오픈API 이용 핀테크서비스(앱/웹) 취약점 점검항목 안내서

- 본 안내서는 금융권 오픈API의 안전한 이용을 위한 API 이용 핀테크서비스 취약점 점검에 대한 이해 및 사전 조치를 돕기 위하여 작성된 참고용 자료입니다.
- 금융보안원에서 사원기관에 공유하는 자료로서 인터넷에 게시되거나 외부에 유출되지 않도록 유의해주시기 바라며, API 이용기관에 취약점 점검 준비를 목적으로 제공 필요시 무단 게시 및 유출되지 않도록 각별히 주의하여 제공해주시기 바랍니다.
- 중점 점검사항에 '주요 취약점 발생 사례'를 예시하고 있으나, 예시된 사례 외에도 다른 취약점이 존재할 수 있음을 유의하여 활용하여 주시기 바랍니다.

1. 모바일앱(안드로이드, iOS)

분야	항목 번호	점검항목	점검항목 개요	중점 점검사항
중요정보 보호	M-I-1	메모리 내 노출 방지 수준	기밀성이 요구되는 이용자 중요정보의 메모리 내 평문 노출 여부를 점검	□ 이용자 중요정보*의 메모리 내 평문(또는 쉽게 평문으로 변환 가능한 문자열) 노출 여부를 점검 * 오픈API 관련 중요정보(access_token, client_secret 등), 이용자 중요정보(고유식별정보, 전자금융거래 관련 비밀번호, 기타 중요 인증정보 등) 등 □ 특히 중요정보 입력 및 전송 과정에서 메모리 내 중요정보 평문 노출 여부를 중점 점검 **※ 주요 취약점 발생 사례*** - 전자금융거래 관련 비밀번호 입력 시 메모리 내 비밀번호가 평문형태로 노출되는 경우 - 전자금융거래 관련 비밀번호 전송 이후 메모리 내 비밀번호가 평문형태로 노출되는 경우 * 발생할 수 있는 취약 사례에 대한 주요 예를 든 것으로 기술한 사례 외에도 취약점이 발생할 수 있음
	M-I-2	네크워크 구간 내 노출 방지 수준	기밀성이 요구되는 중요정보의 네트워크 구간 내 평문 노출 여부 및 네트워크 보안 설정 등을 점검	□ 중요정보의 네트워크 구간 내 평문(또는 쉽게 평문으로 변환 가능한 문자열) 노출 여부를 점검 □ 통신 구간 암호화를 위하여 HTTPS를 적용한 경우, 취약한 HTTPS 정책(취약한 프로토콜 이용, 취약한 암호 알고리즘 이용 등)의 존재 여부 점검 **※ 주요 취약점 발생 사례** - 통신구간 암호화가 적용되지 않아 네트워크 구간 내 전자금융거래 관련 비밀번호가 평문형태로 노출되는 경우 - 취약한 HTTPS 프로토콜(SSL 3.0)을 이용하는 경우
	M-I-3	디버그 로그 내 노출 방지 수준	기밀성이 요구되는 중요정보의 디버그 로그 내 평문 노출 여부를 점검	□ 디버그 로그 내 중요정보의 평문 노출 여부를 점검 **※ 주요 취약점 발생 사례** - 로그인 시 디버그 로그 내 계정정보가 평문형태로 노출되는 경우
	M-I-4	중요정보 파일 저장 수준	기밀성이 요구되는 중요정보의 단말 내 저장 여부를 점검	□ 이용자 단말의 점검대상 앱 관련 폴더 및 외부 저장소 내 중요정보 저장 여부를 점검

