

## Linux 서버 취약점 분석·평가 항목

분류	점검항목	항목중요도	항목코드
계정 관리	root 계정 원격 접속 제한	상	L-01
	패스워드 복잡성 설정	상	L-02
파일 및 디렉토리 관리	파일 및 디렉토리 소유자 설정	상	L-03
	/etc/passwd 파일 소유자 및 권한 설정	상	L-04
	/etc/hosts 파일 소유자 및 권한 설정	상	L-05
	/etc/syslog.conf 파일 소유자 및 권한 설정	상	L-06
서비스 관리	cron 파일 소유자 및 권한 설정	상	L-07
	DNS 보안 버전 패치	상	L-08
	DNS Zone Transfer 설정	상	L-09
	웹 서비스 웹 프로세스 권한 제한	상	L-10
	웹 서비스 불필요한 파일 제거	상	L-11
로그 관리	로그의 정기적 검토 및 보고	상	L-12

L-01 (상)	1. 계정관리 > 1.1 root 계정 원격 접속 제한
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>시스템 정책에 root 계정의 원격 터미널 접속 차단 설정이 적용 되어 있는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>관리자 계정 탈취로 인한 시스템 장애를 방지하기 위해 외부 비인가자의 root 계정 접근 시도를 원천적으로 차단하기 위함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>LINUX(UBUNTU)</li> </ul>
판단기준	양호 : 원격 터미널 서비스를 사용하지 않거나 사용시 root 직접 접속을 차단한 경우
	취약 : 원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우
조치방법	원격 접속 시 root 계정으로 접속 할 수 없도록 설정파일 수정
점검 및 조치사례	
<p><b>[SSH 설정 파일 위치 및 점검 방법]</b></p> <pre># cat /etc/sshd_config PermitRootLogin no</pre> <p><b>[SSH 서비스 사용시]</b></p> <ol style="list-style-type: none"> <li>1) vim 편집기를 사용하여 “/etc/ssh/sshd_config” 파일에 진입</li> <li>2) #PermitRootLogin 주석 제거 후 PermitRootLogin No로 신규 삽입</li> </ol>	

L-02 (상)	1. 계정관리 > 1.2 패스워드 복잡성 설정	
취약점 개요		
점검내용	● 시스템 정책에 사용자 계정 패스워드 복잡성 관련 설정이 되어 있는지 점검	
점검목적	● 패스워드 복잡성 관련 정책이 설정되어 있는지 점검하여 비인가자의 공격(무작위 대입 공격, 사전 대입 공격 등)에 대비가 되어 있는지 확인하기 위함	
판단기준 및 조치방법		
대상	● LINUX(UBUNTU)	
판단기준	양호 : 패스워드 최소 길이 8자리 이상, 영문·숫자·특수문자 최소 입력 기능이 설정된 경우	
	취약 : 패스워드 최소 길이 8자리 이상, 영문·숫자·특수문자 최소 입력 기능이 설정된 경우	
조치방법	계정과 유사하지 않은 8자 이상의 영문, 숫자, 특수문자의 조합으로 암호 설정 및 패스워드 복잡성 옵션 설정	
점검 및 조치사례		

L-02 (상)	1. 계정관리 > 1.2 패스워드 복잡성 설정
<p><b>【비밀번호 복잡성 설정 파일 위치 및 점검 방법】</b>  <code>/etc/pam.d/common-password</code></p> <p><b>【비밀번호 복잡성 수정】</b></p> <ol style="list-style-type: none"> <li>1) vim 편집기를 사용하여 “<code>/etc/pam.d/common-password</code>” 파일에 진입</li> <li>2) 파일에서 <code>password requisite pam_pwquality.so</code> 줄을 찾음</li> <li>3) 줄뒤에 신규 <code>retry=3 minlen=8 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1</code> 로 삽입</li> </ol> <p><b>【각 변수에 대한 설명】</b></p> <p><code>retry</code> : 패스워드 재시도 횟수 제한  <code>minlen</code> : 패스워드의 최소 길이 제한  <code>lcredit</code> : 패스워드에 소문자의 최소 개수를 지정  <code>ucredit</code> : 패스워드에 대문자의 최소 개수를 지정  <code>dcredit</code> : 패스워드에 숫자의 최소 개수를 지정  <code>ocredit</code> : 패스워드에 특수 문자의 최소 개수를 지정</p>	

L-03 (상)	2. 파일 및 디렉터리 관리 > 2.1 파일 및 디렉터리 소유자 설정
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>• 소유자 불분명한 파일이나 디렉터리가 존재하는지 여부를 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>• 소유자가 존재하지 않는 파일 및 디렉터리를 삭제 및 관리하여 임의의 사용자가 해당 파일을 열람, 수정하는 행위를 사전에 차단하기 위함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>• LINUX(UBUNTU)</li> </ul>
판단기준	양호 : 소유자가 존재하지 않는 파일 및 디렉터리가 존재하지 않는 경우

	취약 : 소유자가 존재하지 않는 파일 및 디렉터리가 존재하는 경우
조치방법	소유자가 존재하지 않는 파일 및 디렉터리 삭제 또는, 소유자 변경
점검 및 조치사례	
<p>1) 소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 <b>rm</b> 명령으로 삭제</p> <ul style="list-style-type: none"> <li>- <b>rm &lt;file_name&gt;</b></li> <li>- <b>rm &lt;directory_name&gt;</b></li> </ul> <p>2) 필요한 경우 <b>chown</b> 명령으로 소유자 및 그룹 변경</p> <ul style="list-style-type: none"> <li>- <b>chown &lt;user_name&gt; &lt;file_name&gt;</b></li> </ul>	

L-04 (상)	2. 파일 및 디렉토리 관리 > 2.2 /etc/passwd 파일 소유자 및 권한 설정
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>• /etc/passwd 파일 권한 적절성 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>• /etc/passwd 파일의 임의적인 변경을 차단하기 위함을 통해 비인가자가 권한 상승하는 것을 막기 위함</li> </ul>

판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>LINUX(UBUNTU)</li> </ul>
판단기준	양호 : /etc/passwd 파일의 소유자가 root이고, 권한이 644 이하인 경우
	취약 : /etc/passwd 파일의 소유자가 root가 아니거나, 권한이 644 이하가 아닌 경우
조치방법	“/etc/passwd” 파일의 소유자 및 권한 변경(소유자 : root, 권한 : 644)
점검 및 조치사례	
<p><b>【설정 파일 위치 및 점검 방법】</b></p> <pre># ls -l /etc/passwd</pre> <p>rw-r—r—root &lt;passwd 파일&gt;</p> <p><b>【소유자 권한 변경】</b></p> <p>“/etc/passwd” 파일의 소유자 및 권한 변경(소유자 : root, 권한 : 644)</p> <pre>#chown root /etc/passwd</pre> <pre>#chmod 644 /etc/passwd</pre>	

L-05 (상)	2. 파일 및 디렉터리 관리 > 2.3 /etc/hosts 파일 소유자 및 권한 설정
취약점 개요	

점검내용	<ul style="list-style-type: none"> <li>• /etc/hosts 파일의 권한 적절성 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>• /etc/hosts 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의적인 파일 변조를 방지하기 위함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>• LINUX(UBUNTU)</li> </ul>
판단기준	양호 : /etc/hosts 파일의 소유자가 root이고, 권한이 600인 이하 경우
	취약 : /etc/hosts 파일의 소유자가 root가 아니거나, 권한이 600 이상인 경우
조치방법	“/etc/hosts” 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)
점검 및 조치사례	
<p><b>[hosts 설정 파일 위치 및 점검 방법]</b></p> <pre># ls -l /etc/hosts</pre> <pre>rw----- root &lt;hosts 파일&gt;</pre> <p><b>[hosts 파일 소유자 및 권한 변경]</b></p> <p>“/etc/hosts” 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)</p> <pre>#chown root /etc/hosts</pre> <pre>#chmod 600 /etc/hosts</pre>	

L-06 (상)	2. 파일 및 디렉터리 관리 > 2.4 /etc/syslog.conf파일소유자 및 권한 설정	
취약점 개요		
점검내용	• /etc/syslog.conf 파일 권한 적절성 검사	
점검목적	• /etc/syslog.conf 파일의 권한 적절성을 점검하여, 관리자 외 비인가자의 임의적인 syslog.conf 파일 변조를 방지 하기 위함	
판단기준 및 조치방법		
대상	• LINUX(UBUNTU)	
판단기준	양호 : /etc/syslog.conf 파일의 소유자가 root(또는 bin, sys)이고, 권한이 640 이하인 경우	
	취약 : /etc/syslog.conf 파일의 소유자가 root(또는 bin, sys)가 아니거나, 권한이 640이하가 아닌 경우	
조치방법	“/etc/syslog.conf” 파일의 소유자 및 권한 변경 (소유자 root(또는 bin, sys), 권한 644 이하)	
점검 및 조치사례		
<div>[syslog.conf설정 파일 위치 및 점검 방법]</div> <div># /etc/syslog.conf</div> <div>ls -l /etc/syslog.conf</div> <div>rw-r----- root &lt;syslog.conf 파일&gt;</div> <div>[syslog.conf 소유자 및 권한 변경]</div> <div>#chown root /etc/rsyslog.conf</div> <div>#chmod 644 /etc/rsyslog.conf</div>		



L-07 (상)	3. 서비스 관리 > 3.1 cron파일 소유자 및 권한 설정	
취약점 개요		
점검내용	● Cron 관련 파일의 권한 적절성 점검	
점검목적	● 관리자 외 cron 서비스를 사용할 수 없도록 설정하고 있는지 점검하는 것을 목적으로 함	
판단기준 및 조치방법		
대상	● LINUX(UBUNTU)	
판단기준	양호 : crontab 명령어 일반사용자 금지 및 cron 관련 파일 640 이하인 경우	
	취약 : crontab 명령어 일반사용자 사용가능 하거나, crond 관련 파일 640 이상인 경우	
조치방법	Crontab 명령어 750 이하, cron 관련 파일 소유자 및 권한 변경(소유자 root, 권한 640 이하)	
점검 및 조치사례		

**[Cron 설정 파일 위치 및 점검 방법]**

# /etc/crontab

# ls -al /usr/bin/crontab

rw-r----- root &lt;cron 접근제어 파일&gt;

**[Crontab 사용자 권한 부여]**

1) Crontab 명령어 일반사용자 권한 삭제

※ Crontab 명령어는 SUID가 설정되어 있으므로 SUID 설정 제거

# ls -l /usr/bin/crontab

# chmod 750 /usr/bin/crontab

2) Cron 관련 설정파일 소유자 및 권한 설정

# chown root &lt;cron 관련 파일&gt;

# chmod 640 &lt;cron 관련 파일&gt;

관련 설정파일	설명
< cron 디렉터리> /crontab	예약 작업을 등록하는 파일
/etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly, /etc/cron.monthly	시간, 일, 주, 월 단위 실행스크립트 등록

L-08 (상)	3. 서비스 관리 > 3.2 DNS 보안 버전 패치
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>BIND 최신버전 사용 유무 및 주기적 보안 패치 여부 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>취약점이 발표되지 않은 BIND 버전의 사용을 목적으로 함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>LINUX(UBUNTU)</li> </ul>
판단기준	양호 : DNS 서비스를 사용하지 않거나 주기적으로 패치를 관리하고 있는 경우

	취약 : DNS 서비스를 사용하며 주기적으로 패치를 관리하고 있지 않는 경우
조치방법	DNS 서비스를 사용하지 않을 경우 서비스 중지, 사용할 경우 패치 관리 정책을 수립하여 주기적으로 패치 적용
점검 및 조치사례	
<p><b>[BIND 설정 파일 위치 및 점검 방법]</b></p> <p># ps -ef   grep named(bind) Named -v or BIND -v</p> <p><b>[DNS 서비스 사용시]</b></p> <p>“DNS” 서비스를 사용하지 않은 경우 서비스 중지</p> <p><b>[DNS 서비스 사용시]</b></p> <p>“DNS” 서비스를 사용하는 경우 BIND 버전 확인 후 보안설정 방법에 따라 최신 버전으로 업데이트</p> <p>※ Bind 최신 버전 다운로드 : <code>sudo apt install bind 9*</code></p> <p>※ 버전에 대한 취약점 정보 사이트 : <a href="https://kb.isc.org/article/AA-00913/74/BIND-9-Security-Vulnerability-Matrix.html">https://kb.isc.org/article/AA-00913/74/BIND-9-Security-Vulnerability-Matrix.html</a></p>	

L-09 (상)	3. 서비스 관리 > 3.3 DNS Zone Transfer 설정
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>Secondary Name Server로만 Zone 정보 전송 제한 여부 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>허가되지 않는 사용자에게 Zone Transfer를 제한함으로써 호스트 정보, 시스템 정보 등 정보 유출의 방지를 목적으로 함</li> </ul>

