Аутентификация и авторизация с SESSION

- Введение
- Практика аутентификации
- Пользователь коварен

Введение

Текущая тема является **завершающе**й в серии, посвященных разработке безопасных приложений. Вся теория пройдена в предыдущих темах. Теперь аймемся практикой реализации аутентификаций, построенных на **сессиях**.

Тема построена по принципу – от **очевидных** решений к **правильным**.

Прежде чем приступить к выполнению, проверьте себя. Вы точно понимаете, чем отличаются следующие **настройки времени выполнения**?

```
// варианты настроек времени выполнения
// вариант 1
ini_set('session.use_cookies', 0);
ini_set("session.use_only_cookies", 0);
ini_set("session.use_trans_sid", 1);
// вариант 2
ini_set('session.use_cookies', 0);
ini_set("session.use_only_cookies", 0);
ini_set("session.use_trans_sid", 0);
```

Ответ:

- вариант 1 – файлы **cookie запрещены**. **Идентификатор** сессии (SID) пересылается посредством элементов, в которых указан **URL-адрес** (ссылки, формы).
- вариант 2 – файлы **cookie запрещены**. **Идентификатор** сессии (SID) **не пересылается**.

Если приведенный пример для вас не очевиден, задания вполне могут быть выполнены. Поняты, вряд ли...

> ***Примечание.*** Все предыдущие темы и демонстрационные примеры выполнялись *во* многом с одной целью – разобраться с аутентификацией и авторизацией при помощи механизма сессий

Но перед тем, как начать, предложу скрипт регистрации **нового пользователя** системы.

Демонстрационный пример **example_1** содержит следующий файлы:

- **index.html** – стартовый файл. Форма добавления пользователя;
- **reg.php** – файл регистрации нового пользователя;
- **out-user.php** – файл вывода списка пользователей системы;
- **delete-user.php** – файл удаления пользователя.

example_1. index.html

```
<h2>Просмотреть список пользователей</h2>
<a href='out-user.php'>Список пользователей</a>
<h2>Регистрация нового пользователя</h2>
<form action="reg.php" method="post">
    Логин: <input type="text" name="login" value=""><p>
    Пароль: <input type="text" name="pwd" value=""><p>
```

```
    Роль:
    <select name="role">
        <option value="user">Пользователь</option>
        <option value="moderator">Модератор</option>
        <option value="admin">Администратор</option>
    </select><p>
    <button>Регистрация</button>
</form>
```

example_1. reg.php

```
<?php
    // подключение к базе данных
    $mysqli = new mysqli ('localhost', 'root', '', 'db_auth');
    // подготовка / привязка параметров / выполнение запроса
    $insert = 'INSERT INTO `user_hash` SET `login` = ?, `pwd` =
    ?, `role` = ?';
    $stmt = $mysqli->prepare($insert);
    $pwd = password_hash($_POST['pwd'], PASSWORD_DEFAULT);
    $stmt->bind_param('sss', $_POST['login'], $pwd,
    $_POST['role']);
    // если ошибка выполнения - сформируем сообщение
    if (!$stmt->execute()) {
        $err = '?err=Что-то пошло не так :(';
    };
    $err = $err?? '';
    // переход к странице списка пользователей
    header('Location:/out-user.php' . $err);
```

```
    exit;
```

example_1. out-user.php

```
<a href="/">Добавить нового пользователя</a>
<?php
    if (isset($_GET['err'])) {
        // в случае возникновения ошибки выведем предупреждение
        echo "<h3>{$_GET['err']}</h3>";
        echo "При добавлении пользователя произошла ошибка";
    } else {
        // подключение к базе данных
        $mysqli = new mysqli ('localhost', 'root', '',
        'db_auth');
        // подготовка / привязка параметров / выполнение запроса
        $stmt = $mysqli->prepare('SELECT `id_user`,`login`,
        `role` FROM `user_hash`');
        $stmt->execute();
        // привязка переменных к результату запроса
        $stmt->bind_result($id_user, $login, $role);
        // хеш пароля выводить не имеет смысла
        echo "<p><b>Логин / Роль</b></p>";
        // вывод списка пользователей
        while($stmt->fetch()){
            echo "$login / $role (<a href='delete-
            user.php?id={$id_user}'>удалить</a>)<p>";
        }
    }
```

```
?>
```

example_1. delete-user.php

```
<?php
    // подключение к базе данных
    $mysqli = new mysqli ('localhost', 'root', '', 'db_auth');
    // подготовка / привязка параметров / выполнение запроса
    $insert = 'DELETE FROM `user_hash` WHERE `id_user` = ?';
    $stmt = $mysqli->prepare($insert);
    $stmt->bind_param('d', $_GET['id']);
    // если ошибка выполнения - сформируем сообщение
    if (!$stmt->execute()) {
        $err = '?err=Что-то пошло не так :(';
    };
    $err = $err?? '';
    // переход к странице списка пользователей
    header('Location:/out-user.php' . $err);
    exit;
```

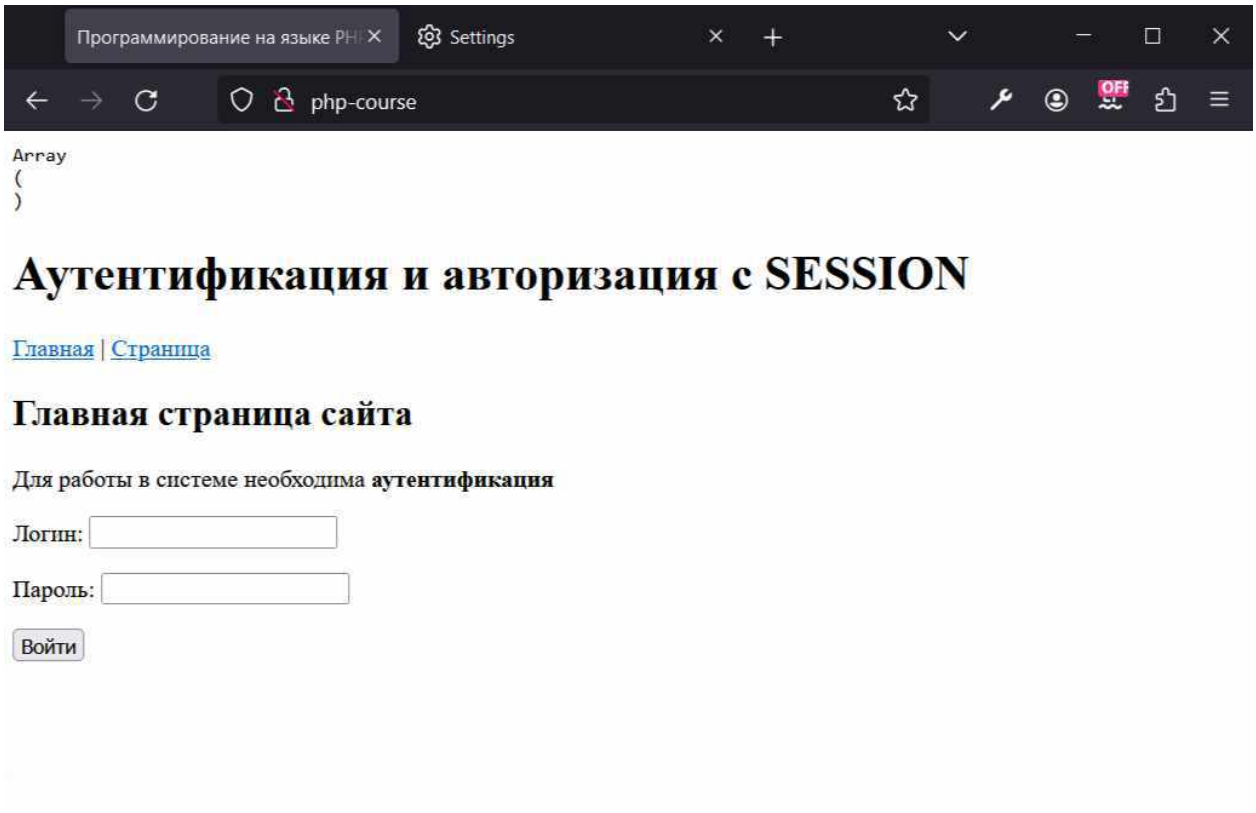
Практика аутентификации

Каждый из демонстрационных примеров содержит **интерфейс**, представленный на следующем скриншоте.

