

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ  
КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»  
(СПбГУТ)

---

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

**Лабораторная работа №1**

Выполнили студенты группы ИКТЗ-83:

Громов А.А., Миколаени М.С., Мазеин Д.С.

(Ф.И.О., № группы)

\_\_\_\_\_  
(подпись)

Проверил:

Казанцев А.А.

(уч. степень, уч. звание, Ф.И.О.)

\_\_\_\_\_  
(подпись)

Санкт-Петербург

2021

## Пункт 1

### Установка и запуск ХАМРР.

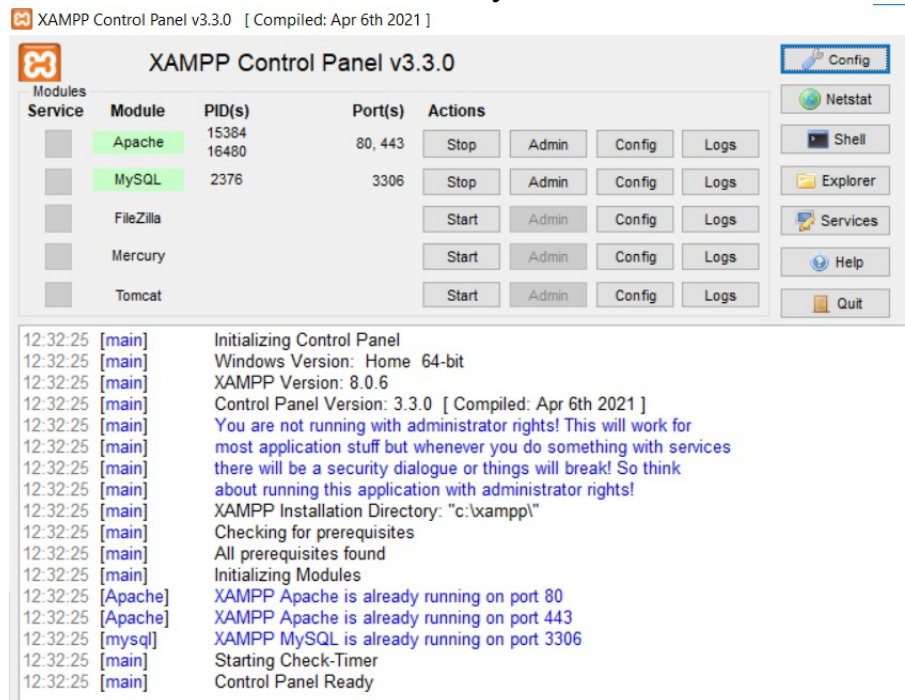


Рис. 1 Панель ХАМРР.