판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>LINUX(UBUNTU)</li> </ul>
판단기준	양호 : DNS 서비스 미사용 또는, Zone Transfer를 허가된 사용자에게만 허용한 경우
	취약 : DNS 서비스를 사용하며 Zone Transfer를 모든 사용자에게 허용한 경우
조치방법	DNS 서비스를 사용하지 않을 경우 서비스 중지, 사용할 경우 DNS 설정을 통해 내부 Zone 파일을 임의의 외부 서버에서 전송 받지 못하게 하고, 아무나 쿼리 응답을 받을 수 없도록 수정
점검 및 조치사례	
<p><b>[DNS 설정 파일 위치 및 점검 방법]</b></p> <pre># ps -ef   grep named   grep -v "grep"</pre> <pre># cat /etc/named.conf</pre> <p><b>[Bind DNS named.conf 설정]</b></p> <p>Vim /etc/named.conf -&gt; options { allow-transfer (존 파일 전송을 허용하고자 하는 IP); };</p>	

L-10 (상)	3. 서비스 관리 > 3.4 웹서비스 웹 프로세스 권한 제한
취약점 개요	

점검내용	<ul style="list-style-type: none"> <li>• Apache 데몬이 root 권한으로 구동되는지 여부 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>• Apache 데몬을 root 권한으로 구동하지 않고 별도의 권한으로 구동함으로써 침해사고 발생 시 피해범위 확산 방지를 목적으로 함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>• LINUX(UBUNTU)</li> </ul>
판단기준	양호 : Apache 데몬이 root 권한으로 구동되지 않는 경우
	취약 : Apache 데몬이 root 권한으로 구동되지 경우
조치방법	Apache 데몬을 root 가 아닌 별도 계정으로 구동
점검 및 조치사례	
<p><b>[Apache 설정 파일 위치 및 점검 방법]</b></p> <pre># vim /[Apache_home]/conf/httpd.conf</pre> <p>User [root가 아닌 별도 계정명]</p> <p>Group [root가 아닌 별도 계정명]</p>	

L-11 (상)	3. 서비스 관리 > 3.5 웹 서비스 불필요한 파일 제거	
취약점 개요		
점검내용	● Apache 설치 시 기본으로 생성되는 불필요한 파일의 삭제 여부 점검	
점검목적	● Apache 설치 시 디폴트로 설치되는 불필요한 파일을 제거함을 목적으로 함	
판단기준 및 조치방법		
대상	● LINUX(UBUNTU)	
판단기준	양호 : 기본으로 생성되는 불필요한 파일 및 디렉터리가 제거되어 있는 경우	
	취약 : 기본으로 생성되는 불필요한 파일 및 디렉터리가 제거되지 않은 경우	
조치방법	불필요한 파일 및 디렉터리 제거	
점검 및 조치사례		
<p><b>[Apache설정 파일 위치 및 점검 방법]</b></p> <p>불필요한 파일 및 디렉토리 존재 여부 확인</p> <pre>#ls -ld /[Apache_home]/htdocs/manual</pre> <pre>#ls -ld /[Apache_home]/manual</pre> <p><b>[ls 명령어로 확인된 매뉴얼 디렉터리 및 파일 제거]</b></p> <pre>#rm -rf /[Apache_home]/htdocs/manual</pre> <pre>#rm -rf /[Apache_home]/manual</pre> <p><b>[ls 명령어로 확인된 매뉴얼 디렉터리 및 파일 제거 확인]</b></p> <pre>#ls -ld /[Apache_home]/htdocs/manual</pre> <pre>#ls -ld /[Apache_home]/manual</pre>		

L-12 (상)	4. 로그 관리 > 4.1 로그의 정기적 검토 및 보고	
취약점 개요		
점검내용	● 로그의 정기적 검토 및 보고 여부 점검	
점검목적	● 정기적인 로그 점검을 통해 안정적인 시스템 상태 유지 및 외부 공격 여부를 파악하기 위함	
판단기준 및 조치방법		
대상	● LINUX(UBUNTU)	
판단기준	양호 : 접속기록 등의 보안 로그, 응용 프로그램 및 시스템 로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지는 경우	
	취약 : 위 로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지지 않는 경우	
조치방법	로그 기록 검토 및 분석을 시행하여 리포트를 작성하고 정기적으로 보고함	
점검 및 조치사례		
<p><b>【로그 분석 설정 파일 위치 및 점검 방법】</b></p> <p># 로그 분석 계획 수립 여부 및 로그 분석 결과에 따른 점검</p> <p><b>【정기적인 로그 분석을 위한 절차 수립】</b></p> <p>1) 정기적인 로그 검토 및 분석 주기 수립</p> <p>2) 로그 분석에 대한 결과 보고서 작성</p> <p>3) 로그 분석 결과 보고서 보고 체계 수립</p>		

보안장비 취약점 분석·평가 항목
-------------------

분류	점검항목	항목중요도	항목코드
계정관리	보안장비 <b>Default</b> 계정 변경	상	S-01
	보안장비 <b>Default</b> 패스워드 변경	상	S-02
	보안장비 계정별 권한 설정	상	S-03
	보안장비 계정 관리	상	S-04
접근 관리	보안장비 원격 관리 접근 통제	상	S-05
	보안장비 보안 접속	상	S-06
로그 관리	보안장비 로그 설정	중	S-07
	보안장비 로그 정기적 검토	중	S-08
기능 관리	정책 관리	상	S-09
	NAT 설정	상	S-10
	DMZ 설정	상	S-11
	최소한의 서비스만 제공	상	S-12
	이상징후 탐지 모니터링 수행	상	S-13



S-01 (상)	1. 계정 관리 > 1.1 보안장비 Default 계정 변경	
취약점 개요		
점검내용	● 보안장비에 기본적으로 설정되어 있는 관리자 계정의 변경 여부 점검	
점검목적	● 보안장비의 기본 관리자 계정 패스워드는 인터넷이나 매뉴얼 등에 공개되어 있으므로 보안장비의 기본 관리자 계정을 변경하여 공격자가 기본 관리자 계정 정보를 통해 보안장비를 장악하지 못하게 하기 위함	
판단기준 및 조치방법		
대상	● 방화벽, IPS, VPN, IDS, WAF 등	
판단기준	양호 : 장비에서 제공하고 있는 디폴트 계정을 변경하여 사용하는 경우	
	취약 : 장비에서 제공하고 있는 디폴트 계정을 변경이 가능함에도 변경하지 않고 사용하는 경우	
조치방법	디폴트 계정 변경	
점검 및 조치사례		

## 【점검방법】

- 1) Web을 통한 접속
- 2) 디폴트 계정, 비밀번호 입력
- 3) 접속 확인

## 【조치방법】

- 1) 보안장비에서 제공하고 있는 계정 메뉴에서 **Default** 계정 변경
- 2) **Default** 계정 변경이 불가능할 경우 기본 패스워드 변경으로 보완 필요

S-02 (상)	1. 계정 관리 > 1.2 보안장비 <b>Default</b> 패스워드 변경
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>보안장비에 기본적으로 설정되어 있는 관리자 계정의 패스워드를 변경 없이 사용하고 있는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>보안장비의 기본 관리자 계정 패스워드는 인터넷이나 매뉴얼 등에 공개되어 있으므로 보안장비의 기본 관리자 계정 패스워드를 변경하여 공격자가 기본 관리자 계정 정보를 통해 보안장비를 장악하지 못하게 하기 위함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>방화벽, IPS, VPN, IDS, WAF 등</li> </ul>

판단기준	양호 : 장비 디폴트 패스워드 또는 유추 가능한 패스워드를 사용하지 않은 경우
	취약 : 장비 디폴트 패스워드 또는 유추 가능한 패스워드를 사용하는 경우
조치방법	디폴트 패스워드를 특수문자, 숫자, 영문 대소문자 포함하여 8자리 이상으로 변경
점검 및 조치사례	
<p><b>【점검방법】</b></p> <ol style="list-style-type: none"> <li>1) Web을 통한 접속</li> <li>2) 디폴트 계정, 비밀번호 입력</li> <li>3) 접속 확인</li> </ol> <p><b>【조치방법】</b></p> <ol style="list-style-type: none"> <li>1) 패스워드 메뉴에서 패스워드 변경</li> <li>2) 보안장비가 제공하는 범위에서 패스워드 설정(특수문자, 숫자, 영소문자 포함 8자리 이상)</li> </ol>	

S-03 (상)	1. 계정 관리 > 1.3 보안장비 계정 별 권한 설정
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>• 보안장비에 등록된 계정들에 대해 업무에 불필요한 권한 여부 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>• 보안장비 계정 별 권한 설정이 없을 경우, 권한 없는 사용자의 의도하지 않은 보안정책 수정이나 보안장비 설정 값 변경을 통하여 공격자에게 시스템 침입 경로를 제공할 수 있음</li> </ul>

판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>방화벽, IPS, VPN, IDS, WAF 등</li> </ul>
판단기준	양호 : 사용자별 계정의 용도 파악 및 적절한 권한을 부여하는 경우
	취약 : 사용자별 계정의 용도 파악 및 적절한 권한을 부여하지 않는 경우
조치방법	사용자별 계정의 용도 파악 및 적절한 권한 부여
점검 및 조치사례	
<p><b>【점검 방법】</b></p> <p>1) 보안장비에서 제공하고 있는 계정 메뉴에서 계정 별 권한 확인</p> <p><b>【조치 방법】</b></p> <p>1) 보안장비에서 제공하고 있는 계정 메뉴에서 기존 계정의 권한 검토(불필요한 권한 삭제)</p> <p>2) 단일 계정을 여러 사용자가 공유 시 사용자 별 계정 생성 및 권한 차등 부여</p>	

취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>보안장비에 등록되어 있는 계정 중 사용하지 않는 계정을 제거 또는 관리하고 있는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>사용하지 않는 불필요한 계정을 관리함으로써 관리되지 않은 계정을 통한 공격을 차단하기 위함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>방화벽, IPS, VPN, IDS, WAF 등</li> </ul>
판단기준	양호 : 불필요한 공용계정 및 휴면계정을 제거하거나 관리하는 경우
	취약 : 불필요한 공용계정 및 휴면계정을 제거하지 않고 관리하지 않는 경우
조치방법	불필요한 공용계정 및 휴면계정 제거
점검 및 조치사례	
<p><b>【점검 방법】</b></p> <p>1) 보안장비에서 제공하고 있는 계정 메뉴에서 계정 확인 및 담당자 인터뷰</p> <p><b>【조치 방법】</b></p> <p>1) 사용하지 않는 계정 삭제</p> <p>2) 공용계정 사용 시 사용자별 계정 생성 및 시스템 접근 이력을 관리하여 책임 추적성 확보</p>	

S-05 (상)	2. 접근 관리 > 2.1 보안장비 원격 관리 접근 통제	
취약점 개요		
점검내용	● 보안장비 원격 관리 시 관리자 IP 또는 특정 IP 만 접근이 가능하도록 설정하였는지 점검	
점검목적	● 보안장비에 원격으로 접근할 수 있는 IP를 등록함으로써 비인가자의 보안장비 접근을 차단하고 보안장비에 접근이 허용된 특정인들만 보안장비에 접근을 가능하도록 하기 위함	
판단기준 및 조치방법		
대상	● 방화벽, IPS, VPN, IDS, WAF 등	
판단기준	양호 : 원격 관리 시 관리자 IP 또는 특정 IP만 접근 가능하도록 설정한 경우	
	취약 : 원격 관리 시 관리자 IP 또는 특정 IP만 접근 가능하도록 설정하지 않은 경우	
조치방법	원격 관리 시 관리자 및 특정 IP만 접근 가능하도록 함	
점검 및 조치사례		
<b>[점검 방법]</b> 1) 보안장비에서 제공하고 있는 메뉴에서 접속 IP나 계정 제한 확인		
<b>[조치 방법]</b> 1) 관리자 IP 또는 특정 IP 및 계정에서만 접속할 수 있도록 설정		

S-06 (상)	2. 접근 관리 > 2.2 보안장비 보안 접속	
취약점 개요		
점검내용	● 보안장비에 접속할 때 암호화 프로토콜을 이용하여 접속하는지 여부를 점검	
점검목적	● 보안장비 접속 시 평문 전송하는 Telnet, HTTP 접속을 사용하지 않고 데이터가 암호화되는 SSH, SSL 인증 등의 암호화 접속을 통하여 공격자의 데이터 스니핑에 대비하기 위함	
판단기준 및 조치방법		
대상	● 방화벽, IPS, VPN, IDS, WAF 등	
판단기준	양호 : 보안장비 접속 시 암호화 통신을 하는 경우	
	취약 : 보안장비 접속 시 암호화 통신을 하지 않는 경우	
조치방법	보안장비 접속 시, 가능하다면 SSL 등의 암호화 접속 활용	
점검 및 조치사례		
<b>[점검 방법]</b> 1) HTTPS 또는 SSH 등 암호화 통신을 통한 접속 확인		
<b>[조치 방법]</b> 1) 보안장비 접속 시, SSL, HTTPS 등의 암호화 접속 활용		