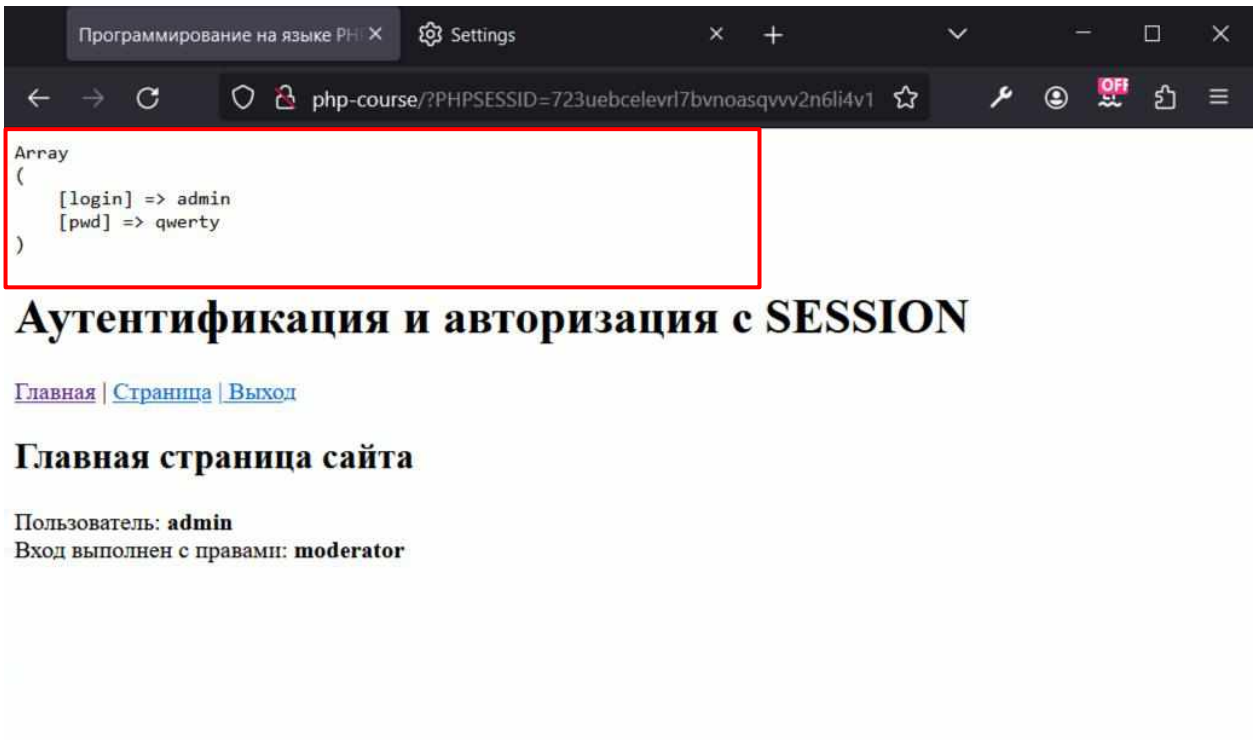
Для наглядности, сессионный массив выводится на каждой странице сайта:

```
// тестовый вывод данных сессии
echo "<pre>";
```

```php
print_r ($_SESSION);

echo "</pre>";
```



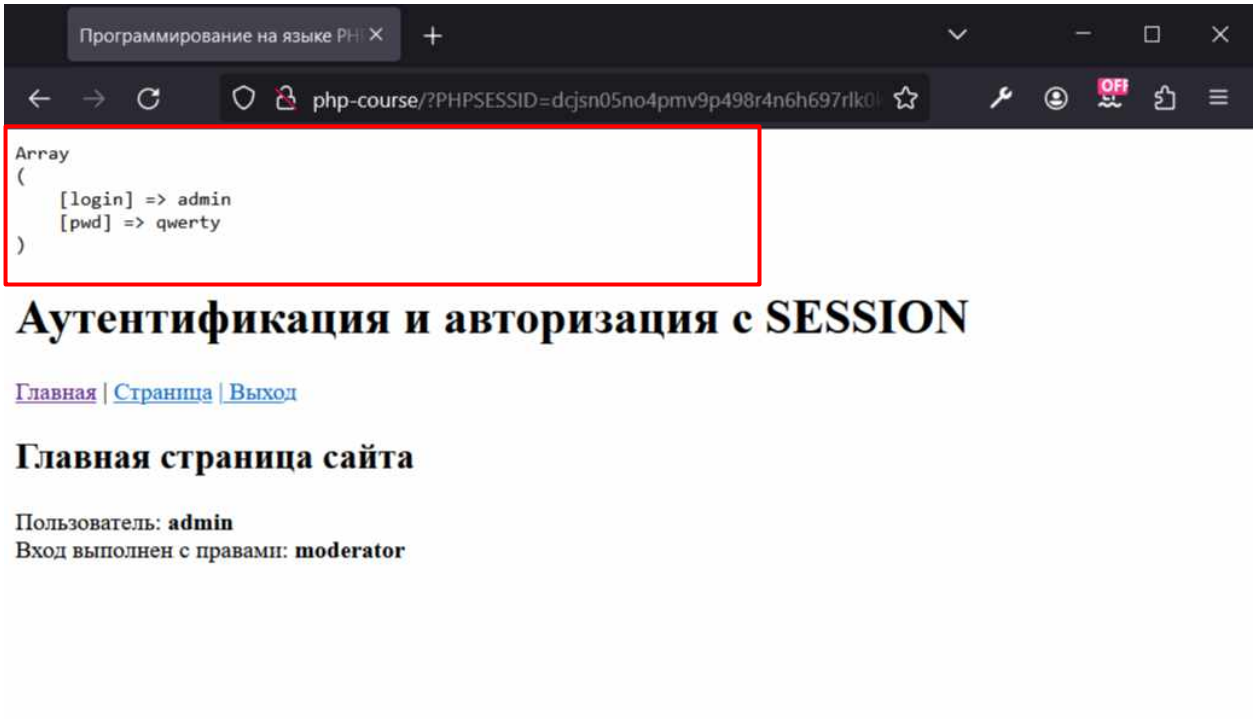
При желании вывод массива можно закомментировать.



Аутентификация с помощью пары логин – пароль

В демонстрационном примере **example_2** аутентификация выполняется с помощью **пары логин** (login) – **открытый пароль** (pwd).

- Запись и сохранение в сессию **логина** (login) и **открытого пароля** (pwd).
- Сессия передается через автоматическую вставку идентификатора **SID**. Настройки времени выполнения:
    - `ini_set('session.use_cookies', 0);`
    - `ini_set("session.use_only_cookies", 0);`
    - `ini_set("session.use_trans_sid", 1);`
- Управление пунктом меню по результату аутентификации.



example_2. index.php

```php
<?php

    // настройки времени выполнения

    ini_set('session.use_cookies', 0);
```

```
    ini_set("session.use_only_cookies", 0);
    ini_set("session.use_trans_sid", 1);
    session_start();
    // тестовый вывод данных сессии
    echo "<pre>";
    print_r ($_SESSION);
    echo "</pre>";
?>
<!-- ... -->
<!-- меню сайта -->
<p>
    <a href='/'>Главная</a> |
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['login']) && isset($_SESSION['pwd']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Главная страница сайта</h2>
<?php
    // если сессионные данные существуют
    if (isset($_SESSION['login']) && isset($_SESSION['pwd'])):
        // подключение к базе данных
        $mysqli = new mysqli ('localhost', 'root', '',
        'db_auth');
```

```
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
        `login` = ?');
        $stmt->bind_param('s', $_SESSION['login']);
        // получение результата
        $stmt->execute();
        $result = $stmt->get_result();
        // если запрос вернул запись
        if ($result->num_rows):
            $row = $result->fetch_assoc();
            // проверка совпадения паролей
            if (password_verify($_SESSION['pwd'], $row['pwd'])):
                $auth = true; // аутентификация успешна
            else:
                $auth = false; // если пароли не совпадают
            endif;
        else:
            $auth = false; // если указанного логина нет в базе
        endif;
    else:
        $auth = false; // если нет сессионных данных
    endif;
    // если аутентификация успешна
    if ($auth):
        echo "<p>Пользователь:<b> {$row['login']} </b><br>";
        echo "Вход выполнен с правами:<b> {$row['role']}
        </b></p>";
```

```
    else:
?>
        <!-- если аутентификация не состоялась -->
        <p>Для работы в системе необходима
        <b>аутентификация</b></p>
        <form action="auth.php" method="post">
            Логин: <input type="text" name="login" value=""><p>
            Пароль: <input type="text" name="pwd" value=""><p>
            <button>Войти</button>
        </form>
<?php
    endif;
?>
```

example_2. auth.php

```
<?php
    // настройки времени выполнения
    ini_set('session.use_cookies', 0);
    ini_set("session.use_only_cookies", 0);
    ini_set("session.use_trans_sid", 1);
    session_start();
    // echo "<pre>";
    // print_r ($_SESSION);
    // echo "</pre>";
    // подключение к базе данных
    $mysqli = new mysqli ('localhost', 'root', '', 'db_auth');
    // создание, выполнение подготовленного запроса
```

```
    $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
    `login` = ?');
    $stmt->bind_param('s', $_POST['login']);
    // получение результата
    $stmt->execute();
    $result = $stmt->get_result();
    // если запрос вернул запись
    if ($result->num_rows) {
        $row = $result->fetch_assoc();
        if (password_verify($_POST['pwd'], $row['pwd'])) {
            // сохраняем в сессию данные пользователя
            $_SESSION['login'] = $_POST["login"];
            $_SESSION['pwd'] = $_POST["pwd"];
            header('Location:/?' . SID);
            exit;
        } else $err = true;
    } else $err = true;
?>
<!-- ... -->
<?php
    if (isset($err)):
?>
        <!-- меню сайта -->
        <p>
            <a href='/'>Главная</a> |
            <a href='/page.php'>Страница</a>
            <?php
```

```
                // определяем пункт меню
                if (isset($_SESSION['login']))
                echo '<a href="/logout.php"> | Выход</a>';
            ?>
        </p>
        <h3>Пользователь с такими данными в системе не
        найден</h3>
        <p><a href='/'>Попробовать еще раз</a></p>
<?php
    endif;
?>
```

