

프로젝트명	CSRF WITH ME!
팀명 (팀원,팀원)	Sumoker(박지영, 김수환)
진행일자	2023.05.18~05.26

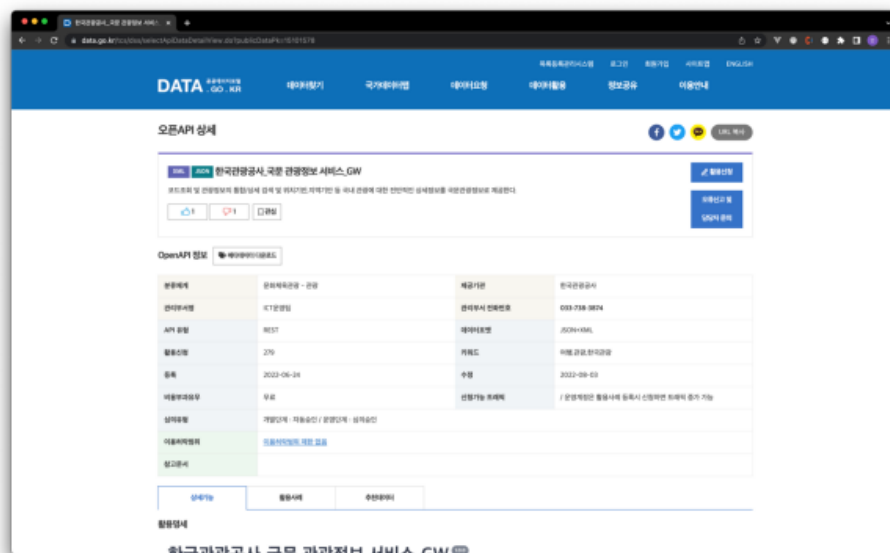
## 1. 목표

- Web Architecture 를 이해하고 활용하여 Web Project 를 설계하고 구현할 수 있다.
- Spring & MyBatis Framework, SpringBoot, Vue.js 를 이해하고 활용할 수 있다.
- JWT 로그인, REST API 등의 기술을 활용하여 MSA 를 도입해 본다.
- 추가 : XSS 와 CSRF 를 이해하고 보안을 위해 Lucy filter 와 Captcha 를 활용할 수 있다

## 2. 준비사항

### 1) 사용 데이터

- 전국관광지 정보  
한국관광공사\_국문관광정보 서비스\_GW.  
(<https://www.data.go.kr/tcs/dss/selectApiDataDetailView.do?publicDataPk=15101578>)



- 관광지 사진정보  
한국관광공사\_관광사진정보 서비스\_GW.

### 2) 개발언어/프로그래밍

- Java/STS/Tomcat/MySQL/VSCode

### 3) 필수 라이브러리 / 오픈소스

- Spring Framework (SpringBoot)
- MyBatis framework
- Vue.js / JavaScript / Bootstrap-Vue

### 4) 다양한 알고리즘

- AES
- SHA256

## 3. 요구사항

사용자에게 한국의 다양한 관광지, 먹거리, 축제, 행사 등을 소개하여 지역관광 활성화를 위한 소개 페이지를 구축하려 한다. 한국관광공사에서 제공하는 국문관광정보서비스\_GW 의 다양한 상세기능정보 API 를 활용하여 지역별 관광지 data 를 분석하고 화면에 표시한다. 또한 나만의 숨은 관광지를 소개하는 게시판 등을 구현해본다.

추가적으로 보안과 관련하여 비밀번호 암호화와 XSS, CSRF 공격에 대하여 추가적인 기능을 구현한다.

### Usecase Form

no	요구사항명	요구사항 상세	우선순위	구현여부(O/X)
F01	지역별 관광지 정보 수집	한국관광공사의 지역별 관광지 정보를 얻어와 화면에 표시	필수	O
F02	관광지, 숙박, 음식점 조회	관광지 정보를 지역별 원하는 콘텐츠 별 조회	필수	O
F03	문화시설, 공연,여행코스,쇼핑 조회	관광지 정보를 지역별 원하는 콘텐츠 별 조회	필수	O
F04	여행 계획 경로 설정	조회한 관광지를 활용하여 여행 계획, 여행 경로를 저장	추가	
F05	회원 주도의 핫플레이스 등록	지도와 사진을 활용한 핫플레이스 등록	추가	

