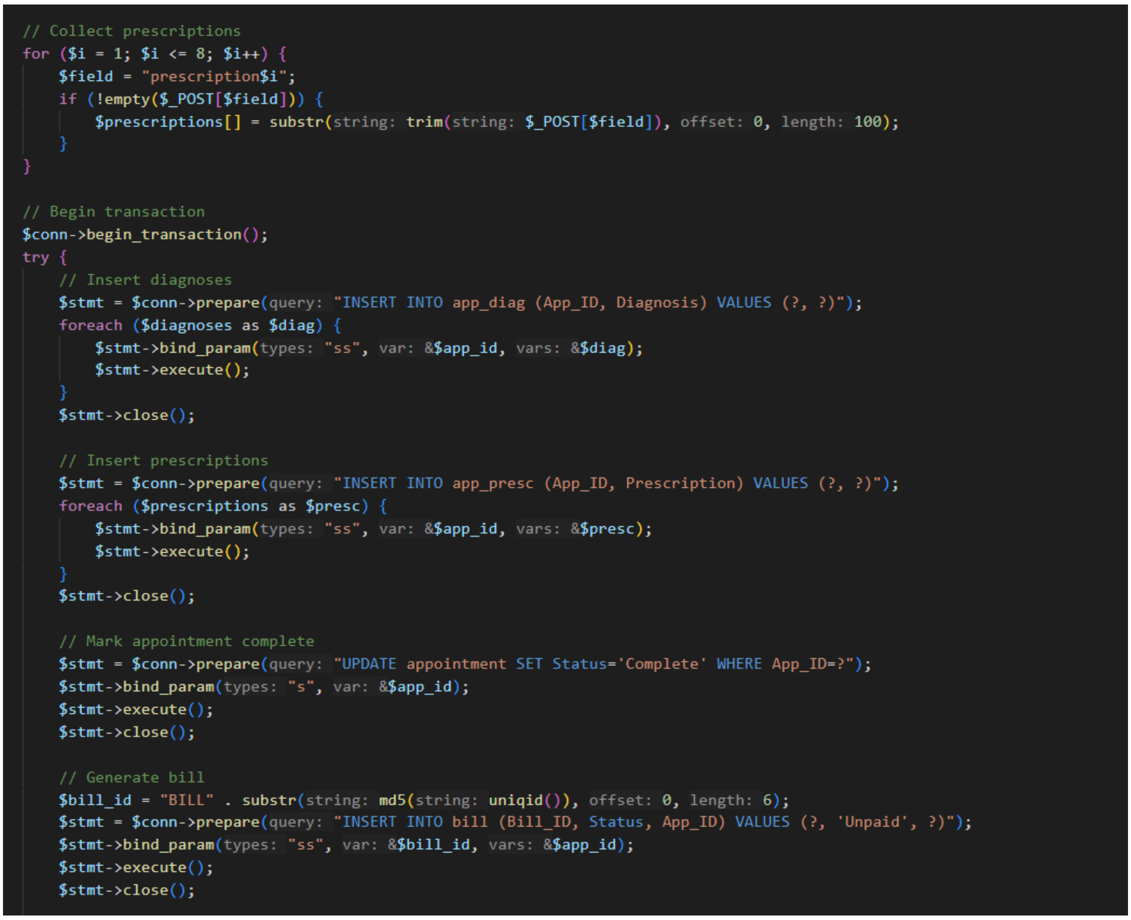
```php

// Handle form submit
if ($_SERVER['REQUEST_METHOD'] == 'POST' && isset($_POST['date'], $_POST['time'])) {
    $new_date = $_POST['date'];
    $new_time = $_POST['time'];

    if ($new_date <= $today) {
        $message = "Cannot set appointment for today or past.";
    } elseif (date(format: 'N', timestamp: strtotime(datetime: $new_date)) == 5) { // No Friday
        $message = "Appointments are not allowed on Fridays.";
    } else {
        $conn->begin_transaction();
        try {
            // Check doctor conflict
            $stmt = $conn->prepare(query: "SELECT 1 FROM appointment
                                    WHERE Doctor_ID=? AND Date=? AND Time=? AND Status='Upcoming' AND App_ID<>?");
            $stmt->bind_param(types: "ssss", var: &$appointment['Doctor_ID'], vars: &$new_date, $new_time, $app_id);
            $stmt->execute();
            $doc_conflict = $stmt->get_result()->num_rows > 0;
            $stmt->close();

            // Check patient conflict
            $stmt = $conn->prepare(query: "SELECT 1 FROM appointment
                                    WHERE Patient_ID=? AND Date=? AND Time=? AND Status='Upcoming' AND App_ID<>?");
            $stmt->bind_param(types: "ssss", var: &$pid, vars: &$new_date, $new_time, $app_id);
            $stmt->execute();
            $pat_conflict = $stmt->get_result()->num_rows > 0;
            $stmt->close();

            if ($doc_conflict || $pat_conflict) {
                $message = "Conflict: Either doctor or patient already has an appointment at this time.";
                $conn->rollback();
            } else {
                // Update appointment
                $stmt = $conn->prepare(query: "UPDATE appointment SET Date=?, Time=? WHERE App_ID=? AND Patient_ID=? AND Status='Upcoming'");
                $stmt->bind_param(types: "ssss", var: &$new_date, vars: &$new_time, $app_id, $pid);
                $stmt->execute();
                $stmt->close();

                $conn->commit();
                $message = "Appointment updated successfully!";
            }
        } catch (Exception $e) {
            $conn->rollback();
            $message = "Failed to update: " . $e->getMessage();
        }
    }
}
?>

```

Doctors can also reschedule upcoming appointments:

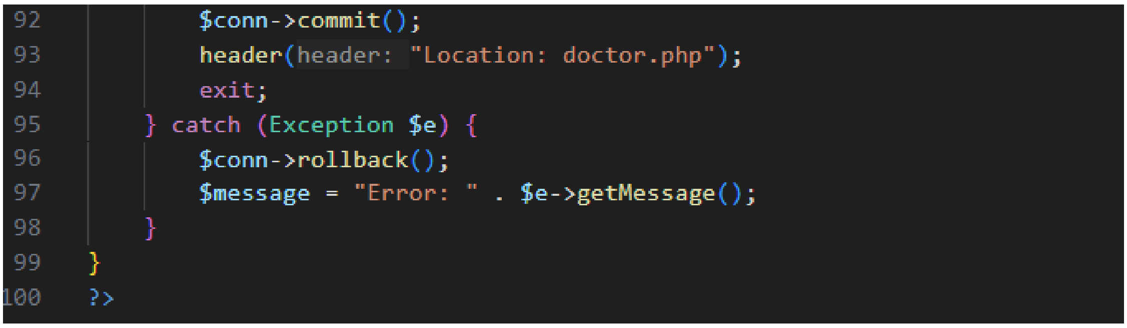


```php
// Handle form submit
if ($_SERVER['REQUEST_METHOD'] == 'POST' && isset($_POST['date'], $_POST['time'])) {
    $new_date = $_POST['date'];
    $new_time = $_POST['time'];

    if ($new_date <= $today) {
        $message = "Cannot set appointment for today or past.";
    } elseif (date(format: 'N', timestamp: strtotime(datetime: $new_date)) == 5) { // No Friday
        $message = "Appointments are not allowed on Fridays.";
    } else {
        $conn->begin_transaction();
        try {
            // Check doctor conflict
            $stmt = $conn->prepare(query: "SELECT 1 FROM appointment
                                    WHERE Doctor_ID=? AND Date=? AND Time=? AND Status='Upcoming' AND App_ID<>?");
            $stmt->bind_param(types: "ssss", var: &$appointment['DoctorID'], vars: &$new_date, $new_time, $app_id);
            $stmt->execute();
            $doc_conflict = $stmt->get_result()->num_rows > 0;
            $stmt->close();

            // Check patient conflict
            $stmt = $conn->prepare(query: "SELECT 1 FROM appointment
                                    WHERE Patient_ID=? AND Date=? AND Time=? AND Status='Upcoming' AND App_ID<>?");
            $stmt->bind_param(types: "ssss", var: &$appointment['PatientID'], vars: &$new_date, $new_time, $app_id);
            $stmt->execute();
            $pat_conflict = $stmt->get_result()->num_rows > 0;
            $stmt->close();

            if ($doc_conflict || $pat_conflict) {
                $message = "Conflict: Either doctor or patient already has an appointment at this time.";
                $conn->rollback();
            } else {
                // Update appointment
                $stmt = $conn->prepare(query: "UPDATE appointment SET Date=?, Time=? WHERE App_ID=? AND Doctor_ID=? AND Status='Upcoming'");
                $stmt->bind_param(types: "ssss", var: &$new_date, vars: &$new_time, $app_id, $doctor_id);
                $stmt->execute();
                $stmt->close();

                $conn->commit();
                $message = "Appointment updated successfully.";
            }
        } catch (Exception $e) {
            $conn->rollback();
            $message = "Failed to update: " . $e->getMessage();
        }
    }
}
?>
```

Doctor attends appointment: Doctors can enter the diagnostics and prescriptions for each patient in a from

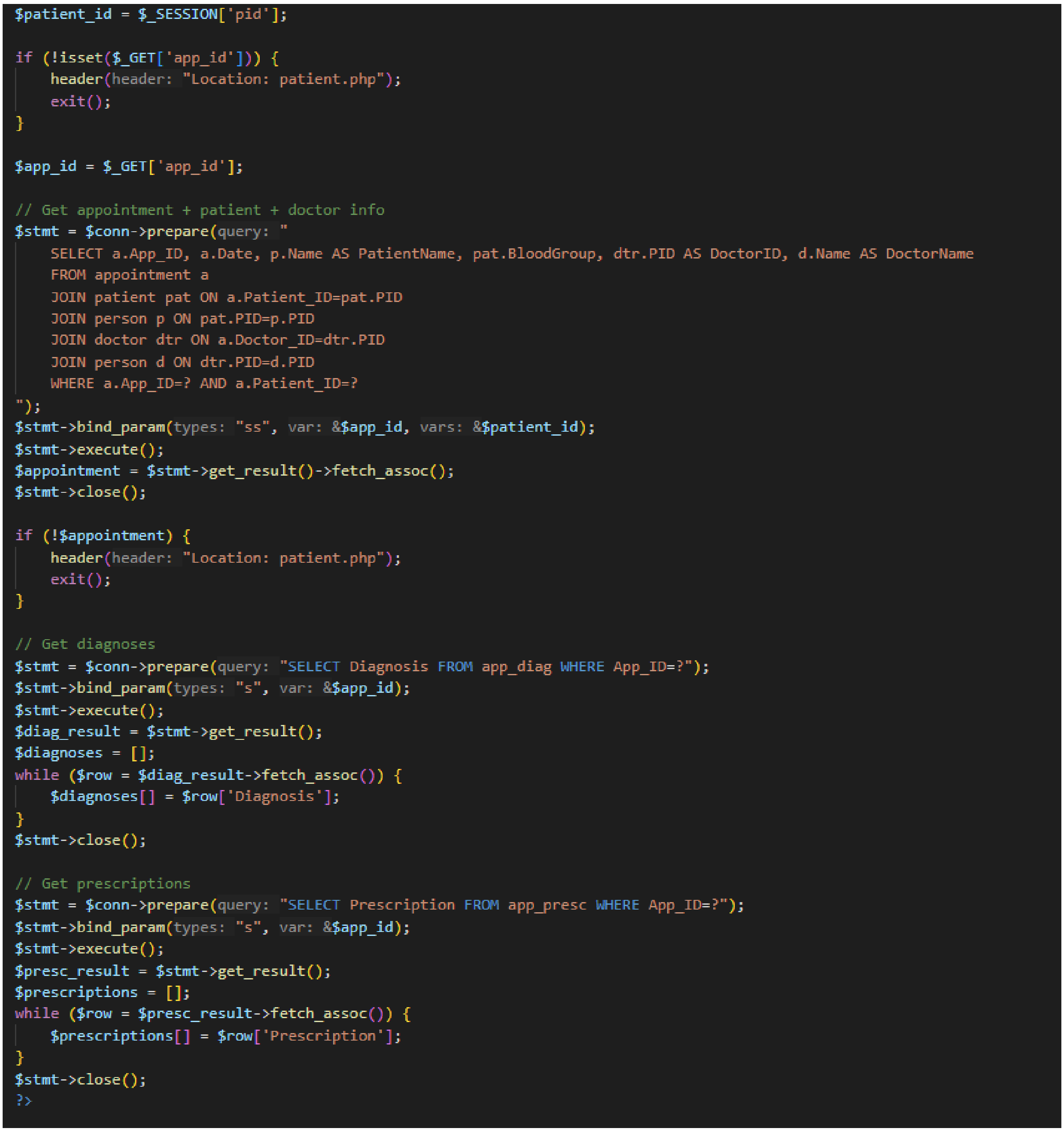


```php
// Collect prescriptions
for ($i = 1; $i <= 8; $i++) {
    $field = "prescription$i";
    if (!empty($_POST[$field])) {
        $prescriptions[] = substr(string: trim(string: $_POST[$field]), offset: 0, length: 100);
    }
}

// Begin transaction
$conn->begin_transaction();
try {
    // Insert diagnoses
    $stmt = $conn->prepare(query: "INSERT INTO app_diag (App_ID, Diagnosis) VALUES (?, ?)");
    foreach ($diagnoses as $diag) {
        $stmt->bind_param(types: "ss", var: &$app_id, vars: &$diag);
        $stmt->execute();
    }
    $stmt->close();

    // Insert prescriptions
    $stmt = $conn->prepare(query: "INSERT INTO app_presc (App_ID, Prescription) VALUES (?, ?)");
    foreach ($prescriptions as $presc) {
        $stmt->bind_param(types: "ss", var: &$app_id, vars: &$presc);
        $stmt->execute();
    }
    $stmt->close();

    // Mark appointment complete
    $stmt = $conn->prepare(query: "UPDATE appointment SET Status='Complete' WHERE App_ID=?");
    $stmt->bind_param(types: "s", var: &$app_id);
    $stmt->execute();
    $stmt->close();

    // Generate bill
    $bill_id = "BILL" . substr(string: md5(string: uniqid()), offset: 0, length: 6);
    $stmt = $conn->prepare(query: "INSERT INTO bill (Bill_ID, Status, App_ID) VALUES (?, 'Unpaid', ?)");
    $stmt->bind_param(types: "ss", var: &$bill_id, vars: &$app_id);
    $stmt->execute();
    $stmt->close();
```



