문서번호	J.W.P. MagicShop-250825
작성자	취약점진단팀
보안등급	Confidential
Ver	ver 1.0

"J.W.P. MagicShop" 취약점 진단

DBMS 진단 상세결과

2025년 08월 25일

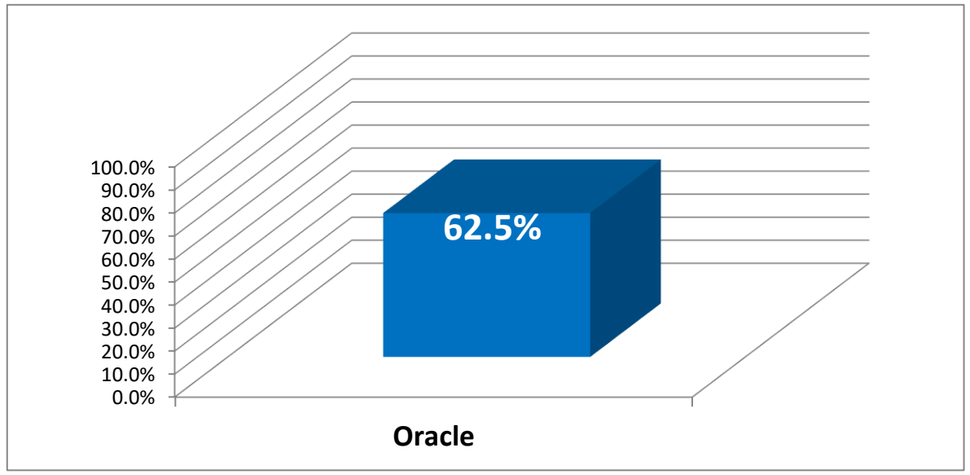
※ 진단 대상 리스트 - DBMS 1대 (Oracle 1대)

순번	진단 대상				비고
	Hostname	IP Address	버전정보	용도	
Oracle					
1	jwp-db-01	10.0.8.8	Oracle 21c XE	DBMS	

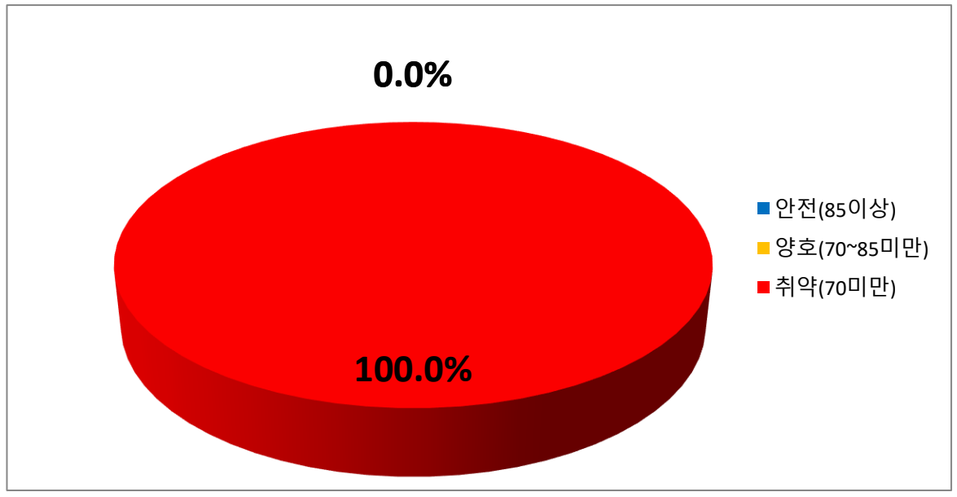
※ 대상별 평균 점수 그래프

대상별 평균 점수 현황

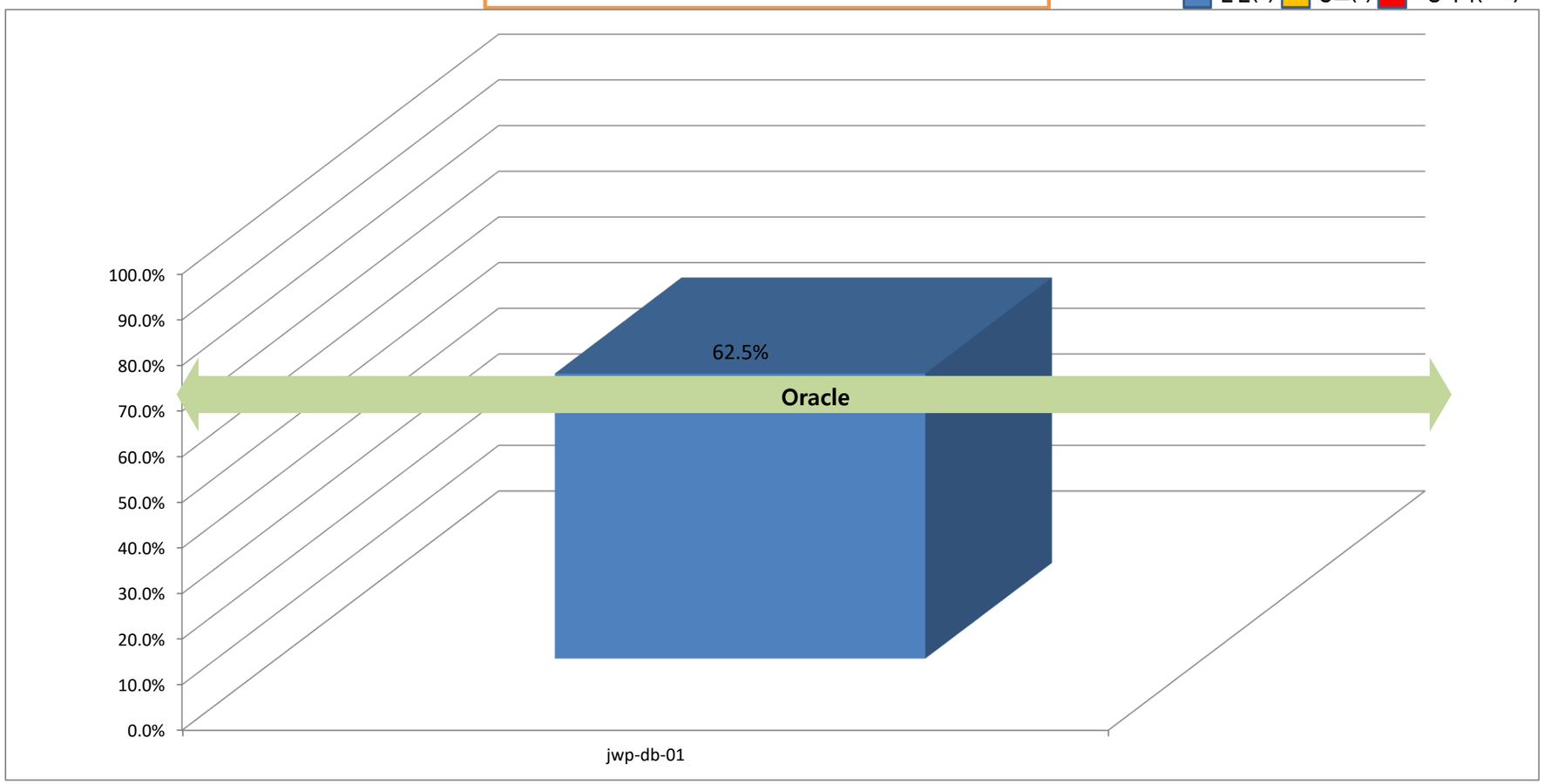
진단 대상	평균	수량
Oracle	62.5%	1



전체		1
안전(85이상)	0.0%	0
양호(70~85미만)	0.0%	0
취약(70미만)	100.0%	1



서버 진단결과

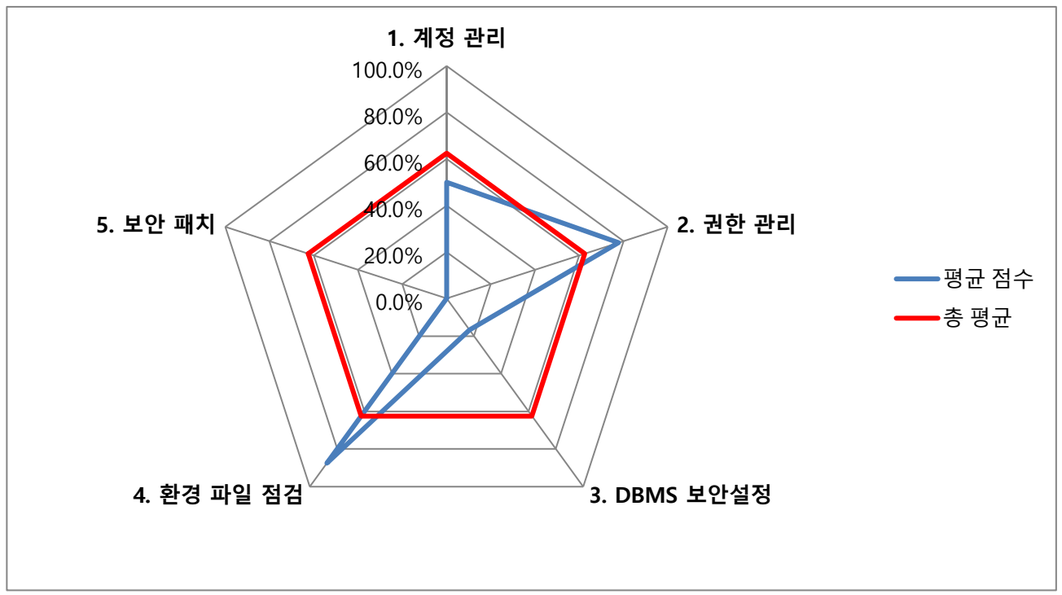


Oracle		
NO.	Hostname	점수
1	jwp-db-01	62.5%

Infosec | SK C&C

진단 도메인	평균 점수	총 평균
1. 계정 관리	50.0%	62.5%
2. 권한 관리	77.8%	62.5%
3. DBMS 보안설정	16.7%	62.5%
4. 환경 파일 점검	87.5%	62.5%
5. 보안 패치	0.0%	62.5%
6. 보안 감사 설정	100.0%	62.5%
7. 네트워크 접근 제어	N/A	62.5%

