

목 차

1. DBMS	2
1.1. 계정 관리.....	2
1.1.1. 기본 계정의 패스워드, 정책 등을 변경하여 사용	2
1.1.2. scott 등 Demonstration 및 불필요 계정을 제거하거나 잠금 설정 후 사용.....	4
1.1.3. 패스워드의 사용기간 및 복잡도 기관 정책에 맞도록 설정	5
1.1.4. 데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용	8
1.1.5. 패스워드 재사용에 대한 제약	10
1.1.6. DB 사용자 계정 개별적 부여	11
1.2. 접근관리.....	13
1.2.1. 원격에서 DB 서버로의 접속 제한	13
1.2.2. DBA이외의 인가되지 않은 사용자 시스템 테이블 접근 제한 설정	15
1.2.3. 오라클 데이터베이스의 경우 리스너 패스워드 설정	17
1.2.4. 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거.....	18
1.2.5. 일정 횟수의 로그인 실패 시 잠금 정책 설정	19
1.2.6. 데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정	20
1.2.7. 데이터베이스의 주요 설정파일, 패스워드 파일 등 주요 파일들의 접근 권한 설정.....	21
1.2.8. 관리자 이외의 사용자가 오라클 리스너의 접속을 통해 리스너 로그 및 trace 파일에 대한 변경 권한 제한	23
1.3. 옵션관리.....	24
1.3.1. 응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되지 않도록 조정	24
1.3.2. OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정.....	25
1.3.3. 패스워드 확인함수가 설정되어 적용되는가?.....	26
1.3.4. 인가되지 않은 Object Owner가 존재하지 않는가?.....	28
1.3.5. grant option이 role에 의해 부여되도록 설정	29
1.3.6. 데이터베이스의 자원 제한 기능을 TRUE로 설정.....	30
1.4. 패치관리.....	31
1.4.1. 데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용.....	31
1.4.2. 데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에' 적합하도록 설정 34	
1.4.3. 보안에 취약하지 않은 버전의 데이터베이스를 사용하고 있는가?.....	36
1.5. 로그관리.....	37
1.5.1. Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정.....	37

1. DBMS

1.1. 계정 관리

1.1.1. 기본 계정의 패스워드, 정책 등을 변경하여 사용

대상	Oracle, MSSQL, MySQL	위험도	상	code	D-01
취약점 개요	<p>■ Oracle - 데이터베이스의 기본 계정(system, scott 등)의 패스워드 또는, 접근제어 정책을 변경하지 않고 사용할 경우 공격자는 알려진 정보를 이용하여 데이터베이스에 쉽게 접근할 수 있는 취약점이 존재함.</p> <p>■ MSSQL - sa 계정 null 암호 취약점은 비인가자에 의해 sa 계정으로 데이터베이스에 침입하여 정보 삭제, 변경 등의 행위를 할 수 있는 위험이 있음.</p> <p>■ MySQL - root 계정의 패스워드가 디폴트 설정 값인 null을 사용할 경우, 시스템에 접근한 임의의 모든 사용자가 root 권한으로 접속하여 mysql의 모든 작업을 할 수 있어 mysql DB에 저장된 모든 정보가 유출 되는 등의 침해사고를 일으킬 위험이 있음. 기본 계정을 변경하지 않고 사용하는 경우 공격자에게 정보가 노출될 가능성이 있으므로 변경하여야 함.</p>				
보안대책					
판단기준	양호: 기본 계정의 패스워드를 변경하여 사용하는 경우				
	취약: 기본 계정의 디폴트 설정을 변경하지 않고 사용하는 경우				
조치방법	기본(관리자) 계정의 패스워드 및 정책 변경				
보안설정방법					
<p>■ Oracle</p> <p>1. 사용자 계정과 상태를 점검함 SQL> SELECT username, account_status FROM dba_users;</p> <p>2. 특정 사용자 계정의 잠금과 기간만료 설정 SQL> ALTER USER <사용자명> ACCOUNT LOCK PASSWORD expire;</p> <p>3. 불필요한 계정인 경우 계정 삭제 SQL> DROP USER username;</p> <p>4. 사용되는 계정인 경우 계정의 기본 패스워드 변경 후 사용 SQL> alter user username identified by new_passwd;</p> <p>※ 그 이외에 객체 권한 부여 및 기본 role 확인 및 변경 수행 ※ DBSNMP 파일의 접근권한 설정이 필요함 chmod 700 snmp_rw.ora (결과값 -rwx-----snmp_rw.ora)</p>					
Oracle 설치 시 생성되는 디폴트 계정 정보					
User	Password	User	Password		
scott	tiger or tigger	system	manager		

dbsnmp	dbsnmp	sys	changeon_install
tracesvr	trace	outln	outln
ordplugins	ordplugins	ordsys	ordsys
ctxsys	ctxsys	mdsys	mdsys
adams	wood	blake	papr
clark	clth	jones	steel
lbacsys	lbacsys		

■ MS SQL

sa 계정 패스워드 변경

Alter login sa with password='new password'

■ MySQL

root 계정 패스워드 변경

mysql> use mysql

mysql> update user set password=password('new password') where user='root';

mysql> flush privileges;

mysql> set password for root=password('new password')

※ 패스워드가 취약하게 설정된 경우 패스워드를 아래 기준을 준수하여 변경함

< 패스워드 관리 방법 >

1. 영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정

※ 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성

가. 영문 대문자(26개)

나. 영문 소문자(26개)

다. 숫자(10개)

라. 특수문자(32개)

2. 시스템마다 상이한 패스워드 사용

3. 패스워드를 기록해 놓을 경우 변형하여 기록

4. 가급적 자주 패스워드를 변경할 것

조치 시 영향

불필요한 계정 사용 불가

1.1.2. scott 등 Demonstration 및 불필요 계정을 제거하거나 잠금 설정 후 사용

대상	Oracle, MSSQL, MySQL	위험도	상	code	D-02
취약점 개요	데이터베이스의 계정 중 실질적으로 업무에 사용하지 않는 SCOTT, PM, ADAMS, CLARK 등의 Demonstration 계정이 삭제되지 않고 존재하면 공격자가 데이터베이스 시스템에 쉽게 접근하여 데이터를 열람, 삭제, 수정할 위험이 존재함.				
보안대책					
판단기준	양호: 계정 정보를 확인하여 불필요한 계정이 없는 경우				
	취약: 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 불필요한 계정이 존재하는 경우				
조치방법	기본 계정 외 계정의 용도를 파악 후 불필요한 계정 삭제				
보안설정방법					
<p>■ Oracle</p> <p>1. 불필요한 Demonstration 계정 및 오브젝트 삭제 SQL> DROP USER '삭제할 계정'</p> <p>2. 계정 잠금/만료 SQL> ALTER USER '잠금/만료 계정' ACCOUNT LOCK PASSWORD EXPIRE</p> <p>■ MSSQL</p> <p>불필요한 계정 삭제 Exec sp_droplogin '삭제할 계정'</p> <p>■ MySQL</p> <p>불필요한 계정 삭제 mysql> Delete from user where user='삭제할 계정'</p>					
조치 시 영향	Demonstration 계정 / 오브젝트 사용 불가 / 삭제된 계정 사용 불가				

