

문서번호	J.W.P. MagicShop-250901
작성자	취약점진단팀
보안등급	Confidential
Ver	ver 1.0

"J.W.P. MagicShop" 취약점 조치 이행

# WAS 서버 이행 점검 상세결과

2025년 09월 01일

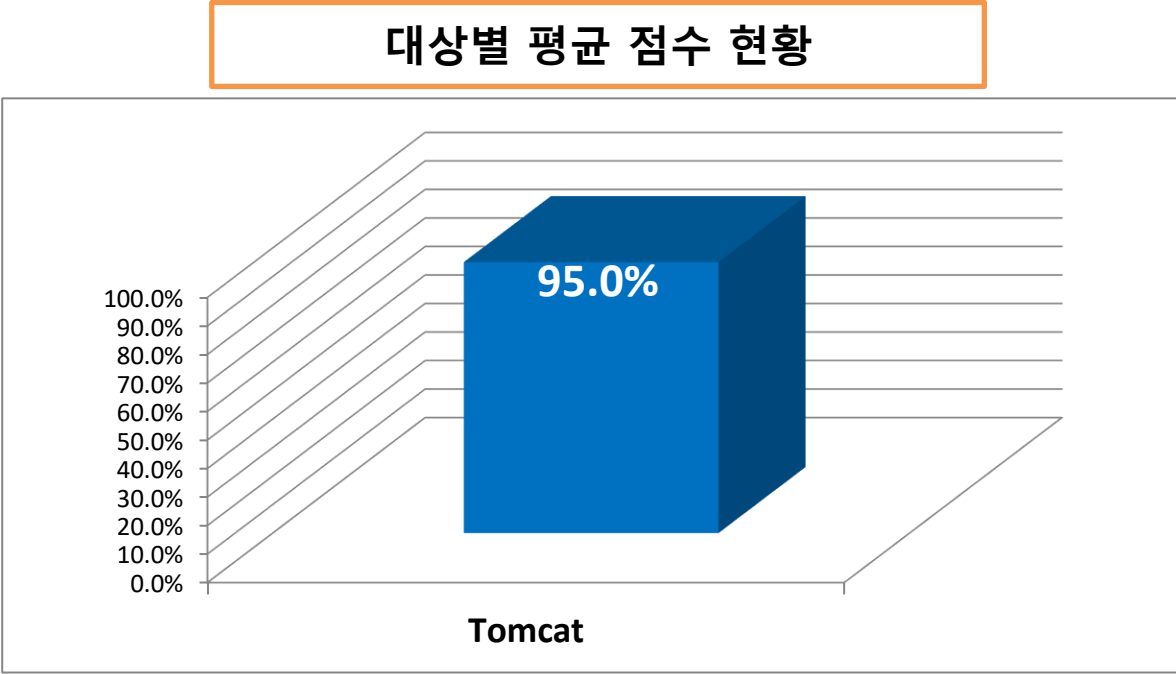


※ 진단 대상 리스트 - WAS 1대 (Tomcat 1대)

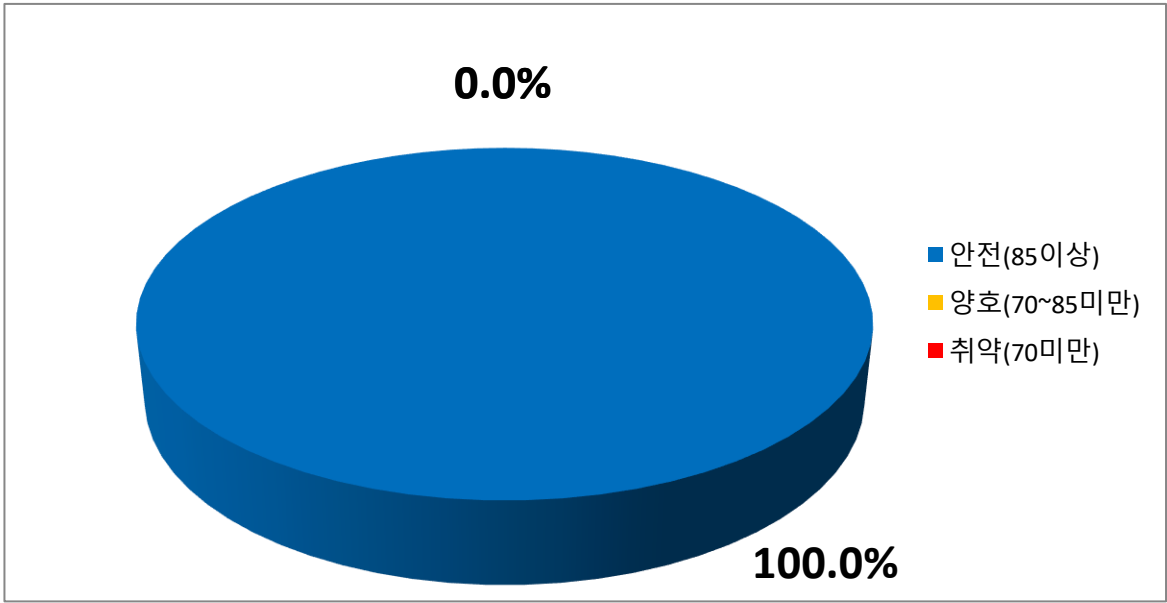
순번	진단 대상				비고
	Hostname	IP Address	버전정보	용도	
Tomcat					
1	jwp-was-01	10.0.4.135	Tomcat 9.0.107	WAS Service	

