

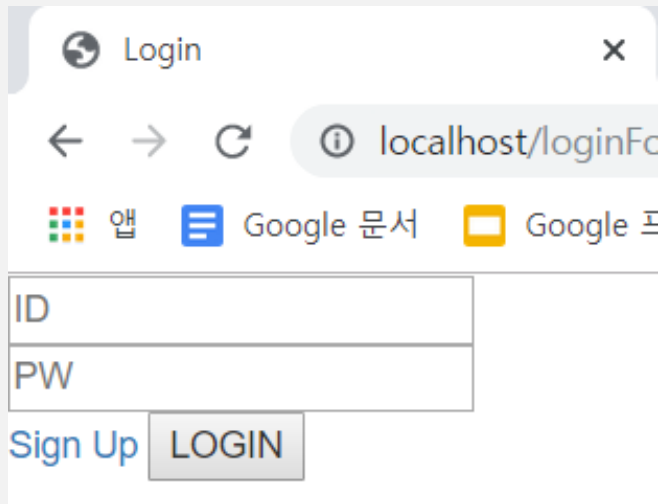
Web Hacking

CONTENTS

Contents 1

- 홈페이지 구축

- C:\Bitnami\wampstack-7.3.6-2\apache2의 기존 **htdocs** 파일 삭제 후 알집 htdocs 풀기



Login

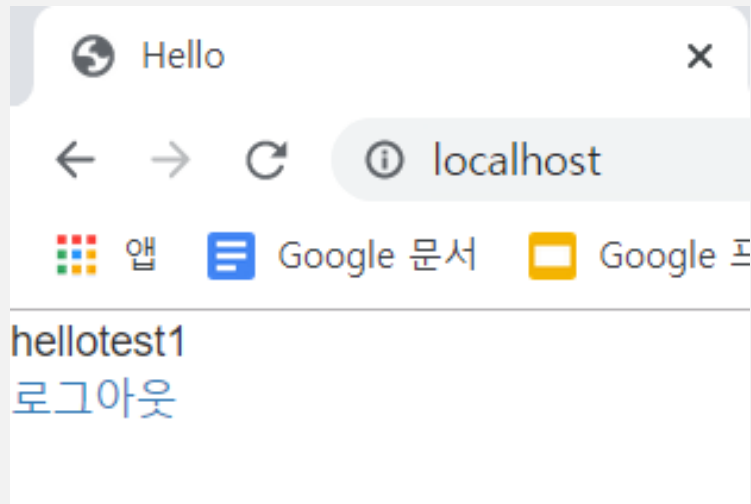
localhost/loginFc

ID

PW

Sign Up LOGIN

- 로그인 창



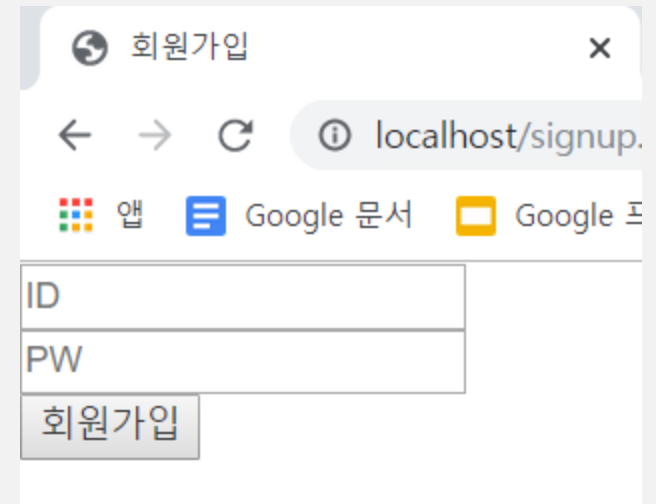
Hello

localhost

hellotest1

로그아웃

- 로그아웃 창



회원가입

localhost/signup.

