Созд6 Министерство науки и высшего образования Российской федерации

Федерального государственного бюджетного образовательного учреждения высшего образования

Московский государственный технический университет имени Н. Э. Баумана

(Национальный исследовательский университет)

Московский техникум космического приборостроения

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №10**

по теме: «Использование PHP MySQL»

Специальность: 09.02.07 Информационные системы и программирование – квалификация «Программист»

Группа ТИП-51

|  |  |
| --- | --- |
| Проверил  Разработал | Осипова Н. М.  Симонян П. Р. |

Москва 2021

СОДЕРЖАНИЕ

[1. Создание базы данных 3](#_Toc11942)

[2. Создание панели админа 4](#_Toc16081)

[3. Авторизация и безопасность 11](#_Toc14629)

# Создание базы данных

В соответствии с тематикой сайта была создана новая база данных.

Она представляет из себя базу данных типичного форума и содержит: пользователей (ID, логин, хэш-код пароля, привилегии, статус), посты (ID, заголовок, категория, автор, содержание), категории постов (название, путь к иконке на сервере).

Код создания:

create database AnForum;

use anforum;

create table Usr(

id int auto\_increment,

username varchar(200) not null,

passhash varchar(512) not null,

rights varchar(10) not null default '100100100',

#Слева направо:

#0 символ- Просмотр пользователей

#1-Редактирование пользователей

#2-Удаление пользователей

#3-Просмотр категорий

#4-Редактирование категорий

#5-Удаление категорий

#6-Создание постов (просматривать посты могут все пользователи)

#7-Редактирование постов

#8-Удаление постов

descr varchar(200),

primary key (id)

);

alter table usr add unique (username);

create table Category(

c\_name varchar(60) not null,

iconPath varchar(150) not null,

primary key (c\_name)

);

create table Post(

id int auto\_increment,

author int not null,

category varchar(50),

title varchar(200) not null,

content text,

primary key(id),

foreign key (author) references Usr(id),

foreign key (category) references Category(c\_name)

);

insert into usr(username, passhash, rights, descr)

values('psrar', '25d55ad283aa400af464c76d713c07ad', '101111111', 'Я ваш отец'),

('sashkaool', '5e8667a439c68f5145dd2fcbecf02209', '100100100', 'Ненавижу феминитивы');

# Создание панели админа

Было решено реализовать множество функций работы с базой данных сайта. Панель администратора сайта выглядит так:

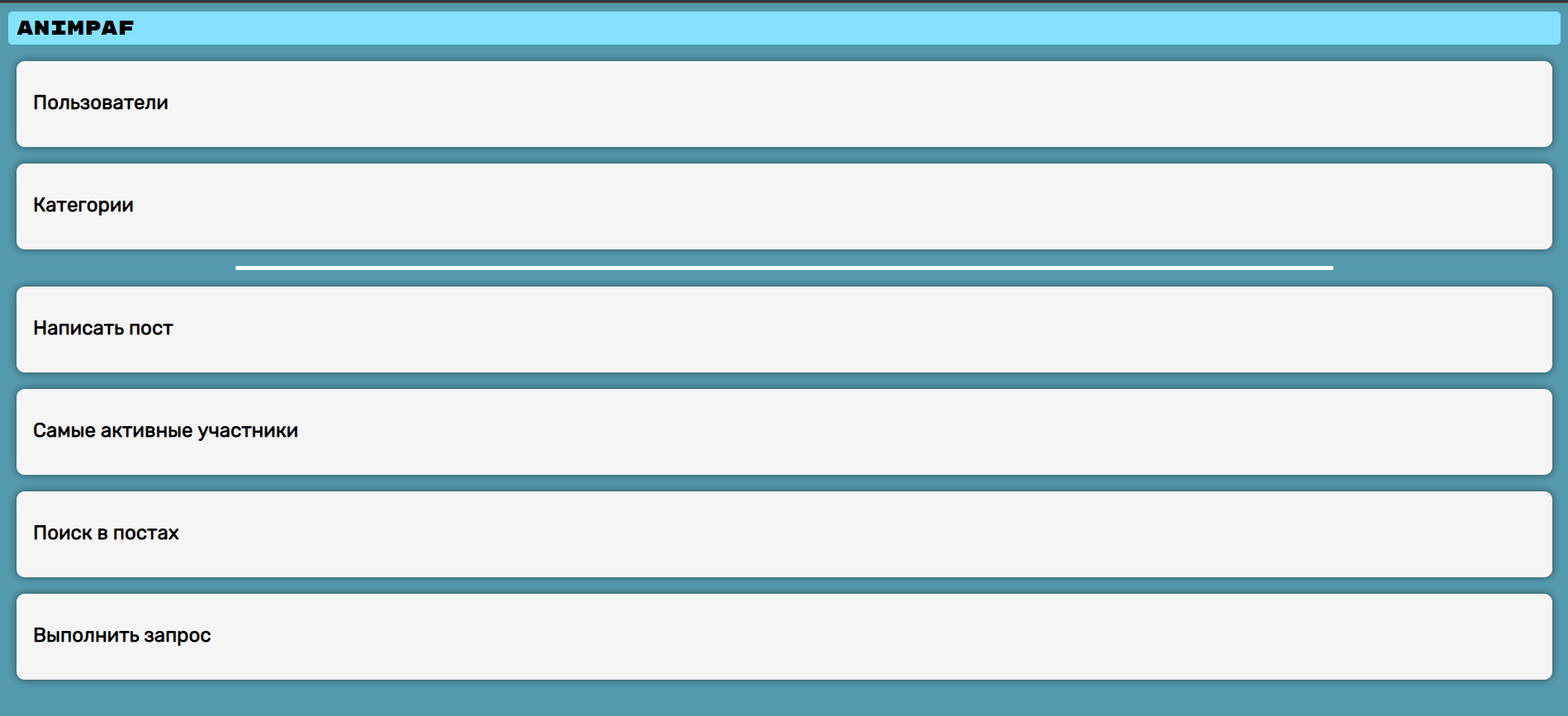


Рисунок 2.1 - Панель администратора

Она содержит различные настроенные команды для отображения данных сайта.

Первые два пункта отображают пользователей и категории, сохраненные в базе данных.

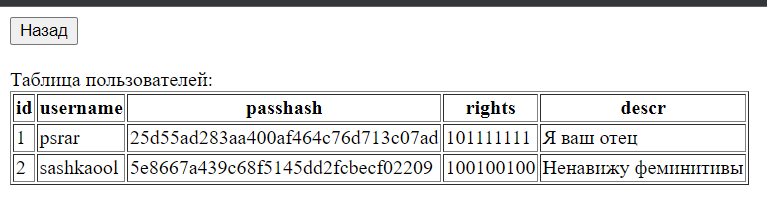


Рисунок 2.2 - Меню пользователей



Рисунок 2.3 - Меню категорий

Код отображения таблиц практически идентичен. Указывается лишь описание на русском и название таблицы в базе данных. Поэтому ниже приведен листинг только файла users.php, отображающий на странице всех пользователей.

Листинг 2.1 файла users.php:

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta http-equiv="X-UA-Compatible" content="IE=edge">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

</head>

<body>

    <button onclick="location.href='/dbwork/adminpanel.html'">Назад

    </button><br><br>

<?php

$mysqlcon = mysqli\_connect('localhost', 'root', '2030203pa', 'anforum', $port = 3306);

$table = 'usr';

echo 'Таблица пользователей:<br>';

echo '<table border=\'1px\'>';

$query = 'SELECT \* from ' . $table;

$res = mysqli\_query($mysqlcon, $query);

$colNames = mysqli\_fetch\_fields($res);

foreach ($colNames as $var) {

    echo '<th>' . $var->name . '</th>';

}

$data = mysqli\_fetch\_all($res);

$length = count($colNames);

$rowCount = mysqli\_num\_rows($res);

for ($r = 0; $r < $rowCount; $r++) {

    echo '<tr>';

    for ($i = 0; $i < $length; $i++) {

        echo

        '<td>' . $data[$r][$i] . '</td>';

    };

    echo '</tr>';

}

echo '</table><br>';

echo

'</body>

</html>';

?>

Ниже на панели администратора присутствуют другие функции и выборки. Первая из них - «Написать пост».

