Министерство образования и науки Российской Федерации

Государственное образовательное учреждение

высшего профессионального образования

Уфимский государственный авиационный технический университет

Лабораторная работа №5

Выполнил ст. гр. ПИ-321

Газин Д.Р.

Проверил:

Канашин В.В.

Уфа – 2021

**Порядок выполнения работы**

Задача 6.1.

Внесите изменения в предыдущую лабораторную работу: необходимо добавить пользователей с раздельными правами доступа. Такие пользователи смогут авторизоваться в системе и, в зависимости от своего типа, будут иметь разные права доступа, отражающиеся на доступных возможностях в интерфейсе.

1) Создадим новую таблицу users с полями username, password, rule.

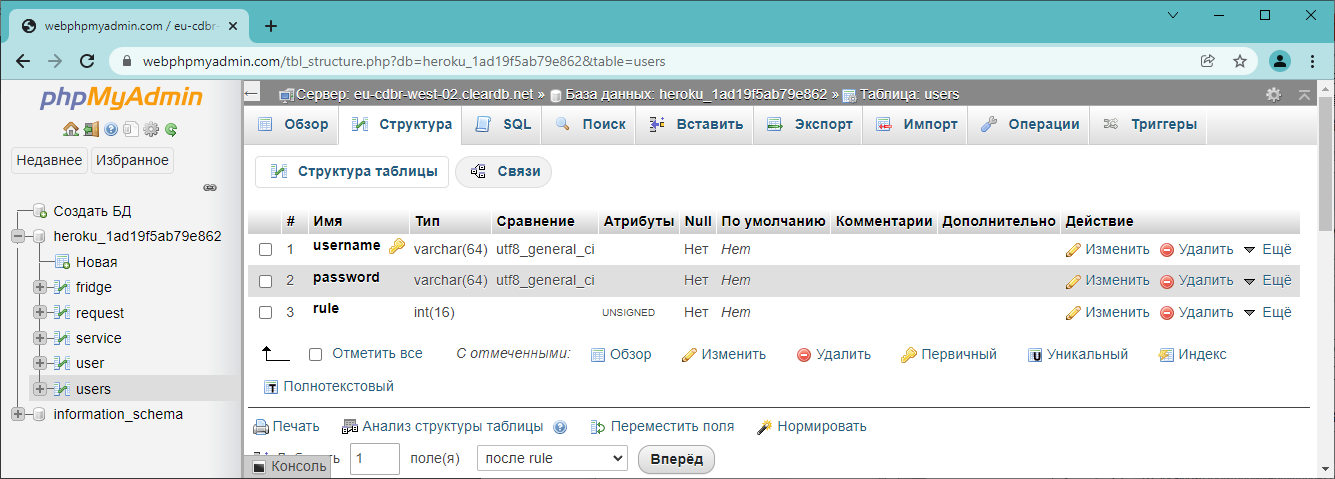


Рис. 1 – Структура таблицы users

2) Добавим администратора в таблицу.

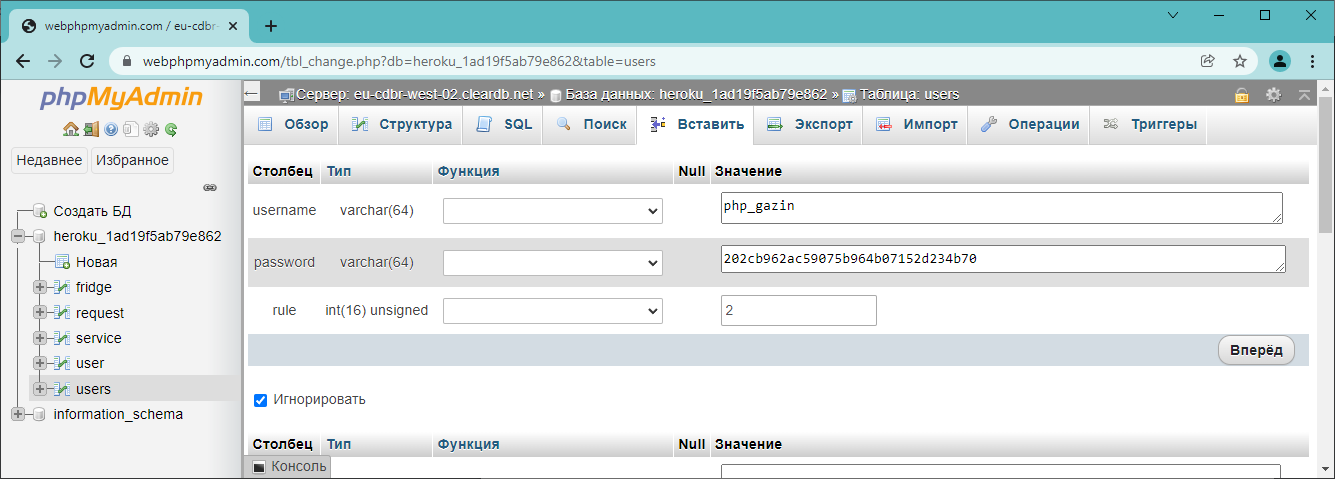


Рис. 2 – Добавление пользователя с правами администратора в таблицу

3) Создадим интерфейс на главной странице для ввода логина и пароля.

