SWING 25-1

OOP PROJECT PROPOSAL

TOPIC **주제**	**MCP & Prompt Injection**		
PARTICIPANTS **참여자 및 역할**	33기	김보현	팀원
	33기	김주영	팀원
	33기	천민진	팀원
	33기	최윤서	팀원
OBJECTIVES **목표**	MCP, 프롬프트 인젝션의 구현 및 방어 체계 생성		

PROGRESS
진행 상황

MCP와 API 비교 탐구

- MCP의 개념과 핵심 요소, 작동 방식을 중심으로 MCP에 대해 학습하고, 기존의 API 방식과 비교하며 차이점을 정리하였다.
- Claude를 활용하여 MCP 구현 실습을 진행하며, 외부 도구 연동 시 나타날 수 있는 보안 이슈를 실험적으로 분석하였다.

프롬프트 인젝션 이해 및 구현

- 프롬프트 인젝션(Prompt Injection)의 개념과 주요 유형에 대해 조사하고, 실제 적용 가능한 시나리오를 구성하였다.
- C++를 활용하여 프롬프트 인젝션 공격 코드를 구현하였으며, 단순 구현에 그치지 않고 공격을 방어하기 위한 코드를 함께 제작하였다.
- '해커 – 사용자 – 화이트 해커' 시나리오로 역할을 구분하여 공격 및 방어 과정을 설명할 수 있도록 구성하였고, 각 상황별 대응 로직을 직접 구현하며 보안 대응 능력을 기르는 데 초점을 맞추었다.

CHALLENGE
어려운 점

프롬프트 인젝션 방어 코드 제작 과정에서 우회 입력을 적용하려 해도 서버 코드에서 제대로 작동되지 않아 어려움을 겪었다.
입력값이 예상대로 처리되지 않아 여러 번 코드를 수정하고 테스트하는 과정을 거쳐야 했다.