패스워드의 사용기간 및 복잡도 기관 정책에 맞도록 설정

대상	Oracle, MSSQL, MySQL	위험도	상	code	D-03
취약점 개요	<p>주기적인 패스워드 변경이 없을 경우 공격자는 Brute force 공격을 통하여 패스워드를 획득할 위험이 존재함.</p> <p>I Oracle - PASSWORD_LIFE_TIME 값은 패스워드가 만기된 이후에 사용가능한 일수에 대한 제한을 제공함.</p>				
보안대책					
판단기준	양호: 패스워드를 주기적으로 변경하고, 패스워드 정책이 적용되어 있는 경우				
	취약: 패스워드를 주기적으로 변경하지 않거나, 패스워드 정책이 없는 경우				
조치방법	주기적 패스워드 변경, 패스워드 적용 정책 마련				
보안설정방법					
<p>■ Oracle</p> <p>1.패스워드 정책 상태 점검 SQL> SELECT RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE PROFILE='DEFAULT';</p> <p>2.미 설정 시 패스워드 정책 프로파일 생성 Sql> CREATE PROFILE grace_5 LIMIT FAILED_LOGIN_ATTEMPTS 3 (패스워드 실패를 3번까지만 가능) PASSWORD_LOCK_TIME 1/1440 (패스워드 잠금이 해제 될 때까지의 시간, 1/1440 = 1분) PASSWORD_LIFE_TIME 90 (90일동안만 패스워드를 사용) PASSWORD_GRACE_TIME 5 (만료되기 5일전부터 변경하라는 알람) PASSWORD_REUSE_TIME 30 (한번 사용한 패스워드를 다시 사용 하려면 30일 후부터 재사용 가능) PASSWORD_VERIFY_FUNCTION verify_function; (패스워드 확인 함수)</p> <p>3.사용자에게 패스워드 프로파일 적용 SQL> ALTER USER haksa PROFILE scott_pass; haksa 사용자에게 scott_pass 프로파일을 적용.</p> <p>참고 URL : http://radiocom.kunsan.ac.kr/lecture/oracle/what_is/password.html</p> <p>■ MSSQL</p> <p>1. 패스워드 변경 주기가 60일 이내로 설정되지 않은 경우 패스워드 변경 주기 설정 MSSQL에서 '암호 만료 강제 적용'을 체크함으로써 주기적으로 변경이 가능하며, 변경기간은 OS의 '암호정책'에서 적용 받으므로 '암호 정책 > 최대 암호 사용 기간' 설정도 같이 변경해야 함</p> <p>2. 암호 만료 강제 적용 [보안]> [로그인]> [각 로그인 계정]> [속성]></p>					

로그인 이름(N):

Windows 인증(W)

SQL Server 인증(S)

암호(P):

암호 확인(C):

이전 암호 지정(I)

이전 암호(O):

암호 정책 강제 적용(F)

암호 만료 강제 적용(X)

다음 로그인할 때 반드시 암호 변경(U)

암호 만료 강제 적용: 설정(체크) 확인

3. OS의 암호 정책 설정

[관리도구] > [로컬 보안 정책] > [보안 설정] > [계정 정책] > [암호 정책]

로컬 보안 정책

파일(F) 동작(A) 보기(V) 도움말(H)

정책	보안 설정
암호는 복잡성을 만족해야 함	사용
최근 암호 기억	12 개 암호 기억됨
최대 암호 사용 기간	60 일
최소 암호 길이	8 문자
최소 암호 사용 기간	1 일
해독 가능한 암호화를 사용하...	사용 안 함

'최대 암호 사용 기간 : '60일' 설정

■ MySQL

1. 패스워드 설정 규칙 적용

패스워드 설정 규칙에 맞추어 패스워드를 설정할 수 있도록 시스템 차원에서 기능 제공

2. 패스워드 관리 적용

패스워드 신규 적용 및 초기화 시 설정 규칙에 맞추어 관리하고, 저장 시에는 일방향 암호 알고리즘을 통한 암호화 처리(One-Way Encryption)

3. 패스워드 변경기능 구현

사용자가 패스워드 설정규칙 내에서 스스로 패스워드를 변경할 수 있도록 기능 제공

패스워드 설정은 다음과 같은 방법으로 가능

```
mysql> use mysql
```

```
mysql> update user set password=password('new password') where user='user name';
```

```
mysql> flush privileges; 또는,
```

```
mysql> set password for 'user name'@'%'=password('new password')
```

```
mysql> flush privileges;
```

조치 시 영향	주기적인 패스워드 교체 필요
----------------	-----------------

1.1.3. 데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용

대상	Oracle	위험도	상	code	D-04
취약점 개요	DBA에게만 허용되어야 하는 SYSDBA 권한이 응용프로그램 계정 또는 일반 사용자 계정에 허용되어 있는 경우 공격자는 이를 이용하여 쉽게 DBA 권한으로 데이터베이스에 접근 가능함.				
보안대책					
판단기준	양호: 계정별 관리자권한이 차등 부여 되어 있는 경우				
	취약: 일반 사용자 계정에 불필요하게 관리자 권한이 부여되어 있는 경우				
조치방법	계정별 관리자 권한 차등 부여, 삭제				
보안설정방법					
<p>■ Oracle</p> <p>1. SYSDBA 권한 점검 SQL> SELECT USERNAME FROM V\$PWFILERS WHERE USERNAME NOT IN (SELECT GRANTEE FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE='DBA') and USERNAME !='INTERNAL' and sysdba='TRUE'; (어떠한 계정이라도 나오는 경우 취약)</p> <p>2. 특정 계정에 SYSDBA 권한 적용 SQL> GRANT sysdba TO scott;</p> <p>3. 특정 계정에 SYSDBA 권한 제거 SQL> REVOKE FROM sysdba FROM scott;;</p> <p>※ 불필요하게 시스템 권한을 부여한 계정의 권한 변경 필요 ※ 시스템 권한 부여가 필요한 경우 필요한 테이블별 권한 부여 ※ 인가된 사용자는 관리자 권한에 role을 grant한 후, 시스템 권한을 grant하고 role을 인가된 사용자에게 grant 함</p> <p>■ MSSQL</p> <p>1. sysadmin 서버 역할의 계정 목록을 확인 후 해당 서버 역할에 불필요한 계정이 있는 경우 서버 역할에서 삭제 sysadmin 서버 역할에서 불필요한 계정 삭제 Exec sp_droprolemember 'user_name', 'sysadmin'</p> <p>(예) Exec sp_dropsvrolemember 'user01', 'sysadmin' (user01 계정을 sysadmin 서버 역할에서 삭제)</p> <p>■ MySQL</p> <p>1. mysql.user 테이블에 적용된 권한은 모든 데이터베이스에 적용되므로 host, user, password를 제외한 나머지 권한은 허용하지 않음('N')으로 설정</p>					

- 사용자 등록

```
mysql> insert into mysql.user (host, name, password) values('%', 'user name', password ('password')) ※ 디폴트로 모든 권한 'N' 설정
```

- 권한 변경

```
mysql> update mysql.user set <권한>='N' where user='user name'
```

2. 각 사용자는 접근하고자 하는 DB를 mysql.db에 등록 후 접근 권한을 부여하여 사용

- DB등록 시 권한 부여

```
mysql> insert into mysql.db values('%','DB name', 'username', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y')
```

```
mysql> flush privileges
```

- DB 권한 업데이트

```
mysql> update mysql.db set <권한>='Y' where db=<DB name> and user='user name'
```

```
mysql> flush privileges
```

조치 시 영향	일반적으로 영향 없음
----------------	-------------

1.1.4. 패스워드 재사용에 대한 제약

대상	Oracle	위험도	중	code	D-05
취약점 개요	PASSWORD_REUSE_TIME 값은 패스워드가 재사용될 수 있기 전에 일수를 명시하는 파라미터이며, PASSWORD_REUSE_MAX는 횟수 설정 파라미터임. 파라미터 미설정 시 패스워드 노출 가능성이 증가함.				
보안대책					
판단기준	양호: PASSWORD_REUSE_TIME, PASSWORD_REUSE_MAX 파라미터 설정이 적용된 경우				
	취약: PASSWORD_REUSE_TIME, PASSWORD_REUSE_MAX 파라미터 설정이 적용되지 않은 경우				
조치방법	PASSWORD_REUSE_TIME, PASSWORD_REUSE_MAX 파라미터 설정				
보안설정방법					
<p>■ Oracle</p> <p>1. 설정확인(SQL*Plus)</p> <pre>-- Check for both reuse max and reuse time not set: select profile from DBA_PROFILES where (resource_name='PASSWORD_REUSE_MAX' and limit in ('UNLIMITED','NULL')) or profile in (select profile from DBA_PROFILES where resource_name='PASSWORD_REUSE_TIME') and limit in ('UNLIMITED','NULL'); -- Check for reuse max with value that is less than allowed minimum select profile from DBA_PROFILES where resource_name='PASSWORD_REUSE_MAX' and limit not in ('UNLIMITED','NULL') and limit < '10'; -- Check for reuse time that is less than allowed minimum select profile from DBA_PROFILES where resource_name='PASSWORD_REUSE_TIME' and limit not in ('UNLIMITED','NULL')and limit < '365';</pre> <p>2. PASSWORD_REUSE_TIME 및 프로파일 파라미터 수정</p> <pre>SQL> alter profile default limit password_reuse_time 365 password_reuse_max 10; SQL> alter profile [profile name] limit password_reuse_time default password_reuse_max default;</pre>					
조치 시 영향	일반적으로 영향 없음				

