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

"J.W.P. MagicShop" 취약점 진단

WEB 서버 진단 상세결과

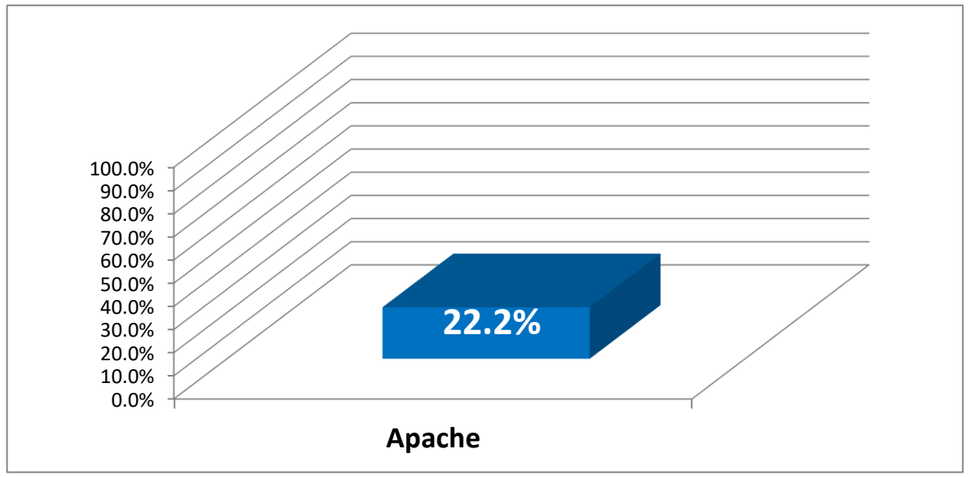
2025년 08월 25일

※ 진단 대상 리스트 - WEB 1대 (Apache 1대)

순번	진단 대상				비고
	Hostname	IP Address	버전정보	용도	
Apache					
1	jwp-web-01	10.0.0.14	Apache 2.4.52	WEB Service	