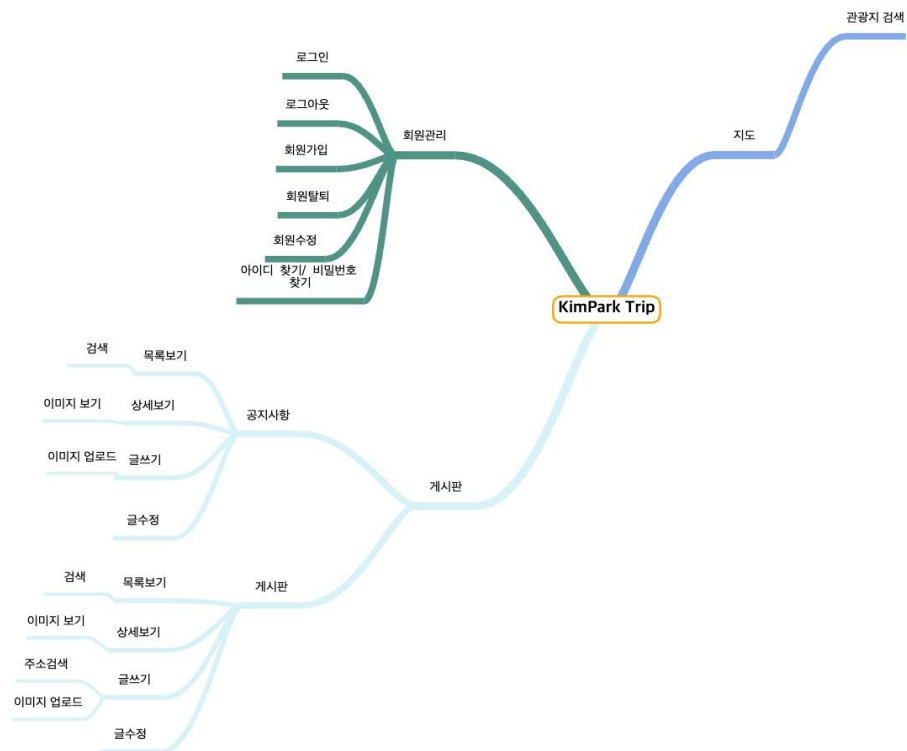
F06	관광지 관련 뉴스 정보 크롤링	관광지 정보를 크롤링하여 DB 에 저장	심화	
F07	회원관리	회원가입/수정/조회/탈퇴	필수	O
F08	인증관리	로그인/로그아웃/비밀번호 찾기	필수	O
F09	공지사항	공지사항 등록/수정/삭제/조회	심화	O
F10	공유게시판	게시판 등록/수정/삭제/조회	심화	O
F11	관광지 날씨	관광지의 기간별 날씨 출력		
F12	관광지 사진	관광지별 추천 사진 출력		
F13	일출, 일몰 시각	관광지별 일출, 일몰 시간 출력		
F14	전기자동차 충전소	전기자동차의 충전소의 위치 및 충전 상태 출력		
비기능적 요구사항				
NF1	공공데이터의 정확성	공공데이터 API 를 활용함으로 인한 정확성이 요구됨		O
NF2	가용성	언제나 (어떤 디바이스로든) 서비스 가능해야 함		O
NF3	응답성	조회에 대한 결과를 빠르게 응답해야 함		O
NF4	사용자 편의성	웹 사이트에 대한 사전 지식이 없어도 쓰기 편해야 함		O
NF5	안전성	비밀번호 해싱		O
NF6	안전성	주민번호 암호화		
NF7	안전성	XSS 방어		O
NF8	안전성	CSRF 방어		O
NF9	안전성	FileUpload/download 취약점 방어		
NF10	안전성	세션 하이재킹 방어		
NF11	안전성	Jwt 암호화		O

NF12	안전성	SALT, 암호화 키 관리		O
NF13	안전성	게시판 이미지 암호화		O

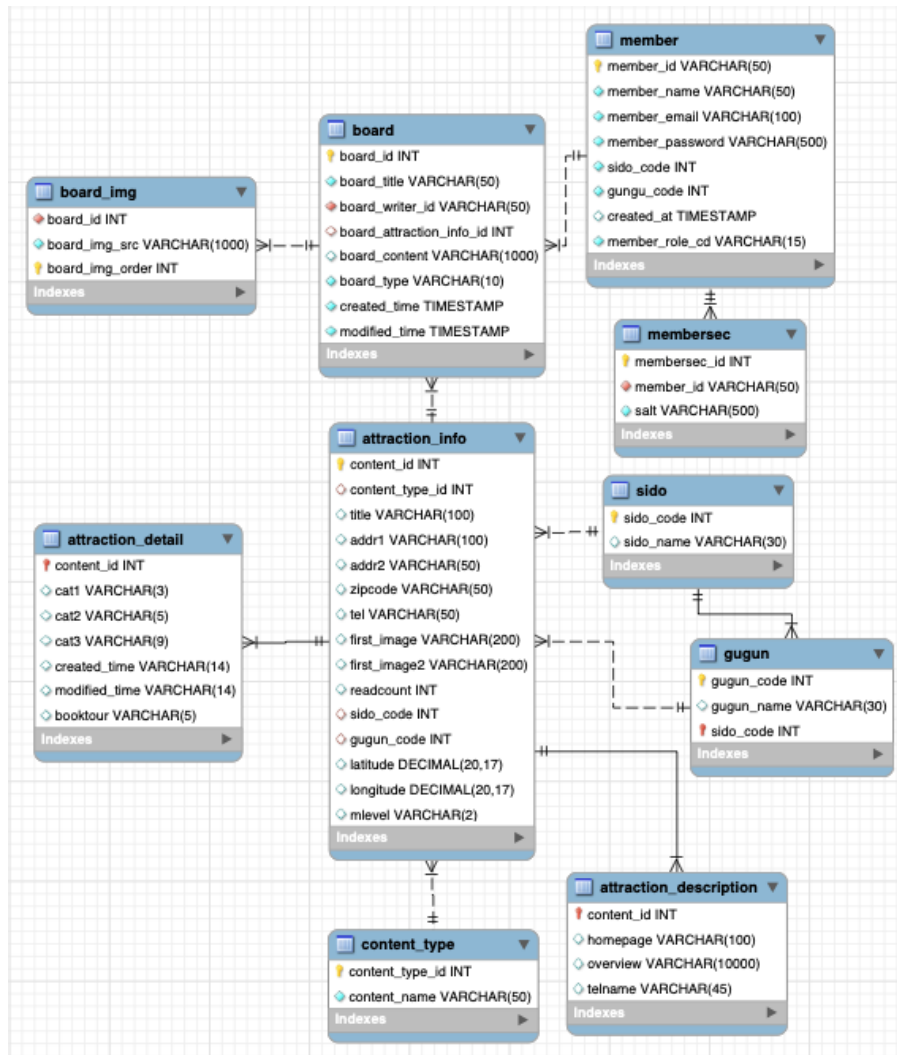
#### 4. 결과 (산출물)