분야	항목 번호	점검항목	점검항목 개요	중점 점검사항
				※ **주요 취약점 발생 사례** - 이용자 단말의 점검대상 앱 관련 폴더 내 계정정보를 평문 형태로 저장하는 경우
	M-I-5	중요정보 화면 표시 및 보호 수준	기밀성이 요구되는 중요정보의 화면 표시 및 화면캡처를 통한 탈취 가능 여부를 점검	□ 중요정보의 화면 표시 및 평문(원본*) 노출 여부를 점검 * 본인인증을 위해 신분증 이미지파일을 업로드하는 경우, 신분증에 기재된 중요정보가 마스킹되지 않은 원본 이미지파일을 의미 □ 중요정보가 평문(원본) 형태로 화면에 표시되는 경우 화면캡처를 통한 탈취 가능 여부, 백그라운드 상태로 진입 시 저장되는 스냅샷 파일 내 평문(원본) 노출 여부 등을 점검 ※ **주요 취약점 발생 사례** - 본인인증을 위한 신분증 촬영 시 원본파일이 노출되는 동시에 화면캡처가 가능한 경우
	M-I-6	입력정보 보호 적용 수준	이용자 입력 중요정보의 노출 방지를 위해 구현된 보호기능 적용 여부를 점검	□ 이용자가 입력하는 중요정보의 노출 방지를 위해 구현된 보호기능 적용 여부를 점검 ※ **주요 취약점 발생 사례** - 전자금융거래 관련 비밀번호 입력 시 별도의 보호기능이 적용되지 않은 경우
거래정보 위·변조	M-F-1	계좌정보 변조 방지 수준	전자금융거래 이용 중 무결성이 요구되는 계좌정보를 메모리 및 네트워크 구간에서 위·변조 시 부정이체 가능 여부를 점검	□ 전자금융거래 이용 중 메모리 및 네트워크 구간에서 계좌정보 위·변조 시 타인계좌 조회 및 위·변조된 계좌로 부정이체 가능 여부를 점검 ※ **주요 취약점 발생 사례** - 계좌이체 각 단계에서 입·출금 계좌번호를 타인의 계좌번호로 변조 후 이체거래가 정상적으로 진행되는 경우
	M-F-2	금액변조 방지 수준	전자금융거래 이용 중 무결성이 요구되는 금액정보를 메모리 및 네트워크 구간에서 위·변조 시 부정이체 가능 여부를 점검	□ 전자금융거래 이용 중 메모리 및 네트워크 구간에서 금액정보 위·변조 시 위·변조된 금액으로 부정이체 가능 여부를 점검

분야	항목 번호	점검항목	점검항목 개요	중점 점검사항
				※ 주요 취약점 발생 사례 - 계좌이체 각 단계에서 이체금액 변조 후 이체거래가 정상적으로 진행되는 경우 - 계좌이체 시 이체가 제한되는 금액*으로 이체거래가 정상적으로 진행되는 경우 * 예: 이체한도 초과 금액, 음수 등
	M-F-3	거래정보 재사용 방지 수준	전자금융거래에 이용되는 거래정보의 재사용 가능 여부를 점검	□ 전자금융거래시 이용된 거래정보를 재전송하여 재사용 및 타인에 의해 무단사용 가능 여부를 점검 **※ 주요 취약점 발생 사례** - 계좌이체 시 이용된 거래정보(패킷)를 취득 후 재전송하여 이체거래가 정상적으로 진행되는 경우 - 타 이용자의 거래정보를 취득 후 재전송하여 이체거래가 정상적으로 진행되는 경우
클라이언트 보안	M-C-1	앱 위·변조 탐지 적용 수준	점검대상 앱의 중요파일에 대한 위·변조 수행 후 서비스 정상 실행 가능 여부를 점검	□ 변조된 프로그램이 정상실행될 경우 악성코드가 포함되어 재배포 되는 등의 보안 위협이 존재함에 따라, 변조* 프로그램 이용 시 정상 실행 가능 여부를 점검 * 앱 설치파일, 설치 후 실행파일 등의 변조 **※ 주요 취약점 발생 사례** - 점검대상 앱 설치파일 위·변조 후 설치 시 정상 실행이 가능한 경우 - 점검대상 앱 설치 후 중요파일* 위·변조 후 정상 실행이 가능한 경우 * 예: 실행파일, 관련 라이브러리 등
	M-C-2	해킹OS 탐지 적용 수준	루팅/탈옥된 단말에서 점검대상 앱 실행 시 정상 실행 가능 여부를 점검	□ 루팅/탈옥된 단말에서 점검대상 앱 실행 시 정상 실행 가능 여부를 점검 **※ 주요 취약점 발생 사례** - 루팅/탈옥된 단말에서 점검대상 앱을 설치 후 실행 시 정상 실행이 가능한 경우
	M-C-3	안티디버깅 적용·탐지 수준	디버거를 이용한 동적 디버깅 시도 시 정상 실행 가능 여부를 점검	□ 동적 디버깅 가능 시, 프로그램 흐름 파악 등이 용이함에 따라 안티디버깅 기능 적용 여부를 점검