Oracle 항목별 진단 결과

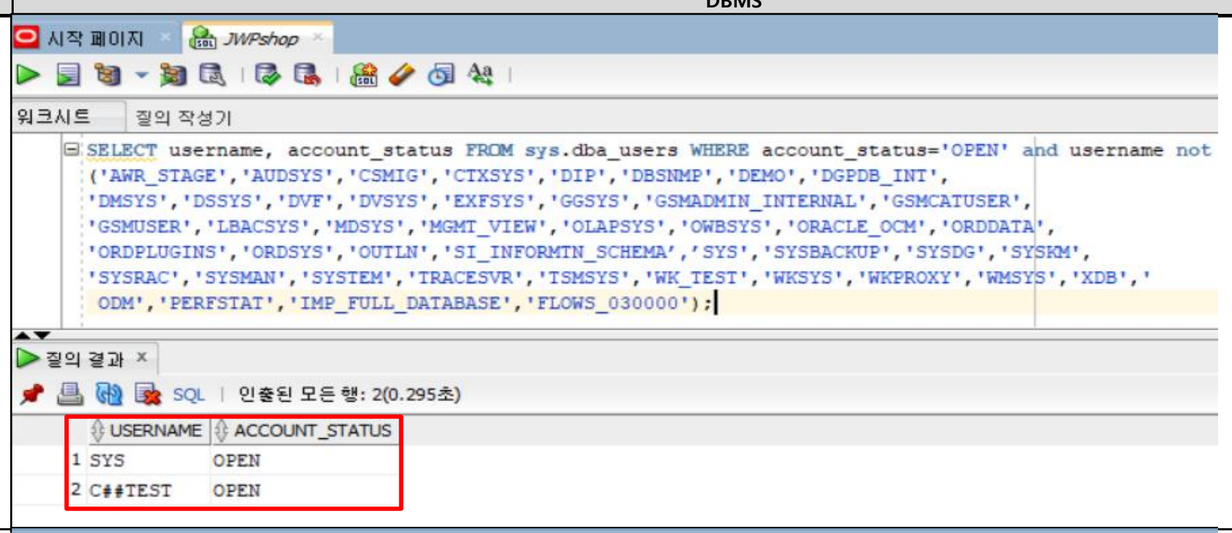
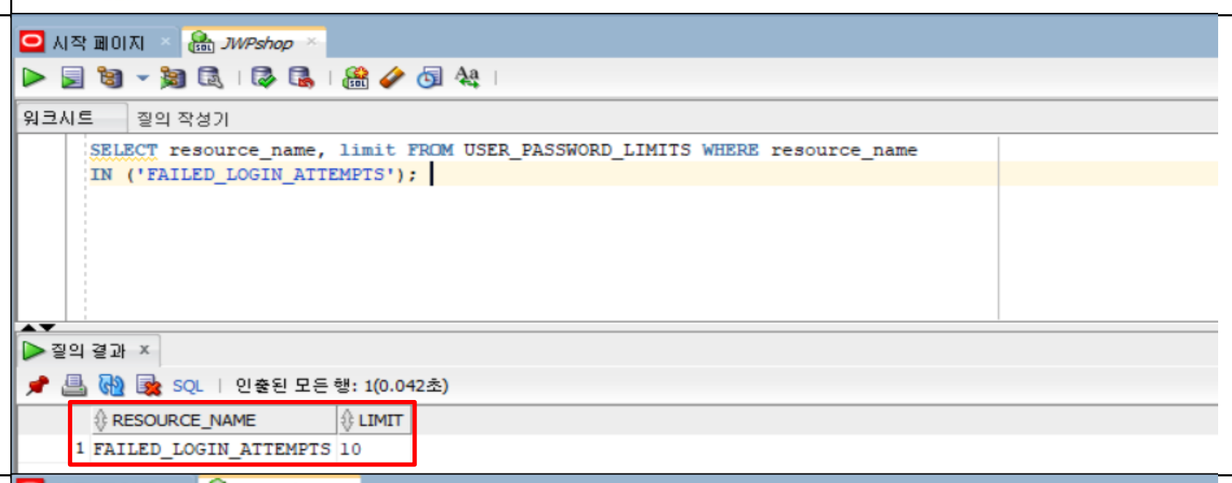
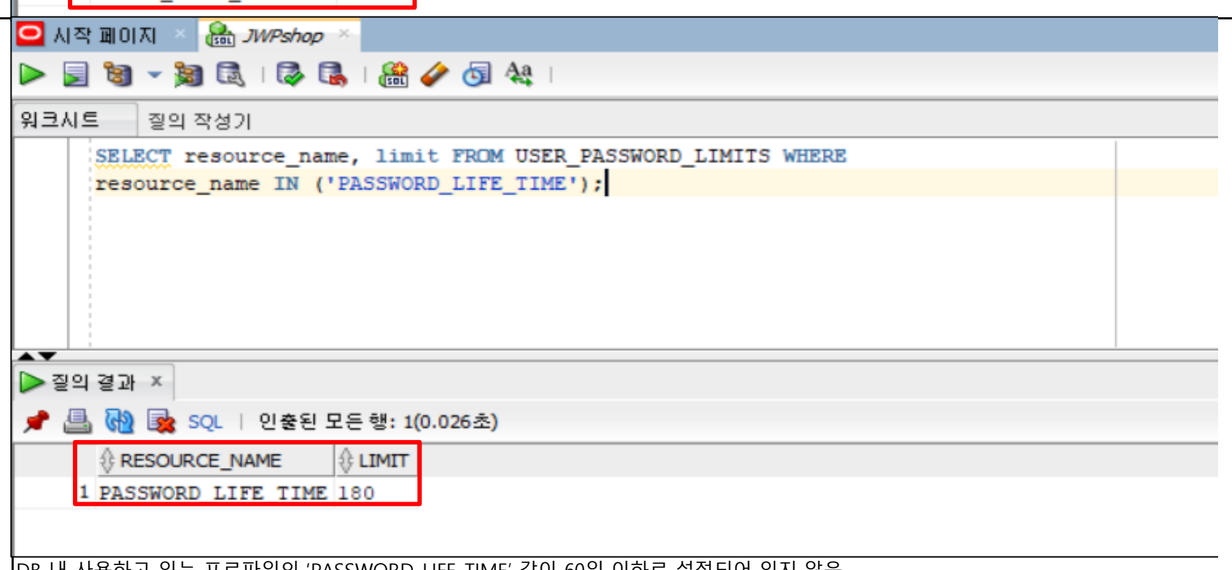
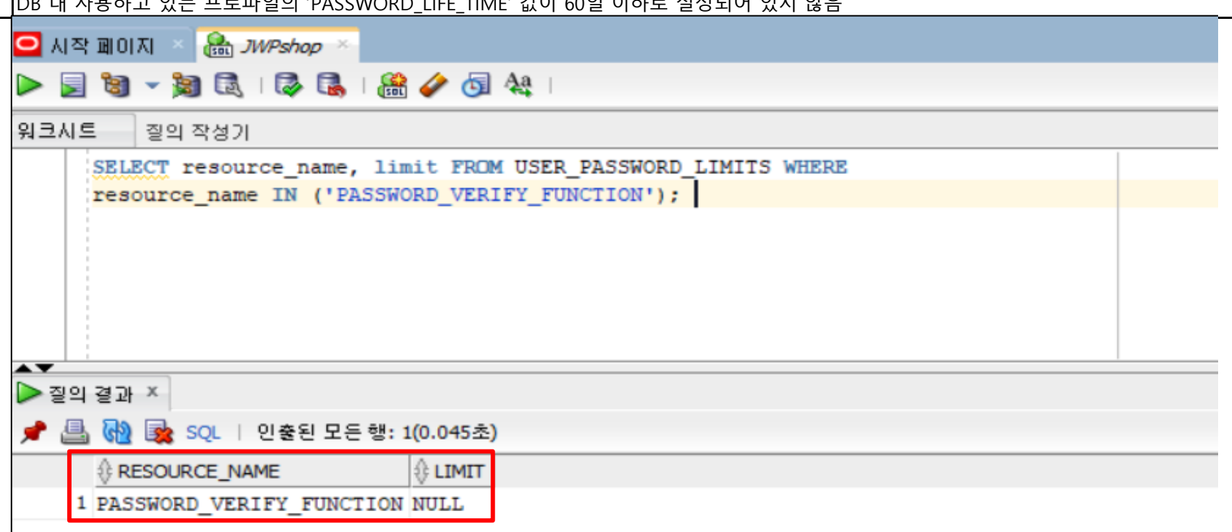
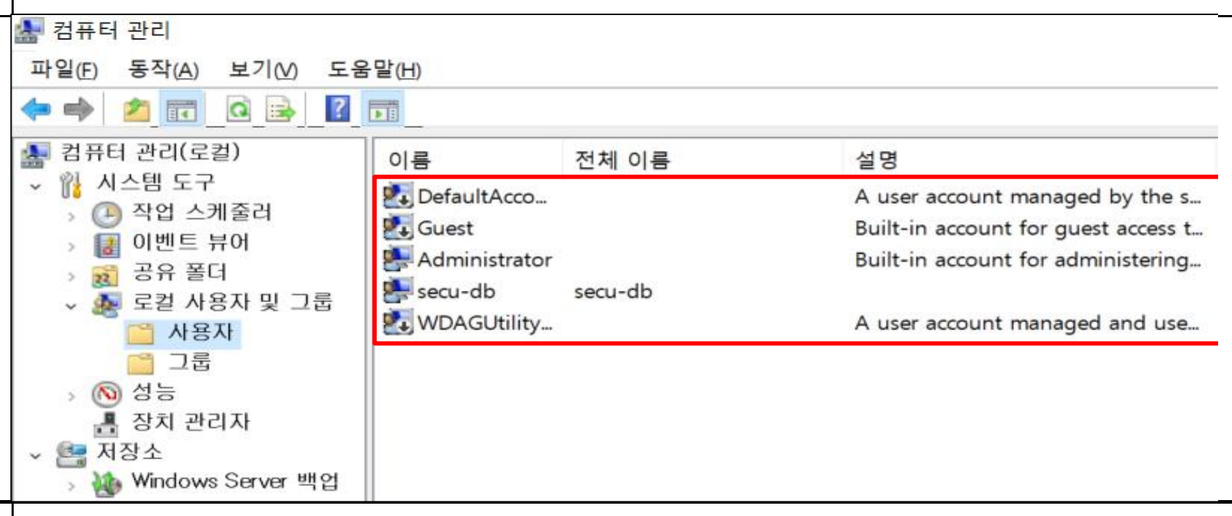