Добавим форму для входа:

<?php

echo "<html><head><title>Авторизация</title></head><body>";

echo "<h1>Газин Д. Р.</h1>";

echo "<form method='post' action='". $PHP\_SELF ."'>";

echo "<p>Пользователь:</p><input type='text' name='username' size='16'>";

echo "<p>Пароль:</p><input type='password' name='password' size='16'><br><br>";

echo "<input type='submit' name='submit' value='Войти'></form>";

echo "<br><a href='..'>Назад</a><br>";

?>

Добавим вывод содержимого базы данных:

<?php

if($\_SESSION["username"]) {

$query=mysqli\_query($conn, "SELECT rule FROM users WHERE username='" . $\_SESSION["username"] . "'");

if($fetch = mysqli\_fetch\_array($query)) $\_SESSION["rule"] = $fetch["rule"];

echo "<html><head><title>База данных</title></head><body>";

echo "<h2>Холодильники:</h2>";

echo "<table border='1'>";

echo "<tr><th> id </th>";

echo "<th> Марка </th> <th> Модель </th>";

echo "<th> Тип разморозки </th> <th> Внутренний объем, л. </th> <th> Срок гарантии, г. </th>";

echo "<th> Редактировать </th>";

if($\_SESSION["rule"] == 2) echo "<th>Уничтожить</th>";

echo "</tr>";

$result=mysqli\_query($conn, "SELECT \* FROM fridge");

while ($row=mysqli\_fetch\_array($result)){

echo "<tr>";

echo "<td>" . $row["id"] . "</td>";

echo "<td>" . $row["name"] . "</td>";

echo "<td>" . $row["model"] . "</td>";

echo "<td>" . $row["type"] . "</td>";

echo "<td>" . $row["volume"] . "</td>";

echo "<td>" . $row["time"] . "</td>";

echo "<td><a href='edit\_fridge.php?id=" . $row["id"]

. "'>Редактировать</a></td>";

if($\_SESSION["rule"] == 2) echo "<td><a href='delete\_fridge.php?id=" . $row["id"]

. "'>Удалить</a></td>";

echo "</tr>";

}

echo "</table>";

$num\_rows = mysqli\_num\_rows($result);

echo "<p> Всего записей: $num\_rows </p>";

echo "<a href='new\_fridge.php'> Добавить запись </a><br><br>";

echo "<h2>Сервисные центры:</h2>";

echo "<table border='1'>";

echo "<tr><th> id </th>";

echo "<th> Название </th> <th> Адрес </th>";

echo "<th> Редактировать </th>";

if($\_SESSION["rule"] == 2) echo "<th> Уничтожить </th></tr>";

$result=mysqli\_query($conn, "SELECT \* FROM service");

while ($row=mysqli\_fetch\_array($result)){

echo "<tr>";

echo "<td>" . $row["id"] . "</td>";

echo "<td>" . $row["name"] . "</td>";

echo "<td>" . $row["address"] . "</td>";

echo "<td><a href='edit\_service.php?id=" . $row["id"]

. "'>Редактировать</a></td>";

if($\_SESSION["rule"] == 2) echo "<td><a href='delete\_service.php?id=" . $row["id"]

. "'>Удалить</a></td>";

echo "</tr>";

}

echo "</table>";

$num\_rows = mysqli\_num\_rows($result);

echo "<p> Всего записей: $num\_rows </p>";

echo "<a href='new\_service.php'> Добавить запись </a><br><br>";

echo "<h2>Заявки на ремонт:</h2>";

echo "<table border='1'>";

echo "<tr><th> id </th>";

echo "<th> Дата начала </th> <th> Дата окончания </th>";

echo "<th> id Холодильника </th> <th> id Сервисного центра </th>";

echo "<th> ФИО </th> <th> Стоимость, руб. </th>";

echo "<th> Редактировать </th>";

if($\_SESSION["rule"] == 2) echo "<th> Уничтожить </th> </tr>";

$result=mysqli\_query($conn, "SELECT \* FROM request");

while ($row=mysqli\_fetch\_array($result)){

echo "<tr>";

echo "<td>" . $row["id"] . "</td>";

echo "<td>" . $row["date\_in"] . "</td>";

echo "<td>" . $row["date\_out"] . "</td>";

echo "<td>" . $row["id\_fridge"] . "</td>";

echo "<td>" . $row["id\_service"] . "</td>";

echo "<td>" . $row["fio"] . "</td>";

echo "<td>" . $row["price"] . "</td>";

echo "<td><a href='edit\_request.php?id=" . $row["id"]