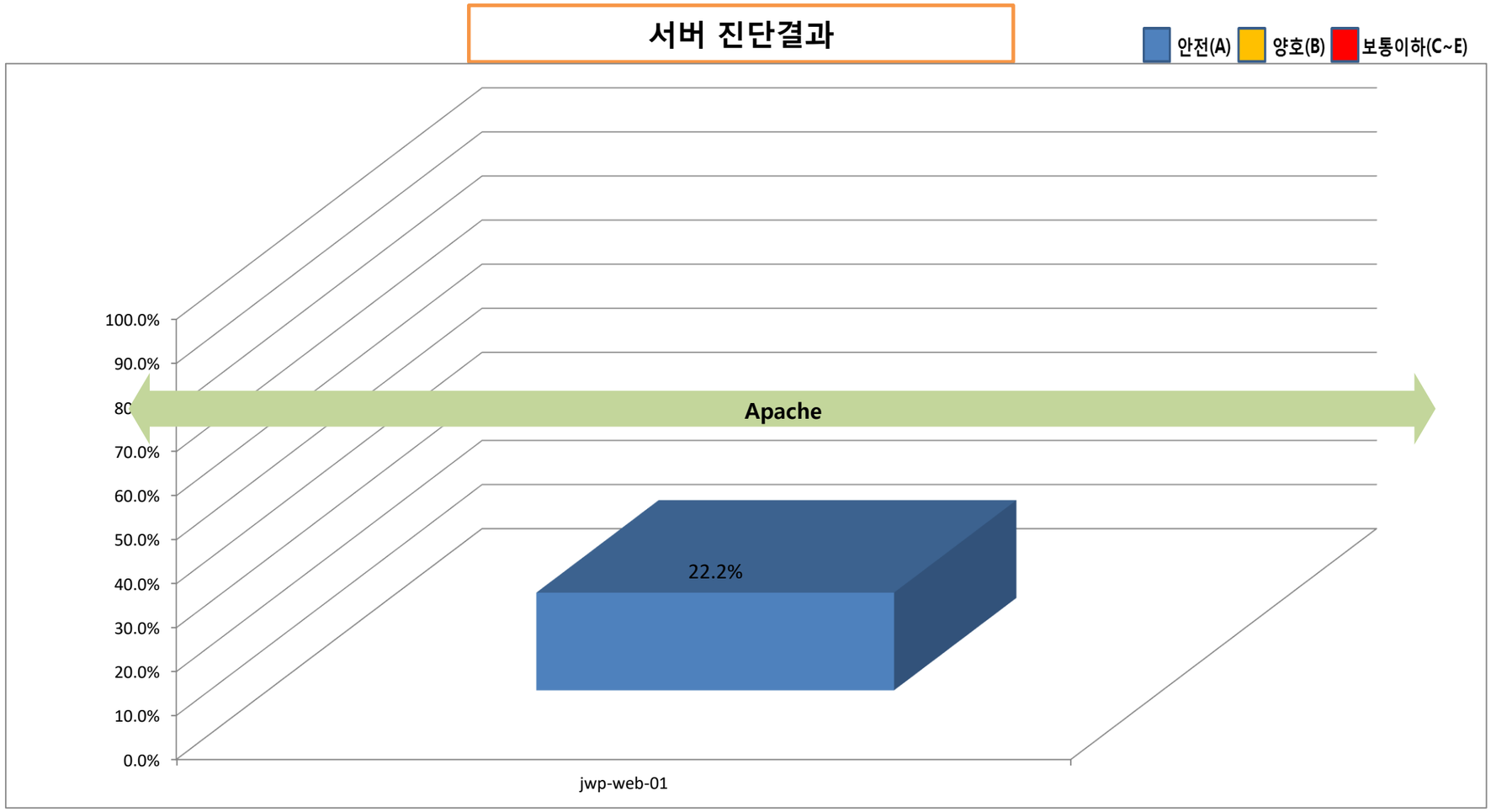
※ 대상별 평균 점수 그래프

진단 대상	평균	수량
Apache	22.2%	1



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

서버 진단결과

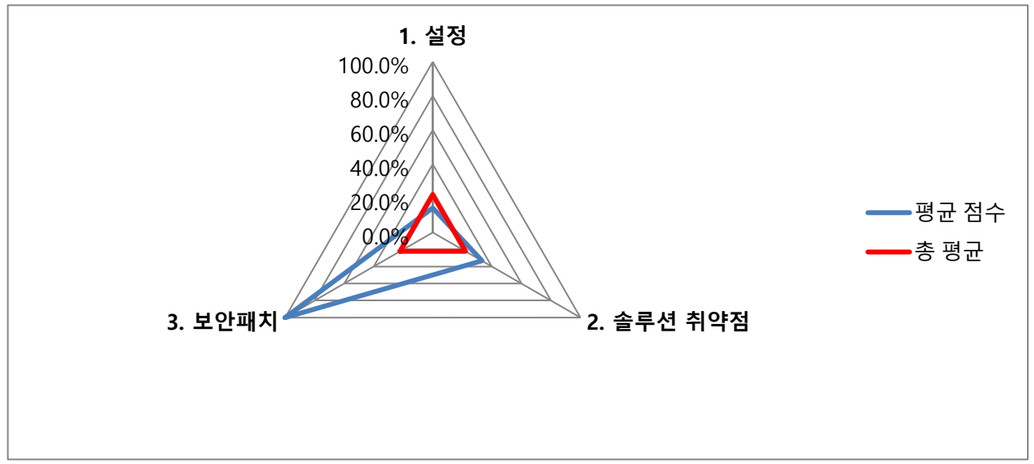


Apache		
NO.	Hostname	점수
1	jwp-web-01	22.2%

Infosec | SK C&C

진단 도메인	평균 점수	총 평균
1. 설정	14.3%	22.2%
2. 솔루션 취약점	33.3%	22.2%
3. 보안패치	100.0%	22.2%

Apache 항목별 진단 결과



Apache 취약점 진단 요약결과(18항목)

진단항목	No.	세부 진단항목	중요도	1
				jwp-web-01
				10.0.0.14
1. 설정	1	데몬 관리	상	양호
	2	관리 서버 디렉터리 권한 설정	중	취약
	3	설정 파일 권한 설정	상	취약
	4	디렉터리 검색 기능 제거	중	취약
	5	로그 디렉터리/파일 권한 설정	중	취약
	6	로그 포맷 설정	상	양호
	7	로그 저장 주기	상	취약
	8	헤더 정보 노출 방지	하	취약
	9	HTTP Method 제한	하	취약
	10	에러 메시지 관리	중	취약
	11	FollowSymLinks 옵션 비활성화	중	취약
	12	MultiViews 옵션 비활성화	중	취약
	13	상위 디렉터리 접근 금지 설정	상	취약
	14	웹 서비스 영역 분리 설정	상	취약
2. 솔루션 취약점	1	불필요한 파일 삭제	하	양호
	2	기본 문서명 사용 제한	하	취약
	3	SSL v3.0 POODLE 취약점	상	취약
3. 보안패치	1	보안 패치 적용	상	양호
점검결과				14
		보안 적용율 (양호항목 / 진단항목) %		22.2%