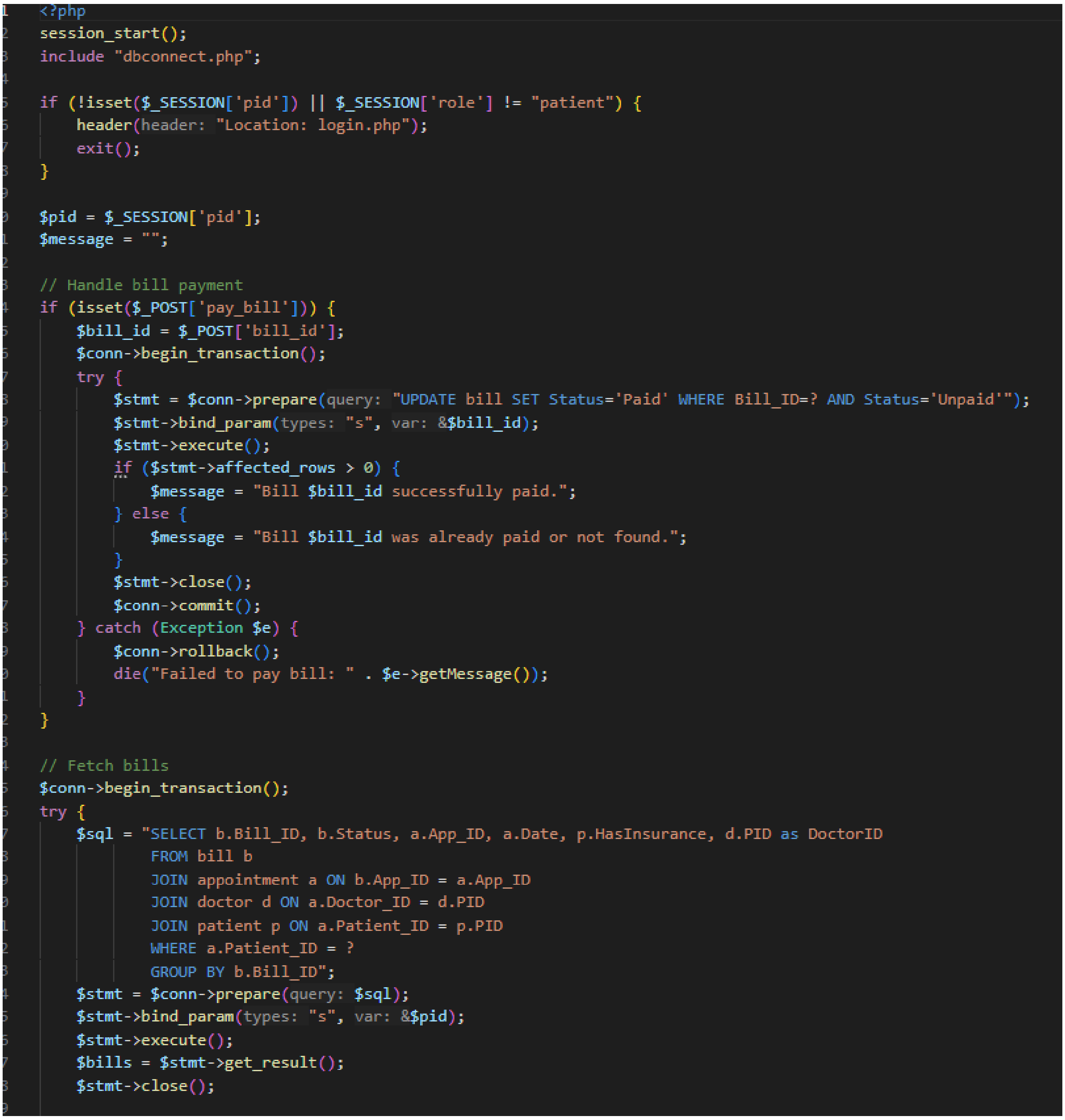
```php
        $conn->commit();
        header(header: "Location: doctor.php");
        exit;
    } catch (Exception $e) {
        $conn->rollback();
        $message = "Error: " . $e->getMessage();
    }
}
?>
```

Patient can check their diagnosis and treatment:

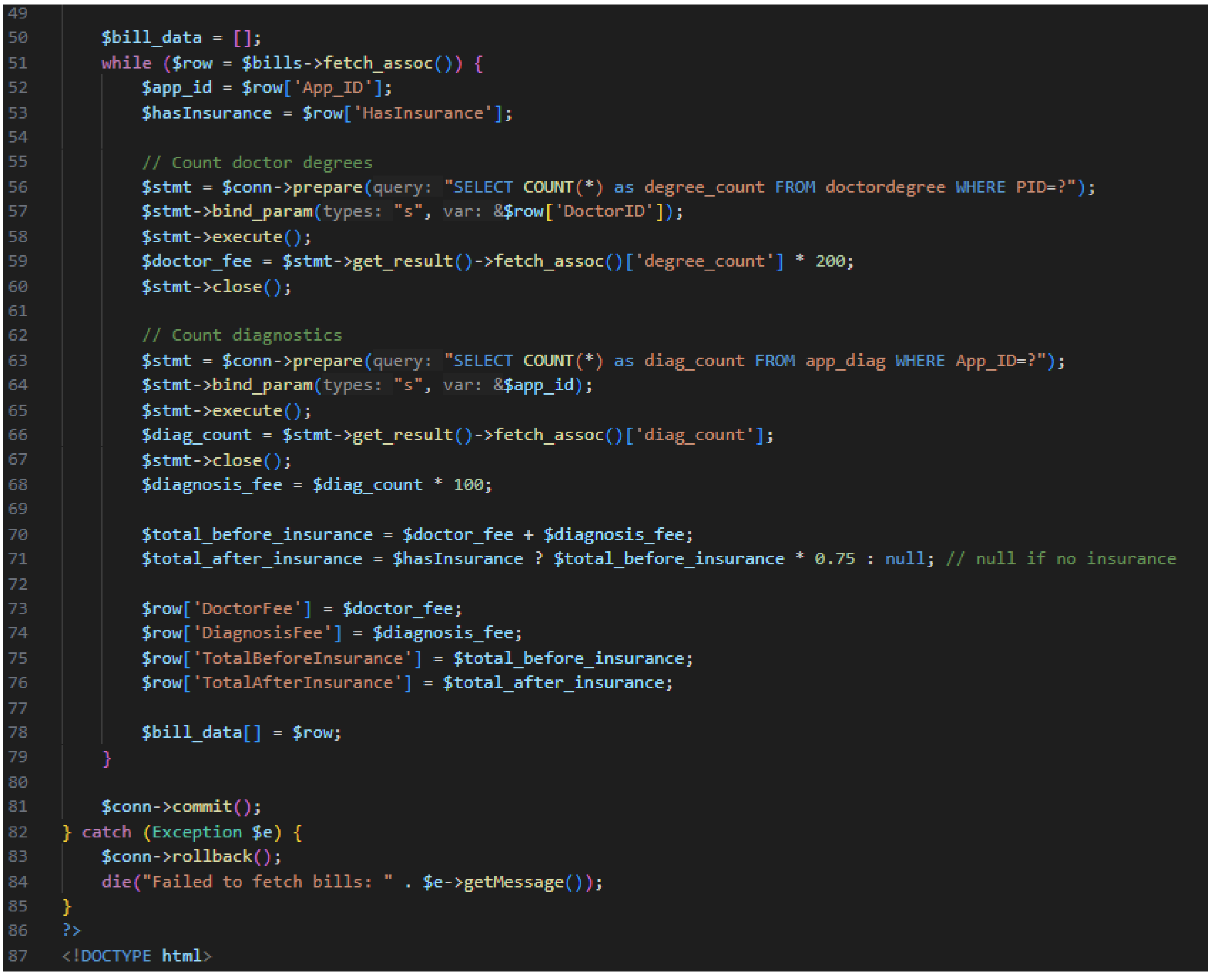


```php
$patient_id = $_SESSION['pid'];

if (!isset($_GET['app_id'])) {
    header(header: "Location: patient.php");
    exit();
}

$app_id = $_GET['app_id'];

// Get appointment + patient + doctor info
$stmt = $conn->prepare(query: "
    SELECT a.App_ID, a.Date, p.Name AS PatientName, pat.BloodGroup, dtr.PID AS DoctorID, d.Name AS DoctorName
    FROM appointment a
    JOIN patient pat ON a.Patient_ID=pat.PID
    JOIN person p ON pat.PID=p.PID
    JOIN doctor dtr ON a.Doctor_ID=dtr.PID
    JOIN person d ON dtr.PID=d.PID
    WHERE a.App_ID=? AND a.Patient_ID=?
");
$stmt->bind_param(types: "ss", var: &$app_id, vars: &$patient_id);
$stmt->execute();
$appointment = $stmt->get_result()->fetch_assoc();
$stmt->close();

if (!$appointment) {
    header(header: "Location: patient.php");
    exit();
}

// Get diagnoses
$stmt = $conn->prepare(query: "SELECT Diagnosis FROM app_diag WHERE App_ID=?");
$stmt->bind_param(types: "s", var: &$app_id);
$stmt->execute();
$diag_result = $stmt->get_result();
$diagnoses = [];
while ($row = $diag_result->fetch_assoc()) {
    $diagnoses[] = $row['Diagnosis'];
}
$stmt->close();

// Get prescriptions
$stmt = $conn->prepare(query: "SELECT Prescription FROM app_presc WHERE App_ID=?");
$stmt->bind_param(types: "s", var: &$app_id);
$stmt->execute();
$presc_result = $stmt->get_result();
$prescriptions = [];
while ($row = $presc_result->fetch_assoc()) {
    $prescriptions[] = $row['Prescription'];
}
$stmt->close();
?>
```

Patient can view and pay their bills: Bill depends on doctor's number of degree, however there are issues that prevented accurate calculation.



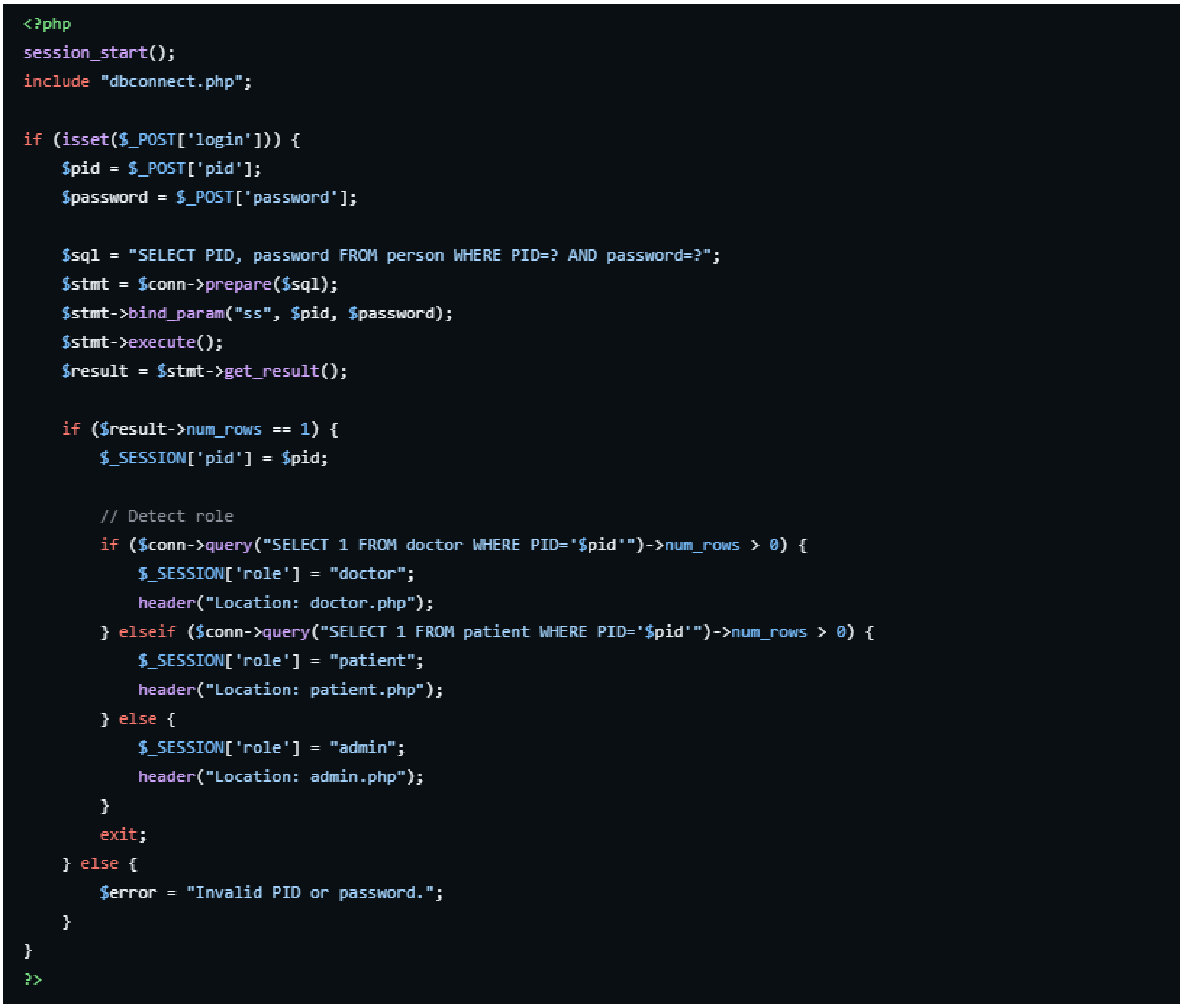
```php
<?php
session_start();
include "dbconnect.php";

if (!isset($_SESSION['pid']) || $_SESSION['role'] != "patient") {
    header(header: "Location: login.php");
    exit();
}

$pid = $_SESSION['pid'];
$message = "";

// Handle bill payment
if (isset($_POST['pay_bill'])) {
    $bill_id = $_POST['bill_id'];
    $conn->begin_transaction();
    try {
        $stmt = $conn->prepare(query: "UPDATE bill SET Status='Paid' WHERE Bill_ID=? AND Status='Unpaid'");
        $stmt->bind_param(types: "s", var: &$bill_id);
        $stmt->execute();
        if ($stmt->affected_rows > 0) {
            $message = "Bill $bill_id successfully paid.";
        } else {
            $message = "Bill $bill_id was already paid or not found.";
        }
        $stmt->close();
        $conn->commit();
    } catch (Exception $e) {
        $conn->rollback();
        die("Failed to pay bill: " . $e->getMessage());
    }
}

// Fetch bills
$conn->begin_transaction();
try {
    $sql = "SELECT b.Bill_ID, b.Status, a.App_ID, a.Date, p.HasInsurance, d.PID as DoctorID
            FROM bill b
            JOIN appointment a ON b.App_ID = a.App_ID
            JOIN doctor d ON a.Doctor_ID = d.PID
            JOIN patient p ON a.Patient_ID = p.PID
            WHERE a.Patient_ID = ?
            GROUP BY b.Bill_ID";
    $stmt = $conn->prepare(query: $sql);
    $stmt->bind_param(types: "s", var: &$pid);
    $stmt->execute();
    $bills = $stmt->get_result();
    $stmt->close();
```