S-07 (중)	3. 로그 관리 > 3.1 보안장비 로그 설정	
취약점 개요		
점검내용	● 보안장비에 로그 설정이 적용되어 있는지 확인하고 로그 정책이 기관 정책에 맞게 적용되어 있는지 점검	
점검목적	● 로그 설정을 점검하여 보안장비의 이상 유무와 보안장비 및 보안장비에 의해 보호받고 있는 정보시스템에 대한 비인가자의 침입 및 공격을 식별하고 있는지 확인하기 위함	
판단기준 및 조치방법		
대상	● 방화벽, IPS, VPN, IDS, WAF 등	
판단기준	양호 : 기관 정책에 따른 로그 설정이 되어있는 경우	
	취약 : 기관 정책에 따른 로그 설정이 되어있지 않은 경우	
조치방법	기관 정책에 따른 로깅 설정	
점검 및 조치사례		
<b>【점검 방법】</b> 1) 보안장비의 로그 설정 메뉴 확인		
<b>【조치 방법】</b> 1) 기관 정책에 따른 로깅 설정 (각 벤더 별 설정 방법이 상이함)		



S-08 (중)	3. 로그 관리 > 3.2 보안장비 로그 정기적 검토	
취약점 개요		
점검내용	● 로그 분석 도구(보안장비 로그 모니터링 기능, 로그 분석 프로그램 등)를 이용하여 보안장비 로그를 정기적으로 검토하는지 점검	
점검목적	● 정기적으로 로그 검토를 이행하는지 점검하여 보안장비의 이상 유무와 비인가자의 공격 및 침입을 식별하고 있는지 확인하기 위함	
판단기준 및 조치방법		
대상	● 방화벽, IPS, VPN, IDS, WAF 등	
판단기준	양호 : 로그 검토를 정기적으로 이행하는 경우	
	취약 : 로그 검토를 정기적으로 이행하지 않는 경우	
조치방법	보안장비 로그를 정기적으로 분석 및 검토 실시	
점검 및 조치사례		
<b>[점검 방법]</b> 1) 보안장비의 로그를 정기적으로 분석하고 검토하는지 확인(정기점검보고서, 검토보고서 등)		
<b>[조치 방법]</b> 1) 기관 정책에 따른 보안장비 로그 수집 설정 2) 로그 분석 도구를 사용하여 결과 생성 및 리포트 제공 (로그를 수집하여 수작업으로 분석하는 것은 시간과 인적으로 무리가 있으므로 자동 로그 분석 도구를 사용) 3) 보안장비 로그에 대해 정기적인 분석 및 검토 실시		

S-09 (상)	4. 기능 관리 > 4.1 정책 관리	
취약점 개요		
점검내용	● 보안장비 정책에 미사용 및 중복된 정책이 존재하는지 점검	
점검목적	● 주기적인 정책 검토를 통해 미사용 및 중복된 정책을 제거하여 향후 발생 가능한 보안 위협을 제거하고 보안장비의 고가용성을 유지하기 위함	
판단기준 및 조치방법		
대상	● 방화벽, IPS, VPN, IDS, WAF 등	
판단기준	양호 : 정책에 대한 주기적인 검사로 미사용 및 중복된 정책을 확인하여 제거하는 경우	
	취약 : 정책에 대한 주기적인 검사를 하지 않고 미사용 및 중복된 정책을 확인하여 제거하지 않은 경우	
조치방법	정책에 대한 주기적인 검사로 미사용 및 중복된 정책을 확인하여 제거	
점검 및 조치사례		
<b>[점검 방법]</b> 1) 정책에 대한 주기적인 검사로 미사용 & 중복된 정책 확인		
<b>[조치 방법]</b> 1) 보안장비 정책의 주기적인 검사 및 미사용 & 중복된 정책 제거 2) 정책 관리 방법 2-1. 보안장비 정책 입력 시 IP 대신 이름을 사용하도록 함 2-2. 공통 정책은 그룹으로 관리하도록 함 2-3. 사용빈도가 높은 정책은 정책 설정 시 상단에 위치하도록 함 2-4. 위 내용을 포함한 정책에 대해 주기적으로 점검하도록 함		

S-10 (상)	4. 기능 관리 > 4.2 NAT 설정	
취약점 개요		
점검내용	● 외부 공개 필요성이 없는 정보시스템에 NAT 설정 여부를 점검	
점검목적	● 외부 침입자가 내부 시스템을 공격하기 위해서는 내부 사설 IP를 알아야 하므로 NAT 설정을 통해 내부 네트워크를 보호할 수 있음	
판단기준 및 조치방법		
대상	● 방화벽, IPS, VPN, IDS, WAF 등	
판단기준	양호 : 외부 공개 필요성이 없는 서버, 단말기 등 정보시스템에 대해 NAT 설정을 적용한 경우	
	취약 : 외부 공개 필요성이 없는 서버, 단말기 등 정보시스템에 대해 NAT 설정을 적용하지 않은 경우	
조치방법	외부 공개 필요성이 없는 정보시스템에 대해 공인 IP 지정 여부를 확인하여 사설 IP로 변경한 후 보안장비에서 NAT 설정을 적용	
점검 및 조치사례		
<b>【점검 방법】</b> 1) 공인 IP 확인 사이트(포털 등)에 접속하여 사용 중인 단말의 IP 확인		
<b>【조치 방법】</b> 1) 대부분의 네트워크 보안 제품들은 NAT 기술을 기본으로 채택하고 있으므로 내부 사설 IP부여 정책에 맞춰 적용하도록 함		

S-11 (상)	4. 기능 관리 > 4.3 DMZ 설정
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>내부 네트워크와 외부 서비스 네트워크(DMZ)를 구분하고 있는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>외부 네트워크로 서비스를 제공하는 호스트에서 내부 네트워크로의 접근이 통제되고 있는지 확인하기 위함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>방화벽, IPS, VPN, IDS, WAF 등</li> </ul>
판단기준	양호 : DMZ를 구성하여 내부 네트워크를 보호하는 경우
	취약 : DMZ를 구성하지 않고 사설망에서 외부 공개 서비스를 제공하는 경우
조치방법	DMZ를 구성하여 내부 네트워크와 외부 서비스 네트워크 분리
점검 및 조치사례	
<p><b>[점검 방법]</b></p> <p>1) 네트워크 구성도 또는 방화벽 설정 확인</p> <p><b>[조치 방법]</b></p> <p>1) UTM 방화벽의 옵션 설정</p> <p>2) 이중 방화벽 사용</p> <p>DMZ는 두 개의 방화벽 중간에 위치하며, 두 개의 방화벽과 연결됨          하나의 방화벽은 내부 네트워크와 연결되고 다른 하나는 외부 네트워크와 연결됨          우연한 설정 실수를 통해 외부 네트워크가 내부 네트워크로 연결할 수 있게 되는 상황을 방지함          이런 구성 형식을 차단된 서브넷 방화벽이라고 함.</p>	

S-12 (상)	4. 기능 관리 > 4.4 최소한의 서비스만 제공	
취약점 개요		
점검내용	● 방화벽에서 필요한 서비스만 제공하고 있는지 점검	
점검목적	● 방화벽 정책을 검토하여 사용하지 않는 IP 와 Port를 제거하여 네트워크 및 시스템 운영의 보안성을 유지하기 위함	
판단기준 및 조치방법		
대상	● 방화벽, IPS, VPN, IDS, WAF 등	
판단기준	양호 : all deny 설정을 하고, 방화벽에 최소 서비스만 허용할 경우	
	취약 : all deny 설정이 되어있지 않거나, 방화벽에 불필요한 서비스를 허용할 경우	
조치방법	방화벽에 최소 서비스만 허용하도록 설정함	
점검 및 조치사례		
<div>【점검 방법】</div> <div>1) 방화벽에서 허용되지 않은 포트 접속 확인</div> <div>【조치 방법】</div> <div>1) 방화벽 기본 정책인 all deny에 최소 서비스만 허용 확인 (허용된 IP와 서비스 포트만 오픈, 모든 IP 및 서비스 허용 금지)</div>		

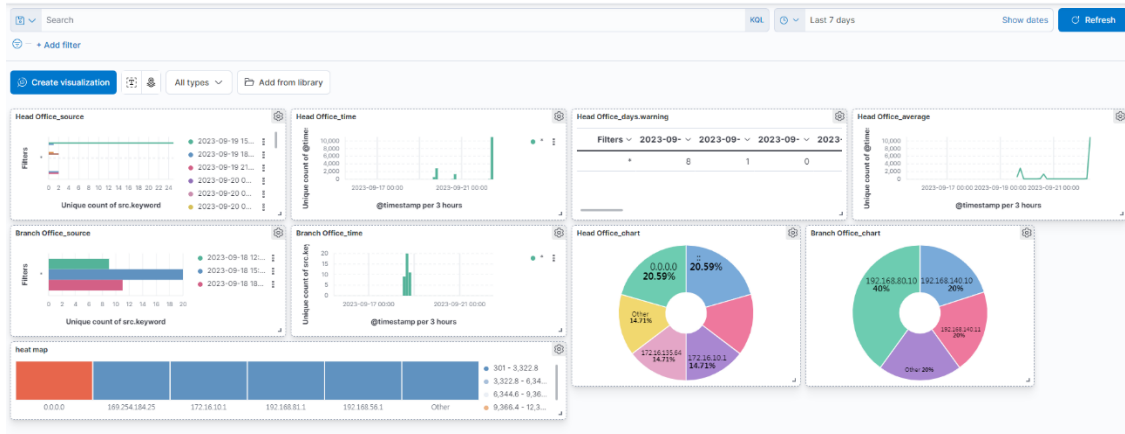
S-13 (상)	4. 기능 관리 > 4.5 이상징후 탐지 모니터링 수행	
취약점 개요		
점검내용	● 보안장비에 이상 징후 탐지 모니터링을 수행하고 있는지 점검	
점검목적	● 이상 징후가 탐지되는 경우 사고 예방 및 신속한 조치를 이행하기 위함	
판단기준 및 조치방법		
대상	● 방화벽, IPS, VPN, IDS, WAF 등	
판단기준	양호 : 이상징후 탐지 모니터링을 수행하고 있는 경우	
	취약 : 이상징후 탐지 모니터링을 수행하고 있지 않은 경우	
조치방법	이상징후 탐지 시 담당자/관리자가 즉시 확인할 수 있도록 모니터링 수행	
점검 및 조치사례		

## [점검 방법]

- 1) 보안장비의 이상 징후 탐지 모니터링 기능(알림, 이메일, SMS 등)이 설정되어 담당자가 즉시 인지할 수 있는 방안이 있는지 여부를 점검
- 2) 장비 자체 기능 대신 **syslog**를 통해 모니터링 시스템(ESM)으로 전송하는 경우, 해당 시스템의 모니터링 기능 설정 여부를 점검

## [조치 방법]

- 1) 보안장비 이상징후에 대해 실시간 모니터링 실시



- 2) 24시간 모니터링을 통한 검사가 여건상 어려울 경우 이메일이나 SMS를 통한 경고 기능 설정으로 대체

## 네트워크장비 취약점 분석·평가 항목

분류	점검항목	항목중요도	항목코드
계정 관리	패스워드 설정	상	N-01
	패스워드 복잡성 설정	상	N-02
	암호화된 패스워드 사용	상	N-03
접근 관리	로그온 시 경고 메시지 설정	중	N-04
	Session Timeout 설정	상	N-05
패치 관리	최신 보안 패치 및 벤더 권고사항 적용	상	N-06
기능 관리	TFTP 서비스 차단	상	N-07
	사용하지 않는 인터페이스의 Shutdown 설정	상	N-08
	웹 서비스 차단	중	N-09
	Bootp 서비스 차단	중	N-10
	Source 라우팅 차단	중	N-11
	ICMP unreachable, Redirect 차단	중	N-12
	Directed-broadcast 차단	중	N-13
	Domain lookup 차단	중	N-14



N-01 (상)	1. 계정 관리 > 1.1 패스워드 설정	
취약점 개요		
점검내용	● 관리 터미널(콘솔, SSH, https 등)을 통해 네트워크 장비 접근 시 기본 패스워드 (기본 관리자 계정도 함께 변경하도록 권고)를 사용하는지 점검	
점검목적	● 기본 패스워드를 변경 후 사용하는지 점검하여 기본 패스워드를 변경하지 않고 사용함으로써 발생할 수 있는 비인가자의 네트워크 장비 접근에 대한 통제가 이루어지는지 확인하기 위함	
판단기준 및 조치방법		
대상	● Cisco	
판단기준	양호 : 기본 패스워드를 변경한 경우	
	취약 : 기본 패스워드를 변경하지 않거나 패스워드를 설정하지 않은 경우	
조치방법	기본 패스워드를 관리기관의 패스워드 작성규칙을 준용하여 변경	
점검 및 조치사례		

**[네트워크 장비 별 점검 방법]****▶ Cisco IOS**

Router> enable

Router# show running-config

1. **enable** 패스워드 설정 확인
2. VTY, 콘솔 포트의 로그인 인증 방식 및 패스워드 설정 확인
  - login: 라인 패스워드 인증
  - login local: 로컬 사용자 인증
  - login authentication: AAA 인증