example_2. page.php

```
<?php
    // настройки времени выполнения
    ini_set('session.use_cookies', 0);
    ini_set("session.use_only_cookies", 0);
    ini_set("session.use_trans_sid", 1);
    session_start();
    // тестовый вывод данных сессии
    echo "<pre>";
    print_r ($_SESSION);
    echo "</pre>";
?>
<!-- ... -->
<!-- меню сайта -->
<p>
```

```
    <a href='/'>Главная</a> |
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['login']) && isset($_SESSION['pwd']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Страница сайта</h2>
<?php
    // если сессионные данные существуют
    if (isset($_SESSION['login']) && isset($_SESSION['pwd'])):
        // подключение к базе данных
        $mysqli = new mysqli ('localhost', 'root', '',
        'db_auth');
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
        `login` = ?');
        $stmt->bind_param('s', $_SESSION['login']);
        // получение результата
        $stmt->execute();
        $result = $stmt->get_result();
        // если запрос вернул запись
        if ($result->num_rows):
            $row = $result->fetch_assoc();
            // проверка совпадения паролей
```

```
            if (password_verify($_SESSION['pwd'], $row['pwd'])) {
                $auth = true; // аутентификация успешна
            else:
                $auth = false; // если пароли не совпадают
            endif;
        else:
            $auth = false; // если указанного логина нет в базе
        endif;
    else:
        $auth = false; // если нет сессионных данных
    endif;
    // если аутентификация успешна
    if ($auth):
        echo "<p>Пользователь:<b> {$row['login']} </b><br>";
        echo "Вход выполнен с правами:<b> {$row['role']}
        </b></p>";
    else:
        // если аутентификация не состоялась
        echo "<p>Для работы в системе необходима
        <b>аутентификация</b></p>";
    endif;
?>
```

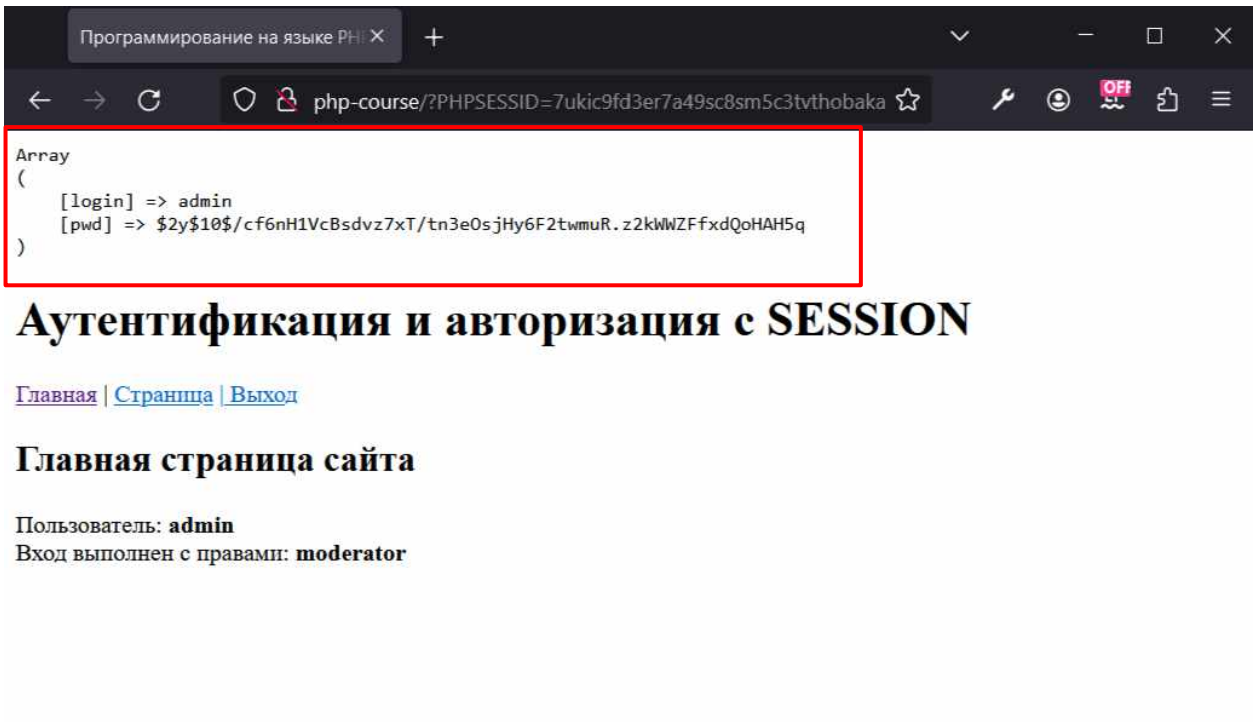
example_2. logout.php

```
<?php
    // удаляем данные, уничтожаем сессию
    session_start();
```

```php
    session_unset();
    session_destroy();
    // echo "<pre>";
    // print_r($_SESSION);
    // echo "</pre>";
    // exit;
    header('Location:/');
    exit;
```

В демонстрационном примере **example_3** аутентификация выполняется с помощью **пары логин** (login) **– хешированный пароль** (pwd).

- Запись и сохранение в сессию **логина** (login) и **хешированного пароля** (pwd).
- Сессия передается через автоматическую вставку идентификатора **SID**. Настройки времени выполнения:
    - `ini_set('session.use_cookies', 0);`
    - `ini_set("session.use_only_cookies", 0);`
    - `ini_set("session.use_trans_sid", 1);`
- Управление пунктом меню по результату аутентификации.



example_3. index.php

```php
<?php

    // настройки времени выполнения

    ini_set('session.use_cookies', 0);

    ini_set("session.use_only_cookies", 0);

    ini_set("session.use_trans_sid", 1);

    session_start();

    // тестовый вывод данных сессии

    echo "<pre>";

    print_r ($_SESSION);

    echo "</pre>";

?>

<!-- ... -->

<!-- меню сайта -->

<p>

    <a href='/'>Главная</a> |
```

```
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['login']) && isset($_SESSION['pwd']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Главная страница сайта</h2>
<?php
    // если сессионные данные существуют
    if (isset($_SESSION['login']) && isset($_SESSION['pwd'])):
        // подключение к базе данных
        $mysqli = new mysqli ('localhost', 'root', '',
        'db_auth');
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
        `login` = ? AND `pwd` = ?');
        $stmt->bind_param('ss', $_SESSION['login'],
        $_SESSION['pwd']);
        // получение результата
        $stmt->execute();
        $result = $stmt->get_result();
        // если запрос вернул запись
        if ($result->num_rows):
            $row = $result->fetch_assoc();
            $auth = true; // аутентификация успешна
        else:
```

```
            $auth = false; // если укаазанной пары логин-пароль
            нет в базе
        endif;
    else:
        $auth = false; // если нет сессионных данных
    endif;
    // если аутентификация успешна
    if ($auth):
        echo "<p>Пользователь:<b> {$row['login']} </b><br>";
        echo "Вход выполнен с правами:<b> {$row['role']}
        </b></p>";
    else:
?>
        <!-- если аутентификация не состоялась -->
        <p>Для работы в системе необходима
        <b>аутентификация</b></p>
        <form action="auth.php" method="post">
            Логин: <input type="text" name="login" value=""><p>
            Пароль: <input type="text" name="pwd" value=""><p>
            <button>Войти</button>
        </form>
<?php
    endif;
?>
```

example_3. auth.php

```
<?php
```

```php
// настройки времени выполнения
ini_set('session.use_cookies', 0);
ini_set("session.use_only_cookies", 0);
ini_set("session.use_trans_sid", 1);
session_start();
// echo "<pre>";
// print_r ($_SESSION);
// echo "</pre>";
// подключение к базе данных
$mysqli = new mysqli ('localhost', 'root', '', 'db_auth');
// создание, выполнение подготовленного запроса
$stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
`login` = ?');
$stmt->bind_param('s', $_POST['login']);
// получение результата
$stmt->execute();
$result = $stmt->get_result();
// если запрос вернул запись
if ($result->num_rows) {
    $row = $result->fetch_assoc();
    if (password_verify($_POST['pwd'], $row['pwd'])) {
        // сохраняем в сессию данные пользователя
        $_SESSION['login'] = $_POST["login"];
        $_SESSION['pwd'] = $row["pwd"];
        header('Location:/?' . SID);
        exit;
    } else $err = true;
```

```
    } else $err = true;
?>
<!-- ... -->
<?php
    if (isset($err)):
?>
        <!-- меню сайта -->
        <p>
            <a href='/'>Главная</a> |
            <a href='/page.php'>Страница</a>
            <?php
                // определяем пункт меню
                if (isset($_SESSION['login']))
                echo '<a href="/logout.php"> | Выход</a>';
            ?>
        </p>
        <h3>Пользователь с такими данными в системе не
        найден</h3>
        <p><a href='/'>Попробовать еще раз</a></p>
<?php
    endif;
?>
```