1.1.5. DB 사용자 계정 개별적 부여

대상	Oracle, MSSQL, MySQL	위험도	중	code	D-06
취약점 개요	데이터베이스의 사용자 계정이 사용자, 프로세스와 응용 프로그램 등에 동일하게 사용하게 될 경우 침해사고 발생 시 책임 추적에 영향을 주며, 계정별 권한 부여가 불가능해지고 사용하지 않는 계정을 이용한 비인가 사용자 접속이 가능함.				
보안대책					
판단기준	양호: 사용자별 계정을 사용하고 있는 경우				
	취약: 공용 계정을 사용하고 있는 경우				
조치방법	사용자별 계정 생성 및 권한 부여				
보안설정방법					
<p>■ Oracle</p> <ol style="list-style-type: none"> 계정 확인(SQL*Plus) SQL> select username from dba_users order by username;(사용하지 않거나 모르는 계정 확인) 공통으로 사용하는 계정 삭제 SQL> DROP USER '삭제할 계정' 사용자별, 응용프로그램별 계정 생성 SQL> Create user username identified by passwd 권한 부여 SQL> grant connect, resource to username <p>■ MSSQL</p> <ol style="list-style-type: none"> 불필요한 계정 삭제 Exec sp_droplogin '삭제할 계정' 사용자별, 응용프로그램별 계정 생성 CREATE login '생성 계정' WITH password = '패스워드' CREATE user '생성 계정' FOR login '생성 계정' WITH default_schema = '생성 계정'; ALTER USER '생성 계정' WITH DEFAULT_SCHEMA = '생성 계정' EXEC sp_adduser '생성 계정', '생성 계정', 'db_owner' EXEC sp_adduser '생성 계정', '생성 계정', '생성 계정' EXEC sp_grantdbaccess '생성 계정','생성 계정' <p>■ MySQL</p> <ol style="list-style-type: none"> 불필요한 계정 삭제 mysql> Delete from user where user='삭제할 계정' 사용자별, 응용프로그램별 계정 생성, 권한 설정 mysql> insert into user('localhost','user', 'password') values('localhost', '생성 계정', 'password('패스워드 ')); mysql> insert into mysql.db values('%','DB name', 'username', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y') 					

```
mysql> flush privileges
```

조치 시 영향	일반적으로 영향 없음
----------------	-------------

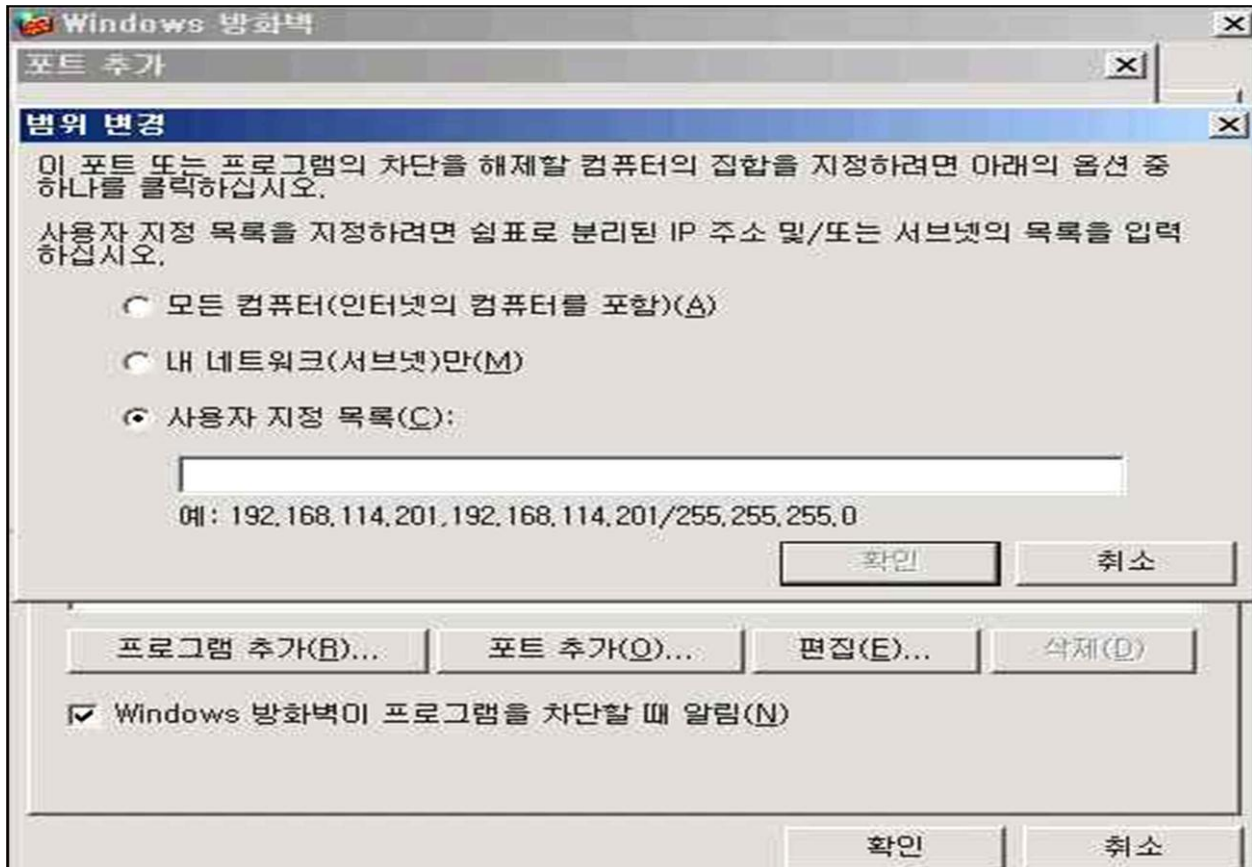
1.2. 접근관리

1.2.1. 원격에서 DB 서버로의 접속 제한

대상	Oracle, MySQL	위험도	상	code	D-07
취약점 개요	<p>허용되지 않은 IP에서 원격으로 DB에 접속이 허용되어 있는 경우 공격자에 의해 네트워크 서비스 스캐닝을 통한 DB 사용 여부가 확인되어 공격 대상이 될 수 있으며, DB 내의 데이터 유출이 가능함.</p> <p>■ Oracle - REMOTE_OS_AUTHENT 값이 TRUE로 설정되어 있으면 안전하지 않은 연결을 통한 원격지의 OS의 인증을 허용함. 이는 원격지 OS의 사용자인 것처럼 속이는 공격자를 허용할 수 있으며, 패스워드 없이 DB 접근을 허용함.</p>				
보안대책					
판단기준	양호: 허용된 IP 및 포트에 대한 접근 통제가 되어 있는 경우				
	취약: IP에 대해 접근 통제가 이루어지지 않는 경우				
조치방법	허용된 IP 및 포트에 대한 접근 통제 적용				

보안설정방법

■ OS



특정 IP에서만 접속 가능하도록 방화벽 등이 설정되어 있는지 확인

시작 > 제어판 > 보안 센터 > windows 방화벽 설정

- 예외 tab -> 포트추가 -> 1433 -> TCP 추가 -> 범위 변경
- 예외 tab -> 포트추가 -> 135 -> TCP 추가 -> 범위 변경
- 예외 tab -> 포트추가 -> 1434 -> UDP 추가 -> 범위 변경

■ Oracle

1. 원격 OS 인증 방식이 불필요한 경우, SYS 계정으로 접속하여 'REMOTE_OS_AUTHENT=FALSE'로 설정

- spfile 사용하는 경우 아래와 같이 설정

```
SQL> ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE SCOPE=spfile
```

- pfile 사용하는 경우 init<SID>.ora 파일 안에 아래와 같이 설정

```
SQL> ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE
```

2. 원격 OS 인증 방식이 필요한 경우

- 방화벽을 통한 원격 접근 IP 제한
- NAT(Network Address Translation)를 사용하여 비공인 IP 부여 후 외부 접근 제한

■ MySQL

1. mysql.user 테이블과 mysql.db 테이블을 조회하여 host가 "%"인 필드 삭제하고 접속 IP를 지정하여 등록

```
mysql> delete from user where host='%';
```

```
mysql> delete from db where host='%';
```