ID

PW

회원가입

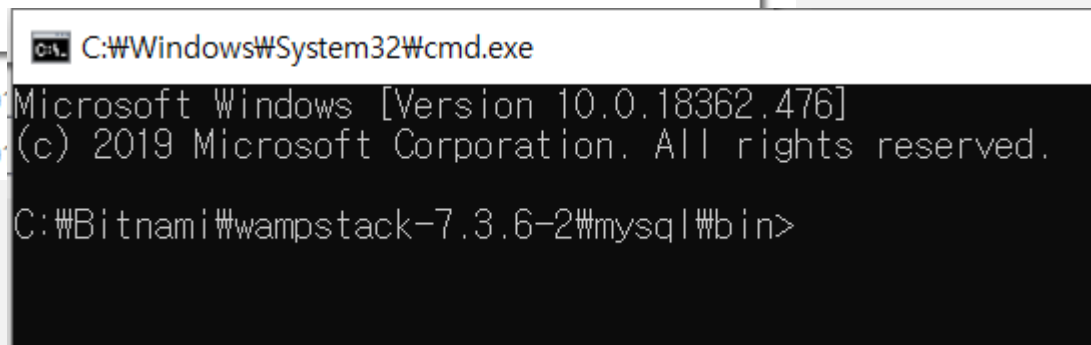
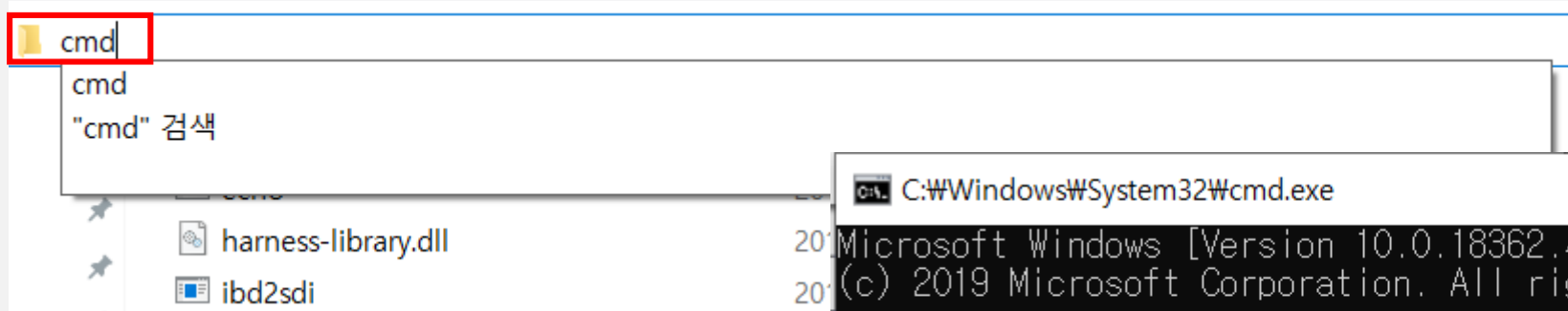
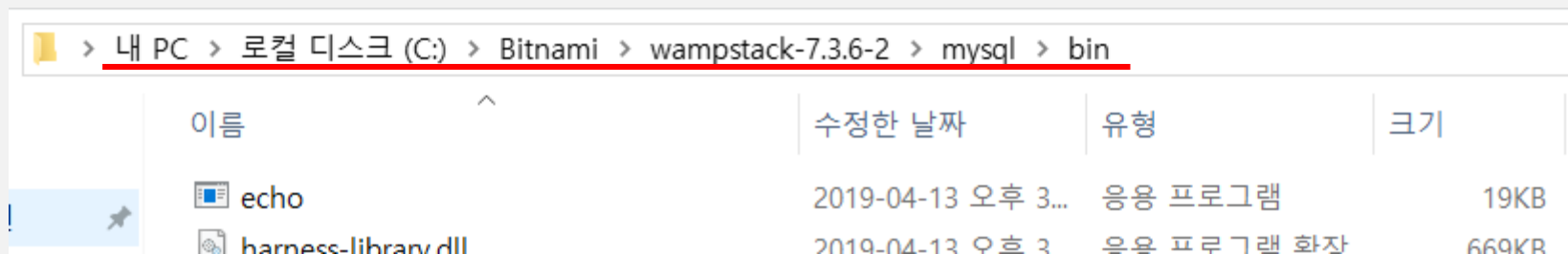
- 회원가입 창