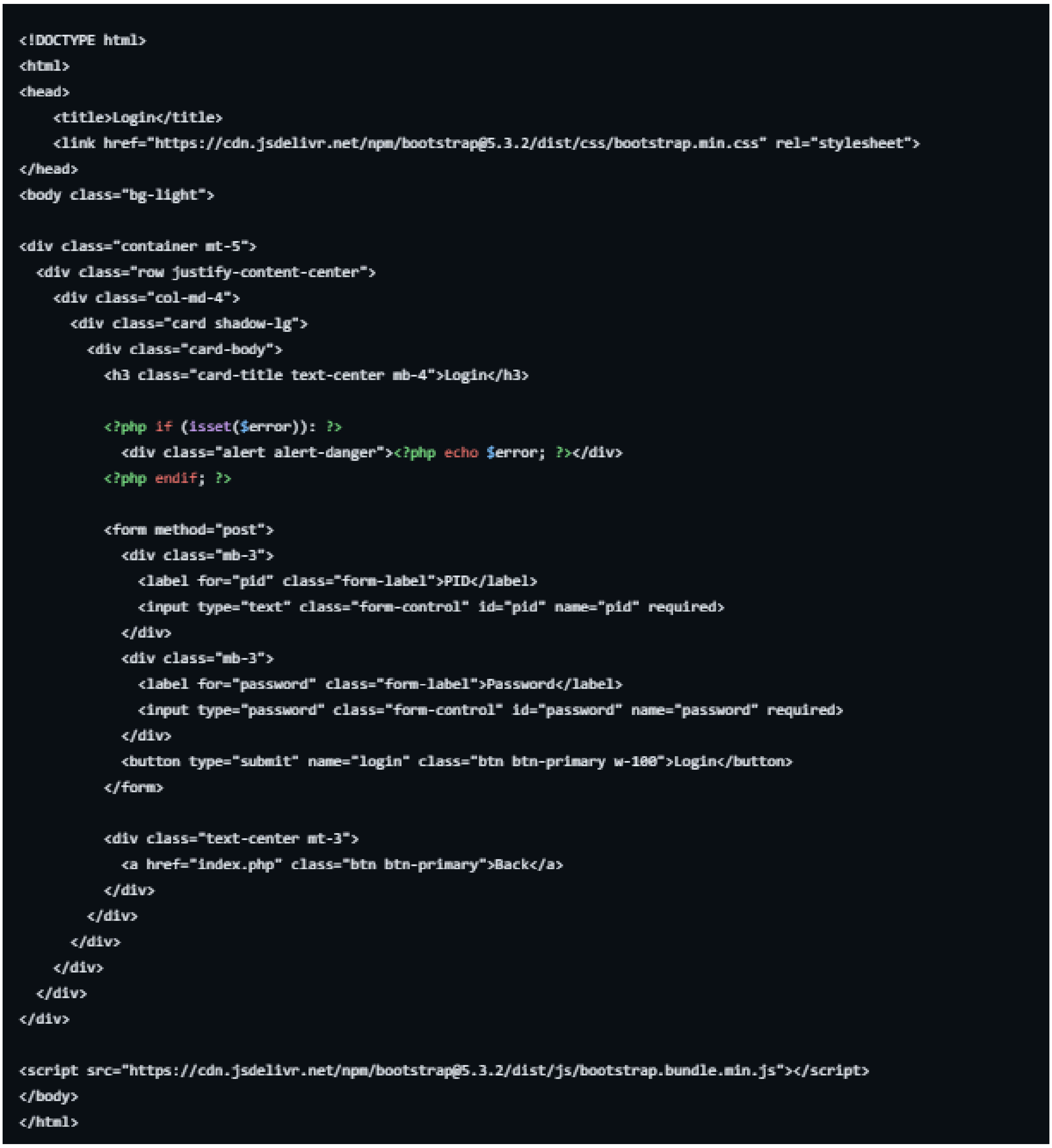
```
    $bill_data = [];
    while ($row = $bills->fetch_assoc()) {
        $app_id = $row['App_ID'];
        $hasInsurance = $row['HasInsurance'];

        // Count doctor degrees
        $stmt = $conn->prepare(query: "SELECT COUNT(*) as degree_count FROM doctordegree WHERE PID=?");
        $stmt->bind_param(types: "s", var: &$row['DoctorID']);
        $stmt->execute();
        $doctor_fee = $stmt->get_result()->fetch_assoc()['degree_count'] * 200;
        $stmt->close();

        // Count diagnostics
        $stmt = $conn->prepare(query: "SELECT COUNT(*) as diag_count FROM app_diag WHERE App_ID=?");
        $stmt->bind_param(types: "s", var: &$app_id);
        $stmt->execute();
        $diag_count = $stmt->get_result()->fetch_assoc()['diag_count'];
        $stmt->close();
        $diagnosis_fee = $diag_count * 100;

        $total_before_insurance = $doctor_fee + $diagnosis_fee;
        $total_after_insurance = $hasInsurance ? $total_before_insurance * 0.75 : null; // null if no insurance

        $row['DoctorFee'] = $doctor_fee;
        $row['DiagnosisFee'] = $diagnosis_fee;
        $row['TotalBeforeInsurance'] = $total_before_insurance;
        $row['TotalAfterInsurance'] = $total_after_insurance;

        $bill_data[] = $row;
    }

    $conn->commit();
} catch (Exception $e) {
    $conn->rollback();
    die("Failed to fetch bills: " . $e->getMessage());
}
?>
<!DOCTYPE html>
```

Contribution of ID : 20201089, Name : Rezowana Mehjabin Lorel

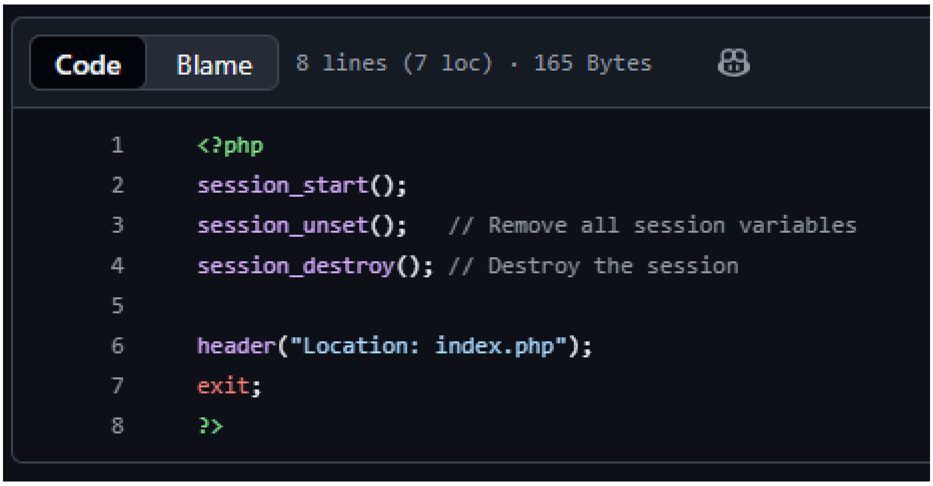
Login and logout :



```
<?php
session_start();
include "dbconnect.php";

if (isset($_POST['login'])) {
    $pid = $_POST['pid'];
    $password = $_POST['password'];

    $sql = "SELECT PID, password FROM person WHERE PID=? AND password=?";
    $stmt = $conn->prepare($sql);
    $stmt->bind_param("ss", $pid, $password);
    $stmt->execute();
    $result = $stmt->get_result();

    if ($result->num_rows == 1) {
        $_SESSION['pid'] = $pid;

        // Detect role
        if ($conn->query("SELECT 1 FROM doctor WHERE PID='$pid'")->num_rows > 0) {
            $_SESSION['role'] = "doctor";
            header("Location: doctor.php");
        } elseif ($conn->query("SELECT 1 FROM patient WHERE PID='$pid'")->num_rows > 0) {
            $_SESSION['role'] = "patient";
            header("Location: patient.php");
        } else {
            $_SESSION['role'] = "admin";
            header("Location: admin.php");
        }
        exit;
    } else {
        $error = "Invalid PID or password.";
    }
}
?>
```



```
<!DOCTYPE html>
<html>
<head>
    <title>Login</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" rel="stylesheet">
</head>
<body class="bg-light">

<div class="container mt-5">
  <div class="row justify-content-center">
    <div class="col-md-4">
      <div class="card shadow-lg">
        <div class="card-body">
          <h3 class="card-title text-center mb-4">Login</h3>

          <?php if (isset($error)): ?>
            <div class="alert alert-danger"><?php echo $error; ?></div>
          <?php endif; ?>

          <form method="post">
            <div class="mb-3">
              <label for="pid" class="form-label">PID</label>
              <input type="text" class="form-control" id="pid" name="pid" required>
            </div>
            <div class="mb-3">
              <label for="password" class="form-label">Password</label>
              <input type="password" class="form-control" id="password" name="password" required>
            </div>
            <button type="submit" name="login" class="btn btn-primary w-100">Login</button>
          </form>

          <div class="text-center mt-3">
            <a href="index.php" class="btn btn-primary">Back</a>
          </div>
        </div>
      </div>
    </div>
  </div>
</div>

<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/js/bootstrap.bundle.min.js"></script>
</body>
</html>
```



```
<?php
session_start();
session_unset();   // Remove all session variables
session_destroy(); // Destroy the session

header("Location: index.php");
exit;
?>
```

The main authentication query here is $sql = "SELECT PID, password FROM person WHERE PID=? AND password=?"; it verifies the provided PID and password combination’s existence in the database.

```
$sql = "SELECT PID, password FROM person WHERE PID=? AND password=?";
$stmt = $conn->prepare($sql);
$stmt->bind_param("ss", $pid, $password);
$stmt->execute();
$result = $stmt->get_result();
```

This user authentication part verifies the user credentials PID and password.

```
$conn->query("SELECT 1 FROM doctor WHERE PID='$pid'")->num_rows > 0
$conn->query("SELECT 1 FROM patient WHERE PID='$pid'")->num_rows > 0
```

This role detection query checks the user's role by checking which role-specific table contains their PID.

```
$_SESSION['pid'] = $pid;
$_SESSION['role'] = "doctor"; // or "patient" or "admin"
```

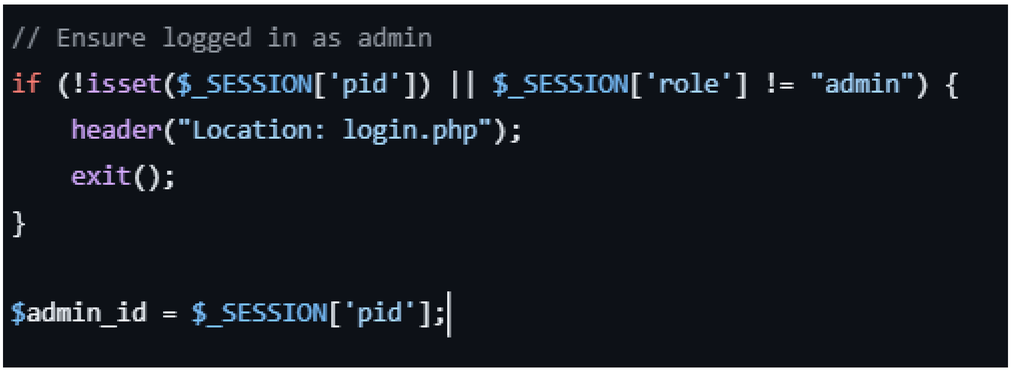
This handles the session management part. This stores user identity and role in session variables for later use

For authentication purposes, this code retrieves information from the database. Consequently, it makes no changes to the data.

In the logout feature header("Location: index.php") redirects the user to the homepage after logout. This part of the code does not execute any database queries.

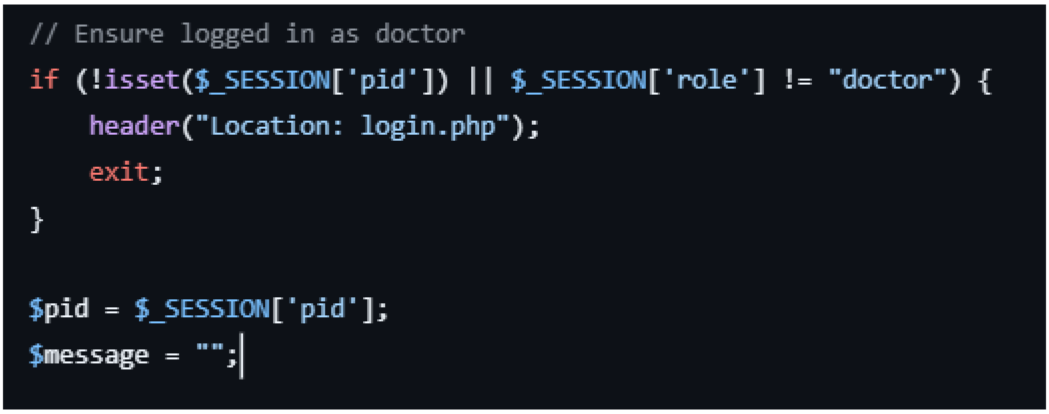
Role based access control :

Admin



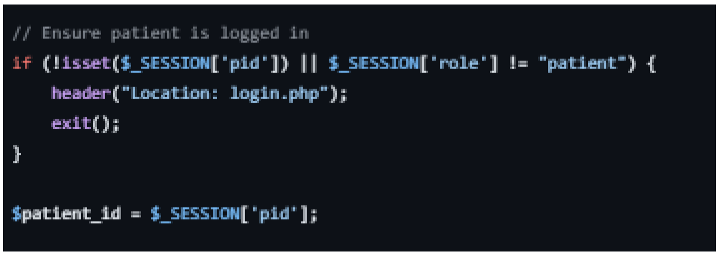
```
// Ensure logged in as admin
if (!isset($_SESSION['pid']) || $_SESSION['role'] != "admin") {
    header("Location: login.php");
    exit();
}

$admin_id = $_SESSION['pid'];
```

Doctor



```
// Ensure logged in as doctor
if (!isset($_SESSION['pid']) || $_SESSION['role'] != "doctor") {
    header("Location: login.php");
    exit;
}

$pid = $_SESSION['pid'];
$message = "";
```