**[네트워크 장비 조치방법]****1) enable 패스워드 설정**

Router# config terminal

Router(config)# enable secret <패스워드>

or

Router(config)# enable password <패스워드>

Router(config)# end

**2) 가상터미널(VTY) 패스워드 설정**

Router# config terminal

Router(config)# line vty 0 4

Router(config-line)# login

Router(config-line)# password <패스워드>

**3) 콘솔 패스워드 설정**

Router# config terminal

Router(config)# line console 0

Router(config-line)# login

Router(config-line)# password <패스워드>

N-02 (상)	1. 계정 관리 > 1.2 패스워드 복잡성 설정
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>네트워크 장비에 기관 정책에 맞는 계정 패스워드 복잡성 정책이 적용되어 있는지 점검</li> <li>패스워드 복잡성 정책 설정 기능이 장비에 존재하지 않을 경우 기관 정책에 맞게 계정 패스워드를 설정하여 사용하는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>패스워드 복잡성 정책이 장비 정책에 적용되어 있는지 점검하여 비인가자의 네트워크 장비 터미널(콘솔, SSH, https 등) 접근 시도 공격(무작위 대입 공격, 사전 대입 공격 등)에 대한 대비 여부를 확인하기 위함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>공통</li> </ul>
판단기준	양호 : 기관 정책에 맞는 패스워드 복잡성 정책을 설정하거나 패스워드 복잡성 설정 기능이 없는 장비는 기관 정책에 맞게 패스워드를 사용하는 경우
	취약 : 기관 정책에 맞지 않는 패스워드를 설정하여 사용하는 경우
조치방법	관리기관의 패스워드 작성규칙에 맞게 패스워드 복잡성 정책 및 패스워드 설정
점검 및 조치사례	
<p><b>【네트워크 장비 별 점검 방법】</b></p> <p>▶ 공통</p> <p>장비에 패스워드 복잡성 정책을 설정하거나 패스워드 복잡성 설정 기능이 없는 장비는 기관 정책에 따라 패스워드를 설정하여 사용하는지 확인</p> <p><b>【네트워크 장비 별 조치 방법】</b></p> <p>▶ 공통</p> <p>주요정보통신기반시설 관리기관의 패스워드 작성규칙과 관련 법규를 준수하여 패스워드 복잡성 정책을 설정하고 안전한 패스워드를 사용</p> <p>▶Cisco IOS</p> <p>Router# config terminal</p> <p>Router(config)# security password min-length &lt;길이&gt;</p>	

N-03 (상)	1. 계정 관리 > 1.3 암호화 된 패스워드 사용	
취약점 개요		
점검내용	● 계정 패스워드 암호화 설정이 적용되어 있는지 점검	
점검목적	● 계정 패스워드 암호화 설정 유무를 점검하여 비인가자의 네트워크 장비 터미널 접근으로 인해 발생할 수 있는 장비 내 계정 패스워드 유출에 대비가 되어 있는지 확인하기 위함	
판단기준 및 조치방법		
대상	● Cisco	
판단기준	양호 : 패스워드 암호화 설정을 적용한 경우	
	취약 : 패스워드 암호화 설정을 적용하지 않은 경우	
조치방법	패스워드 암호화 설정 적용	
점검 및 조치사례		

**[네트워크 장비 별 점검 방법]****▶ Cisco IOS**

Router# show running-config

1. enable secret 사용 확인
2. username secret 사용 확인
3. Password-Encryption 서비스 동작 확인

**[네트워크 장비 별 조치 방법]****▶ Cisco IOS**

- 1) enable secret 설정

Router# config terminal

Router(config)# enable secret <패스워드>

- 2) username secret 설정

Router# config terminal

Router(config)# username <사용자이름> secret <패스워드>

- 3) Password-Encryption 서비스 설정

Router# config terminal

Router(config)# service password-encryption

Router(config)# end

Router# show running-config

```
enable secret 5 $1$SWqG$jwqu7ZrcVwuvEn9g.PsHo.
```

N-04 (중)	2. 접근 관리 > 2.1 로그인 시 경고 메시지 설정	
취약점 개요		
점검내용	● 터미널 접속 화면에 비인가자의 불법 접근에 대한 경고 메시지를 표시하도록 설정되어 있는지 점검	
점검목적	● 경고 메시지 표시 설정 적용 유무를 점검하여 비인가자에게 불법 적으로 터미널 접근 시 법적인 처벌에 대해 경각심을 가질 수 있게 하는지 확인하기 위함	
판단기준 및 조치방법		
대상	● Cisco	
판단기준	양호 : 로그인 시 접근에 대한 경고 메시지를 설정한 경우	
	취약 : 로그인 시 접근에 대한 경고 메시지를 설정하지 않거나 시스템 관련 정보가 노출되는 경우	
조치방법	네트워크 장비 접속 시 경고 메시지 설정	
점검 및 조치사례		
<p>[네트워크 장비 별 점검 방법]</p> <p>▶ Cisco IOS</p> <p>Router# show running-config -&gt; Banner 설정 내용 확인</p> <p>[네트워크 장비 별 조치 방법]</p> <p>▶ Cisco IOS</p> <p>Router# config terminal</p> <p>Router(config)# banner motd #</p> <pre>banner exec ^C During using equipment, privacy of individuals is not guaranteed. All access and usage is monitored and recorded and can be provided evidence as court or related organization. Use of this system constitutes consent to monitoring for these purposes. ^C</pre>		

N-05 (상)	2. 접근 관리 > 2.2 Session Timeout 설정
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>기관 정책에 맞게 Session Timeout 설정이 적용되어 있는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>Session Timeout 설정 유무를 점검하여 터미널 접속 후 일정 시간이 지난 뒤 터미널 세션이 자동으로 종료되어 관리자의 부재(터미널 작업 중 자리 비움, 작업 완료 후 터미널 접속을 종료하지 않음) 시 발생 가능한 비인가자의 터미널 접근 통제가 되는지 확인하기 위함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>공통</li> </ul>
판단기준	양호 : Session Timeout 시간을 기관 정책에 맞게 설정한 경우
	취약 : Session Timeout 시간을 기관 정책에 맞게 설정하지 않은 경우
조치방법	Session Timeout 설정 (5분 이하)
점검 및 조치사례	
<p><b>[네트워크 장비 별 점검 방법]</b></p> <p>▶ <b>Cisco IOS</b></p> <p>Router# show running-config</p> <p>각 Line Access의 exec-timeout 설정 확인</p> <p><b>[네트워크 장비 별 조치 방법]</b></p> <p>▶ <b>Cisco IOS</b></p> <p>1. Console</p> <p>Router# config terminal</p> <p>Router(config)# line console 0</p> <p>Router(config-line)# exec-timeout 5 0</p> <p>2. VTY</p> <p>Router# config terminal</p> <p>Router(config)# line vty 0 4</p> <p>Router(config-line)# exec-timeout 5 0</p>	

N-06 (상)	3. 패치 관리 > 3.1 최신 보안 패치 및 벤더 권고사항 적용	
취약점 개요		
점검내용	● 패치 적용 정책에 따라 주기적인 패치를 하고 있는지 점검	
점검목적	● 네트워크 장비의 보안 수준을 높이고 성능 및 기능 향상을 위해서 버전 업그레이드 및 보안 패치 작업을 수행해야 함	
판단기준 및 조치방법		
대상	● 공통	
판단기준	양호 : 주기적으로 보안 패치 및 벤더 권고사항을 적용하는 경우	
	취약 : 주기적으로 보안 패치 및 벤더 권고사항을 적용하지 않은 경우	
조치방법	장비 별 제공하는 최신 취약점 정보를 파악 후 최신 패치 및 업그레이드를 수행	
점검 및 조치사례		



## [네트워크 장비 별 점검 방법]

## ▶ Cisco IOS

Router# show version -> 버전정보 확인

## [네트워크 장비 별 조치 방법]

## ▶ 공통

주기적으로 보안 패치 및 벤더 권고사항을 검토하여 적용

## 1) 패치 식별

- 각 네트워크 장비의 하드웨어, 소프트웨어, EOL, 패치 적용 현황을 문서화하여 관리
- 운영 중인 네트워크 장비의 보안 패치 및 벤더 권고사항을 입수

## 2) 패치 분석

- 취약점의 영향도와 발생가능성을 분석하여 패치 적용 여부와 우선순위를 결정
- 패치 없이 네트워크 장비 설정 변경 등으로 해결이 가능한 경우 대체 조치를 수행

## 3) 패치 테스트

- 테스트베드 또는 시뮬레이션에서 운영환경(GNS3)과 최대한 유사하게 테스트 환경 구축
- 패치가 식별한 문제를 해결하고 정상 동작하는지 체크리스트를 구성하여 검증

## 4) 패치 적용

- 패치 적용 전에 네트워크 장비의 이미지와 설정을 백업하여 복구지점을 생서
- 예비장비를 보유한 경우 운영장비 설정과 패치를 예비장비에 적용한 후 운영장비와 교체하고 운영장비는 비상상황에 대비하여 일정기간 유지
- 패치 적용 후 모든 인터페이스와 중요 호스트로의 통신이 정상 동작하는지 확인

N-07 (상)	4. 기능 관리 > 4.1 TFTP 서비스 차단
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>네트워크 장비 서비스 중 불필요한 TFTP 서비스가 구동되어 있거나 TFTP 서비스 사용 시 ACL을 적용하여 허용된 시스템에서만 TFTP 서비스를 사용하도록 설정되어 있는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>인증 기능이 없는 TFTP 단점을 보완하기 위해 사용이 허용된 시스템만 TFTP를 통해 악성 코드가 삽입된 파일을 올려 사용자에게 배포할 수 있고, 네트워크 설정 파일이나 중요한 내부 정보를 유추할 수 있음</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>공통</li> </ul>
판단기준	양호 : TFTP 서비스를 차단한 경우
	취약 : 네트워크 장비의 TFTP 서비스를 차단하지 않은 경우
조치방법	네트워크 장비의 불필요한 TFTP 서비스를 비활성화 설정
점검 및 조치사례	
<p><b>[네트워크 장비 별 점검 방법]</b></p> <p>▶ <b>Cisco IOS</b></p> <p>Router# show running-config -&gt; TFTP 설정 정보 확인</p> <p><b>[네트워크 장비 별 조치 방법]</b></p> <p>▶ <b>Cisco IOS</b></p> <p>Router# config terminal</p> <p>Router(config)# no service tftp</p>	

N-08 (상)	4. 기능 관리 > 4.2 사용하지 않는 인터페이스의 Shutdown 설정	
취약점 개요		
점검내용	● 사용하지 않는 인터페이스가 비활성화 상태인지 점검	
점검목적	● 필요한 인터페이스만 활성화하여 비인가자가 사용하지 않는 인터페이스를 통하여 네트워크에 접근하는 것을 차단하기 위함	
판단기준 및 조치방법		
대상	● 공통	
판단기준	양호 : 사용하지 않는 인터페이스를 비활성화한 경우	
	취약 : 사용하지 않는 인터페이스를 비활성화하지 않은 경우	
조치방법	네트워크 장비에서 사용하지 않는 모든 인터페이스를 비활성화 설정	
점검 및 조치사례		
<p>[네트워크 장비 별 점검 방법]</p> <p>▶ Cisco IOS</p> <p>Router# show interface -&gt; 비활성화한 인터페이스는 Administratively down으로 표시</p> <p>[네트워크 장비 별 조치 방법]</p> <p>▶ Cisco IOS</p> <p>Router# config terminal</p> <p>Router(config)# interface &lt;인터페이스&gt;</p> <p>Router(config-line)# shutdown</p>		

N-09 (중)	4. 기능 관리 > 4.3 웹 서비스 차단	
취약점 개요		
점검내용	● 네트워크 장비의 웹 서비스를 비활성화하거나 특정 IP 주소만 접근을 허용하는지 점검	
점검목적	● 허용된 IP 만 웹 관리자 페이지에 접속할 수 있도록 설정하는지 점검하여 비인가자가 웹 관리자 페이지를 공격하여 네트워크 장비를 장악하지 못하도록 하기 위함	
판단기준 및 조치방법		
대상	● 공통	
판단기준	양호 : 불필요한 웹 서비스를 차단하거나 허용된 IP에서만 웹서비스 관리 페이지에 접속이 가능한 경우	
	취약 : 불필요한 웹 서비스를 차단하지 않은 경우	
조치방법	HTTP 서비스 차단 또는 HTTP 서버를 관리하는 관리자 접속 IP 설정	
점검 및 조치사례		
<p>[네트워크 장비 별 점검 방법]</p> <p>▶ Cisco IOS</p> <p>Router# show running-config -&gt; 웹 서비스 설정 확인</p> <p>[네트워크 장비 별 조치 방법]</p> <p>▶Cisco IOS</p> <p>Router# config terminal</p> <p>Router(config)# no ip http server</p> <p>Router(config)# no ip http secure-server</p> <p>Router(config)# ip http active-session-modules exclude_webexec</p> <p>Router(config)# ip http secure-active-session-modules exclude_webexec</p> <p>Router(config)# end</p>		

