

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



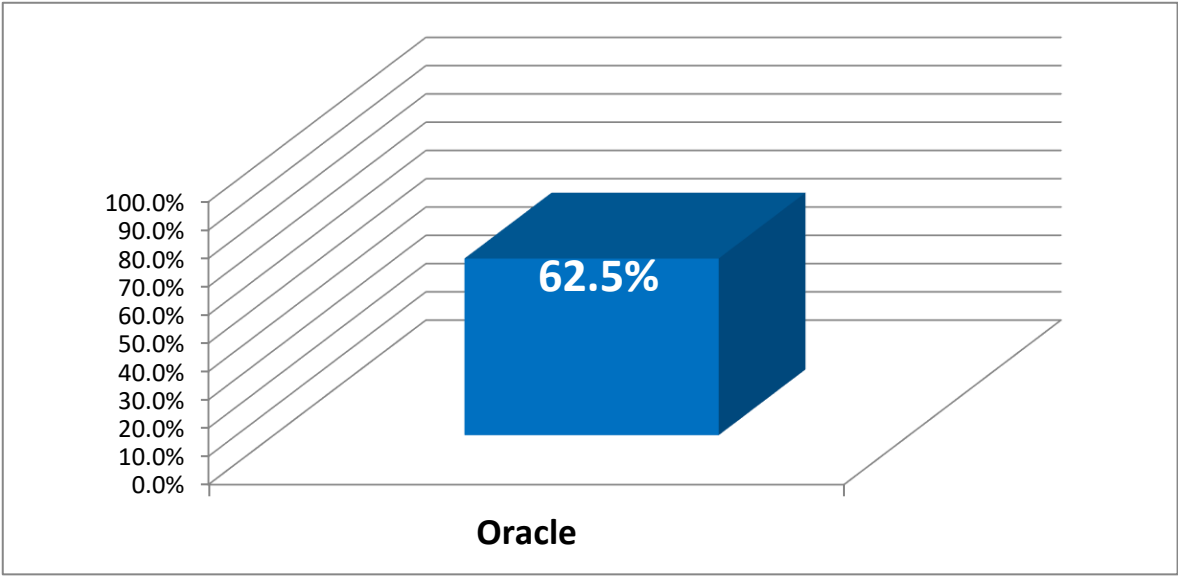
※ 진단 대상 리스트 - DBMS 1대 (Oracle 1대)

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

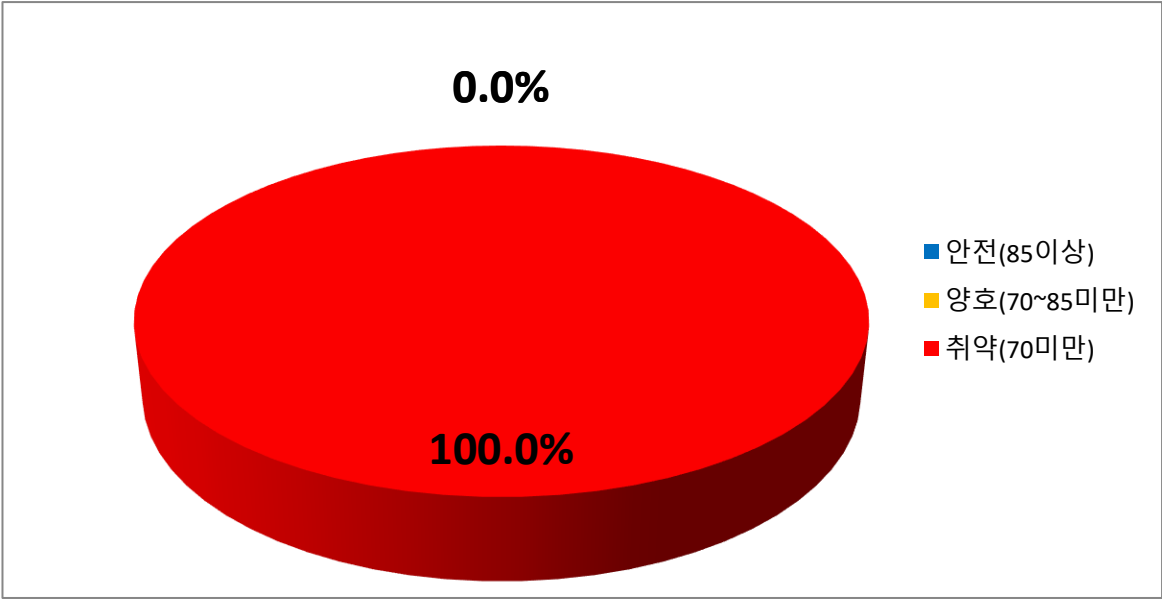
※ 대상별 평균 점수 그래프

대상별 평균 점수 현황

진단 대상	평균	수량
Oracle	62.5%	1



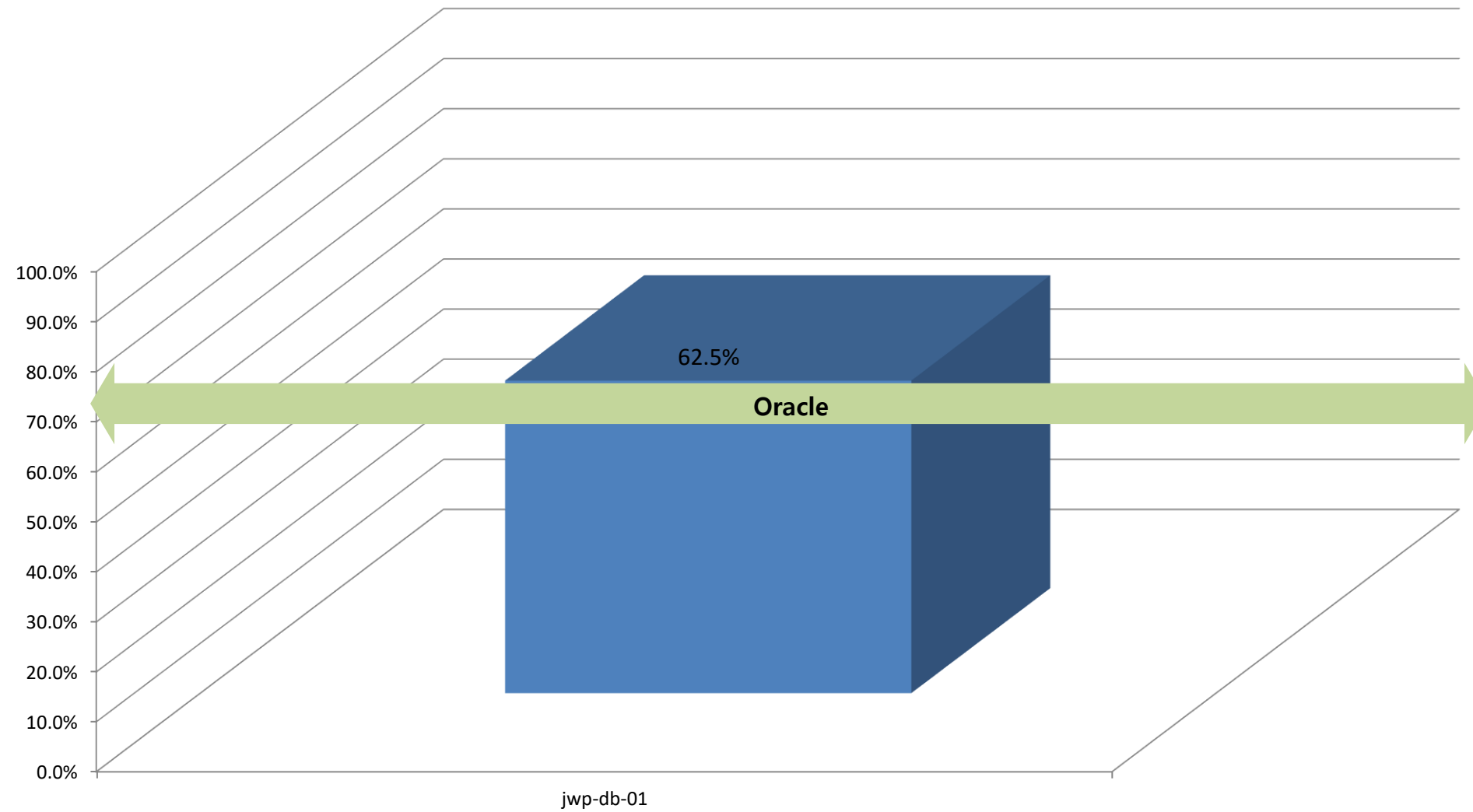
전체		수량
안전(85이상)	0.0%	0
양호(70~85미만)	0.0%	0
취약(70미만)	100.0%	1



