

# 웹 게시판 개발

20204 김태훈

01

게시판 소개

02

기능 및 코드 소개

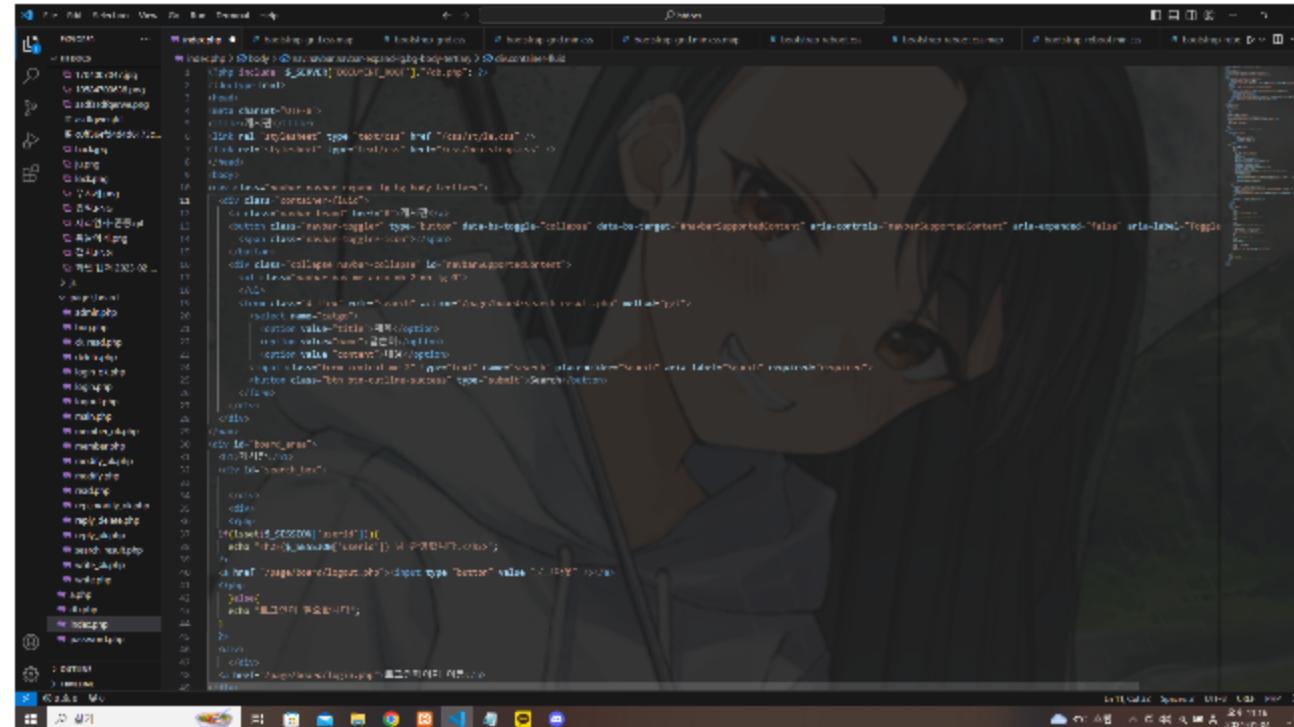
03

문제점 및 해결

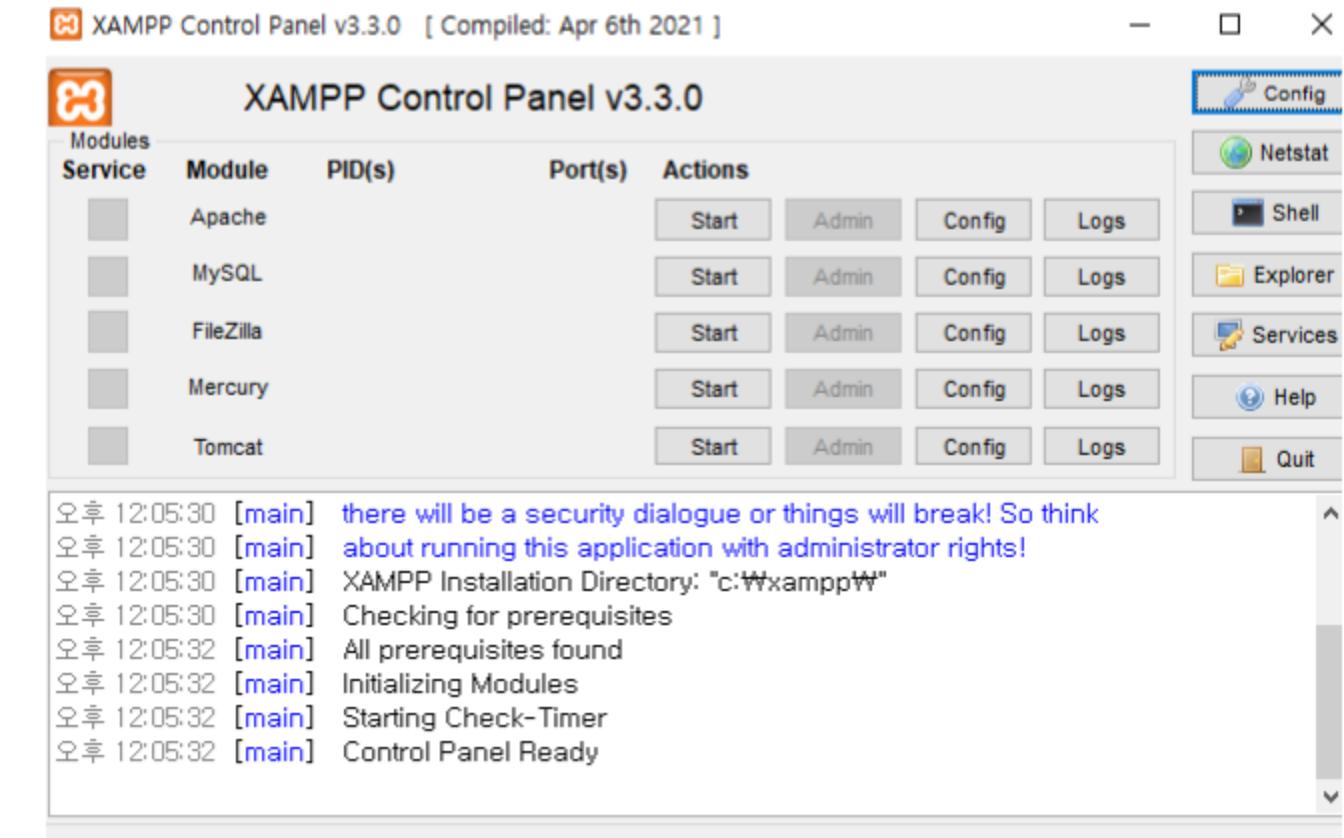
04

질문 및 마무리

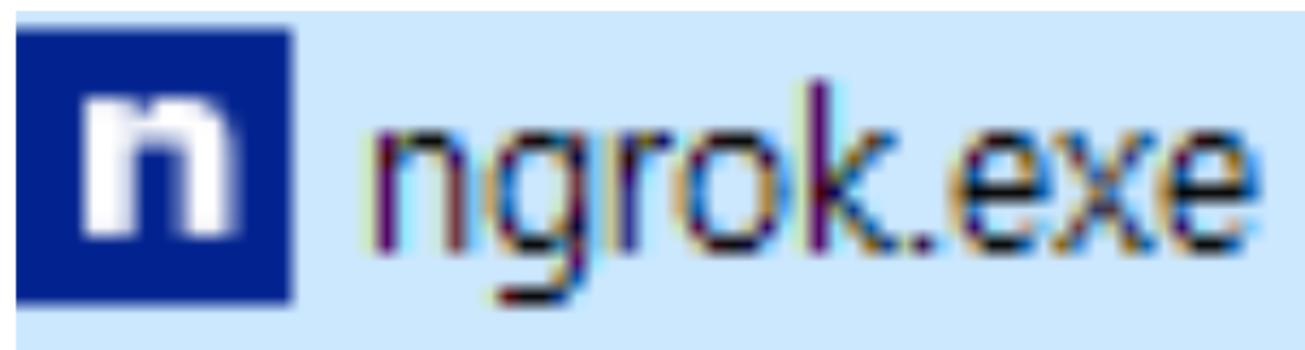
## 개발 환경 및 사용 언어



vscode 꺼드럭



apache + php + mysql let's go



배포를 위한 ngrok

# 게시판 소개

## 주요 페이지

글, 댓글 쓰고 지우고 수정하고 삭제하고 아무튼 꺼드럭

The screenshot shows a web browser window with the URL <http://127.0.0.1:8080/>. The title bar says "게시판". The main content area is titled "게시판" and includes