※ 대상별 평균 점수 그래프

진단 대상	평균	수량
Tomcat	95.0%	1



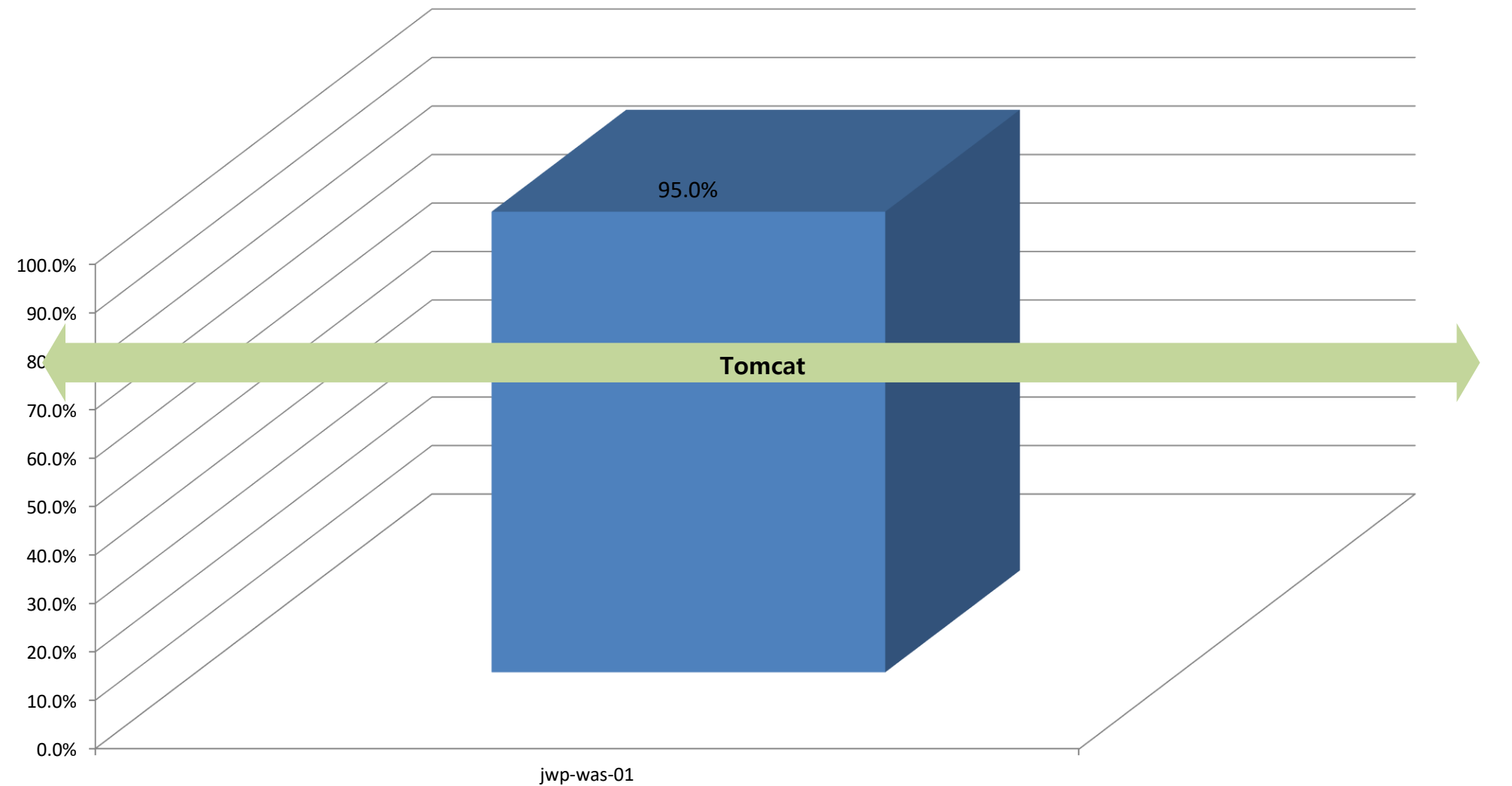
전체		1
안전(85이상)	100.0%	1
양호(70~85미만)	0.0%	0
취약(70미만)	0.0%	0