. "'>Редактировать</a></td>";

if($\_SESSION["rule"] == 2) echo "<td><a href='delete\_request.php?id=" . $row["id"]

. "'>Удалить</a></td>";

echo "</tr>";

}

echo "</table>";

$num\_rows = mysqli\_num\_rows($result);

echo "<p> Всего записей: $num\_rows </p>";

echo "<a href='new\_request.php'> Добавить запись </a><br><br>";

echo "<br><a href='gen\_pdf.php'> Сохранить PDF </a><br>";

echo "<a href='gen\_xls.php'> Сохранить Excel </a><br>";

$\_SESSION["count"]++;

echo "<br>Подключений за сессию: " . $\_SESSION["count"];

echo "<br><a href='exit.php'>Выход</a><br>";

echo "<br><a href='..'>Назад</a><br>";

echo "</body></html>";

}?>

4) Создадим файл exit.php для удаления данных сессии.

<?php

session\_start();

session\_destroy();

header("Location: .");

?>

5) Добавим вывод базы данных users для пользователей с правами администратора и ограничим доступ к функции удаления строк из таблицы os для пользователей операторов.

Вывод базы данных users для пользователей с правами администратора

if($\_SESSION["type"] == 2) {

echo "<h2>Пользователи:</h2>";

echo "<table border='1'>";

echo "<tr><th>Имя пользователя</th><th>Пароль</th><th>Права доступа</th>";

echo "<th>Редактировать</th><th>Уничтожить</th></tr>";

$query=mysql\_query("SELECT \* FROM users");

while($fetch=mysql\_fetch\_array($query)) {

echo "<tr><td>" . $fetch["username"] . "</td>";

echo "<td>" . $fetch["password"] . "</td>";

echo "<td>" . $fetch["rule"] . "</td>";

echo "<td><a href='edit\_users.php?name=" . $fetch["name"] . "'>Редактировать</a></td>";

echo "<td><a href='delete.php?name=" . $fetch["name"]. "'>Удалить</a></td></tr>";

}

echo "</table><br>";

Добавим ограничение к функциям удаления строк из таблиц fridge, service и request для пользователей операторов:

if($\_SESSION["rule"] == 2) echo "<td><a href='delete.php?name=" . $fetch["name"]. "'>Удалить</a></td>";

if($\_SESSION["rule"] == 2) echo "<td><a href='delete\_ds.php?id=" . $fetch["id"]. "'>Удалить</a></td>";

if($\_SESSION["rule"] == 2) echo "<td><a href='delete\_dk.php?id=" . $fetch["id"]. "'>Удалить</a></td>";

Итоговый код скрипта index.php:

<?php header('Content-Type: text/html; charset=windows-1251'); ?>

<html>

<body>

<?php

session\_start();

$conn = mysqli\_connect("eu-cdbr-west-02.cleardb.net","b374ee7921ac55","547aa47c", "heroku\_1ad19f5ab79e862") or die ("Невозможно подключиться к серверу");

mysqli\_query($conn, "SET NAMES cp1251");

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

$query=mysqli\_query($conn, "SELECT \* FROM users WHERE username='".$\_POST["username"]."' AND password='".md5($\_POST["password"])."'");

if($fetch = mysqli\_fetch\_array($query)) {

$\_SESSION["username"] = $fetch["username"];

$\_SESSION["rule"] = $fetch["rule"];

$\_SESSION["count"] = 0;

}

else {

echo "<html><head><title>Авторизация</title></head><body>";

echo "Неверное имя пользователя или пароль!<br>";

echo "<br><a href='.'> Вернуться </a>";

}

}

elseif(!$\_SESSION["username"]) {

echo "<html><head><title>Авторизация</title></head><body>";

echo "<h1>Газин Д. Р.</h1>";

echo "<form method='post' action='". $PHP\_SELF ."'>";

echo "<p>Пользователь:</p><input type='text' name='username' size='16'>";

echo "<p>Пароль:</p><input type='password' name='password' size='16'><br><br>";

echo "<input type='submit' name='submit' value='Войти'></form>";

echo "<br><a href='..'>Назад</a><br>";

}

if($\_SESSION["username"]) {

$query=mysqli\_query($conn, "SELECT rule FROM users WHERE username='" . $\_SESSION["username"] . "'");

if($fetch = mysqli\_fetch\_array($query)) $\_SESSION["rule"] = $fetch["rule"];

echo "<html><head><title>База данных</title></head><body>";

echo "<h2>Холодильники:</h2>";

echo "<table border='1'>";

echo "<tr><th> id </th>";

echo "<th> Марка </th> <th> Модель </th>";

echo "<th> Тип разморозки </th> <th> Внутренний объем, л. </th> <th> Срок гарантии, г. </th>";

echo "<th> Редактировать </th>";

if($\_SESSION["rule"] == 2) echo "<th>Уничтожить</th>";

echo "</tr>";