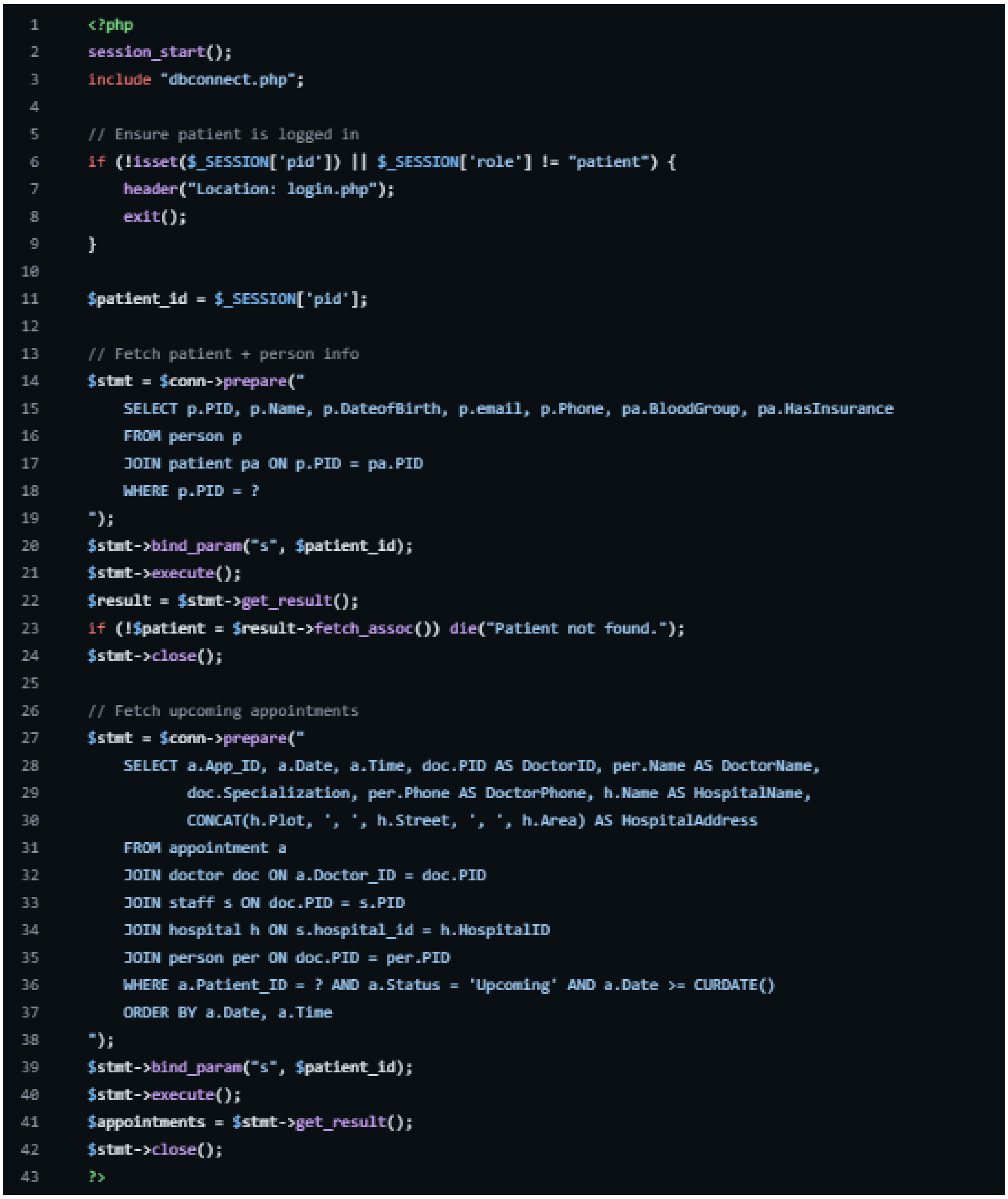
Patient



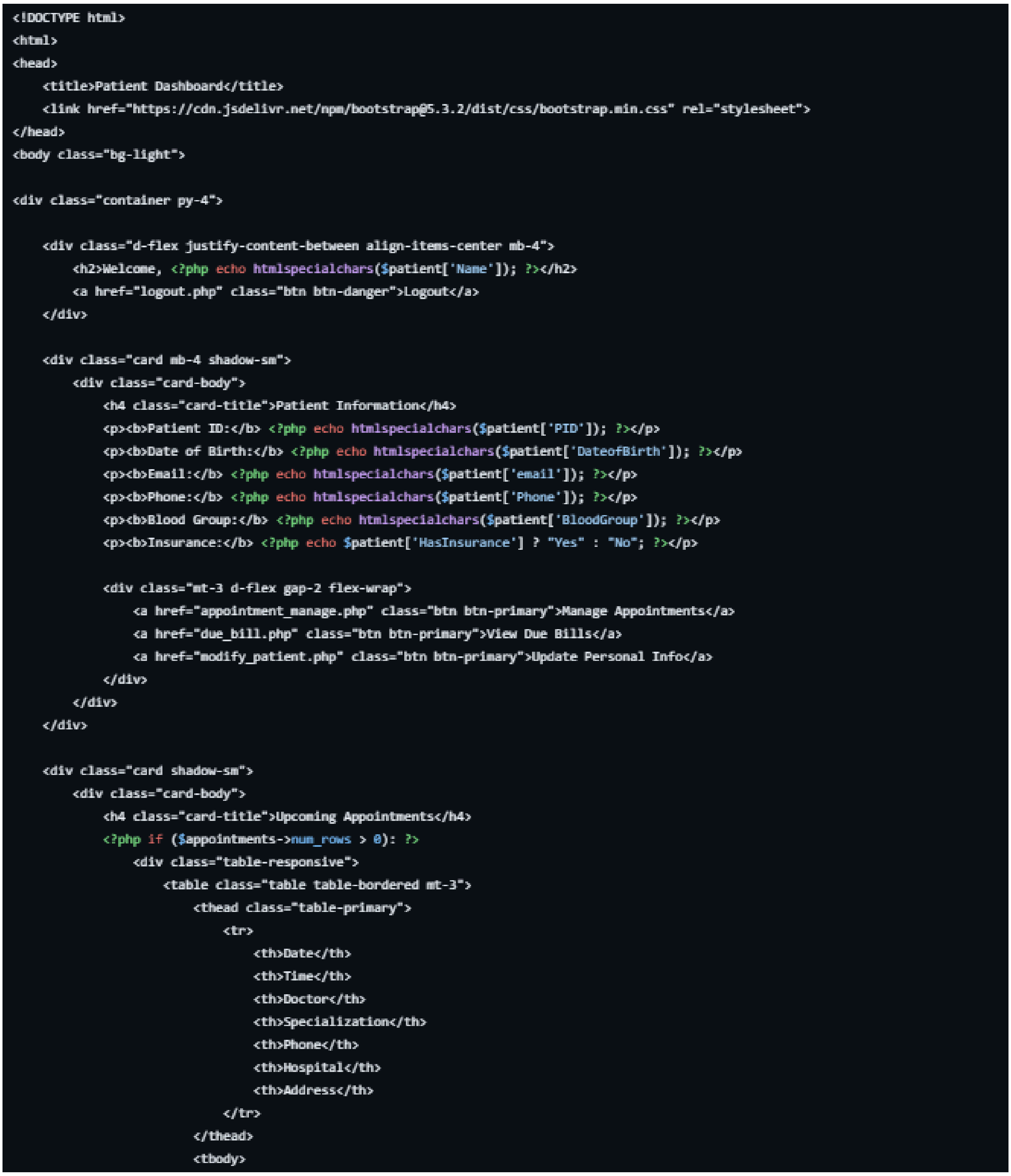
```
// Ensure patient is logged in
if (!isset($_SESSION['pid']) || $_SESSION['role'] != "patient") {
    header("Location: login.php");
    exit();
}

$patient_id = $_SESSION['pid'];
```

Here, by verifying session variables checking is done for logged in scenerio. $_SESSION['pid'] checks about the user's active session. This helps to verify the exact role of the person . If the person (Admin/doctor/patient) is not authenticated, the code redirects to login.php. It stores patient id from the session into a variable.

Patient Dashboard :



```php
<?php
session_start();
include "dbconnect.php";

// Ensure patient is logged in
if (!isset($_SESSION['pid']) || $_SESSION['role'] != "patient") {
    header("Location: login.php");
    exit();
}

$patient_id = $_SESSION['pid'];

// Fetch patient + person info
$stmt = $conn->prepare("
    SELECT p.PID, p.Name, p.DateofBirth, p.email, p.Phone, pa.BloodGroup, pa.HasInsurance
    FROM person p
    JOIN patient pa ON p.PID = pa.PID
    WHERE p.PID = ?
");
$stmt->bind_param("s", $patient_id);
$stmt->execute();
$result = $stmt->get_result();
if (!$patient = $result->fetch_assoc()) die("Patient not found.");
$stmt->close();

// Fetch upcoming appointments
$stmt = $conn->prepare("
    SELECT a.App_ID, a.Date, a.Time, doc.PID AS DoctorID, per.Name AS DoctorName,
           doc.Specialization, per.Phone AS DoctorPhone, h.Name AS HospitalName,
           CONCAT(h.Plot, ', ', h.Street, ', ', h.Area) AS HospitalAddress
    FROM appointment a
    JOIN doctor doc ON a.Doctor_ID = doc.PID
    JOIN staff s ON doc.PID = s.PID
    JOIN hospital h ON s.hospital_id = h.HospitalID
    JOIN person per ON doc.PID = per.PID
    WHERE a.Patient_ID = ? AND a.Status = 'Upcoming' AND a.Date >= CURDATE()
    ORDER BY a.Date, a.Time
");
$stmt->bind_param("s", $patient_id);
$stmt->execute();
$appointments = $stmt->get_result();
$stmt->close();
?>
```



```
<!DOCTYPE html>
<html>
<head>
    <title>Patient Dashboard</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" rel="stylesheet">
</head>
<body class="bg-light">

<div class="container py-4">

    <div class="d-flex justify-content-between align-items-center mb-4">
        <h2>Welcome, <?php echo htmlspecialchars($patient['Name']); ?></h2>
        <a href="logout.php" class="btn btn-danger">Logout</a>
    </div>

    <div class="card mb-4 shadow-sm">
        <div class="card-body">
            <h4 class="card-title">Patient Information</h4>
            <p><b>Patient ID:</b> <?php echo htmlspecialchars($patient['PID']); ?></p>
            <p><b>Date of Birth:</b> <?php echo htmlspecialchars($patient['DateofBirth']); ?></p>
            <p><b>Email:</b> <?php echo htmlspecialchars($patient['email']); ?></p>
            <p><b>Phone:</b> <?php echo htmlspecialchars($patient['Phone']); ?></p>
            <p><b>Blood Group:</b> <?php echo htmlspecialchars($patient['BloodGroup']); ?></p>
            <p><b>Insurance:</b> <?php echo $patient['HasInsurance'] ? "Yes" : "No"; ?></p>

            <div class="mt-3 d-flex gap-2 flex-wrap">
                <a href="appointment_manage.php" class="btn btn-primary">Manage Appointments</a>
                <a href="due_bill.php" class="btn btn-primary">View Due Bills</a>
                <a href="modify_patient.php" class="btn btn-primary">Update Personal Info</a>
            </div>
        </div>
    </div>

    <div class="card shadow-sm">
        <div class="card-body">
            <h4 class="card-title">Upcoming Appointments</h4>
            <?php if ($appointments->num_rows > 0): ?>
                <div class="table-responsive">
                    <table class="table table-bordered mt-3">
                        <thead class="table-primary">
                            <tr>
                                <th>Date</th>
                                <th>Time</th>
                                <th>Doctor</th>
                                <th>Specialization</th>
                                <th>Phone</th>
                                <th>Hospital</th>
                                <th>Address</th>
                            </tr>
                        </thead>
                        <tbody>
```

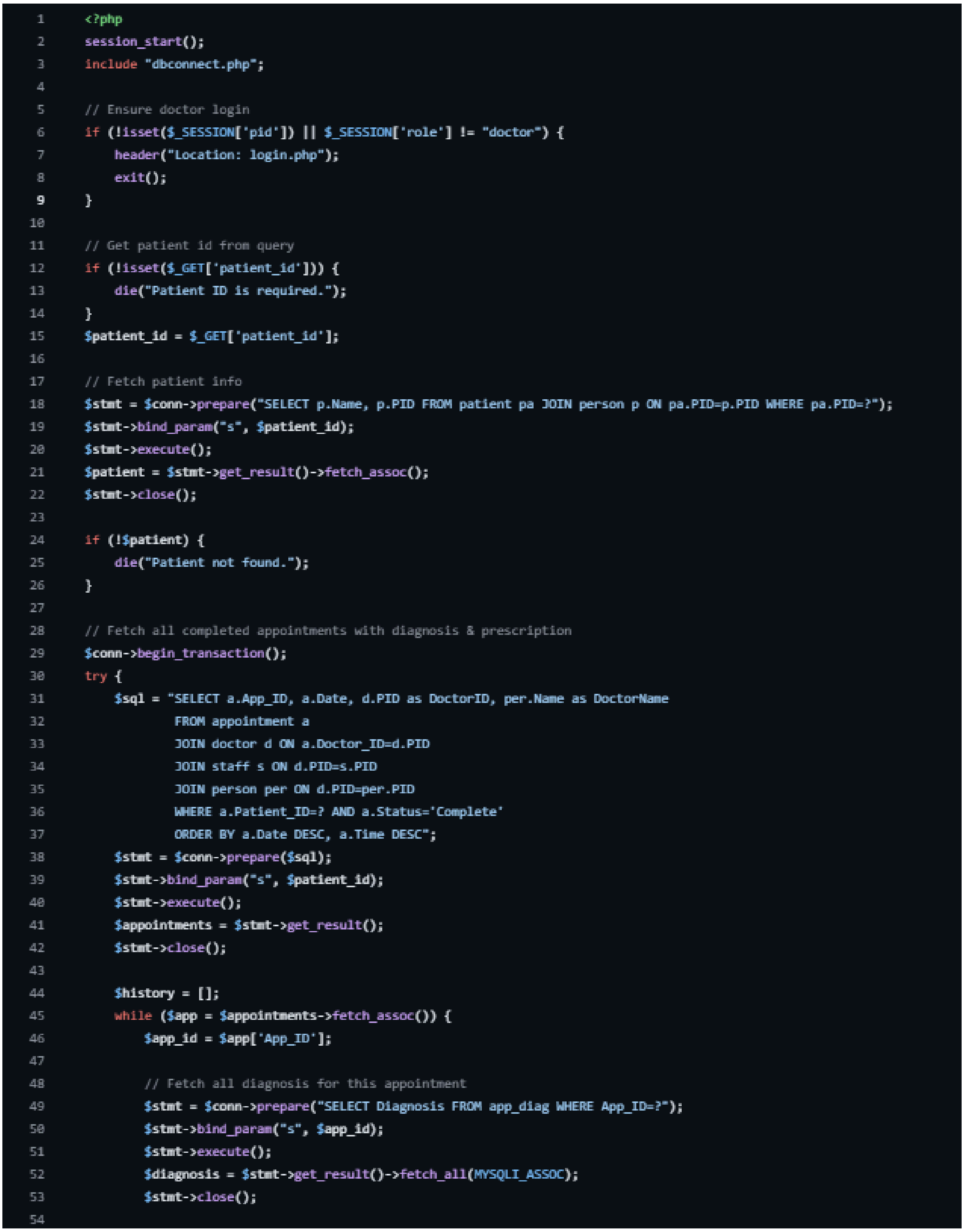
SELECT p.PID, p.Name, p.DateofBirth, p.email, p.Phone, pa.BloodGroup, pa.HasInsurance
FROM person p
JOIN patient pa ON p.PID = pa.PID
WHERE p.PID = ?

This part of the code can fetch information for patients personal (email, phone number etc.) and medical data (blood group, insurance status).

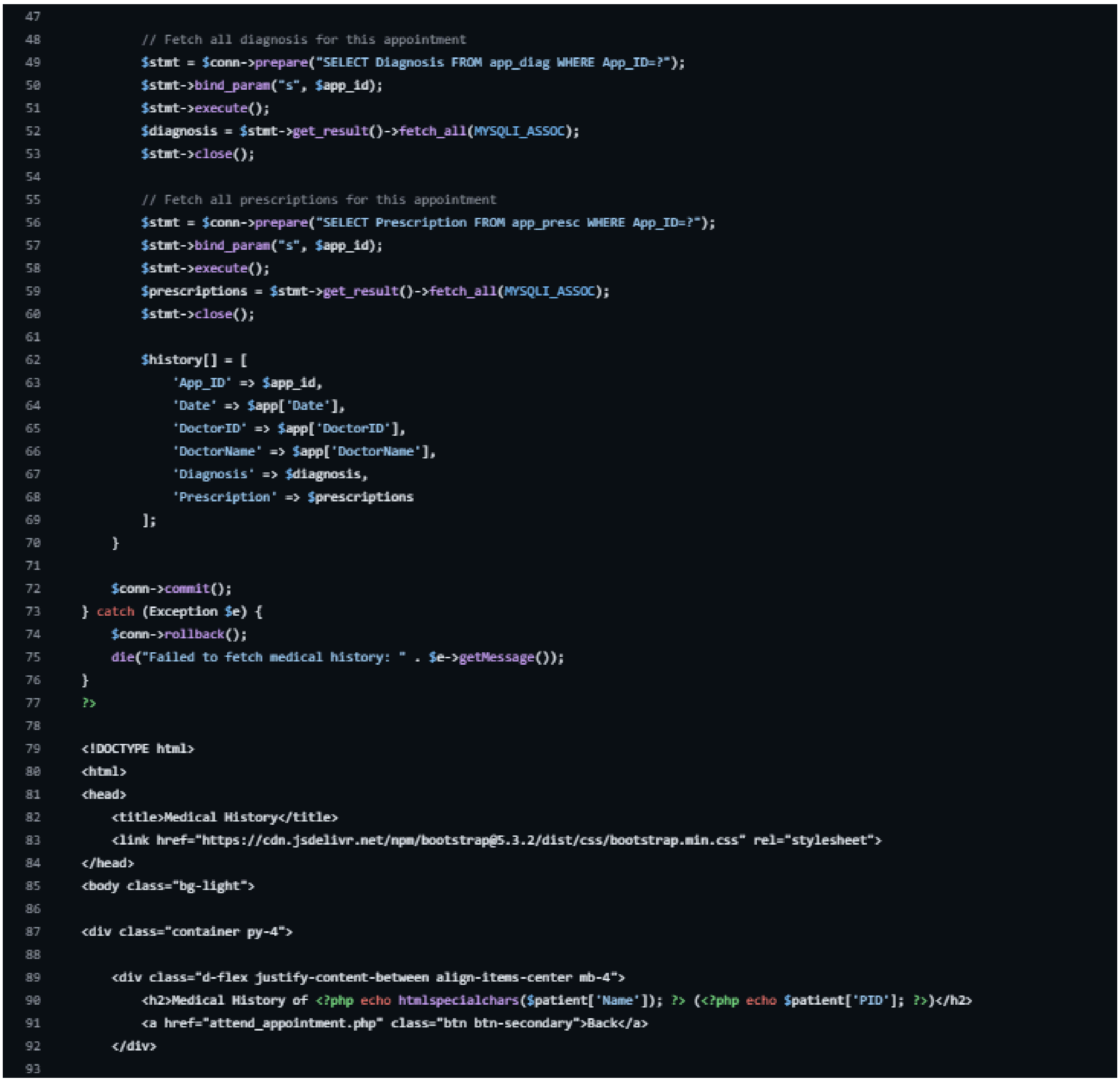
```
SELECT a.App_ID, a.Date, a.Time, doc.PID AS DoctorID, per.Name AS DoctorName,
    doc.Specialization, per.Phone AS DoctorPhone, h.Name AS HospitalName,
    CONCAT(h.Plot, ', ', h.Street, ', ', h.Area) AS HospitalAddress
FROM appointment a
JOIN doctor doc ON a.Doctor_ID = doc.PID
JOIN staff s ON doc.PID = s.PID
JOIN hospital h ON s.hospital_id = h.HospitalID
JOIN person per ON doc.PID = per.PID
WHERE a.Patient_ID = ? AND a.Status = 'Upcoming' AND a.Date >= CURDATE()
ORDER BY a.Date, a.Time
```

These are the upcoming appointment query and only upcoming appointments are allowed for today and future dates. Here, fetched data for appointment is date and time. Doctor information name, specialization, phone has been fetched and finally for hospital information name and full address are the fetched data. Used tables are appointment, doctor, staff, hospital, person (multiple joins). This code only fetches and displays data. Therefore, it does not modify any data in the database.