## 서버 진단결과

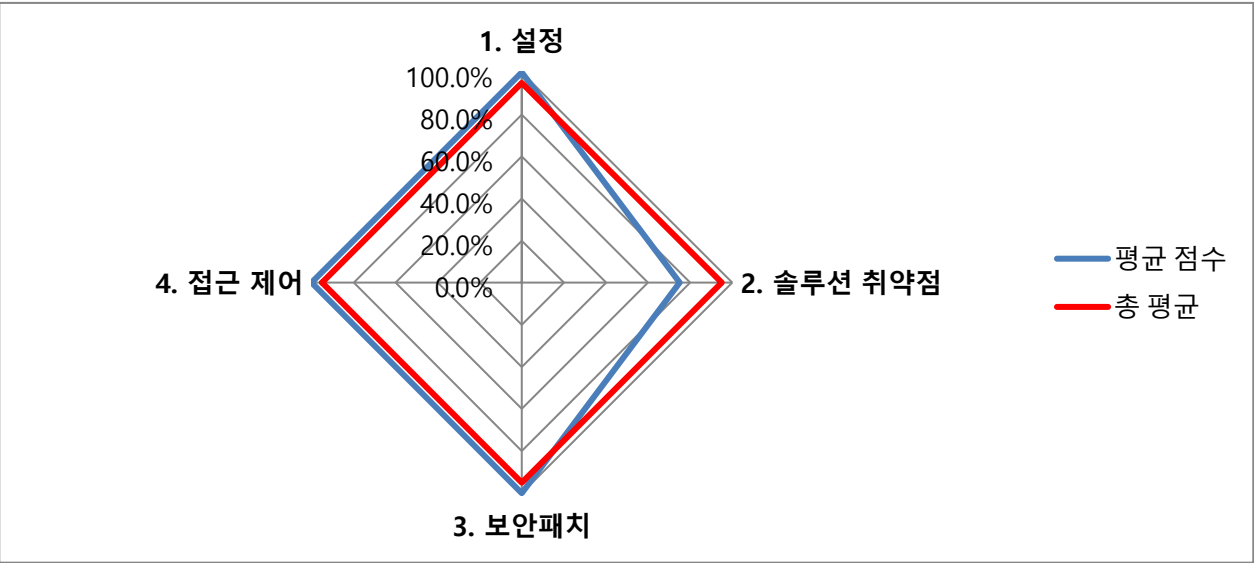
■ 안전(A)
 ■ 양호(B)
 ■ 보통이하(C~E)

Tomcat		
NO.	Hostname	점수
1	jwp-was-01	95.0%



진단 도메인	평균 점수	총 평균
1. 설정	100.0%	95.0%
2. 솔루션 취약점	75.0%	95.0%
3. 보안패치	100.0%	95.0%
4. 접근 제어	100.0%	95.0%

Tomcat 항목별 진단 결과



Tomcat 취약점 진단 요약결과(20항목)

진단항목	No.	세부 진단항목	중 요 도	1
				jwp-was-01
				10.0.4.135
1. 설정	1	데몬 관리	상	양호
	2	관리 서버 디렉터리 권한 설정	중	양호
	3	설정 파일 권한 설정	상	양호
	4	로그 디렉터리/파일 권한 설정	중	양호
	5	로그 포맷 설정	상	양호
	6	로그 저장 주기	상	양호
	7	HTTP Method 제한	하	양호
	8	디렉터리 검색 기능 제거	중	양호
	9	Session Timeout 설정	중	양호
	10	헤더 정보 노출 방지	하	양호
	11	에러 메시지 관리	중	양호
2. 솔루션 취약점	1	불필요한 파일 삭제	하	양호
	2	프로세스 관리 기능 삭제	하	양호
	3	SSL v3.0 POODLE 취약점	상	양호
	4	Apache Commons-Collection 라이브러리 취약점	상	취약
3. 보안패치	1	보안 패치 적용	상	양호
4. 접근 제어	1	관리자 콘솔 접근통제	중	양호
	2	관리자 default 계정명 변경	하	양호
	3	관리자 패스워드 암호 정책	상	양호
	4	패스워드 파일 권한 설정	중	양호
점검결과				1
	보안 적용율 (양호항목 / 진단항목) %			95.0%

영역별점수	점수	양호	취약	N/A
100.0%	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
75.0%	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	0.0%	0	1	0
100.0%	100.0%	1	0	0
100.0%	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0



Tomcat 취약점 진단 상세결과(20항목)