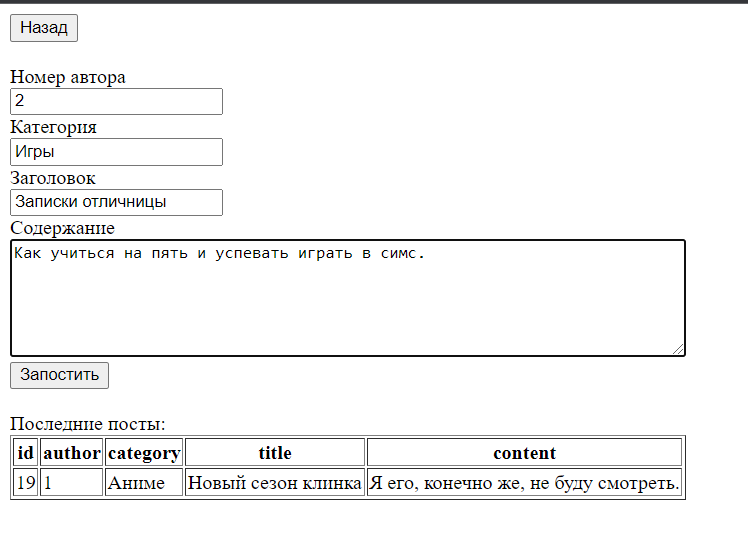


Рисунок 2.4 - Форма публикации поста

На данной странице совершается публикация постов и просмотр последних из них. Все взаимодействие с постами осуществляется через базу данных. Листинг страницы представлен ниже.

Листинг 2.2 файла posting.php:

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta http-equiv="X-UA-Compatible" content="IE=edge">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

</head>

<body>

    <button onclick="location.href='/dbwork/adminpanel.html'">Назад

    </button><br><br>

    <form action="" , method="POST">

        Номер автора <br><input type="number" name="authorid" value="1" required></input><br>

        Категория <br><input type="text" name="category" required></input><br>

        Заголовок <br><input type="text" name="title" required></input><br>

        Содержание <br><textarea name="content" cols="80" rows="10" required></textarea></input><br>

        <input type="submit" name="submit" value="Запостить"></input>

    </form><br>

    <?php

    $mysqlcon = mysqli\_connect('localhost', 'root', '2030203pa', 'anforum', $port = 3306);

    if ($\_POST['title'] != '' and $\_POST['content'] != '' and $\_POST['category'] != '') {

        try {

            mysqli\_query($mysqlcon, 'insert into post(author, category, title, content) values(\'' .

                $\_POST['authorid'] . '\',\'' . $\_POST['category'] . '\',\'' . $\_POST['title'] . '\',\'' . $\_POST['content'] .

                '\');');

            echo 'Запись опубликована<br><br>';

        } catch (\*Throwable* $th) {

            echo $th . '<br><br>';

        }

    }

    $table = 'post';

    echo 'Последние посты:<br>';

    echo '<table border=\'1px\'>';

    $query = 'SELECT \* from ' . $table . ' order by id desc limit 100;';

    $res = mysqli\_query($mysqlcon, $query);

    $colNames = mysqli\_fetch\_fields(mysqli\_query($mysqlcon, $query));

    foreach ($colNames as $var) {

        echo '<th>' . $var->name . '</th>';

    }

    $data = mysqli\_fetch\_all($res);

    $length = count($colNames);

    $rowCount = mysqli\_num\_rows($res);

    for ($r = 0; $r < $rowCount; $r++) {

        echo '<tr>';

        for ($i = 0; $i < $length; $i++) {

            echo

            '<td>' . $data[$r][$i] . '</td>';

        };

        echo '</tr>';

    }

    echo '</table><br>';

    echo

    '</body>

</html>';

    ?>

В случае некорректного ввода администратору выводится ошибка:

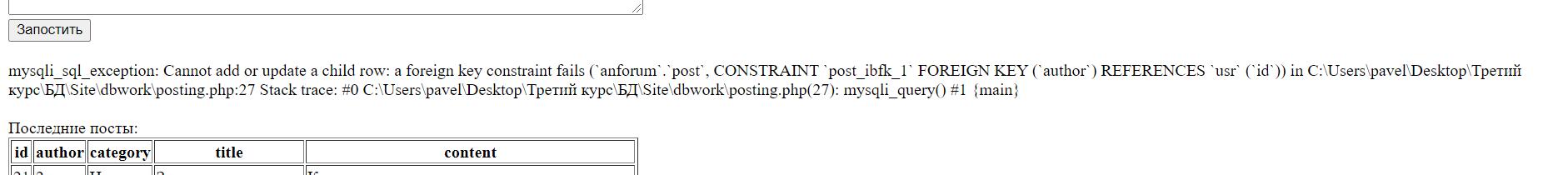
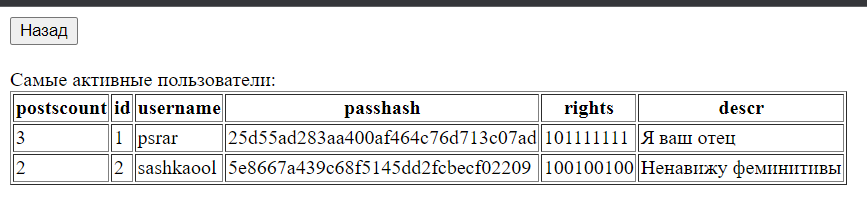


Рисунок 2.5 - Вывод ошибки при некорректном вводе

Еще одной полезной функцией является вывод участников, написавших наибольшее количество постов.

Рисунок 2.6 - Таблица самых активных участников

Вывод данных для всех запросов идентичен, поэтому предлагаю сразу обратить внимание на запрос, помеченный в листинге 2.3 красным цветом.

Листинг 2.3 файла activitystats.php, отображающего список самых активных участников:

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta http-equiv="X-UA-Compatible" content="IE=edge">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

</head>

<body>

    <button onclick="location.href='/dbwork/adminpanel.html'">Назад

    </button><br><br>

    <?php

    $mysqlcon = mysqli\_connect('localhost', 'root', '2030203pa', 'anforum', $port = 3306);

    echo 'Самые активные пользователи:<br>';

    echo '<table border=\'1px\'>';

    $query = 'select count(post.id) as postscount, usr.\*

    from usr join post on usr.id = post.author group by usr.id order by postscount desc;';

    $res = mysqli\_query($mysqlcon, $query);

    $colNames = mysqli\_fetch\_fields($res);

    foreach ($colNames as $var) {

        echo '<th>' . $var->name . '</th>';

    }

    $data = mysqli\_fetch\_all($res);

    $length = count($colNames);

    $rowCount = mysqli\_num\_rows($res);

    for ($r = 0; $r < $rowCount; $r++) {

        echo '<tr>';

        for ($i = 0; $i < $length; $i++) {

            echo

            '<td>' . $data[$r][$i] . '</td>';

        };

        echo '</tr>';

    }

    echo '</table><br>';

    echo

    '</body>

</html>';

?>

Еще одной интересной функцией является поиск среди записей, показанный на изображении ниже.

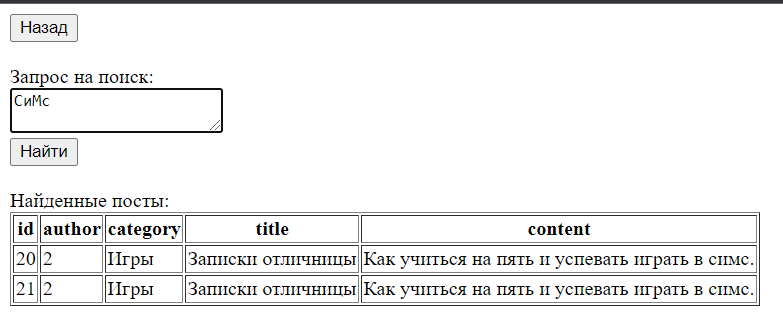


Рисунок 2.7 - Результат поиска

Запрос включает поиск как по содержимому, так и по названию публикаций. Листинг страницы представлен ниже.

Листинг 2.4 файла postsfind.php:

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta http-equiv="X-UA-Compatible" content="IE=edge">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

</head>

<body>

    <button onclick="location.href='/dbwork/adminpanel.html'">Назад

    </button><br><br>

    <form action="" , method="POST">

        Запрос на поиск: <br><textarea name="content" cols="20" rows="2" required></textarea></input><br>

        <input type="submit" name="submit" value="Найти"></input>

    </form><br>

    <?php

    $mysqlcon = mysqli\_connect('localhost', 'root', '2030203pa', 'anforum', $port = 3306);

    if ($\_POST['content'] != '') {

        try {

            $query = "select \* from post where lower(content) like lower('%" . $\_POST['content'] . "%')

        or lower(title) like lower('%" . $\_POST['content'] . "%');";