## Пункт 2

### Проверка работоспособности страницы регистрации, авторизации и профиля.

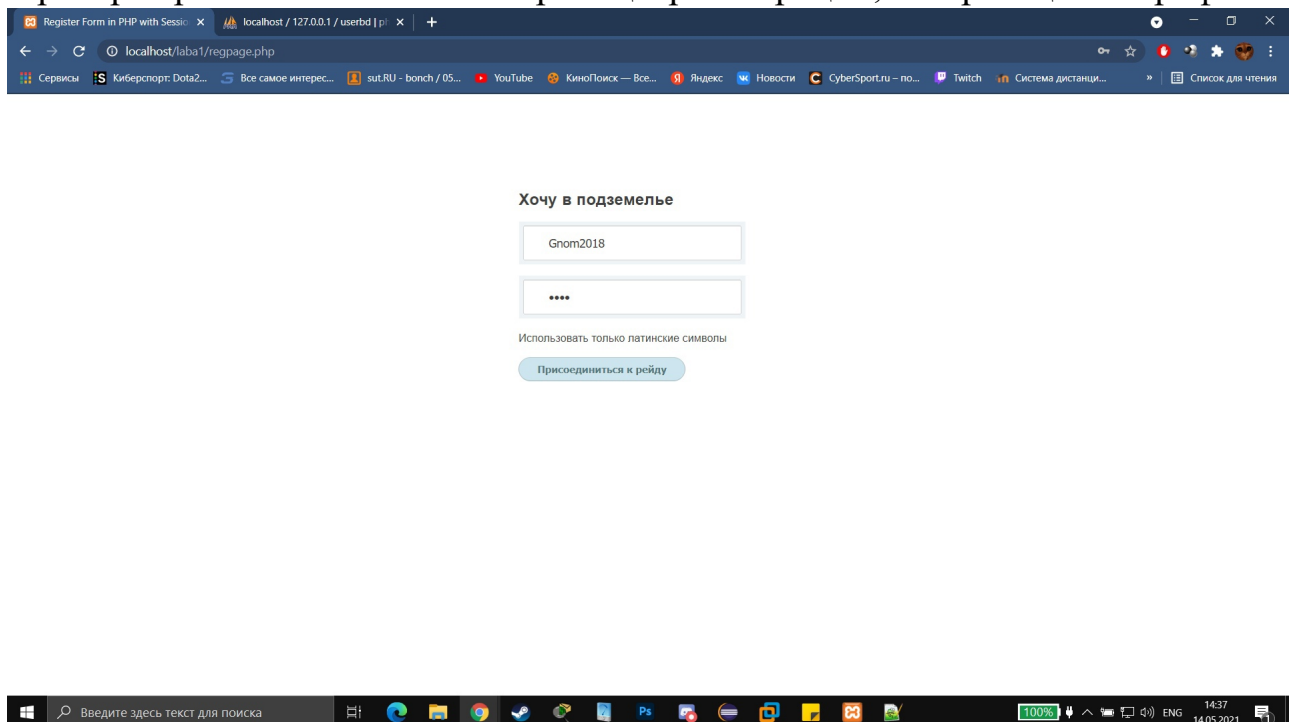


Рис. 2 Страница регистрации.

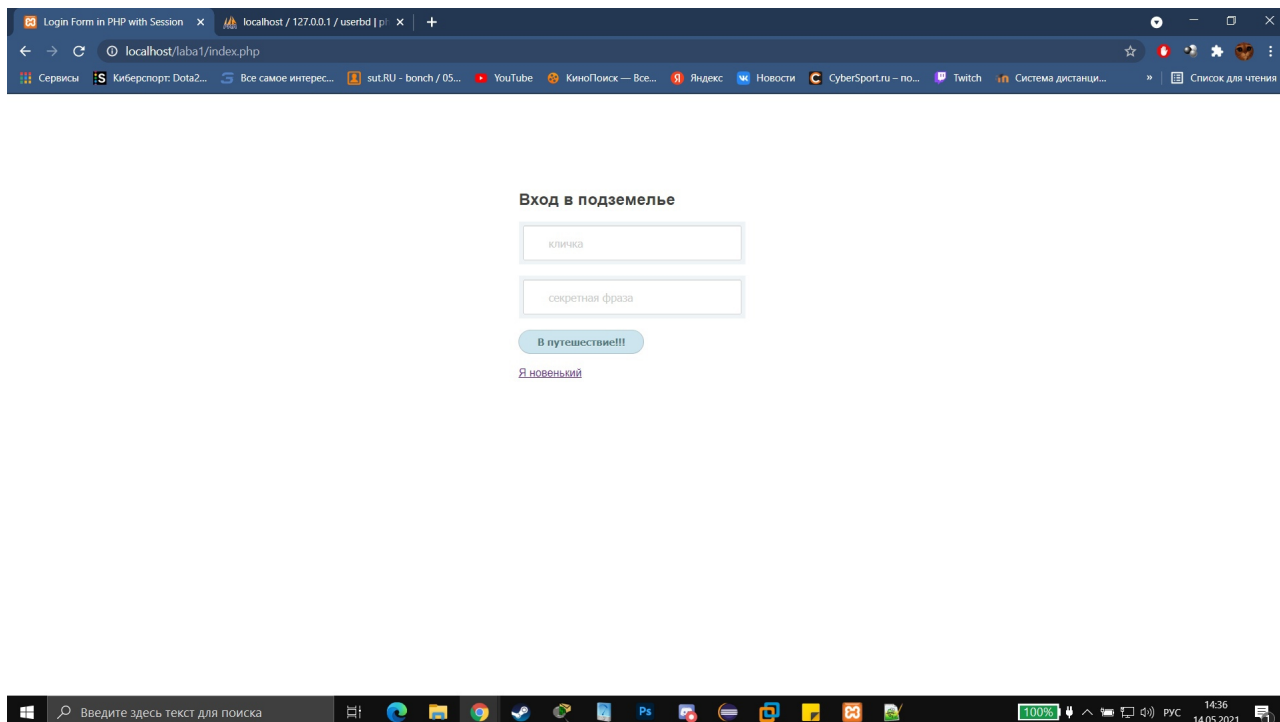


Рис. 3 Страница авторизации.