a search bar with dropdown options "제목" and "Search". Below the search bar is a table with columns: 글쓴이, 제목, 작성일, 조회수. The table contains five rows of post data. At the bottom of the page are navigation links like "처음" and "마지막" and a "글쓰기" button.

The screenshot shows a post detail page. The post ID is 1, posted on 2023-02-26 at 15:58. The content of the post is "asdasd" and it includes a small image thumbnail. Below the post are buttons for "[목록으로]", "[수정]", and "[삭제]". To the right of the post, there is a section titled "댓글목록" (Comment List) which lists three comments: "a", "w", and "o". Each comment has a timestamp, a link to edit or delete it, and a "수정" (Edit) link.



## 메인 페이지

글 읽을 수 있는 페이지

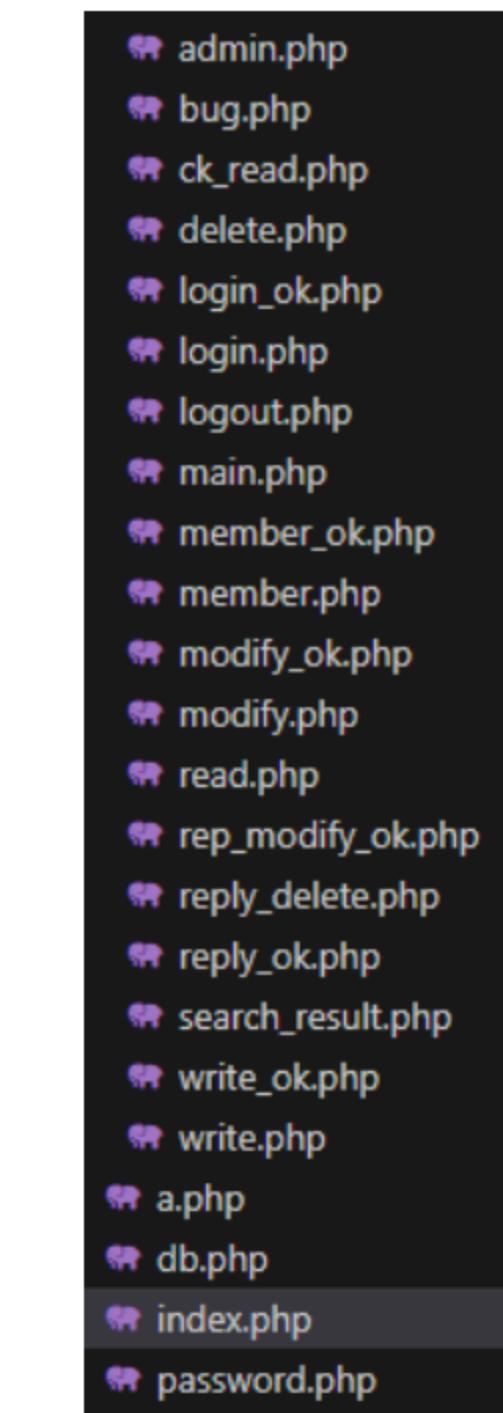
The screenshot shows a Windows desktop environment. On the left is a taskbar with pinned icons. On the right is a window with a login form. It has fields for "아이디" and "비밀번호", a large empty text input field, and a "댓글" (Comment) button.