example_3. page.php

```
<?php
    // настройки времени выполнения
    ini_set('session.use_cookies', 0);
```

```
    ini_set("session.use_only_cookies", 0);
    ini_set("session.use_trans_sid", 1);
    session_start();
    // тестовый вывод данных сессии
    echo "<pre>";
    print_r ($_SESSION);
    echo "</pre>";
?>
<!-- ... -->
<!-- меню сайта -->
<p>
    <a href='/'>Главная</a> |
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['login']) && isset($_SESSION['pwd']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Страница сайта</h2>
<?php
    // если сессионные данные существуют
    if (isset($_SESSION['login']) && isset($_SESSION['pwd'])):
        // подключение к базе данных
        $mysqli = new mysqli ('localhost', 'root', '',
        'db_auth');
```

```
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
        `login` = ? AND `pwd` = ?');
        $stmt->bind_param('ss', $_SESSION['login'],
        $_SESSION['pwd']);
        // получение результата
        $stmt->execute();
        $result = $stmt->get_result();
        // если запрос вернул запись
        if ($result->num_rows):
            $row = $result->fetch_assoc();
            $auth = true; // аутентификация успешна
        else:
            $auth = false; // если указанной пары логин-пароль
            нет в базе
        endif;
    else:
        $auth = false; // если нет сессионных данных
    endif;
    // если аутентификация успешна
    if ($auth):
        echo "<p>Пользователь:<b> {$row['login']} </b><br>";
        echo "Вход выполнен с правами:<b> {$row['role']}
        </b></p>";
    else:
        // если аутентификация не состоялась
        echo "<p>Для работы в системе необходима
        <b>аутентификация</b></p>";
```

```
    endif;
?>
```

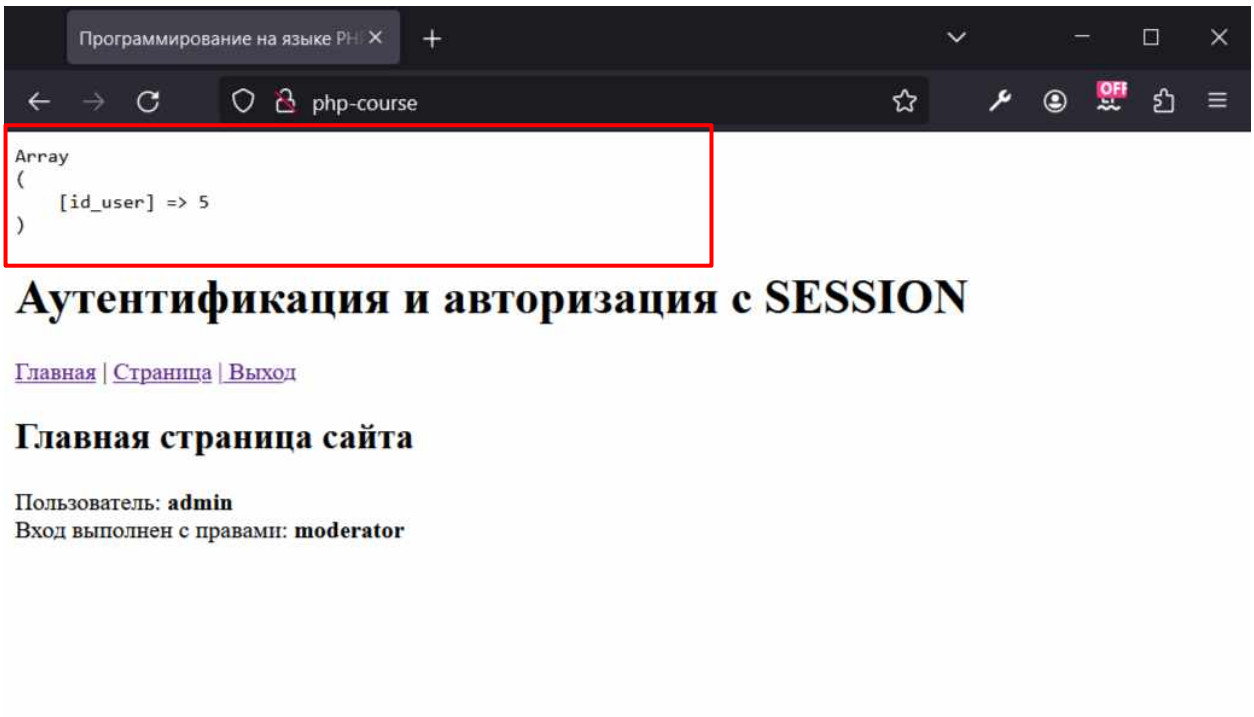
example_3. logout.php

```
<?php
    // удаляем данные, уничтожаем сессию
    session_start();
    session_unset();
    session_destroy();
    // echo "<pre>";
    // print_r($_SESSION);
    // echo "</pre>";
    // exit;
    header('Location:/');
    exit;
```

Аутентификация с помощью идентификатора первичного ключа

В демонстрационном примере **example_4** аутентификация выполняется с помощью **идентификатора первичного ключа** (id_user).

- Запись и сохранение в сессии **идентификатора** (id_user).
- Сессия передается через сессионный **cookie**. Настройки времени выполнения:
    - `ini_set('session.use_cookies', 1);`
    - `ini_set("session.use_only_cookies", 1);`
- Управление пунктом меню по результату аутентификации.



example_4. index.php

```php
<?php

    // настройки времени выполнения

    ini_set('session.use_cookies', 1);

    ini_set("session.use_only_cookies", 1);

    // ini_set("session.use_trans_sid", 1);

    session_start();

    // тестовый вывод данных сессии

    echo "<pre>";

    print_r ($_SESSION);

    echo "</pre>";

?>

<!-- ... -->

<!-- меню сайта -->

<p>

    <a href='/'>Главная</a> |
```

```
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['id_user']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Главная страница сайта</h2>
<?php
    // если сессионные данные существуют
    if (isset($_SESSION['id_user'])):
        // подключение к базе данных
        $mysqli = new mysqli ('localhost', 'root', '',
        'db_auth');
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
        `id_user` = ?');
        $stmt->bind_param('d', $_SESSION['id_user']);
        // получение результата
        $stmt->execute();
        $result = $stmt->get_result();
        // если запрос вернул запись
        if ($result->num_rows):
            $row = $result->fetch_assoc();
            $auth = true; // аутентификация успешна
        else:
            $auth = false; // если пользователя с id_user нет в
```

```
            базе
        endif;
    else:
        $auth = false; // если нет сессионных данных
    endif;
    // если аутентификация успешна
    if ($auth):
        echo "<p>Пользователь:<b> {$row['login']} </b><br>";
        echo "Вход выполнен с правами:<b> {$row['role']}
        </b></p>";
    else:
?>
        <!-- если аутентификация не состоялась -->
        <p>Для работы в системе необходима
        <b>аутентификация</b></p>
        <form action="auth.php" method="post">
            Логин: <input type="text" name="login" value=""><p>
            Пароль: <input type="text" name="pwd" value=""><p>
            <button>Войти</button>
        </form>
<?php
    endif;
?>
```

example_4. auth.php

```
<?php
    // настройки времени выполнения
```

```php
    ini_set('session.use_cookies', 1);
    ini_set("session.use_only_cookies", 1);
    // ini_set("session.use_trans_sid", 1);
    session_start();
    // echo "<pre>";
    // print_r ($_SESSION);
    // echo "</pre>";
    // подключение к базе данных
    $mysqli = new mysqli ('localhost', 'root', '', 'db_auth');
    // создание, выполнение подготовленного запроса
    $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
    `login` = ?');
    $stmt->bind_param('s', $_POST['login']);
    // получение результата
    $stmt->execute();
    $result = $stmt->get_result();
    // если запрос вернул запись
    if ($result->num_rows) {
        $row = $result->fetch_assoc();
        if (password_verify($_POST['pwd'], $row['pwd'])) {
            // сохраняем в сессию идентификатор пользователя
            $_SESSION['id_user'] = $row["id_user"];
            header('Location:/');
            exit;
        } else $err = true;
    } else $err = true;
?>
```

```
<!-- ... -->
<?php
    if (isset($err)):
?>
        <!-- меню сайта -->
        <p>
            <a href='/'>Главная</a> |
            <a href='/page.php'>Страница</a>
            <?php
                // определяем пункт меню
                if (isset($_SESSION['id_user']))
                    echo '<a href="/logout.php"> | Выход</a>';
            ?>
        </p>
        <h3>Пользователь с такими данными в системе не
        найден</h3>
        <p><a href='/'>Попробовать еще раз</a></p>
<?php
    endif;
?>
```

example_4. page.php

```
<?php
    // настройки времени выполнения
    ini_set('session.use_cookies', 1);
    ini_set("session.use_only_cookies", 1);
    // ini_set("session.use_trans_sid", 1);
```

```
    session_start();
    // тестовый вывод данных сессии
    echo "<pre>";
    print_r ($_SESSION);
    echo "</pre>";
?>
<!-- ... -->
<!-- меню сайта -->
<p>
    <a href='/'>Главная</a> |
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['id_user']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Страница сайта</h2>
<?php
    // если сессионные данные существуют
    if (isset($_SESSION['id_user'])):
        // подключение к базе данных
        $mysqli = new mysqli ('localhost', 'root', '',
        'db_auth');
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
```