            $res = mysqli\_query($mysqlcon, $query);

            echo 'Найденные посты:<br>';

            echo '<table border=\'1px\'>';

            $colNames = mysqli\_fetch\_fields($res);

            foreach ($colNames as $var) {

                echo '<th>' . $var->name . '</th>';

            }

            $data = mysqli\_fetch\_all($res);

            $length = count($colNames);

            $rowCount = mysqli\_num\_rows($res);

            for ($r = 0; $r < $rowCount; $r++) {

                echo '<tr>';

                for ($i = 0; $i < $length; $i++) {

                    echo

                    '<td>' . $data[$r][$i] . '</td>';

                };

                echo '</tr>';

            }

            echo '</table><br>';

        } catch (\*Throwable* $th) {

            echo $th . '<br><br>';

        }

    }

    echo

    '</body>

</html>';

    ?>

Самым продвинутым инструментом является вкладка «Выполнить запрос».

Она позволяет выполнять собственные команды SQL.

Пример:

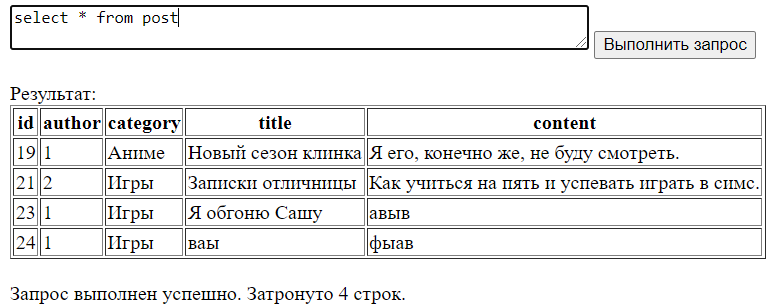


Рисунок 2.8 - Исходная таблица публикаций

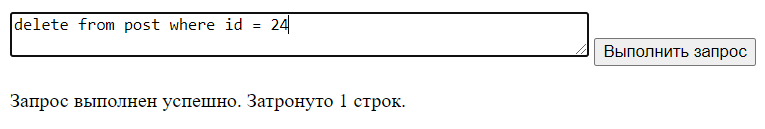


Рисунок 2.9 - Процесс выполнения запроса на удаление

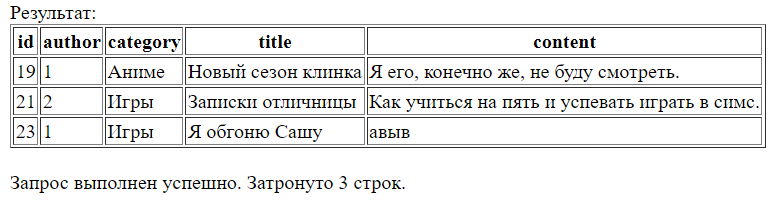


Рисунок 2.10 - Итоговая таблица публикаций

Листинг 2.5 страницы custom.php для выполнения собственных запросов:

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta http-equiv="X-UA-Compatible" content="IE=edge">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

</head>

<body>

    <button onclick="location.href='/dbwork/adminpanel.html'">Назад

    </button><br><br>

    <form action="" , method="POST">

        <textarea type="text" name="query" cols="60"></textarea>

        <input type="submit" name="submit" value="Выполнить запрос"></input>

    </form><br>

</body>

</html>

<?php

$mysqlcon = mysqli\_connect('localhost', 'root', '2030203pa', 'anforum', $port = 3306);

if ($\_POST['query'] != '') {

    try {

        $res = mysqli\_query($mysqlcon, $\_POST['query']);

        if (!is\_bool($res)) {

            echo 'Результат:<br>';

            echo '<table border=\'1px\'>';

            $colNames = mysqli\_fetch\_fields($res);

            foreach ($colNames as $var) {

                echo '<th>' . $var->name . '</th>';

            }

            $data = mysqli\_fetch\_all($res);

            $length = count($colNames);

            $rowCount = mysqli\_num\_rows($res);

            for ($r = 0; $r < $rowCount; $r++) {

                echo '<tr>';

                for ($i = 0; $i < $length; $i++) {

                    echo

                    '<td>' . $data[$r][$i] . '</td>';

                };

                echo '</tr>';

            }

            echo '</table><br>';

            echo 'Запрос выполнен успешно. Затронуто '. mysqli\_affected\_rows($mysqlcon).' строк.';

        } else if ($res == false)

            echo 'Запрос не выполнен.';

        else echo 'Запрос выполнен успешно. Затронуто '. mysqli\_affected\_rows($mysqlcon).' строк.';

    } catch (\*Throwable* $th) {

        echo $th . '<br><br>';

    }

}

?>

# Авторизация и безопасность

Вход в панель админа происходит на специальной странице. Ее внешний вид и код представлены ниже.