실제로 접속 해보자

(필요 시 연락)

## 기능 및 코드 소개

### 여러 php 파일들



A screenshot of a code editor with two tabs open. Both tabs show PHP code. The tabs are labeled 'index.php' and 'index.php'. The code contains various PHP functions like 'echo', 'if', 'for', and database queries using MySQL syntax.

A screenshot of a Microsoft Edge browser window. The address bar shows 'http://127.0.0.1:5000/'. The page content includes a search bar with placeholder text 'Search' and a button labeled 'Search'. Below the search bar, there is some explanatory text and a link to 'http://127.0.0.1:5000/page/board/login.php'. The page has a dark background with a cartoon horse illustration.

코드가 너무 길어서 직접 보여드리면서 설명 해  
드리겠습니다.

게시판을 구성하는 여러 기능들

## 데이터베이스 구조

<input type="checkbox"/>	1	idx	🔑	int(11)	아니오	없음	AUTO_INCREMENT	변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	2	name		varchar(100) utf8mb4_general_ci	아니오	없음		변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	3	pw		varchar(100) utf8mb4_general_ci	아니오	없음		변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	4	title		varchar(100) utf8mb4_general_ci	아니오	없음		변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	5	content		text utf8mb4_general_ci	아니오	없음		변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	6	date		date	아니오	없음		변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	7	hit		int(11)	아니오	없음		변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	8	lock_post		int(11)	아니오	없음		변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	9	file		varchar(100) utf8mb4_general_ci	아니오	없음		변경	삭제	<a href="#">더보기</a>

board 테이블

## 데이터베이스 구조

<input type="checkbox"/>	1	idx	🔑 int(11)	아니오	없음	AUTO_INCREMENT	변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	2	id	varchar(100) utf8mb4_general_ci	아니오	없음		변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	3	pw	varchar(100) utf8mb4_general_ci	아니오	없음		변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	4	name	varchar(100) utf8mb4_general_ci	아니오	없음		변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	5	sex	varchar(100) utf8mb4_general_ci	아니오	없음		변경	삭제	<a href="#">더보기</a>
<input type="checkbox"/>	6	email	varchar(100) utf8mb4_general_ci	아니오	없음		변경	삭제	<a href="#">더보기</a>

member 테이블

## 데이터베이스 구조

	1	idx	int(11)	아니오	없음	AUTO_INCREMENT	변경	삭제	더보기
	2	con_num	int(11)	아니오	없음		변경	삭제	더보기
	3	name	varchar(100) utf8_general_ci	아니오	없음		변경	삭제	더보기
	4	pw	varchar(100) utf8_general_ci	아니오	없음		변경	삭제	더보기
	5	content	text utf8_general_ci	아니오	없음		변경	삭제	더보기
	6	date	datetime	아니오	없음		변경	삭제	더보기

reply 테이블

## 겪은 문제점...

```
select .... where id='or 1=1#' and pw=''
```

기본적인 공격으로도 뚫리는 보안성



잦은 버그



20년대라고 볼 수 없는 디자인

## 보안 강화를 위한 노력

디렉토리 인덱싱

php 에러구문 미출력

sql injection

XSS

파일 업로드



### 디렉토리 인덱싱

```
<Directory "/">
*****
Options Indexes
*****
</Directory>
```



```
<Directory "/">
*****
Options --Indexes
*****
</Directory>
```

### 아파치 설정 변경

<https://ksj20180624.tistory.com/25>

### php 에러구문

#### 에러 출력하지 않는 방법

에러가 나온다면 아래의 방법으로 에러를 출력하지 않을 수 있습니다.