영역별점수	점수	양호	취약	N/A
14.3%	100.0%	1	0	0
	0.0%	0	1	0
	0.0%	0	1	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
	0.0%	0	1	0
	0.0%	0	1	0
	0.0%	0	1	0
	0.0%	0	1	0
33.3%	100.0%	1	0	0
	0.0%	0	1	0
	0.0%	0	1	0
100.0%	100.0%	1	0	0

Apache 취약점 진단 상세결과(18항목)

진단항목	No.	세부 진단항목	진단기준	1	jwp-web-01 10.0.0.14 WEB Service
1. 설정	1	데몬 관리	양호 - 로그인 불가한 전용 Web Server 계정으로 설정 및 데몬이 구동 중인 경우 취약 - 로그인 가능한 전용 Web Server 계정으로 설정 및 데몬이 구동 중인 경우	양호	secu-web@jwp-web-01:~$ cat /etc/apache2/apache2.conf | grep "User|Group" User ${APACHE_RUN_USER} Group ${APACHE_RUN_GROUP} LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combin LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined LogFormat "%{User-agent}i" agent secu-web@jwp-web-01:~$ cat /etc/passwd | grep www-data www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin secu-web@jwp-web-01:~$ ps -ef | grep httpd secu-web 43409 43373 0 01:17 pts/0 00:00:00 grep --color=auto httpd secu-web@jwp-web-01:~$
	2	관리 서버 디렉터리 권한 설정	양호 - 전용 Web Server 계정 소유이고, 750(drwxr-x---) 권한인 경우 취약 - 전용 Web Server 계정 소유가 아니거나, 750(drwxr-x---) 권한 초과인 경우	취약	secu-web@jwp-web-01:~$ cat /etc/apache2/apache2.conf | grep "ServerRoot" # ServerRoot: The top of the directory tree under which the server's #ServerRoot "/etc/apache2" secu-web@jwp-web-01:~$ ls -ald /etc/apache2/ drwxr-xr-x 8 root root 4096 Aug 14 06:40 /etc/apache2/ secu-web@jwp-web-01:~$ 관리 서버의 디렉터리인 /etc/apache2/가 root 소유이며, 권한은 755로 설정되어 있어 일반 사용자에 불필요한 권한이 부여됨
	3	설정 파일 권한 설정	양호 - 전용 Web Server 계정 소유이고, 600(-rw-------) 또는 700(-rwx-------) 권한인 경우 취약 - 전용 Web Server 계정 소유가 아니거나, 600(-rw-------) 또는 700(-rwx-------) 권한 초과인 경우	취약	secu-web@jwp-web-01:~$ find /etc/apache2/ -name "*.conf" -exec ls -al {} \; lrwxrwxrwx 1 root root 35 Aug 5 06:22 /etc/apache2/sites-enabled/000-default.conf -> ../si -rw-r--r-- 1 root root 1554 Aug 24 05:03 /etc/apache2/sites-available/000-default.conf -rw-r--r-- 1 root root 6338 Mar 18 2024 /etc/apache2/sites-available/default-ssl.conf -rw-r--r-- 1 root root 320 Mar 18 2024 /etc/apache2/ports.conf lrwxrwxrwx 1 root root 28 Aug 6 08:46 /etc/apache2/mods-enabled/proxy.conf -> ../mods-avai lrwxrwxrwx 1 root root 27 Aug 5 06:22 /etc/apache2/mods-enabled/mime.conf -> ../mods-avail lrwxrwxrwx 1 root root 32 Aug 5 06:22 /etc/apache2/mods-enabled/autoindex.conf -> ../mods- lrwxrwxrwx 1 root root 30 Aug 5 06:22 /etc/apache2/mods-enabled/deflate.conf -> ../mods-av lrwxrwxrwx 1 root root 31 Aug 5 06:22 /etc/apache2/mods-enabled/setenvif.conf -> ../mods-a lrwxrwxrwx 1 root root 34 Aug 5 06:22 /etc/apache2/mods-enabled/negotiation.conf -> ../mod lrwxrwxrwx 1 root root 32 Aug 5 06:22 /etc/apache2/mods-enabled/mpm_event.conf -> ../mods- lrwxrwxrwx 1 root root 25 Aug 5 06:22 /etc/apache2/mods-enabled/jk.conf -> ../mods-availab lrwxrwxrwx 1 root root 26 Aug 5 06:22 /etc/apache2/mods-enabled/dir.conf -> ../mods-availa lrwxrwxrwx 1 root root 33 Aug 5 06:22 /etc/apache2/mods-enabled/reqtimeout.conf -> ../mods lrwxrwxrwx 1 root root 29 Aug 5 06:22 /etc/apache2/mods-enabled/status.conf -> ../mods-ava lrwxrwxrwx 1 root root 28 Aug 5 06:22 /etc/apache2/mods-enabled/alias.conf -> ../mods-avai -rw-r--r-- 1 root root 7224 Jul 14 16:29 /etc/apache2/apache2.conf -rw-r--r-- 1 root root 402 Mar 18 2024 /etc/apache2/mods-available/info.conf -rw-r--r-- 1 root root 822 Mar 18 2024 /etc/apache2/mods-available/proxy.conf -rw-r--r-- 1 root root 7696 Mar 18 2024 /etc/apache2/mods-available/mime.conf -rw-r--r-- 1 root root 3374 Mar 18 2024 /etc/apache2/mods-available/autoindex.conf -rw-r--r-- 1 root root 347 Mar 18 2024 /etc/apache2/mods-available/proxy_balancer.conf -rw-r--r-- 1 root root 115 Mar 18 2024 /etc/apache2/mods-available/cgid.conf -rw-r--r-- 1 root root 460 Mar 18 2024 /etc/apache2/mods-available/deflate.conf -rw-r--r-- 1 root root 1373 Mar 18 2024 /etc/apache2/mods-available/setenvif.conf Web Server 관련 파일 및 디렉터리 권한이 644, 777로 설정되어 있어 그룹과 일반 사용자에 불필요한 권한이 부여됨
	4	디렉터리 검색 기능 제거	양호 - IncludesNoExec 또는 -Indexes 옵션이 설정되어 있을 경우 취약 - Indexes 옵션이 설정되어 있을 경우	취약	secu-web@jwp-web-01:~$ sudo cat /etc/apache2/apache2.conf | grep "Directory|Options" <Directory /> Options FollowSymLinks </Directory> <Directory /usr/share> </Directory> <Directory /var/www/> Options Indexes FollowSymLinks </Directory> #<Directory /srv/> # Options Indexes FollowSymLinks #</Directory> secu-web@jwp-web-01:~$ Indexes 옵션이 설정되어 있어 디렉터리 검색이 가능함
	5	로그 디렉터리/파일 권한 설정	양호 - 전용 Web Server 계정 소유이고, 디렉터리는 750(drwxr-x---), 파일은 640(-rw-r-----) 권한인 경우 취약 - 전용 Web Server 계정 소유가 아니거나, 디렉터리는 750(drwxr-x---), 파일은 640(-rw-r-----) 초과인 경우	취약	secu-web@jwp-web-01:~$ sudo ls -al /var/log/apache2/ total 404 drwxr-x--- 2 root adm 4096 Aug 27 00:00 . drwxrwxr-x 11 root syslog 4096 Aug 24 00:00 .. -rw-r----- 1 root adm 1316 Aug 27 01:21 access.log -rw-r----- 1 root adm 183772 Aug 26 23:29 access.log.1 -rw-r----- 1 root adm 1544 Aug 17 23:57 access.log.10.gz -rw-r----- 1 root adm 3635 Aug 16 23:42 access.log.11.gz -rw-r----- 1 root adm 5215 Aug 15 23:44 access.log.12.gz -rw-r----- 1 root adm 2142 Aug 14 08:26 access.log.13.gz -rw-r----- 1 root adm 10067 Aug 13 23:59 access.log.14.gz -rw-r----- 1 root adm 7998 Aug 25 23:27 access.log.2.gz -rw-r----- 1 root adm 933 Aug 24 22:48 access.log.3.gz -rw-r----- 1 root adm 775 Aug 23 23:54 access.log.4.gz -rw-r----- 1 root adm 809 Aug 22 23:52 access.log.5.gz -rw-r----- 1 root adm 903 Aug 21 23:52 access.log.6.gz -rw-r----- 1 root adm 1321 Aug 20 23:56 access.log.7.gz -rw-r----- 1 root adm 942 