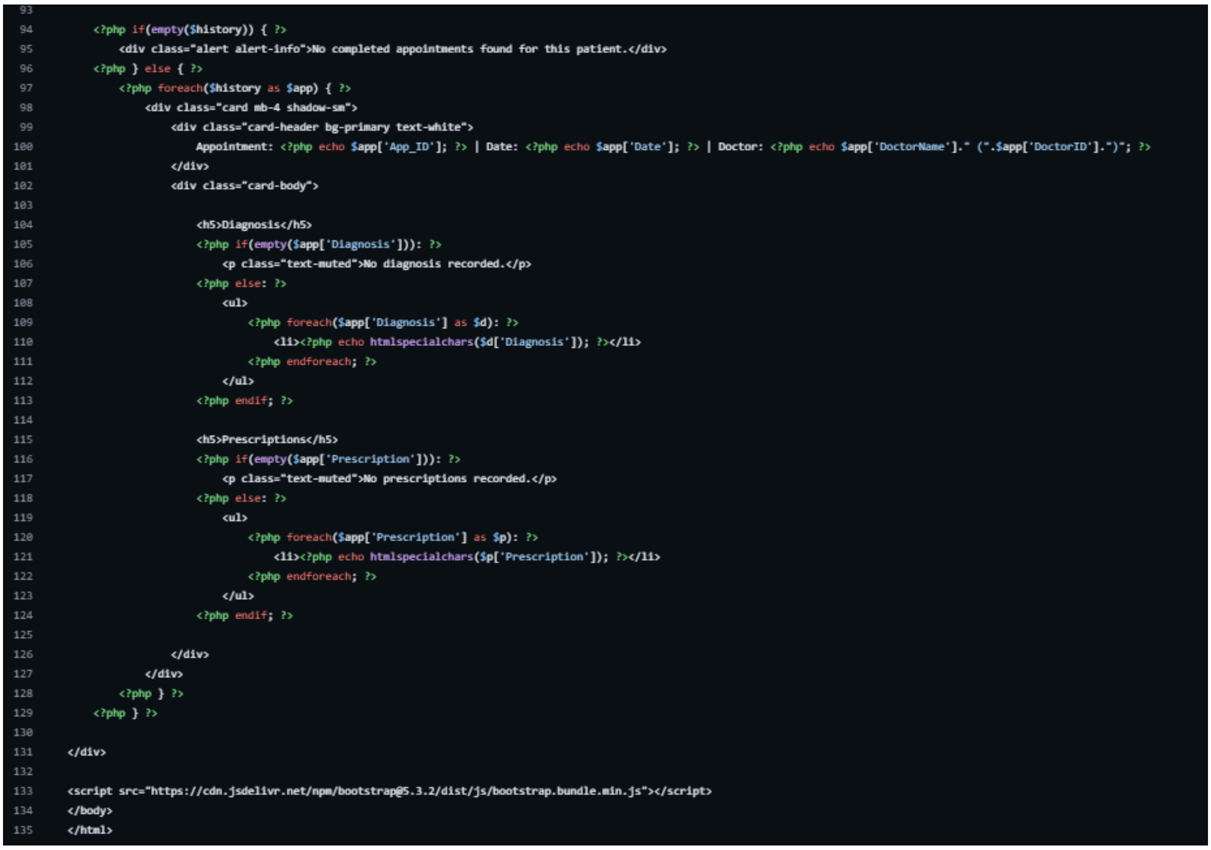
Medical History :



```php
<?php
session_start();
include "dbconnect.php";

// Ensure doctor login
if (!isset($_SESSION['pid']) || $_SESSION['role'] != "doctor") {
    header("Location: login.php");
    exit();
}

// Get patient id from query
if (!isset($_GET['patient_id'])) {
    die("Patient ID is required.");
}
$patient_id = $_GET['patient_id'];

// Fetch patient info
$stmt = $conn->prepare("SELECT p.Name, p.PID FROM patient pa JOIN person p ON pa.PID=p.PID WHERE pa.PID=?");
$stmt->bind_param("s", $patient_id);
$stmt->execute();
$patient = $stmt->get_result()->fetch_assoc();
$stmt->close();

if (!$patient) {
    die("Patient not found.");
}

// Fetch all completed appointments with diagnosis & prescription
$conn->begin_transaction();
try {
    $sql = "SELECT a.App_ID, a.Date, d.PID as DoctorID, per.Name as DoctorName
            FROM appointment a
            JOIN doctor d ON a.Doctor_ID=d.PID
            JOIN staff s ON d.PID=s.PID
            JOIN person per ON d.PID=per.PID
            WHERE a.Patient_ID=? AND a.Status='Complete'
            ORDER BY a.Date DESC, a.Time DESC";
    $stmt = $conn->prepare($sql);
    $stmt->bind_param("s", $patient_id);
    $stmt->execute();
    $appointments = $stmt->get_result();
    $stmt->close();

    $history = [];
    while ($app = $appointments->fetch_assoc()) {
        $app_id = $app['App_ID'];

        // Fetch all diagnosis for this appointment
        $stmt = $conn->prepare("SELECT Diagnosis FROM app_diag WHERE App_ID=?");
        $stmt->bind_param("s", $app_id);
        $stmt->execute();
        $diagnosis = $stmt->get_result()->fetch_all(MYSQLI_ASSOC);
        $stmt->close();

```



```

        // Fetch all diagnosis for this appointment
        $stmt = $conn->prepare("SELECT Diagnosis FROM app_diag WHERE App_ID=?");
        $stmt->bind_param("s", $app_id);
        $stmt->execute();
        $diagnosis = $stmt->get_result()->fetch_all(MYSQLI_ASSOC);
        $stmt->close();

        // Fetch all prescriptions for this appointment
        $stmt = $conn->prepare("SELECT Prescription FROM app_presc WHERE App_ID=?");
        $stmt->bind_param("s", $app_id);
        $stmt->execute();
        $prescriptions = $stmt->get_result()->fetch_all(MYSQLI_ASSOC);
        $stmt->close();

        $history[] = [
            'App_ID' => $app_id,
            'Date' => $app['Date'],
            'DoctorID' => $app['DoctorID'],
            'DoctorName' => $app['DoctorName'],
            'Diagnosis' => $diagnosis,
            'Prescription' => $prescriptions
        ];
    }

    $conn->commit();
} catch (Exception $e) {
    $conn->rollback();
    die("Failed to fetch medical history: " . $e->getMessage());
}
?>

<!DOCTYPE html>
<html>
<head>
    <title>Medical History</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" rel="stylesheet">
</head>
<body class="bg-light">

<div class="container py-4">

    <div class="d-flex justify-content-between align-items-center mb-4">
        <h2>Medical History of <?php echo htmlspecialchars($patient['Name']); ?> (<?php echo $patient['PID']; ?>)</h2>
        <a href="attend_appointment.php" class="btn btn-secondary">Back</a>
    </div>

```



```
        <?php if(empty($history)) { ?>
            <div class="alert alert-info">No completed appointments found for this patient.</div>
        <?php } else { ?>
            <?php foreach($history as $app) { ?>
                <div class="card mb-4 shadow-sm">
                    <div class="card-header bg-primary text-white">
                        Appointment: <?php echo $app['App_ID']; ?> | Date: <?php echo $app['Date']; ?> | Doctor: <?php echo $app['DoctorName']." (".$app['DoctorID'].")"; ?>
                    </div>
                    <div class="card-body">

                        <h5>Diagnosis</h5>
                        <?php if(empty($app['Diagnosis'])): ?>
                            <p class="text-muted">No diagnosis recorded.</p>
                        <?php else: ?>
                            <ul>
                                <?php foreach($app['Diagnosis'] as $d): ?>
                                    <li><?php echo htmlspecialchars($d['Diagnosis']); ?></li>
                                <?php endforeach; ?>
                            </ul>
                        <?php endif; ?>

                        <h5>Prescriptions</h5>
                        <?php if(empty($app['Prescription'])): ?>
                            <p class="text-muted">No prescriptions recorded.</p>
                        <?php else: ?>
                            <ul>
                                <?php foreach($app['Prescription'] as $p): ?>
                                    <li><?php echo htmlspecialchars($p['Prescription']); ?></li>
                                <?php endforeach; ?>
                            </ul>
                        <?php endif; ?>

                    </div>
                </div>
            <?php } ?>
        <?php } ?>

    </div>

    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/js/bootstrap.bundle.min.js"></script>
    </body>
    </html>
```

$stmt = $conn->prepare("SELECT p.Name, p.PID FROM patient pa JOIN person p ON pa.PID=p.PID WHERE pa.PID=?"); This part verifies if the requested patient exists in the system. Here, the fetched data is patient name and id.

```
$sql = "SELECT a.App_ID, a.Date, d.PID as DoctorID, per.Name as DoctorName
    FROM appointment a
    JOIN doctor d ON a.Doctor_ID=d.PID
    JOIN staff s ON d.PID=s.PID
    JOIN person per ON d.PID=per.PID
    WHERE a.Patient_ID=? AND a.Status='Complete'
    ORDER BY a.Date DESC, a.Time DESC";
```

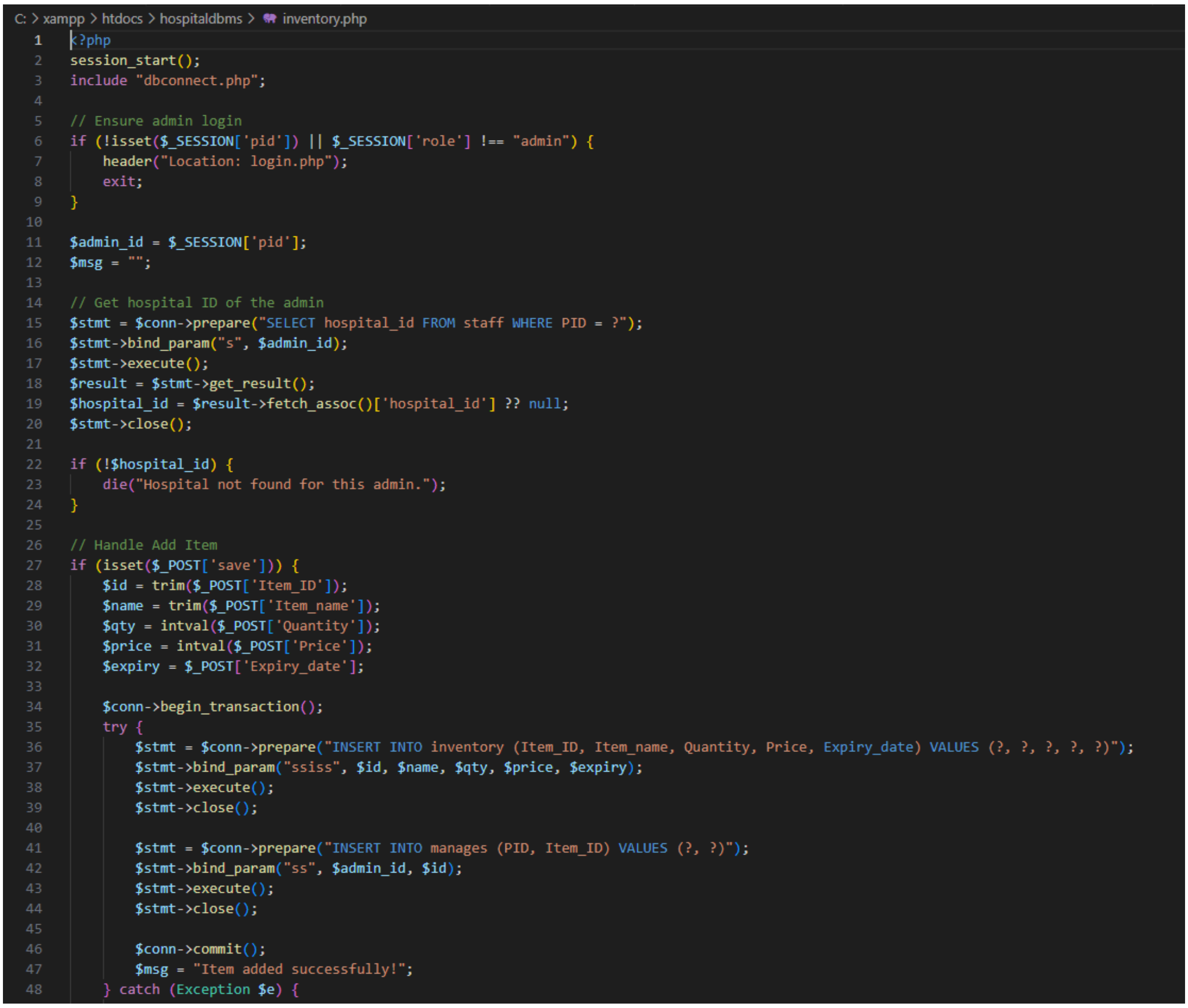
This part fetches all the completed appointments for the patient. This part filters for the specific patient completed appointments only.

$stmt = $conn->prepare("SELECT Diagnosis FROM app_diag WHERE App_ID=?"); for a specific appointment it retrieves all the diagnosis.