서버 진단결과

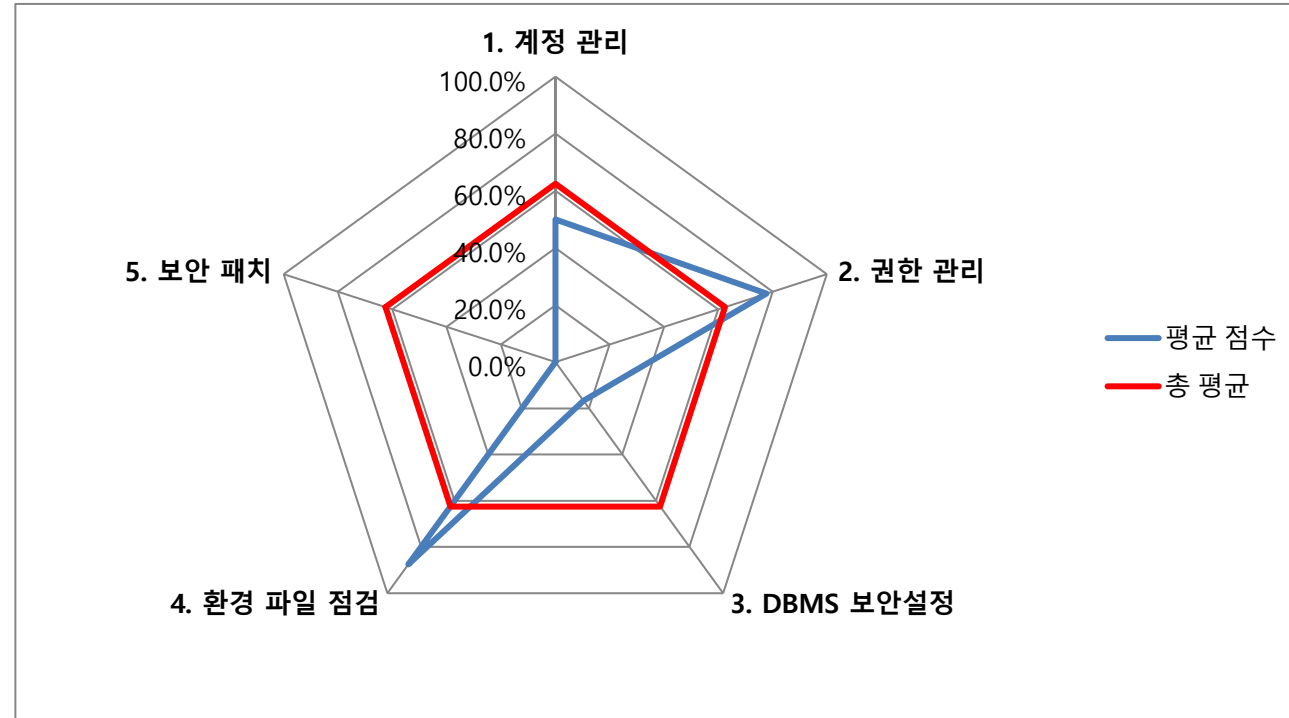
■ 안전(A)
 ■ 양호(B)
 ■ 보통이하(C~E)