- dbConnect.php 파일에서 "sql0202"부분 본인 mysql의 비밀번호로 변경 -> "password"



```
1 <?php
2
3     $conn = mysqli_connect("localhost", "root", "sql0202");
4     if(!$conn){
5         die('connect Error : MySQL');
6     }
7
8     mysqli_select_db($conn, $dbName);
9
10    ?>
```

- C:\Bitnami\wampstack-7.3.6-2\mysql\bin에서 cmd창 실행



- Apache에서 제공하는 mysql DB에 접근

```
C:\Windows\System32\cmd.exe - mysql -u root -p
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Bitnami\wampstack-7.3.6-2\mysql\bin>mysql -u root -p
Enter password: *****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 19
Server version: 8.0.16 MySQL Community Server - GPL

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

- User 데이터 베이스의 account 테이블을 조회하여 현재 회원정보 확인

```
mysql> use User;
Database changed
mysql> show tables;
+-----+
| Tables_in_user |
+-----+
| account         |
| board           |
| test            |
+-----+
3 rows in set (0.00 sec)

mysql> select * from account;
+----+-----+-----+
| id | username | userpass |
+----+-----+-----+
| 16 | test1    | test1    |
| 17 | test2    | test2    |
+----+-----+-----+
2 rows in set (0.00 sec)
```

- User 데이터 베이스가 없다면 User 데이터 베이스와 account 테이블 생성

```
mysql> CREATE DATABASE User;
Query OK, 1 row affected (0.03 sec)

mysql> use User;
Database changed
mysql> CREATE TABLE account
-> (
-> id int NOT NULL AUTO_INCREMENT,
-> username char(32),
-> userpass char(32),
-> PRIMARY KEY(id)
-> );
Query OK, 0 rows affected (0.09 sec)

mysql> show tables;
+-----+
| Tables_in_user |
+-----+
| account         |
+-----+
1 row in set (0.06 sec)
```


이름	수정한 날짜	유형	크기
css	2019-06-30 ...	파일 폴더	
img	2019-07-01 ...	파일 폴더	
js	2019-06-30 ...	파일 폴더	
index.php	2019-07-01 ...	PHP 파일	1KB
login.php	2019-07-01 ...	PHP 파일	1KB
loginForm.html	2019-07-01 ...	Chrome HTML Do...	1KB
logout.php	2019-07-01 ...	PHP 파일	1KB
signup.html	2019-07-01 ...	Chrome HTML Do...	1KB
signup.php	2019-07-01 ...	PHP 파일	1KB

- 기존의 소스 코드들은 <html>, <head> 태그 태의 값이 거의 비슷하여 **중복**됨
- 또한 소스 코드 전부를 한 곳에 두고 관리하는 것은 복잡하며 이후 **수정하기도 힘들**
- 따라서 **각자 최소한의 기능을 가진 모듈로 분할**하여 나누고 필요할 때 불러서 쓰는 것이 좋음
- 기능 혹은 성격에 따라서 폴더도 나누고 소스코드 파일도 나누어서 저장

```
loginForm.html x logout.php index.php x signup.html signup.php login.php
<!DOCTYPE html>
<html>
<head>
  <title>로그인 페이지</title>
  <meta charset="utf-8">
  <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.2/css/bootstrap.min.css">
</head>
<body>
  <form action="login.php" method="POST">
    <input type="text" name="id" placeholder="ID"><br>
    <input type="password" name="password" placeholder="PW"><br>
    <a href="signup.html">Sign Up</a>
    <input class="btn btn-default" type="submit" value="로그인">
  </form>
</body>
</html>
```

- 빨간 박스의 내용은 대부분의 소스코드에서 사용되므로 모듈로 따로 빼는 것이 좋다. -> head.php

```
head.php      logout.php      index.php

<!DOCTYPE html>
<html>
<head>
  <title><?php echo $title; ?></title>
  <meta charset="utf-8">
  <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css">
</head>
```