조치 시 영향

허용되지 않은 IP에서 접속 제한

1.2.2. DBA이외의 인가되지 않은 사용자 시스템 테이블 접근 제한 설정

대상	Oracle, MSSQL, MySQL	위험도	상	code	D-08
취약점 개요	DBA만 접근 가능해야 할 테이블을 잘못 설정할 경우 비인가 사용자가 시스템의 주요 정보를 획득하거나, 주요 데이터베이스 설정 변경이 가능함.				
보안대책					
판단기준	양호: DBA만 접근 가능한 테이블에 일반 사용자 접근이 불가능 할 경우				
	취약: DBA만 접근 가능한 테이블에 일반 사용자 접근이 가능한 경우				
조치방법	DBA만 접근 가능한 테이블(System Table)의 접근 권한 변경				
보안설정방법					
<p>■ Oracle</p> <p>1. DBA만 접근 가능한 테이블의 권한 확인(SQL*Plus) SQL> select grantee, privilege, owner, table_name from dba_tab_privs where (owner='SYS' or table_name like 'DBA_%') and privilege <> 'EXECUTE' and grantee not in ('PUBLIC', 'AQ_ADMINISTRATOR_ROLE', 'AQ_USER_ROLE', 'AURORA\$JIS\$UTILITY\$', 'OSE\$HTTP\$ADMIN', 'TRACESVR', 'CTXSYS', 'DBA', 'DELETE_CATALOG_ROLE', 'EXECUTE_CATALOG_ROLE', 'EXP_FULL_DATABASE', 'GATHER_SYSTEM_STATISTICS', 'HS_ADMIN_ROLE', 'IMP_FULL_DATABASE', 'LOGSTDBY_ADMINISTRATOR', 'MDSYS','ODM', 'OEM_MONITOR', 'OLAPSYS', 'ORDSYS', 'OUTLN', 'RECOVERY_CATALOG_OWNER', 'SELECT_CATALOG_ROLE', 'SNMPAGENT', 'SYSTEM', 'WKSYS', 'WKUSER', 'WMSYS', 'WM_ADMIN_ROLE', 'XDB', 'LBACSYS', 'PERFSTAT', 'XDBADMIN') and grantee not in (select grantee from dba_role_privs where granted_role='DBA') order by grantee; (어떤 계정이나 role이 나타나지 않으면 양호)</p> <p>2. 불필요하게 테이블 접근 권한이 사용자 계정에 할당된 경우(SQL*Plus) SQL> REVOKE 권한 on 객체 FROM User</p> <p>■ MSSQL</p> <p>1. System tables 접근 권한이 Public, Guest 또는 비 인가된 사용자에게 부여된 경우 접근 권한을 Public, Guest, 비인가된 사용자로부터 권한 제거 Use database name Revoke <권한> on <object> from [user name][public][guest]</p> <p>2. 시스템 테이블에 접근하기 위해서는 stored procedure 또는, information_schema views를 통해 접근해야 함</p> <p>3. 시스템 테이블에 접근 가능한 stored procedure는 사용이 제한되어야 함</p>					

■ MySQL

1. 일반 사용자로부터 mysql.user 테이블 모든 접근 권한 제거

```
mysql> revoke all on mysql.user from '[user name]'@[hosts];
```

```
mysql> flush privileges
```


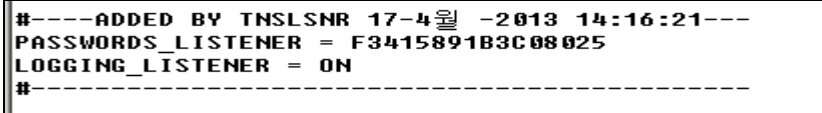
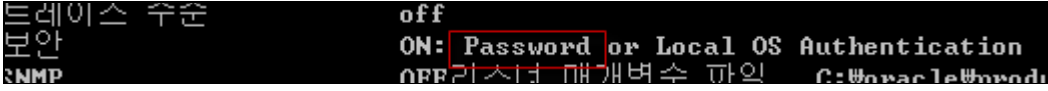
2. 일반 사용자로부터 mysql.user 테이블 접근 권한 제거

```
mysql> revoke [권한] on mysql.user from [user name];
```

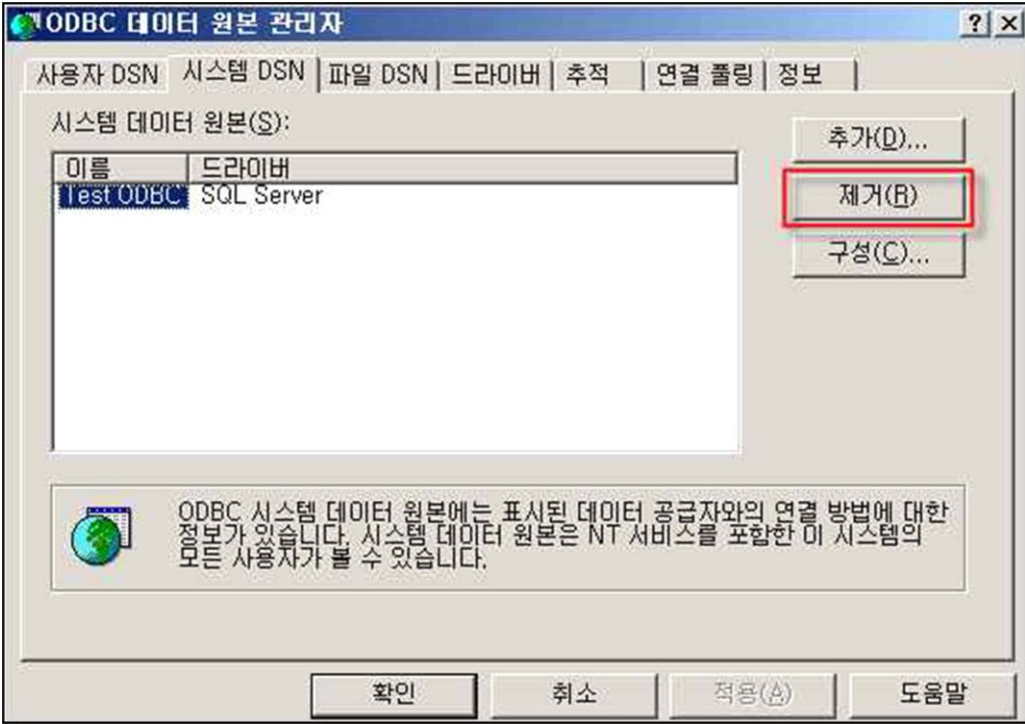
```
mysql> flush privileges
```

조치 시 영향	사용자 계정으로 시스템 테이블 접근 불가
----------------	------------------------

1.2.3. 오라클 데이터베이스의 경우 리스너 패스워드 설정

대상	Oracle	위험도	상	code	D-09
취약점 개요	Listener의 패스워드가 설정되어 있지 않은 경우, Listener의 Owner라면 DBA가 아니라도 Listener를 Shutdown 시키거나 DB 서버에 임의의 파일을 생성할 수 있으며, 원격에서 LSNRCTL 유틸리티를 사용하여 listener.ora 파일에 대한 변경이 가능하므로 이를 수정하지 못하도록 설정해야 함.				
보안대책					
판단기준	양호: Listener의 패스워드가 설정되어 있는 경우				
	취약: Listener의 패스워드가 설정되어 있지 않은 경우				
조치방법	Listener 패스워드 설정				
보안설정방법					
<p>■ Oracle</p> <p>Listener에 패스워드가 설정되지 않은 경우 DoS, 정보 획득, Listener 프로세서를 다운 시킬 수 있는 위험이 있으므로 반드시 Listener 패스워드 설정 필요</p> <pre>LSNRCTL> status</pre>  <p>또는 => listener.ora 설정 파일에 암호화된 패스워드 미 확인 시 취약</p> <p><조치 방법></p> <p>cmd -> lsnrctl 명령으로 LISTENER 프롬프트 모드로 접속</p> <pre>LSNRCTL> change_password</pre> <p>old password: 초기 지정인경우 [Enter]</p> <p>new password : <password></p> <p>reenter new password : <password></p> <p>LSNRCTL> save => listener.ora 설정 파일에 업데이트</p>  <p>또는</p> <pre>LSNRCTL> status</pre>  <p>LSNRCTL> reload Listener 재시작</p>					
조치 시 영향	일반적으로 영향 없음				