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



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

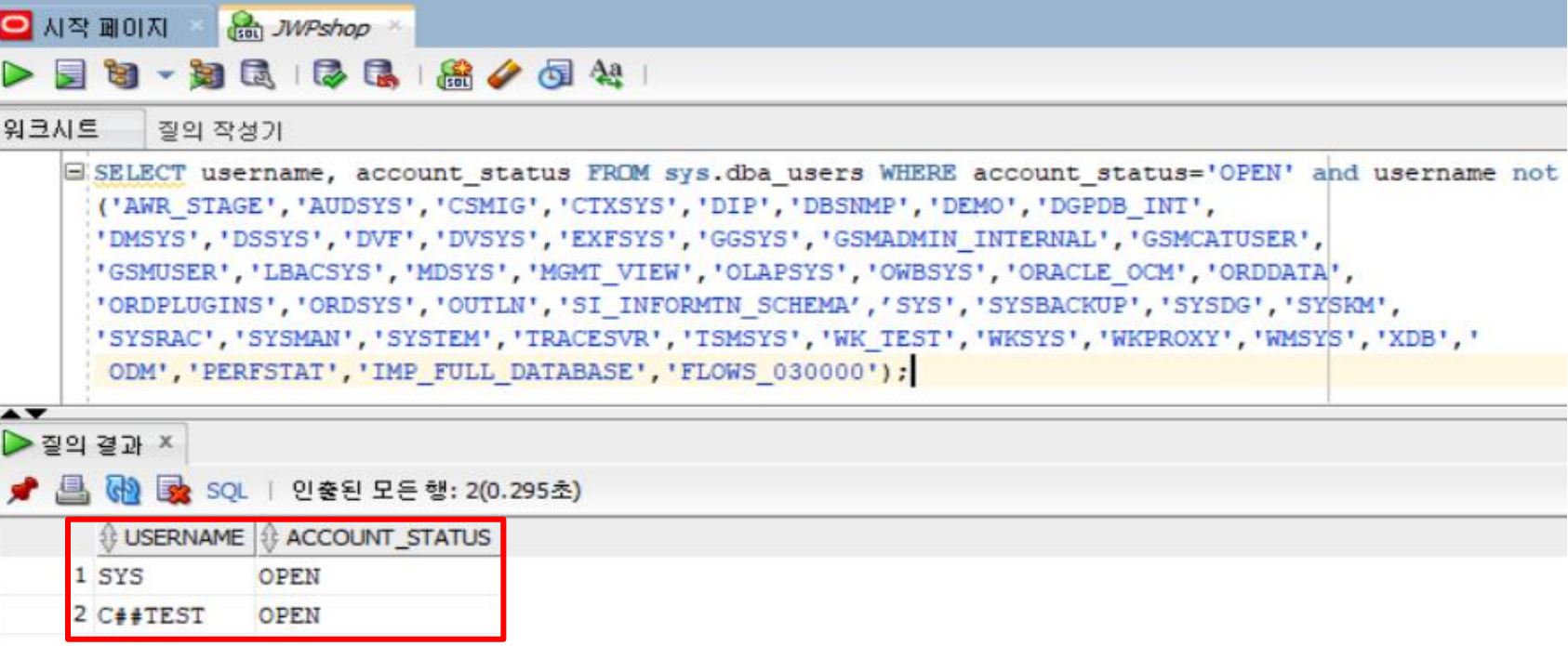
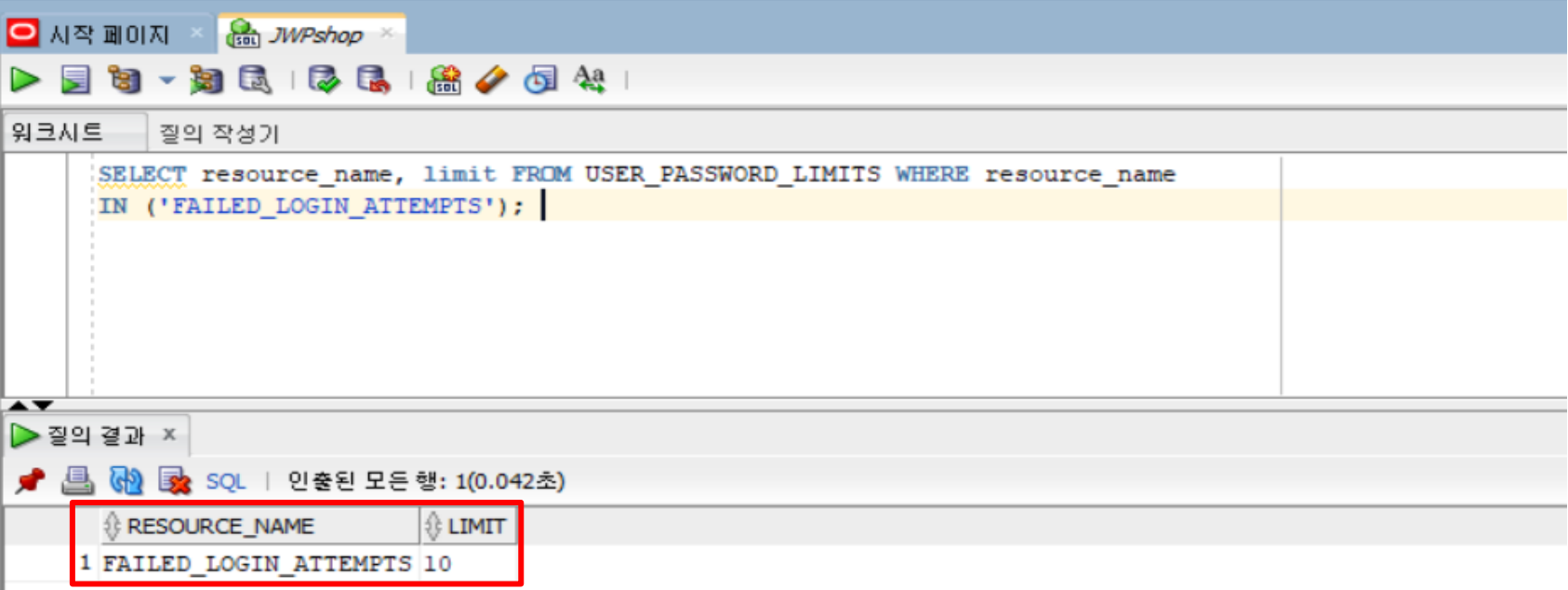
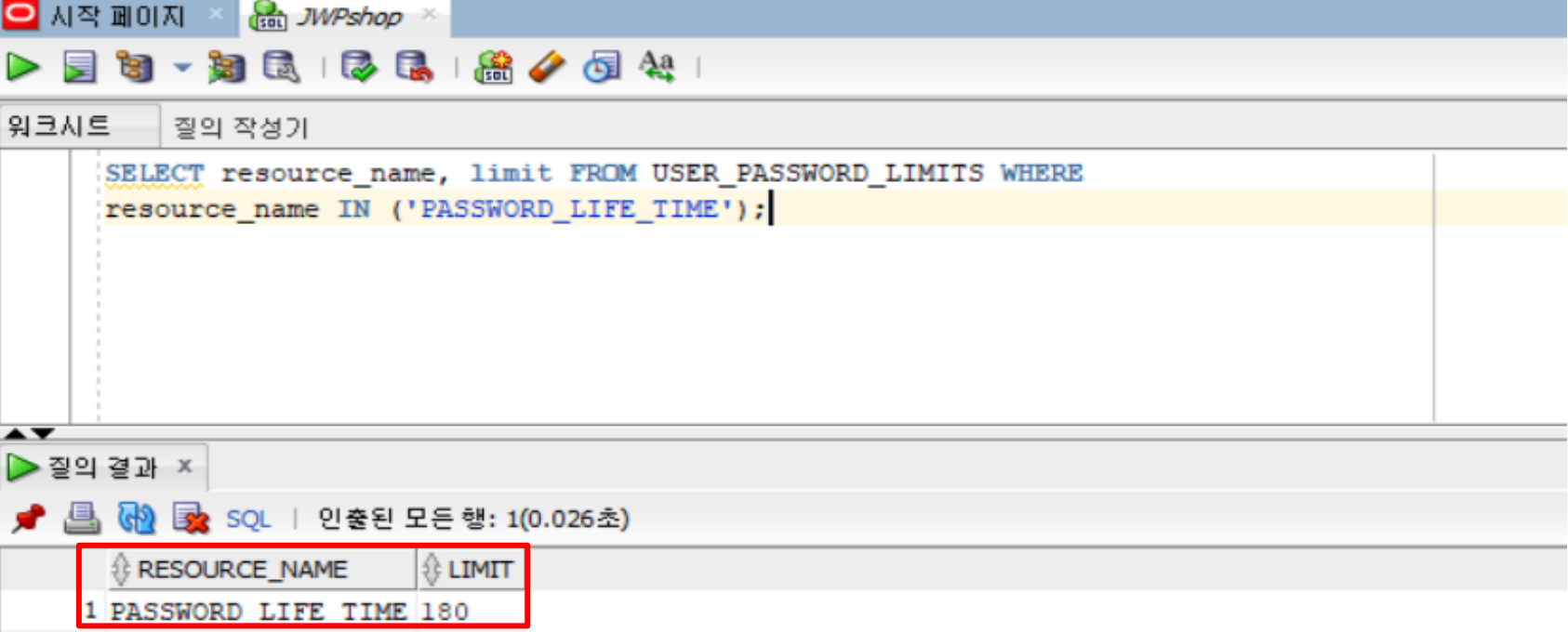
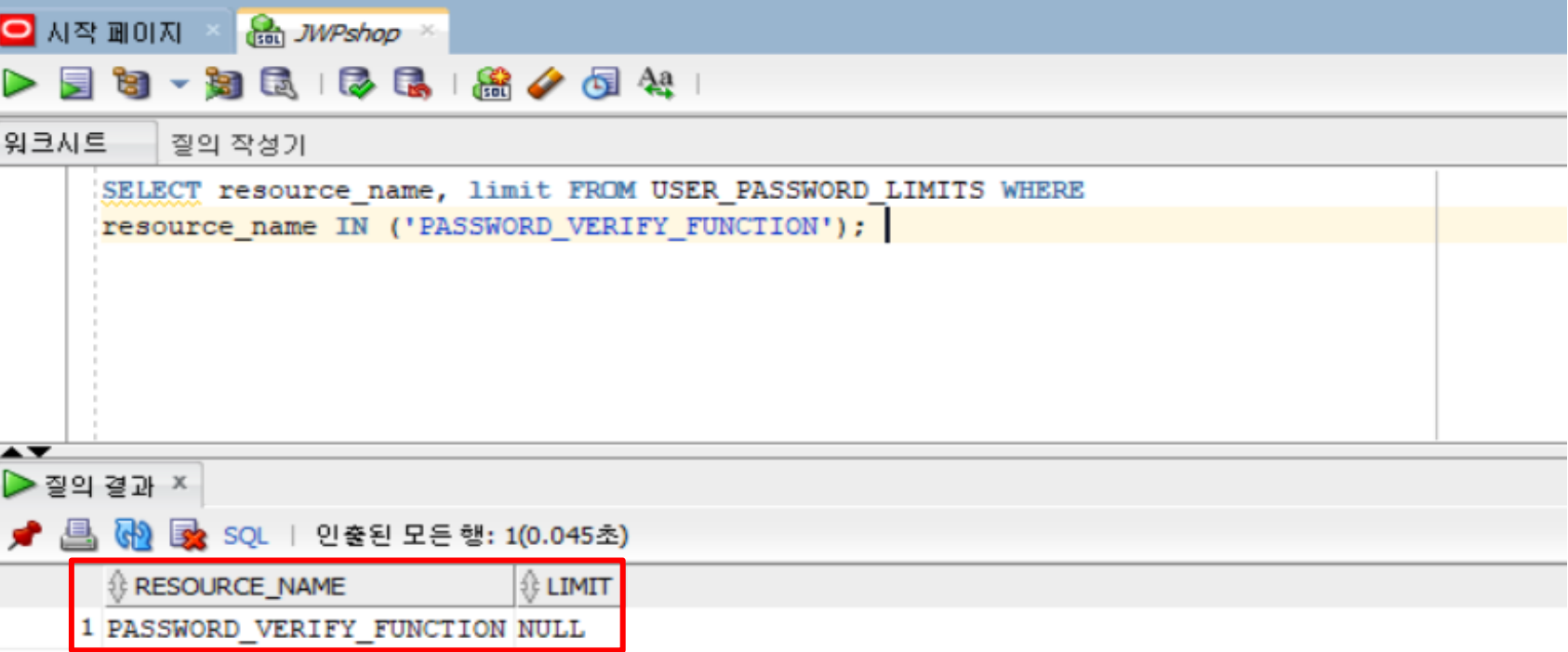
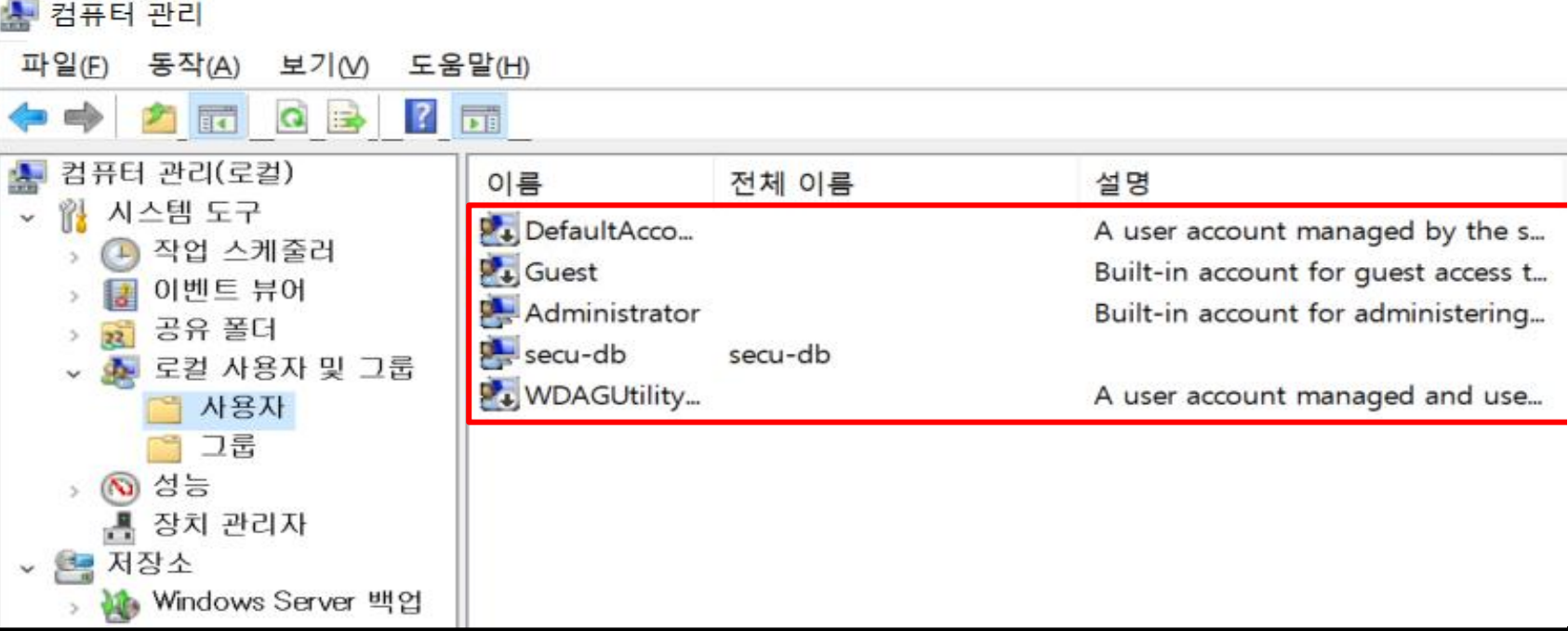