N-10 (중)	4. 기능 관리 > 4.4 Bootp 서비스 차단
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>• Bootp 서비스의 차단 여부 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>• 서비스 제거를 통해 비인가자에게 OS 정보가 노출되는 것을 차단함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>• 공통</li> </ul>
판단기준	양호 : Bootp 서비스가 제한되어 있는 경우
	취약 : Bootp 서비스가 제한되어 있지 않은 경우
조치방법	각 장비별 Bootp 서비스 제한 설정
점검 및 조치사례	
<p>[네트워크 장비 별 점검 방법]</p> <p>▶ Cisco IOS</p> <p>Router# show running-config -&gt; ip bootp server 설정 확인</p> <p>[네트워크 장비 별 조치 방법]</p> <p>▶Cisco IOS</p> <p>라우터를 자동리부팅 하는 취약점이 존재하므로 서비스를 차단하여 방어하기를 권고함 Bootp 차단 설정</p> <p>Router# config terminal</p> <p>Router(config)# no ip bootp server</p>	

N-11(중)	4. 기능 관리 > 4.5 Source 라우팅 차단
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>source routing을 차단하는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>인터페이스마다 no ip source-route를 적용하여 ip spoofing을 차단함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>공통</li> </ul>
판단기준	양호 : ip source route를 차단하는 경우
	취약 : ip source route를 차단하지 않는 경우
조치방법	각 인터페이스에서 ip source route 차단 설정
점검 및 조치사례	
<p><b>[네트워크 장비 별 점검 방법]</b></p> <p>▶ <b>Cisco IOS</b></p> <p>Router# show running-config -&gt; 각 인터페이스에서 no ip source-route 설정 확인</p> <p><b>[네트워크 장비 별 조치 방법]</b></p> <p>▶ <b>Cisco IOS</b></p> <p>글로벌 Configuration 모드에서 no ip source-route 명령어를 실행하여 비활성화</p> <p>Router# config terminal</p> <p>Router(config)# no ip source-route</p>	

N-12(중)	4. 기능 관리 > 4.6 ICMP unreachable, Redirect 차단	
취약점 개요		
점검내용	● ICMP unreachable, ICMP redirect를 차단하는지 점검	
점검목적	● ICMP unreachable 차단으로 DoS 공격을 차단하고 공격자가 네트워크 스캔시 소요되는 시간을 길어지게 하여 스캔 공격을 지연 및 차단함 ● ICMP redirect 차단으로 라우팅 테이블이 변경되는 것을 차단하기 위함	
판단기준 및 조치방법		
대상	● 공통	
판단기준	양호 : ICMP unreachable, ICMP Redirect를 차단하는 경우	
	취약 : ICMP unreachable, ICMP Redirect를 차단하지 않는 경우	
조치방법	각 인터페이스에서 ICMP Unreachables, ICMP Redirects 비활성화	
점검 및 조치사례		
[네트워크 장비 별 점검 방법]		
▶ Cisco IOS		
Router# enable		
Router# show running-config -> 각 인터페이스에서 no ip unreachable과 no ip redirects 설정을 확인		
[네트워크 장비 별 조치 방법]		
▶Cisco IOS		
Interface Configuration 모드에서 no ip unreachable과 no ip redirects 명령어를 실행		
Router# config terminal		
Router(config)# interface <인터페이스 넘버>		
Router(config-if)# no ip unreachablees		
Router(config-if)# no ip redirects		
Router(config-if)# end		

N-13(중)	4. 기능 관리 > 4.7 Directed-broadcast 차단
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>Directed-broadcast를 차단하는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>Directed-broadcast 서비스 차단을 통해 DoS 공격을 방지하기 위함</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>공통</li> </ul>
판단기준	양호 : Directed-broadcasts를 차단하는 경우
	취약 : Directed-broadcasts를 차단하지 않은 경우
조치방법	각 장치별로 Directed-broadcasts 제한 설정
점검 및 조치사례	
<p>[네트워크 장비 별 점검 방법]</p> <p>▶ Cisco IOS</p> <p>Router# show running-config -&gt; Directed-broadcast 설정 확인</p> <p>[네트워크 장비 별 조치 방법]</p> <p>▶Cisco IOS</p> <p>Router# config terminal</p> <p>Router(config)# interface &lt;인터페이스 번호&gt;</p> <p>Router(config-if)# no ip directed-broadcast</p>	



N-14(중)	4. 기능 관리 > 4.8 Domain lookup 차단
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>Domain Lookup을 차단하는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>명령어를 잘못 입력할 때 발생하는 불필요한 Domain Lookup 차단</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>공통</li> </ul>
판단기준	양호 : Domain Lookup을 차단하는 경우
	취약 : Domain Lookup을 차단하지 않은 경우
조치방법	Domain Lookup 비활성화
점검 및 조치사례	
<p>[네트워크 장비 별 점검 방법]</p> <p>▶ Cisco IOS</p> <p>Router# show running-config -&gt; no ip domain-lookup 설정 확인</p> <p>[네트워크 장비 별 조치 방법]</p> <p>▶Cisco IOS</p> <p>Router# config terminal</p> <p>Router(config)# no ip domain lookup</p>	

PC 취약점 분석·평가 항목

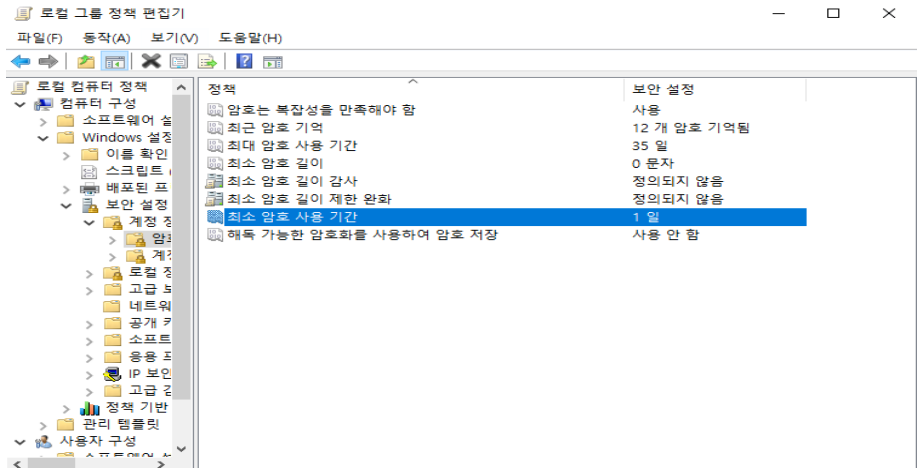
분류	점검항목	중요도	항목코드
계정 관리	패스워드의 주기적 변경	상	PC-01
	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	상	PC-02
서비스 관리	불필요한 서비스 제거	상	PC-03
패치 관리	HOT FIX 등 최신 보안패치 적용	상	PC-04
	최신 서비스팩 적용	상	PC-05
보안 관리	바이러스 백신 프로그램 설치 및 주기적 업데이트	상	PC-06
	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상	PC-07
	OS에서 제공하는 침입차단 기능 활성화	상	PC-08
	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상	PC-09

PC-01(상 )	1. 계정 관리 > 1.1 패스워드의 주기적 변경	
취약점 개요		
점검내용	● 최대 암호 사용 기간이 “35일” 이하로 설정되어 있는지 점검	
점검목적	● 패스워드를 주기적으로 변경하여 암호 크래킹의 가능성을 낮추고, 불법으로 획득한 암호의 무단 사용을 방지하고자 함	
판단기준 및 조치방법		
대상	● Windows	
판단기준	양호 : 최대 암호 사용 기간이 “35일”이하로 설정되어 있는 경우	
	취약 : 암호 사용 기간이 “제한없음”이거나 “35일”을 초과하여 설정되어 있는 경우	
조치방법	최대 암호 사용 기간 “35일” 설정 최소 암호 사용 기간 “1일” 설정 최근 암호 기억 설정 (권장 : 12개 암호 기억)	
점검 및 조치사례		


[OS 점검 및 조치 방법]

▶ Window XP, Window 7, Window 10

- 1) 윈도우+영문자R 키 입력 -> 실행 -> "lusrmgr.msc" 입력 -> 사용자 -> Administrator 우클릭 -> 속성 -> "암호 사용 기간 제한 없음", "계정 사용 안함 체크 해제"
- 2) 윈도우+영문자R 키 입력 -> 실행 -> "gpedit.msc" 입력 -> 컴퓨터 구성 -> Windows 설정 -> 보안 설정 -> 계정 정책 -> 암호 설정



PC-02(상 )	1. 계정 관리 > 1.2 패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	
취약점 개요		
점검내용	● 패스워드 설정 정책이 복잡성을 만족하는지 점검	
점검목적	● 안전한 패스워드를 사용함으로써 무작위 대입 공격, 사전공격 등 패스워드 탈취 목적의 공격에 대한 대비를 목적으로 함	
판단기준 및 조치방법		
대상	● Windows	
판단기준	양호 : 복잡성을 만족하는 패스워드 정책이 설정되어 있는 경우	
	취약 : 암호를 사용하지 않거나, 추측하기 쉬운 문자조합으로 이루어진 짧은 자릿수의 패스워드를 사용하는 경우	
조치방법	최소 암호 길이를 해당 기관의 보안 정책에 적합하게 설정	

점검 및 조치사례	
<p><b>[OS 점검 및 조치 방법]</b></p> <p>▶ <b>Window XP, Window 7, Window 10</b></p> <p>&lt; 비밀번호 설정 기준 &gt;</p> <ul style="list-style-type: none"> <li>- 영문, 숫자, 특수문자를 조합하여 계정명과 상이한 <b>8자 이상</b>의 패스워드 설정</li> </ul> <p>※ 다음 각 항목의 문자 종류 중 <b>2종류 이상</b>을 조합하여 <b>최소 10자리 이상</b> 또는, <b>3종류 이상</b>을 조합하여 <b>최소 8자리 이상</b>의 길이로 구성</p> <p>가. 영문 대문자(13개)</p> <p>나. 영문 소문자(13개)</p> <p>다. 숫자(10개)</p> <p>라. 특수문자(18개)</p> <p>1) 윈도우+영문자R 키 입력 -&gt; 실행 -&gt; “gpedit.msc” 입력 -&gt; 컴퓨터 구성 -&gt; Windows 설정 -&gt; 보안 설정 -&gt; 계정 정책 -&gt; 암호 설정</p> <div> <p>로컬 보안 설정    설명</p>  <p>암호는 복잡성을 만족해야 함</p> <p><input checked="" type="radio"/> 사용(E)</p> <p><input type="radio"/> 사용 안 함(S)</p> </div>	

PC-03(상 )	2. 서비스 관리 > 2.1 불필요한 서비스 제거	
취약점 개요		
점검내용	● 사용하지 않는 서비스나 디폴트로 설치되어 실행되고 있는 서비스가 있는지 점검	
점검목적	● 사용하지 않는 서비스나 디폴트로 설치된 서비스들을 제거하여 시스템 자원의 낭비를 막고 해당 서비스 포트를 통한 침입을 방지	
판단기준 및 조치방법		
대상	● Windows	
판단기준	양호 : 일반적으로 불필요한 서비스가 중지되어 있는 경우	
	취약 : 일반적으로 불필요한 서비스가 구동 중인 경우	

조치방법	불필요한 서비스 중지
점검 및 조치사례	
<b>[OS 점검 및 조치 방법]</b> <b>▶ Window XP, Window 7, Window 10</b> 1) 시작 -> 실행 -> “services.msc” 입력 -> 해당 서비스 선택 -> 속성 2) 불필요한 서비스 -> 중지 /시작 유형 -> 사용 안 함 3) 각 서비스 마다 옵션을 아래와 같이 선택할 수 있음	
서비스 시작 유형	설 명
사용 안 함	설치되어 있으나 실행되지 않음
수동	다른 서비스나 응용 프로그램에서 해당 기능을 필요로 할 때만 시작됨
자동	부팅 시에 해당 장치 드라이버가 로드된 후에 운영체제에 의해 시작됨

PC-04(상)	3. 패치 관리 > 3.1 HOT FIX 등 최신 보안패치 적용
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>시스템에 관련한 공개된 취약점에 대한 최신 보안패치를 적용하였는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>HOT Fix 및 최신 보안패치 적용을 시키지 않을 경우, 이미 공개된 취약점을 통하여 비인가자의 시스템 접근 및 관리자 권한 획득이 가능해짐</li> </ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>Windows</li> </ul>
판단기준	양호 : HOT Fix 설치 및 자동 업데이트 설정이 되어 있고 내부적으로 관리 절차를 수립하여 이행하고 있는 경우
	취약 : HOT Fix가 설치되어 있지 않거나 내부적으로 관리 절차가 수립되어 있지 않은 경우

조치방법	Windows Update 사이트에 접속하여 최신 패치 존재 여부 확인 및 패치 적용
점검 및 조치사례	
<p><b>[OS 점검 및 조치 방법]</b></p> <p>▶ <b>Window 7, Window 10</b></p> <ol style="list-style-type: none"><li>1) 인터넷에 연결되는 경우 Windows Update 사이트에 접속하여 최신 패치 존재 여부 확인</li><li>2) 제어판 -&gt; Windows Update -&gt; “업데이트 확인”, “설정 변경”, “업데이트 기록 보기”를 통하여 HOT Fix, 최신 보안 업데이트 등의 설치 여부 확인 및 설정 변경</li><li>3) 업데이트 확인 후 미설치 된 HOT FIX, 최신 보안 업데이트 등의 설치</li></ol>	

