

# Задание 38. Хэширование пароля

## Шахназарян Вачик (РИМ-130990)

Добавил хэширование пароля

```
// Если форма регистрации отправлена...
if (!empty($_POST['login'] && !empty($_POST['password']))) {
    $login = $_POST['login'];
    $password = $_POST['password'];
    $hash_password = md5($password);
    $confirm_password = $_POST['confirm_password'];
    $email = $_POST['email'];
    $birthday = $_POST['birthday'];
    $date = date('Y-m-d'); // Получаем текущую дату
```

Запись хэша в БД

```
// Проверка совпадения пароля
if ($password == $confirm_password) {
    $query = "INSERT INTO $table SET login= '$login', password='$hash_password', email='$email', birthday='$birthday', registration_date='$date'";
    mysqli_query($link, $query);
}
```

Кол-во ошибок: 0

## Регистрация

<input type="text" value="user15"/>	<input type="password" value="....."/>	<input type="password" value="....."/>
<input type="text" value="vachikpuper@gmail.com"/>	<input type="text" value="22.02.2001"/>	<input type="checkbox"/>
<input type="button" value="Отправить"/>		

☐ Изменить Копировать Удалить 51 user15 f5bb0c8de146c67b44babbf4e6584cc0 vachikpuper@gmail.com 2001-02-22 2024-04-24

Добавил соль к хэшу

```
// Если форма регистрации отправлена...
if (!empty($_POST['login'] && !empty($_POST['password']))) {
    $login = $_POST['login'];
    $password = $_POST['password'];

    $salt = generateSalt();
    $hash_password = md5($salt . $password);

    $confirm_password = $_POST['confirm_password'];
    $email = $_POST['email'];
    $birthday = $_POST['birthday'];
    $date = date('Y-m-d'); // Получаем текущую дату
```

## Функция соли

```
function generateSalt() {
    $salt = '';
    $salt_length = 8;

    for ($i = 0; $i < $salt_length; $i++) {
        $salt .= chr(mt_rand(33, 126)); // любой символ из ASCII
    }

    return $salt;
}
```

## Добавил salt в БД

<div><div><div></div><div></div><div></div></div></div>				id	login	password	salt	email	birthday	registration_date			
<div><div><div></div><div></div><div></div></div></div>	<div><div><div></div><div></div><div></div></div></div>	Изменить	<div><div><div></div><div></div><div></div></div></div>	Копировать	<div><div><div></div><div></div><div></div></div></div>	Удалить	1	user	12345	NULL	NULL	NULL	NULL
<div><div><div></div><div></div><div></div></div></div>	<div><div><div></div><div></div><div></div></div></div>	Изменить	<div><div><div></div><div></div><div></div></div></div>	Копировать	<div><div><div></div><div></div><div></div></div></div>	Удалить	2	admin	123	NULL	NULL	NULL	NULL
<div><div><div></div><div></div><div></div></div></div>	<div><div><div></div><div></div><div></div></div></div>	Изменить	<div><div><div></div><div></div><div></div></div></div>	Копировать	<div><div><div></div><div></div><div></div></div></div>	Удалить	3	vachik	159	NULL	NULL	NULL	NULL
<div><div><div></div><div></div><div></div></div></div>	<div><div><div></div><div></div><div></div></div></div>	Изменить	<div><div><div></div><div></div><div></div></div></div>	Копировать	<div><div><div></div><div></div><div></div></div></div>	Удалить	51	user15	f5bb0c8de146c67b44babbf4e6584cc0	NULL	vachikpuper@gmail.com	2001-02-22	2024-04-24
<div><div><div></div><div></div><div></div></div></div>	<div><div><div></div><div></div><div></div></div></div>	Изменить	<div><div><div></div><div></div><div></div></div></div>	Копировать	<div><div><div></div><div></div><div></div></div></div>	Удалить	52	user16	0f3ee264402255446d0151ebe2459b81	Um"KE5zQ	vachiksuper@gmail.com	2001-01-22	2024-04-24

## Написал проверку пароля в авторизации

```
// Если форма авторизации отправлена...
if (!empty($_POST['login'] && !empty($_POST['password']))) {
    $login = $_POST['login'];

    $query = "SELECT * FROM $table WHERE login='$login'";
    $result = mysqli_query($link, $query);




    $user = mysqli_fetch_assoc($result);

    if (!empty($user)) {
        $salt = $user['salt'];
        $hash_password = $user['password'];

        $password = md5($salt . $_POST['password']);

        if ($password == $hash_password) {
            $_SESSION['auth'] = true;
            echo "Пользователь прошел авторизацию";
        } else {
            echo "Пара логин-пароль неверна";
        }
    } else {
        echo "Пользователь неверно ввел логин или пароль";
    }
}
}
```

Проверка функционала

□  Изменить  Копировать  Удалить 53 user17 d4f98399a4da18f2849cabe0161267c4 oITW0`2 vachikduper@gmail.com 2001-03-22 2024-04-24

## Авторизация

user17	.....	Отправить
--------	-------	-----------

Пользователь прошел авторизацию

Переписал функционал хэширования пароля через **password\_hash** и **password\_verify**

В файле регистрации удалил функцию для получения соли + добавил хэширование новым способом:

```
$hash = password_hash($password, PASSWORD_DEFAULT);
```

В файле логина переписал проверку на соответствие пароля к хэшу:

```
if (!empty($user)) {  
    $hash = $user['password'];  
  
    // Проверяем соответствие пароля и хэша  
    if (password_verify($_POST['password'], $hash)) {  
        $_SESSION['auth'] = true;  
        echo "Пользователь прошел авторизацию";  
    } else {  
        echo "Пара логин-пароль неверна";  
    }  
} else {  
    echo "Пользователь неверно ввел логин или пароль";  
}
```

Проверка функционала. Зарегистрировал пользователя user18. В БД поле, предназначенное для соли теперь пустое.

□ Изменить Копировать Удалить 54 user18 \$2y\$10\$UlxY8UkJFalbdLHK3vC1e3Lct2HV/Wn6yCu0M7vjDi...

vachikruper@gmail.com 2001-04-22 2024-04-24

Авторизация проходит успешно

Пользователь прошел авторизацию

## Авторизация

<input type="text"/>	<input type="text"/>	<input type="button" value="Отправить"/>
----------------------	----------------------	--

[Страница 1](#) [Регистрация](#) [Выйти](#)

Поменял алгоритм шифрования на BCrypt

```
$hash = password_hash($password, PASSWORD_BCRYPT);
```