#### 문서에서 설정하는 방법

문서에 다음의 코드를 추가합니다.

```
<?php
ini_set( 'display_errors', '0' );
?>
```

#### 서버에서 설정하는 방법

php.ini에 있는 다음과 같은 코드를

```
display_errors = On
```

다음과 같이 변경합니다.

```
display_errors = Off
```

### php 에러 출력 X

<https://www.codingfactory.net/12217>

## xss

### `mysqli_real_escape_string()` 함수 사용

`NULL(\x00), \n, \r, \', \'` 문자 앞(왼쪽)에 \를 붙여 사용자의 입력에 의해 악의적인 쿼리문이 실행되는 것을 막는다.

## sql injection

### `htmlspecialchars(), strip_tags()` 함수 사용

`strip_tags()` 함수를 사용하여 1차적으로 HTML 태그와 PHP의 태그를 제거한다.

`htmlspecialchars()` 함수로 ", ', <, > 등 특정한 특수 문자를 HTML 엔티티로 변환한다.

### 파일 업로드 취약점

```
11 var $tmpfile;
12 if(empty($_FILES['b_file']['tmp_name'])){
13     echo "<p>";
14 }else{
15     $tmpfile = $_FILES['b_file']['tmp_name'];
16     $fileTypeExt = explode("/", $_FILES['b_file']['type']);
17     $fileType = $fileTypeExt[0];
18     $fileExt = $fileTypeExt[1];
19     $extStatus = false;
20     switch($fileExt){
21         case 'jpeg':
22         case 'JPEG':
23         case 'jpg':
24         case 'JPG':
25         case 'gif':
26         case 'GIF':
27         case 'bmp':
28         case 'BMP':
29         case 'png':
30         case 'PNG':
31             $extStatus = true;
32             break;
33     default:
34         echo "이미지 전용 확장자(jpg, bmp, gif, png)외에는 사용이 불가합니다.";
35         exit;
36         break;
37 }
38 if($fileType == 'image'){
39     if($extStatus){
40         $resFile = ".../img/".hash("sha256",time()).$_FILES['b_file']['name']);
41         $imageUpload = move_uploaded_file($tmpfile, $resFile);
42
43         if($imageUpload == true){
44             }else{
45                 echo "파일 업로드에 실패했습니다.";
46             }
47     }else [
48         echo "파일 확장자는 jpg, bmp, gif, png 이어야 합니다.";
49         exit;
50     ]
51 }
52 else {
53     echo "이미지 파일이 아닙니다.";
54     exit;
55 }
56
57 $o_name = hash("sha256",time()).$_FILES['b_file']['name']);
58 $filename = iconv("UTF-8", "EUC-KR",hash("sha256",time()).$_FILES['b_file']['name']));
59 }
```

### 파일 검사 및 파일명 변경

파일의 확장자와 파일 타입을 검사하여  
이미지 파일만 업로드 가능

파일 명이 겹치지 않게끔 time() 함수를 이용하여 파일명 해시화

## 최근 고친 코드들

비밀번호 없이 글과 댓글 수정, 삭제 가능

글 작성시 업로드 한 파일이 없을때 글 작성불가

파일이 없는데도 이미지 표시가 뜸

업로드 파일명 겹칠시 최근 업로드한 파일로 대체

---

## 추가하고 싶은것들

메일 보내는 기능

디자인

다른 커뮤니티 사이트같은 여러 갤러리 기능

회원별 레벨 기능(출석, 작성 글 개수 등)

유저끼리의 채팅기능

---

질문

---

## 질문 받습니다



# 이상으로 발표를 마치겠습니다



끝까지 들어주셔서 감사합니다.

작성자: 김태훈

인스타:@taehoon2006

메일: dvgvchnh@gmail.com