PC-05(상)	3. 패치 관리 > 3.2 최신 서비스팩 적용
취약점 개요	
점검내용	<ul style="list-style-type: none"><li>● 시스템에 최신 서비스팩이 적용되어 있는지 점검</li></ul>
점검목적	<ul style="list-style-type: none"><li>● 최신 서비스팩이 적용되어 있는지 점검하여 시스템 취약점을 이용한 공격에 대비가 되어 있는지 확인하기 위함</li></ul>

판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>Windows</li> </ul>
판단기준	양호 : 최신 서비스팩이 적용 되어 있고 내부적으로 관리 절차를 수립하여 이행하고 있는 경우
	취약 : 최신 서비스팩이 적용 되어 있고 내부적으로 관리 절차를 수립하여 이행하고 있지 않은 경우
조치방법	Windows Update 사이트에 접속하여 최신 서비스팩 여부 확인 및 적용
점검 및 조치사례	
<p><b>[OS 점검 및 조치 방법]</b></p> <p>▶ <b>Window 7</b></p> <ol style="list-style-type: none"> <li>1) 현재 시스템에 설치되어 있는 서비스팩 확인 실행 -&gt; “winver” 입력 -&gt; Windows 정보 확인</li> <li>2) 서비스팩 확인 후 최신 버전이 아닐 경우 다운로드하여 설치</li> </ol> <p>▶ <b>Window 10</b></p> <ul style="list-style-type: none"> <li>- 서비스팩이 아닌 윈도우 업데이트를 통해 진행하며 HOT FIX 패치를 통해 업데이트</li> </ul> <p>※ 웜(Worm), 랜섬웨어(Ransomware) 등의 위협을 피하기 위해 네트워크를 물리적으로 단절한 후 서비스팩 설치 및 업데이트 진행을 권장함</p>	

PC-06(상)	4. 보안 관리 > 4.1 바이러스 백신 프로그램 설치 및 주기적 업데이트
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>시스템에 백신이 설치되어 있는지 점검</li> <li>설치된 백신이 주기적으로 자동 업데이트되도록 설정되어 있는지 백신의 환경 설정 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>시스템의 백신 설치 여부와 설치된 백신이 주기적으로 업데이트가 되는지 점검하여 악성코드(바이러스, 웜, 랜섬웨어, 스파이웨어 등) 감염에 대한 대비를 하고 있는지 확인하기 위함</li> </ul>



판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>Windows</li> </ul>
판단기준	양호 : 백신이 설치되어 있고, 최신 업데이트가 적용 되어 있는 경우
	취약 : 백신이 설치되어 있지 않거나, 최신 업데이트가 적용 되어 있지 않은 경우
조치방법	바이러스 백신 설치 및 최신 업데이트 적용
점검 및 조치사례	
<p><b>[OS 점검 및 조치 방법]</b></p> <p>▶ <b>Window 7</b></p> <ol style="list-style-type: none"> <li>1) V3 Internet security 8.0 설치 여부 및 업데이트 설정 확인</li> <li>2) V3 Internet security 8.0 업데이트 적용</li> </ol> <p>▶ <b>Window 10 (Windows Defender 사용 예시)</b></p> <ol style="list-style-type: none"> <li>1) 오른쪽 하단 아이콘 모음 -&gt; Windows Defender 오른쪽 클릭 -&gt; 보호 업데이트 확인</li> <li>2) 업데이트 확인 후 업데이트 실행</li> </ol>	

PC-07(상)	4. 보안 관리 > 4.2 바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>시스템에 설치된 백신 프로그램의 환경 설정에 실시간 감시 기능이 적용되어 있는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>사용자가 인터넷을 통해 파일을 다운로드하거나 다운로드 받은 파일을 실행할 경우 백신 프로그램이 악성코드 감염을 실시간으로 점검하고 있는지 확인하기 위함</li> </ul>

판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>Windows</li> </ul>
판단기준	양호 : 설치된 백신의 실시간 감시 기능이 활성화 되어 있는 경우
	취약 : 백신이 설치되어 있지 않거나, 실시간 감시 기능이 비활성화 되어 있는 경우
조치방법	백신을 설치하고 실시간 감시 기능을 활성화함
점검 및 조치사례	
<p><b>[OS 점검 및 조치 방법]</b></p> <p>▶ <b>Window 7</b></p> <p>1) 백신의 실시간 검사 기능 활성화</p> <p>▶ <b>Window 10(Windows Defender 사용 예시)</b></p> <p>1) 시작키 -&gt; '바이러스 및 위협 방지' 선택</p> <p>2) 시작키 -&gt; '바이러스 및 위협 방지' 설정에서 켜기</p>	

PC-08(상)	4. 보안 관리 > 4.3 OS에서 제공하는 침입차단 기능 활성화
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>시스템의 방화벽 기능이 활성화 되어 있는지 점검</li> </ul>
점검목적	<ul style="list-style-type: none"> <li>방화벽 기능 활성화 여부를 점검하여 시스템에서 외부망의 비인가 접근 및 외부망으로 통신을 시도하는 프로그램에 대해 통제하고 있는지 확인하기 위함</li> </ul>
판단기준 및 조치방법	

대상	<ul style="list-style-type: none"> <li>Windows</li> </ul>						
판단기준	양호 : Windows 방화벽 “사용”으로 설정되어 있는 경우 또는 유·무료 기타 방화벽을 사용하고 있는 경우						
	취약 : Windows 방화벽 “사용 안 함”으로 설정되어 있는 경우 또는 유·무료 기타 방화벽을 사용하고 있지 않은 경우						
조치방법	Windows 방화벽 “사용”으로 설정 또는 유·무료 기타 방화벽을 사용						
점검 및 조치사례							
<p><b>[OS 점검 및 조치 방법]</b></p> <p>▶ 제어판을 통해서 설정하는 방법</p> <ol style="list-style-type: none"> <li>시작 -&gt; 실행 -&gt; “firewall.cpl” 입력</li> <li>Windows 방화벽 “사용” 설정</li> </ol> <p>▶ 레지스트리 값으로 설정하는 방법</p> <ol style="list-style-type: none"> <li>시작 -&gt; 실행 -&gt; “regedit” 입력</li> <li>레지스트리 경로로 이동</li> <li>설정값 입력</li> </ol>							
<table border="1"> <tr> <td>Value name</td><td>EnableFirewall</td></tr> <tr> <td>Data Type</td><td>DWORD 값</td></tr> <tr> <td>Value</td><td>1</td></tr> </table>		Value name	EnableFirewall	Data Type	DWORD 값	Value	1
Value name	EnableFirewall						
Data Type	DWORD 값						
Value	1						

PC-09(상)	4. 보안 관리 > 4.4 화면 보호기 대기 시간을 5분으로 설정 및 재시작 시 암호로 보호되게 설정
취약점 개요	
점검내용	<ul style="list-style-type: none"> <li>화면보호기 대기 시간 및 화면보호기 재시작 시 암호 설정 여부 점검</li> </ul>
	<ul style="list-style-type: none"> <li>사용자가 일정 시간 동안 아무런 작업을 수행하지 않을 경우, 자동으로 로그 오프 되거나</li> </ul>

점검목적	워크스테이션이 잠기도록 함
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"> <li>Windows</li> </ul>
판단기준	양호 : 화면보호기 설정(대기시간 10분 이하) 및 암호로 보호가 설정되어 있는 경우
	취약 : 화면보호기 설정(대기시간 10분 초과) 및 암호로 보호가 설정되어 있지 않은 경우
조치방법	화면보호기 설정 및 암호화 보호 설정
점검 및 조치사례	
<p><b>[OS 점검 및 조치 방법]</b></p> <p>▶ <b>Window 7</b></p> <ol style="list-style-type: none"> <li>시작 -&gt; 제어판 -&gt; 개인설정 -&gt; 화면보호기 <ul style="list-style-type: none"> <li>화면보호기 실행 기타 방법1: 윈도우+R -&gt; control 입력 -&gt; 제어판 -&gt; 개인설정 -&gt; 화면보호기</li> <li>화면보호기 실행 기타 방법2: 바탕화면 -&gt; 마우스 우클릭 -&gt; 개인설정 -&gt; 화면보호기</li> </ul> </li> <li>대기 시간을 5분 ~ 10분 사이로 설정 후 “다시 시작할 때 로그인 화면 표시(R)” 체크</li> </ol> <p>▶ <b>Window 10 (Windows Defender 사용 예시)</b></p> <ol style="list-style-type: none"> <li>시작 -&gt; 설정 -&gt; 개인설정 -&gt; 잠금화면 -&gt; 화면보호기 설정 <ul style="list-style-type: none"> <li>화면보호기 실행 기타 방법1: 바탕화면 -&gt; 마우스 우클릭 -&gt; 개인설정 -&gt; 잠금화면 -&gt; 화면보호기 설정</li> </ul> </li> </ol>	

**WEB** 취약점 분석·평가 항목

점검항목	항목중요도	항목코드
크로스사이트 스크립팅	상	XS
SQL인젝션	상	SI
크로스사이트 리퀘스트 변조(CSRF)	상	CF
디렉터리 인덱싱	상	DI

XS (상)	1. 크로스사이트 스크립팅	
취약점 개요		
점검내용	■ 웹 사이트 내 크로스사이트 스크립팅 취약점 존재 여부 점검	
점검목적	■ 웹 사이트 내 크로스사이트 스크립팅 취약점을 제거하여 악성 스크립트의 실행을 차단	
판단기준 및 조치방법		
대상	■ 웹 애플리케이션 소스코드, 웹 방화벽	
판단기준	양호 : 사용자 입력 값에 대한 검증 및 필터링이 이루어지는 경우	
	취약 : 사용자 입력 값에 대한 검증 및 필터링이 이루어지지 않으며, <b>HTML</b> 코드가 입력·실행되는 경우	
조치방법	웹 사이트의 게시판, 1:1 문의, <b>URL</b> 등에서 사용자 입력 값에 대해 검증 로직을 추가하거나 입력되더라도 실행되지 않게 하고, 웹 소스코드로 <b>HTM</b> 코드 입력을 필터링 되게 한다.	
점검 및 조치사례		
<b>[점검방법]</b> ※ XSS 취약 유형		
XSS에 취약한 페이지 유형	1. HTML을 지원하는 게시판 2. Search Page 3. Join Form Page 4. Referrer를 이용하는 Page 5. 그 외 사용자로부터 입력받아 화면에 출력하는 모든 페이지에서 발생 가능	
XSS를 유발할 수 있는 스크립트	<script> ... </script>  <iframe></iframe> ※ Filtering을 우회하기 위해 다양한 표현 가능 ◆ %3Cscript%3E.....%3Cscript%3E ◆ Jav&#97;script; ◆ Java&#13;script ◆ Java&#0013;script	
사용자 입력 값을 전달받는 애플리케이션(회원정보 변경, 게시판, 댓글, 자료실 등)에 스크립트 입력 후 실행되는지 확인		

← → ↻ ⚠ 주의 요함 testla.com/qna.php

메인 합격자 발표 공지사항 문의하기 마이페이지 로그아웃

게시글 작성

제목:

XSS TEST

작성자:1

문의내용:

<script>while(1){alert("XSS TEST");}</script>

등록

취소

← → × ⚠ 주의 요함 testla.com/qna\_view.php?no=54

www.testla.com 내용:

XSS TEST

확인

■ 보안설정방법

- \* 웹 사이트에 사용자 입력 값이 저장되는 페이지는 공격자가 웹 브라우저를 통해 실행되는 스크립트 언어(HTML, Javascript, VBScript 등)를 사용하여 공격하므로 해당되는 태그 사용을 사전에 제한하고, 사용자 입력 값에 대한 필터링 작업이 필요함
- \* 게시물의 본문뿐만 아니라 제목, 댓글, 검색어 입력 창, 그 외 사용자 측에서 넘어오는 값을 신뢰하는 모든 form과 파라미터 값에 대해서 필터링을 수행함
- \* 입력 값에 대한 필터링 로직 구현 시 공백 문자를 제거하는 trim, replace 함수를 사용하여 반드시 서버 측에서 구현되어야 함
- \* URLDecoder 클래스에 존재하는 decode 메소드를 통해 URL 인코딩이 적용된 사용자 입력값을 디코딩함으로써 우회 공격 차단
- \* 웹 방화벽에 모든 사용자 입력 품(회원정보 변경, 게시판, 댓글, 자료실, 검색, URL 등)을 대상으로 특수문자, 특수 구문 필터링하도록 룰셋 적용

※ 필터링 조치 대상 입력 값

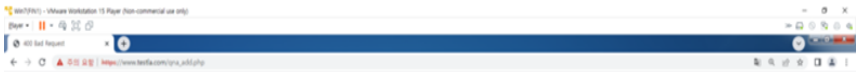
- 스크립트 정의어 : <SCRIPT>, <OBJECT>, <APPLET>, <EMBED>, <FORM>, <IFRAME> 등
- 특수문자 : <, >, ", ', &, %, %00(null) 등

[웹 애플리케이션 별 상세 설정]

**PHP** - htmlspecialchars 함수를 사용하여 사용자 입력에서 HTML 특수 문자를 이스케이프

```
<?php
require "sql_connect.php";
session_start();
$author = $_SESSION['loginID'];
$title = htmlspecialchars($_POST['title']);
$content = htmlspecialchars($_POST['content']);
... 종략 ...
```

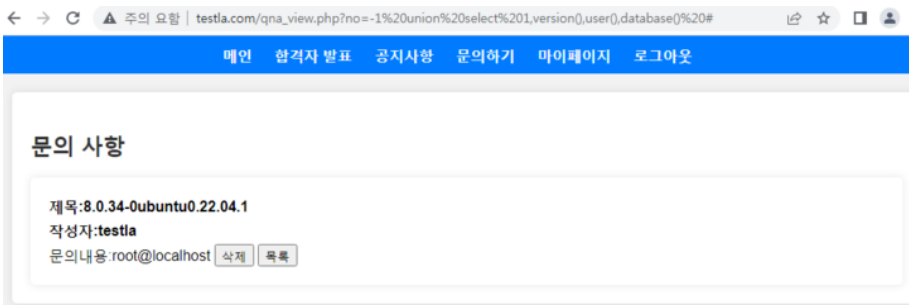
WAF



400 Bad Request

The server cannot or will not process the request due to an apparent client error (e.g., malformed request syntax, invalid request message framing, or deceptive request routing).