##### 1) 설계서

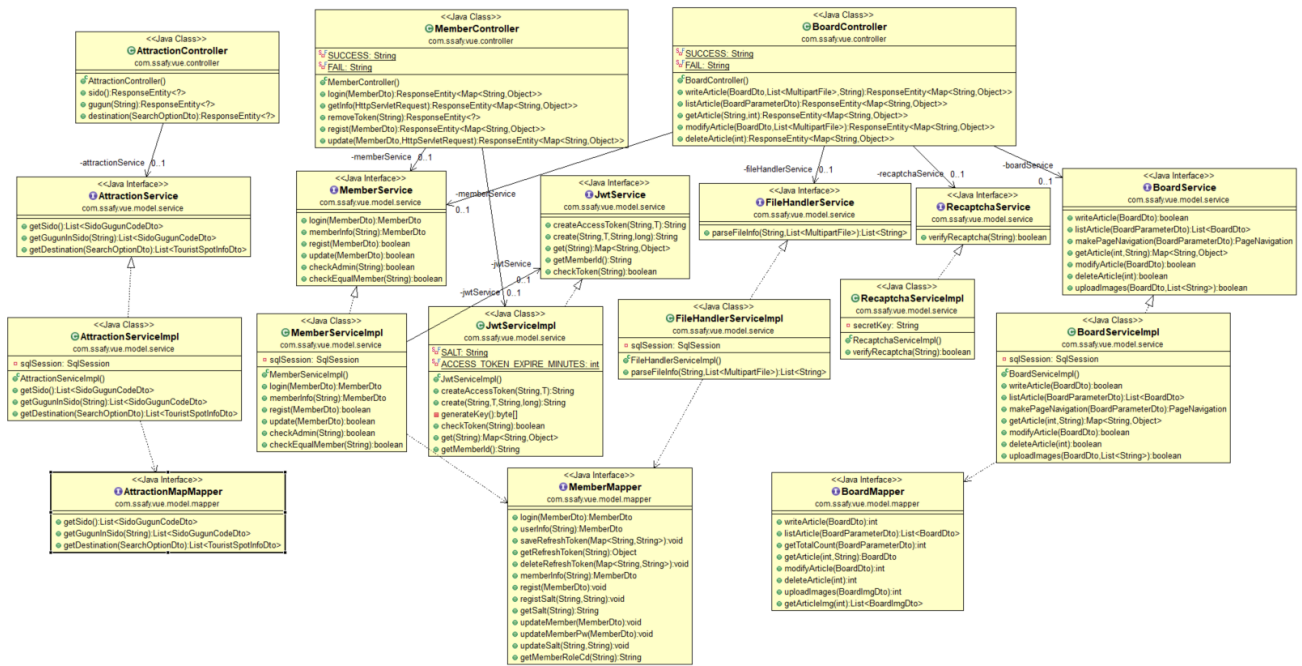
##### (1) Usecase Diagram (기능 설명)