$result=mysqli\_query($conn, "SELECT \* FROM fridge");

while ($row=mysqli\_fetch\_array($result)){

echo "<tr>";

echo "<td>" . $row["id"] . "</td>";

echo "<td>" . $row["name"] . "</td>";

echo "<td>" . $row["model"] . "</td>";

echo "<td>" . $row["type"] . "</td>";

echo "<td>" . $row["volume"] . "</td>";

echo "<td>" . $row["time"] . "</td>";

echo "<td><a href='edit\_fridge.php?id=" . $row["id"]

. "'>Редактировать</a></td>";

if($\_SESSION["rule"] == 2) echo "<td><a href='delete\_fridge.php?id=" . $row["id"]

. "'>Удалить</a></td>";

echo "</tr>";

}

echo "</table>";

$num\_rows = mysqli\_num\_rows($result);

echo "<p> Всего записей: $num\_rows </p>";

echo "<a href='new\_fridge.php'> Добавить запись </a><br><br>";

echo "<h2>Сервисные центры:</h2>";

echo "<table border='1'>";

echo "<tr><th> id </th>";

echo "<th> Название </th> <th> Адрес </th>";

echo "<th> Редактировать </th>";

if($\_SESSION["rule"] == 2) echo "<th> Уничтожить </th></tr>";

$result=mysqli\_query($conn, "SELECT \* FROM service");

while ($row=mysqli\_fetch\_array($result)){

echo "<tr>";

echo "<td>" . $row["id"] . "</td>";

echo "<td>" . $row["name"] . "</td>";

echo "<td>" . $row["address"] . "</td>";

echo "<td><a href='edit\_service.php?id=" . $row["id"]

. "'>Редактировать</a></td>";

if($\_SESSION["rule"] == 2) echo "<td><a href='delete\_service.php?id=" . $row["id"]

. "'>Удалить</a></td>";

echo "</tr>";

}

echo "</table>";

$num\_rows = mysqli\_num\_rows($result);

echo "<p> Всего записей: $num\_rows </p>";

echo "<a href='new\_service.php'> Добавить запись </a><br><br>";

echo "<h2>Заявки на ремонт:</h2>";

echo "<table border='1'>";

echo "<tr><th> id </th>";

echo "<th> Дата начала </th> <th> Дата окончания </th>";

echo "<th> id Холодильника </th> <th> id Сервисного центра </th>";

echo "<th> ФИО </th> <th> Стоимость, руб. </th>";

echo "<th> Редактировать </th>";

if($\_SESSION["rule"] == 2) echo "<th> Уничтожить </th> </tr>";

$result=mysqli\_query($conn, "SELECT \* FROM request");

while ($row=mysqli\_fetch\_array($result)){

echo "<tr>";

echo "<td>" . $row["id"] . "</td>";

echo "<td>" . $row["date\_in"] . "</td>";

echo "<td>" . $row["date\_out"] . "</td>";

echo "<td>" . $row["id\_fridge"] . "</td>";

echo "<td>" . $row["id\_service"] . "</td>";

echo "<td>" . $row["fio"] . "</td>";

echo "<td>" . $row["price"] . "</td>";

echo "<td><a href='edit\_request.php?id=" . $row["id"]

. "'>Редактировать</a></td>";

if($\_SESSION["rule"] == 2) echo "<td><a href='delete\_request.php?id=" . $row["id"]

. "'>Удалить</a></td>";

echo "</tr>";

}

echo "</table>";

$num\_rows = mysqli\_num\_rows($result);

echo "<p> Всего записей: $num\_rows </p>";

echo "<a href='new\_request.php'> Добавить запись </a><br><br>";

if($\_SESSION["rule"] == 2) {

echo "<h2>Пользователи:</h2>";

echo "<table border='1'>";

echo "<tr><th>Имя пользователя</th><th>Пароль</th><th>Права доступа</th>";

echo "<th>Редактировать</th><th>Уничтожить</th></tr>";

$query=mysqli\_query($conn, "SELECT \* FROM users");

while($fetch=mysqli\_fetch\_array($query)) {

echo "<tr><td>" . $fetch["username"] . "</td>";

echo "<td>" . $fetch["password"] . "</td>";

echo "<td>" . $fetch["rule"] . "</td>";

echo "<td><a href='edit\_users.php?username=" . $fetch["username"] . "'>Редактировать</a></td>";

echo "<td><a href='delete\_users.php?username=" . $fetch["username"]. "'>Удалить</a></td></tr>";