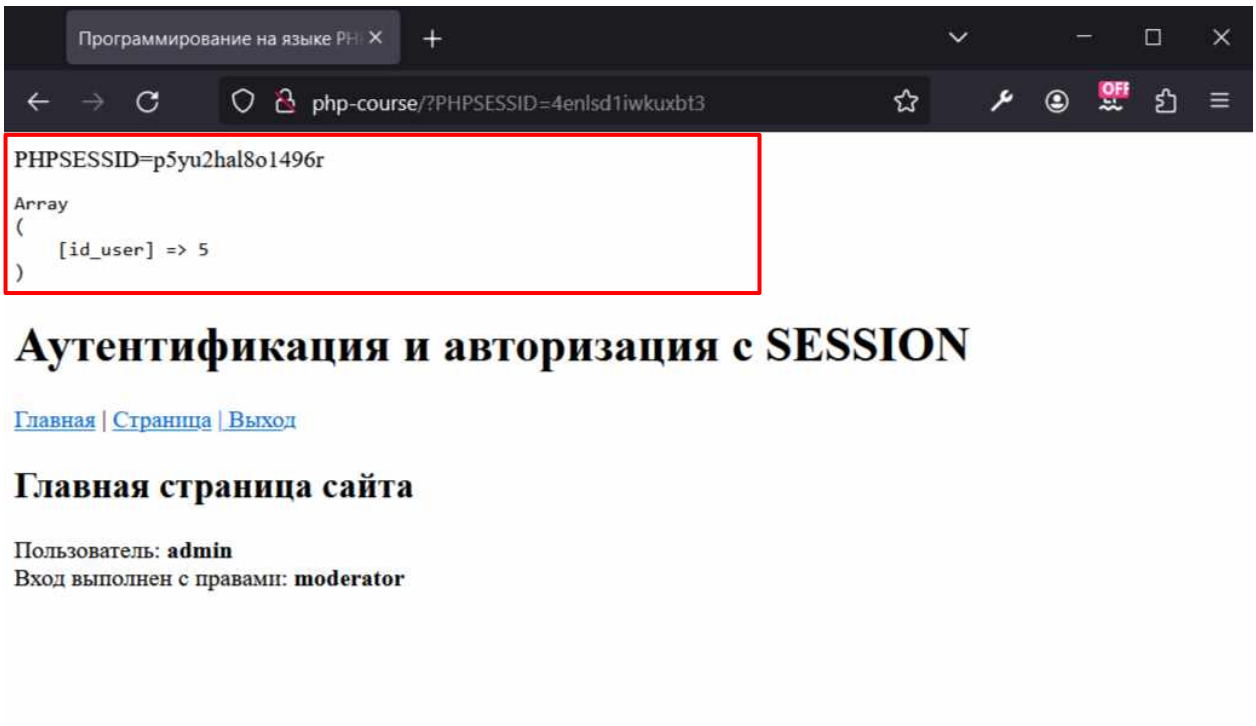
```
        `id_user` = ?');
        $stmt->bind_param('d', $_SESSION['id_user']);
        // получение результата
        $stmt->execute();
        $result = $stmt->get_result();
        // если запрос вернул запись
        if ($result->num_rows):
            $row = $result->fetch_assoc();
            $auth = true; // аутентификация успешна
        else:
            $auth = false; // если пользователя с id_user нет в
            базе
        endif;
    else:
        $auth = false; // если нет сессионных данных
    endif;
    // если аутентификация успешна
    if (isset($auth) && $auth == true):
        echo "<p>Пользователь:<b> {$row['login']} </b><br>";
        echo "Вход выполнен с правами:<b> {$row['role']}
        </b></p>";
    else:
        // если аутентификация не состоялась
        echo "<p>Для работы в системе необходима
        <b>аутентификация</b></p>";
    endif;
?>
```

example_4. logout.php

```php
<?php

    // удаляем данные, уничтожаем сессию

    session_start();

    session_unset();

    session_destroy();

    // echo "<pre>";

    // print_r($_SESSION);

    // echo "</pre>";

    // exit;

    header('Location:/');

    exit;
```

В демонстрационном примере **example_5** аутентификация выполняется с помощью **идентификатора первичного ключа** (id_user).

- **Динамическое** генерирование идентификатора сессии **после каждого запроса к серверу** (на каждой странице сайта).
- Запись в сессию **идентификатора** (id_user).
- Сессия передается через автоматическую вставку константы **SID**. Настройки времени выполнения:
    - `ini_set('session.use_cookies', 0);`
    - `ini_set("session.use_only_cookies", 0);`
    - `ini_set("session.use_trans_sid", 1);`
- Управление пунктом меню по результату аутентификации.



example_5. index.php

```php
<?php

    // настройки времени выполнения

    ini_set('session.use_cookies', 0);

    ini_set("session.use_only_cookies", 0);

    ini_set("session.use_trans_sid", 1);

    session_start();

    // сохраняем сессионные данные

    $data = $_SESSION;

    // удаляем сессию

    session_unset();

    session_destroy();

    // набор символов для генерации идентификатора сессии

    $chars = '0123456789abcdefghijklmnopqrstuvwxyz';

    $session_id = substr(str_shuffle($chars), 0, 15);

    // устанавливаем пользовательский идентификатор
```

```
    session_id($session_id);
    // стартуем новую сессию
    session_start();
    echo session_name() . "=" . session_id() . "<br>";
    // перезаписываем сессионные данные
    $_SESSION = $data;
    // тестовый вывод данных сессии
    echo "<pre>";
    print_r ($_SESSION);
    echo "</pre>";
?>
<!-- ... -->
<!-- меню сайта -->
<p>
    <a href='/'>Главная</a> |
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['id_user']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Главная страница сайта</h2>
<?php
    // если сессионные данные существуют
    if (isset($_SESSION['id_user'])):
```

```php
        // подключение к базе данных
        $mysqli = new mysqli ('localhost', 'root', '',
        'db_auth');
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
        `id_user` = ?');
        $stmt->bind_param('d', $_SESSION['id_user']);
        // получение результата
        $stmt->execute();
        $result = $stmt->get_result();
        // если запрос вернул запись
        if ($result->num_rows):
            $row = $result->fetch_assoc();
            $auth = true; // аутентификация успешна
        else:
            $auth = false; // если пользователя с id_user нет в
            базе
        endif;
    else:
        $auth = false; // если нет сессионных данных
    endif;
    // если аутентификация успешна
    if ($auth):
        echo "<p>Пользователь:<b> {$row['login']} </b><br>";
        echo "Вход выполнен с правами:<b> {$row['role']}
        </b></p>";
    else:
?>
```

```
        <!-- если аутентификация не состоялась -->
        <p>Для работы в системе необходима
        <b>аутентификация</b></p>
        <form action="auth.php" method="post">
            Логин: <input type="text" name="login" value=""><p>
            Пароль: <input type="text" name="pwd" value=""><p>
            <button>Войти</button>
        </form>
<?php
    endif;
?>
```

example_5. auth.php

```
<?php
    // настройки времени выполнения
    ini_set('session.use_cookies', 0);
    ini_set("session.use_only_cookies", 0);
    ini_set("session.use_trans_sid", 1);
    session_start();
    // подключение к базе данных
    $mysqli = new mysqli ('localhost', 'root', '', 'db_auth');
    // создание, выполнение подготовленного запроса
    $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
    `login` = ?');
    $stmt->bind_param('s', $_POST['login']);
    // получение результата
    $stmt->execute();
```

```
    $result = $stmt->get_result();
    // если запрос вернул запись
    if ($result->num_rows) {
        $row = $result->fetch_assoc();
        if (password_verify($_POST['pwd'], $row['pwd'])) {
            // сохраняем в сессию идентификатор пользователя
            $_SESSION['id_user'] = $row["id_user"];
            header('Location:/?'. SID);
            exit;
        } else $err = true;
    } else $err = true;
?>
<!-- ... -->
<?php
    if (isset($err)):
?>
        <!-- меню сайта -->
        <p>
            <a href='/'>Главная</a> |
            <a href='/page.php'>Страница</a>
            <?php
                // определяем пункт меню
                if (isset($_SESSION['id_user']))
                echo '<a href="/logout.php"> | Выход</a>';
            ?>
        </p>
        <h3>Пользователь с такими данными в системе не
```

```
        найден</h3>
        <p><a href='/'>Попробовать еще раз</a></p>
<?php
    endif;
?>
```

example_5. page.php

```
<?php
    // настройки времени выполнения
    ini_set('session.use_cookies', 0);
    ini_set("session.use_only_cookies", 0);
    ini_set("session.use_trans_sid", 1);
    session_start();
    // сохраняем сессионные данные
    $data = $_SESSION;
    // удаляем сессию
    session_unset();
    session_destroy();
    // набор символов для генерации идентификатора сессии
    $chars = '0123456789abcdefghijklmnopqrstuvwxyz';
    $session_id = substr(str_shuffle($chars), 0, 15);
    // устанавливаем пользовательский идентификатор
    session_id($session_id);
    // стартуем новую сессию
    session_start();
    echo session_name() . "=" . session_id() . "<br>";
    // перезаписываем сессионные данные
```

```
    $_SESSION = $data;
    // тестовый вывод данных сессии
    echo "<pre>";
    print_r($_SESSION);
    echo "</pre>";
?>
<!-- ... -->
<!-- меню сайта -->
<p>
    <a href='/'>Главная</a> |
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['id_user']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Страница сайта</h2>
<?php
    // если сессионные данные существуют
    if (isset($_SESSION['id_user'])):
        // подключение к базе данных
        $mysqli = new mysqli ('localhost', 'root', '',
        'db_auth');
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
```

```
        `id_user` = ?');
        $stmt->bind_param('d', $_SESSION['id_user']);
        // получение результата
        $stmt->execute();
        $result = $stmt->get_result();
        // если запрос вернул запись
        if ($result->num_rows):
            $row = $result->fetch_assoc();
            $auth = true; // аутентификация успешна
        else:
            $auth = false; // если пользователя с id_user нет в
            базе
        endif;
    else:
        $auth = false; // если нет сессионных данных
    endif;
    // если аутентификация успешна
    if ($auth):
        echo "<p>Пользователь:<b> {$row['login']} </b><br>";
        echo "Вход выполнен с правами:<b> {$row['role']}
        </b></p>";
    else:
        // если аутентификация не состоялась
        echo "<p>Для работы в системе необходима
        <b>аутентификация</b></p>";
    endif;
?>
```