1.2.4. 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거

대상	Windows OS	위험도	중	code	D-10
취약점 개요	애플리케이션에 따라 샘플 데이터베이스를 위해서 ODBC 데이터 소스를 설치하거나 불필요한 ODBC/OLE-DB 데이터베이스 드라이브를 설치하여 사용하는 경우 임의의 명령어 실행, 임의의 파일 수정, 시스템 관리자 권한 획득이 가능함				
보안대책					
판단기준	양호: 불필요한 ODBC/OLE-DB가 설치되지 않은 경우				
	취약: 불필요한 ODBC/OLE-DB가 설치된 경우				
조치방법	불필요한 ODBC/OLE-DB 제거				
보안설정방법					
<p>■ Windows NT</p> <ol style="list-style-type: none"> 사용하지 않는 불필요한 ODBC 데이터 소스 제거 시작 > 설정 > 제어판 > 데이터 원본(ODBC) > 시스템 DSN 사용하지 않는 데이터 소스 제거 <p>■ Windows 2000, 2003</p> <ol style="list-style-type: none"> 사용하지 않는 불필요한 ODBC 데이터 소스 제거 시작 > 설정 > 제어판 > 관리도구 > 데이터 원본 (ODBC) > 시스템DSN > 해당 드라이브 클릭 사용하지 않는 데이터 소스 제거 					
					
조치 시 영향	일반적으로 영향 없음				

1.2.5. 일정 횟수의 로그인 실패 시 잠금 정책 설정

대상	Oracle	위험도	중	code	D-11
취약점 개요	일정한 횟수의 로그인 실패 횟수 발생 시 이를 제한하지 않으면 무작위 추측 공격 (Brute force)을 통하여 데이터베이스에 접근이 가능함.				
보안대책					
판단기준	양호: 로그인 시도 횟수를 제한하는 값을 설정한 경우				
	취약: 로그인 시도 횟수가 UNLIMITED로 설정된 경우				
조치방법	로그인 시도 횟수 제한 값 설정				
보안설정방법					
<p>■ Oracle</p> <p>1. 접근 횟수 제한을 위해 파라미터 설정 Failed_login_attempts 프로파일 파라미터 수정 SQL> ALTER PROFILE LIMIT FAILED_LOGIN_ATTEMPTS XXX XXX회 이하로 설정</p> <p>2. 프로파일 적용 SQL> connect / as sysdba SQL> @\$Ora_Home/rdbms/admin/utlpwdmg.sql 또는, default profile에 unlimited로 설정하고 이 default 값을 적용하고자 하는 profile에 적용 SQL> Alter profile default limit password_lock_time unlimited; SQL> Alter profile [profile name] limit password_lock_time default;</p>					
조치 시 영향	일반적으로 영향 없음				

1.2.6. 데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정

대상	Unix OS	위험도	하	code	D-12
취약점 개요	Oracle 소프트웨어의 주요 파일에 대한 보호 등을 위해 Oracle 계정의 umask는 022 이상으로 설정되어야 하며, 설정되어있지 않은 경우 인가되지 않은 사용자가 이를 이용하여 관련 소프트웨어를 실행할 수 있는 위험이 있음.				
보안대책					
판단기준	양호: 계정의 umask가 022 이상으로 설정되어있는 경우				
	취약: 계정의 umask가 022 이하로 설정되어있는 경우				
조치방법	계정의 umask를 022 이상으로 설정 변경				
보안설정방법					
<p>■ Unix OS</p> <p>일시적 설정으로 umask 명령을 이용하여 umask 022 이상 설정 > 시스템 재부팅 > 설정 내역 유지를 위해 .bashrc, .cshrc, .login, .profile 등의 환경 변수 지정 파일에 umask 022(이상 설정)를 추가함</p>					
조치 시 영향	일반적으로 영향 없음				

1.2.7. 데이터베이스의 주요 설정파일, 패스워드 파일 등 주요 파일들의 접근 권한 설정

대상	Unix OS, Windows OS	위험도	중	code	D-13
취약점 개요	비인가자가 redo 파일, 데이터베이스 설정 파일, 데이터 파일, 네트워크 설정 파일, Oracle 패스워드 관련 파일인 orapw.ora, listener.ora, init<SID>.ora 등의 주요 파일에 접근하여 수정·삭제하면 Oracle 데이터베이스 운영에 오류가 발생함.				
보안대책					
판단기준	양호: 주요 설정 파일 및 디렉터리의 퍼미션 설정이 되어있는 경우				
	취약: 주요 설정 파일 및 디렉터리의 퍼미션 설정이 되어있지 않은 경우				
조치방법	주요 설정 파일 및 디렉터리의 퍼미션 설정 변경				
보안설정방법					
<p>■ Oracle</p> <p>I Unix OS</p> <p>1. 디렉터리 또는 파일의 퍼미션 점검</p> <p>\$ORACLE_HOME/bin/oracle (퍼미션 755)</p> <p>\$ORACLE_HOME/bin/ 아래 (퍼미션 755)</p> <p>.sqlplus, sqlldr, sqlload, proc, oraenv, oerr, exp, imp, tkprof, tnsping, wrap</p> <p>\$ORACLE_HOME/bin 아래 (퍼미션 750)</p> <p>.svrmgrl, lsnrctl, dbsnmp</p> <p>\$ORACLE_HOME/network (퍼미션 755)</p> <p>\$ORACLE_HOME/network/admin (퍼미션 755)</p> <p>.listener.ora, sqlnet.ora 등</p> <p>\$ORACLE_HOME/lib (퍼미션 755)</p> <p>\$ORACLE_HOME/network/admin 아래 환경파일 (퍼미션 644)</p> <p>.tnsnames.ora, protocol.ora, sqlpnet.ora</p> <p>\$ORACLE_HOME/dbs/init.ora (퍼미션 640)</p> <p>\$ORACLE_HOME/dbs/init<SID>.ora (퍼미션 640)</p> <p>- Find \$ORACLE_HOME .name init*.ora .print</p> <p>2. redo 파일, 데이터베이스 설정 파일, 데이터 파일 위치 확인(SQL*Plus)</p> <p>SQL> Select value from v\$parameter where name='spfile';</p> <p>SQL> Select 'Control Files: ' value from v\$parameter where name='control_files';</p> <p>SQL> select 'Control Files: ' value from v\$parameter where name='spfile';</p> <p>SQL> select 'Logfile: ' member from v\$logfile;</p> <p>SQL> select 'Datafile: ' name from v\$datafile;</p> <p>- 파일 및 디렉터리의 퍼미션 설정 변경</p> <p>I Windows OS</p>					

1. 패스워드 파일(orapw<SID>) 접근 권한은 administrators, system group, owner group, oracle service account, DBAs에게 모든 권한 또는, 그 이하로 설정하고 다른 그룹은 제거함

■ **MySQL**

┆ **Unix OS**

초기화 파일(my.cnf, my.ini)의 접근 권한을 초기화 파일에 대한 보호를 위하여 600 또는, 640으로 설정
my.cnf 파일 디폴트 위치: /etc/my.cnf, <각 홈디렉터리>/my.cnf
chmod 600 ./my.cnf

┆ **Windows OS**

초기화 파일의 접근 권한은 Administrators, SYSTEM, Owner에게 모든 권한 또는, 그 이하로 설정하고 다른 그룹은 제거함

조치 시 영향	일반적으로 영향 없음
----------------	-------------

1.2.8. 관리자 이외의 사용자가 오라클 리스너의 접속을 통해 리스너 로그 및 trace 파일에 대한 변경 권한 제한

대상	Oracle	위험도	하	code	D-14
취약점 개요	Oracle의 LSNRCTL 도구를 이용하여 리스너에 직접 접근 시 set 명령어를 이용하여 리스너의 모든 파라미터를 변경할 수 있음. 파라미터 변경이 가능한 경우, trace파일 및 리스너 로그 파일 변경이 가능함.				
보안대책					
판단기준	양호: 주요 설정 파일 및 로그 파일에 대한 퍼미션을 관리자로 설정한 경우				
	취약: 주요 설정 파일 및 로그 파일에 대한 퍼미션이 일반 사용자로 설정되어있는 경우				
조치방법	주요 파일 및 로그 파일에 대한 퍼미션을 관리자로 제한				
보안설정방법					
<p>■ Oracle</p> <p>1. 파일 퍼미션 확인 \$ORACLE_HOME/network/admin 디렉터리의 퍼미션을 ls-al(Unix 계열 시스템) 또는, 파일 속성(Windows 계열)을 통해 확인</p> <p>LSNRCTL> status ListenerName LISTENER.ORA 파일 확인 ADMIN_RESTRICTIONS_ListenerName=ON</p> <p>2. listener.ora 파일에 ADMIN_RESTRICTIONS_LISTENER=ON 라인 추가 listener를 재실행하거나 lsnrctl reload 명령어를 실행하여 listener 재 로딩함</p> <pre>#vi /Oracle_HomeDirectory/network/admin/listener.ora - ADMIN_RESTRICTIONS_LISTENER=ON 추가 ※ ListenerName은 DBA가 제공한 리스너 이름 #cd /Oracle_Homedirectory/bin/에서 #LSNRCTL> reload</pre>					
조치 시 영향	일반적으로 영향 없음				