}

echo "</table>";

$num\_rows = mysqli\_num\_rows($query);

echo "<p> Всего записей: $num\_rows </p>";

echo "<a href='new\_users.php'>Добавить запись</a><br><br>";

}

echo "<br><a href='gen\_pdf.php'> Сохранить PDF </a><br>";

echo "<a href='gen\_xls.php'> Сохранить Excel </a><br>";

$\_SESSION["count"]++;

echo "<br>Подключений за сессию: " . $\_SESSION["count"];

echo "<br><a href='exit.php'>Выход</a><br>";

echo "<br><a href='..'>Назад</a><br>";

echo "</body></html>";

}

?>

Ниже представлены результаты работы скрипта index.php:

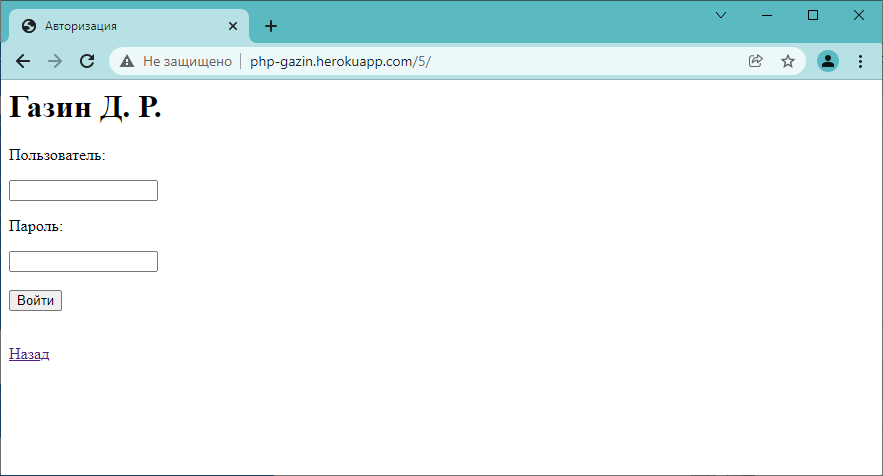


Рис. 3 – Форма авторизации

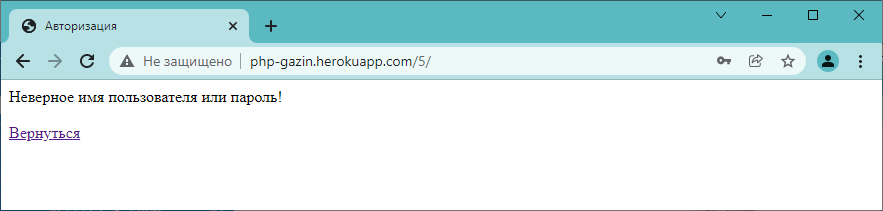


Рис. 4 – Ввод неверного имени пользователя или пароля

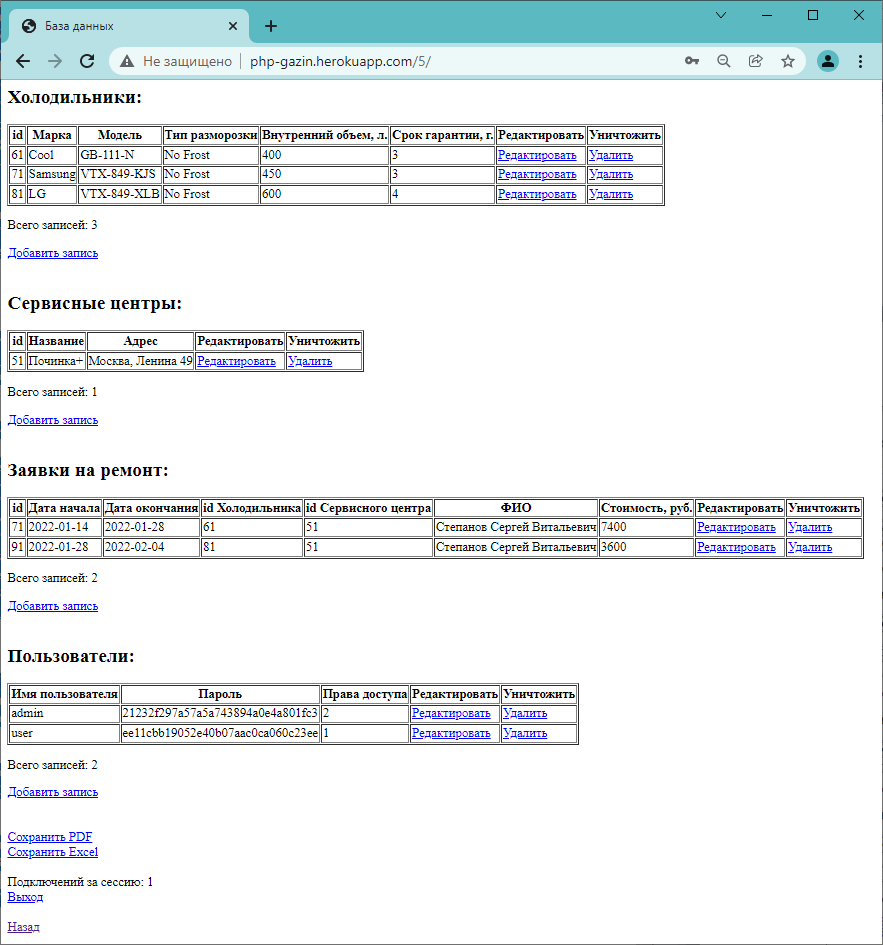
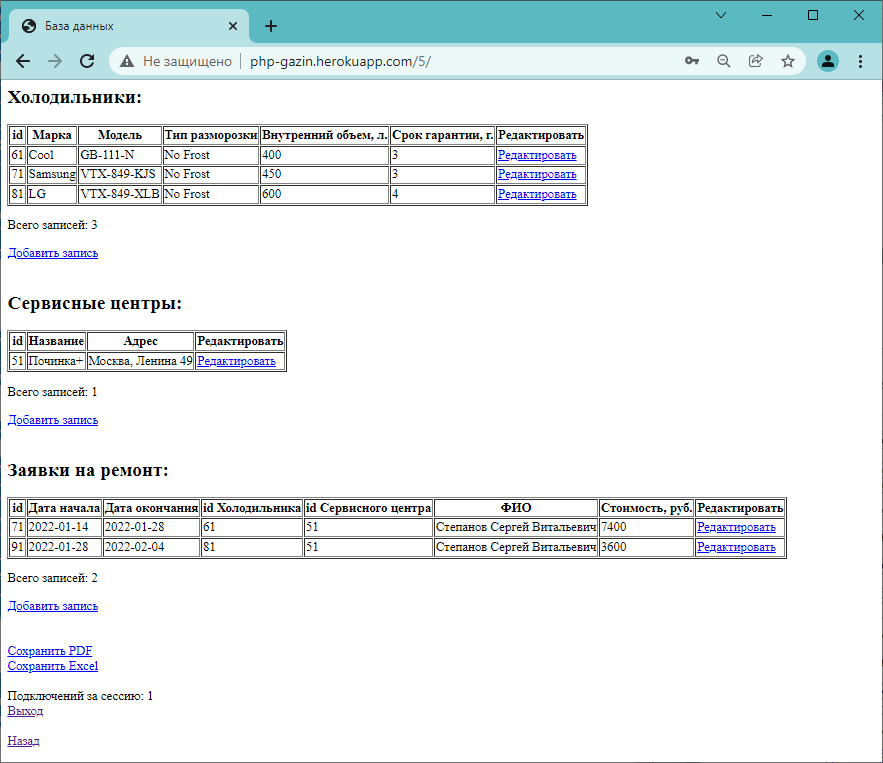


Рис. 5 – Авторизация пользователя-администратора

Рис. 6 – Авторизация пользователя оператора

При активной сессии, можно снова перейти на сайт, без прохождения авторизации.

При неактивной сессии доступ к функциям будет закрыт, и переход по скриптам по ссылку будет пересылать на страницу авторизации

При нажатии на ссылку «Выход», данные о сессии сбросятся, и при обновлении страницы снова появится форма для входа.