진단항목	No.	세부 진단항목	진단기준	1	jwp-was-01 10.0.4.135 WAS Service	jwp-was-01 10.0.4.135 WAS Service
1. 설정	1	데몬 관리	양호 - 구동 중인 Tomcat 데몬의 계정이 전용 WAS 계정인 경우 취약 - 구동 중인 Tomcat 데몬의 계정이 root인 경우	양호	<pre>secu-was@jwp-was-01:~\$ ps -ef   grep tomcat root      1948      1 99 14:29 ?        00:00:06 /usr/bin/java -Djava.util.logging.confi 0.107/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogMan va.protocol.handler.pkgs=org.apache.catalina.webresources -Dsun.io.useCanonCaches=false -Do r.UMASK=0027 -Dignore.endorsed.dirs= -classpath /home/admin/Desktop/apache-tomcat-9.0.107/b -tomcat-9.0.107/bin/tomcat-juli.jar -Dcatalina.base=/home/admin/Desktop/apache-tomcat-9.0.1 he-tomcat-9.0.107 -Djava.io.tmpdir=/home/admin/Desktop/apache-tomcat-9.0.107/temp org.apach secu-was   1968      928  0 14:29 pts/0    00:00:00 grep tomcat secu-was@jwp-was-01:~\$</pre> Tomcat 데몬의 계정이 전용 WAS 계정이 아님	<pre>secu-was@jwp-was-01:~\$ ps -ef   grep tomcat infra-w+  1713      1 98 14:25 ?        00:00:02 /usr/bin/java -Djava.util.logging.conf1 0.107/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogMan va.protocol.handler.pkgs=org.apache.catalina.webresources -Dsun.io.useCanonCaches=false -Do r.UMASK=0027 -Dignore.endorsed.dirs= -classpath /home/admin/Desktop/apache-tomcat-9.0.107/b -tomcat-9.0.107/bin/tomcat-juli.jar -Dcatalina.base=/home/admin/Desktop/apache-tomcat-9.0.1 he-tomcat-9.0.107 -Djava.io.tmpdir=/home/admin/Desktop/apache-tomcat-9.0.107/temp org.apach secu-was   1730      928  0 14:25 pts/0    00:00:00 grep tomcat secu-was@jwp-was-01:~\$</pre>
	2	관리 서버 디렉터리 권한 설정	양호 - 전용 WAS 계정 소유이고, 권한이 750(drwxr-x---) 이하인 경우 취약 - 전용 WAS 계정 소유가 아니거나, 권한이 750(drwxr-x---) 초과인 경우	양호	<pre>secu-was@jwp-was-01:~\$ sudo ls -ald \ &gt; /home/admin/Desktop/apache-tomcat-9.0.107/webapps/manager/ drwxr-xr-x 6 admin admin 4096 8월  5일 21:45 /home/admin/Desktop/apache-tomcat-9.0.107/we secu-was@jwp-was-01:~\$</pre> Tomcat의 권한 확인 결과 전용 WAS 계정 소유가 아니고 other에 읽기 권한과 실행 권한이 허용됨	<pre>secu-was@jwp-was-01:~\$ sudo ls -ald /home/admin/Desktop/\ apache-tomcat-9.0.107/webapps/manager/ drwxr-xr-x 6 infra-was infra-was 4096 8월  5일 21:45 /home/admin/Desktop/apache-tomcat-9. secu-was@jwp-was-01:~\$</pre>
	3	설정 파일 권한 설정	양호 - 전용 WAS 계정 소유이고, 권한이 700(-rwx-----) 이하인 경우 취약 - 전용 WAS 계정 소유가 아니거나, 권한이 700(-rwx-----) 초과인 경우	양호	<pre>secu-was@jwp-was-01:~\$ sudo find /home/admin/Desktop/apache-tomcat-9.0.107/conf \ -name "*.xml" -ls -o \ -name "*.policy" -ls -o \ -name "*.properties" -ls 410022      8 -rw----r-x  1 admin  admin    8015  8월  27 10:00 /home/admin/Desktop/ 429107     16 -rw----r-x  1 admin  admin   12953  7월  2 16:01 /home/admin/Desktop/ y 429724      4 -rw----r-x  1 admin  admin    1149  7월  2 16:01 /home/admin/Desktop/ rs.xml 444046      4 -rw----r-x  1 admin  admin    2851  8월 14 16:56 /home/admin/Desktop/ ml 429722      8 -rw----r-x  1 admin  admin    7654  7월  2 16:01 /home/admin/Desktop/ rties 429726      4 -rw----r-x  1 admin  admin    4003  7월  2 16:01 /home/admin/Desktop/ ties 429723      4 -rw----r-x  1 admin  admin    1400  7월  2 16:01 /home/admin/Desktop/ 409992     172 -rw----r-x  1 admin  admin   173781 8월 24 16:16 /home/admin/Desktop/ secu-was@jwp-was-01:~\$</pre> Tomcat 설정 파일의 권한 확인 결과 전용 WAS 계정 소유가 아니고 other의 권한에 읽기 권한과 실행 권한이 허용됨	<pre>secu-was@jwp-was-01:~\$ sudo find /home/admin/Desktop/apache-tomcat-9.0.107/conf/ \ -name "*.xml" -ls -o \ -name "*.policy" -ls -o \ -name "*.properties" -ls 447067      8 -rw-----  1 infra-was infra-was    7991  8월 27 13:17 /home/admin/Desk 429107     16 -rw-----  1 infra-was infra-was   12953  7월  2 16:01 /home/admin/Desk icy 429724      4 -rw-----  1 infra-was infra-was    1149  7월  2 16:01 /home/admin/Desk ders.xml 444046      4 -rw-----  1 infra-was infra-was    2851  8월 14 16:56 /home/admin/Desk .xml 429722      8 -rw-----  1 infra-was infra-was    7654  7월  2 16:01 /home/admin/Desk perties 429726      4 -rw-----  1 infra-was infra-was    4003  7월  2 16:01 /home/admin/Desk erties 429723      4 -rw-----  1 infra-was infra-was    1400  7월  2 16:01 /home/admin/Desk 409992     172 -rw-----  1 infra-was infra-was   173781 8월 24 16:16 /home/admin/Desk secu-was@jwp-was-01:~\$</pre>