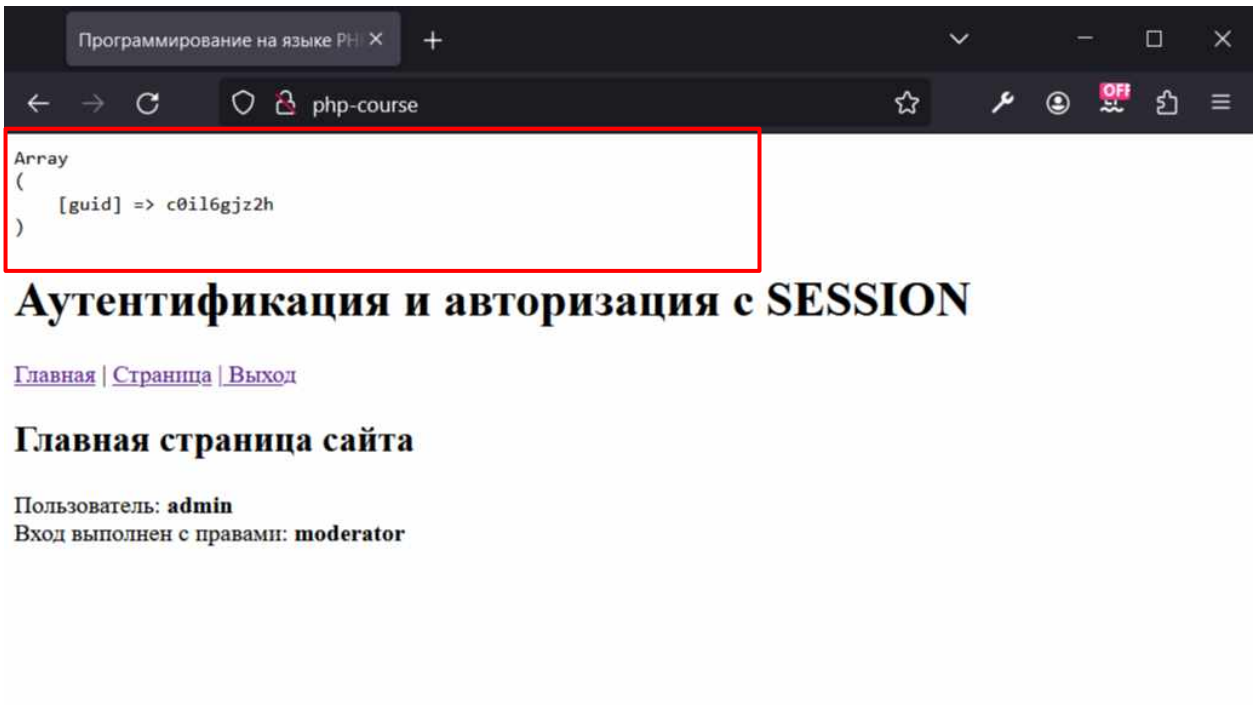
example_5. logout.php

```php
<?php

    // удаляем данные, уничтожаем сессию

    session_start();

    session_unset();

    session_destroy();

    // echo "<pre>";

    // print_r($_SESSION);

    // echo "</pre>";

    // exit;

    header('Location:/');

    exit;
```

Аутентификация с помощью идентификатора GUID

В демонстрационном примере **example_6** аутентификация выполняется с помощью **идентификатора GUID.**

- **Динамическое** генерирование идентификатора **GUID на каждом сеансе** (при каждой аутентификации пользователя).
- Запись в сессию **идентификатора GUID**(guid).
- Сессия передается через сессионный **cookie**. Настройки времени выполнения:
    - `ini_set('session.use_cookies', 1);`
    - `ini_set("session.use_only_cookies", 1);`
- Управление пунктом меню по результату аутентификации.



example_6. index.php

```php
<?php

    // настройки времени выполнения

    ini_set('session.use_cookies', 1);

    ini_set("session.use_only_cookies", 1);

    // ini_set("session.use_trans_sid", 1);

    session_start();

    // тестовый вывод данных сессии

    echo "<pre>";

    print_r ($_SESSION);

    echo "</pre>";

?>

<!-- ... -->

<!-- меню сайта -->

<p>

    <a href='/'>Главная</a> |
```

```
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['guid']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Главная страница сайта</h2>
<?php
    // если сессионные данные существуют
    if (isset($_SESSION['guid'])):
        // подключение к базе данных
        $mysqli = new mysqli ('localhost', 'root', '',
        'db_auth');
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
        `guid` = ?');
        $stmt->bind_param('s', $_SESSION['guid']);
        // получение результата
        $stmt->execute();
        $result = $stmt->get_result();
        // если запрос вернул запись
        if ($result->num_rows):
            $row = $result->fetch_assoc();
            $auth = true; // аутентификация успешна
        else:
```

```
            $auth = false; // если указанного guid нет в базе
        endif;
    else:
        $auth = false; // если нет сессионных данных
    endif;
    // если аутентификация успешна
    if (isset($auth) && $auth == true):
        echo "<p>Пользователь:<b> {$row['login']} </b><br>";
        echo "Вход выполнен с правами:<b> {$row['role']}
        </b></p>";
    else:
?>
        <!-- если аутентификация не состоялась -->
        <p>Для работы в системе необходима
        <b>аутентификация</b></p>
        <form action="auth.php" method="post">
            Логин: <input type="text" name="login" value=""><p>
            Пароль: <input type="text" name="pwd" value=""><p>
            <button>Войти</button>
        </form>
<?php
    endif;
?>
```

example_6. auth.php

```
<?php
    // настройки времени выполнения
```

```php
ini_set('session.use_cookies', 1);
ini_set("session.use_only_cookies", 1);
// ini_set("session.use_trans_sid", 1);
session_start();
// подключение к базе данных
$mysqli = new mysqli ('localhost', 'root', '', 'db_auth');
// создание, выполнение подготовленного запроса
$stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
`login` = ?');
$stmt->bind_param('s', $_POST['login']);
// получение результата
$stmt->execute();
$result = $stmt->get_result();
// если запрос вернул запись
if ($result->num_rows) {
    $row = $result->fetch_assoc();
    if (password_verify($_POST['pwd'], $row['pwd'])) {
        // набор символов для генерации идентификатора GUID
        $chars = '0123456789abcdefghijklmnopqrstuvwxyz';
        $guid = substr(str_shuffle($chars), 0, 10);
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('UPDATE `user_hash` SET
        `guid` = ? WHERE `login` = ?');
        $stmt->bind_param('ss', $guid, $_POST['login']);
        if ($stmt->execute()) {
            // сохраняем в сессию признак пользователя
            $_SESSION['guid'] = $guid;
```

```
                header('Location:/');
                exit;
            };
        } else $err = true;
    } else $err = true;
?>
<!-- ... -->
<?php
    if (isset($err)):
?>
        <!-- меню сайта -->
        <p>
            <a href='/'>Главная</a> |
            <a href='/page.php'>Страница</a>
            <?php
            // определяем пункт меню
            if (isset($_SESSION['guid']))
            echo '<a href="/logout.php"> | Выход</a>';
            ?>
        </p>
        <h3>Пользователь с такими данными в системе не
        найден</h3>
        <p><a href='/'>Попробовать еще раз</a></p>
<?php
    endif;
?>
```

example_6. page.php

```php
<?php
    // настройки времени выполнения
    ini_set('session.use_cookies', 1);
    ini_set("session.use_only_cookies", 1);
    // ini_set("session.use_trans_sid", 1);
    session_start();
    // тестовый вывод данных сессии
    echo "<pre>";
    print_r ($_SESSION);
    echo "</pre>";
?>
<!-- ... -->
<!-- меню сайта -->
<p>
    <a href='/'>Главная</a> |
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['guid']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Страница сайта</h2>
<?php
    // если сессионные данные существуют
```

```php
if (isset($_SESSION['guid'])):
    // подключение к базе данных
    $mysqli = new mysqli ('localhost', 'root', '',
    'db_auth');
    // создание, выполнение подготовленного запроса
    $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
    `guid` = ?');
    $stmt->bind_param('s', $_SESSION['guid']);
    // получение результата
    $stmt->execute();
    $result = $stmt->get_result();
    // если запрос вернул запись
    if ($result->num_rows):
        $row = $result->fetch_assoc();
        $auth = true; // аутентификация успешна
    else:
        $auth = false; // если указанного guid нет в базе
    endif;
else:
    $auth = false; // если нет сессионных данных
endif;
// если аутентификация успешна
if (isset($auth) && $auth == true):
    echo "<p>Пользователь:<b> {$row['login']} </b><br>";
    echo "Вход выполнен с правами:<b> {$row['role']}
    </b></p>";
else:
    // если аутентификация не состоялась
```