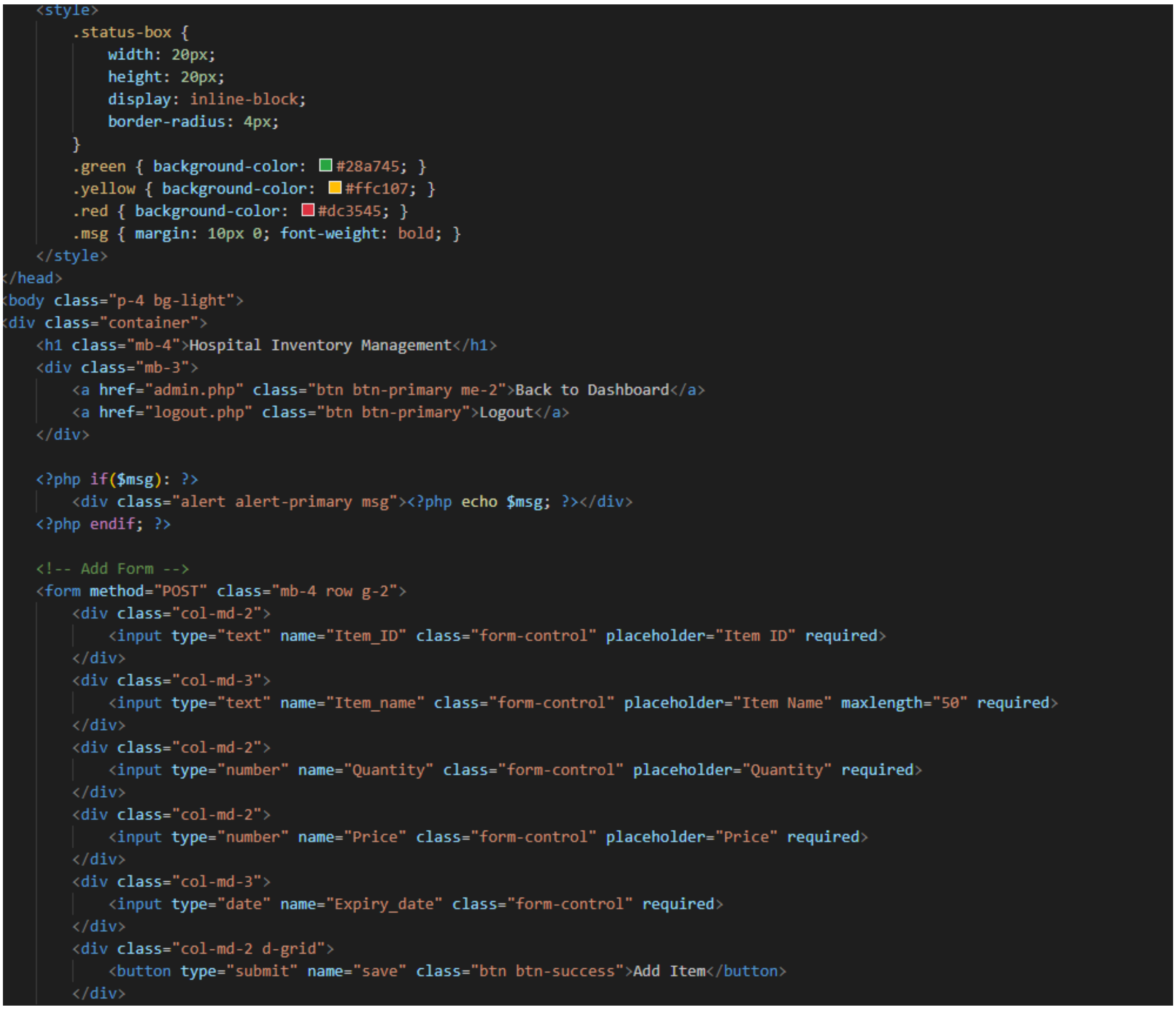
This code doesn't change any database records. Therefore, it just retrieves and shows data. To sum up, the system here shows the patient's entire medical history after the doctor chooses a patient from their appointment list. Doctors have access to previous diagnoses and treatments. When finished, the doctor can go back to the appointment management screen.

Contribution of ID : 21301594, Name : Mydul Islam Lisun

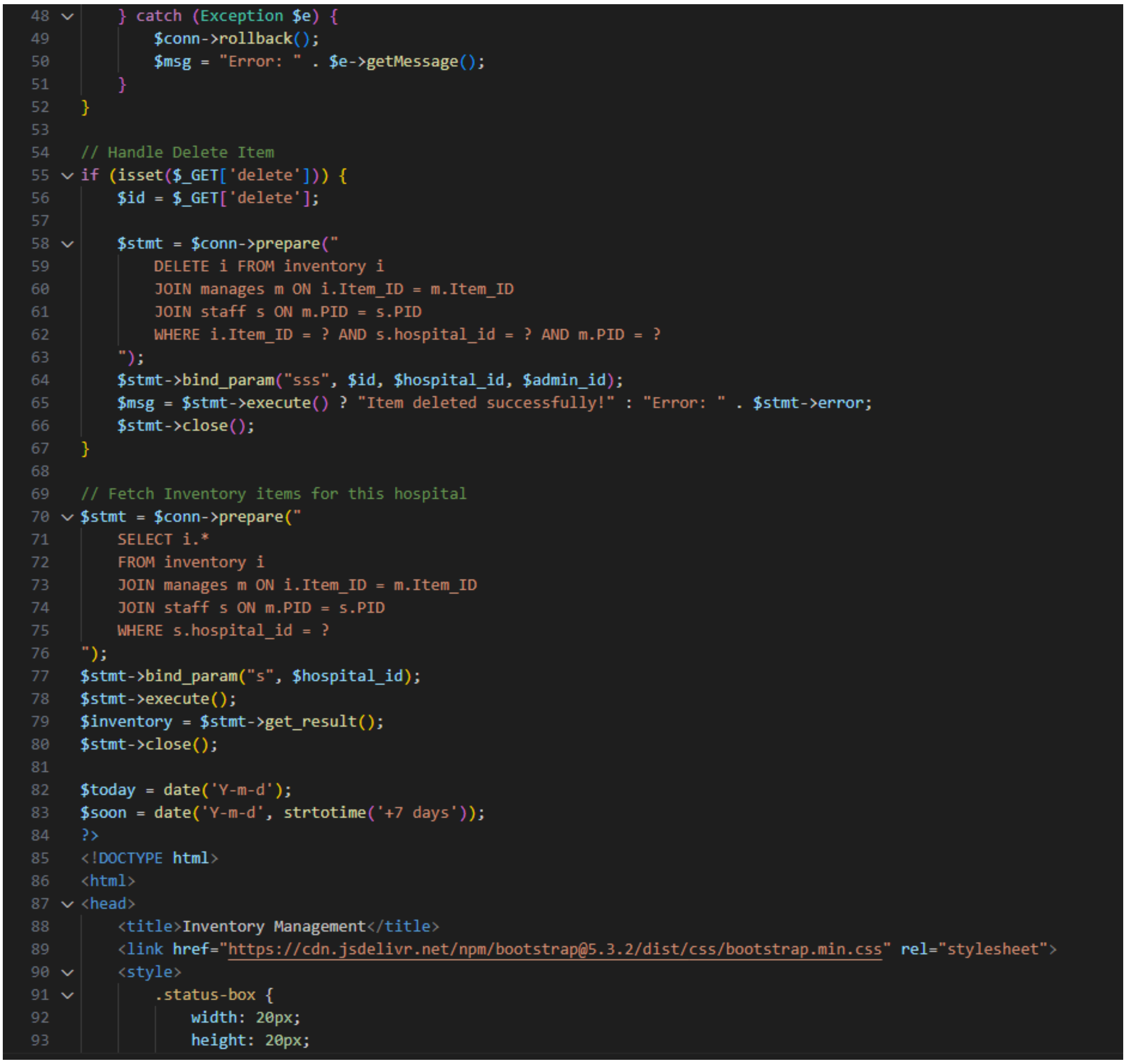
Inventory management:



```php
<?php
session_start();
include "dbconnect.php";

// Ensure admin login
if (!isset($_SESSION['pid']) || $_SESSION['role'] !== "admin") {
    header("Location: login.php");
    exit;
}

$admin_id = $_SESSION['pid'];
$msg = "";

// Get hospital ID of the admin
$stmt = $conn->prepare("SELECT hospital_id FROM staff WHERE PID = ?");
$stmt->bind_param("s", $admin_id);
$stmt->execute();
$result = $stmt->get_result();
$hospital_id = $result->fetch_assoc()['hospital_id'] ?? null;
$stmt->close();

if (!$hospital_id) {
    die("Hospital not found for this admin.");
}

// Handle Add Item
if (isset($_POST['save'])) {
    $id = trim($_POST['Item_ID']);
    $name = trim($_POST['Item_name']);
    $qty = intval($_POST['Quantity']);
    $price = intval($_POST['Price']);
    $expiry = $_POST['Expiry_date'];

    $conn->begin_transaction();
    try {
        $stmt = $conn->prepare("INSERT INTO inventory (Item_ID, Item_name, Quantity, Price, Expiry_date) VALUES (?, ?, ?, ?, ?)");
        $stmt->bind_param("ssiss", $id, $name, $qty, $price, $expiry);
        $stmt->execute();
        $stmt->close();

        $stmt = $conn->prepare("INSERT INTO manages (PID, Item_ID) VALUES (?, ?)");
        $stmt->bind_param("ss", $admin_id, $id);
        $stmt->execute();
        $stmt->close();

        $conn->commit();
        $msg = "Item added successfully!";
    } catch (Exception $e) {
```

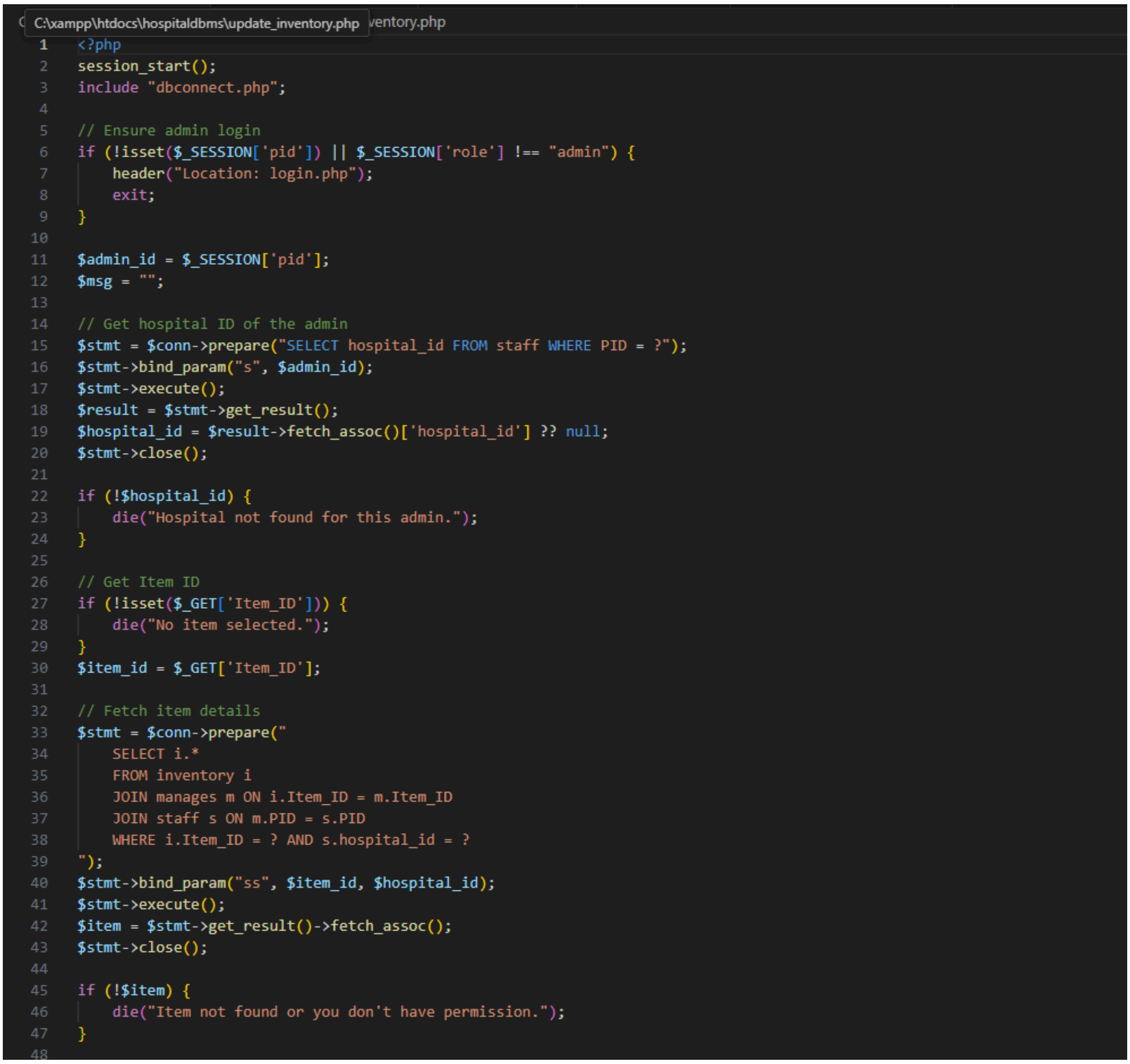


```
    <style>
        .status-box {
            width: 20px;
            height: 20px;
            display: inline-block;
            border-radius: 4px;
        }
        .green { background-color: 🟩#28a745; }
        .yellow { background-color: 🟨#ffc107; }
        .red { background-color: 🟥#dc3545; }
        .msg { margin: 10px 0; font-weight: bold; }
    </style>
</head>
<body class="p-4 bg-light">
<div class="container">
    <h1 class="mb-4">Hospital Inventory Management</h1>
    <div class="mb-3">
        <a href="admin.php" class="btn btn-primary me-2">Back to Dashboard</a>
        <a href="logout.php" class="btn btn-primary">Logout</a>
    </div>

    <?php if($msg): ?>
        <div class="alert alert-primary msg"><?php echo $msg; ?></div>
    <?php endif; ?>

    <!-- Add Form -->
    <form method="POST" class="mb-4 row g-2">
        <div class="col-md-2">
            <input type="text" name="Item_ID" class="form-control" placeholder="Item ID" required>
        </div>
        <div class="col-md-3">
            <input type="text" name="Item_name" class="form-control" placeholder="Item Name" maxlength="50" required>
        </div>
        <div class="col-md-2">
            <input type="number" name="Quantity" class="form-control" placeholder="Quantity" required>
        </div>
        <div class="col-md-2">
            <input type="number" name="Price" class="form-control" placeholder="Price" required>
        </div>
        <div class="col-md-3">
            <input type="date" name="Expiry_date" class="form-control" required>
        </div>
        <div class="col-md-2 d-grid">
            <button type="submit" name="save" class="btn btn-success">Add Item</button>
        </div>
```