```
head.php      loginForm.html      logout.php      index.php

<?php
$title = "Login";
require_once('head.php');
?>

<body>
  <form action="login.php" method="POST">
    <input type="text" name="id" placeholder="ID"><br>
    <input type="password" name="password" placeholder="PW"><br>
    <a href="signup.html">Sign Up</a>
    <input class="btn btn-default" type="submit" value="로그인">
  </form>
</body>
</html>
```

- 중복되는 내용을 head.php 파일로 저장하고, 페이지 마다 title이 다를 수 있으므로 title부분은 php변수로 출력
- loginForm.html에서 require_once 함수를 사용하여 head.php파일을 불러와 사용

```
<?php
$conn = mysqli_connect("localhost", "root", 설치 시 설정한 비밀번호);
if(!$conn){
    die('Connect Error : MySQL');
}
```

```
mysqli_select_db($conn, "User");
```






```
$query = "SELECT * FROM account WHERE username = ";
$result = mysqli_query($conn, $query);
if(mysqli_num_rows($result) > 0){
    echo '<script>alert("이미 존재하는 아이디 입니다");' . "\n";
    echo 'history.back();</script>';
    exit;
}
```

```
dbConnect.php  head.php  loginForm.html

<?php
$conn = mysqli_connect($server, $user, $password);
if(!$conn){
    die('Connect Error : MySQL');
}

mysqli_select_db($conn, $dbName);
?>
```

- Mysql에 연동하기 위하여 사용하는 부분도 회원가입, 로그인 등 중복이 많으니 dbConnect.php로 모듈화함

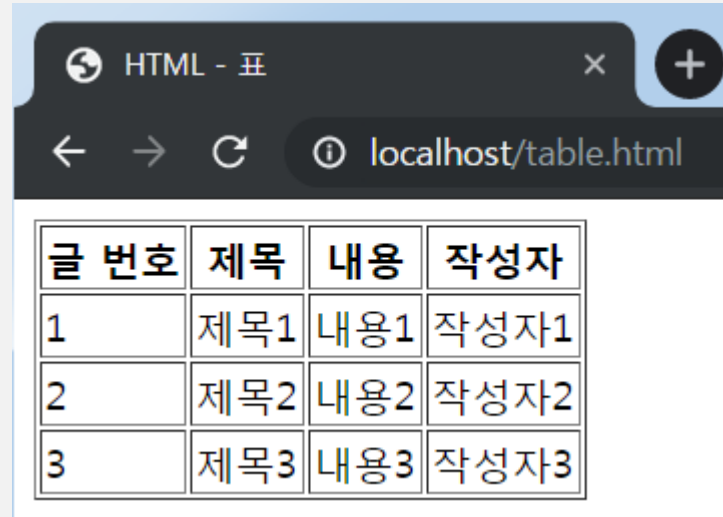
이름	수정한 날짜	유형	크기
 process	2019-11-25 오전...	파일 폴더	
 template	2019-07-08 오전...	파일 폴더	
 index	2019-11-25 오전...	PHP 파일	1KB
 loginForm	2019-11-25 오전...	Chrome HTML D...	1KB
 signup	2019-07-05 오전...	Chrome HTML D...	1KB

- process 폴더에는 로그인, 회원가입 등 실질적으로 데이터 베이스를 처리하는 php를 모아둠
- template 폴더에는 head.php를 두어 다른 소스 코드에서도 많이 불러오는 소스를 넣음

No.	제목	첨부파일	작성자	작성일	조회
133	[제목] 게시글 제목입니다. 		운영자	2019-06-25	1,888
132	[제목] 게시글 제목입니다. 		운영자	2019-06-24	4,020
131	게시글 제목입니다. 		운영자	2019-06-25	5,025
130	게시글 제목입니다. 		운영자	2019-06-13	7,617
129	게시글 제목입니다. 		운영자	2019-06-11	4,928
128	게시글 제목입니다. 		운영자	2019-06-12	6,900

- 현재는 login 이후 아무런 기능이 없으므로 login을 하면 게시판을 이용할 수 있도록 구현
- 구현할 기능은 게시판 글 목록, 조회, 작성, 삭제, 수정
- 게시판은 표를 이용하여 보여 지기 때문에 HTML에서 표를 구현하는 것을 알아야함

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <title>HTML - 표</title>
5   <meta charset="utf-8">
6 </head>
7 <body>
8   <table border="1">
9     <tr>
10      <th>글 번호</th>
11      <th>제목</th>
12      <th>내용</th>
13      <th>작성자</th>
14    </tr>
15    <tr>
16      <td>1</td>
17      <td>제목1</td>
18      <td>내용1</td>
19      <td>작성자1</td>
20    </tr>
21    <tr>
22      <td>2</td>
23      <td>제목2</td>
24      <td>내용2</td>
25      <td>작성자2</td>
26    </tr>
27    <tr>
28      <td>3</td>
29      <td>제목3</td>
30      <td>내용3</td>
31      <td>작성자3</td>
32    </tr>
33  </table>
34 </body>
35 </html>
```