Aug 19 23:47 access.log.8.gz -rw-r----- 1 root adm 1659 Aug 18 23:54 access.log.9.gz -rw-r----- 1 root adm 543 Aug 27 01:04 error.log -rw-r----- 1 root adm 2706 Aug 27 00:00 error.log.1 -rw-r----- 1 root adm 5375 Aug 18 00:00 error.log.10.gz -rw-r----- 1 root adm 5116 Aug 17 00:00 error.log.11.gz -rw-r----- 1 root adm 8605 Aug 16 00:00 error.log.12.gz -rw-r----- 1 root adm 712 Aug 15 05:10 error.log.13.gz 로그 디렉터리/파일 소유자가 전용 Web Server 계정이 아닌 root 계정으로 설정됨
	6	로그 포맷 설정	양호 - 로그 포맷 설정 값이 combined 이거나 그에 준하는 포맷 스트링으로 설정되어 있는 경우 취약 - 로그 포맷 설정 값이 combined가 아니거나 그에 준하지 않는 포맷 스트링으로 설정되어 있는 경우	양호	secu-web@jwp-web-01:~$ grep -i "CustomLog" /etc/apache2/sites-available/*.conf /etc/apache2/sites-available/000-default.conf: CustomLog ${APACHE_LOG_DIR}/access.log combined /etc/apache2/sites-available/000-default.conf: CustomLog ${APACHE_LOG_DIR}/access.log combined /etc/apache2/sites-available/default-ssl.conf: CustomLog ${APACHE_LOG_DIR}/access.log combined secu-web@jwp-web-01:~$
	7	로그 저장 주기	양호 - 로그 저장 주기 기준에 맞게 운영 중일 경우 취약 - 로그 저장 주기 기준에 맞게 운영 중이 아닐 경우	취약	담당자 인터뷰 결과 로그 관리 정책이 없는 것을 확인
	8	헤더 정보 노출 방지	양호 - ServerTokens 설정 값이 Prod이고, ServerSignature 설정 값이 Off 이거나, SecRuleEngine on, ServerTokens Minimal, SecServerSignatue 설정 값이 존재할 경우 취약 - ServerTokens 설정 값이 Prod가 아니고, ServerSignature 설정 값이 On 이거나, SecRuleEngine on, ServerTokens Minimal, SecServerSignatue 설정 값이 존재하지 않을 경우	취약	secu-web@jwp-web-01:~$ grep -r "ServerTokens|ServerSignature" /etc/apache2/ | grep -v "#" /etc/apache2/conf-available/security.conf:ServerTokens OS /etc/apache2/conf-available/security.conf:ServerSignature On secu-web@jwp-web-01:~$ ServerTokens 설정 값이 OS이고, ServerSignature 설정 값이 On으로 설정되어 있음
	9	HTTP Method 제한	양호 - LimitExcept를 설정했거나 TraceEnable, Dav 설정 값이 Off 인 경우 취약 - LimitExcept를 설정하지 않았거나 TraceEnable, Dav 설정 값이 On 인 경우	취약	secu-web@jwp-web-01:~$ grep -Ri "LimitExcept|TraceEnable|Dav on" /etc/apache2/ /etc/apache2/conf-enabled/security.conf:TraceEnable Off /etc/apache2/conf-enabled/security.conf:#TraceEnable On /etc/apache2/conf-available/security.conf:TraceEnable Off /etc/apache2/conf-available/security.conf:#TraceEnable On secu-web@jwp-web-01:~$ LimitExcept 설정 값이 존재하지 않음
	10	에러 메시지 관리	양호 - 필수 에러 코드 핸들링 설정 및 에러 페이지가 존재하는 경우 취약 - 필수 에러 코드 핸들링 설정 및 에러 페이지가 존재하지 않는 경우	취약	secu-web@jwp-web-01:~$ grep -RE "ErrorDocument" /etc/apache2/ /etc/apache2/conf-enabled/localized-error-pages.conf:#ErrorDocument 500 "The server made a /etc/apache2/conf-enabled/localized-error-pages.conf:#ErrorDocument 404 /missing.html /etc/apache2/conf-enabled/localized-error-pages.conf:#ErrorDocument 404 "/cgi-bin/missing_h /etc/apache2/conf-enabled/localized-error-pages.conf:#ErrorDocument 402 http://www.example. ErrorDocument 설정이 주석 처리되어 있음