분야	항목 번호	점검항목	점검항목 개요	중점 점검사항
				※ 주요 취약점 발생 사례 - 디버거를 이용하여 동적 디버깅 시도 시 정상 실행이 가능한 경우 - 안드로이드의 경우 앱 설정파일 내 디버깅 설정*이 “true”로 되어있는 경우 * AndroidManifest.xml 파일 내 android:debuggable 플래그
	M-C-4	코드 난독화 적용 수준	점검대상 앱의 디컴파일 가능 여부 및 복구된 소스코드의 난독화 적용 여부를 점검	□ 점검대상 앱을 디컴파일하여 복구된 소스코드에 클래스명, 함수명 등이 노출될 경우 공격자의 프로그램 구조 및 코드 흐름 파악이 용이해짐에 따라 코드 난독화 적용 여부를 점검 **※ 주요 취약점 발생 사례** - 점검대상 앱의 디컴파일이 가능한 경우 디컴파일하여 복구된 소스코드에 프로그램 구조 및 코드 흐름 파악에 도움이 되는 정보(클래스명 함수명 등)가 평문형태로 노출되는 경우
	M-C-5	안티바이러스 적용 수준	점검대상 앱 실행 시 악성코드 방지 대책을 점검	□ 악성코드에 대한 대응이 필요함에 따라, 점검대상 앱 실행 시 안티바이러스 프로그램 실행 여부 등을 점검 **※ 주요 취약점 발생 사례** - 점검대상 앱 실행 시 안티바이러스 프로그램이 실행되지 않는 경우
서버 보안	M-S-1	서버 보안 적용 수준	잘 알려진 웹서비스 취약점에 대한 보안대책 적용 등 서버 보안대책의 적용 여부를 점검	□ SQL 인젝션, XSS, CSRF 등의 웹 취약점 존재 여부 □ 리다이렉트 기능이 존재하는 경우 URL 인자값을 임의의 페이지로 변경하여 변경된 페이지로 이동 가능 여부를 점검 □ 불필요한 웹 메소드 허용 여부를 점검 □ 검색엔진 등을 통해 점검대상 관련 중요정보의 획득 가능 여부를 점검 □ HTTP 응답헤더, 에러페이지 등을 통한 서버정보(버전정보, 절대경로, 소스코드 등) 노출 여부를 점검 □ 유추 가능한 경로 등을 통한 관리자 페이지 접근 가능 여부를 점검 □ 불필요한 파일(테스트 파일, 백업 파일 등) 노출 여부를

분야	항목 번호	점검항목	점검항목 개요	중점 점검사항
				점검 **※ 주요 취약점 발생 사례** - URL 파라미터 등에 SQL 구문을 입력 시 구문의 의미에 따라 결과값이 변화하는 경우 - 요청값에 삽입한 스크립트가 이용자 구간에서 실행이 가능한 경우 - 파일 업로드/다운로드 등의 웹 취약점이 존재하는 경우 - 에러페이지 내 서버 버전정보, 에러가 발생한 소스코드, 에러가 발생한 파일의 절대경로 등이 노출되는 경우 - 관리자페이지에 유추 가능한 경로(/admin, /manager 등)를 통해 접근이 가능한 경우
인증	M-A-1	멀티로그인 탐지 적용 수준	서로 다른 단말에서 동일 계정으로 로그인 시 탐지 및 대응 여부를 점검	□ 멀티로그인 가능할 경우 제3자의 로그인에 대해 추적 및 관리가 불가능함에 따라 멀티 디바이스 로그인 제한* 여부를 점검 * 예시: 접속 차단, 경고메시지 출력 등 **※ 주요 취약점 발생 사례** - 서로 다른 단말에서 동일 계정으로 로그인이 가능하며, 별도의 대응이 없는 경우
	M-A-2	인증 우회 방지 적용 수준	이용자 인증 및 세션 관리와 관련된 기능 구현의 적정성을 점검	□ 이용자 인증 시 사용된 인증정보를 재전송하여 인증권한 획득 가능 여부를 점검 □ 이용자 인증 후 세션ID를 타 단말에 적용 시 인증절차 우회 가능 여부를 점검 □ 이용자 인증 후 서비스 이용 없이 일정 시간 경과 시 세션 종료 여부를 점검 □ 이용자 인증 시 이용되는 인증정보(예:세션ID, SMS 인증코드 등)를 가변적으로 생성하여 사용하는지 여부를 점검 □ 전자금융거래, 로그인 등의 절차 진행 시 요구되는 비밀번호의 보호조치* 적용 여부를 점검 * 복잡도 검증, 오류횟수 제한 등 ※ 이체거래 시 추가 인증수단(예: 거래 비밀번호)이 적용되어 있지 않은 경우 추가 인증수단 적용을 권고 □ 이용자 인증이 요구되는 페이지*에 접근 시 이용자 권한 확인 및 파라미터 변조, 클라이언트 스크립트 변조 등을 통한 인증 우회 가능 여부를 점검