SI (상)	2. SQL 인젝션	
취약점 개요		
점검내용	■ 웹페이지 내 SQL 인젝션 취약점 존재 여부 점검	
점검목적	■ 대화형 웹 사이트에 비정상적인 사용자 입력 값 허용을 차단하여 악의적인 데이터베이스 접근 및 조작을 방지하기 위함	
판단기준 및 조치방법		
대상	● 웹 애플리케이션 소스코드, 웹 방화벽	
판단기준	양호 : 임의로 작성된 SQL 쿼리 입력에 대한 검증이 이루어지는 경우	
	취약 : 임의로 작성된 SQL 쿼리 입력에 대한 검증이 이루어지지 않는 경우	
조치방법	소스코드에 SQL 쿼리를 입력 값으로 받는 함수나 코드를 사용할 경우, 임의의 SQL 쿼리 입력에 대한 검증 로직을 구현하여 서버에 검증되지 않는 SQL 쿼리 요청 시 에러 페이지가 아닌 정상 페이지가 반환되도록 필터링 처리하고 웹 방화벽에 SQL 인젝션 관련 룰셋을 적용하여 SQL 인젝션 공격을 차단함	
점검 및 조치사례		
<div>■ 점검방법</div> <div>Step 1) 사용자 입력 값에 특수문자나 임의의 SQL 쿼리를 삽입하여 DB 에러 페이지가 반환되는지 확인</div> <div></div> <div>Step 2) 로그인 페이지에 참이 되는 SQL 쿼리를 전달하여 로그인되는지 확인</div> <div><div>로그인</div><div><div>ID:</div><div><input type="text" value="' or '1'"/></div></div><div><div>비밀번호:</div><div><input type="password" value="*****"/></div></div><div><div>로그인</div></div></div> <div>로그인 성공(success) <a href="#">메인페이지</a></div>		
<div>■ 보안설정방법</div> <div>* SQL 쿼리에 사용되는 문자열의 유효성을 검증하는 로직 구현</div>		

■ 보안설정방법

\* SQL 쿼리에 사용되는 문자열의 유효성을 검증하는 로직 구현

SI (상)

2. SQL 인젝션

\* 아래와 같은 특수문자를 사용자 입력 값으로 지정 금지  
(아래 문자들은 해당 데이터베이스에 따라 달라질 수 있음)

문자 설명	문자 설명
,	문자 데이터 구분기호
;	쿼리 구분 기호
--, #	해당라인 주석 구분 기호
/* */ * 와 */	사이 구문 주석

- \* Dynamic SQL 구문 사용을 지양하며 파라미터에 문자열 검사 필수적용
- \* 시스템에서 제공하는 에러 메시지 및 DBMS에서 제공하는 에러 코드가 노출되지 않도록 예외처리

\* Dynamic SQL 예시

```
try{
    String tableName = props.getProperty("jdbc.tableName");
    String name = props.getProperty("jdbc.name")
    String query = "SELECT * FROM ? WHERE Name = ?";
    stmt = con.prepareStatement(query);
    stmt.setString(1, tableName);
    stmt.setString(2, name);
    rs = stmt.executeQuery();
    .....
}
C
```

Ⅰ PHP

Dynamic SQL 구문 사용 금지 – procedure로 대체

```
*
<?php
    $order_id = $_POST['order_id'];
    $user_name = $_POST['user_name'];
    require "sql_connect.php";
    $sql_str = "call Evaluation('$order_id', '$user_name')";
    $return = sql_con($sql_str);
    $result = mysqli_fetch_array($return);
    echo $result;
?>
```

## I GET방식으로 쿼리값 사용금지

← → ↻ ⚠ 주의 요함 | [https://www.testtla.com/qna\\_view.php?no=165%20and%201=1](https://www.testtla.com/qna_view.php?no=165%20and%201=1)

항후 Chrome 업데이트를 받으려면 Windows 10 이상이 필요합니다. 이 컴퓨터에서는 Windows 7을 사용 중입니다.

[메인](#) [암격자 발표](#) [공지사항](#) [문의하기](#) [마이페이지](#) [로그인](#)

### 문의 사항

제목:  
작성자:  
문의내용:

← → ↻ ⓘ testtla.com/qna\_view.php?no=-1%20union%20select%201,2,3,4%20#

항후 Chrome 업데이트를 받으려면 Windows 10 이상이 필요합니다. 이 컴퓨터에서는 Windows 7을 사용 중입니다.



페이지가 작동하지 않습니다.

현재 [www.testtla.com](http://www.testtla.com)에서 요청을 처리할 수 없습니다.

HTTP ERROR 500

CF (상)	3. 크로스사이트 리퀘스트 변조(CSRF)
취약점 개요	
점검내용	■ 사용자의 신뢰(인증) 정보의 변조 여부 점검
점검목적	■ 사용자 입력 값에 대한 적절한 필터링 및 인증에 대한 유효성을 검증하여 신뢰(인증) 정보 내의 요청(Request)에 대한 변조 방지
판단기준 및 조치방법	
대상	● 웹 애플리케이션 소스코드, 웹 방화벽
판단기준	양호 : 사용자 입력 값에 대한 검증 및 필터링이 이루어지는 경우
	취약 : 사용자 입력 값에 대한 필터링이 이루어지지 않으며, <b>HTML 코드(또는 스크립트)</b> 를 입력하여 실행되는 경우
조치방법	사용자 입력 값에 대해 검증 로직 및 필터링 추가 적용
점검 및 조치사례	
<div>■ 점검방법</div> <div>Step 1) XSS 취약점이 존재하는지 확인</div> <div><div><div><div><div>←</div><div>→</div><div>↺</div></div><div>주의 요함   testla.com/qna.php</div><div><div>🔗</div><div>☆</div><div>🖨</div><div>👤</div></div></div></div><div><div>메인</div><div>합격자 발표</div><div>공지사항</div><div>문의하기</div><div>마이페이지</div><div>로그아웃</div></div><div><div>게시글 작성</div><div><div>제목:</div><div>XSS TEST</div></div><div><div>작성자:1</div><div>문의내용:</div><div>&lt;script&gt;while(1){alert("XSS TEST");}&lt;/script&gt;</div></div><div><div>등록</div><div>취소</div></div></div></div> <div><div><div>←</div><div>→</div><div>×</div></div><div>주의 요함   testla.com/qna_view.php?no=54</div><div><div>🔗</div><div>☆</div><div>🖨</div><div>👤</div></div></div> <div><div>www.testla.com 내용:</div><div>XSS TEST</div><div>확인</div></div>	

Step 2) 등록 및 변경 등의 데이터 수정 기능의 페이지가 있는지 조사함

#### 게시글 작성

제목:  
관리자님 글해요ㅠㅠ

작성자:1

문의내용:

```
<form id="f" method="post" action="notice_insert.php">
<input type="hidden" name="subject" value="사이트 폐쇄">
<input type="hidden" name="content" value="우리사이트의 개인정보가 유출됨. 탈퇴바람">
</form>
<script>document.getElementById("f").submit();</script>
```

등록 취소

Step 3) 데이터 수정 페이지에서 전송되는 요청(Request) 정보를 분석하여 임의의 명령을 수행하는 스크립트 삽입 후 해당 게시글을 타 사용자가 열람하였을 경우 스크립트가 실행되는지 확인

#### 글 등록 성공

번호 : 1 제목 : 테스트 공지 작성자 : admin

번호 : 2 제목 : 사이트 폐쇄 작성자 : admin

#### ■ 보안설정방법

- \* 웹 사이트에 사용자 입력 값이 저장되는 페이지는 요청이 일회성이 될 수 있도록 설계
- \* 사용 중인 프레임워크에 기본적으로 제공되는 **CSRF** 보호 기능 사용
- \* 사용자가 정상적인 프로세스를 통해 요청하였는지 **HTTP** 헤더의 **Referer** 검증 로직 구현
- \* 정상적인 요청(Request)과 비정상적인 요청(Request)을 구분할 수 있도록 **Hidden Form**을 사용하여 임의의 암호화된 토큰(세션 ID, Timestamp, nonce 등)을 추가하고 이 토큰을 검증하도록 설계
- \* **HTML**이나 자바스크립트에 해당되는 태그 사용을 사전에 제한하고, 서버 단에서 사용자 입력 값에 대한 필터링 구현
- \* **HTML Editor** 사용으로 인한 상기사항 조치 불가 시, 서버 사이드/서블릿/DAO(Data Access Object) 영역에서 조치하도록 설계

시큐어 코딩 - csrf 자동 게시글 등록 차단



프로시저로만 SQL QUERY에 접근이 가능하도록 한다.


```
sql_str = "call add_qna('$title', '$author', '$content')";
$return = sql_con($sql_str);
```

**WAF** – 방화벽으로 CSRF 공격을 막아준다



**400** Bad Request

The server cannot or will not process the request due to an apparent client error (e.g., malformed request syntax, invalid request message framing, or deceptive request routing).

DI (상)	4.디렉터리 인덱싱
취약점 개요	
점검내용	■ 웹 서버 내 디렉터리 인덱싱 취약점 존재 여부 점검
점검목적	■ 디렉터리 인덱싱 취약점을 제거하여 특정 디렉터리 내 불필요한 파일 정보의 노출을 차단
판단기준 및 조치방법	
대상	● 웹 서버
판단기준	양호 : 디렉터리 파일 리스트가 노출되지 않는 경우
	취약 : 디렉터리 파일 리스트가 노출되는 경우
조치방법	웹 서버 설정을 변경하여 디렉터리 파일 리스트가 노출되지 않도록 설정
점검 및 조치사례	
<div>■ 점검방법</div> <div>Step 1) URL 경로 중 확인하고자 하는 디렉터리까지만 주소창에 입력하여 인덱싱 여부 확인</div> <div></div> <div>■ 보안설정방법</div> <div>* 웹 서버 환경설정에서 디렉터리 인덱싱 기능 제거</div> <div>Apache</div> <div>httpd.conf 파일 내 DocumentRoot 항목의 Options에서 Indexes 제거</div> <div>Indexes가 해당 디렉터리의 파일 목록을 보여주는 지시자임</div> <div>설정 전</div> <div>&lt;Directory "/var/www/html"&gt;</div> <div>Options Indexes</div> <div>&lt;/Directory&gt;</div> <div>설정 후</div> <div>&lt;Directory "/var/www/html"&gt;</div> <div>Options</div> <div>&lt;/Directory&gt;</div>	

## DBMS 취약점 분석·평가 항목

분류	점검항목	항목중요도	항목코드
계정 관리	기본 계정의 패스워드, 권한 등을 변경하여 사용	상	D-01
	데이터베이스의 불필요 계정을 제거하거나, 잠금설정 후 사용	상	D-02
	패스워드의 사용기간 및 복잡도를 기관 정책에 맞도록 설정	상	D-03
	데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용	상	D-04
	DB 사용자 계정을 개별적으로 부여하여 사용	중	D-05
접근 관리	원격에서 DB 서버로의 접속 제한	상	D-06
	일정 횟수의 로그인 실패 시 이에 대한 잠금정책이 설정	중	D-07
	데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정하여 사용	하	D-08
백업 관리	정기적 백업 관리	상	D-09