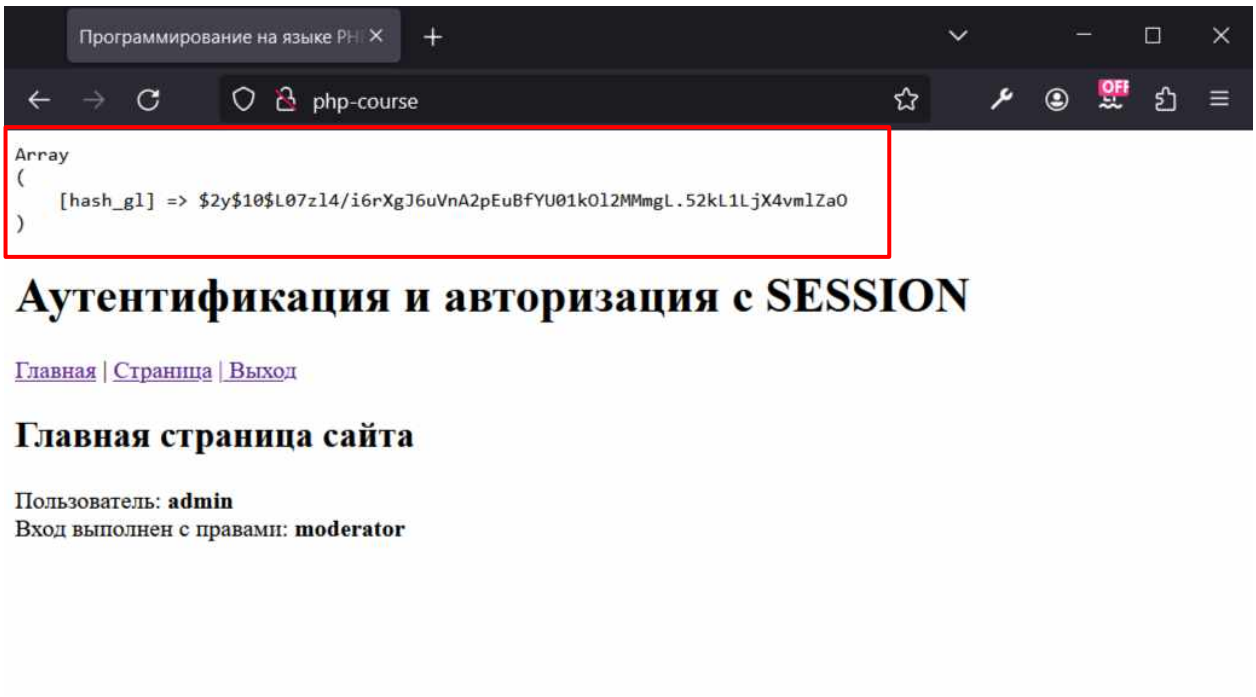
```
        echo "<p>Для работы в системе необходима
        <b>аутентификация</b></p>";
    endif;
?>
```

example_6. logout.php

```
<?php
    // удаляем данные, уничтожаем сессию
    session_start();
    session_unset();
    session_destroy();
    // echo "<pre>";
    // print_r($_SESSION);
    // echo "</pre>";
    // exit;
    header('Location:/');
    exit;
```

В демонстрационном примере **example_7** аутентификация выполняется с помощью **хеша пары идентификатор GUID-логин** (guid.login).

- Запись и сохранение в сессию хеша пары **идентификатор GUID - логин** (guid.login).
- Сессия передается через сессионный **cookie**. Настройки времени выполнения:
    - `ini_set('session.use_cookies', 1);`
    - `ini_set("session.use_only_cookies", 1);`
- Управление пунктом меню по результату аутентификации.



example_7. index.php

```php
<?php

    // настройки времени выполнения

    ini_set('session.use_cookies', 1);

    ini_set("session.use_only_cookies", 1);

    // ini_set("session.use_trans_sid", 1);

    session_start();

    // тестовый вывод данных сессии

    echo "<pre>";

    print_r ($_SESSION);

    echo "</pre>";

?>

<!-- ... -->

<!-- меню сайта -->

<p>

    <a href='/'>Главная</a> |
```

```
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['hash_gl']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Главная страница сайта</h2>
<?php
    // если сессионные данные существуют
    if (isset($_SESSION['hash_gl'])):
        // подключение к базе данных
        $mysqli = new mysqli ('localhost', 'root', '',
        'db_auth');
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
        `guid` = ?');
        $stmt->bind_param('s', $_SESSION['hash_gl']);
        // получение результата
        $stmt->execute();
        $result = $stmt->get_result();
        // если запрос вернул запись
        if ($result->num_rows):
            $row = $result->fetch_assoc();
            $auth = true; // аутентификация успешна
        else:
```

```
            $auth = false; // если указанного guid нет в базе
        endif;
    else:
        $auth = false; // если нет сессионных данных
    endif;
    // если аутентификация успешна
    if (isset($auth) && $auth == true):
        echo "<p>Пользователь:<b> {$row['login']} </b><br>";
        echo "Вход выполнен с правами:<b> {$row['role']}
        </b></p>";
    else:
?>
        <!-- если аутентификация не состоялась -->
        <p>Для работы в системе необходима
        <b>аутентификация</b></p>
        <form action="auth.php" method="post">
            Логин: <input type="text" name="login" value=""><p>
            Пароль: <input type="text" name="pwd" value=""><p>
            <button>Войти</button>
        </form>
<?php
    endif;
?>
```

example_7. auth.php

```
<?php
    // настройки времени выполнения
```

```php
ini_set('session.use_cookies', 1);
ini_set("session.use_only_cookies", 1);
// ini_set("session.use_trans_sid", 1);
session_start();
// подключение к базе данных
$mysqli = new mysqli ('localhost', 'root', '', 'db_auth');
// создание, выполнение подготовленного запроса
$stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
`login` = ?');
$stmt->bind_param('s', $_POST['login']);
// получение результата
$stmt->execute();
$result = $stmt->get_result();
// если запрос вернул запись
if ($result->num_rows) {
    $row = $result->fetch_assoc();
    if (password_verify($_POST['pwd'], $row['pwd'])) {
        // набор символов для генерации идентификатора GUID
        $chars = '0123456789abcdefghijklmnopqrstuvwxyz';
        $guid = substr(str_shuffle($chars), 0, 10);
        $hash_gl = password_hash($guid.$row['login'],
        PASSWORD_DEFAULT);
        // создание, выполнение подготовленного запроса
        $stmt = $mysqli->prepare('UPDATE `user_hash` SET
        `guid` = ? WHERE `login` = ?');
        $stmt->bind_param('ss', $hash_gl, $_POST['login']);
        if ($stmt->execute()) {
            // сохраняем в сессию признак пользователя
```

```
                $_SESSION['hash_gl'] = $hash_gl;
                header('Location:/');
                exit;
            };
        } else $err = true;
    } else $err = true;
?>
<!-- ... -->
<?php
    if (isset($err)):
?>
        <!-- меню сайта -->
        <p>
            <a href='/'>Главная</a> |
            <a href='/page.php'>Страница</a>
            <?php
                // определяем пункт меню
                if (isset($_SESSION['hash_gl']))
                    echo '<a href="/logout.php"> | Выход</a>';
            ?>
        </p>
        <h3>Пользователь с такими данными в системе не
        найден</h3>
        <p><a href='/'>Попробовать еще раз</a></p>
<?php
    endif;
?>
```

example_7. page.php

```
<?php
    // настройки времени выполнения
    ini_set('session.use_cookies', 1);
    ini_set("session.use_only_cookies", 1);
    // ini_set("session.use_trans_sid", 1);
    session_start();
    // тестовый вывод данных сессии
    echo "<pre>";
    print_r ($_SESSION);
    echo "</pre>";
?>
<!-- ... -->
<!-- меню сайта -->
<p>
    <a href='/'>Главная</a> |
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
        // определяем пункт меню
        if (isset($_SESSION['hash_gl']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Страница сайта</h2>
<?php
    // если сессионные данные существуют
```

```php
if (isset($_SESSION['hash_gl'])):
    // подключение к базе данных
    $mysqli = new mysqli ('localhost', 'root', '',
    'db_auth');
    // создание, выполнение подготовленного запроса
    $stmt = $mysqli->prepare('SELECT * FROM `user_hash` WHERE
    `guid` = ?');
    $stmt->bind_param('s', $_SESSION['hash_gl']);
    // получение результата
    $stmt->execute();
    $result = $stmt->get_result();
    // если запрос вернул запись
    if ($result->num_rows):
        $row = $result->fetch_assoc();
        $auth = true; // // аутентификация успешна
    else:
        $auth = false; // если указанного guid нет в базе
    endif;
else:
    $auth = false; // если нет сессионных данных
endif;
// если аутентификация успешна
if (isset($auth) && $auth == true):
    echo "<p>Пользователь:<b> {$row['login']} </b><br>";
    echo "Вход выполнен с правами:<b> {$row['role']}
    </b></p>";
else:
    // если аутентификация не состоялась
```

```
        echo "<p>Для работы в системе необходима
        <b>аутентификация</b></p>";
    endif;
?>
```