(2) ERD

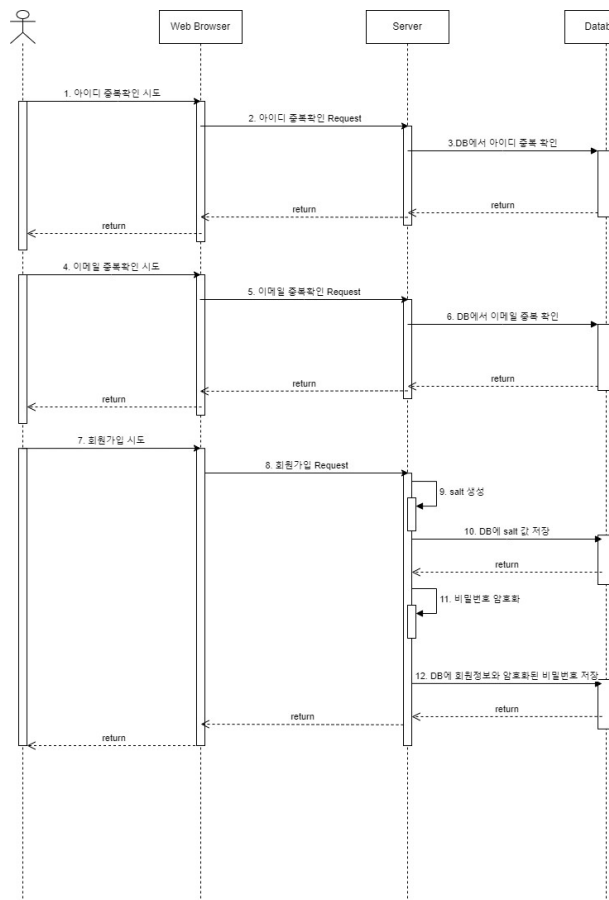


### (3) Class Diagram

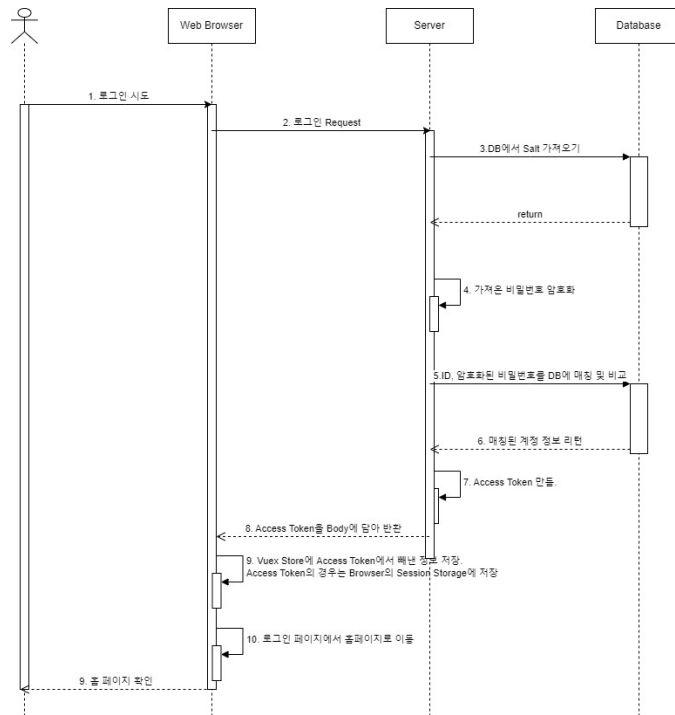


### (4) Sequence Diagram

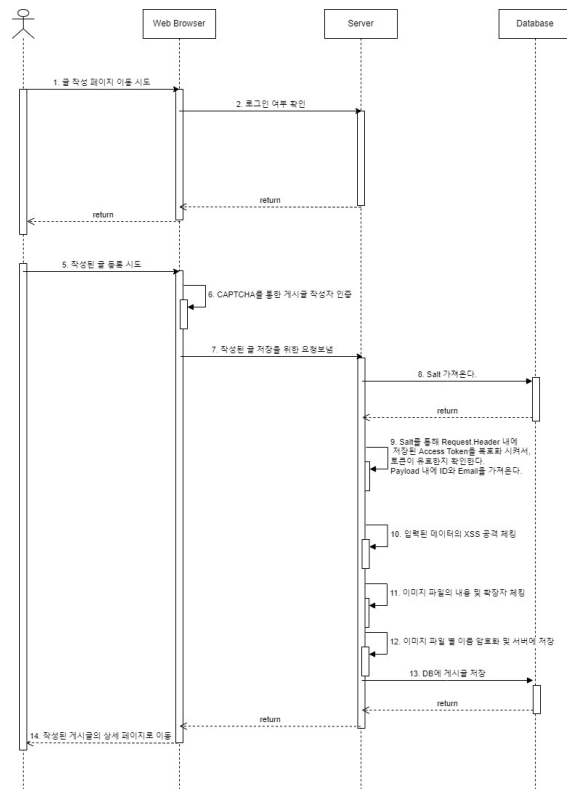
#### - 회원가입



## - 로그인

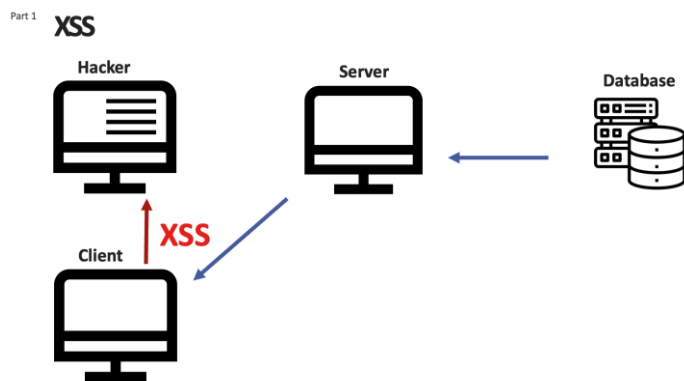


## - 게시물 작성



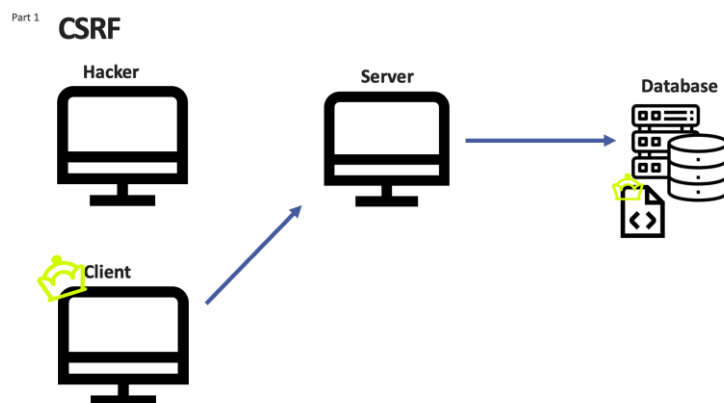
## 5. 프로젝트 핵심

### 1) XSS 개념



XSS 공격이란 스크립트에 악의적인 코드를 집어 넣어 사용자의 정보를 빼가는 해킹 기술 중 하나입니다. 해커가 게시판과 같은 기능에 html 코드등을 이용하여 사용자가 접근하도록 하고 접근한 사용자의 정보는 해커에게 넘어가게 됩니다.