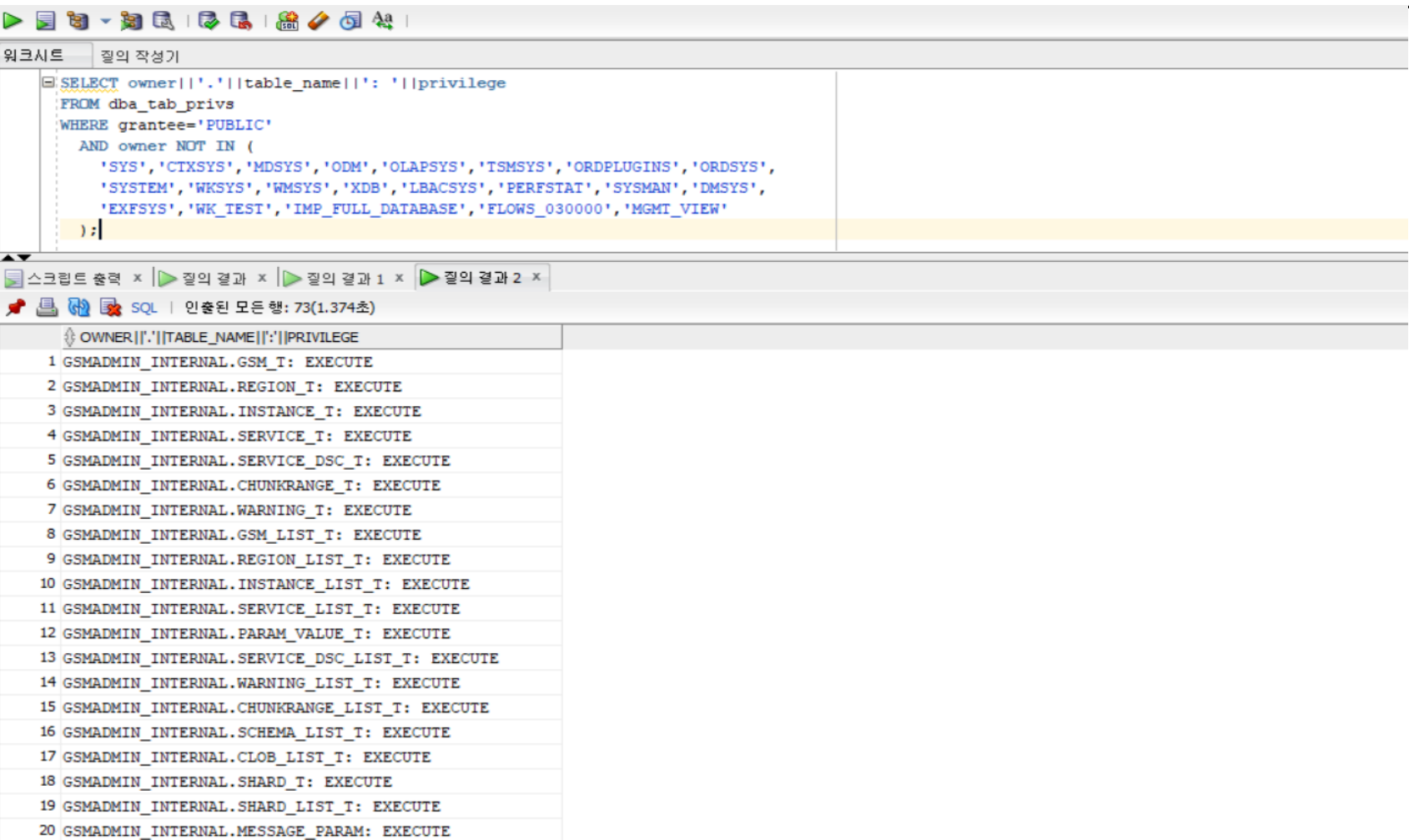
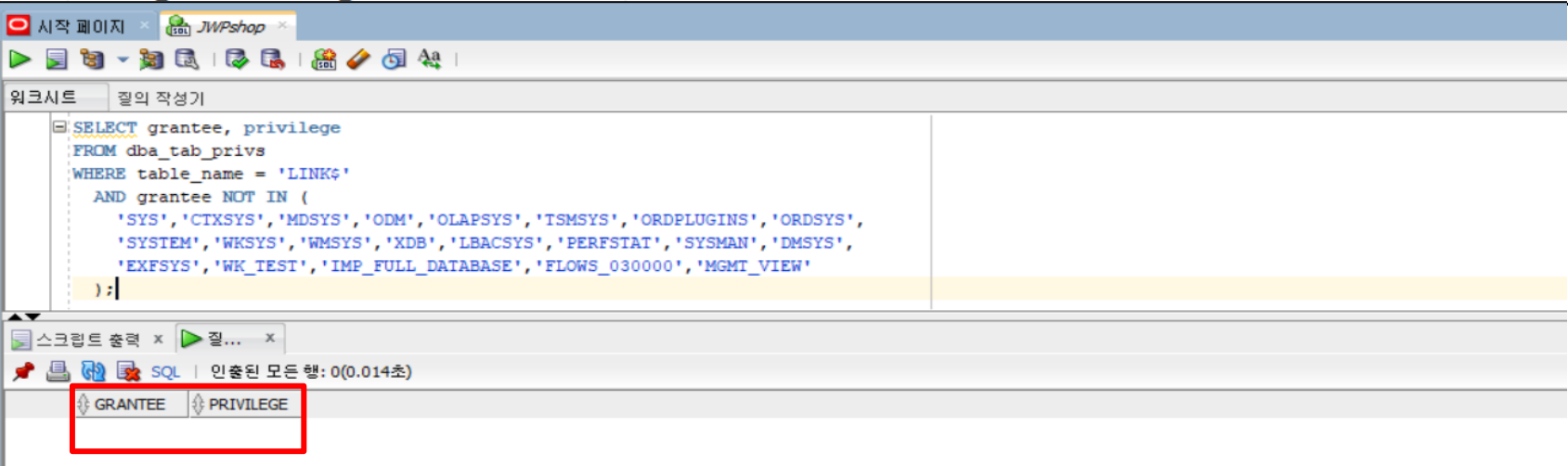
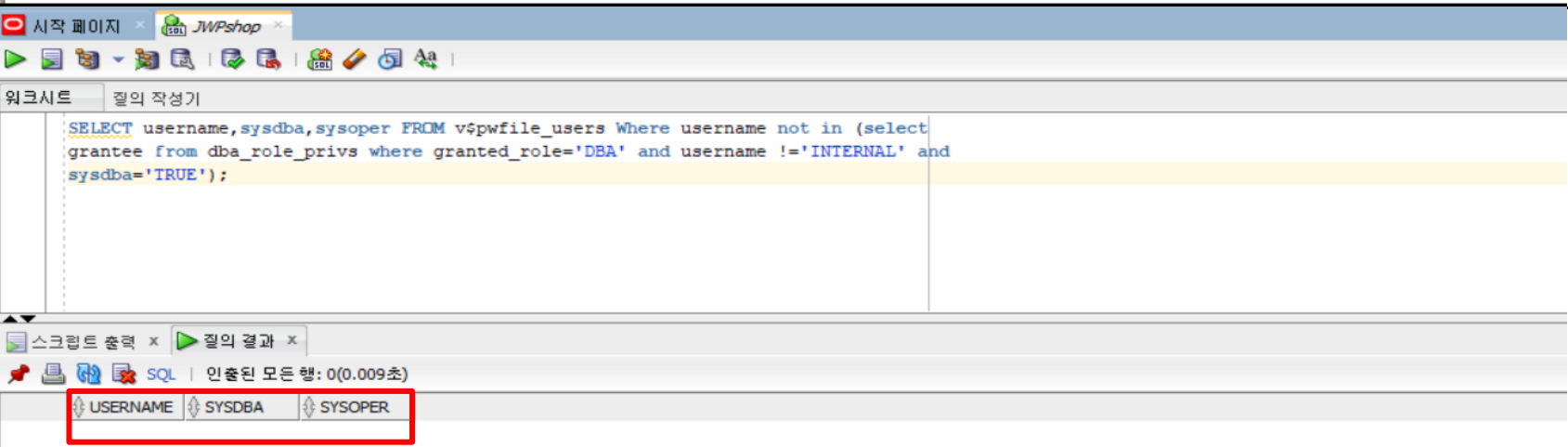