	11	FollowSymLinks 옵션 비활성화	양호 - -FollowSymLinks 설정이 존재하거나 FollowSymLinks 설정이 존재하지 않는 경우 취약 - FollowSymLinks 설정이 존재하는 경우	취약	secu-web@jwp-web-01:~$ grep -RE "FollowSymLink" /etc/apache2/ /etc/apache2/apache2.conf: Options FollowSymLinks /etc/apache2/apache2.conf: Options Indexes FollowSymLinks /etc/apache2/apache2.conf:# Options Indexes FollowSymLinks secu-web@jwp-web-01:~$ FollowSymLinks 설정이 존재함
	12	MultiViews 옵션 비활성화	양호 - -MultiViews 설정이 존재하거나 MultiViews 설정이 존재하지 않는 경우 취약 - MultiViews 설정이 존재하는 경우	취약	secu-web@jwp-web-01:~$ grep -RE "MultiViews" /etc/apache2/ /etc/apache2/mods-available/userdir.conf: Options MultiViews Indexes SymLinks /etc/apache2/conf-enabled/serve-cgi-bin.conf: Options +ExecCGI -MultiView /etc/apache2/conf-available/serve-cgi-bin.conf: Options +ExecCGI -MultiView secu-web@jwp-web-01:~$ Apache 설정 파일(userdir.conf)에서 MultiViews 옵션이 활성화되어 있음
	13	상위 디렉터리 접근 금지 설정	양호 - 상위 디렉터리에 이동 제한이 설정되어 있는 경우 취약 - 상위 디렉터리에 이동 제한이 설정되어 있지 않은 경우	취약	secu-web@jwp-web-01:~$ grep "Directory|AllowOverride" /etc/apache2/apache2.conf <Directory /> AllowOverride None </Directory> <Directory /usr/share> AllowOverride None </Directory> <Directory /var/www/> AllowOverride None </Directory> #<Directory /srv/> # AllowOverride None #</Directory> # for additional configuration directives. See also the AllowOverride secu-web@jwp-web-01:~$ AllowOverride 값이 None으로 설정되어 있음
	14	웹 서비스 영역 분리 설정	양호 - DocumentRoot가 유추할 수 없는 디렉터리로 설정되어 있을 경우 취약 - DocumentRoot가 기본 디렉터리로 설정되어 있을 경우	취약	secu-web@jwp-web-01:~$ grep -Ri "DocumentRoot" /etc/apache2/ /etc/apache2/sites-enabled/000-default.conf: DocumentRoot /var/www/html /etc/apache2/sites-available/000-default.conf: DocumentRoot /var/www/html /etc/apache2/sites-available/default-ssl.conf: DocumentRoot /var/www/html secu-web@jwp-web-01:~$ DocumentRoot가 기본 디렉터리인 /var/www/html로 설정되어 있음
2. 솔루션 취약점	1	불필요한 파일 삭제	양호 - 불필요한 디렉터리 및 스크립트가 존재하지 않는 경우 취약 - 불필요한 디렉터리 및 스크립트가 존재하는 경우	양호	secu-web@jwp-web-01:~$ find /etc/apache2/ -name manual secu-web@jwp-web-01:~$
	2	기본 문서명 사용 제한	양호 - 기본 문서명이 index.html이 아닐 경우 취약 - 기본 문서명이 index.html일 경우	취약	secu-web@jwp-web-01:~$ grep -R "DirectoryIndex" /etc/apache2/ /etc/apache2/mods-enabled/dir.conf: DirectoryIndex index.html index.cgi index.pl index. /etc/apache2/mods-available/dir.conf: DirectoryIndex index.html index.cgi index.pl index. secu-web@jwp-web-01:~$ 기본 문서명(DirectoryIndex)이 index.html로 설정되어 있음
	3	SSL v3.0 POODLE 취약점	양호 - 암호화 통신 프로토콜에서 TLS가 설정되어 있는 경우 취약 - 암호화 통신 프로토콜에서 TLS가 설정되어 있지 않는 경우	취약	secu-web@jwp-web-01:~$ grep -Ri "SSLProtocol" /etc/apache2/ /etc/apache2/mods-available/ssl.conf: SSLProtocol all -SSLv3 secu-web@jwp-web-01:~$ SSLProtocol 설정에 -SSLv2 값이 빠져있음
3. 보안 패치	1	보안 패치 적용	양호 - Apache 권고 기준 이상 버전을 적용중인 경우 취약 - Apache 권고 기준 이상 버전을 적용중이지 않은 경우	양호	secu-web@jwp-web-01:~$ apache2 -v Server version: Apache/2.4.52 (Ubuntu) Server built: 2025-08-11T12:10:10 secu-web@jwp-web-01:~$
점검결과				**14.0**	
			보안 적용율 (양호항목 / 진단항목) %	**22.2%**	