6) Проверки на тип пользователей и авторизацию.

Для этого каждый скрипт обернем в одну из следующих конструкций:

<?php //Для администраторов

session\_start();

if($\_SESSION["type"] == 2) { //Скрипт }

?>

<?php //Для всех пользователей

session\_start();

if($\_SESSION["type"] > 0) { //Скрипт }

?>

Теперь скрипты будут выполняться только при активной сессии и необходимых правах доступа.

7) Добавим скрипты для добавления записей в таблицу users

Скрипт формы добавления новых пользователей:

<?php header('Content-Type: text/html; charset=windows-1251'); ?>

<?php

session\_start();

if($\_SESSION["rule"] == 2) {

echo "<html><head><title>Добавление новой записи</title></head><body>";

echo "<h2>Добавление новой записи:</h2>";

echo "<form action='save\_new\_users.php' metod='get'>";

echo "<br>Имя пользователя: <input name='username' size='20' type='text'>";

echo "<br>Пароль: <input name='password' size='20' type='password'>";

echo "<br>Права доступа: <input name='rule' size='10' type='text'><br><br>";

echo "<input name='add' type='submit' value='Добавить'>";

echo "<input name='b2' type='reset' value='Очистить'></form>";

echo "<a href='index.php'>Вернуться</a></body></html>";