The screenshot shows a web browser window with the title "HTML - 표". The address bar displays "localhost/table.html". The rendered table is as follows:

글 번호	제목	내용	작성자
1	제목1	내용1	작성자1
2	제목2	내용2	작성자2
3	제목3	내용3	작성자3

- <table> 태그를 이용하여 표를 생성할 수 있음
- <tr> 태그는 table의 row(행)을 의미
- <th> 태그는 table의 head를 의미하여 표의 제목을 나타냄
- <td> 태그는 table의 data를 의미하며 실질적인 값

```
mysql> use user;
Database changed
mysql> CREATE TABLE board
-> (
-> id int NOT NULL AUTO_INCREMENT,
-> title char(32),
-> contents text,
-> author char(32),
-> createTime datetime,
-> PRIMARY KEY(id)
-> );
Query OK, 0 rows affected (0.38 sec)
```

```
mysql> desc board;
+-----+-----+-----+-----+-----+-----+
| Field      | Type      | Null | Key | Default | Extra          |
+-----+-----+-----+-----+-----+-----+
| id         | int(11)   | NO   | PRI | NULL    | auto_increment |
| title      | char(32)  | YES  |     | NULL    |                |
| contents   | text      | YES  |     | NULL    |                |
| author     | char(32)  | YES  |     | NULL    |                |
| createTime | datetime  | YES  |     | NULL    |                |
+-----+-----+-----+-----+-----+-----+
```

5 rows in set (0.01 sec)

- mysql에서 게시글을 저장할 table을 만들어 줘야함
- Id는 글의 번호 , title은 글의 제목, contents는 글의 내용, author은 작성자, createTime은 작성시간


```
board.html
1 <?php
2     $title = "Board";
3     require_once($_SERVER['DOCUMENT_ROOT'] . '/template/head.php');
4     ?>
5
6 <body>
7     <div id = "board">
8         <table class = "table table-striped">
9             <tr>
10                 <th>글 번호 </th>
11                 <th>제목</th>
12                 <th>작성자</th>
13                 <th>작성일</th>
14             </tr>
15
16             <?php
17                 require_once($_SERVER['DOCUMENT_ROOT'] . "/process/board.php");
18                 $number = 0;
19                 while($row = mysqli_fetch_array($result)){
20                     $number += 1;
21                     echo "<tr>";
22                     echo "<td>{$number}</td>";
23                     echo "<td><a href='\"/view.html?id={$row['id']}&no={$number}\">{$row['title']}</a></td>";
24                     echo "<td>{$row['author']}</td>";
25                     echo "<td>{$row['createTime']}</td>";
26                     echo "</tr>";
27                 }
28             ?>
29         </table>
30         <a class = "btn btn-default" href = "/write.html" role = button>글쓰기</a>
31         <a class = "btn btn-default" href = "/process/logout.php" role = button>로그아웃</a>
32
33     </div>
34 </body>
35 </html>
```

- \$number로 글 번호 출력
- \$row가 존재하면 행을 만들도록 반복문으로 작성
- Contents를 보기 위해 제목을 클릭하면 페이지가 넘어가도록 <a>태그 설정

```
board.html x board.php x
1 <?php
2     $dbName = "User";
3     require_once('dbConnect.php');
4
5     if(isset($condition)){
6         $query = "SELECT * FROM board WHERE " . $condition;
7     }
8     else{
9         $query = "SELECT * FROM board";
10    }
11
12    $result = mysqli_query($conn, $query);
13
14    mysqli_close($conn);
15    ?>
```