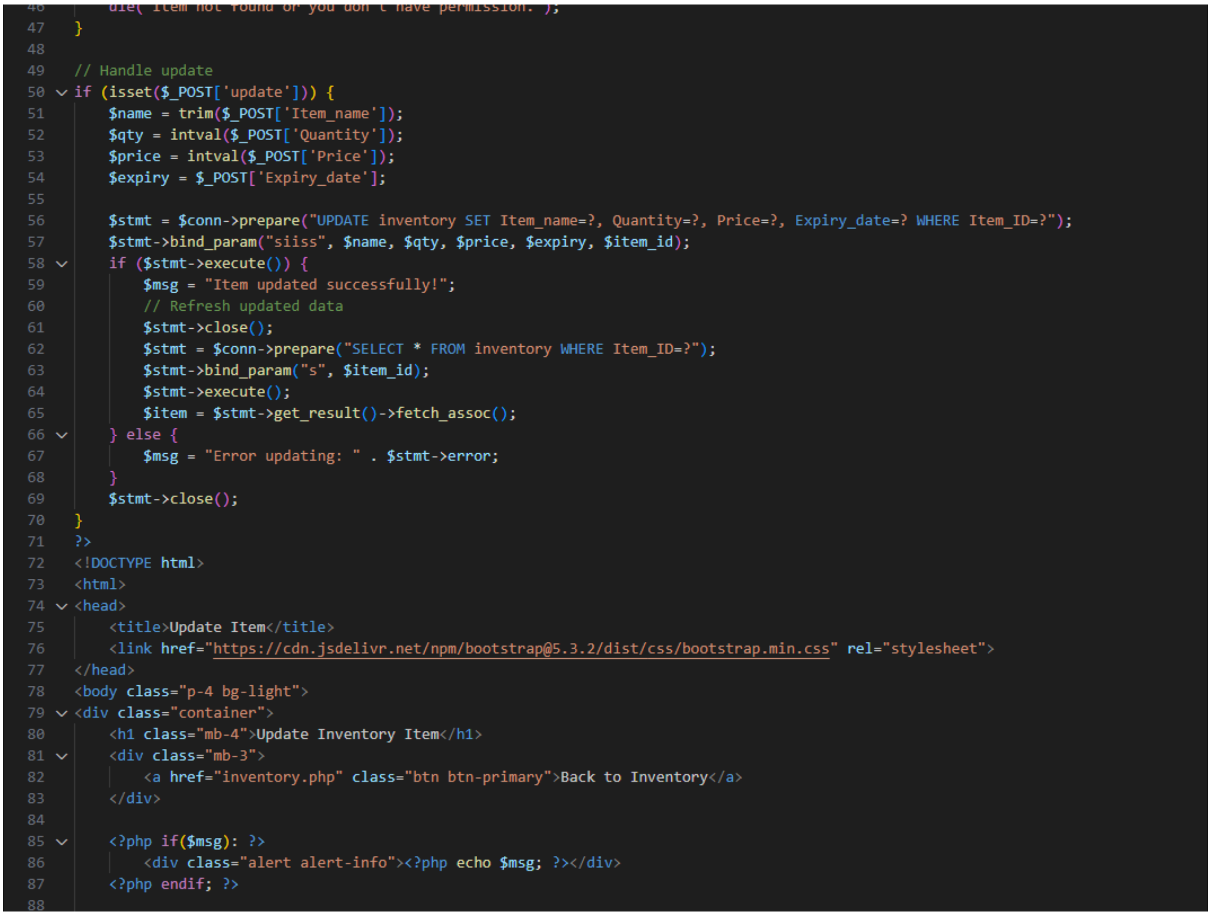


```
    } catch (Exception $e) {
        $conn->rollback();
        $msg = "Error: " . $e->getMessage();
    }
}

// Handle Delete Item
if (isset($_GET['delete'])) {
    $id = $_GET['delete'];

    $stmt = $conn->prepare("
        DELETE i FROM inventory i
        JOIN manages m ON i.Item_ID = m.Item_ID
        JOIN staff s ON m.PID = s.PID
        WHERE i.Item_ID = ? AND s.hospital_id = ? AND m.PID = ?
    ");
    $stmt->bind_param("sss", $id, $hospital_id, $admin_id);
    $msg = $stmt->execute() ? "Item deleted successfully!" : "Error: " . $stmt->error;
    $stmt->close();
}

// Fetch Inventory items for this hospital
$stmt = $conn->prepare("
    SELECT i.*
    FROM inventory i
    JOIN manages m ON i.Item_ID = m.Item_ID
    JOIN staff s ON m.PID = s.PID
    WHERE s.hospital_id = ?
");
$stmt->bind_param("s", $hospital_id);
$stmt->execute();
$inventory = $stmt->get_result();
$stmt->close();

$today = date('Y-m-d');
$soon = date('Y-m-d', strtotime('+7 days'));
?>
<!DOCTYPE html>
<html>
<head>
    <title>Inventory Management</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" rel="stylesheet">
    <style>
        .status-box {
            width: 20px;
            height: 20px;
```

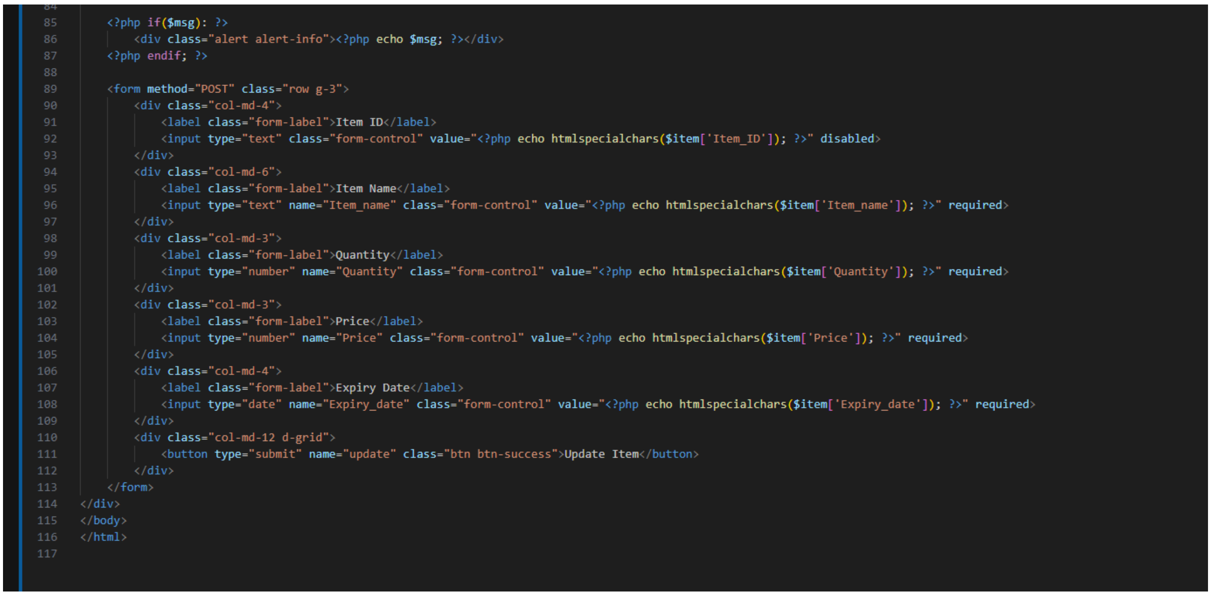
Inventory Update:



```php
<?php
session_start();
include "dbconnect.php";

// Ensure admin login
if (!isset($_SESSION['pid']) || $_SESSION['role'] !== "admin") {
    header("Location: login.php");
    exit;
}

$admin_id = $_SESSION['pid'];
$msg = "";

// Get hospital ID of the admin
$stmt = $conn->prepare("SELECT hospital_id FROM staff WHERE PID = ?");
$stmt->bind_param("s", $admin_id);
$stmt->execute();
$result = $stmt->get_result();
$hospital_id = $result->fetch_assoc()['hospital_id'] ?? null;
$stmt->close();

if (!$hospital_id) {
    die("Hospital not found for this admin.");
}

// Get Item ID
if (!isset($_GET['Item_ID'])) {
    die("No item selected.");
}
$item_id = $_GET['Item_ID'];

// Fetch item details
$stmt = $conn->prepare("
    SELECT i.*
    FROM inventory i
    JOIN manages m ON i.Item_ID = m.Item_ID
    JOIN staff s ON m.PID = s.PID
    WHERE i.Item_ID = ? AND s.hospital_id = ?
");
$stmt->bind_param("ss", $item_id, $hospital_id);
$stmt->execute();
$item = $stmt->get_result()->fetch_assoc();
$stmt->close();

if (!$item) {
    die("Item not found or you don't have permission.");
}
```



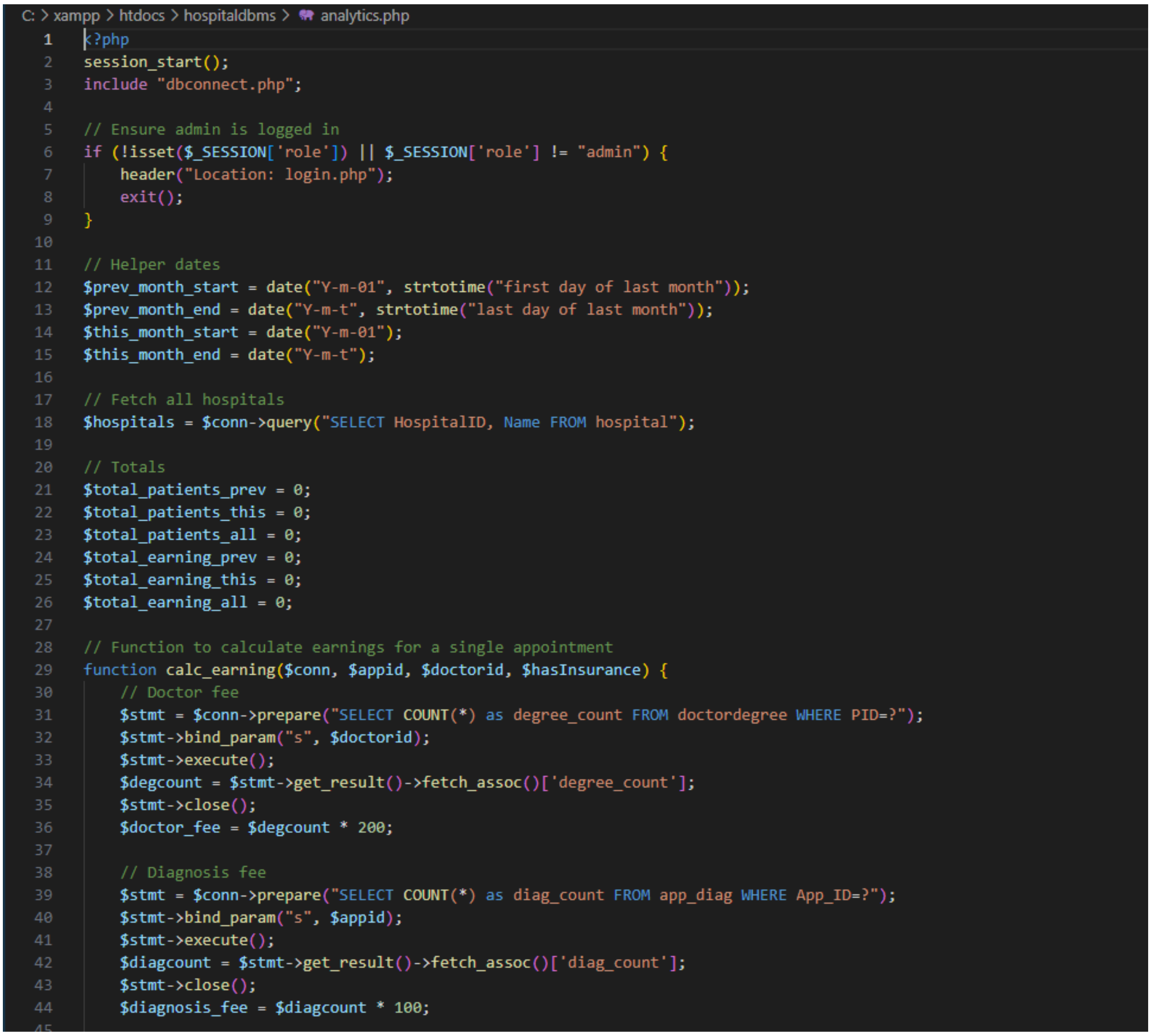
```php
        die("Item not found or you don't have permission.");
}

// Handle update
if (isset($_POST['update'])) {
    $name = trim($_POST['Item_name']);
    $qty = intval($_POST['Quantity']);
    $price = intval($_POST['Price']);
    $expiry = $_POST['Expiry_date'];

    $stmt = $conn->prepare("UPDATE inventory SET Item_name=?, Quantity=?, Price=?, Expiry_date=? WHERE Item_ID=?");
    $stmt->bind_param("siiss", $name, $qty, $price, $expiry, $item_id);
    if ($stmt->execute()) {
        $msg = "Item updated successfully!";
        // Refresh updated data
        $stmt->close();
        $stmt = $conn->prepare("SELECT * FROM inventory WHERE Item_ID=?");
        $stmt->bind_param("s", $item_id);
        $stmt->execute();
        $item = $stmt->get_result()->fetch_assoc();
    } else {
        $msg = "Error updating: " . $stmt->error;
    }
    $stmt->close();
}
?>
<!DOCTYPE html>
<html>
<head>
    <title>Update Item</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" rel="stylesheet">
</head>
<body class="p-4 bg-light">
<div class="container">
    <h1 class="mb-4">Update Inventory Item</h1>
    <div class="mb-3">
        <a href="inventory.php" class="btn btn-primary">Back to Inventory</a>
    </div>

    <?php if($msg): ?>
        <div class="alert alert-info"><?php echo $msg; ?></div>
    <?php endif; ?>

```



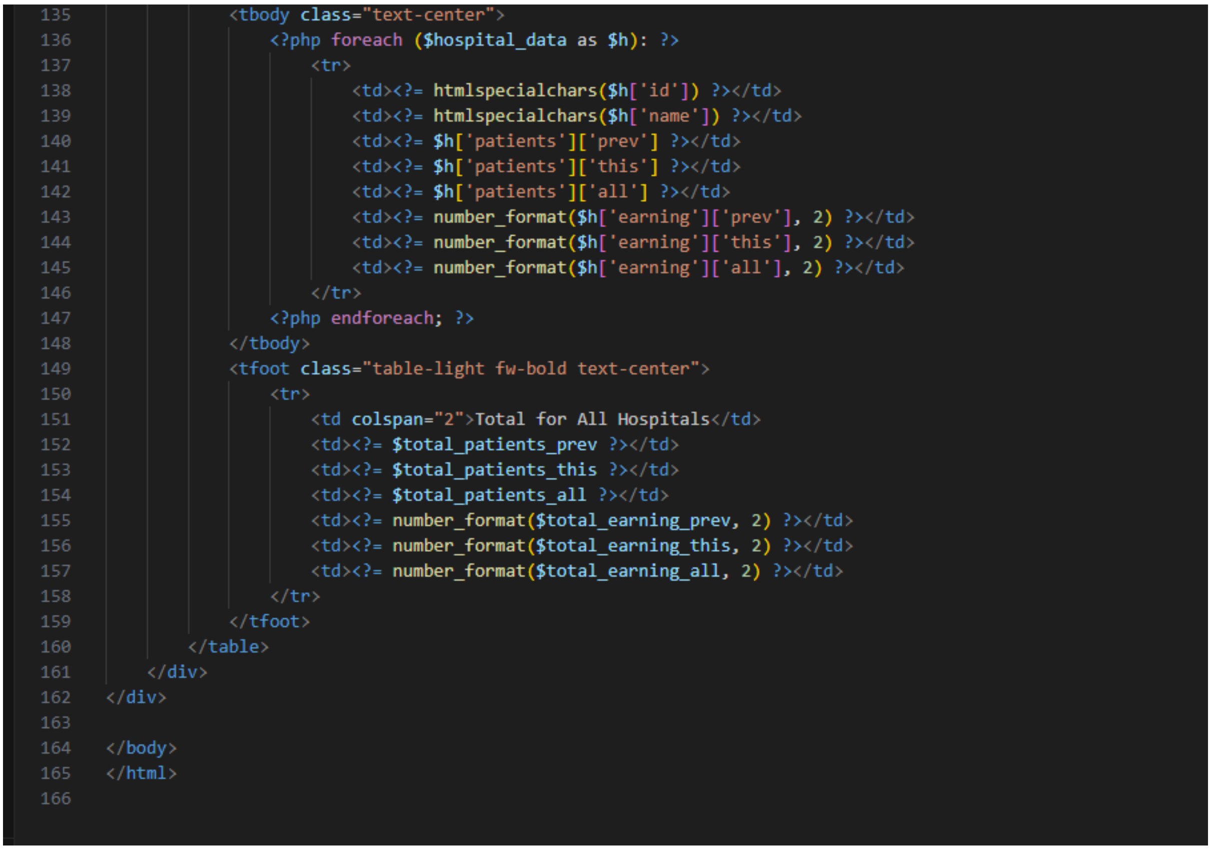
```php
    <?php if($msg): ?>
        <div class="alert alert-info"><?php echo $msg; ?></div>
    <?php endif; ?>
```

```php

    <form method="POST" class="row g-3">
        <div class="col-md-4">
            <label class="form-label">Item ID</label>
            <input type="text" class="form-control" value="<?php echo htmlspecialchars($item['Item_ID']); ?>" disabled>
        </div>
        <div class="col-md-6">
            <label class="form-label">Item Name</label>
            <input type="text" name="Item_name" class="form-control" value="<?php echo htmlspecialchars($item['Item_name']); ?>" required>
        </div>
        <div class="col-md-3">
            <label class="form-label">Quantity</label>
            <input type="number" name="Quantity" class="form-control" value="<?php echo htmlspecialchars($item['Quantity']); ?>" required>
        </div>
        <div class="col-md-3">
            <label class="form-label">Price</label>
            <input type="number" name="Price" class="form-control" value="<?php echo htmlspecialchars($item['Price']); ?>" required>
        </div>
        <div class="col-md-4">
            <label class="form-label">Expiry Date</label>
            <input type="date" name="Expiry_date" class="form-control" value="<?php echo htmlspecialchars($item['Expiry_date']); ?>" required>
        </div>
        <div class="col-md-12 d-grid">
            <button type="submit" name="update" class="btn btn-success">Update Item</button>
        </div>
    </form>
</div>
</body>
</html>