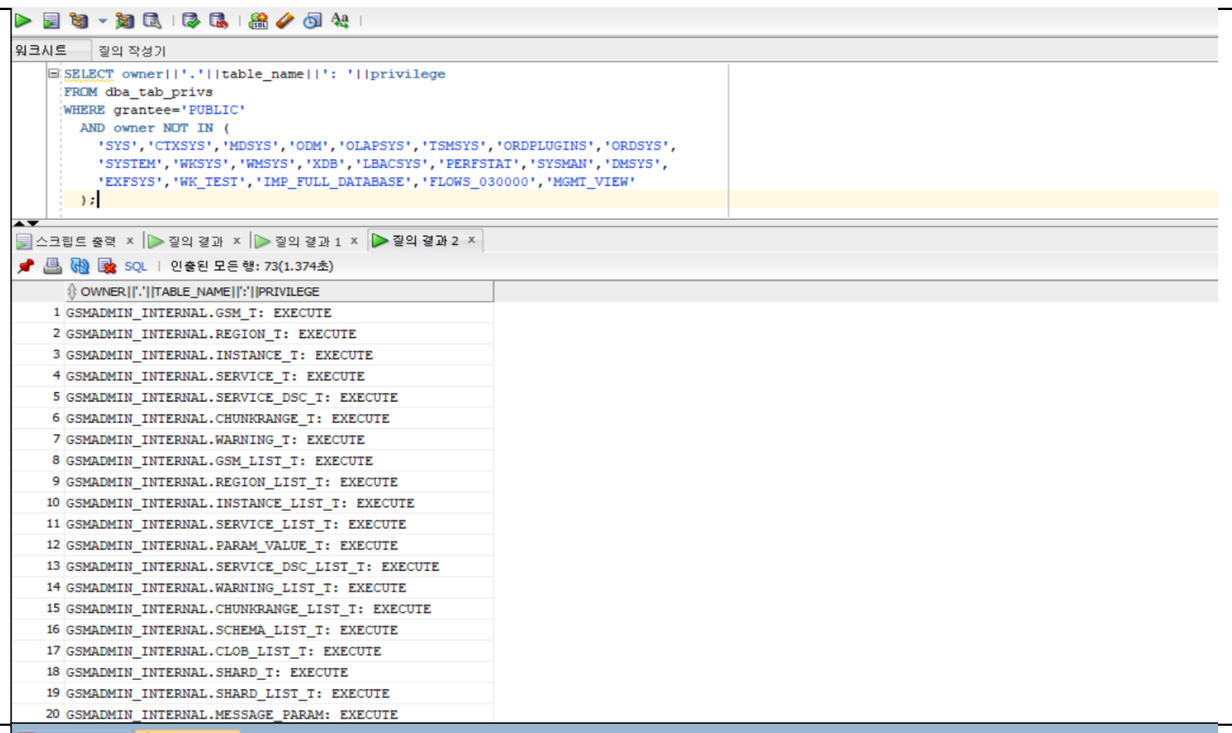
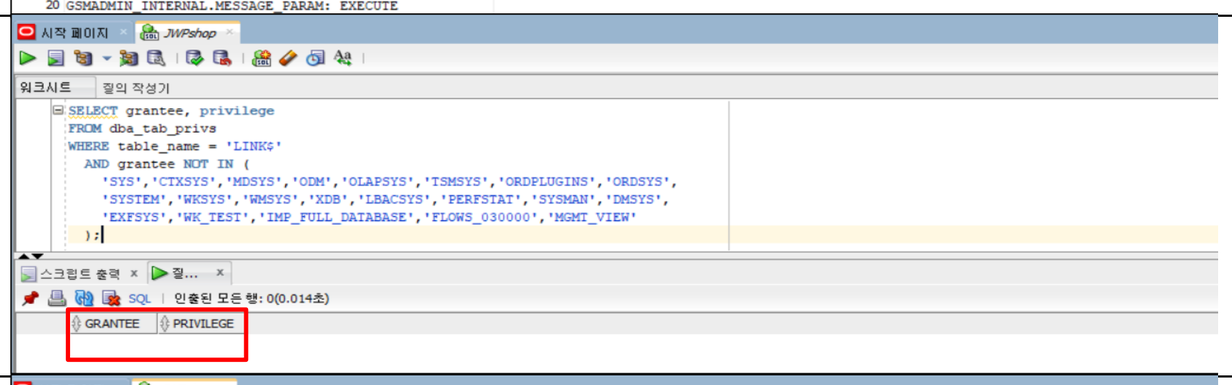
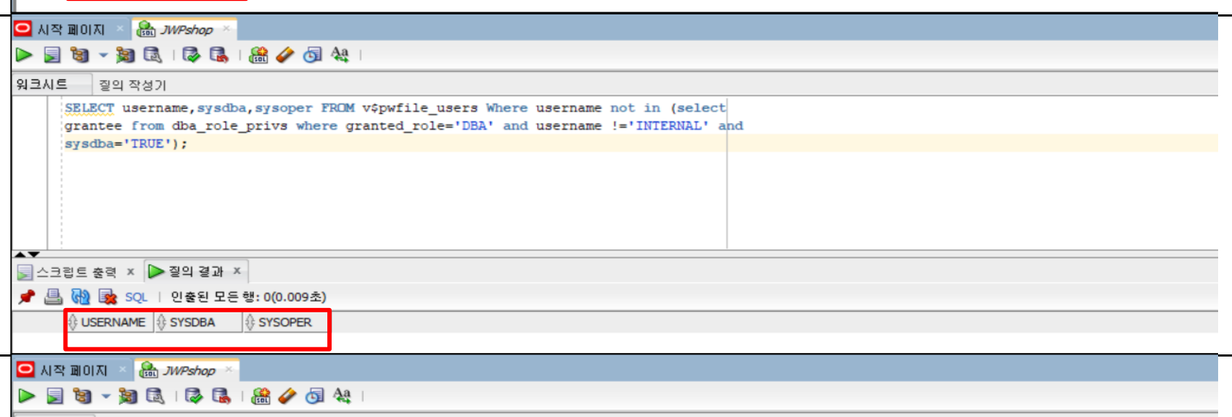
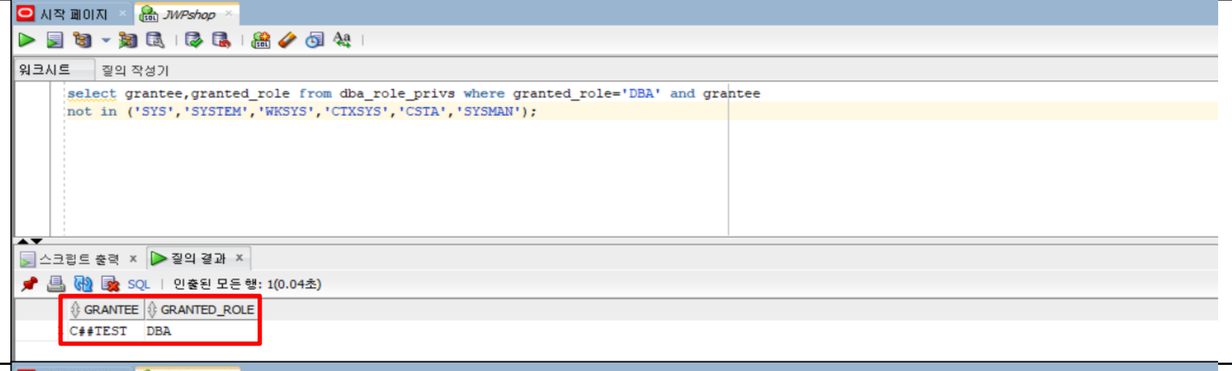
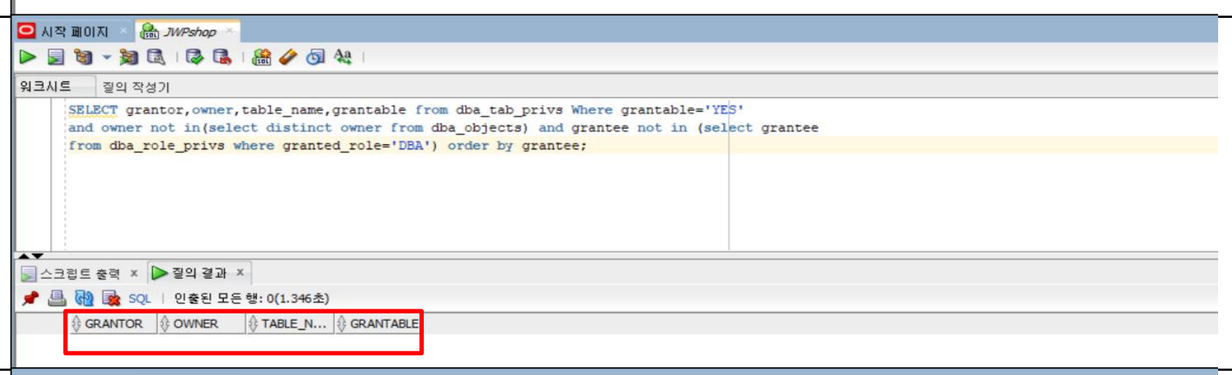
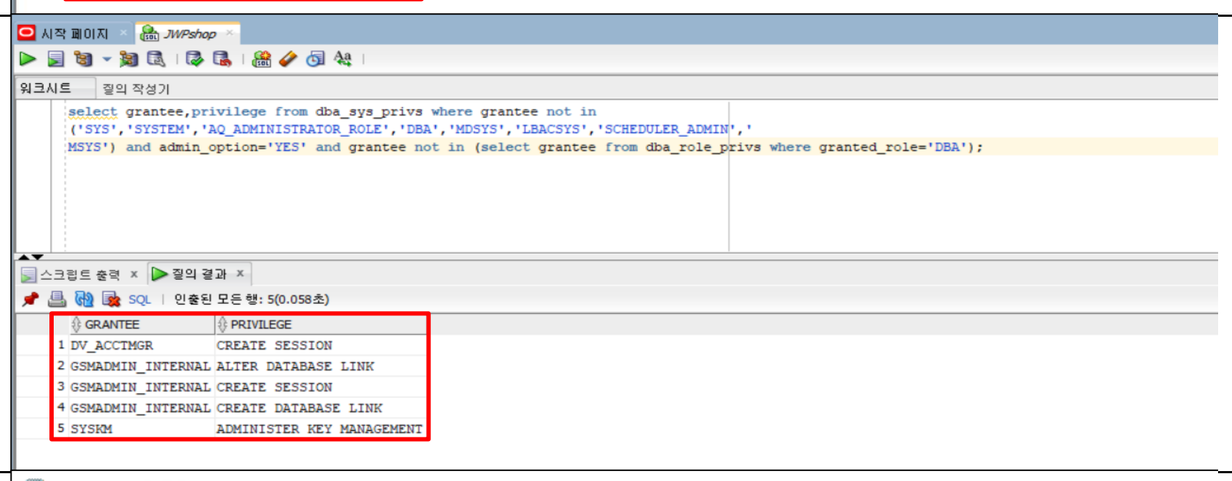
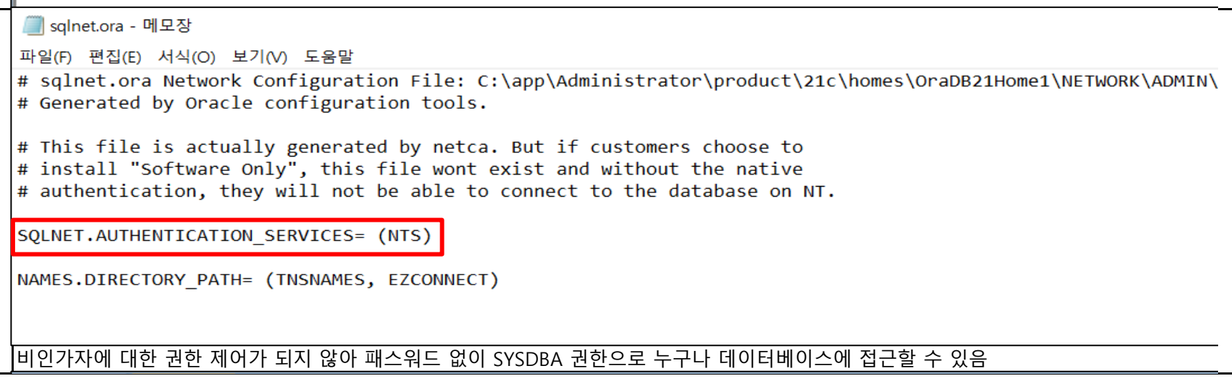
Oracle 취약점 진단 요약결과(34항목)