분야	항목 번호	점검항목	점검항목 개요	중점 점검사항
				* 민감정보가 포함된 페이지, 거래비밀번호 변경 페이지 등 □ 인증파일 변조, 화면 강제실행 등을 통한 인증절차 우회 가능 여부를 점검 ※ OAuth 인증 과정에서 웹뷰를 이용하여 이용자 확인 페이지를 출력하는 경우 피싱의 위협이 있으므로 안전한 방식을 통해 이용자 확인 페이지를 출력할 것을 권고 ※ 이용자 인증 시 타 사이트의 인증을 이용하는 경우(Google 로그인 등) 해당 사이트(Google 등) 계정에 강화된 인증절차 적용을 권고 **※ 주요 취약점 발생 사례** - 전자금융거래시 사용되는 인증정보를 취득 후 재전송하여 정상적으로 권한 획득이 가능한 경우 - 이용자 인증 후 세션ID를 별도의 IP주소를 사용하는 단말에 적용하여 인증절차 우회가 가능한 경우 - 이용자 로그인 시 항상 동일한 세션ID를 부여받는 경우 - 입·출금이체 등의 전자금융거래 진행 시 추가인증절차가 적용되어 있지 않은 경우 - 거래비밀번호에 대한 복잡도 검증이 이루어지지 않아 '000000', '123456' 등의 비밀번호 설정이 가능한 경우 - 파라미터, 쿠키 등을 통해 전달되는 이용자 식별정보를 변조하여 타 이용자 권한 획득이 가능한 경우 - 점검대상 앱 관련 폴더 등에 저장된 이용자 인증파일을 타 단말에 적용하여 인증권한 획득이 가능한 경우

2. 웹(Web)

분야	항목 번호	점검항목	점검항목 개요	중점 점검사항
중요정보 보호	W-I-1	메모리 내 노출 방지 수준	기밀성이 요구되는 이용자 중요정보의 메모리 내 평문 노출 여부를 점검	□ 이용자 중요정보의 메모리 내 평문(또는 쉽게 평문으로 변환 가능한 문자열) 노출 여부를 점검 □ 특히 중요정보 입력 및 전송 과정에서 메모리 내 중요정보 평문 노출 여부를 중점 점검 **※ 주요 취약점 발생 사례** - 전자금융거래 관련 비밀번호 입력 시 메모리 내 비밀번호가 평문형태로 노출되는 경우 - 전자금융거래 관련 비밀번호 전송 이후 메모리 내 비밀번호가 평문형태로 노출되는 경우
	W-I-2	DOM 영역 내 노출 방지 수준	기밀성이 요구되는 중요정보의 DOM 영역 내 평문 노출 여부를 점검	□ 중요정보의 DOM 영역 내 평문 노출 여부를 점검 □ 특히 중요정보 입력 및 전송 이후 과정에서 DOM 내 중요정보 평문 노출 여부를 중점 점검 **※ 주요 취약점 발생 사례** - 전자금융거래 관련 비밀번호 입력 시 DOM 영역 내 비밀번호가 평문형태로 노출되는 경우 - 자바스크립트 소스코드 내 client_secret이 하드코딩 되어있는 경우
	W-I-3	네트워크 구간 내 노출 방지 수준	기밀성이 요구되는 중요정보의 네트워크 구간 내 평문 노출 여부 및 네트워크 보안 설정 등을 점검	□ 중요정보의 네트워크 구간 내 평문(또는 쉽게 평문으로 변환 가능한 문자열) 노출 여부를 점검 □ 통신 구간 암호화를 위하여 HTTPS를 적용한 경우, 취약한 HTTPS 정책(취약한 프로토콜 이용, 취약한 암호 알고리즘 이용 등)의 존재 여부 점검 **※ 주요 취약점 발생 사례** - 통신구간 암호화가 적용되지 않아 네트워크 구간 내 전자금융거래 관련 비밀번호가 평문형태로 노출되는 경우 - 취약한 HTTPS 프로토콜(SSL 3.0)을 이용하는 경우
	W-I-4	중요정보 파일 저장 수준	기밀성이 요구되는 중요정보의 이용자구간 내 저장 여부를 점검	□ 이용자 단말 내 중요정보 파일 저장 여부를 점검 **※ 주요 취약점 발생 사례** - 이용자 인증과정 진행 시 중요정보가 포함된 파일이 생성되는 경우