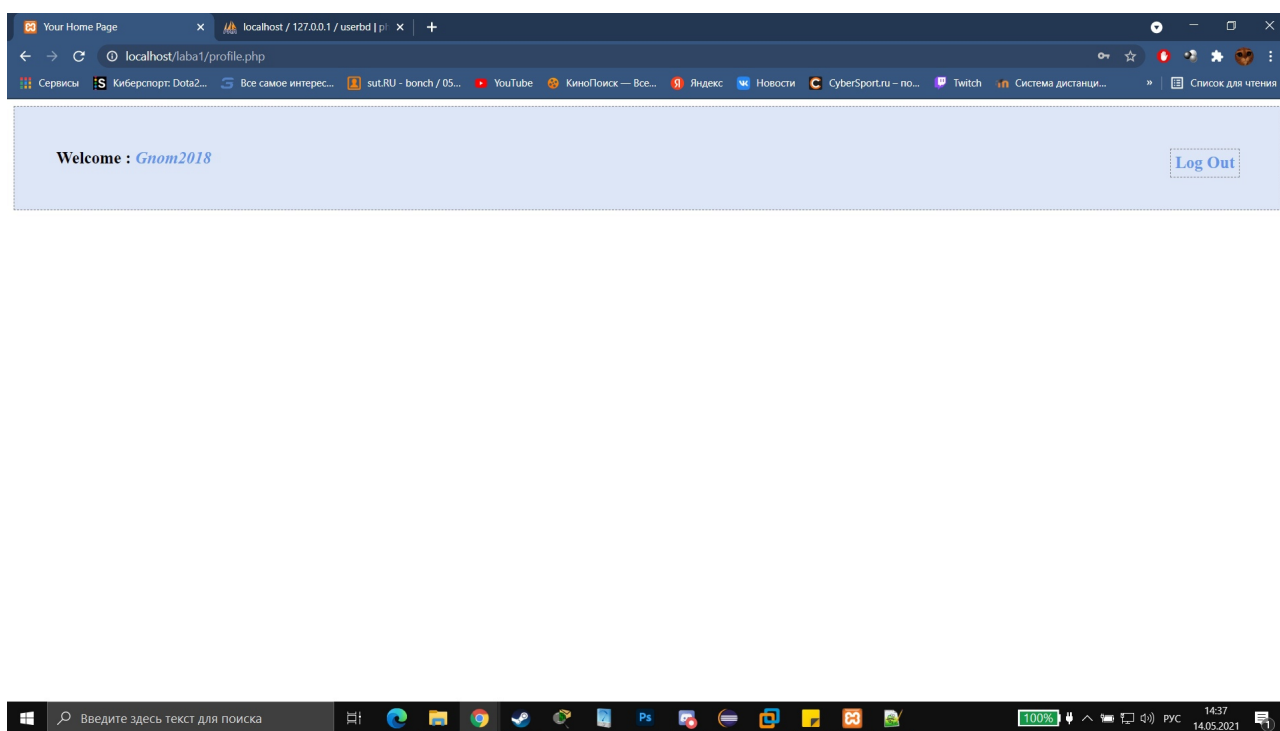


Рис. 4 Страница профиля.

### Пункт 3

Производим SQL-инъекцию(в пароле вводим 'OR1='1).