1.3. 옵션관리

1.3.1. 응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되지 않도록 조정

대상	Oracle, MSSQL	위험도	상	code	D-15
취약점 개요	응용 프로그램 계정의 Role 또는 DBA 계정의 Role이 Public으로 설정되어 있으면, 일반 계정에서도 응용 프로그램 테이블 또는 DBA 테이블로의 접근이 가능함				
보안대책					
판단기준	양호: DBA 계정의 Role이 Public으로 설정되어있지 않은 경우				
	취약: DBA 계정의 Role이 Public으로 설정되어있는 경우				
조치방법	DBA 계정의 Role 설정에서 Public 그룹 권한 취소				
보안설정방법					
<p>■ Oracle</p> <p>1. DBA Role 설정 확인(SQL*Plus) SQL> Select granted_role from dba_role_privs where grantee='PUBLIC'; 위와 같이 롤(role)이 설정되어 있는 경우 취약</p> <p>2. public 그룹의 권한 취소(SQL*Plus) SQL> Revoke role from public;</p> <p>■ MSSQL</p> <p>1. 각 Object의 사용 권한이 불필요하게 Public, Guest에 부여된 경우 권한 제거 Use database name (1) 권한 제거 REVOKE <권한> on <object> FROM public guest; (2) 권한 부여 GRANT <권한> on <object> TO public guest;</p> <p>(예) syscolumns 테이블에 대한 SELECT 권한 제거 USE master REVOKE select on sys.syscolumns FROM public;</p> <p>※ Object 사용 권한이 Public에 부여된 경우, 사용 권한이 없는 모든 계정이 Object에 접근 가능하여 Object의 정보를 획득할 수 있으므로 Object 사용 권한을 Public에 부여하는 것을 제한하여야 함</p>					
조치 시 영향	일반적으로 영향 없음				

1.3.2. OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정

대상	Oracle	위험도	상	code	D-16
취약점 개요	<p>OS_ROLES 설정 파라미터는 데이터베이스 접근 제어로 컨트롤되지 않는 OS 그룹에 의해 grant된 퍼미션이 허락되며, REMOTE_OS_ROLES가 TRUE로 설정되어 있는 경우, 원격 사용자가 OS의 다른 사용자로 속여 데이터베이스에 접근할 수 있음.</p> <p>REMOTE_OS_AUTHENT가 TRUE로 설정되어있는 경우 신뢰하는 원격 호스트에서 인증절차 없이 데이터베이스에 접속할 수 있음.</p>				
보안대책					
판단기준	양호: OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES설정이 FALSE로 되어있는 경우				
	취약: OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES설정이 TRUE로 되어있는 경우				
조치방법	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES 설정을 FALSE로 설정				
보안설정방법					
<p>■ Oracle</p> <p><점검 방법></p> <p>- OS_ROLES , REMOTE_OS_ROLES에 대한 확인</p> <pre>SQL> show parameter os_roles;</pre> <p>- REMOTE_OS_AUTHENTICATION에 대한 확인</p> <pre>SQL> show parameter remote_os_authent;</pre> <p>결과가 FALSE가 아니면 취약함</p> <p><조치 방법></p> <pre>SQL> alter system set OS_ROLES/REMOTE_OS_ROLES/REMOTE_OS_AUTHENT =false scope=spfile;</pre> <p>재시작</p> <pre>SQL> shutdown</pre> <pre>SQL> startup</pre>					
조치 시 영향	일반적으로 영향 없음				

1.3.3. 패스워드 확인함수가 설정되어 적용되는가?

대상 OS	Oracle	위험도	중	code	D-17
취약점 개요	PASSWORD_VERIFY_FUNCTION 값은 이 프로파일에 명시된 사용자가 데이터베이스에 로그인 할 때 패스워드 확인을 위해 PL/SQL 함수가 사용되도록 명시하는 프로파일임. PASSWORD_VERIFY_FUNCTION 값이 명시되지 않은 경우 기본적인 패스워드 정책이 적용되지 않는 경우 존재함.				
보안대책					
판단기준	양호: 패스워드 검증 함수로 검증이 진행되는 경우				
	취약: 패스워드 검증 함수가 설정되지 않은 경우				
조치방법	패스워드 검증 함수(PASSWORD_VERIFY_FUNCTION) 사용 설정				

보안설정방법

■ Oracle

1. 설정 확인(SQL*Plus)

```
SQL> SELECT profile, limit FROM dba_profiles, (SELECT limit AS def_pwd_verify_func FROM dba_profiles WHERE resource_name = 'PASSWORD_VERIFY_FUNCTION' AND profile = 'DEFAULT') WHERE resource_name='PASSWORD_VERIFY_FUNCTION' AND REPLACE(limit,'DEFAULT',def_pwd_verify_func) in ('UNLIMITED','NULL');
```

(반환 레코드가 존재하는 경우 취약)

2. 취약 시 패스워드 확인 함수 생성 (sys 계정으로)

```
SQL> start 드라이브:\oracle\product\11.2.0\dbhome_1\RDMS\ADMIN\utlpwdmg.sql
```

3. 패스워드 프로파일에 VERIFY_FUNCTION 함수 적용

```
SQL> ALTER PROFILE scott_pass LIMIT PASSWORD_VERIFY_FUNCTION verify_function;
```

scott_pass 프로파일에 verify_function 함수를 적용.

PARAMETER 설명	
FAILED_LOGIN_ATTEMPTS	log on 시도 반복 허용 횟수
PASSWORD_LIFE_TIME	password의 수명 날짜 기간
PASSWORD_REUSE_TIME	password의 재사용 금지 날짜 기간
PASSWORD_REUSE_MAX	password의 재사용 가능한 최대 횟수
PASSWORD_VERIFY_FUNCTION	password의 검증 함수로 검증 진행
PASSWORD_LOCK_TIME	password의 log on 허용 횟수 실패 후 계정 잠김 날짜 기간
PASSWORD_GRACE_TIME	password가 만료된 후 password_life_time이 경과되어 비밀번호를 변경해야 할 경우, password를 변경할 수 있는 기간을 날수로 지정

조치 시 영향	일반적으로 영향 없음
---------	-------------

1.3.4. 인가되지 않은 Object Owner가 존재하지 않는가?