	4	로그 디렉터리/파일 권한 설정	양호 - 전용 WAS 계정 소유이고, 디렉토리 권한이 750(drwxr-x---), 파일 권한은 640(-rw-r-----) 이하인 경우 취약 - 전용 WAS 계정 소유가 아니거나, 디렉토리 권한이 750(drwxr-x---), 파일 권한은 640(-rw-r-----) 초과인 경우	양호	<pre>secu-was@jwp-was-01:~\$ sudo ls -al /home/admin/Desktop/apache-tomcat-9.0.107/logs 합계 77224 drwxr-xr-x 2 admin admin    4096  8월 27일 09:07 . drwxr-xr-x 9 admin admin    4096  8월  5일 21:45 .. -rw-r--r-x 1 admin admin   40804  8월  6일 08:40 catalina.2025-08-05.log -rw-r----- 1 admin admin  35487  8월  6일 19:04 catalina.2025-08-06.log -rw-r----- 1 admin admin  74004  8월  8일 08:30 catalina.2025-08-07.log -rw-r----- 1 admin admin  49463  8월  9일 08:59 catalina.2025-08-08.log -rw-r----- 1 admin admin  20076  8월  9일 09:46 catalina.2025-08-09.log -rw-r----- 1 admin admin 120916  8월 10일 22:47 catalina.2025-08-10.log -rw-r----- 1 admin admin  63730  8월 11일 20:35 catalina.2025-08-11.log -rw-r----- 1 admin admin  13347  8월 13일 08:43 catalina.2025-08-12.log secu-was@jwp-was-01:~\$</pre> Tomcat 로그 디렉토리 권한 확인 결과 전용 WAS 계정 소유가 아니고 other의 권한에 읽기 권한과 실행 권한이 허용됨	<pre>secu-was@jwp-was-01:~\$ sudo ls -al /home/admin/Desktop/apache-tomcat-9.0.107/logs/ 합계 77636 drwxr-xr-x 2 infra-was infra-was    4096  8월 27일 14:09 . drwxr-xr-x 9 infra-was infra-was    4096  8월  5일 21:45 .. -rw-r----- 1 infra-was infra-was   40804  8월  6일 08:40 catalina.2025-08-05.log -rw-r----- 1 infra-was infra-was  35487  8월  6일 19:04 catalina.2025-08-06.log -rw-r----- 1 infra-was infra-was  74004  8월  8일 08:30 catalina.2025-08-07.log -rw-r----- 1 infra-was infra-was  49463  8월  9일 08:59 catalina.2025-08-08.log -rw-r----- 1 infra-was infra-was  20076  8월  9일 09:46 catalina.2025-08-09.log -rw-r----- 1 infra-was infra-was 120916  8월 10일 22:47 catalina.2025-08-10.log -rw-r----- 1 infra-was infra-was  63730  8월 11일 20:35 catalina.2025-08-11.log -rw-r----- 1 infra-was infra-was  13347  8월 13일 08:43 catalina.2025-08-12.log secu-was@jwp-was-01:~\$</pre>
	5	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	<pre>secu-was@jwp-was-01:~\$ sudo grep "pattern=" /home/admin/Desktop/apache-tomcat-9.0.107/\ &gt; conf/server.xml Note: The pattern used is equivalent to using pattern="common" --&gt; pattern="%h %L %u %t &amp;quot;%r&amp;quot; %s %b" /&gt; secu-was@jwp-was-01:~\$</pre> 로그 포맷이 common으로 설정되어 있어 combined 수준의 상세 로그(Referer, User-Agent 등)가 기록되지 않음	<pre>secu-was@jwp-was-01:~\$ sudo grep "pattern=" /home/admin/Desktop/apache-tomcat-9.0.107/\ conf/server.xml Note: The pattern used is equivalent to using pattern="common" --&gt; pattern="combined" /&gt; secu-was@jwp-was-01:~\$</pre>
	6	로그 저장 주기	양호 - 로그 저장 주기 기준에 맞게 운영 중일 경우 취약 - 로그 저장 주기 기준에 맞게 운영 중이 아닐 경우	양호	담당자 인터뷰 결과 로그 관리 정책이 없는 것을 확인	로그 관리 정책 수립 (담당자 협의 완료)  1. 로그 파일 저장 기간 - 사용자 접속정보 기록: 6개월 이상 - 개인정보취급자 시스템 접속 기록: 2년 이상 - 개인정보취급자 권한 변경 기록: 5년 이상 2. 정기적 감독 및 관리 - 월 1회 이상 접속 기록 정기 점검 - 오류 또는 부정행위 발생 시 즉시 보고 및 조치 3. 백업 및 보관 - 접속 기록은 별도로 물리적 저장 장치에 보관 및 주 1회 이상 정기적 백업 수행
	7	HTTP Method 제한	양호 - 불필요한 HTTP-Method 제한 설정이 되어 있는 경우 취약 - 불필요한 HTTP-Method 제한 설정이 되어 있지 않은 경우	양호	<pre>secu-was@jwp-was-01:~\$ sudo grep "method" /home/admin/Desktop/apache-tomcat-9.0.107/\ &gt; conf/web.xml secu-was@jwp-was-01:~\$</pre> 설정 존재하지 않음	<pre>secu-was@jwp-was-01:~\$ sudo grep "method" /home/admin/Desktop/\ apache-tomcat-9.0.107/conf/web.xml &lt;http-method&gt;PUT&lt;/http-method&gt; &lt;http-method&gt;DELETE&lt;/http-method&gt; &lt;http-method&gt;TRACE&lt;/http-method&gt; secu-was@jwp-was-01:~\$</pre>
	8	디렉터리 검색 기능 제거	양호 - "listings" param-name의 값이 false인 경우 취약 - "listings" param-name의 값이 false가 아닌 경우	양호	<pre>secu-was@jwp-was-01:~\$ sudo grep "param" /home/admin/Desktop/apache-tomcat-9.0.107/\ &gt; conf/web.xml &lt;!-- parameters (default values are in square brackets): --&gt; &lt;init-param&gt;   &lt;param-name&gt;debug&lt;/param-name&gt;   &lt;param-value&gt;0&lt;/param-value&gt; &lt;/init-param&gt; &lt;init-param&gt;   &lt;param-name&gt;listings&lt;/param-name&gt;   &lt;param-value&gt;true&lt;/param-value&gt; &lt;/init-param&gt; param-name의 값이 true로 디렉터리 검색 기능이 활성화 되어 있음</pre>	<pre>secu-was@jwp-was-01:~\$ sudo grep "param" /home/admin/Desktop/\ apache-tomcat-9.0.107/conf/web.xml &lt;!-- parameters (default values are in square brackets): --&gt; &lt;init-param&gt;   &lt;param-name&gt;debug&lt;/param-name&gt;   &lt;param-value&gt;0&lt;/param-value&gt; &lt;/init-param&gt; &lt;init-param&gt;   &lt;param-name&gt;listings&lt;/param-name&gt;   &lt;param-value&gt;&gt;false&lt;/param-value&gt; &lt;/init-param&gt;</pre>