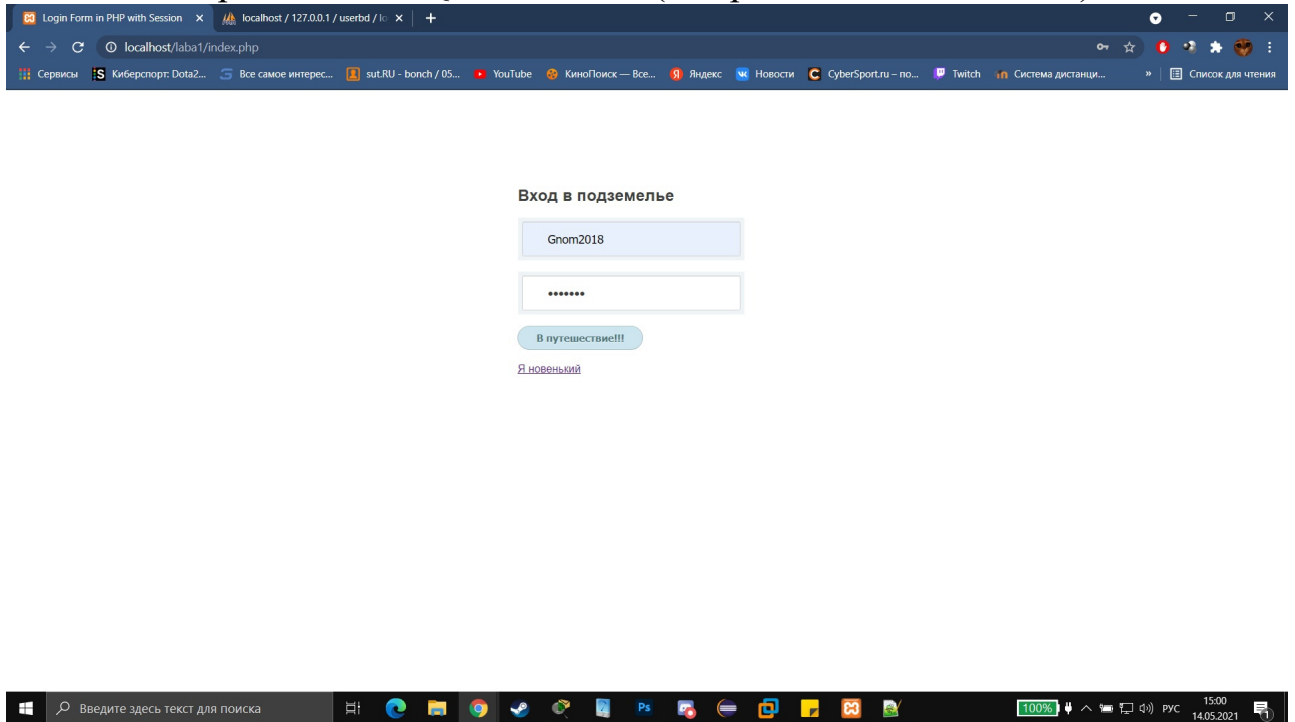


Рис. 5 Ввели в поле пароль - 'OR1='1.