대상 OS	Oracle	위험도	하	code	D-18
취약점 개요	Object Owner는 SYS, SYSTEM과 같은 데이터베이스 관리자 계정과 응용 프로그램의 관리자 계정에만 존재하여야 하며, 일반 계정이 존재할 경우 공격자가 이를 이용하여 Object의 수정, 삭제가 가능함.				
보안대책					
판단기준	양호: Object Owner 의 권한이 SYS, SYSTEM, 관리자 계정 등으로 제한된 경우				
	취약: Object Owner 의 권한이 일반 사용자에게도 부여되어있는 경우				
조치방법	Object Owner의 권한을 SYS, SYSTEM, 관리자 계정으로 제한 설정				
보안설정방법					
<p>■ Oracle</p> <p>1. 설정 확인(SQL*Plus)</p> <pre>SQL> Select distinct owner from dba_objects where owner not in ('SYS','SYSTEM','MDSYS','CTXSYS', 'ORDSYS', 'ORDPLUGINS', 'AURORA\$JIS\$UTILITY\$', 'HR','ODM','ODM_MTR','OE','OLAPDBA','OLA PSYS', 'OSE\$HTTP\$ADMIN', 'OUTLN', 'LBACSYS', 'MTSYS', 'PM', 'PUBLIC', 'QS', 'QS_ADM', 'QS_CB', 'QS_CBADM', 'DBSNMP', 'QS_CS', 'QS_ES','QS_OS', 'QS_WS','RMAN', 'SH', 'WKSYS', 'WMSYS','XDB') and owner not in (select grantee from dba_role_privs where granted_role='DBA');</pre> <p>2. 권한 취소(SQL*Plus)</p> <pre>SQL> REVOKE 권한 on 객체 FROM User</pre>					
조치 시 영향	일반적으로 영향 없음				

1.3.5. grant option이 role에 의해 부여되도록 설정

대상 OS	Oracle	위험도	중	code	D-19
취약점 개요	일반 사용자에게 GRANT OPTION이 설정되어있는 경우 일반 사용자가 객체 소유자인 것과 같이 다른 일반 사용자에게 권한을 부여할 수 있어 WITH_GRANT_OPTION은 role에 의하여 설정되어야 함				
보안대책					
판단기준	양호: WITH_GRANT_OPTION이 ROLE에 의하여 설정되어있는 경우				
	취약: WITH_GRANT_OPTION이 ROLE에 의하여 설정되어있지 않은 경우				
조치방법	WITH_GRANT_OPTION이 ROLE에 의하여 설정되도록 변경				
보안설정방법					
<p>■ Oracle</p> <p>1. 설정 확인(SQL*Plus)</p> <pre>SQL> Select grantee ':' owner ':' table_name from dba_tab_privs where grantable='YES' and owner not in ('SYS','MDSYS','ORDPLUGINS','ORDSYS','SYSTEM', 'WMSYS','SDB','LBACSYS') and grantee not in (select grantee from dba_role_privs where granted_role='DBA') order by grantee;</pre> <p>(계정이 나오는 경우 취약)</p> <p>2. 권한 취소, 재부여(SQL*Plus)</p> <pre>SQL> REVOKE Role FROM User</pre>					
조치 시 영향	일반적으로 영향 없음				

1.3.6. 데이터베이스의 자원 제한 기능을 TRUE로 설정

대상 OS	Oracle	위험도	하	code	D-20
취약점 개요	설정 옵션 RESOURCE_LIMIT에 의해서 모든 프로파일 limit 설정 값을 무시할 수 있음. 기본적으로 설정 옵션 RESOURCE_LIMIT 값이 TRUE로 설정되어있지 않으면 모든 프로파일 limit 설정 값들은 무시될 수 있음.				
보안대책					
판단기준	양호: RESOURCE_LIMIT 설정이 TRUE로 되어있는 경우				
	취약: RESOURCE_LIMIT 설정이 FALSE로 되어있는 경우				
조치방법	RESOURCE_LIMIT 설정을 TRUE로 설정 변경				
보안설정방법					
<p>■ Oracle</p> <p>1. init.ora 설정 파일에 RESOURCE_LIMIT = TRUE' 라인 추가 #vi /Oracle_HomeDirectory/admin/pfile/init.ora</p> <p>또는</p> <p>SQL> show parameter resource_limit;</p> <p>2. SQL*Plus에서</p> <p>SQL> Alter System Set Resource_Limit=TRUE;</p>					
조치 시 영향	일반적으로 영향 없음				

1.4. 패치관리

1.4.1. 데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용

대상	Oracle, MSSQL, MySQL	위험도	상	code	D-21
취약점 개요	데이터베이스의 주요 보안 패치 등을 설치하지 않은 경우 공격자가 알려진 취약점을 이용하여 데이터베이스에 접근 가능함.				
보안대책					
판단기준	양호: 버전별 최신 패치를 적용한 경우				
	취약: 버전별 최신 패치를 적용하지 않은 경우				
조치방법	데이터베이스에 대한 버전을 확인 후 업그레이드 및 패치 적용				
보안설정방법					
<p>■ Oracle</p> <p>ORACLE_HOME에 설치된 Oracle 제품 컴포넌트를 조회하거나, 적용된 임시 패치를 조회할 때는 lsinventory 명령어를 사용함</p> <ul style="list-style-type: none"> Oracle 제공 패치 명령을 이용하여 확인함 <pre>\$opatchlsinventory[-all] [-detail] [-invPtrLoc] [-jre] [-oh]</pre> <p>all : ORACLE_BASE 밑에 설치된 모든ORACLE_HOME 정보를 표시 detail : 설치된 패치 내에 포함된 라이브러리 파일까지 표시하므로 패치 적용 시 충돌되는 객체 파일을 확인 가능함</p> <p>┆ Unix 시스템</p> <pre>\$ORACLE_HOME/OPatch/opatchlsinventory -detail</pre> <p>┆ Windows 시스템</p> <pre>%ORACLE_HOME%\WOPatch\opatchlsinventory -detail</pre> <p>http://metalink.oracle.com에서 최신 패치 버전 확인 후 opatch 명령을 통해 도출된 결과를 비교함</p> <ul style="list-style-type: none"> - 버전이 9.2.0, 10.2.0, or 10.1.0이 아니면 아주 취약함 - Oracle 10g Release 2의 patchset level이 10.2.0.1이나 이후 버전이 아니면 취약함 - Oracle 10g Release 1의 patchset level이 10.1.0.4이나 이후 버전이 아니면 취약함 - Oracle 9i Release 2의 patchset level이 9.2.0.6이나 이후 버전이 아니면 취약함 - Oracle 9.0이 Oracle 9iAS 또는 Oracle AS10g를 지원하기 위해 사용되면 취약함 					
데이터베이스 명			적용 패치		

Oracle 10g Release 2	10.2.0.5 Windows 64bit itanium
Oracle 10g Release 2	10.2.0.4 Windows, MAC OS X
Oracle 10g Release 2	10.2.0.1 All OS
Oracle 10g Release 1	10.2.0.1 All OS
Oracle 9i Release 2	9.2.0.8
Oracle 9i Release 1	9.0.1.4
Oracle 8i Release 3	8.1.7.4
Oracle 8i	8.0.6.3

※ 참고 사이트

<http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html>

■ MSSQL

Release	Sqlserver.exe
SQL Server 2000 SP 4	8.00.2283
SQL Server 2000 SP 3	8.00.1007
SQL Server 2000 SP 2	8.00.534
SQL Server 2000 SP 1	8.00.384
SQL Server 2000 RTM	8.00.194
SQL Server 2005 SP4 CU#3	9.00.5266
SQL Server 2005 SP3 CU#15	9.00.4325
SQL Server 2005 SP2 CU#17	9.00.3356
SQL Server 2005 SP1	9.00.2047
SQL Server 2005 RTM	9.00.1399
SQL Server 2008 R2 SP2 CU #3	10.50.4266.00
SQL Server 2008 R2 SP1 CU #9	10.50.2866.00
SQL Server 2008 R2 RTM CU #13	10.50.1815.00
SQL Server 2008 SP3 CU #8	10.00.5785.00
SQL Server 2008 SP2 CU #11	10.00.4333.00
SQL Server 2008 SP1 CU #16	10.00.2850.00
SQL Server 2008 RTM CU #10	10.00.1835.00
SQL Server 2012 SP1 + KB2765331	11.00.3321.00

※ 참고 사이트

<http://support.microsoft.com/kb/321185/en-us>

<http://www.sqlsecurity.com/FAQs/SQLServerVersionDatabase/tabid/63/Default.aspx>

■ MySQL

<Enterprise Release>

Version	Last Version
6.0	6.0.11
5.6	5.6.9
5.5	5.5.6
5.4	5.4.2
5.1	5.1.40
5.0	5.0.88
4.1	4.1.22

※ 참고 사이트

버그 패치된 릴리즈 사이트 <http://downloads.mysql.com/archives.php>

버그 현황 사이트 <http://bugs.mysql.com/bugstats.php>

조치 시 영향	적용 시 개발자 및 운영자와 협의 후 적용
----------------	-------------------------

1.4.2. 데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에' 적합하도록 설정

대상 OS	Oracle, MSSQL	위험도	상	code	D-22
취약점 개요	데이터베이스의 감사 기록이 기관에서 정의한 감사 기록 정책에 적합하도록 기록해야 함. 데이터베이스는 데이터, 로그와 응용프로그램에 대한 백업 정책을 수립해야 하며, 지속적으로 준수하지 않을 경우 데이터베이스에 문제 발생 시 이를 효과적으로 대처할 수 없음.				
보안대책					
판단기준	양호: DBMS의 감사 로그 저장 정책이 수립되어 있으며, 정책이 적용되어있는 경우				
	취약: DBMS에 대한 감사 로그 저장을 하지 않거나, 정책이 수립되어있지 않은 경우				
조치방법	DBMS에 대한 감사 로그 저장 정책 수립, 적용				