	9	Session Timeout 설정	양호 - timeout 값이 60 이하로 설정되어 있는 경우 취약 - timeout 값이 60 초과로 설정되어 있는 경우	양호	secu-was@jwp-was-01:~\$ sudo grep "session-timeout" /home/admin/Desktop/\> apache-tomcat-9.0.107/conf/web.xml <session-timeout>30</session-timeout> secu-was@jwp-was-01:~\$	
	10	헤더 정보 노출 방지	양호 - Connector 지시어 내 server 속성 값이 있는 경우 취약 - Connector 지시어 내 server 속성 값이 없는 경우	양호	secu-was@jwp-was-01:~\$ sudo grep "Connector port" /home/admin/Desktop/\> apache-tomcat-9.0.107/conf/server.xml <Connector port="8080" protocol="HTTP/1.1" <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" <Connector port="8443" protocol="org.apache.coyote.http11.Http11AprProtocol" secu-was@jwp-was-01:~\$ Tomcat의 server.xml 파일 확인 결과 열려 있는 Connector 지시어에 server 속성이 정의되어 있지 않음	secu-was@jwp-was-01:~\$ sudo grep "Connector port" /home/admin/Desktop/\> apache-tomcat-9.0.107/conf/server.xml <Connector port="8080" protocol="HTTP/1.1" server="server" <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" <Connector port="8443" protocol="org.apache.coyote.http11.Http11AprProtocol" secu-was@jwp-was-01:~\$
	11	에러 메시지 관리	양호 - 에러 핸들링 설정이 되어 있고, 생성한 예러 페이지가 존재하는 경우 취약 - 에러 핸들링 설정이 되어 있지 않거나, 생성한 예러 페이지가 존재하지 않는 경우	양호	secu-was@jwp-was-01:~\$ sudo grep "error" /home/admin/Desktop/apache-tomcat-9.0.107/\> webapps/ROOT/WEB-INF/web.xml secu-was@jwp-was-01:~\$ 에러 핸들링 파일 존재하지 않음	secu-was@jwp-was-01:~\$ sudo ls -al /home/admin/Desktop/apache-tomcat-9.0.107/webapps/ROOT/WEB-INF/views/error.jsp -rw-r--r-- 1 root root 681 8월 27일 16:21 /home/admin/Desktop/apache-tomcat-9.0.107/webapps/ROOT/WEB-INF/views/error.jsp secu-was@jwp-was-01:~\$
2. 솔루션 취약점	1	불필요한 파일 삭제	양호 - Examples 디렉터리가 존재하지 않는 경우 취약 - Examples 디렉터리가 존재하는 경우	양호	secu-was@jwp-was-01:~\$ sudo find /home/admin/Desktop/apache-tomcat-9.0.107/webapps/ \> -name "examples" /home/admin/Desktop/apache-tomcat-9.0.107/webapps/examples /home/admin/Desktop/apache-tomcat-9.0.107/webapps/examples/WEB-INF/classes/examples /home/admin/Desktop/apache-tomcat-9.0.107/webapps/examples/WEB-INF/classes/jsp2/examples secu-was@jwp-was-01:~\$ Examples 디렉터리 존재 확인됨	secu-was@jwp-was-01:~\$ sudo find /home/admin/Desktop/apache-tomcat-9.0.107/webapps \> -name "examples" secu-was@jwp-was-01:~\$
	2	프로세스 관리 기능 삭제	양호 - catalina-manager.jar 파일이 존재하지 않는 경우 취약 - catalina-manager.jar 파일이 존재하는 경우	양호	secu-was@jwp-was-01:~\$ sudo find /home/admin/Desktop/apache-tomcat-9.0.107/webapps/\> manager/ -name "catalina-manager.jar" secu-was@jwp-was-01:~\$	
	3	SSL v3.0 POODLE 취약점	양호 - 암호화 통신 프로토콜에서 TLS가 설정되어 있는 경우 취약 - 암호화 통신 프로토콜에서 TLS가 설정되어 있지 않는 경우	양호	secu-was@jwp-was-01:~\$ sudo grep -A 15 -B 2 "Http11AprProtocol" \> /home/admin/Desktop/apache-tomcat-9.0.107/conf/server.xml --> <!-- <Connector port="8443" protocol="org.apache.coyote.http11.Http11AprProtocol" maxThreads="150" SSLEnabled="true" maxParameterCount="1000" --> <UpgradeProtocol className="org.apache.coyote.http2.Http2Protocol" /> <SSLHostConfig> <Certificate certificateKeyFile="conf/localhost-rsa-key.pem" certificateFile="conf/localhost-rsa-cert.pem" certificateChainFile="conf/localhost-rsa-chain.pem" type="RSA" /> </SSLHostConfig> </Connector> -->	secu-was@jwp-was-01:~\$ sudo grep -A 10 -B 0 "Http11NioProtocol" \> /home/admin/Desktop/apache-tomcat-9.0.107/conf/server.xml --> <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150" SSLEnabled="true" maxParameterCount="1000"> <SSLHostConfig