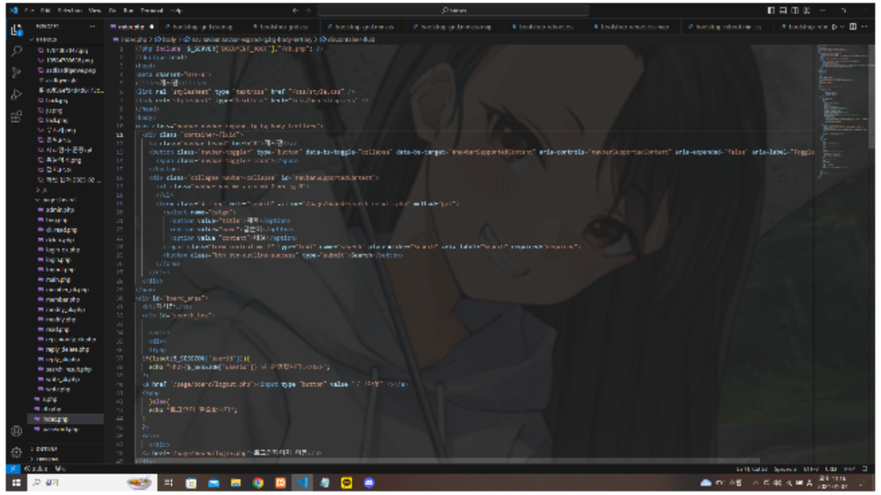
웹 게시판 개발

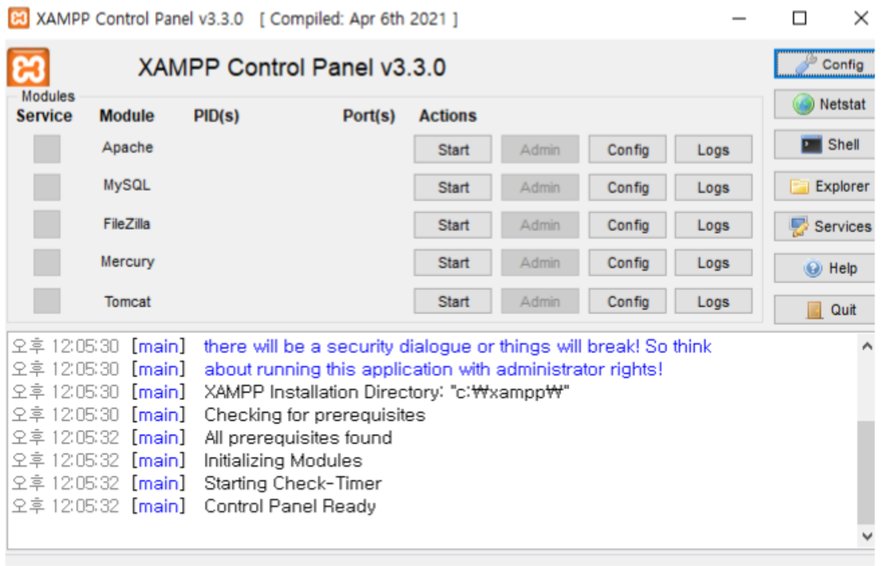
20204 김태훈

목차

개발 환경 및 사용 언어



vscode 꺼드럭



apache + php + mysql let's go