보안설정방법

■ Oracle

데이터베이스 감사 기록 정책 및 백업 정책 수립

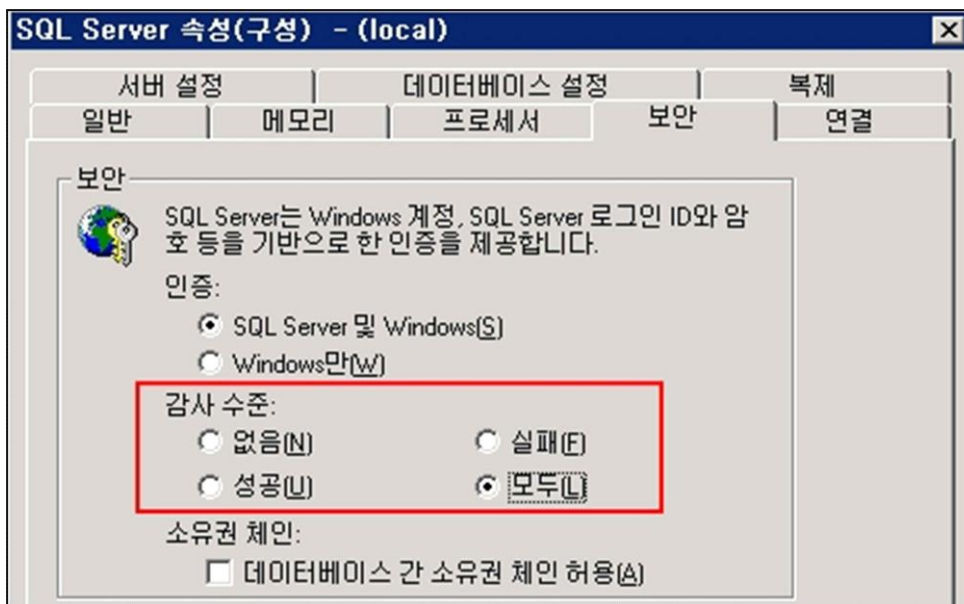
■ MSSQL

데이터베이스 감사 기록 정책 및 백업 정책 수립

Ⅰ MSSQL 2000

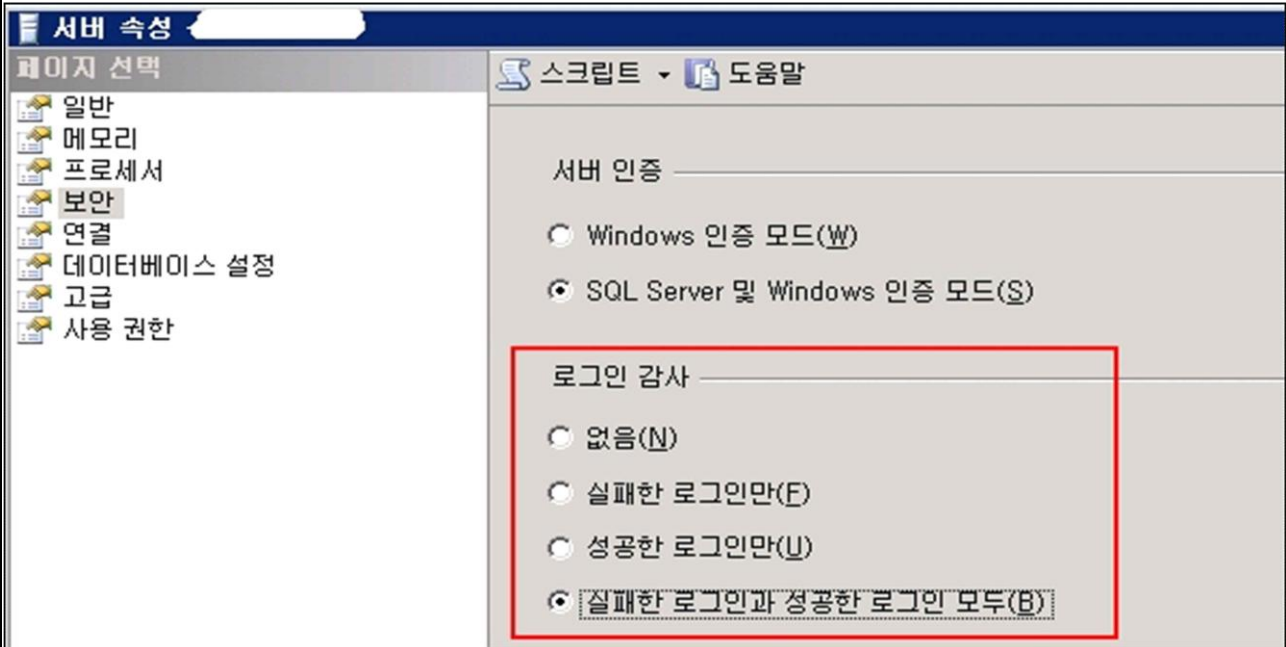
DB 접근에 대한 보안 감사를 할 수 있도록 보안 감사 설정

[SQL SERVER]> [등록정보]> [보안]탭> [감사수준]에서 '모두' 선택



Ⅰ MSSQL 2005

[MSSQL2005]> [오른쪽 마우스 클릭]> [속성]> [보안탭]> [로그인 감사] 옵션>
 '실패한 로그인과 성공한 로그인 모두' 선택



I MSSQL 2008 / 2012

[시스템 이름]> [오른쪽 마우스 클릭]> [속성]> [보안탭]> [로그인 감사] 옵션>
 '실패한 로그인과 성공한 로그인 모두' 선택

조치 시 영향	일반적으로 영향 없음
----------------	-------------

1.4.3. 보안에 취약하지 않은 버전의 데이터베이스를 사용하고 있는가?

대상 OS	Oracle	위험도	중	code	D-23
취약점 개요	벤더에서 보안 패치 등을 지원하지 않는 버전을 사용할 경우 공격자가 시스템 권한 획득 등을 수행할 수 있는 취약점이 존재함.				
보안대책					
판단기준	양호: Oracle 보안 패치가 지원되는 버전을 사용하는 경우				
	취약: Oracle 보안 패치가 지원되지 않는 버전을 사용하는 경우				
조치방법	Oracle 보안패치가 지원되는 버전으로 업데이트				
보안설정방법					
<p>■ Oracle</p> <p>1. 9.2 버전 또는 이전 버전에 대한 업그레이드 계획이 없으면 취약점이 존재함</p> <p>2. 버전 확인(SQL*Plus)</p> <p>SQL> select banner from v\$version where banner like 'Oracle%';</p>					
조치 시 영향	일반적으로 영향 없음				

1.5. 로그관리

1.5.1. Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정

대상	Oracle	위험도	하	code	D-24
취약점 개요	Audit Table은 반드시 SYS, SYSTEM과 같은 데이터베이스 관리자 계정에 속해 있어야 하며, 그렇지 않은 경우 인가되지 않은 사용자가 감사 데이터의 수정, 삭제 등의 수행이 가능함.				
보안대책					
판단기준	양호: Audit Table 접근 권한이 관리자 계정으로 설정한 경우				
	취약: Audit Table 접근 권한이 일반 계정으로 설정한 경우				
조치방법	Audit Table 접근 권한 관리자 계정으로 설정				
보안설정방법					
<p>■ Oracle</p> <p>1. 설정 확인(SQL*Plus)</p> <p>SQL> Select owner from dba_tables where table_name='AUD\$';</p> <p>SYS 또는 SYSTEM이 아닌 계정이 나올 경우 확인 후 권한 삭제</p> <p>2. Audit table에 접근할 권한이 없는 계정이 확인 될 경우 권한 삭제</p> <p>SQL> DROP USER <사용자명>;</p>					
조치 시 영향	일반적으로 영향 없음				