protocols="TLSv1.2,TLSv1.3" ciphers="TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_GCM_SHA256,TLS_AES_128_GCM_SHA256,ECDHE-RSA-AES256-GCM_SHA384,ECDHE-RSA-AES128-GCM_SHA256" honorCipherOrder="true" disableSessionTickets="true"> <Certificate certificateKeyStoreFile="conf/localhost-rsa.jks" certificateKeyStorePassword="changeit" type="RSA" /> </SSLHostConfig> </Connector> --> <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150" SSLEnabled="true"
	4	Apache Commons-Collection 라이브러리 취약점	양호 - 안전한 버전의 라이브러리를 사용하거나, 안전하지 않은 클래스를 사용하지 않을 경우 취약 - 취약한 버전의 라이브러리를 사용하고 있으며, 안전하지 않은 클래스를 사용할 경우	취약	secu-was@jwp-was-01:~\$ sudo jar tf /home/admin/Desktop/apache-tomcat-9.0.107/\> webapps/ROOT/WEB-INF/lib/commons-collections-3.2.jar   \> grep -E "CloneTransformer ForClosure InstantiateFactory InstantiateTransformer InvokerTransformer PrototypeCloneFactory PrototypeSerializationFactory WhileClosure" org/apache/commons/collections/functors/CloneTransformer.class org/apache/commons/collections/functors/ForClosure.class org/apache/commons/collections/functors/InstantiateFactory.class org/apache/commons/collections/functors/InstantiateTransformer.class org/apache/commons/collections/functors/InvokerTransformer.class org/apache/commons/collections/functors/PrototypeFactory\$PrototypeCloneFactory.class org/apache/commons/collections/functors/PrototypeFactory\$PrototypeSerializationFactory.class org/apache/commons/collections/functors/WhileClosure.class secu-was@jwp-was-01:~\$ commons-collections-3.2.jar 안에 다음과 같은 취약 클래스들이 존재함	
3. 보안 패치	1	보안 패치 적용	양호 - Tomcat 권고 기준 이상의 버전을 사용할 경우 취약 - Tomcat 권고 기준 미만의 버전을 사용할 경우	양호	secu-was@jwp-was-01:~\$ sudo /home/admin/Desktop/apache-tomcat-9.0.107/\> bin/version.sh Using CATALINA_BASE: /home/admin/Desktop/apache-tomcat-9.0.107 Using CATALINA_HOME: /home/admin/Desktop/apache-tomcat-9.0.107 Using CATALINA_TMPDIR: /home/admin/Desktop/apache-tomcat-9.0.107/temp Using JRE_HOME: /usr Using CLASSPATH: /home/admin/Desktop/apache-tomcat-9.0.107/bin/bootstrap.jar:/home/admin/Desktop/apache-tomcat-9.0.107/bin/t-juli.jar Using CATALINA_OPTS: NOTE: Picked up JDK_JAVA_OPTIONS: --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.lang.reflect=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED Server version: Apache Tomcat/9.0.107 Server built: Jul 2 2025 07:01:03 UTC Server number: 9.0.107.0 OS Name: Linux OS Version: 6.1.0-38-cloud-amd64 Architecture: amd64 JVM Version: 17.0.16+8-Debian-1deb12u1 JVM Vendor: Debian	
	1	관리자 콘솔 접근통제	양호 - 관리자 콘솔을 사용하지 않거나, Default 포트(8080)가 아닌 경우 취약 - 관리자 콘솔을 사용하고 있으며, Default 포트(8080)인 경우	양호	secu-was@jwp-was-01:~\$ sudo grep "Connector port" /home/admin/Desktop/\> apache-tomcat-9.0.107/conf/server.xml <Connector port="8080" protocol="HTTP/1.1" <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" <Connector port="8443" protocol="org.apache.coyote.http11.Http11AprProtocol" secu-was@jwp-was-01:~\$ server.xml 설정 확인 결과 8080 포트 확인됨	secu-was@jwp-was-01:~\$ sudo grep "Connector port" /home/admin/Desktop/\> apache-tomcat-9.0.107/conf/server.xml <Connector port="4210" protocol="HTTP/1.1" server="server" <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" <Connector port="8443" protocol="org.apache.coyote.http11.Http11AprProtocol" secu-was@jwp-was-01:~\$