### 2) CSRF 개념

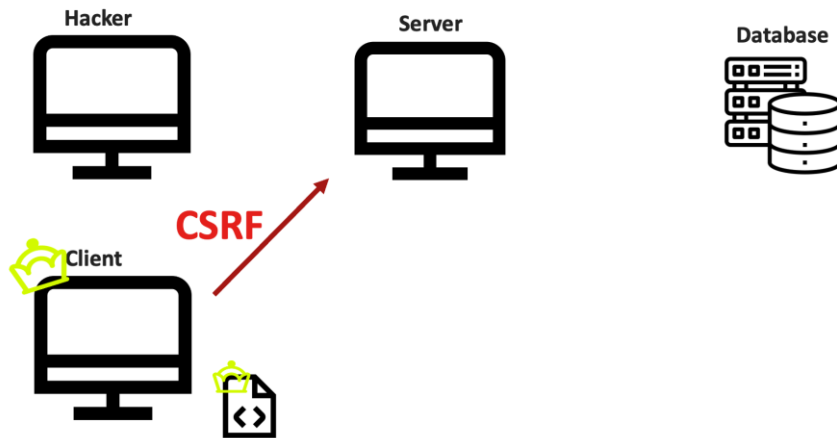


CSRF 공격이란 보통 XSS 의 공격과 마찬가지로 스크립트를 이용해 악의적인 코드를 집어 넣게 됩니다. 이때, 권한을 가진 사용자가 해당 게시물과 같은 스크립트가 들어가 있는 정보를 서버에게 요청을 하게 됩니다.



Part 1

## CSRF

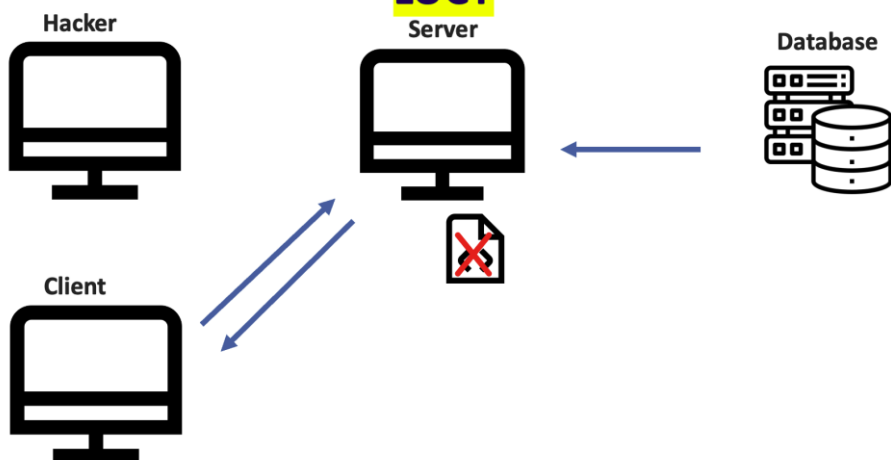


권한을 가진 사용자는 해당 스크립트를 이용하게 되고 사용자의 권한을 이용하여 CSRF 공격이 이루어지게 됩니다. 예를 들어, 서버에 관리자만이 할 수 있는 공지사항과 같은 기능을 해당 스크립트를 접근한 관리자의 계정으로 수행되게 됩니다.

### 3) XSS 방어

Part 1

## XSS



이를 방어하기 위해 LUCY 필터를 사용하고자 하였습니다. 스크립트 태그를 필터링하여 스크립트를 무효화시켜주도록 하여 XSS 스크립트를 방어하고자 하였습니다.

```

@Override
public void configureMessageConverters(List<HttpMessageConverter<?>> converters) {
    converters.add(htmlEscapingConverter());
}

private HttpMessageConverter<?> htmlEscapingConverter() {
    ObjectMapper objectMapper = new ObjectMapper();
    objectMapper.getFactory().setCharacterEscapes(new HTMLCharacterEscapes());

    return new MappingJackson2HttpMessageConverter(objectMapper);
}

```

## 실제 코드

```

public class HTMLCharacterEscapes extends CharacterEscapes {
    private final int[] asciiEscapes;

    public HTMLCharacterEscapes() {
        asciiEscapes = CharacterEscapes.standardAsciiEscapesForJSON();
        asciiEscapes['<'] = CharacterEscapes.ESCAPE_CUSTOM;
        asciiEscapes['>'] = CharacterEscapes.ESCAPE_CUSTOM;
        asciiEscapes['&'] = CharacterEscapes.ESCAPE_CUSTOM;
        asciiEscapes['"'] = CharacterEscapes.ESCAPE_CUSTOM;
        asciiEscapes['\'] = CharacterEscapes.ESCAPE_CUSTOM;
        asciiEscapes['*'] = CharacterEscapes.ESCAPE_CUSTOM;
        asciiEscapes['`'] = CharacterEscapes.ESCAPE_CUSTOM;
    }

    @Override
    public int[] getEscapeCodesForAscii() {
        return asciiEscapes;
    }

    @Override
    public SerializableString getEscapeSequence(int ch) {
        return new SerializedString(StringEscapeUtils.escapeHtml4(Character.toString((char)ch)));
    }
}