- Mysql과 연동하고 데이터를 가져오는 코드를 process/board.php에 작성

```
index.php
1 <?php
2     $title = "Hello";
3     require_once($_SERVER['DOCUMENT_ROOT'] . "/template/head.php");
4
5     if(!isset($_SESSION['user'])){
6         echo '<script>alert("로그인이 필요합니다.");';
7         echo 'location.href="/loginForm.html";</script>';
8     }
9     ?>
10
11
12     <body>
13         안녕하세요! <?php echo $_SESSION['user']; ?> 님<br>
14         <a class ="btn btn-default" href = "/board.html" role = "button"> 게시판 바로가기 </a>
15     </body>
16 </html>
```

- index.php를 다음과 같이 변경
- 로그인 시 게시판으로 연결되는 버튼을 만들어 줌

Contents 1

홈페이지 구축

게시글 조회

```
board.html x view.html x
1 <?php
2     $title = "Board";
3     require_once($_SERVER['DOCUMENT_ROOT'] . "/template/head.php");
4     ?>
5
6 <body>
7     <div id = "board">
8         <?php
9             $condition = "id=" . $_GET['id'];
10            require_once($_SERVER['DOCUMENT_ROOT'] . "/process/board.php");
11            $row = mysqli_fetch_array($result);
12
13            $no = htmlspecialchars($_GET['no']);
14            $row['title'] = htmlspecialchars($row['title']);
15            $row['author'] = htmlspecialchars($row['author']);
16            $row['contents'] = htmlspecialchars($row['contents']);
17
18        ?>
19
20        <table class="table table-bordered">
21            <tr>
22                <th>글 번호</th>
23                <td><?php echo $_GET['no']; ?></td>
24            </tr>
25
26            <tr>
27                <th>제목</th>
28                <td><?php echo $row['title']; ?></td>
29            </tr>
30            <tr>
31                <th>작성자</th>
32                <td><?php echo $row['author']; ?></td>
33            </tr>
34            <tr>
35                <th>작성일</th>
36                <td><?php echo $row['createTime']; ?></td>
37            </tr>
38            <tr>
39                <th colspan="2">내용</th>
40            </tr>
41            <tr>
42                <td colspan="2"><?php echo $row['contents']; ?></td>
43            </tr>
44        </table>
45        <a class="btn btn-default" href="/board.html" role="button">글 목록</a>
46        <?php
47            if($row['author'] === $_SESSION['user']){
48                echo "<a class='btn btn-default' href='/modify.html?id={$row['id']}&no={$_GET['no']}' role='button'>수정하기</a> ";
49                echo "<a class='btn btn-default' href='/process/delete.php?id={$row['id']}' role='button'>삭제하기</a>";
50            }
51        ?>
52    </div>
53 </body>
</html>
```

- Get Method로 id를 인자로 받아 database에서 조회

```
index.php write.html x
1 <?php
2     $title = "Write";
3     require_once ($_SERVER['DOCUMENT_ROOT'] . "/template/head.php");
4     ?>
5
6     <body>
7         <div id = "board">
8             <form action = "/process/write.php" method = "POST">
9                 <table class = "table table-bordered">
10                     <tr>
11                         <th>제목</th>
12                         <td><input type="text" class="form-control" name="title"> </td>
13                     </tr>
14                     <tr>
15                         <th>작성자</th>
16                         <td><?php echo $_SESSION['user']; ?></td>
17                     </tr>
18                     <tr>
19                         <th colspan="2">내용</th>
20                     </tr>
21                     <tr>
22                         <td colspan="2"><textarea class="form-control" name="contents" rows="5"></textarea></td>
23                     </tr>
24                 </table>
25                 <input class="btn btn-default" type="submit" value="완료">
26             </form>
27         </div>
28     </body>
29 </html>
```