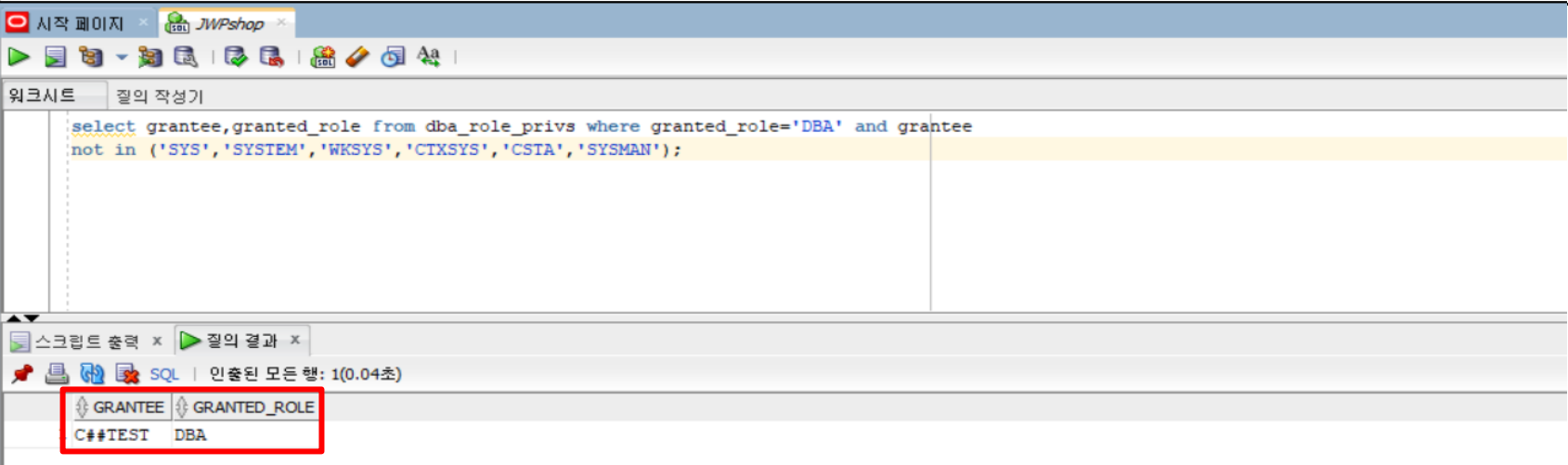
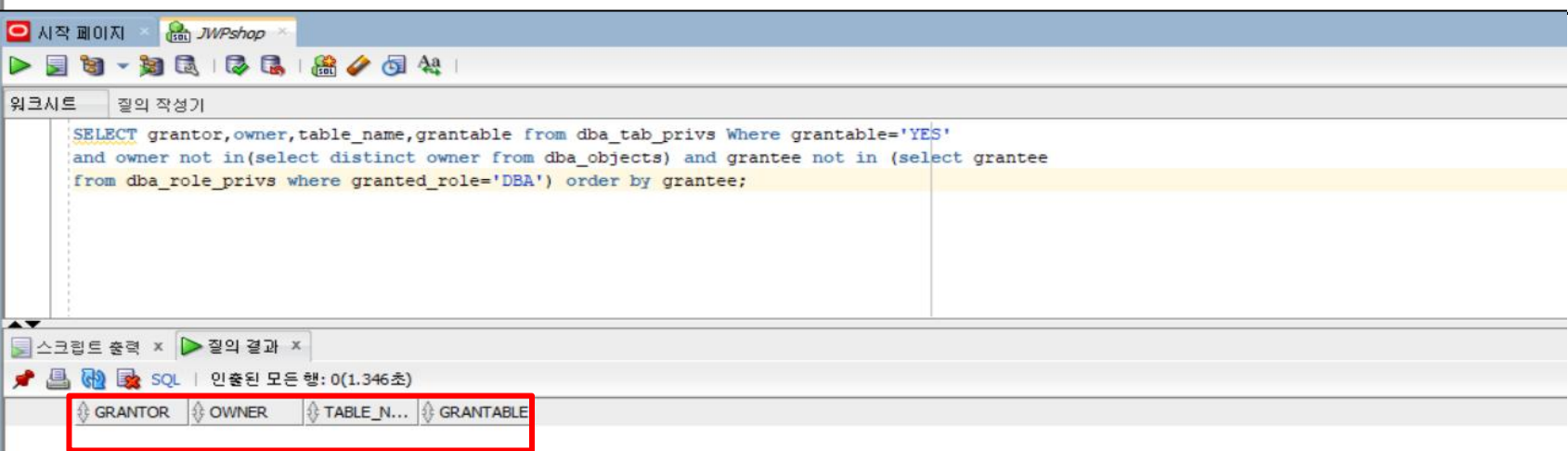
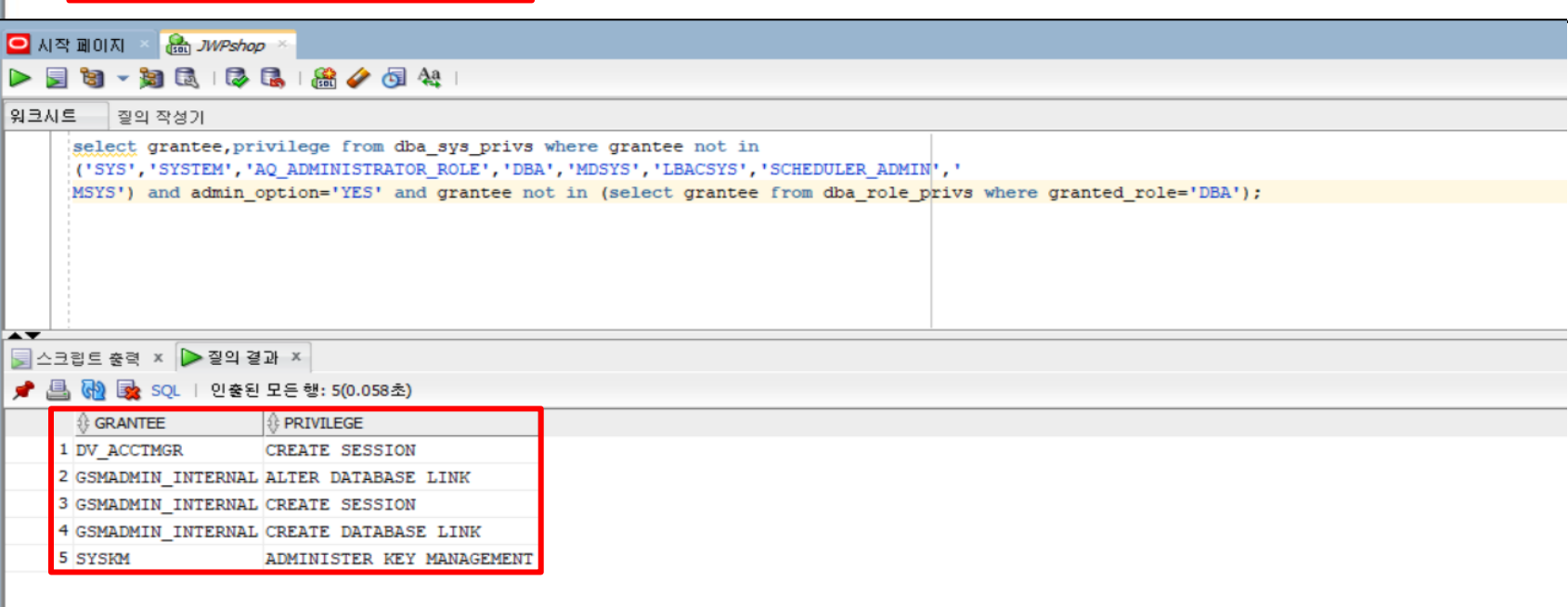
Oracle 취약점 진단 요약결과(34항목)