```

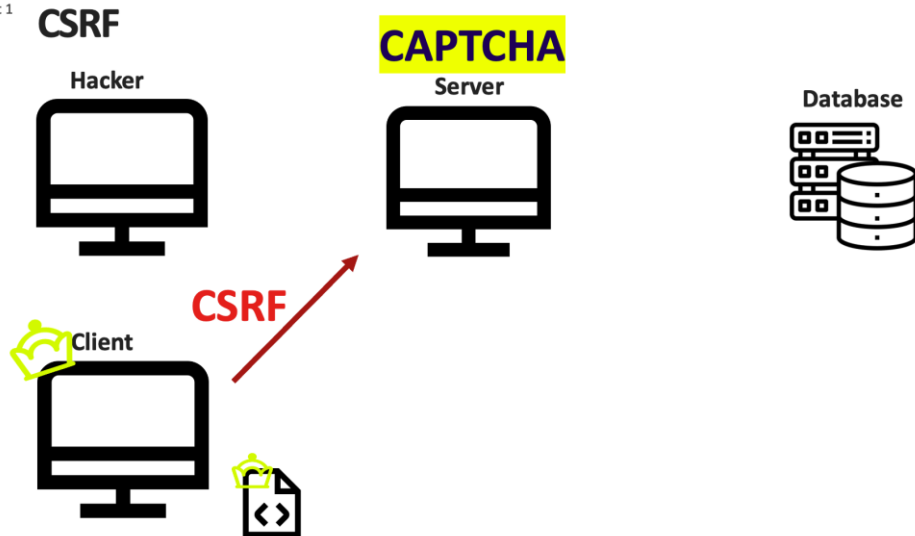
데이터베이스

board_id	board_title	board_writer_id	board_attr...	board_content	board_ty...	created_time	modified_time
18	공지	qwer		&lt;style&gt;&lt;img title=&quot;&lt;style&gt;... notice		2023-05-24 21:3...	2023-05-24 21:37:17

실제 코드와 데이터베이스에 적용된 내용입니다. 해당 필터를 통해 들어온 스크립트 공격에 대하여 필터링되어 데이터베이스에 다음과 같이 저장되는 것을 볼 수 있습니다.

## 4) CSRF 방어

Part 1



CSRF 방어를 위해 CAPTCHA 를 이용하도록 하였습니다. CSRF 공격은 사용자도 모르게 자신의 계정을 통해 서버에 공격을 하게 되는데 이를 예방하기 위해 CAPTCHA 를 적용하여 한번 더 실제 사용자가 이용하려고 하는지를 확인하도록 하였습니다.

실제 구현 결과 입니다.

글작성

제목 :

내용:

✓

로봇이 아닙니다.

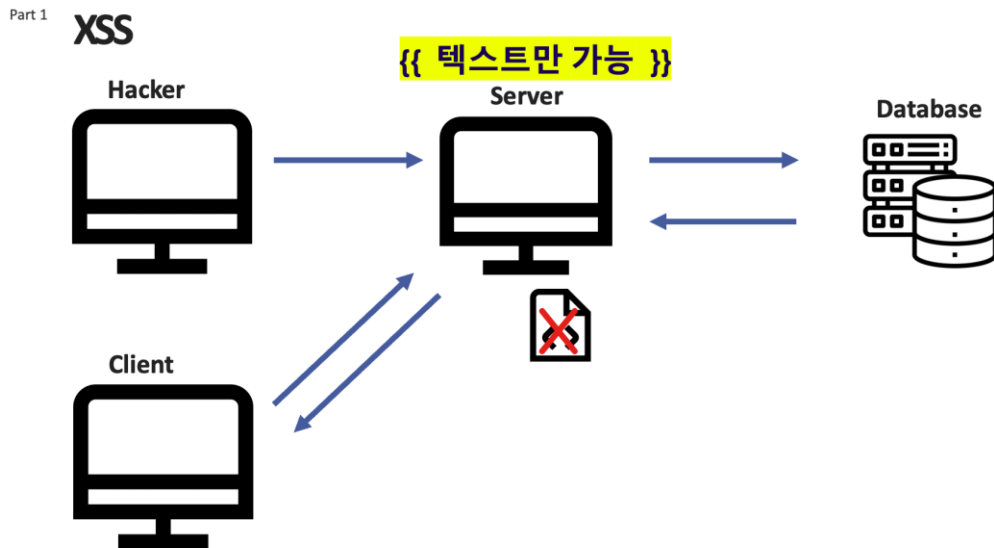
  
reCAPTCHA  
개인정보 보호 · 약관

글작성

초기화

다음과 같이 CAPTCHA 를 통해서 CSRF 에 대한 공격에 대해 방어하고자 하였습니다.

#### 5) 텍스트를 통한 보안



마지막으로 XSS 는 html 을 통해서 일어나는 공격이므로 이를 막고자 텍스트로 화면에 보여주도록 하는 방어입니다. 이는 사용자 편의를 생각하면 좋은 방식은 아니지만 XSS 나 CSRF 공격을 막기 위한 보안 방법 중 하나입니다.

#### 6) 기능 구현 - 회원가입

127.0.0.1:8080/member/join

SAFY 여행지 정보 공지사항 공유 게시판

127.0.0.1:8080 내용:  
박지영님 환영합니다! 로그인 후 이용해주세요

확인

### Member Service

아이디:

이름:

이메일:

비밀번호:

비밀번호 확인:

사는 곳:

가입하기

## 7) 기능구현 - 로그인

127.0.0.1:8080/member/login

SAFY 여행지 정보 공지사항 공유 게시판

### Member Service

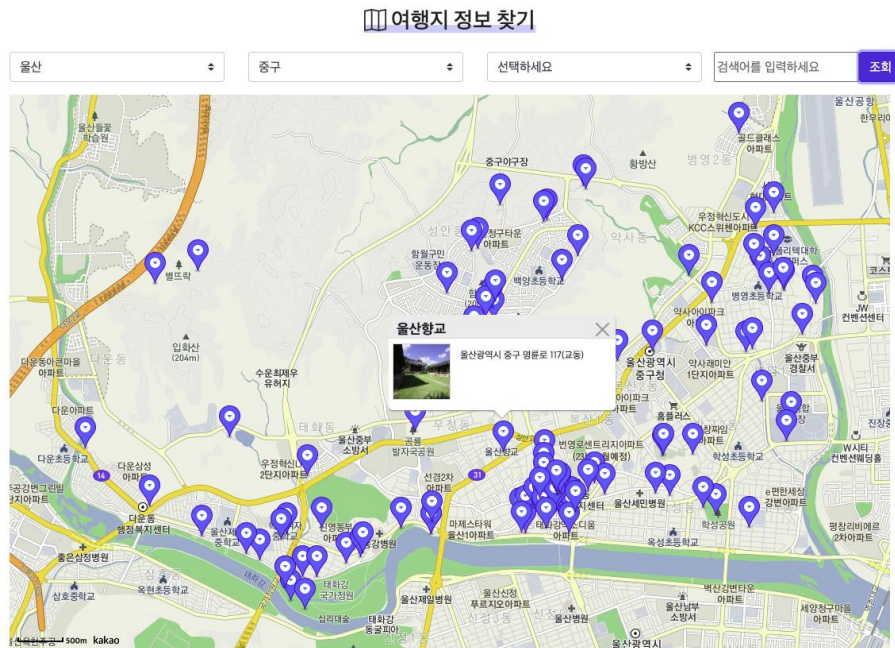
## 로그인

아이디:

비밀번호:

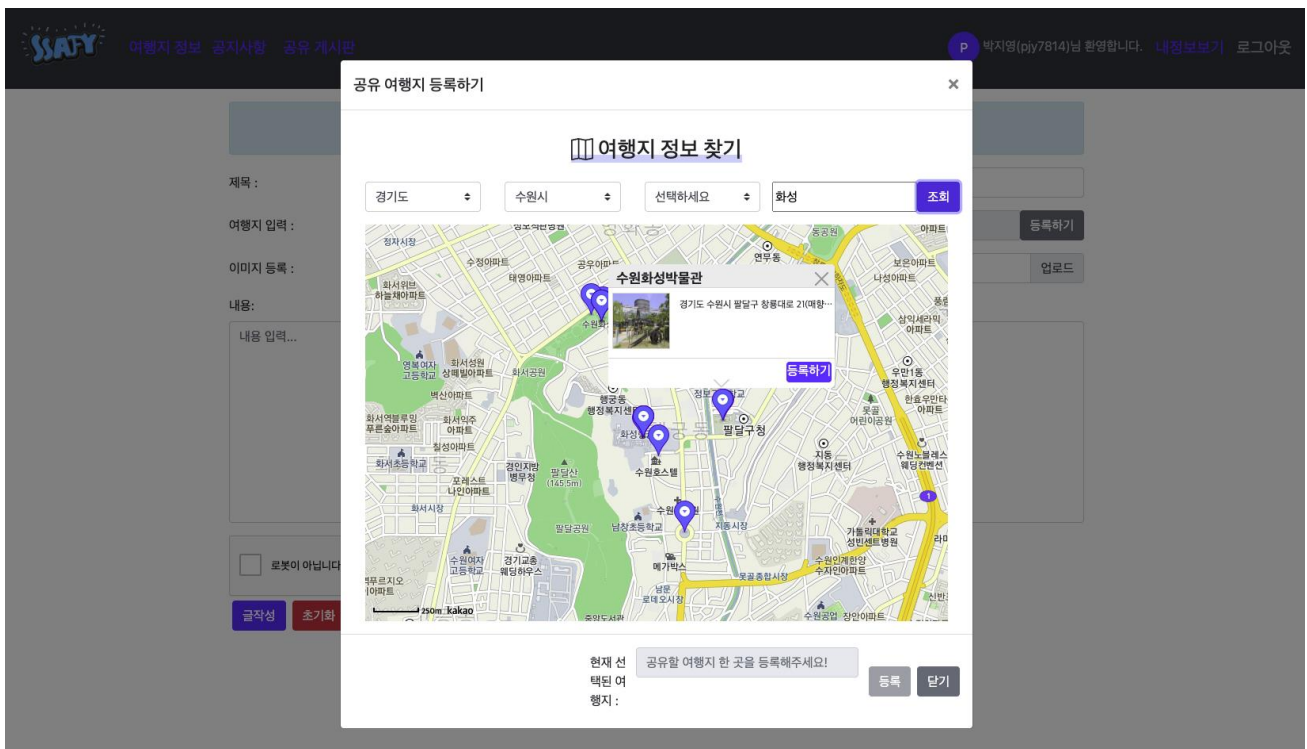
로그인 회원가입

## 8) 기능 구현 - 여행지 정보 검색



여행지 정보를 검색할 수 있습니다.

## 9) 기능 구현 - 공유 게시판 글쓰기



글작성

제목 :

좋은 곳 소개해드립니다!

여행지 입력 :

수원화성박물관

등록하기

이미지 등록 :

수원화성1.jpeg, 수원화성2.jpeg

업로드

내용:

수원화성 박물관에 다녀왔습니다!

✓

로봇이 아닙니다.



reCAPTCHA


개인정보 보호 · 약관

글작성

초기화

공유게시판에 여행지에 대한 정보를 등록할 수 있습니다. 모든 사용자가 접근이 가능하며 사진을 업로드할 수도 있습니다.