D-01 (상)	1. 계정관리 > 1.1 기본 계정의 패스워드, 권한 등을 변경하여 사용
취약점 개요	
점검내용	■ DBMS 기본 계정의 디폴트 패스워드 및 권한 정책을 변경하여 사용하는지 점검
점검목적	■ DBMS 기본 계정의 디폴트 패스워드 및 권한 정책 변경 사용 유무를 점검하여 비인가자의 디폴트 패스워드 대입 공격을 차단하고 있는지 확인하기 위함
판단기준 및 조치방법	
대상	● MySQL
판단기준	기본 계정의 디폴트 패스워드 및 권한 정책을 변경하여 사용하는 경우
	취약 : 기본 계정의 디폴트 패스워드 및 권한 정책을 변경하지 않고 사용하는 경우
조치방법	기본(관리자) 계정의 디폴트 패스워드 및 권한 정책 변경
점검 및 조치사례	
<div>■ MySQL</div> <div>Step 1) root 계정 패스워드 변경</div> <div>mysql&gt; use mysql;</div> <div>mysql&gt; update user set password=password('new password') where user='root';</div> <div>mysql&gt; flush privileges; 또는,</div> <div>mysql&gt; set password for root=password('new password' )</div> <div>&lt; 패스워드 관리 방법 &gt;</div> <div>1. 영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정</div> <div>※ 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성</div> <div>가. 영문 대문자(26개)</div> <div>나. 영문 소문자(26개)</div> <div>다. 숫자(10개)</div> <div>라. 특수문자(32개)</div> <div>2. 시스템마다 상이한 패스워드 사용</div> <div>3. 패스워드를 기록해 놓을 경우 변형하여 기록</div> <div>4. 가급적 자주 패스워드를 변경할 것</div>	

D-02 (상)	1. 계정관리 > 1.2 데이터베이스의 불필요 계정을 제거, 잠금설정	
취약점 개요		
점검내용	■ DBMS에 존재하는 계정 중 DB 관리나 운용에 사용하지 않는 불필요한 계정이 존재하는지 점검	
점검목적	■ 불필요한 계정 존재 유무를 점검하여 불필요한 계정 정보(패스워드)의 유출 시 발생할 수 있는 비인가자의 DB 접근에 대비되어 있는지 확인하기 위함	
판단기준 및 조치방법		
대상	● MySQL	
판단기준	양호 : 계정 정보를 확인하여 불필요한 계정이 없는 경우	
	취약 : 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 불필요한 계정이 존재하는 경우	
조치방법	계정별 용도를 파악한 후 불필요한 계정 삭제	
점검 및 조치사례		
■ MySQL Step 1) 불필요한 계정 삭제 mysql> Delete from user where user='삭제할 계정';		

D-03 (상)	1. 계정관리 > 1.3 패스워드의 사용기간 및 복잡도를 기관 정책에 맞도록 설정
취약점 개요	
점검내 용	■ 기관 정책에 맞게 패스워드 사용기간 및 복잡도 설정이 적용되어 있는지 점검
점검목 적	■ 패스워드 사용기간 및 복잡도 설정 유무를 점검하여 비인가자의 패스워드 추측 공격(무작위 대입 공격, 사전 대입 공격 등)에 대한 대비가 되어있는지 확인하기 위함
판단기준 및 조치방법	
대상	● MySQL,
판단기준	양호 : 기관 정책에 맞게 패스워드 사용기간 및 복잡도 설정이 적용되어 있는 경우
	취약 : 기관 정책에 맞게 패스워드 사용기간 및 복잡도 설정이 적용되어 있지 않은 경우
조치방 법	기관 정책에 맞게 패스워드 사용기간 및 복잡도 정책 설정
점검 및 조치사례	
<div>■ MySQL</div> <div>Step 1) 패스워드 설정 규칙 적용</div> <p>패스워드 설정 규칙에 맞추어 패스워드를 설정할 수 있도록 시스템 차원에서 기능 제공</p> <div>Step 2) 패스워드 관리 적용</div> <p>패스워드 신규 적용 및 초기화 시 설정 규칙에 맞추어 관리하고, 저장 시에는 일방향 암호 알고리즘을 통한 암호화 처리(One-Way Encryption)</p> <div>STEP 3) 패스워드 변경기능 구현</div> <p>사용자가 패스워드 설정 규칙 내에서 스스로 패스워드를 변경할 수 있도록 기능을 제공하며, 패스워드 설정은 다음과 같은 방법으로 가능</p> <pre>mysql&gt; use mysql; mysql&gt; update user set password=password('new password') where user='user name'; mysql&gt; flush privileges; 또는, mysql&gt; set password for 'user name'@'%'=password('new password'); mysql&gt; flush privileges; transfer (존 파일 전송을 허용하고자 하는 IP); ;</pre>	

D-04 (상)	1. 계정관리 > 1.4 데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용
취약점 개요	
점검내용	■ 관리자 권한이 필요한 계정 및 그룹에만 관리자 권한을 부여하였는지 점검
점검목적	■ 관리자 권한이 필요한 계정과 그룹에만 관리자 권한을 부여하였는지 점검하여 관리자 권한의 남용을 방지하여 계정 유출로 인한 비인가자의 DB접근 가능성을 최소화하고자 함
판단기준 및 조치방법	
대상	● MySQL
판단기준	양호 : 관리자 권한이 필요한 계정 및 그룹에만 관리자 권한이 부여된 경우
	취약 : 관리자 권한이 필요 없는 계정 및 그룹에 권한이 부여된 경우
조치방법	관리자 권한이 필요한 계정 및 그룹에만 관리자 권한 부여
점검 및 조치사례	
<p>■ MySQL</p> <p>Step 1) mysql.user 테이블에 적용된 권한은 모든 데이터베이스에 적용되므로 host, user, password를 제외한 나머지 권한은 허용하지 않음('N')으로 설정</p> <p>1. 사용자 등록</p> <pre>mysql&gt; insert into mysql.user (host, name, password) values('%', 'user name', password ('password')); ※ 디폴트로 모든 권한 'N' 설정</pre> <p>2. 권한 변경</p> <pre>mysql&gt; update mysql.user set &lt;권한&gt;='N' where user='user name';</pre> <p>Step 2) 각 사용자는 접근하고자 하는 DB를 mysql.db에 등록 후 접근 권한을 부여하여 사용</p> <p>1. DB등록 시 권한 부여</p> <pre>mysql&gt; insert into mysql.db values('%', 'DB name', 'username', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y'); mysql&gt; flush privileges;</pre> <p>2. DB 권한 업데이트</p> <pre>mysql&gt; update mysql.db set &lt;권한&gt;='Y' where db=&lt;DB name&gt; and user='user name'; mysql&gt; flush privileges;</pre>	

D-05 (중)	1. 계정관리 > 1.6 DB 사용자 계정을 개별적으로 부여하여 사용
취약점 개요	
점검내용	■ DB 접근 시 사용자별로 서로 다른 계정을 사용하여 접근하는지 점검
점검목적	■ 사용자별 별도 DBMS 계정을 사용하여 DB에 접근하는지 점검하여 DB 계정 공유 사용으로 발생할 수 있는 로그 감사 추적 문제를 대비하고자 함
판단기준 및 조치방법	
대상	● MySQL
판단기준	양호 : 사용자별 계정을 사용하고 있는 경우
	취약 : 공용 계정을 사용하고 있는 경우
조치방법	사용자별 계정 생성 및 권한 부여
점검 및 조치사례	
<p>Step 1) 불필요한 계정 삭제</p> <pre>mysql&gt; Delete from user where user='삭제할 계정';</pre> <p>Step 2) 사용자별, 응용프로그램별 계정 생성, 권한 설정</p> <pre>mysql&gt; insert into user('localhost','user', 'password') values('localhost', ' 생성 계정', 'password(패스워드));</pre> <pre>mysql&gt; 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');</pre> <pre>mysql&gt; flush privileges</pre>	

D-06 (상)	2. 접근관리 > 2.1 원격에서 DB 서버로의 접속 제한	
취약점 개요		
점검내용	■ 지정된 IP주소만 DB 서버에 접근 가능하도록 설정되어 있는지 점검	
점검목적	■ 지정된 IP주소만 DB 서버에 접근 가능하도록 설정되어 있는지 점검하여 비인가자의 DB 서버 접근을 원천적으로 차단하고자 함	
판단기준 및 조치방법		
대상	● MySQL	
판단기준	양호 : DB서버에 지정된 IP주소에서만 접근 가능하도록 제한한 경우	
	취약 : DB서버에 지정된 IP주소에서만 접근 가능하도록 제한하지 않은 경우	
조치방법	DB서버에 대해 지정된 IP주소에서만 접근 가능하도록 설정	
점검 및 조치사례		
<div>■ MySQL</div> <div>Step 1) mysql.user 테이블과 mysql.db 테이블을 조회하여 host가 “%”인 필드 삭제하고 접속 IP주소를 지정하여 등록</div> <div>mysql&gt; delete from user where host='%’;</div> <div>mysql&gt; delete from db where host='%’; 불가능할 경우 기본 패스워드 변경으로 보완 필요</div>		

D-07 (중)	2. 접근관리 > 2.6 데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정하여 사용	
취약점 개요		
점검내용	■ 사용자 계정의 umask 설정이 022 이상으로 설정되어 있는지 점검	
점검목적	■ 소프트웨어 설치 때 생성되는 파일에 관리자를 제외한 일반 사용자의 파일 수정 권한을 제거함으로써 비인가자에 의한 DBMS 주요 파일 변경이나 삭제로부터 보호하기 위함	
판단기준 및 조치방법		
대상	● Linux OS	
판단기준	양호: 계정의 umask가 022 이상으로 설정되어 있는 경우	
	취약: 계정의 umask가 022 이상으로 설정되어 있지 않은 경우	
조치방법	계정의 umask를 022 이상으로 설정 변경	
점검 및 조치사례		
<div>- 일시적 설정으로 umask 명령을 이용하여 umask 022 이상 설정&gt; 시스템 재부팅</div> <div>- 설정 내역 유지를 위해 .bashrc, .cshrc, .login,.profile 등의 환경 변수 지정 파일에 umask 022(이상 설정)를 추가함</div> <div># vi &lt;file_name&gt;</div> <div>umask 022</div>		

D-08 (하)	인가되지 않은 <b>GRANT OPTION</b> 사용 제한	
취약점 개요		
점검내용	● 일반사용자에게 <b>Grant Option</b> 이 <b>Role</b> 에 의해 부여되어 있는지 점검	
점검목적	● 일반사용자에게 <b>Grant Option</b> 이 <b>Role</b> 에 의한 부여가 아닐 경우 권한을 취소함	
판단기준 및 조치방법		
대상	● MySQL	
판단기준	양호 : <b>WITH_GRANT_OPTION</b> 이 <b>ROLE</b> 에 의하여 설정되어 있는 경우	
	취약 : <b>WITH_GRANT_OPTION</b> 이 <b>ROLE</b> 에 의하여 설정되어있지 않은 경우	
조치방법	<b>WITH_GRANT_OPTION</b> 이 <b>ROLE</b> 에 의하여 설정되도록 변경	
점검 및 조치사례		
<div>■ MySQL</div> <div>Step 1) 설정 확인</div> <div>SELECT user,grant_priv FROM mysql.user;</div> <div>(계정이 나오는 경우 취약)</div> <div>Step 2) 권한 회수</div> <div>REVOKE 권한종류 ON 대상 FROM 계정;</div>		



D-09 (상)	정기적 백업 관리
취약점 개요	
점검내용	<ul style="list-style-type: none"><li>정기적으로 DB가 백업이 되고 있는 지 점검</li></ul>
점검목적	<ul style="list-style-type: none"><li>DB 가용성을 유지하기 위함</li></ul>
판단기준 및 조치방법	
대상	<ul style="list-style-type: none"><li>MYSQL , Ubuntu Linux</li></ul>
판단기준	양호 : 주기적으로 백업이 유지되는 경우
	취약 : 백업이 실행이 되지 않아 개인정보의 보관이 잘 이루어지지 않는 경우
조치방법	Crontab을 통한 주기적 DB 업데이트
점검 및 조치사례	
<p><b>【점검 방법】</b></p> <p>1) crontab으로 실행한 명령어가 잘 실행이 되는 지 확인</p> <pre>#!/bin/bash  # MySQL 접속 정보 설정 DB_USER="root" DB_PASS="P@ssw0rd" DB_NAME="testla"  # 백업 파일 이름 설정 (날짜와 시간을 포함) BACKUP_FILE="backup-\$(date +%Y%m%d%H%M%S).sql"  # mysqldump를 사용하여 데이터베이스를 백업 mysqldump -u\$DB_USER -p\$DB_PASS \$DB_NAME &gt; \$BACKUP_FILE  # 백업 파일을 원격 서버로 전송 (SCP를 사용) REMOTE_SERVER="root@192.168.140.71:/remote/backup/DB_back/"  sshpass -p 'qwer1234' scp \$BACKUP_FILE \$REMOTE_SERVER  # 로컬에 남겨둔 백업 파일 삭제 (선택 사항) rm \$BACKUP_FILE  * 21 * * 5 root /remote/backup/backup_server.sh &gt;&gt; /var/log/db_back.log</pre>	
<p><b>【조치 방법】</b></p> <p>1) 백업된 자료의 이름과 내용을 확인</p>	