example_7. logout.php

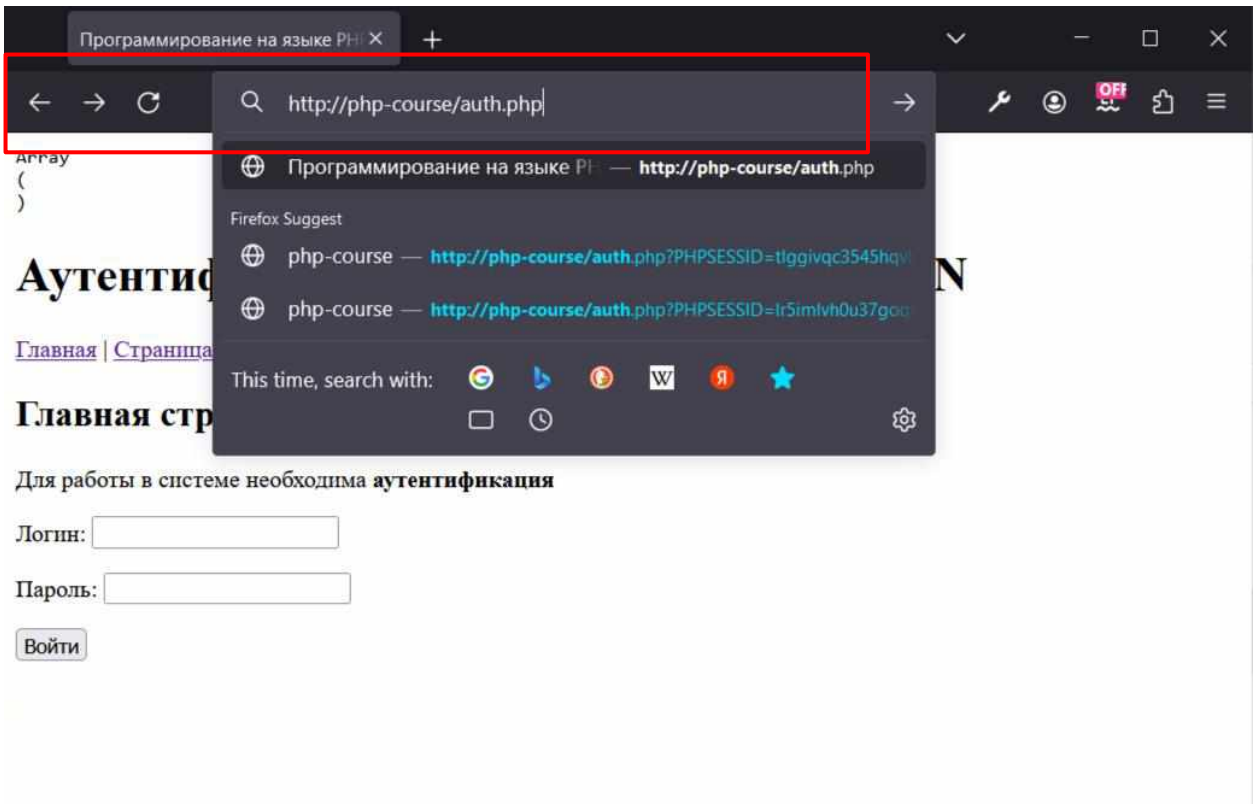
```
<?php
    // удаляем данные, уничтожаем сессию
    session_start();
    session_unset();
    session_destroy();
    // echo "<pre>";
    // print_r($_SESSION);
    // echo "</pre>";
    // exit;
    header('Location:/');
    exit;
```

Пользователь коварен

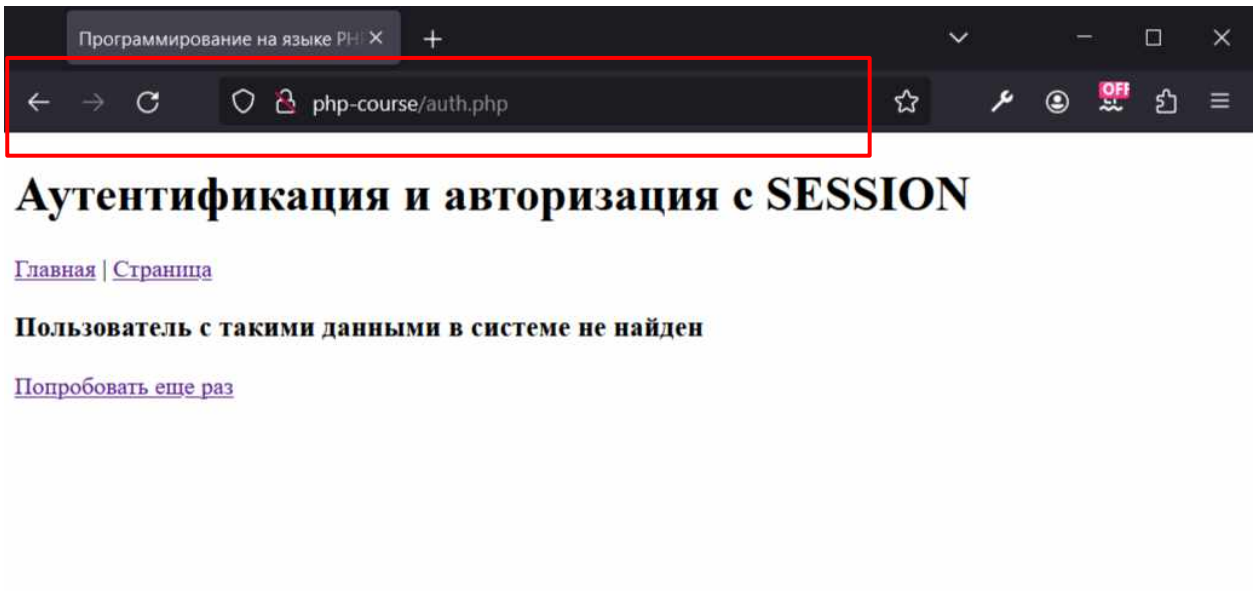
При тестировании приложений мы все время кликали по пунктам **навигационного меню**. Но кто мешает пользователю ввести имя файла сценария непосредственно в адресную строку.

Например, имя файла **auth.php**.

Попробуйте на примере файлов из примера **example_7**.



Результат такого перехода представлен на следующем скриншоте.



Сценарий файла **auth.php** выдал стандартное сообщение: "Пользователь с такими данными в системе не найден". С какими такими?

- пустой логин;

- пустой пароль.

Но в данной ситуации причина появления сообщения совсем другая, **попытка обхода системы аутентификации**. Сценарий ждал массива $_**POST** с данными логина и пароля.

Нет простых решений этой и множества других проблем безопасной работы сценариев. Необходим **комплекс мер**, по защите разрабатываемых приложений:

- обработка ситуации наличия сырых (необработанных, raw) или полного отсутствия данных;
- валидация данных;
- санитизация данных;
- создание безопасных сессий;
- своевременное удаление сессий;
- контроль переходов между страницами приложения;
- и многое другое.

Доработаем код примера **example_7**. В демонстрационном примере **example_8** добавим:

- код файла **auth.php**, отслеживающий наличие аутентификационных данных массива $_**POST**;
- файл **error.php**.

example_8. auth.php

```
<?php

    // настройки времени выполнения

    ini_set('session.use_cookies', 1);

    ini_set("session.use_only_cookies", 1);

    // ini_set("session.use_trans_sid", 1);

    // проверим наличие аутентификационных данных массива $_POST

    if (
```

```
        !isset($_POST['login']) &&
        !isset($_POST['pwd'])
    )
    {
        header('Location:/error.php');
        exit;
    }
    session_start();
    // подключение к базе данных
    $mysqli = new mysqli ('localhost', 'root', '', 'db_auth');
    // ...
```

example_8. error.php

```
<?php
    // настройки времени выполнения
    ini_set('session.use_cookies', 1);
    ini_set("session.use_only_cookies", 1);
    // ini_set("session.use_trans_sid", 1);
    session_start();
?>
<!-- ... -->
<!-- меню сайта -->
<p>
    <a href='/'>Главная</a> |
    <a href='/page.php'>Страница</a>
    <?php
        // если сессионные данные существуют
```

```
        // определяем пункт меню
        if (isset($_SESSION['hash_gl']))
            echo '<a href="/logout.php"> | Выход</a>';
    ?>
</p>
<h2>Так не работает!!!</h2>
<img src="images/error.jpg" width="300px">
```

Остальные файлы без изменений. Теперь попытка обойти аутентификацию приводит к переадресации на файл **error.php**.