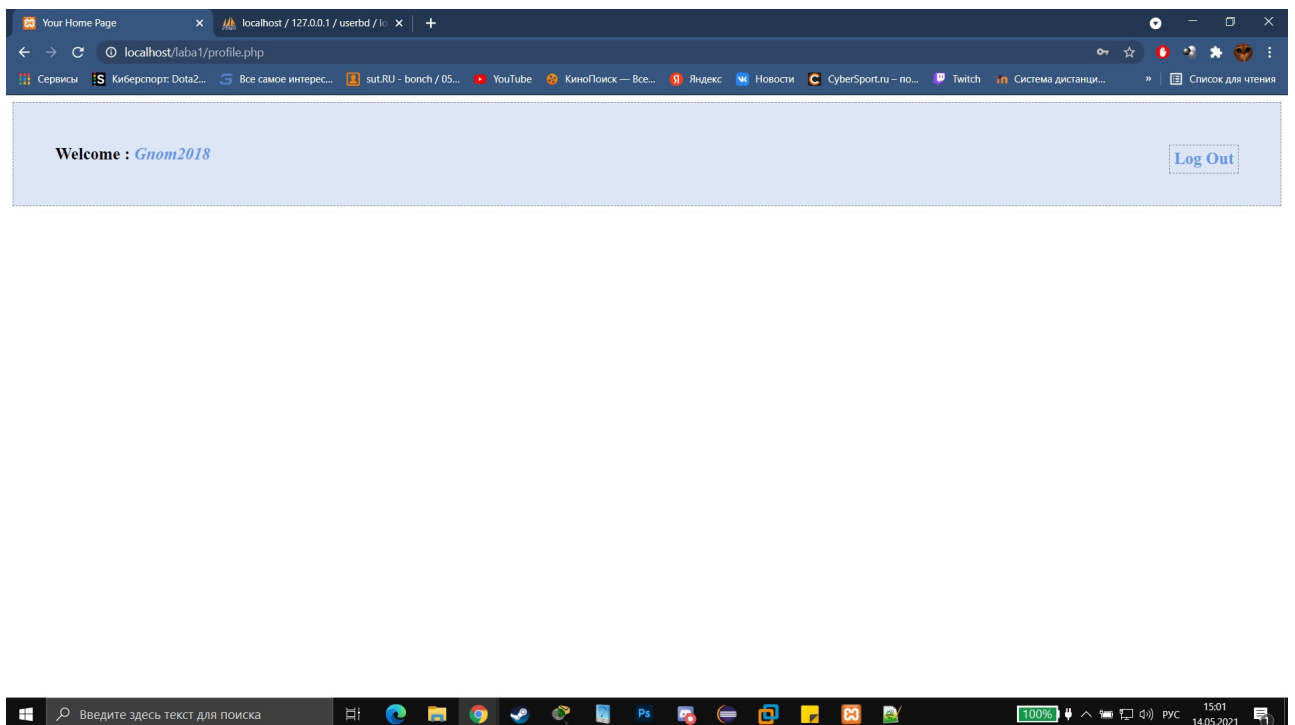
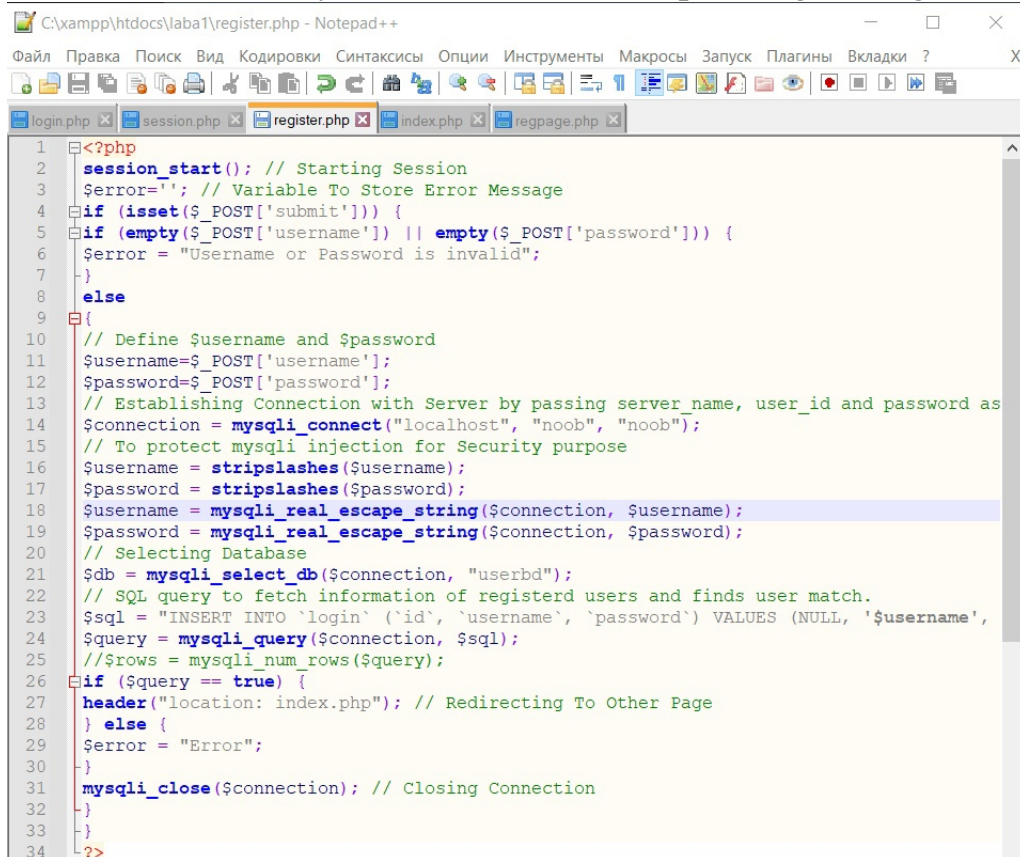


Рис. 6 Успешно авторизовались.