진단항목	No.	세부 진단항목	중 요 도	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
	100.0%	1	0	0
	0.0%	0	1	0
16.7%	100.0%	1	0	0
	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
	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 설정값이 'VERIFY_FUNCTION_11G' 또는 'ORA12C_VERIFY_FUNCTION'으로 설정되어 있는 경우 취약 - 'PASSWORD_VERIFY_FUNCTION'의 설정값이 '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 환경을 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 사용자에게 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	<p>sqlnetora - 메모장</p> <p>파일(F) 편집(E) 서식(O) 보기(V) 도움말</p> <p># sqlnet.ora Network Configuration File: C:\app\Administrator\product\21c\homes\OraDB21Home1\NETWORK\ADMIN\ # Generated by Oracle configuration tools.</p> <p># This file is actually generated by netca. But if customers choose to # install "Software Only", this file wont exist and without the native # authentication, they will not be able to connect to the database on NT.</p> <p>SQLNET.AUTHENTICATION_SERVICES= (NTS)</p> <p>NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)</p> <p>비인가자에 대한 권한 제어가 되지 않아 패스워드 없이 SYSDBA 권한으로 누구나 데이터베이스에 접근할 수 있음</p>

	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	<div><div><div><div><div><div></div><div>시작 페이지</div></div></div><div><div><div></div><div>JWPshap</div></div><div><div></div><div></div></div></div><div><div><div><div>워크시트</div><div>질의 작성기</div></div></div><div><div><div><div><pre>select grantee,privilege from dba_sys_privs where privilege='CREATE ANY DIRECTORY' and grantee not in('DBA','IMP_FULL_DATABASE','WKSYS','SYS','SYSDBA');</pre></div><div></div></div><div><div><div><div>스크립트 출력</div><div>질의 결과</div></div><div>SQL 인출된 모든 행: 1(0.058초)</div></div><div><div><div>GRANTEE</div><div>PRIVILEGE</div></div><div>1 SYSBACKUP CREATE ANY DIRECTORY</div></div></div></div></div></div></div></div></div>																
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	<div><div><div><div><div><div></div><div>시작 페이지</div></div></div><div><div><div></div><div>JWPshap</div></div><div><div></div><div></div></div></div><div><div><div><div>워크시트</div><div>질의 작성기</div></div></div><div><div><div><div><pre>select grantee,owner,grantor,table_name,privilege from dba_tab_privs where grantee='PUBLIC' and privilege='EXECUTE' and table_name in ('UTL_SMTP','UTL_TCP','UTL_HTTP','UTL_FILE','DBMS_RANDOM','DBMS_LOB','DBMS_BACKUP_RESOTRE','DBMS_SQL','DBMS_JOB','DBMS_OBFUSCATION_TOOLKIT','UTL_INADDR');</pre></div><div></div></div><div><div><div><div>스크립트 출력</div><div>질의 결과</div></div><div>SQL 인출된 모든 행: 8(0.965초)</div></div><div><div><div>GRANTEE</div><div>OWNER</div><div>GRANTOR</div><div>TABLE_NAME</div><div>PRIVILEGE</div></div><div>1 PUBLIC SYS SYS DBMS_LOB EXECUTE</div><div>2 PUBLIC SYS SYS UTL_TCP EXECUTE</div><div>3 PUBLIC SYS SYS UTL_HTTP EXECUTE</div><div>4 PUBLIC SYS SYS DBMS_SQL EXECUTE</div><div>5 PUBLIC SYS SYS UTL_FILE EXECUTE</div><div>6 PUBLIC SYS SYS UTL_INADDR EXECUTE</div><div>7 PUBLIC SYS SYS DBMS_JOB EXECUTE</div><div>8 PUBLIC SYS SYS DBMS_RANDOM EXECUTE</div></div></div></div></div></div><div>UTL_FILE, UTL_TCP 등과 같은 패키지의 실행 권한을 사용하지 않지만, Public에 부여되는 권한이 전부 Execute로 되어 있음</div></div></div></div>																
	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 않은 경우	취약	<div><div><div><div><div><div></div><div>sqlnet.ora - 메모장</div></div></div><div><div><div></div><div>파일(F) 편집(E) 서식(O) 보기(V) 도움말</div></div><div><div></div><div># sqlnet.ora Network Configuration File: C:\app\Administrator\product\21c\homes\OraDB21Home1\NETWORK</div></div></div><div><div><div></div><div># Generated by Oracle configuration tools.</div></div><div><div></div><div># This file is actually generated by netca. But if customers choose to</div></div></div><div><div><div></div><div># install "Software Only", this file wont exist and without the native</div></div><div><div></div><div># authentication, they will not be able to connect to the database on NT.</div></div></div><div><div><div></div><div>SQLNET.AUTHENTICATION_SERVICES= (NTS)</div></div><div><div></div><div>NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)</div></div></div></div></div></div> <div>sqlnet.ora 파일 내에서 허용 IP를 제외한 모든 IP를 차단하는 설정인 TCP.INVITED_NODES가 존재하는지 확인한 결과 어떤 설정값도 나오지 않음</div>																
	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	<div><div><div><div><div><div></div><div>시작 페이지</div></div></div><div><div><div></div><div>JWPshap</div></div><div><div></div><div></div></div></div><div><div><div><div>워크시트</div><div>질의 작성기</div></div></div><div><div><div><div><pre>select * from dba_profiles where resource_name = 'IDLE_TIME';</pre></div><div></div></div><div><div><div><div>스크립트 출력</div><div>질의 결과</div></div><div>SQL 인출된 모든 행: 3(0.02초)</div></div><div><div><div>PROFILE</div><div>RESOURCE_NAME</div><div>RESOURCE_TYPE</div><div>LIMIT</div><div>COMMON</div><div>INHERITED</div><div>IMPLICIT</div><div>ORACLE_MAINTAINED</div><div>MANDATORY</div></div><div>1 DEFAULT IDLE_TIME KERNEL UNLIMITED NO NO NO NO YES NO</div><div>2 ORA_CIS_PROFILE IDLE_TIME KERNEL DEFAULT NO NO NO YES NO</div><div>3 ORA_STIG_PROFILE IDLE_TIME KERNEL 15 NO NO NO YES NO</div></div></div></div></div></div><div>Profile 파일에 설정된 IDLE_TIMEOUT의 설정 값이 5분 이상 또는 UNLIMITED, DEFAULT로 되어 있음</div></div></div></div>																
	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	<div><div><div><div><div><div></div><div>ConsoleHost_history.txt 고급 보안 설정</div></div></div><div><div><div></div><div>이름: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt</div></div><div><div></div><div>소유자: Administrators (JWP-DB-01\Administrators) 변경(C)</div></div></div><div><div><div><div>사용 권한</div><div>감사</div><div>유효한 액세스</div></div><div>자세한 내용을 보려면 사용 권한 항목을 두 번 클릭하십시오. 사용 권한 항목을 수정하려면 항목을 선택하고 [편집]을 클릭하십시오(사용 가능한 경우).</div></div><div><div><div>사용 권한 항목:</div><table><tr><th>유형</th><th>보안 주제</th><th>액세스</th><th>다음에서 상속됨</th></tr><tr><td>허용</td><td>SYSTEM</td><td>모든 권한</td><td>C:\Users\Administrator\W</td></tr><tr><td>허용</td><td>Administrators (JWP-DB-01\Administrators)</td><td>모든 권한</td><td>C:\Users\Administrator\W</td></tr><tr><td>허용</td><td>Administrator (JWP-DB-01\Administrator)</td><td>모든 권한</td><td>C:\Users\Administrator\W</td></tr></table></div></div></div></div></div></div>	유형	보안 주제	액세스	다음에서 상속됨	허용	SYSTEM	모든 권한	C:\Users\Administrator\W	허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\Users\Administrator\W	허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\Users\Administrator\W
유형	보안 주제	액세스	다음에서 상속됨																		
허용	SYSTEM	모든 권한	C:\Users\Administrator\W																		
허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\Users\Administrator\W																		
허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\Users\Administrator\W																		