10) 기능 구현 - 글 목록 보기


[여행지 정보](#)
[공지사항](#)
[공유 게시판](#)

P

박지영(pjy7814)님 환영합니다.

[내정보보기](#)

[로그아웃](#)

공유 게시판			
글쓰기			
글번호	제목	작성자	작성일
28	여기 별로예요	pjy7814	21:10:52
27	좋은 곳 소개해드립니다!	pjy7814	21:09:49

<<

<

1

>


>>

Search

Search

최신순으로 글 목록을 불러올 수 있습니다.

## 11) 기능 구현 - 글 상세보기


[여행지 정보](#)
[공지사항](#)
[공유 게시판](#)

 박지영(pjy7814)님 환영합니다.
 [내정보보기](#)
[로그아웃](#)

글보기

[목록](#)
[글수정](#)
[글삭제](#)

### 27. 좋은 곳 소개해드립니다!

pjy7814

2023. 5. 25. 오후 9:09:49






공유 여행지 : 수원화성박물관(경기도 수원시 팔달구 창룡대로 21)

수원화성 박물관에 다녀왔습니다!

여행지를 확인할 수 있으며 업로드된 사진을 가져올 수 있습니다.

## 12) 기능 구현 - 글 수정


[여행지 정보](#)
[공지사항](#)
[공유 게시판](#)

 박지영(pjy7814)님 환영합니다.
 [내정보보기](#)
[로그아웃](#)

127.0.0.1:8080 내용: 글 수정 성공!

확인

글수정

제목 :

여행지 입력 :  [등록하기](#)

이미지 등록 :  [업로드](#)


내용: 

수원화성 박물관에 다녀왔습니다!  
정말 재미있어요~


 로봇이 아닙니다.
 

 hCAPTCHA  
개인정보 보호 · 지원
 
[글수정](#)
[초기화](#)

### 13) 기능 구현 - 글 삭제

[여행지 정보](#) [공지사항](#) [공유 게시판](#)


127.0.0.1:8080 내용:  
글 삭제에 성공했습니다! 리스트 페이지로 돌아갑니다!

P 박지영(pjy7814)님 환영합니다. [내정보보기](#) [로그아웃](#)

글목록

삭제처리중...

### 14) 기능 구현 - 공지사항 (관리자 권한을 가진 사람만 접근 가능)

[여행지 정보](#) [공지사항](#) [공유 게시판](#)

127.0.0.1:8080 내용:  
글 등록 성공!

A 김관리(admin)님 환영합니다. [내정보보기](#) [로그아웃](#)


글작성

제목 :

내용: 

5월 26일 사이트 점검으로 인해서 접속이 불가능합니다.

✓ 로봇이 아닙니다.

  
reCAPTCHA  
개인정보 보호 · 약관

글작성

초기화



## 6. 개발 후기

팀장(박지영)	<p>프로젝트를 시작할 때에는 막막하기도 하였지만 하나 둘씩 기능이 구현되어 가는 과정을 보면서 뿌듯함을 느꼈습니다. 특히, 평소에 관심이 있던 XSS 와 CSRF 에 대한 보안을 생각해보면서 공격에 대한 과정과 이를 방어하기 위한 방법 등 개념을 알 수 있었습니다. 그리고 실제 프로젝트에 적용하고 결과를 보는 과정을 통해 확실하게 이해할 수 있어 좋았습니다.</p> <p>XSS 를 막기 위해 Lucy 필터를 적용하려고 하였으나 JSON 방식으로 넘어갈 경우에는 적용이 되지 않아 따로 커스텀한 필터를 적용해야하는 이슈가 있었습니다. 인터넷에 공개되어 있는 자료를 이용하여 필터링을 하는데에는 성공하였지만 이미 공개되어있는 자료를 이용하여 보안상 좋지 않다는 것을 알게 되었습니다. 추후에 직접 XSS 를 막기 위한 필터를 개발해보고 싶다는 생각이 들었습니다.</p>
팀원(김수환)	<p>이번 프로젝트는 정말 배움과 고민의 연속이었던 것 같습니다. 팀원과 기능 개발에 대해 고민하기 이전에 그 기능이 저희 프로젝트에 들어갔을 때 보안적으로 생겨날 수 있는 문제점에 대해 고민하였고, 대표적으로 게시판 내에서 XSS 를 막기 위한 Lucy, CSRF 를 막기 위해 CAPTCHA 를 저희 프로젝트에 적용해나갔습니다. 그 과정에서, 보안적인 지식을 많이 찾아보며 습득할 수 있었고, 실제 공격방지가 진행되는 것을 두 눈으로 보며 뿌듯함을 느꼈습니다.</p> <p>또한, 그런 뿌듯함을 느낌과 동시에 보안이라는 먼 길에 겨우 첫발을 내딛었다라는 느낌도 들었습니다. XSS, CSRF 를 찾아보며 보안 취약점 리스트 사이트들을 주로 볼 수 있었는데, 저희가 이번 프로젝트에 적용시킨 게시판 보안을 위한 Lucy, Captcha 만으로 대응이 힘든 공격들을 정말 많이 볼 수 있었기 때문입니다. 이는 추후, 지금 이 프로젝트를 되돌아보며 제가 짠 코드에 보안 취약점에 대해 한번 씩 고민해볼 수 있는 개발을 해보자는 동기부여가 됐던 것 같습니다.</p>