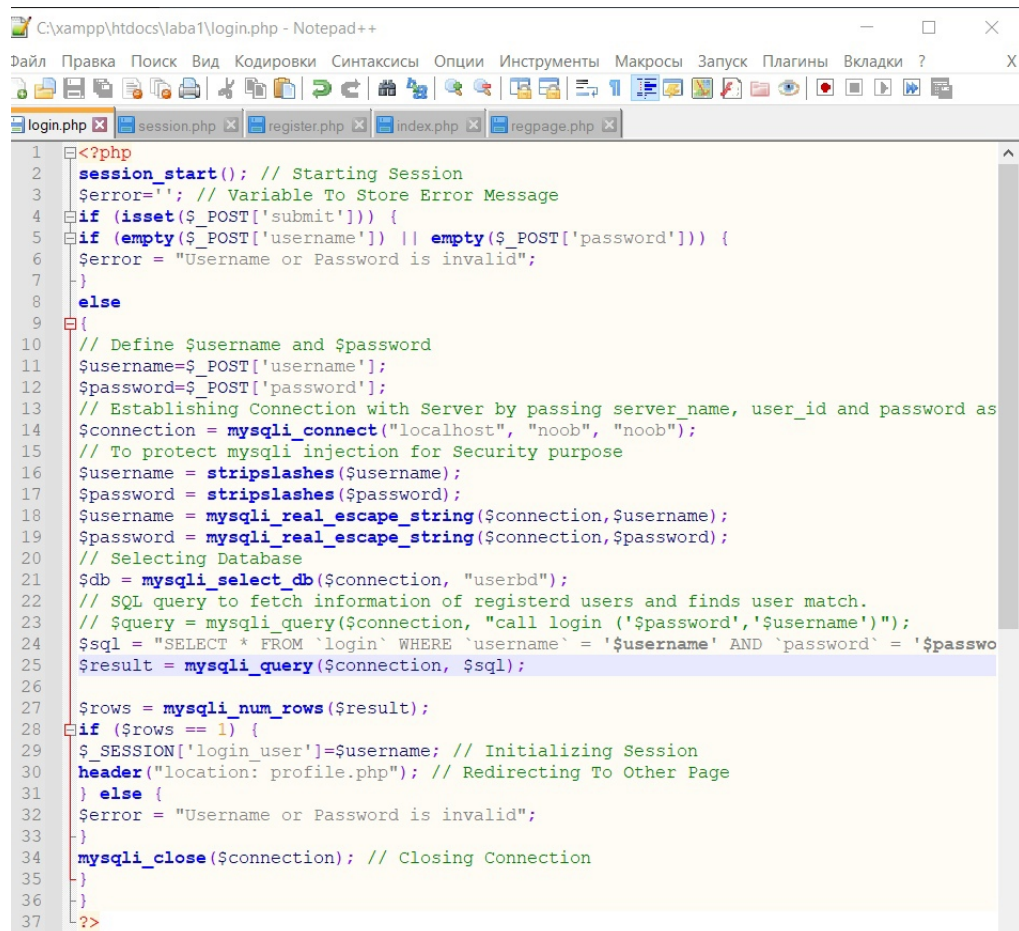
## Пункт 4

Добавляем защиту от SQL-инъекции в файл login и register.



```
1 <?php
2 session_start(); // Starting Session
3 $error=''; // Variable To Store Error Message
4 if (isset($_POST['submit'])) {
5     if (empty($_POST['username']) || empty($_POST['password'])) {
6         $error = "Username or Password is invalid";
7     }
8     else
9     {
10         // Define $username and $password
11         $username=$_POST['username'];
12         $password=$_POST['password'];
13         // Establishing Connection with Server by passing server_name, user_id and password as
14         $connection = mysqli_connect("localhost", "noob", "noob");
15         // To protect mysqli injection for Security purpose
16         $username = stripslashes($username);
17         $password = stripslashes($password);
18         $username = mysqli_real_escape_string($connection, $username);
19         $password = mysqli_real_escape_string($connection, $password);
20         // Selecting Database
21         $db = mysqli_select_db($connection, "userdb");
22         // SQL query to fetch information of registered users and finds user match.
23         $sql = "INSERT INTO `login` (`id`, `username`, `password`) VALUES (NULL, '$username',
24         $query = mysqli_query($connection, $sql);
25         // $rows = mysqli_num_rows($query);
26         if ($query == true) {
27             header("location: index.php"); // Redirecting To Other Page
28         } else {
29             $error = "Error";
30         }
31         mysqli_close($connection); // Closing Connection
32     }
33 }
34 ?>
```

Рис. 7 Редактура файла register.php.



```
1 <?php
2 session_start(); // Starting Session
3 $error=''; // Variable To Store Error Message
4 if (isset($_POST['submit'])) {
5     if (empty($_POST['username']) || empty($_POST['password'])) {
6         $error = "Username or Password is invalid";
7     }
8     else
9     {
10         // Define $username and $password
11         $username=$_POST['username'];
12         $password=$_POST['password'];
13         // Establishing Connection with Server by passing server_name, user_id and password as
14         $connection = mysqli_connect("localhost", "noob", "noob");
15         // To protect mysqli injection for Security purpose
16         $username = stripslashes($username);
17         $password = stripslashes($password);
18         $username = mysqli_real_escape_string($connection, $username);
19         $password = mysqli_real_escape_string($connection, $password);
20         // Selecting Database
21         $db = mysqli_select_db($connection, "userdb");
22         // SQL query to fetch information of registered users and finds user match.
23         // $query = mysqli_query($connection, "call login ('$password','$username')");
24         $sql = "SELECT * FROM `login` WHERE `username` = '$username' AND `password` = '$password'";
25         $result = mysqli_query($connection, $sql);
26
27         $rows = mysqli_num_rows($result);
28         if ($rows == 1) {
29             $_SESSION['login_user']=$username; // Initializing Session
30             header("location: profile.php"); // Redirecting To Other Page
31         } else {
32             $error = "Username or Password is invalid";
33         }
34         mysqli_close($connection); // Closing Connection
35     }
36 }
37 ?>
```

Рис. 8 Редактура файла login.php.

