구분	진단코드	진단항목	취약도	점검결과
보안설정	AP-01	웹 서비스 영역의 분리	상	취약
보안설정	AP-02	불필요한 파일 제거	상	취약
보안설정	AP-03	링크 사용금지	상	취약
보안설정	AP-04	파일 업로드 및 다운로드 제한		다

진단코드		조치방법
AP-01	영역의 분리	1. 기본 디렉터리 변경 1) DocumentRoot 위치 변경 설정 디렉터리]/httpd.conf #Document "/var/apache2/htdocs" #DocumentRo "/export/userid/www"
AP-02	파일 제거	※ 웹 서버를 정기적으로 검사하여 임시 파일들을 삭제하도록 한다. 특 유지보수 시 생성되는 백업파일이나 중요한 파일 등은 작업이 끝난 아파치를 설치하면 기본적으로 설치되는 cgi-bin은 공 격에 이용 manual 파일은 시스템에 대한 정보를 포함하 고 있어서 해킹에 도 서버에서 삭제한다. 정확한 관리를 위해 폴더와 파일의 이름과 위치 문서를 관리하는 것이 좋다. 문서에 등록되지 않은 불필요한 파일들을 한다. 1. 매뉴얼 디렉터리와 cgi-bin 디렉터리 삭제 1) manual 디렉터리 삭제 2) # rm -rf [Apache2 설치 디렉터리]/m -rf [Apache2 설치 디렉터리]/cgi-bin 3) httpd.conf cgi-bin에 관한 설정이 존재할 경우 삭제 또는 주석처리 4) 디렉터리]/httpd.conf
AP-03	지	1. 심볼릭 링크, aliases 사용을 제한 설정 1) httpd 디렉터리별로 Options 항목에 설정된 FollowSymLi -FollowSymLinks 옵션 설정 <Directory MultiViews AllowOverride None
AP-05	디렉터리	1. httpd.conf 파일에 설정된 Opti 하거나 -indexes 옵션설정을 통해 디렉터리 conf 파일에서 indexes 지시자 삭제 3. " ttpd.conf <Directory "/ ndexes ow from es 지시자 설정 irectory FollowSymLinks all </Directory>
AP-06	웹 프로세스 권한 제한	1. httpd.conf 파일에서 Root 권한으로 구동되고 있을 경우에는 Apache 데몬 User/Gro up 변경 2. # vi [Apache2/httpd.conf User apache Group apache 3. /etc/passwd 파일에서 Nobody나 Apache와 (,

름 름