}

else {

header("Location: .");

}

?>

Скрипт обработки добавления новых пользователей:

<?php header('Content-Type: text/html; charset=windows-1251'); ?>

<?php

session\_start();

if($\_SESSION["rule"] == 2) {

$conn = mysqli\_connect("eu-cdbr-west-02.cleardb.net","b374ee7921ac55","547aa47c", "heroku\_1ad19f5ab79e862") or die ("Невозможно подключиться к серверу");

mysqli\_query($conn, 'SET NAMES cp1251');

$sql\_add = "INSERT INTO users SET username='" . $\_GET['username']."', password='".md5($\_GET['password'])."', rule='".$\_GET['rule']. "'";

mysqli\_query($conn, $sql\_add);

if (mysqli\_affected\_rows($conn)>0) { // если нет ошибок при выполнении запроса

echo "Запись сохранена.<br>";

echo "<a href='.'>Вернуться </a>";

}

else {

echo "Ошибка сохранения. <a href='.'>Вернуться </a>";

}

}

else {

header("Location: .");

}

?>

Добавим нового пользователя user с правами оператора (1):

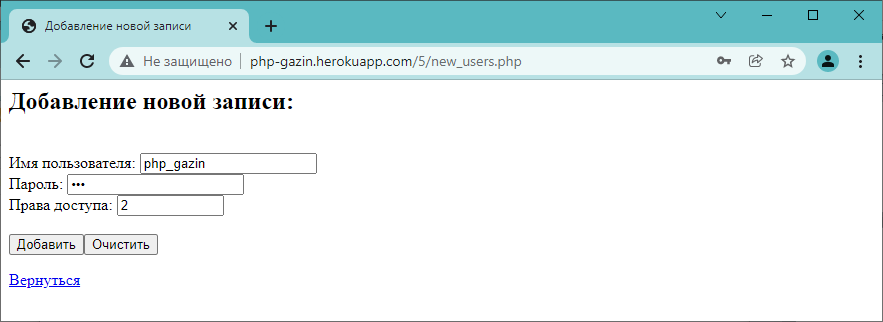


Рис. 8 – Добавление нового пользователя

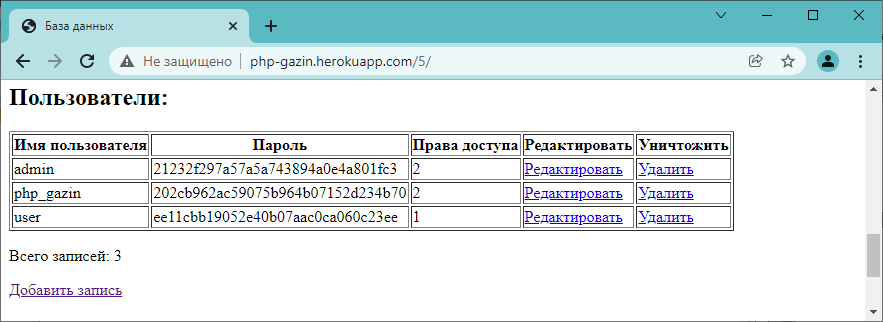


Рис. 9 – Пользователь добавлен

8) Добавим скрипты для редактирования записей таблицы users

Скрипт формы редактирования записей пользователей

<?php header('Content-Type: text/html; charset=windows-1251'); ?>

<?php

session\_start();

if($\_SESSION["rule"] == 2) {

$conn = mysqli\_connect("eu-cdbr-west-02.cleardb.net","b374ee7921ac55","547aa47c", "heroku\_1ad19f5ab79e862") or die ("Невозможно подключиться к серверу");

mysqli\_query($conn, 'SET NAMES cp1251');

$rows=mysqli\_query($conn, "SELECT username, rule FROM users WHERE username='".$\_GET['username']."'");

while ($st = mysqli\_fetch\_array($rows)) {

$username=$\_GET["username"];

$rule = $st['rule'];

}

echo "<html><head><title>Редактирование данных</title></head><body>";

echo "<form action='save\_edit\_users.php' metod='get'>";

echo "Имя пользователя: <input name='username' size='20' type='text' value='".$username."'>";

echo "<br>Пароль: <input name='password' size='20' type='password' value=''>";

echo "<br>Права доступа: <input name='rule' size='10' type='text' value='".$rule."'>";

echo "<input type='submit' name='' value='Сохранить'></form>";

echo "<p><a href='.'> Вернуться </a></body></html>";

}

else {

header("Location: .");

}

?>

Скрипт обработки редактирования записей пользователей:

<?php header('Content-Type: text/html; charset=windows-1251'); ?>

<?php

session\_start();

if($\_SESSION["rule"] != 2) header("Location: .");