## Пункт 5

### Проверка защиты от SQL-инъекции.

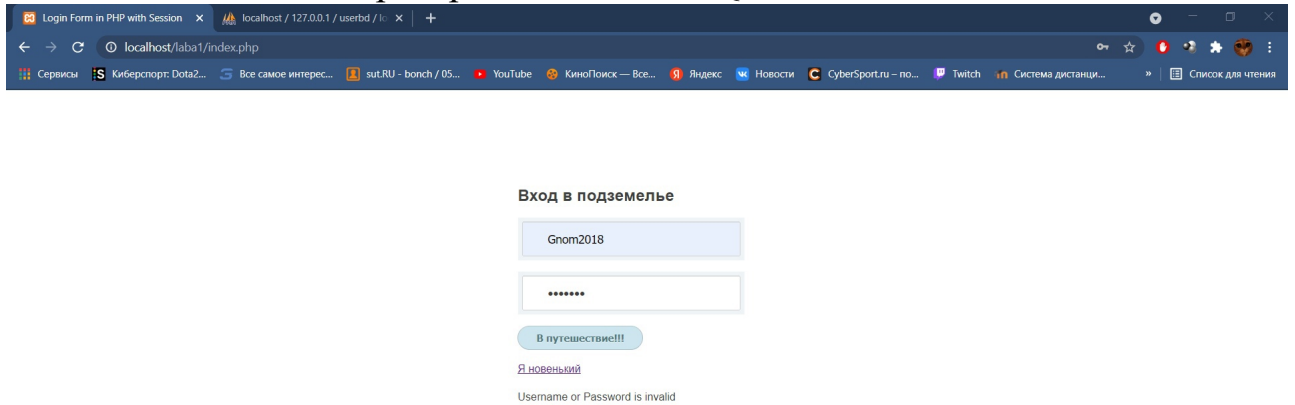


Рис. 9 При попытке зайти с помощью SQL-инъекции, авторизация не удалась.