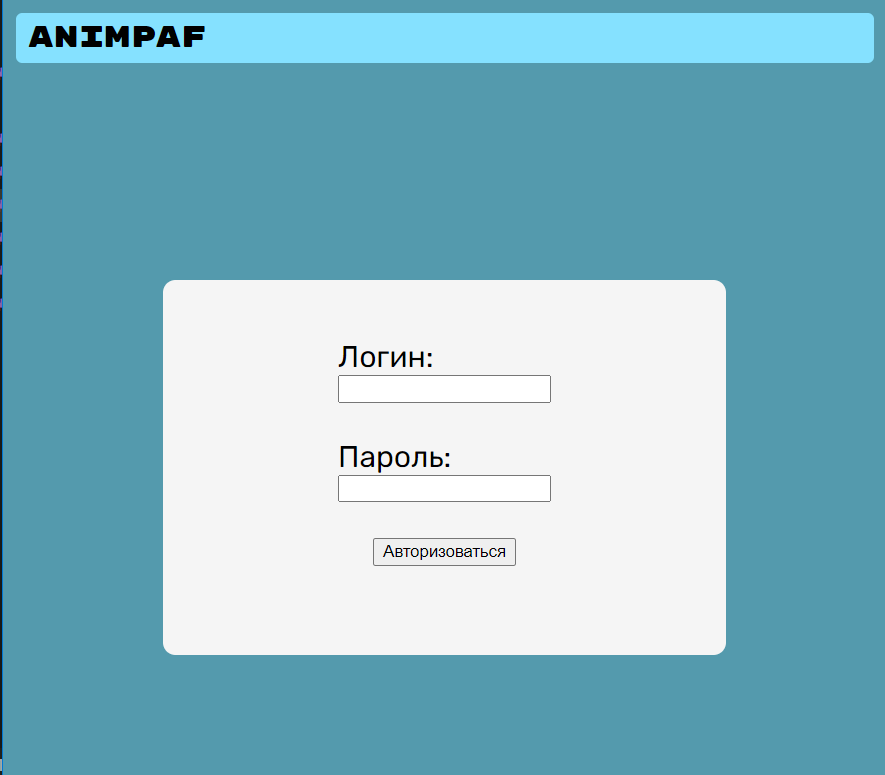


Рисунок 3.1 - Окно входа

Листинг 3.1 страницы login.php:

<?php

*function* alert($message)

{

    echo "<script>alert('$message');</script>";

}

if ($\_POST['Username'] != '' and $\_POST['Password'] != '') {

    $login = $\_POST['Username'];

    $password = $\_POST['Password'];

    if (preg\_match('/[();\*-]/', $login) or preg\_match('/[();\*-]/', $password))

        alert('Прекратите взламывать!');

    else {

        $mysqlcon = mysqli\_connect('localhost', 'root', '2030203pa', 'anforum', $port = 3306);

        $query = "SELECT passhash from usr where username = '" . $\_POST['Username'] . "';";

        $res = mysqli\_query($mysqlcon, $query);

        if (mysqli\_affected\_rows($mysqlcon) != 0) {

            $data = mysqli\_fetch\_assoc($res);

            if ($data['passhash'] == md5($\_POST['Password']))

                echo "<script>location.href='./adminpanel.html'</script>";

            else alert('Неправильный пароль.');

        } else alert('Такого пользователя не существует.');

    }

};

?>

<html lang="ru">

<head>

    <meta charset="UTF-8">

    <meta http-equiv="X-UA-Compatible" content="IE=edge">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

