프로젝트 계획서

**PHP를 통한 웹 개발과 모의해킹 프로젝트**

목차

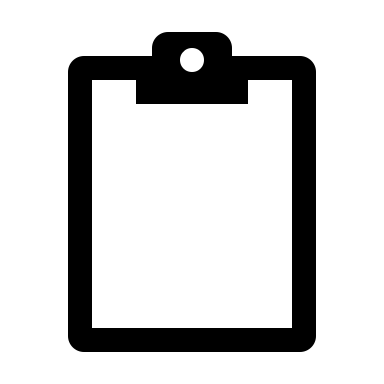
**프로젝트 개요**

**구현 기능**

**서비스 아키텍처**

**예상 발생 취약점**

**발생 취약점 설명**

**역할 분배**

프로젝트 개요

**해당 프로젝트는 저의 웹 해킹 능력 및 웹 개발 능력 향상을 위해**

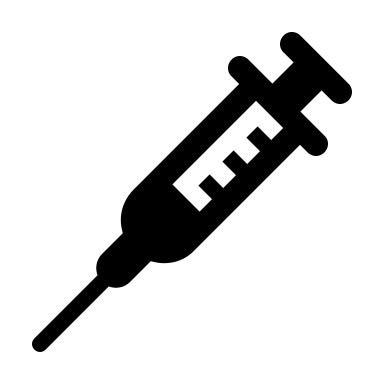
**시작 하였습니다. 서버 개발용 언어 PHP와 HTML, JavaScript를 통해**

**간단한 게시판 서비스를 구현할 예정이며, 구현이 완료되면 제작된**

**페이지를 최대한 다양한 방법을 통해 해킹을 진행하고, 이에 대한**

**공격 연구 보고서를 작성할 예정입니다. 또한 보고서에 웹 페이지를**

**해킹할 때 사용된 취약점이 발생하는 이유, 해당 취약점이 발생하지**

**않게 하기 위한 시큐어 코딩에 대한 정보도 서술할 예정입니다.**

구현 기능

**기능 | 설명**

**글 작성 | 유저가 글을 쓴다.**

**글 조회 | 유저가 글을 조회 한다.**

**글 삭제 | 글을 작성한 유저가 글을 작성한다.**

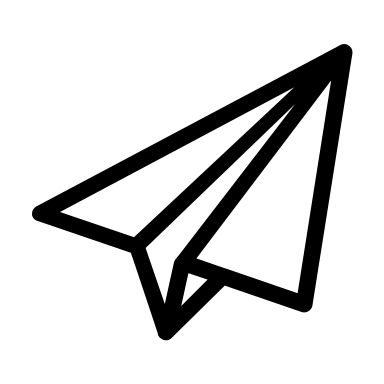
**파일 업로드 | 유저가 마음대로 파일을 업로드 한다.**

**파일 다운로드 | 유저가 업로드한 파일을 다운로드 한다.**

**회원가입 | 아이디와 비밀번호를 기입하여 회원가입 한다.**

**로그인 | 회원가입한 아이디 및 비밀번호로 로그인 한다.**

**아이디 중복 체크 | 유저가 가입하려는 아이디가 중복인지 확인한다.**

****

서비스 아키텍처

**하드웨어, 서버, DB 등 목록과 서비스 구조를 명시**

**해당 웹 페이지는 백엔드에 PHP를, 프론트엔드에 HTML과**

**JavaScript를 사용하였습니다.**

**예상 발생 취약점**

**발생할 것으로 예상되는 취약점 리스트입니다.**

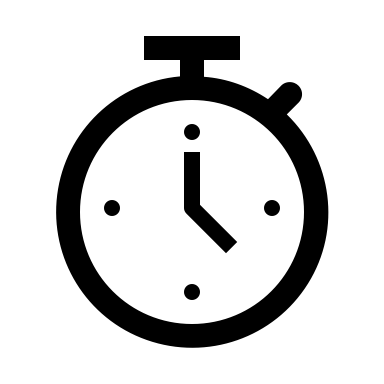
**예상 발생 취약점 | 발생 위치**

**XSS(Cross Site Scriptting) – 게시판 내부**

**SQL Injection – 로그인 및 회원가입 페이지**

**File Upload Vulnerability – 게시판 내부 파일 업로드 페이지**

**File Download Vulnerability – 게시판 내부 파일 다운로드 페이지**

****

**발생 취약점 설명**

**예상되는 발생 취약점에 대해 서술**

**SQL Injection**

**SQL Query문이 삽입 될 수 있는 취약점입니다.**

**주로 로그인과 같은 SELECT 문을 통해 DB에서 정보를 조회하는 곳에서 해당 취약점이 발생합니다.**

**XSS(Cross Site Scripting)**

**서버가 제공하는 페이지에 공격자가 작성한 악성 구문이**

**삽입 될 수 있는 취약점입니다. 주로 게시판과 같은 공격자가 작성한**

**구문이 그대로 다른 유저에게 제공될 수 있는 곳에서**

**해당 취약점이 발생합니다.**

**File Upload Vulnerability**

**서버에 공격자가 원하는 어떤 파일이든 업로드 할 수 있는**

**취약점입니다. 주로 공격자가 업로드하는 파일에 대한 필터링이 존재하지 않을 때 해당 취약점이 발생합니다.**

**File Download Vulnerability**

**서버에 존재하는 파일들을 공격자가 마음대로 다운로드 할 수 있는**

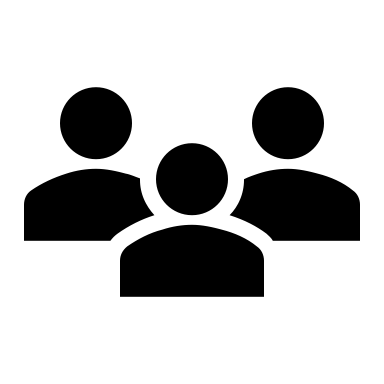
**취약점입니다. 주로 파일을 다운로드하는 URL을 공격자가 예측하기 쉬울 때 해당 취약점이 발생합니다.**

역할 분배

**Back End – 도원준**

**Front End – 도원준**

**Hacking – 도원준**

**보고서 작성 – 도원준**