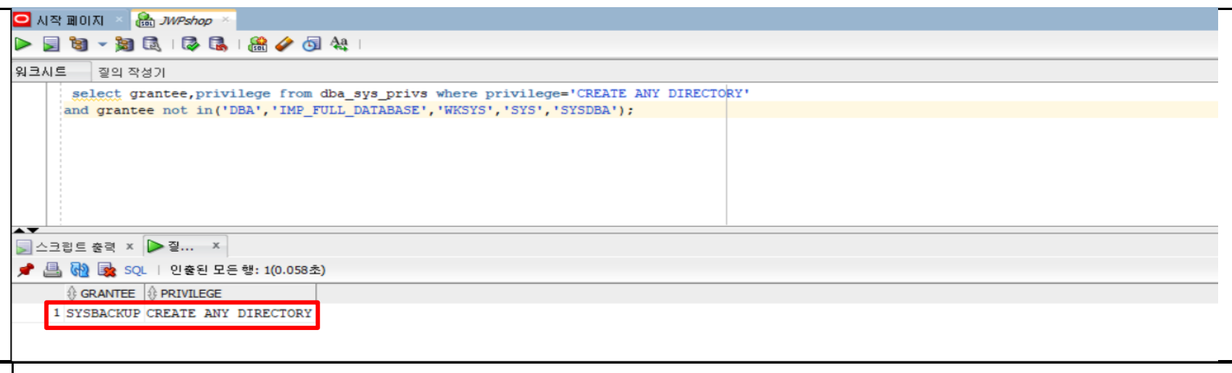
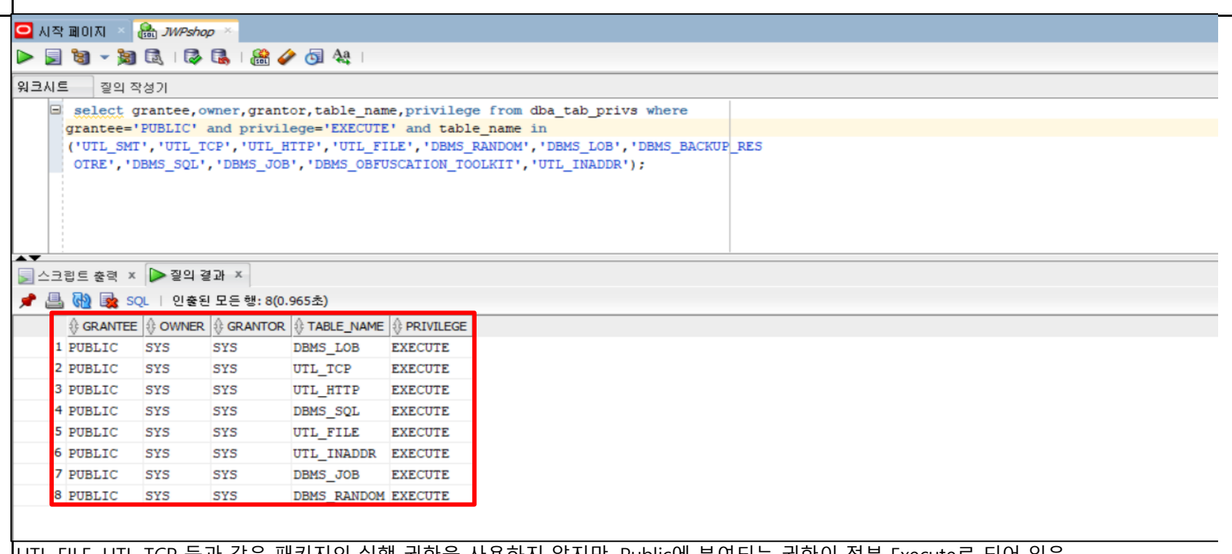
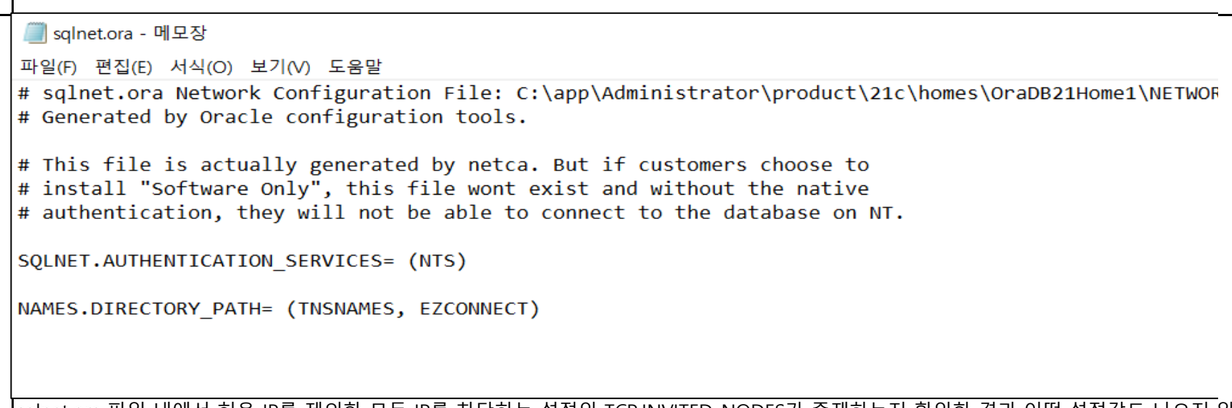
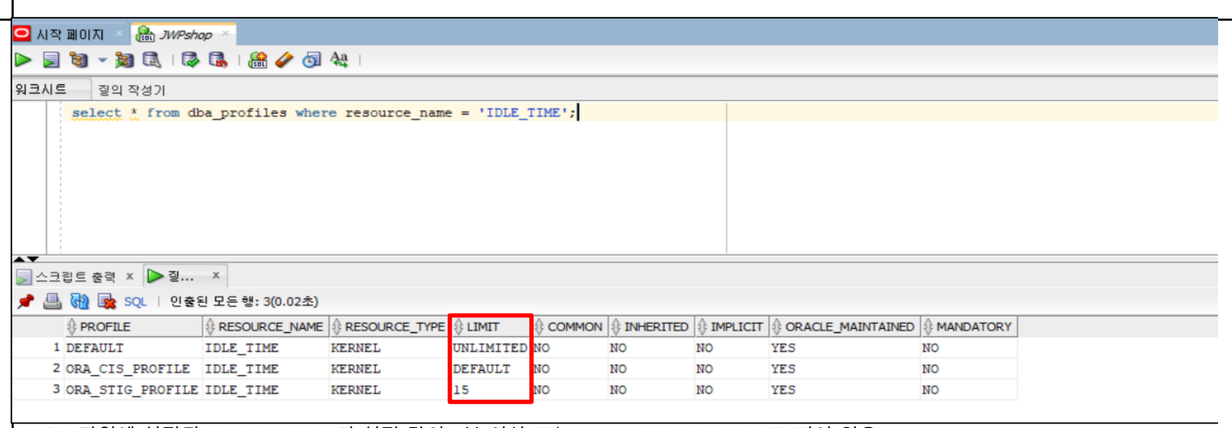
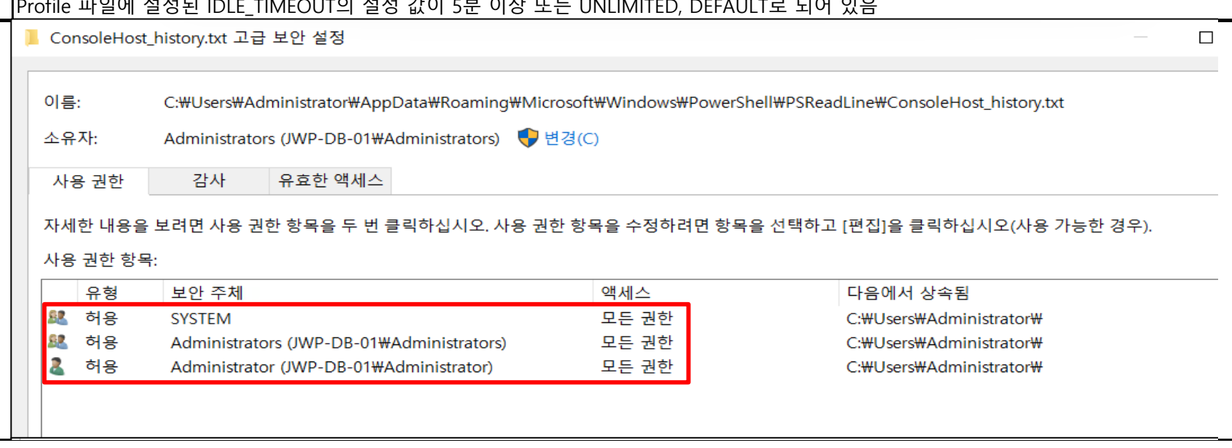
진단항목	No.	세부 진단항목	중요도	1 jwp-db-01 10.0.8.8
1. 계정 관리	1	불필요한 계정 확인	하	양호
	2	무제한 로그인 시도 차단	중	양호
	3	패스워드 주기적 변경	중	취약
	4	패스워드 복잡도 설정	중	취약
	5	취약한 패스워드 사용 점검	상	취약
	6	OS DBA 그룹 멤버 확인	하	양호
2. 권한 관리	1	개발 및 운영 시스템 분리 사용	하	취약
	2	Public에 대한 권한 제한	중	양호
	3	SYS.LINK$ 테이블 접근 제한	중	양호
	4	SYSDBA 권한 제한	상	양호
	5	DBA 권한 제한	상	양호
	6	with grant option 사용 제한	하	양호
	7	with admin option 사용 제한	하	양호
	8	SYSDBA 로그인 제한	상	취약
	9	CREATE ANY DIRECTORY 권한 제한	중	양호
3. DBMS 보안설정	1	백업 관리	하	취약
	2	PL/SQL Package의 Public Role 점검	상	취약
	3	Listener 보안 설정 여부	상	양호
	4	DB 접속 IP 통제	하	취약
	5	로그 저장 주기	상	취약
	6	세션 IDLE_TIMEOUT 설정	하	취약
4. 환경 파일 점검	1	SQL*PLUS 명령 히스토리 검사	하	양호
	2	Initialization 파일 접근 권한 설정	중	양호
	3	Oracle Password 파일 접근 권한 설정	중	양호
	4	AlertLog 파일 접근 제한	하	양호
	5	Trace Log 파일 접근 제한	하	양호
	6	컨트롤, redo 로그파일, 데이터 파일 접근 제한	중	양호
	7	$TNS_ADMIN 파일 접근 제한	중	취약
	8	감사 로그 파일 접근 제한	하	양호
5. 보안 패치	1	보안 패치 적용	상	취약
6. 보안 감사 설정	1	SYS 감사 수행 설정	하	양호
	2	Audit Trail 기록 설정	하	양호
7. 네트워크 접근 제어	1	DATA DICTIONARY 접근 제한	N/A	*N/A*
	2	원격 OS 인증 방식 설정	N/A	*N/A*
점검결과				12
		보안 적용율 (양호항목 / 진단항목) %		62.5%