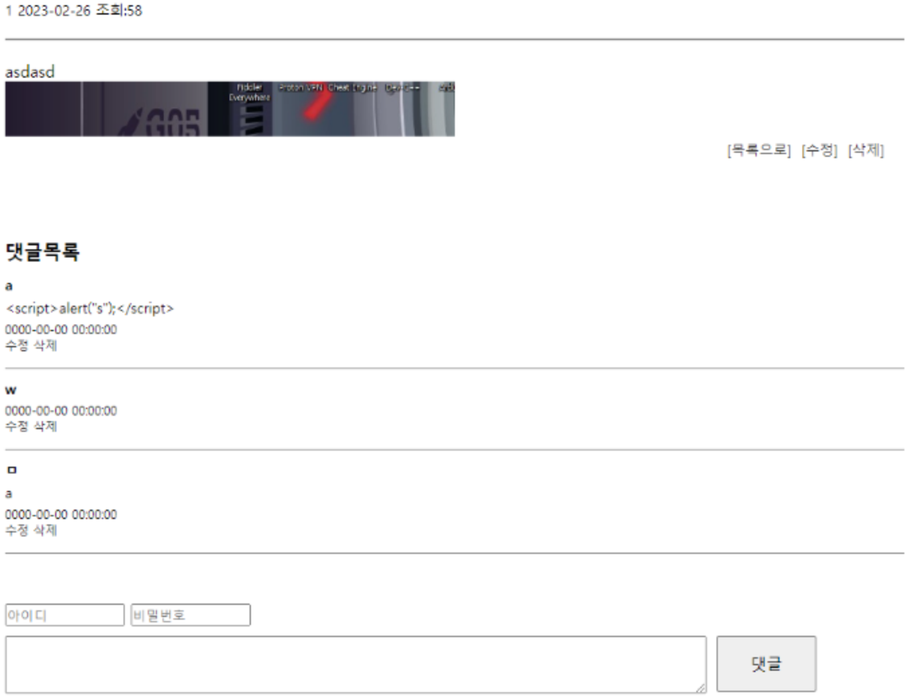
ngrok.exe

배포를 위한 ngrok

주요 페이지

글,댓글 쓰고 지우고 수정하고 삭제하고 아무튼 꺼드럭

메인 페이지



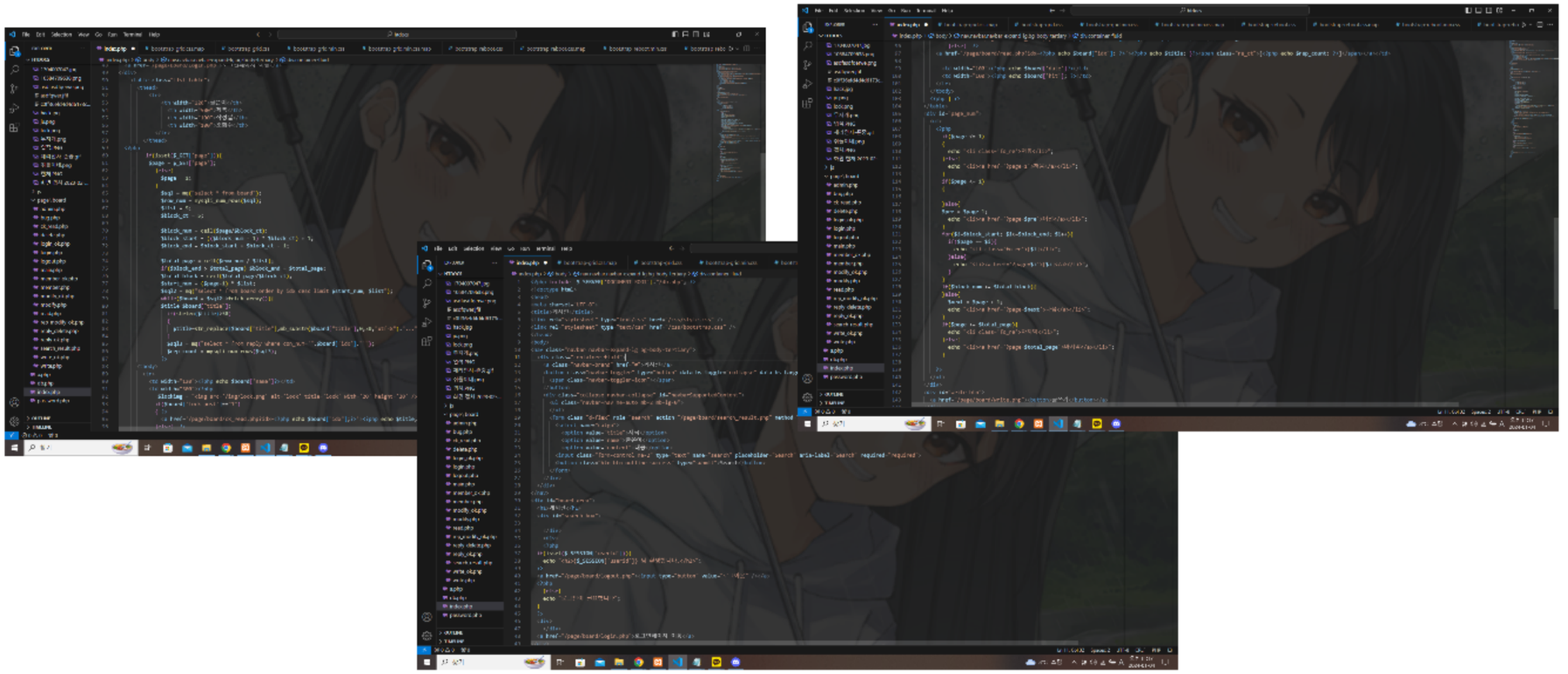
글 읽을 수 있는 페이지

실제로 접속 해보자

(필요 시 연락)