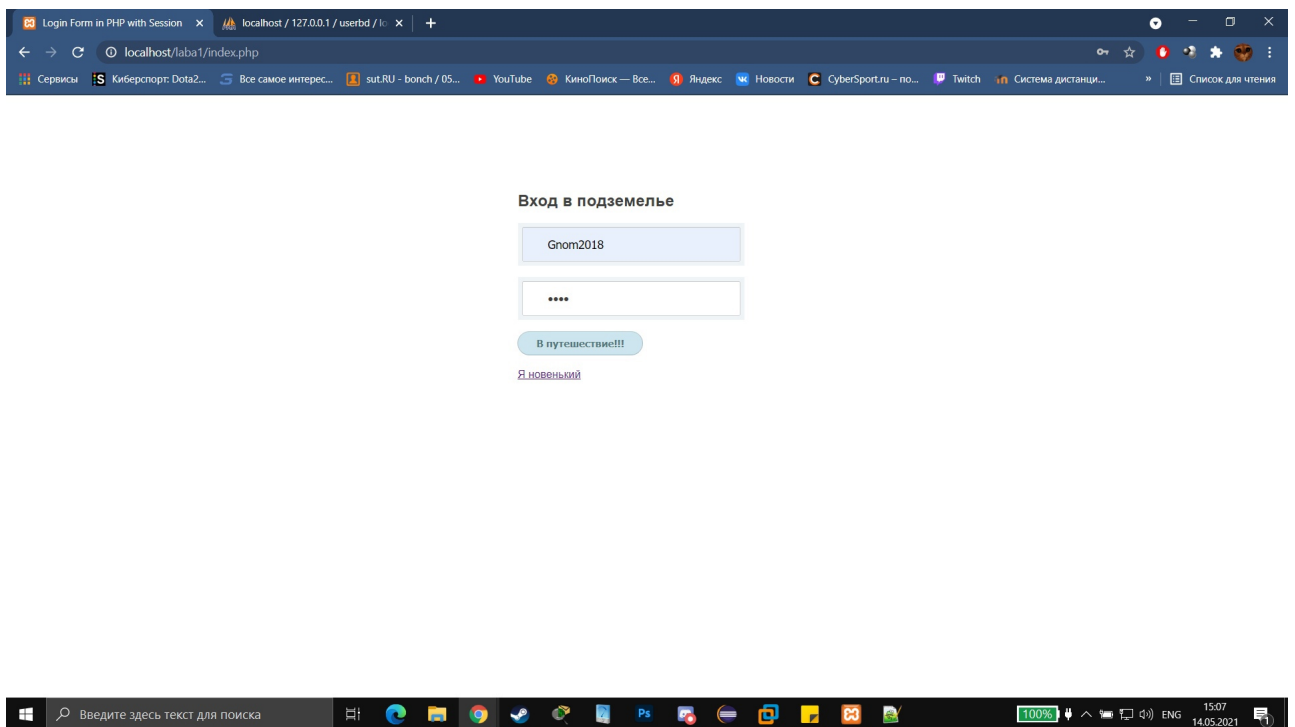


Рис. 10 При вводе валидного пароля, успешно происходит авторизация.

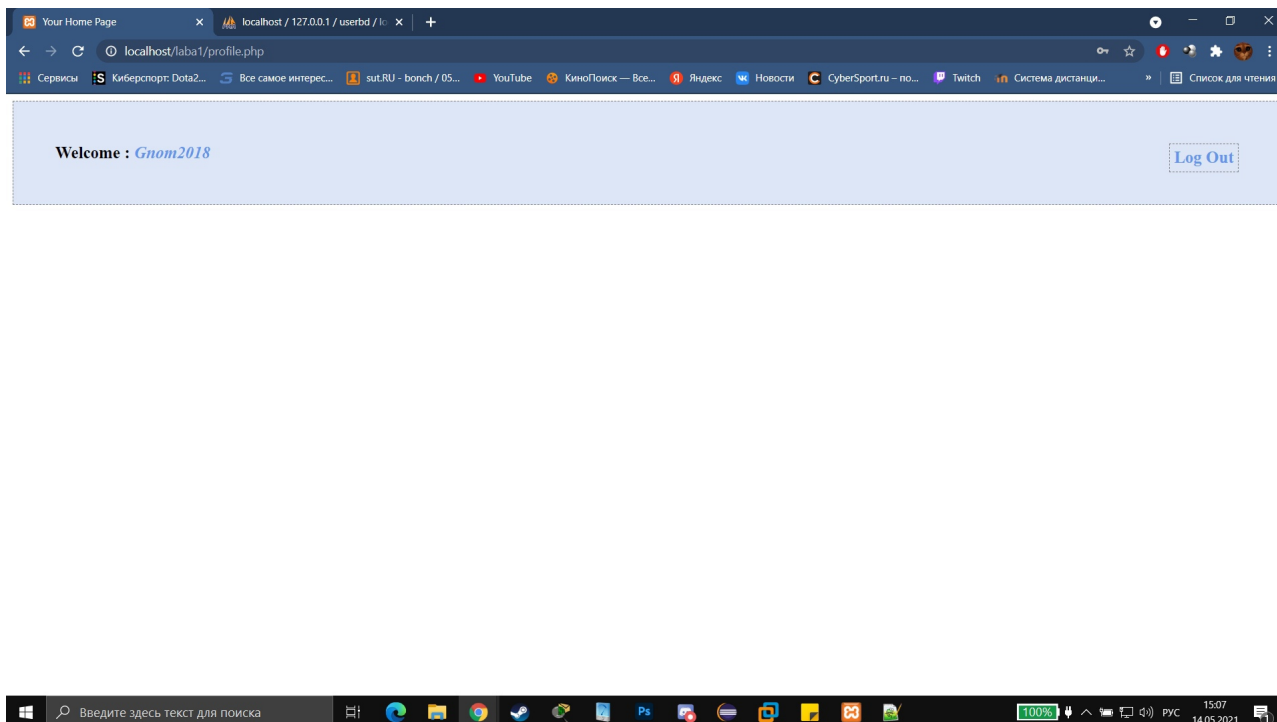


Рис. 11 Страница профиля, после успешной авторизации.

### **Вывод:**

В ходе данной лабораторной работы мы научились разворачивать web-сервер на Windows машине с помощью XAMPP. В XAMPP используется следующий стек технологий: Apache, MariaDB, PHP, Perl. Он распространяется бесплатно, а также позволяет быстро создать web-сервер Apache, и автоматически подключить к нему MariaDB, PHP, Perl.

После установки и настройки XAMMP, мы успешно провели SQL-инъекцию на тестовой странице. После этого мы добавили на тестовую страницу защиту от данной инъекции, и после этого SQL-инъекция не удалась.