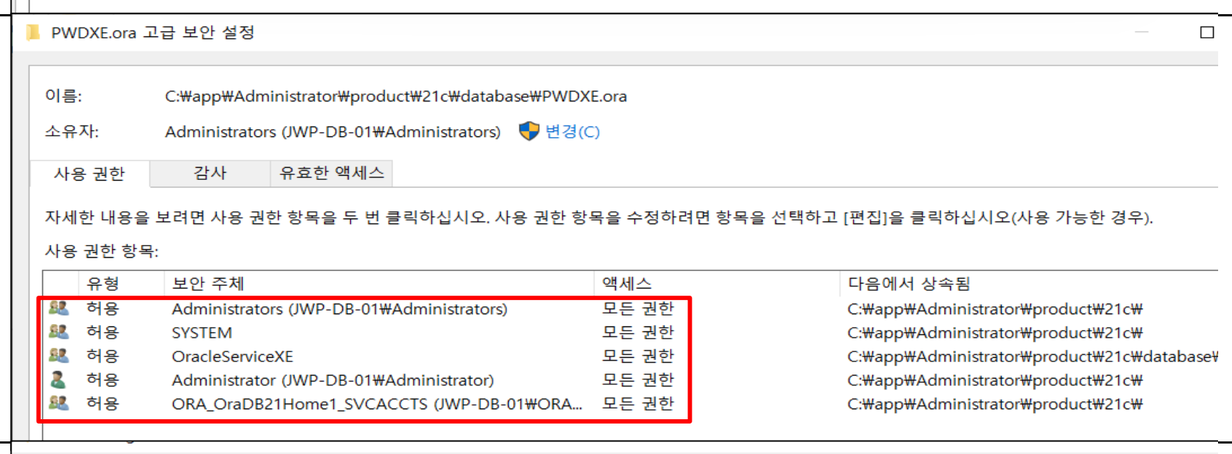
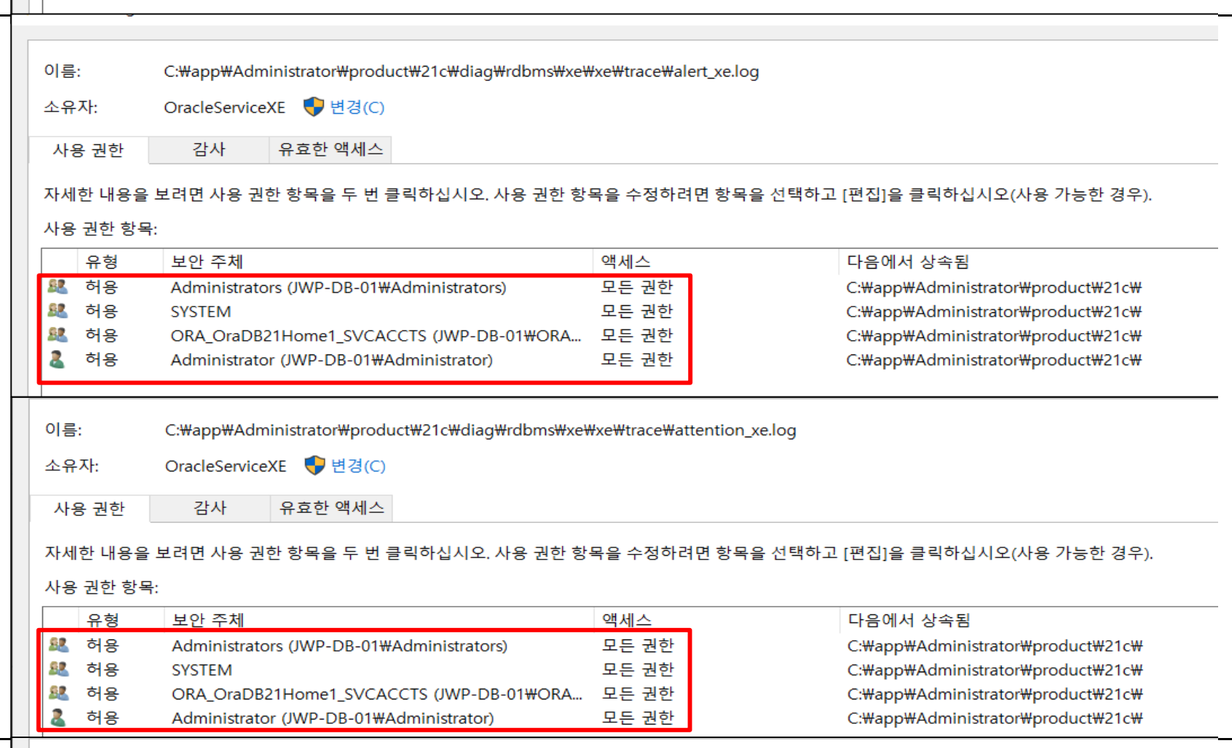
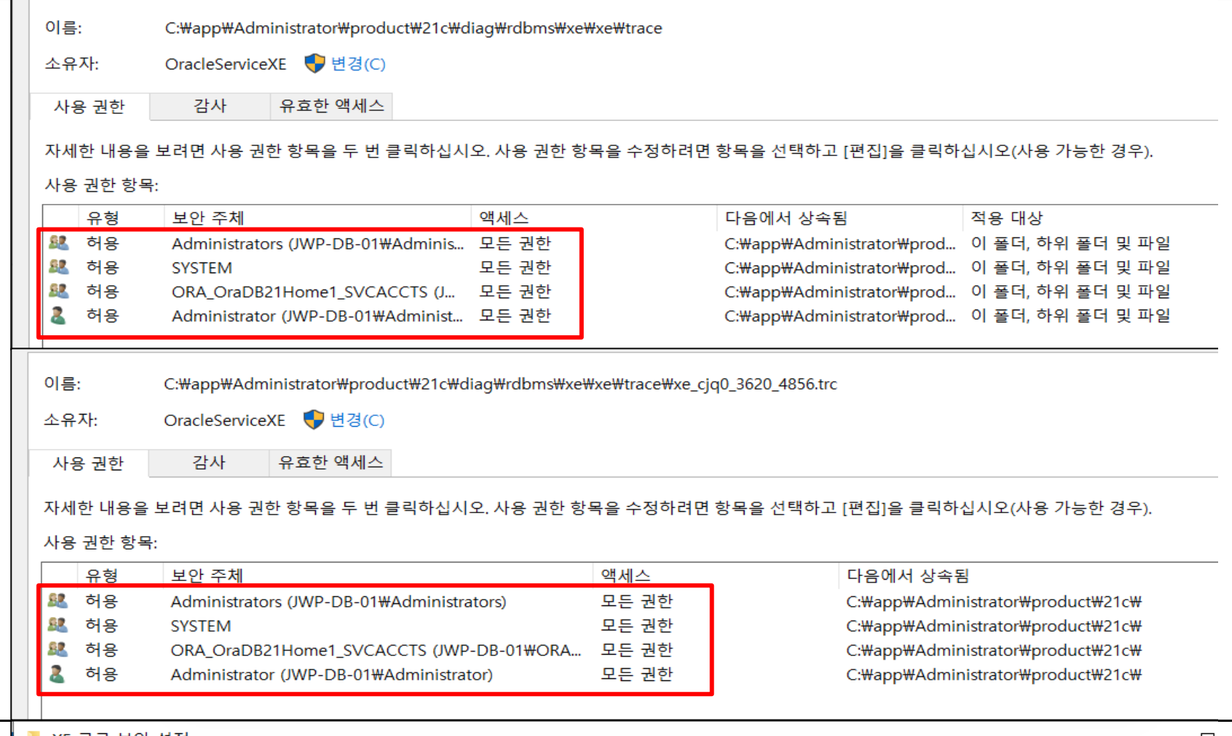
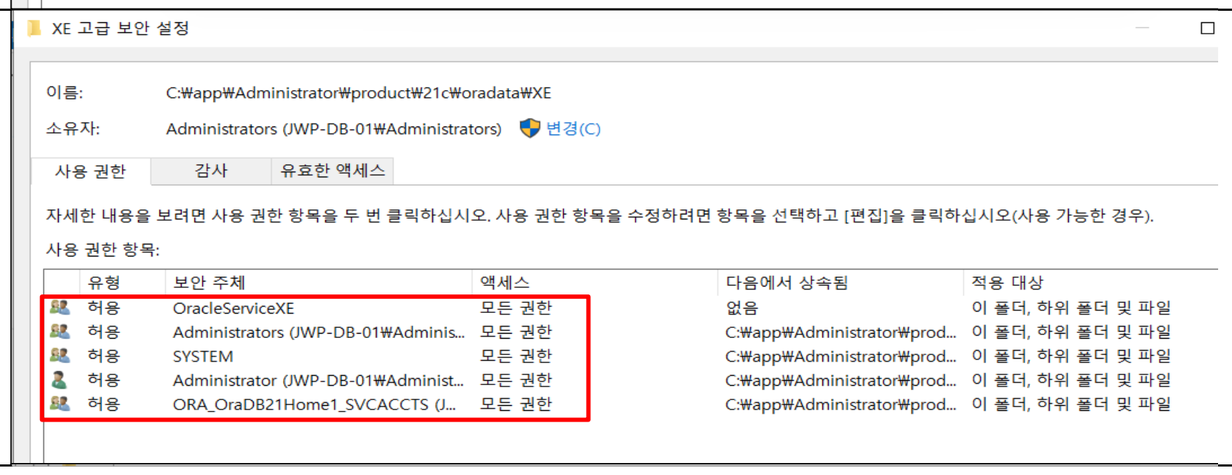
영역별점수	점수	양호	취약	N/A
50.0%	100.0%	1	0	0
	100.0%	1	0	0
	0.0%	0	1	0
	0.0%	0	1	0
	0.0%	0	1	0
	100.0%	1	0	0
77.8%	0.0%	0	1	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	0.0%	0	1	0
	100.0%	1	0	0
16.7%	0.0%	0	1	0
	0.0%	0	1	0
	100.0%	1	0	0
	0.0%	0	1	0
	0.0%	0	1	0
	0.0%	0	1	0
87.5%	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	0.0%	0	1	0
	100.0%	1	0	0
0.0%	0.0%	0	1	0
100.0%	100.0%	1	0	0
	100.0%	1	0	0
N/A	N/A	0	0	1
	N/A	0	0	1