분야	항목 번호	점검항목	점검항목 개요	중점 점검사항
	W-I-5	중요정보 화면 표시 및 보호 수준	기밀성이 요구되는 중요정보의 화면 표시 및 화면캡처를 통한 탈취 가능 여부를 점검	□ 중요정보의 화면 표시 및 평문 노출 여부를 점검 □ 중요정보가 평문 형태로 화면에 표시되는 경우 화면캡처를 통한 탈취 가능 여부 등을 점검 **※ 주요 취약점 발생 사례** - 전자금융거래 관련 비밀번호 입력 시 비밀번호가 평문형태로 노출되는 동시에 화면캡처가 가능한 경우
	W-I-6	입력정보 보호 적용 수준	이용자 입력 중요정보의 노출 방지를 위해 구현된 보호기능 적용 여부를 점검	□ 이용자가 입력하는 중요정보의 노출 방지를 위해 구현된 보호기능 적용 여부를 점검 **※ 주요 취약점 발생 사례** - 전자금융거래 관련 비밀번호 입력 시 별도의 보호기능이 적용되지 않은 경우
거래정보 위·변조	W-F-1	계좌정보 변조 방지 수준	전자금융거래 이용 중 무결성이 요구되는 계좌정보를 메모리 및 네트워크 구간에서 위·변조 시 부정이체 가능 여부를 점검	□ 전자금융거래 이용 중 메모리, DOM 영역 및 네트워크 구간에서 계좌정보 위·변조 시 타인계좌 조회 및 위·변조된 계좌로 부정이체 가능 여부를 점검 **※ 주요 취약점 발생 사례** - 계좌이체 각 단계에서 입·출금 계좌번호를 타인의 계좌번호로 변조 후 이체거래가 정상적으로 진행되는 경우
	W-F-2	금액변조 방지 수준	전자금융거래 이용 중 무결성이 요구되는 금액정보를 메모리 및 네트워크 구간에서 위·변조 시 부정이체 가능 여부를 점검	□ 전자금융거래 이용 중 메모리, DOM 영역 및 네트워크 구간에서 금액정보 위·변조 시 위·변조된 금액으로 부정이체 가능 여부를 점검 **※ 주요 취약점 발생 사례** - 계좌이체 각 단계에서 이체금액 변조 후 이체거래가 정상적으로 진행되는 경우 - 계좌이체 시 이체가 제한되는 금액*으로 이체거래가 정상적으로 진행되는 경우 * 예: 이체한도 초과 금액, 음수 등
	W-F-3	거래정보 재사용 방지 수준	전자금융거래에 이용되는 거래정보의 재사용 가능 여부를 점검	□ 전자금융거래시 이용된 거래정보를 재전송하여 재사용 및 타인에 의해 무단사용 가능 여부를 점검 **※ 주요 취약점 발생 사례** - 계좌이체 시 이용된 거래정보(패킷)를 취득 후 재전송하여 이체거래가 정상적으로 진행되는 경우 - 타 이용자의 거래정보를 취득 후 재전송하여 이체거래가 정상적으로 진행되는 경우

