1. Для выполнения задания отдельно в БД cyb создал новую таблицу выполнив SQL-команду:

CREATE TABLE users (

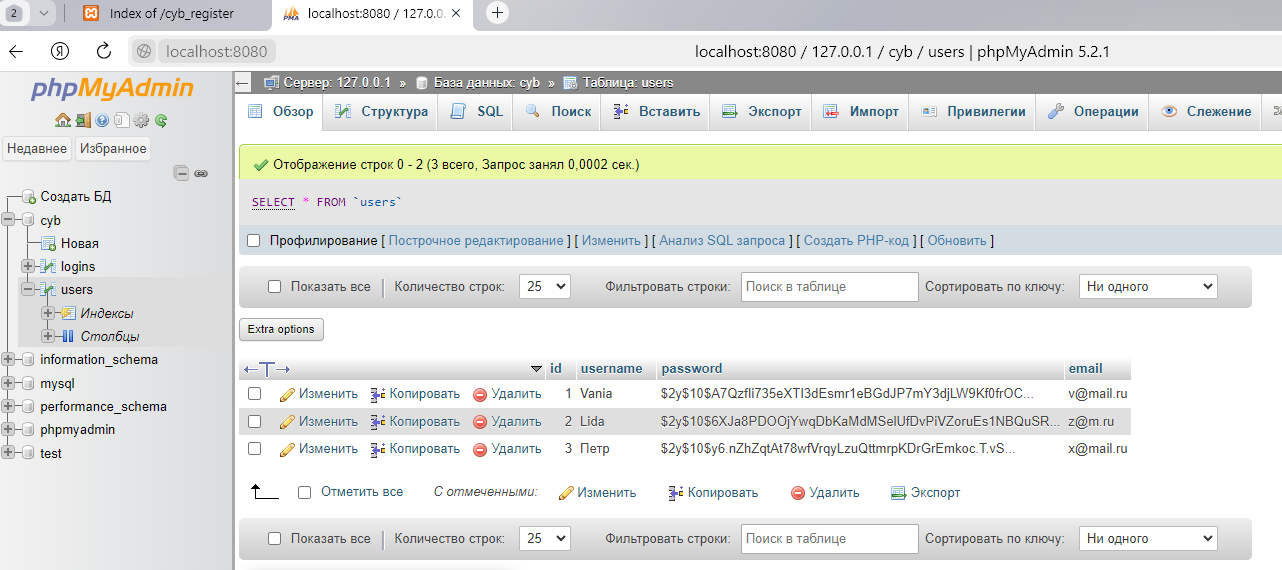
id INT AUTO\_INCREMENT PRIMARY KEY,

username VARCHAR(255) NOT NULL UNIQUE,

password VARCHAR(255) NOT NULL,

email VARCHAR(255) NOT NULL

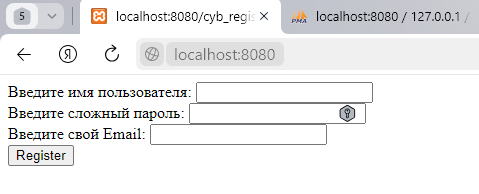
);

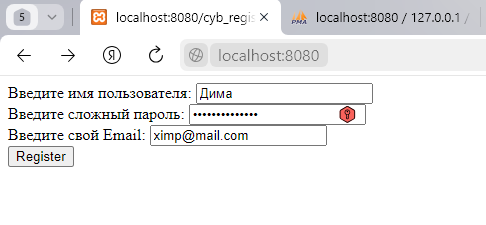


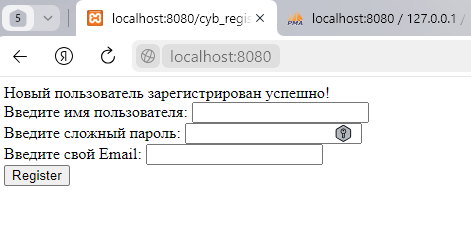
2. Код в файле register.php удовлетворяет условиям задачи, а именно:

* защита от SQL Injection с использованием функции **mysqli\_real\_escape\_string** (экранирует специальные символы в строке для использования в SQL-запросе с учетом текущего набора символов соединения);
* проверка на слабый пароль;
* предотвращение дублирования логинов;
* защита от CSRF атак с использованием токена, сохраненного в сессии;
* вставка данных пользователя в базу данных с хешированием пароля (функцию **password\_hash()** использовал для создания хэша пароля. **PASSWORD\_DEFAULT** применил в качестве алгоритма, при котором PHP автоматически выбирает самый надежный алгоритм, доступный в текущей версии PHP);
* проверки **isset($\_POST['username'], $\_POST['email'], $\_POST['password'])** позволяют убедиться в том, что код будет обрабатывать данные формы только после их отправки. Это устраняет предупреждения о неопределенных индексах массива.

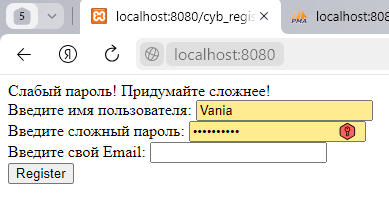
3. Проверка созданных форм и условий.







Придумали слабый пароль



Повторили учетную запись Димы