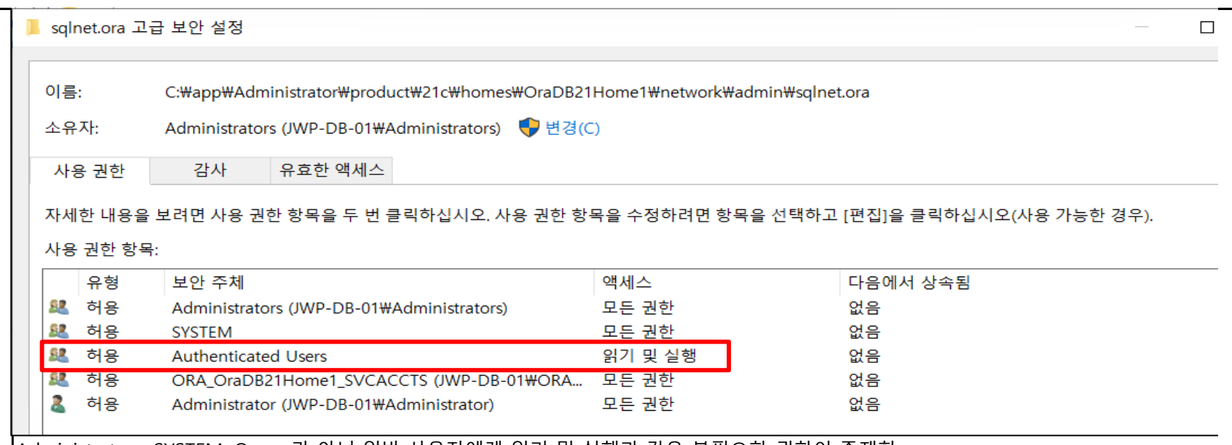
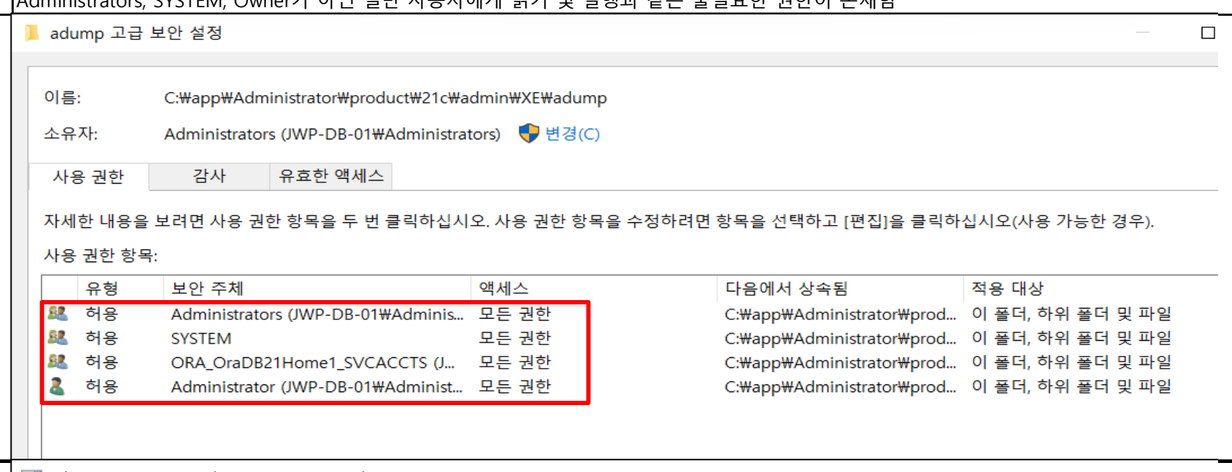
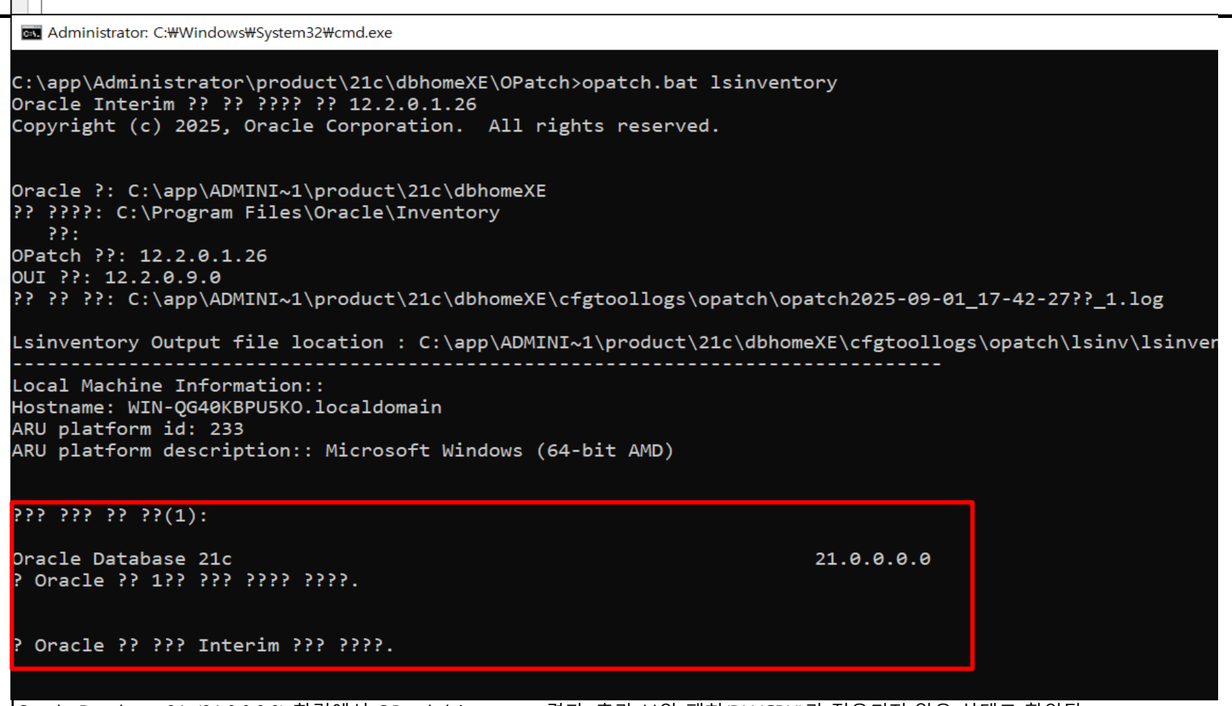
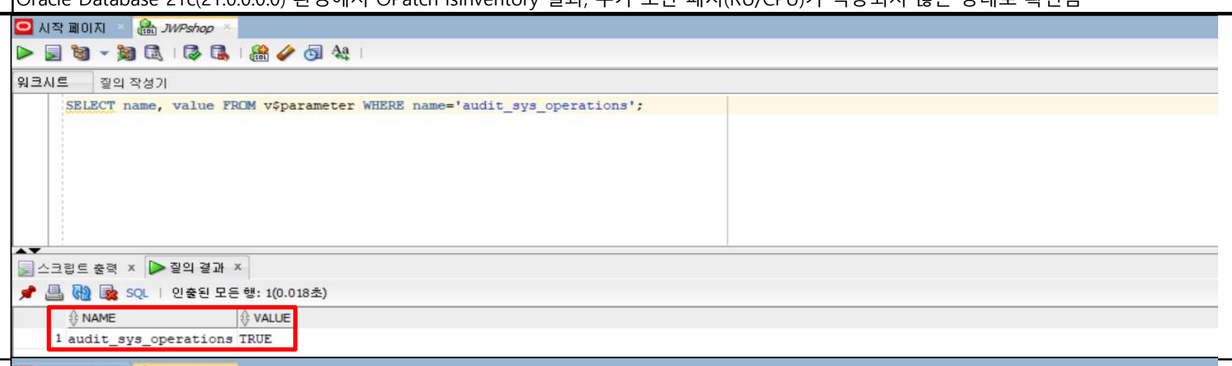
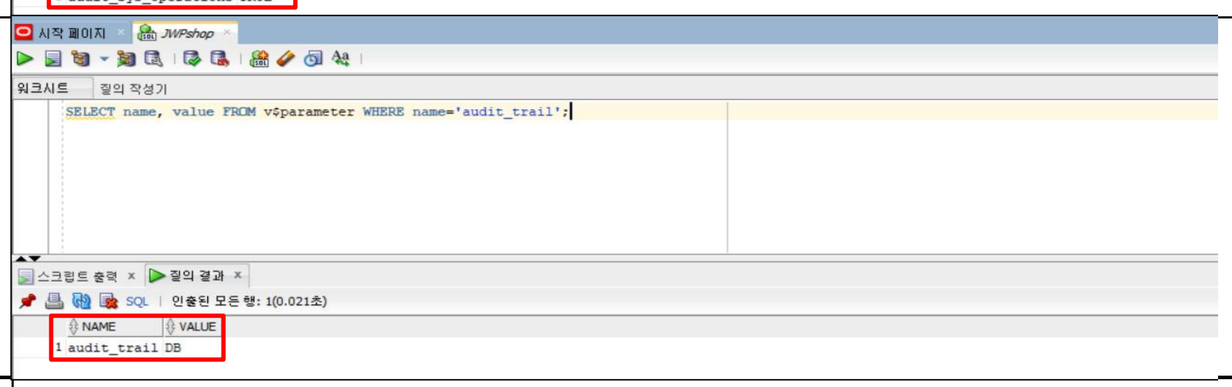
Oracle 취약점 진단 상세결과(34항목)

