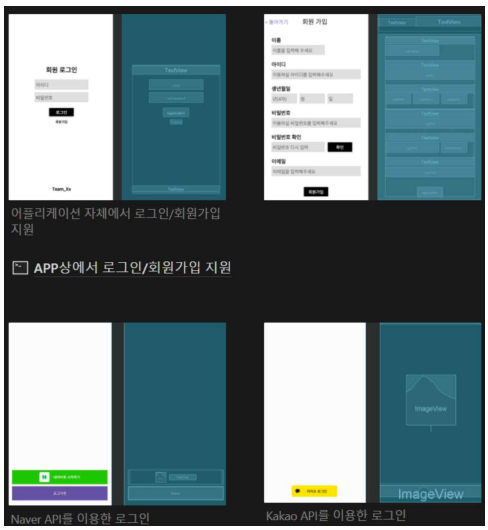
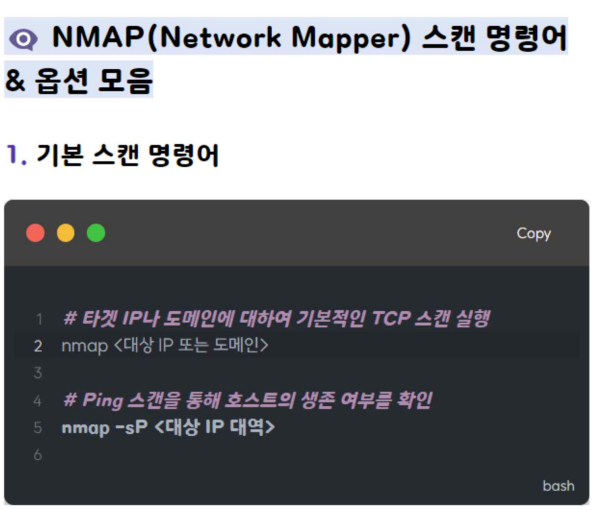
주제	Social Login API & 웹해킹 기초 & NMAP, Personal Access Token 관련 실습		
팀원	이채린, 이가연, 한아림	**결석자**	X
날짜	2023. 07. 16, 2023. 07. 28		
내용	Kakao나 Naver, Google API 등을 이용하여 앱 내에 로그인 버튼을 구현해보는 활동을 진행했다. 먼저 API란 Application Programming Interface의 약자로, 운영체제와 응용프로그램 사이의 통신에 사용되는 언어나 메시지 형식을 말한다. 내부 API는 진동, 플래시 같은 디바이스 제어 기능들을 이용하는 데 사용되고, 외부 API는 네이버 지도 API를 이용하여 위치기반 기능 등을 사용하는 데 사용된다. 웹 해킹의 기초에 대해 스터디를 진행했다. 취약점 분류에는 인증과정에서 발생하는 취약점, SQL 인젝션, 크로스 사이트 스크립팅, 크로스 사이트 요청 위조 등이 있으며, 정보 수집의 경우 검색 엔진을 이용하여 사이트 구조, 보안 설정, 민감한 파일, 노출된 정보 등을 찾을 수 있다. 스캐닝과 익스플로잇의 경우 취약점을 찾기 위해 자동화된 스캐너 도구를 사용하거나 직접 테스트하여 취약점을 발견할 수 있다. 접근 과정의 경우 해커가 발견한 취약점을 이용하여 웹 사이트 또는 웹 서버에 접근을 시도할 수 있다. 권한 상승, 컨트롤과 지속성 확보, 후행 작업 등이 이에 해당한다. NMAP(Network Mapper) 스캔 명령어와 옵션 정리, GitHub(깃허브) Personal Access Token 생성에 대한 학습을 진행하였다. 퍼스널 액세스 토큰이란 깃허브에서 제공하는 인증 방식 중 하나로, 사용자가 자신의 계정을 인증하고 API 요청을 수행할 수 있도록 해주는 보안 인증 키이다. 퍼스널 액세스 토큰은 사용자가 자신의 깃허브 계정과 연결된 권한과 범위를 정의하여 생성되며, 사용자는 토큰의 범위에 따라 특정 깃허브 리포지토리에 대한 읽기나 쓰기, 관리 등의 권한을 허용할 수 있다.		
사진			

2. 포트 스캔 명령어

```
Copy

1  # 특정 포트만 스캔
2  nmap -p <포트 번호> <대상 IP>
3
4  # 모든 포트 스캔
5  nmap -p- <대상 IP>
6
7  # 일반적인 포트만을 빠르게 스캔
8  nmap -F <대상 IP>
9

bash
```

웹 해킹 기초

웹 해킹

: 웹 애플리케이션과 웹 서버의 취약점을 이용하여 불법적인 접근, 정보 유출, 서비스 장애 등을 초래하는 공격 방법

취약점 분류

인증과정의 취약점

: 약한 비밀번호, 인증 우회, 세션 관리 결함 등을 통해 계정을 빼앗거나 다른 사용자로 위장하는 등의 공격 가능

SQL Injection

: 웹 애플리케이션의 입력 폼 등에서 SQL 쿼리를 악의적으로 주입하여 데이터베이스를 조작하는 공격

겨울방학 프로젝트/스터디 활동지