여러 php 파일들

- admin.php
- bug.php
- ck_read.php
- delete.php
- login_ok.php
- login.php
- logout.php
- main.php
- member_ok.php
- member.php
- modify_ok.php
- modify.php
- read.php
- rep_modify_ok.php
- reply_delete.php
- reply_ok.php
- search_result.php
- write_ok.php
- write.php
- a.php
- db.php
- index.php
- password.php



코드가 너무 길어서 직접 보여드리면서 설명 해 드리겠습니다.

게시판을 구성하는 여러 기능들

데이터 베이스 구조

☐	1	idx 🔑	int(11)		아니오	없음	AUTO_INCREMENT	변경	삭제	더보기
☐	2	name	varchar(100)	utf8mb4_general_ci	아니오	없음		변경	삭제	더보기
☐	3	pw	varchar(100)	utf8mb4_general_ci	아니오	없음		변경	삭제	더보기
☐	4	title	varchar(100)	utf8mb4_general_ci	아니오	없음		변경	삭제	더보기
☐	5	content	text	utf8mb4_general_ci	아니오	없음		변경	삭제	더보기
☐	6	date	date		아니오	없음		변경	삭제	더보기
☐	7	hit	int(11)		아니오	없음		변경	삭제	더보기
☐	8	lock_post	int(11)		아니오	없음		변경	삭제	더보기
☐	9	file	varchar(100)	utf8mb4_general_ci	아니오	없음		변경	삭제	더보기

board 테이블

데이터 베이스 구조

☐	1	idx 🔑	int(11)		아니오	없음	AUTO_INCREMENT	변경	삭제	더보기
☐	2	id	varchar(100)	utf8mb4_general_ci	아니오	없음		변경	삭제	더보기
☐	3	pw	varchar(100)	utf8mb4_general_ci	아니오	없음		변경	삭제	더보기
☐	4	name	varchar(100)	utf8mb4_general_ci	아니오	없음		변경	삭제	더보기
☐	5	sex	varchar(100)	utf8mb4_general_ci	아니오	없음		변경	삭제	더보기
☐	6	email	varchar(100)	utf8mb4_general_ci	아니오	없음		변경	삭제	더보기

member 테이블

데이터 베이스 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 injction

xss

파일 업로드

문제점 및 해결

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 injction

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

```php
if(empty($_FILES['b_file']['tmp_name'])){
    echo "<p>";
}else{
$tmpfile =  $_FILES['b_file']['tmp_name'];
$fileTypeExt = explode("/", $_FILES['b_file']['type']);
$fileType = $fileTypeExt[0];
$fileExt = $fileTypeExt[1];
$extStatus = false;
switch($fileExt){
    case 'jpeg':
    case 'JPEG':
    case 'jpg':
    case 'JPG':
    case 'gif':
    case 'GIF':
    case 'bmp':
    case 'BMP':
    case 'png':
    case 'PNG':
        $extStatus = true;
        break;
    default:
        echo "이미지 전용 확장자(jpg, bmp, gif, png)외에는 사용이 불가합니다.";
        exit;
        break;
}
if($fileType == 'image'){
    if($extStatus){
        $resFile = "../../img/".hash("sha256",time().$_FILES['b_file']['name']);
        $imageUpload = move_uploaded_file($tmpfile, $resFile);

        if($imageUpload == true){
        }else{
            echo "파일 업로드에 실패하였습니다.";
        }
    }
    else {
        echo "파일 확장자는 jpg, bmp, gif, png 이어야 합니다.";
        exit;
    }
}
else {
    echo "이미지 파일이 아닙니다.";
    exit;
}
$o_name = hash("sha256",time().$_FILES['b_file']['name']);
$filename = iconv("UTF-8", "EUC-KR",hash("sha256",time().$_FILES['b_file']['name']));
}
```

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 받습니다

이상으로 발표를 마치겠습니다

끝까지 들어주셔서 감사합니다.

작성자: 김태훈
인스타:@taehoon2006
메일: dgvchnh@gmail.com