진단항목	No.	세부 진단항목	진단기준	1	jwp-db-01 10.0.8.8 DBMS
1. 계정관리	1	불필요한 계정 확인	양호 - 불필요한 계정이 존재하지 않는 경우 취약 - 불필요한 계정이 존재할 경우	양호	
	2	무제한 로그인 시도 차단	양호 - FAILED_LOGIN_ATTEMPTS 설정값이 10 이하로 설정되어 있는 경우 취약 - FAILED_LOGIN_ATTEMPTS 설정값이 10 초과로 설정되어 있는 경우	양호	
	3	패스워드 주기적 변경	양호 - 하기 기준 값을 만족할 경우 취약 - 하기 기준 값을 만족하지 않는 경우 ※ DB에서 사용하고 있는 프로파일을 점검하여 "PASSWORD_LIFE_TIME"의 값이 60 이하로 설정되었는지 확인	취약	 DB 내 사용하고 있는 프로파일의 'PASSWORD_LIFE_TIME' 값이 60일 이하로 설정되어 있지 않음
	4	패스워드 복잡도 설정	양호 - 'PASSWORD_VERIFY_FUNCTION'의 설정 값이 'VERIFY_FUNCTION_11G' 또는 'ORA12C_VERIFY_FUNCTION'으로 설정되어 있는 경우 취약 - 'PASSWORD_VERIFY_FUNCTION'의 설정 값이 'VERIFY_FUNCTION_11G' 또는 'ORA12C_VERIFY_FUNCTION'으로 설정되어 있지 않은 경우	취약	 'PASSWORD_VERIFY_FUNCTION'의 값이 'ORA12C_VERIFY_FUNCTION'으로 되어 있어야 하는데, NULL 값으로 되어 있음
	5	취약한 패스워드 사용 점검	양호 - 계정의 패스워드가 안전하게 설정되어 있는 경우 취약 - 계정의 패스워드가 취약하게 설정되어 있거나 없는 경우	취약	담당자 인터뷰를 통해 취약한 비밀번호를 사용 중인 것을 확인
	6	OS DBA 그룹 멤버 확인	양호 - 불필요한 계정이 존재하지 않는 경우 취약 - 불필요한 계정이 존재하는 경우	양호	
	1	개발 및 운영 시스템 분리 사용	양호 - 개발 시스템과 운영시스템을 분리하여 사용하는 경우 취약 - 개발 시스템과 운영시스템을 분리하여 사용하지 않는 경우	취약	담당자 인터뷰 결과 개발과 운영 서비스가 동일한 환경임을 확인