4. 환경 파일 접근

2	Initialization 파일 접근 권한 설정	<div>[Unix 확인방법] 양호 - 초기화 파일 접근 권한이 640 이하로 설정되어 있는 경우 취약 - 초기화 파일 접근 권한이 640 초과로 설정되어 있는 경우</div> <div>[Windows 확인방법] 양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우 취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우</div>	양호	<div>이름: C:\app\Administrator\product\21c\database\initXE.ora 소유자: Administrators (JWP-DB-01\Administrators) </div> <div>사용 권한 <div>감사</div> 유효한 액세스</div> <div>자세한 내용을 보려면 사용 권한 항목을 두 번 클릭하십시오. 사용 권한 항목을 수정하려면 항목을 선택하고 [편집]을 클릭하십시오(사용 가능한 경우).</div> <div>사용 권한 항목:</div> <table><tr><th>유형</th><th>보안 주체</th><th>액세스</th><th>다음에서 상속됨</th></tr><tr><td> 허용</td><td>Administrators (JWP-DB-01\Administrators)</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>SYSTEM</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>OracleServiceXE</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\database\</td></tr><tr><td> 허용</td><td>Administrator (JWP-DB-01\Administrator)</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr></table>	유형	보안 주체	액세스	다음에서 상속됨	허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\app\Administrator\product\21c\	허용	SYSTEM	모든 권한	C:\app\Administrator\product\21c\	허용	OracleServiceXE	모든 권한	C:\app\Administrator\product\21c\database\	허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\app\Administrator\product\21c\	허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...	모든 권한	C:\app\Administrator\product\21c\																					
유형	보안 주체	액세스	다음에서 상속됨																																														
허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\app\Administrator\product\21c\																																														
허용	SYSTEM	모든 권한	C:\app\Administrator\product\21c\																																														
허용	OracleServiceXE	모든 권한	C:\app\Administrator\product\21c\database\																																														
허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\app\Administrator\product\21c\																																														
허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...	모든 권한	C:\app\Administrator\product\21c\																																														
3	Oracle Password 파일 접근 권한 설정	<div>[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</div> <div>[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</div>	양호	<div>이름: C:\app\Administrator\product\21c\database\PWDXE.ora 소유자: Administrators (JWP-DB-01\Administrators) </div> <div>사용 권한 <div>감사</div> 유효한 액세스</div> <div>자세한 내용을 보려면 사용 권한 항목을 두 번 클릭하십시오. 사용 권한 항목을 수정하려면 항목을 선택하고 [편집]을 클릭하십시오(사용 가능한 경우).</div> <div>사용 권한 항목:</div> <table><tr><th>유형</th><th>보안 주체</th><th>액세스</th><th>다음에서 상속됨</th></tr><tr><td> 허용</td><td>Administrators (JWP-DB-01\Administrators)</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>SYSTEM</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>OracleServiceXE</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\database\</td></tr><tr><td> 허용</td><td>Administrator (JWP-DB-01\Administrator)</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr></table>	유형	보안 주체	액세스	다음에서 상속됨	허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\app\Administrator\product\21c\	허용	SYSTEM	모든 권한	C:\app\Administrator\product\21c\	허용	OracleServiceXE	모든 권한	C:\app\Administrator\product\21c\database\	허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\app\Administrator\product\21c\	허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...	모든 권한	C:\app\Administrator\product\21c\																					
유형	보안 주체	액세스	다음에서 상속됨																																														
허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\app\Administrator\product\21c\																																														
허용	SYSTEM	모든 권한	C:\app\Administrator\product\21c\																																														
허용	OracleServiceXE	모든 권한	C:\app\Administrator\product\21c\database\																																														
허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\app\Administrator\product\21c\																																														
허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...	모든 권한	C:\app\Administrator\product\21c\																																														
4	AlertLog 파일 접근 제한	<div>[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</div> <div>[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</div>	양호	<div>이름: C:\app\Administrator\product\21c\diag\rdbs\%xe%\trace\alert_xe.log 소유자: OracleServiceXE </div> <div>사용 권한 <div>감사</div> 유효한 액세스</div> <div>자세한 내용을 보려면 사용 권한 항목을 두 번 클릭하십시오. 사용 권한 항목을 수정하려면 항목을 선택하고 [편집]을 클릭하십시오(사용 가능한 경우).</div> <div>사용 권한 항목:</div> <table><tr><th>유형</th><th>보안 주체</th><th>액세스</th><th>다음에서 상속됨</th></tr><tr><td> 허용</td><td>Administrators (JWP-DB-01\Administrators)</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>SYSTEM</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>Administrator (JWP-DB-01\Administrator)</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr></table> <div>이름: C:\app\Administrator\product\21c\diag\rdbs\%xe%\trace\attention_xe.log 소유자: OracleServiceXE </div> <div>사용 권한 <div>감사</div> 유효한 액세스</div> <div>자세한 내용을 보려면 사용 권한 항목을 두 번 클릭하십시오. 사용 권한 항목을 수정하려면 항목을 선택하고 [편집]을 클릭하십시오(사용 가능한 경우).</div> <div>사용 권한 항목:</div> <table><tr><th>유형</th><th>보안 주체</th><th>액세스</th><th>다음에서 상속됨</th></tr><tr><td> 허용</td><td>Administrators (JWP-DB-01\Administrators)</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>SYSTEM</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>Administrator (JWP-DB-01\Administrator)</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr></table>	유형	보안 주체	액세스	다음에서 상속됨	허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\app\Administrator\product\21c\	허용	SYSTEM	모든 권한	C:\app\Administrator\product\21c\	허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...	모든 권한	C:\app\Administrator\product\21c\	허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\app\Administrator\product\21c\	유형	보안 주체	액세스	다음에서 상속됨	허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\app\Administrator\product\21c\	허용	SYSTEM	모든 권한	C:\app\Administrator\product\21c\	허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...	모든 권한	C:\app\Administrator\product\21c\	허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\app\Administrator\product\21c\					
유형	보안 주체	액세스	다음에서 상속됨																																														
허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\app\Administrator\product\21c\																																														
허용	SYSTEM	모든 권한	C:\app\Administrator\product\21c\																																														
허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...	모든 권한	C:\app\Administrator\product\21c\																																														
허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\app\Administrator\product\21c\																																														
유형	보안 주체	액세스	다음에서 상속됨																																														
허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\app\Administrator\product\21c\																																														
허용	SYSTEM	모든 권한	C:\app\Administrator\product\21c\																																														
허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...	모든 권한	C:\app\Administrator\product\21c\																																														
허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\app\Administrator\product\21c\																																														
5	Trace Log 파일 접근 제한	<div>[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</div> <div>[Windows 확인방법] 양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우 취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우</div>	양호	<div>이름: C:\app\Administrator\product\21c\diag\rdbs\%xe%\trace 소유자: OracleServiceXE </div> <div>사용 권한 <div>감사</div> 유효한 액세스</div> <div>자세한 내용을 보려면 사용 권한 항목을 두 번 클릭하십시오. 사용 권한 항목을 수정하려면 항목을 선택하고 [편집]을 클릭하십시오(사용 가능한 경우).</div> <div>사용 권한 항목:</div> <table><tr><th>유형</th><th>보안 주체</th><th>액세스</th><th>다음에서 상속됨</th><th>적용 대상</th></tr><tr><td> 허용</td><td>Administrators (JWP-DB-01\Adminis...</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr><tr><td> 허용</td><td>SYSTEM</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr><tr><td> 허용</td><td>ORA_OraDB21Home1_SVCACCTS (J...</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr><tr><td> 허용</td><td>Administrator (JWP-DB-01\Administ...</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr></table> <div>이름: C:\app\Administrator\product\21c\diag\rdbs\%xe%\trace\%xe_cjq0_3620_4856.trc 소유자: OracleServiceXE </div> <div>사용 권한 <div>감사</div> 유효한 액세스</div> <div>자세한 내용을 보려면 사용 권한 항목을 두 번 클릭하십시오. 사용 권한 항목을 수정하려면 항목을 선택하고 [편집]을 클릭하십시오(사용 가능한 경우).</div> <div>사용 권한 항목:</div> <table><tr><th>유형</th><th>보안 주체</th><th>액세스</th><th>다음에서 상속됨</th></tr><tr><td> 허용</td><td>Administrators (JWP-DB-01\Administrators)</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>SYSTEM</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr><tr><td> 허용</td><td>Administrator (JWP-DB-01\Administrator)</td><td>모든 권한</td><td>C:\app\Administrator\product\21c\</td></tr></table>	유형	보안 주체	액세스	다음에서 상속됨	적용 대상	허용	Administrators (JWP-DB-01\Adminis...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일	허용	SYSTEM	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일	허용	ORA_OraDB21Home1_SVCACCTS (J...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일	허용	Administrator (JWP-DB-01\Administ...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일	유형	보안 주체	액세스	다음에서 상속됨	허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\app\Administrator\product\21c\	허용	SYSTEM	모든 권한	C:\app\Administrator\product\21c\	허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...	모든 권한	C:\app\Administrator\product\21c\	허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\app\Administrator\product\21c\
유형	보안 주체	액세스	다음에서 상속됨	적용 대상																																													
허용	Administrators (JWP-DB-01\Adminis...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																																													
허용	SYSTEM	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																																													
허용	ORA_OraDB21Home1_SVCACCTS (J...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																																													
허용	Administrator (JWP-DB-01\Administ...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																																													
유형	보안 주체	액세스	다음에서 상속됨																																														
허용	Administrators (JWP-DB-01\Administrators)	모든 권한	C:\app\Administrator\product\21c\																																														
허용	SYSTEM	모든 권한	C:\app\Administrator\product\21c\																																														
허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\ORA...	모든 권한	C:\app\Administrator\product\21c\																																														
허용	Administrator (JWP-DB-01\Administrator)	모든 권한	C:\app\Administrator\product\21c\																																														
6	컨트롤, redo 로그파일, 데이터 파일 접근 제한	<div>[Unix 확인방법] 양호 - 접근 권한이 640 이하로 설정되어 있는 경우 취약 - 접근 권한이 640 초과로 설정되어 있는 경우</div> <div>[Windows 확인방법] 양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우 취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우</div>	양호	<div>이름: C:\app\Administrator\product\21c\oradata\XE 소유자: Administrators (JWP-DB-01\Administrators) </div> <div>사용 권한 <div>감사</div> 유효한 액세스</div> <div>자세한 내용을 보려면 사용 권한 항목을 두 번 클릭하십시오. 사용 권한 항목을 수정하려면 항목을 선택하고 [편집]을 클릭하십시오(사용 가능한 경우).</div> <div>사용 권한 항목:</div> <table><tr><th>유형</th><th>보안 주체</th><th>액세스</th><th>다음에서 상속됨</th><th>적용 대상</th></tr><tr><td> 허용</td><td>OracleServiceXE</td><td>모든 권한</td><td>없음</td><td>이 폴더, 하위 폴더 및 파일</td></tr><tr><td> 허용</td><td>Administrators (JWP-DB-01\Adminis...</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr><tr><td> 허용</td><td>SYSTEM</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr><tr><td> 허용</td><td>Administrator (JWP-DB-01\Administ...</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr><tr><td> 허용</td><td>ORA_OraDB21Home1_SVCACCTS (J...</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr></table>	유형	보안 주체	액세스	다음에서 상속됨	적용 대상	허용	OracleServiceXE	모든 권한	없음	이 폴더, 하위 폴더 및 파일	허용	Administrators (JWP-DB-01\Adminis...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일	허용	SYSTEM	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일	허용	Administrator (JWP-DB-01\Administ...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일	허용	ORA_OraDB21Home1_SVCACCTS (J...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일															
유형	보안 주체	액세스	다음에서 상속됨	적용 대상																																													
허용	OracleServiceXE	모든 권한	없음	이 폴더, 하위 폴더 및 파일																																													
허용	Administrators (JWP-DB-01\Adminis...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																																													
허용	SYSTEM	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																																													
허용	Administrator (JWP-DB-01\Administ...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																																													
허용	ORA_OraDB21Home1_SVCACCTS (J...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																																													