?>

<html><body>

<?php

$conn = mysqli\_connect("eu-cdbr-west-02.cleardb.net","b374ee7921ac55","547aa47c", "heroku\_1ad19f5ab79e862") or die ("Невозможно подключиться к серверу");

mysqli\_query($conn, 'SET NAMES cp1251');

$zapros="UPDATE users SET username='".$\_GET['username']."', password='".md5($\_GET['password'])."', rule='".$\_GET['rule']."' WHERE username='".$\_GET['username']."'";

mysqli\_query($conn, $zapros);

if (mysqli\_affected\_rows($conn) > 0) {

echo "Все сохранено. <a href='.'> Вернуться на главную</a>";

}

else {

echo "Ошибка сохранения. <a href='.'> Вернуться на главную </a>";

}

?>

</body></html>

Отредактируем собственную запись пользователя, сделаем ее оператором

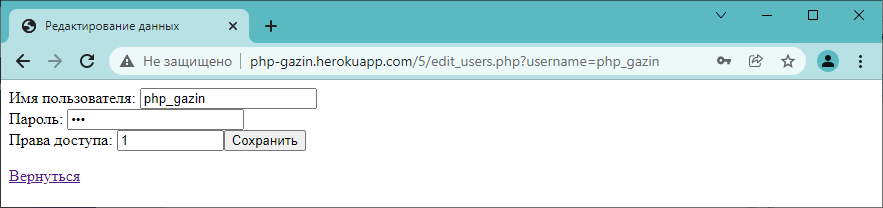


Рис. 10 – Редактирование записи пользователя

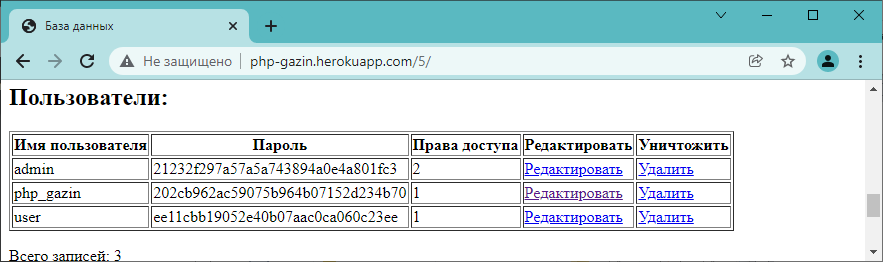


Рис. 11 – Запись пользователя отредактирована

9) Добавим скрипт для удаления записей из таблицы users

<?php

session\_start();

if($\_SESSION["rule"] == 2) {

$conn = mysqli\_connect("eu-cdbr-west-02.cleardb.net","b374ee7921ac55","547aa47c", "heroku\_1ad19f5ab79e862") or die ("Невозможно подключиться к серверу");

$zapros="DELETE FROM users WHERE username='" . $\_GET['username']."'";

mysqli\_query($conn, $zapros);

if($\_GET['username'] == $\_SESSION['username']) session\_destroy();

}

header("Location: .");

?>

Удалим собственную учетную запись:

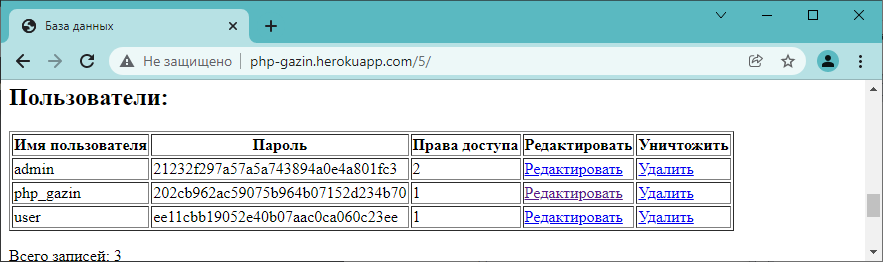


Рис. 12 – Таблица перед удалением записи

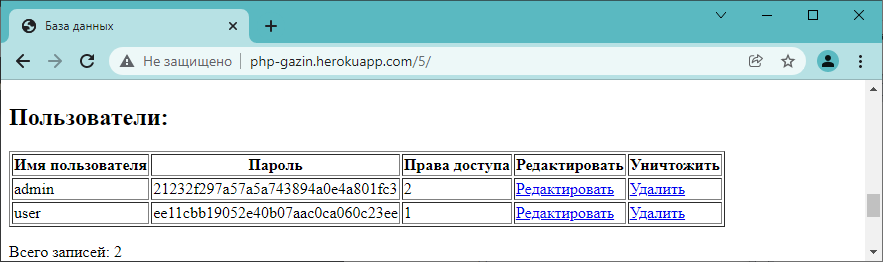


Рис. 13 – Таблица после удаления записи