2. 권한 관리	2	Public에 대한 권한 제한	양호 - Object의 사용 권한이 불필요하게 public, guest에 부여되어 있지 않은 경우 취약 - Object의 사용 권한이 불필요하게 public, guest에 부여되어 있는 경우	양호	
	3	SYS.LINK$ 테이블 접근 제한	양호 - SYS.LINK$ 접근 권한을 DBA 권한이 있는 올바른 사용자에게 부여한 경우 취약 - DBA 권한이 아닌 일반 사용자에 SYS.LINK$ 접근 권한을 부여한 경우	양호	
	4	SYSDBA 권한 제한	양호 - SYSDBA 권한이 일반 사용자에게 불필요하게 부여되지 않은 경우 취약 - SYSDBA 권한이 일반 사용자에게 불필요하게 부여된 경우	양호	
	5	DBA 권한 제한	양호 - DBA 권한이 적절한 사용자에게 부여된 경우 취약 - DBA 권한이 적절한 사용자에게 부여되지 않은 경우	양호	
	6	with grant option 사용 제한	양호 - with grant option이 적절한 사용자에게 부여되어 있는 경우 취약 - with grant option이 적절한 사용자에게 부여되어 있지 않은 경우	양호	
	7	with admin option 사용 제한	양호 - with admin option이 적절한 사용자에게 부여되어 있는 경우 취약 - with admin option이 적절한 사용자에게 부여되어 있지 않은 경우	양호	
	8	SYSDBA 로그인 제한	양호 - (sqlplus / as sysdba) 같은 명령어로 연결이 불가능한 경우 취약 - (sqlplus / as sysdba) 같은 명령어로 연결이 가능한 경우	취약	 비인가자에 대한 권한 제어가 되지 않아 패스워드 없이 SYSDBA 권한으로 누구나 데이터베이스에 접근할 수 있음

	9	CREATE ANY DIRECTORY 권한 제한	양호 - "CREATE ANY DIRECTORY" 권한이 불필요한 계정에 부여되지 않은 경우 취약 - "CREATE ANY DIRECTORY" 권한이 불필요한 계정에 부여된 경우	양호	
3. DBMS 보안설정	1	백업 관리	양호 - 주기적으로 백업을 수행하는 경우 취약 - 주기적으로 백업을 수행하지 않는 경우	취약	담당자 인터뷰 결과 백업 정책이 없는 것을 확인
	2	PL/SQL Package의 Public Role 점검	양호 - PL/SQL package에 접근 권한이 설정되어 있는 경우 취약 - PL/SQL package에 접근 권한이 설정되어 있지 않은 경우 경우	취약	 UTL_FILE, UTL_TCP 등과 같은 패키지의 실행 권한을 사용하지 않지만, Public에 부여되는 권한이 전부 Execute로 되어 있음
	3	Listener 보안 설정 여부	양호 - Listener 파일의 패스워드 설정이 되어 있는 경우 취약 - Listener 파일의 패스워드 설정이 되어 있지 않은 경우	양호	Oracle 12.1 Version 부터 Listener 패스워드 기능 미지원
	4	DB 접속 IP 통제	양호 - IP 차단이 설정되어 있는 경우 취약 - IP 차단이 설정되어 있지 않는 경우	취약	 sqlnet.ora 파일 내에서 허용 IP를 제외한 모든 IP를 차단하는 설정인 TCP.INVITED_NODES가 존재하는지 확인한 결과 어떤 설정값도 나오지 않음
	5	로그 저장 주기	양호 - 주기적으로 로그 저장, 백업, 감독되고 있는 경우 취약 - 로그 저장, 백업, 감독하지 않는 경우	취약	담당자 인터뷰 결과 로그 관리 정책이 없는 것을 확인
	6	세션 IDLE_TIMEOUT 설정	양호 - IDLE_TIMEOUT이 5분 이하로 설정되어 있는 경우 취약 - IDLE_TIMEOUT이 5분 초과로 설정되어 있는 경우	취약	 Profile 파일에 설정된 IDLE_TIMEOUT의 설정 값이 5분 이상 또는 UNLIMITED, DEFAULT로 되어 있음
	1	SQL*PLUS 명령 히스토리 검사	양호 - 히스토리 파일 접근 권한이 600 이하로 설정되어 있는 경우 취약 - 히스토리 파일 접근 권한이 600 초과로 설정되어 있는 경우	양호	

4. 환경 파일 점검	2	Initialization 파일 접근 권한 설정	[Unix 확인방법] 양호 - 초기화 파일 접근 권한이 640 이하로 설정되어 있는 경우 취약 - 초기화 파일 접근 권한이 640 초과로 설정되어 있는 경우 [Windows 확인방법] 양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우 취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우	양호	
	3	Oracle Password 파일 접근 권한 설정	[Unix 확인방법] 양호 - 패스워드 파일 접근 권한이 640 이하로 설정되어 있는 경우 취약 - 패스워드 파일 접근 권한이 640 초과로 설정되어 있는 경우 ※ 패스워드 파일(orapw(SID))의 접근 권한 설정 확인 [Windows 확인방법] 양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우 취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우 ※ 패스워드 파일(orapw(SID))의 접근 권한 설정 확인	양호	
	4	AlertLog 파일 접근 제한	[Unix 확인방법] 양호 - 파일 접근 권한이 640 이하로, 디렉토리 접근 권한이 750 이하로 설정되어 있는 경우 취약 - 파일 접근 권한이 640 초과로, 디렉토리 접근 권한이 750 초과로 설정되어 있는 경우 ※ Alert_<SID>.log, Attention_<SID>.log의 접근 권한 설정 확인 [Windows 확인방법] 양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우 취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우 ※ Alert_<SID>.log, Attention_<SID>.log의 접근 권한 설정 확인	양호	
	5	Trace Log 파일 접근 제한	[Unix 확인방법] 양호 - 파일 접근 권한이 640 이하로, 디렉토리 접근 권한이 750 이하로 설정되어 있는 경우 취약 - 파일 접근 권한이 640 초과로, 디렉토리 접근 권한이 750 초과로 설정되어 있는 경우 [Windows 확인방법] 양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우 취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우	양호	
	6	컨트롤, redo 로그파일, 데이터 파일 접근 제한	[Unix 확인방법] 양호 - 접근 권한이 640 이하로 설정되어 있는 경우 취약 - 접근 권한이 640 초과로 설정되어 있는 경우 [Windows 확인방법] 양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우 취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우	양호	

	7	$TNS_ADMIN 파일 접근 제한	[Unix 확인방법] 양호 - 접근 권한이 644 이하로 설정되어 있는 경우 취약 - 접근 권한이 644 초과로 설정되어 있는 경우 [Windows 확인방법] 양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우 취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우	취약	 Administrators, SYSTEM, Owner가 아닌 일반 사용자에게 읽기 및 실행과 같은 불필요한 권한이 존재함
	8	감사 로그 파일 접근 제한	[Unix 확인방법] 양호 - 접근 권한이 750 이하로 설정되어 있는 경우 취약 - 접근 권한이 750 초과로 설정되어 있는 경우 ※ Audit_file_dest에 설정된 경로의 디렉터리의 접근 권한 설정 확인 [Windows 확인방법] 양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우 취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우 ※ Audit_file_dest에 설정된 경로의 디렉터리의 접근 권한 설정 확인	양호	
5. 보안 패치	1	보안 패치 적용	양호 - 최신의 서비스 팩 적용한 경우, Opatch 2016년 1월 패치 적용 취약 - 최신의 서비스 팩 적용하지 않을 경우. Opatch 2016년 1월 이전 패치 적용	취약	 Oracle Database 21c(21.0.0.0.0) 환경에서 OPatch lsinventory 결과, 추가 보안 패치(RU/CPU)가 적용되지 않은 상태로 확인됨
6. 보안 감사 설정	1	SYS 감사 수행 설정	양호 - "AUDIT_SYS_OPERATION"의 값이 "TRUE"로 설정 되어 있는 경우 취약 - "AUDIT_SYS_OPERATION"의 값이 "FALSE"로 설정 되어 있는 경우	양호	
	2	Audit Trail 기록 설정	양호 - 감사 설정을 위해 트리거, FGA를 사용하는 경우 취약 - "Audit_trail"의 값이 'none' 으로 설정되어 있는 경우	양호	
7. 네트워크 접근 제어	1	DATA DICTIONARY 접근 제한	양호 - "O7_DICTIONARY_ACCESSIBILITY" 값이 FALSE로 되어 있는 경우 취약 - "O7_DICTIONARY_ACCESSIBILITY" 값이 TRUE로 되어 있는 경우	*N/A*	Oracle 19c 버전 이상부터 O7_DICTIONARY_ACCESSIBILITY 미지원
	2	원격 OS 인증 방식 설정	양호 - "REMOTE_OS_AUTHENT"의 값이 FALSE로 설정되어 있는 경우 취약 - "REMOTE_OS_AUTHENT"의 값이 TRUE로 설정되어 있는 경우 ※ 원격 OS 인증(REMOTE_OS_AUTHENT) 기능은 21c 버전 이상부터 지원하지 않음	*N/A*	Oracle 21c 버전 이상부터 원격 OS 인증(REMOTE_OS_AUTHENT) 기능 미지원
점검결과				**12.0**	
			보안 적용율 (양호항목 / 진단항목) %	**62.5%**	