    <title>Animpaf Studio</title>

    <link rel="stylesheet" href="/style.css">

</head>

<body>

    <div class="header">

        <a class="header\_ref" href="/index.html ">Animpaf</a>

    </div>

    <div class="logincanvas">

        <div class="login">

            <form action="" method="POST">

                Логин: <br><input type="text" name="Username" required>

                <br><br> Пароль:<br><input type="password" name="Password" required><br><br>

                <div style="display: flex; justify-content: center;">

                    <input type="submit" name="submit" value="Авторизоваться">

                </div>

            </form>

        </div>

    </div>

</body>

<style>

    body {

*font-family*: RubikReg;

*font-size*: x-large;

    }

    .logincanvas {

*width*: 100%;

*height*: 90%;

*display*: flex;

*justify-content*: center;

*align-items*: center;

    }

    .login {

*margin*: auto;

*display*: flex;

*justify-content*: center;

*align-items*: center;

*width*: 450px;

*height*: 300px;

*background-color*: whitesmoke;

*border-radius*: 10px;

    }

</style>

</html>

Как видно в коде, авторизация происходит с помощью таблицы базы данных под названием usr (пользователи), а не логинов MySQL.

Присутствует базовая проверка на SQL - инъекции. В кода она помечена красным цветом.

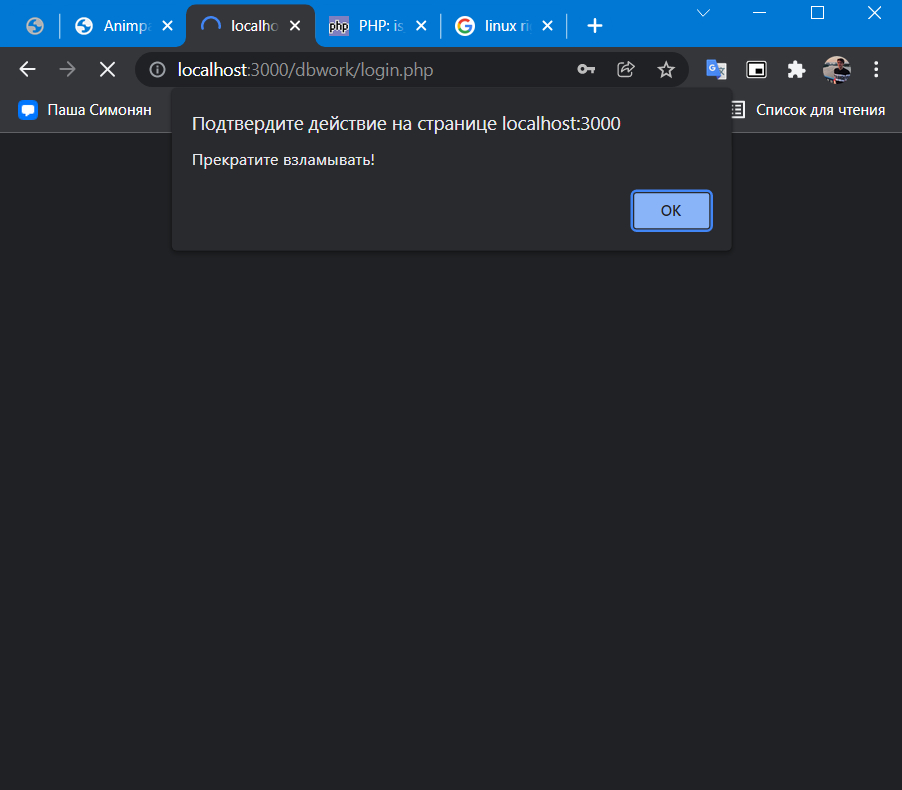


Рисунок 3.2 - Пример работы защиты от SQL инъекций

В примере выше в поле было введено “psrar”, а в поле пароля - “(--”.

Пароль хэшируется и передается методом POST, что затрудняет его отслеживание. На данном этапе подразумевается, что все пользователи базы данных - администраторы, но поле rights таблицы usr позволяет легче разграничивать права пользователей (следуя примеру обозначения прав на файлы в Linux, имеющего вид “- rwx rwx rwx”, где каждый символ определяет аспект привилегий).

Вывод: в данной работе продемонстрирована работа с СУБД MySQL с помощью PHP библиотеки mysqli. Были применены некоторые запросы на выборку, предоставлена возможность выполнения запросов на добавление, удаление и изменение данных на сайте.