- 작성자는 로그인한 유저이기 때문에 session에서 가져오며 제목과 내용만 입력 받음
- 입력을 모두 받은 뒤 완료버튼을 누르면 process/write.php로 인자 전달

```
1 <?php
2 session_start();
3 $dbName = "User";
4 require_once('dbConnect.php');
5
6 $query = "
7     INSERT INTO board(title, contents, author, createTime)
8     VALUES (
9         '$_POST['title']}',
10        '$_POST['contents']}',
11        '$_SESSION['user']}',
12        now()
13    )
14 ";
15 $result = mysqli_query($conn, $query);
16 mysqli_close($conn);
17 ?>
18
19 <script type = "text/javascript">
20     alert("글을 작성하였습니다.");
21     location.href = "/board.html";
22 </script>
```

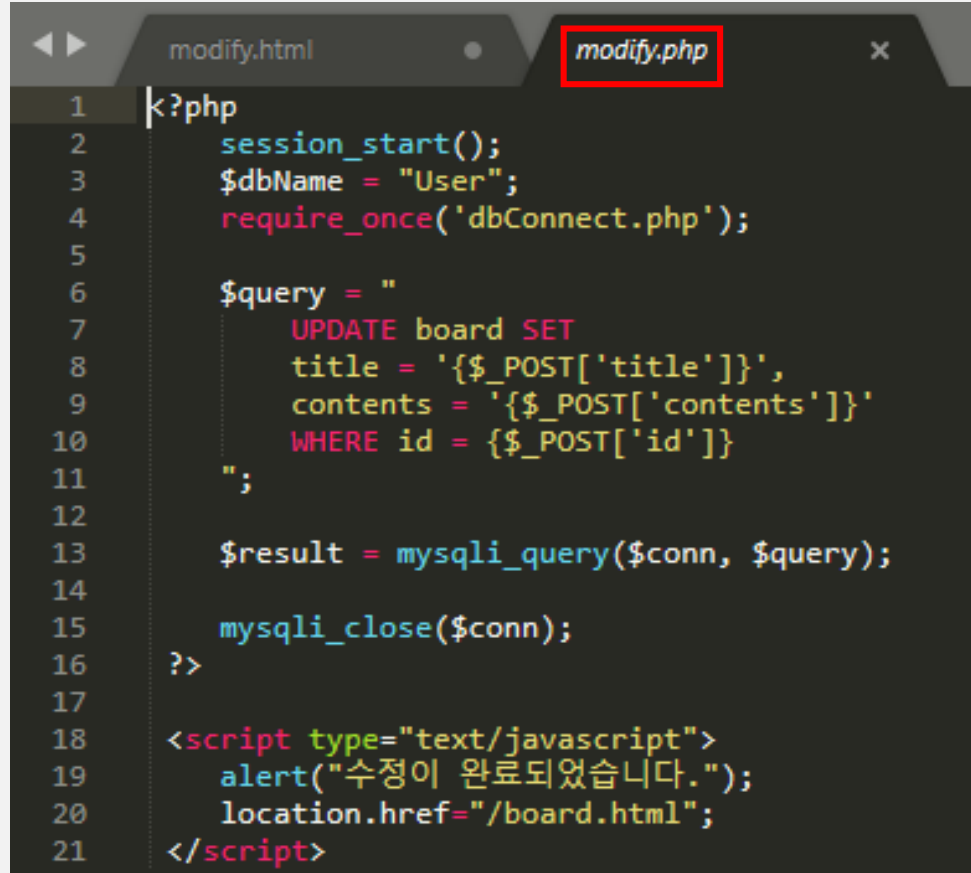
- POST method의 인자로 넘어온 title과 contents, session값을 이용하여 작성자를 삽입
- 글을 작성한 뒤에는 게시판 목록 페이지로 이동