```

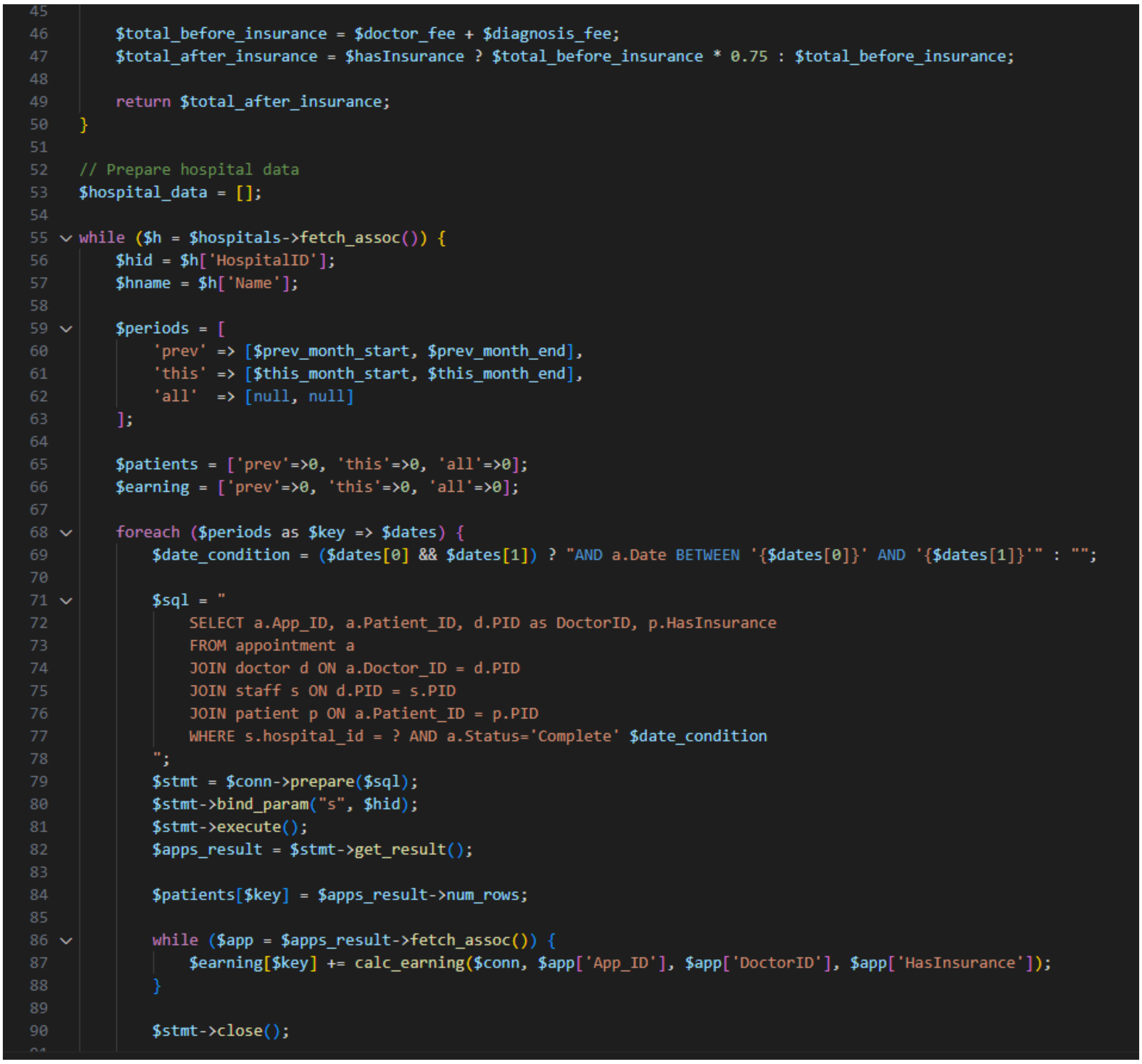
Analytics Dashboard for district health authority:



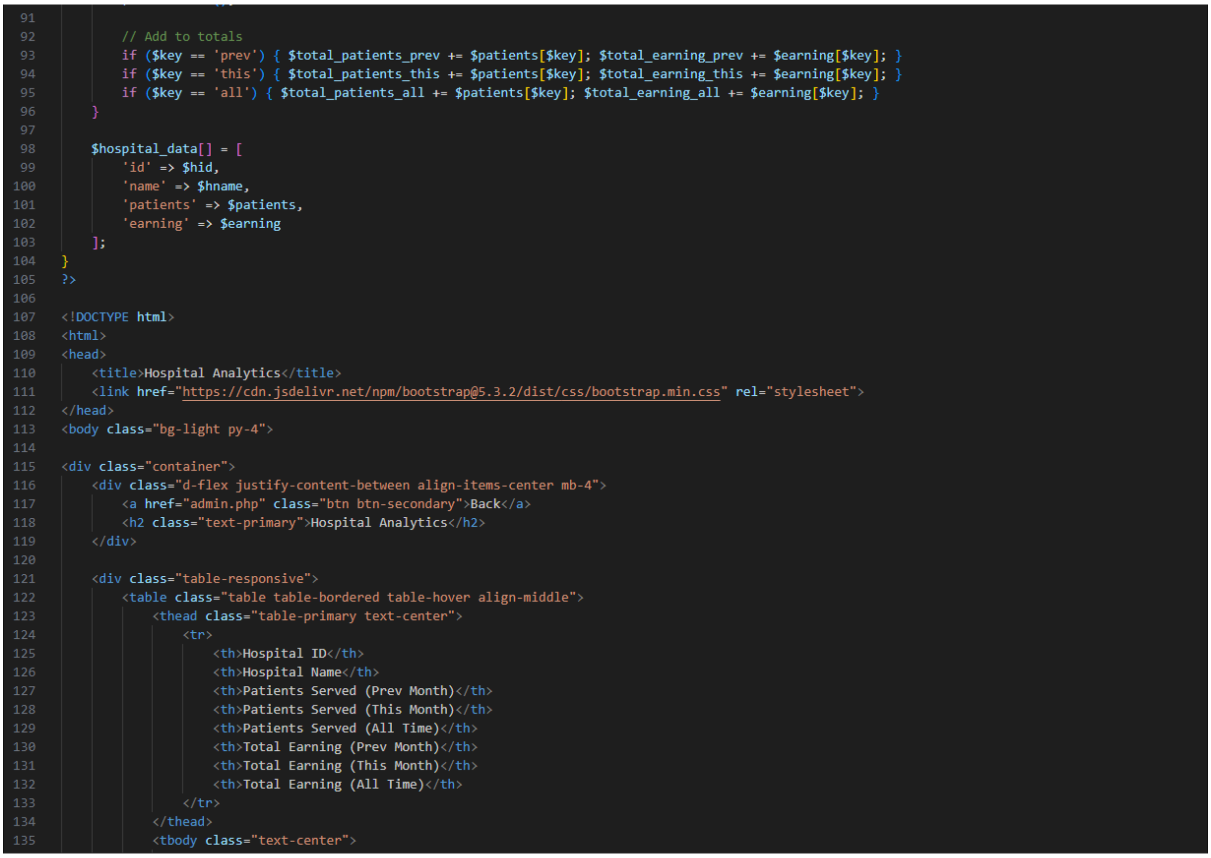
```php
<?php
session_start();
include "dbconnect.php";

// Ensure admin is logged in
if (!isset($_SESSION['role']) || $_SESSION['role'] != "admin") {
    header("Location: login.php");
    exit();
}

// Helper dates
$prev_month_start = date("Y-m-01", strtotime("first day of last month"));
$prev_month_end = date("Y-m-t", strtotime("last day of last month"));
$this_month_start = date("Y-m-01");
$this_month_end = date("Y-m-t");

// Fetch all hospitals
$hospitals = $conn->query("SELECT HospitalID, Name FROM hospital");

// Totals
$total_patients_prev = 0;
$total_patients_this = 0;
$total_patients_all = 0;
$total_earning_prev = 0;
$total_earning_this = 0;
$total_earning_all = 0;

// Function to calculate earnings for a single appointment
function calc_earning($conn, $appid, $doctorid, $hasInsurance) {
    // Doctor fee
    $stmt = $conn->prepare("SELECT COUNT(*) as degree_count FROM doctordegree WHERE PID=?");
    $stmt->bind_param("s", $doctorid);
    $stmt->execute();
    $degcount = $stmt->get_result()->fetch_assoc()['degree_count'];
    $stmt->close();
    $doctor_fee = $degcount * 200;

    // Diagnosis fee
    $stmt = $conn->prepare("SELECT COUNT(*) as diag_count FROM app_diag WHERE App_ID=?");
    $stmt->bind_param("s", $appid);
    $stmt->execute();
    $diagcount = $stmt->get_result()->fetch_assoc()['diag_count'];
    $stmt->close();
    $diagnosis_fee = $diagcount * 100;
```



```
            <tbody class="text-center">
                <?php foreach ($hospital_data as $h): ?>
                    <tr>
                        <td><?= htmlspecialchars($h['id']) ?></td>
                        <td><?= htmlspecialchars($h['name']) ?></td>
                        <td><?= $h['patients']['prev'] ?></td>
                        <td><?= $h['patients']['this'] ?></td>
                        <td><?= $h['patients']['all'] ?></td>
                        <td><?= number_format($h['earning']['prev'], 2) ?></td>
                        <td><?= number_format($h['earning']['this'], 2) ?></td>
                        <td><?= number_format($h['earning']['all'], 2) ?></td>
                    </tr>
                <?php endforeach; ?>
            </tbody>
            <tfoot class="table-light fw-bold text-center">
                <tr>
                    <td colspan="2">Total for All Hospitals</td>
                    <td><?= $total_patients_prev ?></td>
                    <td><?= $total_patients_this ?></td>
                    <td><?= $total_patients_all ?></td>
                    <td><?= number_format($total_earning_prev, 2) ?></td>
                    <td><?= number_format($total_earning_this, 2) ?></td>
                    <td><?= number_format($total_earning_all, 2) ?></td>
                </tr>
            </tfoot>
        </table>
    </div>
</div>

</body>
</html>
```



```
    $total_before_insurance = $doctor_fee + $diagnosis_fee;
    $total_after_insurance = $hasInsurance ? $total_before_insurance * 0.75 : $total_before_insurance;

    return $total_after_insurance;
}

// Prepare hospital data
$hospital_data = [];

while ($h = $hospitals->fetch_assoc()) {
    $hid = $h['HospitalID'];
    $hname = $h['Name'];

    $periods = [
        'prev' => [$prev_month_start, $prev_month_end],
        'this' => [$this_month_start, $this_month_end],
        'all'  => [null, null]
    ];

    $patients = ['prev'=>0, 'this'=>0, 'all'=>0];
    $earning = ['prev'=>0, 'this'=>0, 'all'=>0];

    foreach ($periods as $key => $dates) {
        $date_condition = ($dates[0] && $dates[1]) ? "AND a.Date BETWEEN '{$dates[0]}' AND '{$dates[1]}'" : "";

        $sql = "
            SELECT a.App_ID, a.Patient_ID, d.PID as DoctorID, p.HasInsurance
            FROM appointment a
            JOIN doctor d ON a.Doctor_ID = d.PID
            JOIN staff s ON d.PID = s.PID
            JOIN patient p ON a.Patient_ID = p.PID
            WHERE s.hospital_id = ? AND a.Status='Complete' $date_condition
        ";
        $stmt = $conn->prepare($sql);
        $stmt->bind_param("s", $hid);
        $stmt->execute();
        $apps_result = $stmt->get_result();

        $patients[$key] = $apps_result->num_rows;

        while ($app = $apps_result->fetch_assoc()) {
            $earning[$key] += calc_earning($conn, $app['App_ID'], $app['DoctorID'], $app['HasInsurance']);
        }

        $stmt->close();
```



```

        // Add to totals
        if ($key == 'prev') { $total_patients_prev += $patients[$key]; $total_earning_prev += $earning[$key]; }
        if ($key == 'this') { $total_patients_this += $patients[$key]; $total_earning_this += $earning[$key]; }
        if ($key == 'all') { $total_patients_all += $patients[$key]; $total_earning_all += $earning[$key]; }
    }

    $hospital_data[] = [
        'id' => $hid,
        'name' => $hname,
        'patients' => $patients,
        'earning' => $earning
    ];
}
?>

<!DOCTYPE html>
<html>
<head>
    <title>Hospital Analytics</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" rel="stylesheet">
</head>
<body class="bg-light py-4">

<div class="container">
    <div class="d-flex justify-content-between align-items-center mb-4">
        <a href="admin.php" class="btn btn-secondary">Back</a>
        <h2 class="text-primary">Hospital Analytics</h2>
    </div>

    <div class="table-responsive">
        <table class="table table-bordered table-hover align-middle">
            <thead class="table-primary text-center">
                <tr>
                    <th>Hospital ID</th>
                    <th>Hospital Name</th>
                    <th>Patients Served (Prev Month)</th>
                    <th>Patients Served (This Month)</th>
                    <th>Patients Served (All Time)</th>
                    <th>Total Earning (Prev Month)</th>
                    <th>Total Earning (This Month)</th>
                    <th>Total Earning (All Time)</th>
                </tr>
            </thead>
            <tbody class="text-center">
```

Source Code Repository

[Source Code]

Conclusion

Our project was mostly successful in solving the goal we set at the start, letting patients make appointments throughout a district, while avoiding schedule conflicts.
In terms of improvement we still need to fix the bill calculation formula and refine it further.
We can also further refine the system to allow doctors to have more freedom in terms of when they work instead of having rigid 6 day work weeks.
We could also add a system where patients could buy required prescriptions through the website to make it easier for patients to get required medicine.
We can also add further security features such as storing the passwords after encryption and using encoded urls to make unauthorized access in some edge cases difficult.

References

1. **https://www.w3schools.com/php/**
2. **https://getbootstrap.com/**
3. **https://www.youtube.com/watch?v=2HVKizgcfjo**
4. **https://www.youtube.com/watch?v=2fM6BJXvP6A**