<네트워크보안 실습 과제 (2)>

[개요]

안드로이드 어플리케이션 취약점 분석 경험과 관련 기술을 활용하여, (Option A: 분석) 혹은 (Option B: 구현) 중에서 하나를 선택하여 진행한다.

- **(Option A: 분석) 타겟 어플리케이션의 보안 취약점 분석 (100점)**
- **(Option B: 구현) 보안 취약점을 실제 어플리케이션 형태로 구현 (100점 + @)**

[Option A: 분석]

요구사항	안드로이드 어플리케이션 2개의 보안 취약점 분석을 진행한다. - 타겟 어플리케이션은 취약점이 존재한다고 알려진 안드로이드 어플리케이션을 선택하거나 (InsecureBankv2 제외), 새로운 취약 어플리케이션을 탐색하여 진행 가능 - 취약점 분석에는 실습1에서 사용한 도구들 외에도 사용 가능 - 단, 실습 3-2의 취약점 제외 - 본인이 직접 수행한 것이 증빙 가능해야 함
제출물	보고서 (양식 준수)
평가기준	1. 타겟 어플리케이션 설명 (어플리케이션 당 각 10점, 총 20점) 2. 취약점에 대한 공격 재현 (screenshot 필수, 어플리케이션 당 각 10점, 총 20점) 3. 취약점 분석에 사용한 모든 도구 및 분석 방법 설명 (screenshot 필수, 어플리케이션 당 각 15점, 총 30점) 4. 취약점 분석 결과 설명 (screenshot 필수, 어플리케이션 당 각 10점, 총 20점) 5. 취약점 대응 방안 설명 (어플리케이션 당 각 5점, 총 10점)

[Option B: 구현]

요구사항	보안 취약점을 내재한 안드로이드 어플리케이션 1개를 구현한다. - 구현 어플리케이션은 1개 이상의 정상적인 기능과 1개 이상의 보안 취약점을 내재해야 함 - 구현 어플리케이션은 처음부터 설계 및 구현, 혹은 기존의 어플리케이션(InsecureBankv2 제외)을 수정하는 것 중 선택하여 진행 가능 - 단, 실습 3-2의 취약점 제외 - 본인이 직접 수행한 것이 증빙 가능해야 함
제출물	APK 파일, 소스 코드, 보고서 (양식 준수)
평가기준	1. 구현 어플리케이션 설명 (20점) 2. 취약점에 대한 공격 재현 (screenshot 필수, 20점) 3. 구현 어플리케이션 취약점 설명 (screenshot 필수, 20점) 4. 구현 어플리케이션 완성도 (30점) 5.. 취약점 구현 독창성 (10점) *가산점: 취득 점수의 50% (APK 파일의 AVD runtime 정상 동작 확인 시)