분야	항목 번호	점검항목	점검항목 개요	중점 점검사항
서버 보안	W-S-1	서버 보안 적용 수준	잘 알려진 웹서비스 취약점에 대한 보안 대책 적용 등 서버 보안대책의 적용 여부를 점검	□ SQL 인젝션, XSS, CSRF 등의 웹 취약점 존재 여부 □ 리다이렉트 기능이 존재하는 경우 URL 인자값을 임의의 페이지로 변경하여 이동 가능 여부를 점검 □ 불필요한 웹 메소드 허용 여부를 점검 □ 검색엔진 등을 통해 점검대상 관련 중요정보의 획득 가능 여부를 점검 □ HTTP 응답헤더, 에러페이지 등을 통한 서버정보(버전정보, 절대경로, 소스코드 등) 노출 여부를 점검 □ 유추 가능한 경로 등을 통한 관리자 페이지 접근 가능 여부를 점검 □ 불필요한 파일(테스트 파일, 백업 파일 등) 노출 여부를 점검 **※ 주요 취약점 발생 사례** - URL 파라미터 등에 SQL 구문을 입력 시 구문의 의미에 따라 결과값이 변화하는 경우 - 요청값에 삽입한 스크립트가 이용자 구간에서 실행이 가능한 경우 - 파일 업로드/다운로드 등의 웹 취약점이 존재하는 경우 - 에러페이지 내 서버 버전정보, 에러가 발생한 소스코드, 에러가 발생한 파일의 절대경로 등이 노출되는 경우 - 관리자페이지에 유추 가능한 경로(/admin, /manager 등)를 통해 접근이 가능한 경우
인증	W-A-1	멀티로그인 탐지 적용 수준	서로 다른 단말에서 동일 계정으로 로그인 시 탐지 및 대응 여부를 점검	□ 멀티로그인 가능할 경우 제3자의 로그인에 대해 추적 및 관리가 불가능함에 따라 멀티 디바이스 로그인 제한* 여부를 점검 * 예시: 접속 차단, 경고메시지 출력 등 **※ 주요 취약점 발생 사례** - 서로 다른 단말에서 동일 계정으로 로그인이 가능하며, 별도의 대응이 없는 경우
	W-A-2	인증 우회 방지 수준	이용자 인증 및 세션 관리와 관련된 기능 구현의 적정성을 점검	□ 이용자 인증 시 사용된 인증정보를 재전송하여 인증권한 획득 가능 여부를 점검 □ 이용자 인증 후 세션ID를 타 단말에 적용 시 인증절차 우회 가능 여부를 점검 □ 이용자 인증 후 서비스 이용 없이 일정 시간 경과 시 세션 종료 여부를 점검

분야	항목 번호	점검항목	점검항목 개요	중점 점검사항
				□ 이용자 인증 시 이용되는 인증정보(예:세션ID, SMS 인증코드 등)를 가변적으로 생성하여 사용하는지 여부를 점검 □ 전자금융거래, 로그인 등의 절차 진행 시 요구되는 비밀번호의 보호조치* 적용 여부를 점검 * 복잡도 검증, 오류횟수 제한 등 ※ 이체거래 시 추가 인증수단(예: 거래 비밀번호)이 적용되어 있지 않은 경우 추가 인증수단 적용을 권고 □ 이용자 인증이 요구되는 페이지*에 접근 시 이용자 권한 확인 및 파라미터 변조, 클라이언트 스크립트 변조 등을 통한 인증 우회 가능 여부를 점검 * 민감정보가 포함된 페이지, 거래비밀번호 변경 페이지 등 ※ OAuth 이용자 인증 과정에서 iframe을 이용하여 이용자 확인 페이지를 출력하는 경우 피싱의 위협이 있으므로 안전한 방식을 통해 이용자 확인 페이지를 출력할 것을 권고 ※ 이용자 인증 시 타 사이트의 인증을 이용하는 경우(Google 로그인 등) 해당 사이트(Google 등) 계정에 강화된 인증절차 적용을 권고 **※ 주요 취약점 발생 사례** - 전자금융거래시 사용되는 인증정보를 취득 후 재전송하여 정상적으로 권한 획득이 가능한 경우 - 이용자 인증 후 세션ID를 별도의 IP주소를 사용하는 단말에 적용하여 인증절차 우회가 가능한 경우 - 이용자 로그인 시 항상 동일한 세션ID를 부여받는 경우 - 입·출금이체 등의 전자금융거래 진행 시 추가인증절차가 적용되어 있지 않은 경우 - 거래비밀번호에 대한 복잡도 검증이 이루어지지 않아 '000000', '123456' 등의 비밀번호 설정이 가능한 경우 - 파라미터, 쿠키 등을 통해 전달되는 이용자 식별정보를 변조하여 타 이용자 권한 획득이 가능한 경우