	7	\$TNS_ADMIN 파일 접근 제한	<div>[Unix 확인방법]</div> <div>양호 - 접근 권한이 644 이하로 설정되어 있는 경우</div> <div>취약 - 접근 권한이 644 초과로 설정되어 있는 경우</div> <div>[Windows 확인방법]</div> <div>양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우</div> <div>취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우</div>	취약	<div>sqlnet.ora 고급 보안 설정</div> <div>이름: C:\app\Administrator\product\21c\homes\OraDB21Home1\network\admin\sqlnet.ora</div> <div>소유자: Administrators (JWP-DB-01\Administrators) 변경(C)</div> <div>사용 권한 감사 유효한 액세스</div> <div>자세한 내용을 보려면 사용 권한 항목을 두 번 클릭하십시오. 사용 권한 항목을 수정하려면 항목을 선택하고 [편집]을 클릭하십시오.(사용 가능한 경우).</div> <div>사용 권한 항목:</div> <table><tr><th>유형</th><th>보안 주제</th><th>액세스</th><th>다음에서 상속됨</th></tr><tr><td>허용</td><td>Administrators (JWP-DB-01\Administrators)</td><td>모든 권한</td><td>없음</td></tr><tr><td>허용</td><td>SYSTEM</td><td>모든 권한</td><td>없음</td></tr><tr><td>허용</td><td>Authenticated Users</td><td>읽기 및 실행</td><td>없음</td></tr><tr><td>허용</td><td>ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\WORA...</td><td>모든 권한</td><td>없음</td></tr><tr><td>허용</td><td>Administrator (JWP-DB-01\Administrator)</td><td>모든 권한</td><td>없음</td></tr></table> <div>Administrators, SYSTEM, Owner가 아닌 일반 사용자에게 읽기 및 실행과 같은 불필요한 권한이 존재함</div>	유형	보안 주제	액세스	다음에서 상속됨	허용	Administrators (JWP-DB-01\Administrators)	모든 권한	없음	허용	SYSTEM	모든 권한	없음	허용	Authenticated Users	읽기 및 실행	없음	허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\WORA...	모든 권한	없음	허용	Administrator (JWP-DB-01\Administrator)	모든 권한	없음
	유형	보안 주제	액세스	다음에서 상속됨																									
허용	Administrators (JWP-DB-01\Administrators)	모든 권한	없음																										
허용	SYSTEM	모든 권한	없음																										
허용	Authenticated Users	읽기 및 실행	없음																										
허용	ORA_OraDB21Home1_SVCACCTS (JWP-DB-01\WORA...	모든 권한	없음																										
허용	Administrator (JWP-DB-01\Administrator)	모든 권한	없음																										
8	감사 로그 파일 접근 제한	<div>[Unix 확인방법]</div> <div>양호 - 접근 권한이 750 이하로 설정되어 있는 경우</div> <div>취약 - 접근 권한이 750 초과로 설정되어 있는 경우</div> <div>※ Audit_file_dest에 설정된 경로의 디렉터리의 접근 권한 설정 확인</div> <div>[Windows 확인방법]</div> <div>양호 - Administrators, SYSTEM, Owner에게 모든 권한 또는 이하인 경우</div> <div>취약 - 기타 다른 그룹에 권한이 부여되어 있을 경우</div> <div>※ Audit_file_dest에 설정된 경로의 디렉터리의 접근 권한 설정 확인</div>	양호	<div>adump 고급 보안 설정</div> <div>이름: C:\app\Administrator\product\21c\admin\XE\adump</div> <div>소유자: Administrators (JWP-DB-01\Administrators) 변경(C)</div> <div>사용 권한 감사 유효한 액세스</div> <div>자세한 내용을 보려면 사용 권한 항목을 두 번 클릭하십시오. 사용 권한 항목을 수정하려면 항목을 선택하고 [편집]을 클릭하십시오.(사용 가능한 경우).</div> <div>사용 권한 항목:</div> <table><tr><th>유형</th><th>보안 주제</th><th>액세스</th><th>다음에서 상속됨</th><th>적용 대상</th></tr><tr><td>허용</td><td>Administrators (JWP-DB-01\Adminis...</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr><tr><td>허용</td><td>SYSTEM</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr><tr><td>허용</td><td>ORA_OraDB21Home1_SVCACCTS (J...</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr><tr><td>허용</td><td>Administrator (JWP-DB-01\Administ...</td><td>모든 권한</td><td>C:\app\Administrator\prod...</td><td>이 폴더, 하위 폴더 및 파일</td></tr></table>	유형	보안 주제	액세스	다음에서 상속됨	적용 대상	허용	Administrators (JWP-DB-01\Adminis...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일	허용	SYSTEM	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일	허용	ORA_OraDB21Home1_SVCACCTS (J...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일	허용	Administrator (JWP-DB-01\Administ...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일
유형	보안 주제	액세스	다음에서 상속됨	적용 대상																									
허용	Administrators (JWP-DB-01\Adminis...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																									
허용	SYSTEM	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																									
허용	ORA_OraDB21Home1_SVCACCTS (J...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																									
허용	Administrator (JWP-DB-01\Administ...	모든 권한	C:\app\Administrator\prod...	이 폴더, 하위 폴더 및 파일																									
5. 보안 패치	1	보안 패치 적용	<div>양호 - 최신의 서비스 팩 적용한 경우, Opatch 2016년 1월 패치 적용</div> <div>취약 - 최신의 서비스 팩 적용하지 않을 경우. Opatch 2016년 1월 이전 패치 적용</div>	취약	<div>Administrator: C:\Windows\System32\cmd.exe</div> <div>C:\app\Administrator\product\21c\dbhomeXE\OPatch>opatch.bat lsinventory</div> <div>Oracle Interim ?? ?? 12.2.0.1.26</div> <div>Copyright (c) 2025, Oracle Corporation. All rights reserved.</div> <div>Oracle ? : C:\app\ADMINI~1\product\21c\dbhomeXE</div> <div>?? ????: C:\Program Files\Oracle\Inventory</div> <div>??:</div> <div>OPatch ??? : 12.2.0.1.26</div> <div>OUI ??? : 12.2.0.9.0</div> <div>?? ?? ??: C:\app\ADMINI~1\product\21c\dbhomeXE\cfgtoollogs\opatch\opatch2025-09-01_17-42-27??_1.log</div> <div>Lsinventory Output file location : C:\app\ADMINI~1\product\21c\dbhomeXE\cfgtoollogs\opatch\lsinv\lsinv</div> <div>-----</div> <div>Local Machine Information::</div> <div>Hostname: WIN-QG40KBPU5KO.localdomain</div> <div>ARU platform id: 233</div> <div>ARU platform description:: Microsoft Windows (64-bit AMD)</div> <div>-----</div> <div>??? ??? ? ?(1):</div> <div>Oracle Database 21c 21.0.0.0.0</div> <div>? Oracle ?? 1?? ??? ?????</div> <div>? Oracle ?? ??? Interim ???</div> <div>Oracle Database 21c(21.0.0.0) 환경에서 Opatch lsinventory 결과, 추가 보안 패치(RU/CPU)가 적용되지 않은 상태로 확인됨</div>																								
6. 보안 감사 설정	1	SYS 감사 수행 설정	<div>양호 - "AUDIT_SYS_OPERATION"의 값이 "TRUE"로 설정 되어 있는 경우</div> <div>취약 - "AUDIT_SYS_OPERATION"의 값이 "FALSE"로 설정 되어 있는 경우</div>	양호	<div>시작 관리자 JWPatch</div> <div>워크시트 질의 작성기</div> <div>SELECT name, value FROM v\$parameter WHERE name='audit_sys_operations';</div> <div>스크립트 출력 질의 결과 x</div> <div>SQL 인출된 모든 행: 1(0.018초)</div> <table><tr><th>NAME</th><th>VALUE</th></tr><tr><td>audit_sys_operations</td><td>TRUE</td></tr></table>	NAME	VALUE	audit_sys_operations	TRUE																				
	NAME	VALUE																											
audit_sys_operations	TRUE																												
2	Audit Trail 기록 설정	<div>양호 - 감사 설정을 위해 트리거, FGA를 사용하는 경우</div> <div>취약 - "Audit_trail"의 값이 'none' 으로 설정되어 있는 경우</div>	양호	<div>시작 관리자 JWPatch</div> <div>워크시트 질의 작성기</div> <div>SELECT name, value FROM v\$parameter WHERE name='audit_trail';</div> <div>스크립트 출력 질의 결과 x</div> <div>SQL 인출된 모든 행: 1(0.021초)</div> <table><tr><th>NAME</th><th>VALUE</th></tr><tr><td>audit_trail</td><td>DB</td></tr></table>	NAME	VALUE	audit_trail	DB																					
NAME	VALUE																												
audit_trail	DB																												
7. 네트워크 접근 제어	1	DATA DICTIONARY 접근 제한	<div>양호 - "O7_DICTIONARY_ACCESSIBILITY" 값이 FALSE로 되어 있는 경우</div> <div>취약 - "O7_DICTIONARY_ACCESSIBILITY" 값이 TRUE로 되어 있는 경우</div>	N/A	Oracle 19c 버전 이상부터 O7_DICTIONARY_ACCESSIBILITY 미지원																								
	2	원격 OS 인증 방식 설정	<div>양호 - "REMOTE_OS_AUTHENT"의 값이 FALSE로 설정되어 있는 경우</div> <div>취약 - "REMOTE_OS_AUTHENT"의 값이 TRUE로 설정되어 있는 경우</div> <div>※ 원격 OS 인증(REMOTE_OS_AUTHENT) 기능은 21c 버전 이상부터 지원하지 않음</div>	N/A	Oracle 21c 버전 이상부터 원격 OS 인증(REMOTE_OS_AUTHENT) 기능 미지원																								
점검결과				12.0																									
	보안 적용율 (양호항목 / 진단항목) %			62.5%																									