Contents 1

홈페이지 구축

게시글 수정

```
modify.html
1 <?php
2 $title = "게시판 수정";
3 require_once($_SERVER['DOCUMENT_ROOT'] . "/template/head.php");
4 ?>
5
6 <body>
7     <div id="board">
8         <?php
9             $condition = "id=" . $_GET['id'];
10            require_once($_SERVER['DOCUMENT_ROOT'] . "/process/board.php");
11            $row = mysqli_fetch_array($result);
12            ?>
13            <form action = "/process/modify.php" method = "POST">
14                <table class="table table-bordered">
15                    <tr>
16                        <th>글 번호</th>
17                        <th><?php echo $_GET['no']; ?></th>
18                    </tr>
19                    <tr>
20                        <th>제목</th>
21                        <td><input type="text" class="form-control" name="title" value=<?php echo "{$row['title']}\n"; ?></td>
22                    </tr>
23                    <tr>
24                        <th>작성자</th>
25                        <td><?php echo $row['author']; ?></td>
26                    </tr>
27                    <tr>
28                        <th>작성일</th>
29                        <td><?php echo $row['createTime']; ?></td>
30                    </tr>
31                    <tr>
32                        <th colspan="2">내용</th>
33                    </tr>
34                    <tr>
35                        <td colspan="2"><textarea class="form-control" name="contents" rows="5"><?php echo $row['contents']; ?></textarea></td>
36                    </tr>
37                </table>
38                <input type="hidden" name="id" value=<?php echo "{$_GET['id']}\n"; ?>
39                <input class="btn btn-default" type="submit" value="완료">
40            </form>
41        </div>
42    </body>
43 </html>
```



```
1 <?php
2     session_start();
3     $dbName = "User";
4     require_once('dbConnect.php');
5
6     $query = "
7         UPDATE board SET
8         title = '{$_POST['title']}',
9         contents = '{$_POST['contents']}'
10        WHERE id = {$_POST['id']}
11    ";
12
13    $result = mysqli_query($conn, $query);
14
15    mysqli_close($conn);
16 ?>
17
18 <script type="text/javascript">
19     alert("수정이 완료되었습니다.");
20     location.href="/board.html";
21 </script>
```

- UPDATE SET 구문을 통해 글을 수정
- 글을 수정한 뒤 게시판으로 돌아 감


```
1 k?php
2 session_start();
3 $dbName = "User";
4 require_once('dbConnect.php');
5
6 $query = "
7     DELETE FROM board WHERE id = {$_GET['id']}
8 ";
9
10 $result = mysqli_query($conn, $query);
11
12 mysqli_close($conn);
13 ?>
14
15 <script type="text/javascript">
16     alert("삭제가 완료되었습니다.");
17     location.href="/board.html";
18 </script>
```

- DELETE FROM 구문을 통해 글을 삭제
- 글을 삭제한 뒤 게시판으로 돌아 감

```
signup.php
1 <?php
2     $dbName = "User";
3     require_once('dbConnect.php');
4
5     $query = "SELECT * FROM account WHERE username = '{$_POST['username']}'";
6     $result = mysqli_query($conn, $query);
7     if(mysqli_num_rows($result) > 0){
8         echo "<script>alert('이미 존재하는 아이디 입니다.');";
9         echo 'history.back();</script>';
10        exit;
11    }
12
13    $password = password_hash($_POST['password'], PASSWORD_DEFAULT);
14
15    $query = "
16        INSERT INTO account(username, userpass)
17        VALUES('".$_POST['id']."', '$_POST['password'].');
18    ";
19    $result = mysqli_query($conn, $query);
20    if(!$result){
21        echo "<script>alert('회원 가입에 실패하였습니다.');";
22        echo "history.back();</script>";
23    }
24    ?>
25
26    <script type="text/javascript">
27        alert("회원 가입에 성공하였습니다. 로그인 페이지로 이동합니다.");
28        location.href="/loginForm.html";
29    </script>
```

```
mysql> select * from account;
```

id	username	userpass
16	test1	test1
17	test2	test2
18	user123	\$2y\$10\$Wg.TfhzbeZs98mD4p5AZLuv2666e0hucJus7rcVyLD8jMn/qKXaPi

3 rows in set (0.00 sec)

- password_hash() 함수로 password를 평문이 아닌 hash값으로 DB에 저장
- 관리자가 데이터베이스 조회를 통해 이용자의 password를 조회할 수 없음

감사합니다