4. 접근 제어	2	관리자 default 계정명 변경	양호 - 관리자/사용자 계정 생성 및 역할에 따른 각각의 role을 부여한 경우 취약 - Default 계정 사용 및 역할에 따른 각각의 role을 부여하지 않은 경우	양호 secu-was@jwp-was-01:~\$ sudo grep -A 1 -B 1 "username" /home/admin/Desktop/\apache-tomcat-9.0.107/conf/tomcat-users.xml to operate the "/manager/html" web application. If you wish to use this app, you must define such a user - the username and password are arbitrary. -- <!-- <user username="admin" password="<must-be-changed>" roles="manager-gui"/> <user username="robot" password="<must-be-changed>" roles="manager-script"/> --> -- <role rolename="role1"/> <user username="tomcat" password="<must-be-changed>" roles="tomcat"/> <user username="both" password="<must-be-changed>" roles="tomcat,role1"/> <user username="role1" password="<must-be-changed>" roles="role1"/> --> <role rolename="manager-gui"/> <user username="test" password="test" roles="manager-gui"/> </tomcat-users> secu-was@jwp-was-01:~\$ tomcat-users.xml 확인 결과 admin, tomcat 같은 기본 계정 그대로 존재함	secu-was@jwp-was-01:~\$ sudo grep -A 1 -B 1 "username" /home/admin/Desktop/\apache-tomcat-9.0.107/conf/tomcat-users.xml to operate the "/manager/html" web application. If you wish to use this app, you must define such a user - the username and password are arbitrary. -- <!-- <user username="admin" password="<must-be-changed>" roles="manager-gui"/> <user username="robot" password="<must-be-changed>" roles="manager-script"/> --> -- <role rolename="role1"/> <user username="tomcat" password="<must-be-changed>" roles="tomcat"/> <user username="both" password="<must-be-changed>" roles="tomcat,role1"/> <user username="role1" password="<must-be-changed>" roles="role1"/> --> <role rolename="manager-gui"/> <user username="infra-was" password="Qkrtnclndir!" roles="manager-gui"/> </tomcat-users> secu-was@jwp-was-01:~\$
	3	관리자 패스워드 암호 정책	양호 - 보안 기준에 충족하는 패스워드로 설정되어 있는 경우 취약 - 보안 기준에 충족하지 않는 패스워드로 설정되어 있는 경우	양호 secu-was@jwp-was-01:~\$ sudo grep -A 1 -B 1 "username" /home/admin/Desktop/\apache-tomcat-9.0.107/conf/tomcat-users.xml to operate the "/manager/html" web application. If you wish to use this app, you must define such a user - the username and password are arbitrary. -- <!-- <user username="admin" password="<must-be-changed>" roles="manager-gui"/> <user username="robot" password="<must-be-changed>" roles="manager-script"/> --> -- <role rolename="role1"/> <user username="tomcat" password="<must-be-changed>" roles="tomcat"/> <user username="both" password="<must-be-changed>" roles="tomcat,role1"/> <user username="role1" password="<must-be-changed>" roles="role1"/> --> <role rolename="manager-gui"/> <user username="test" password="test" roles="manager-gui"/> </tomcat-users> secu-was@jwp-was-01:~\$ tomcat-users.xml 확인 결과 패스워드가 기본값으로 보안 기준에 충족하지 않는 패스워드 사용하는 것이 확인됨	secu-was@jwp-was-01:~\$ sudo grep -A 1 -B 1 "username" /home/admin/Desktop/\apache-tomcat-9.0.107/conf/tomcat-users.xml to operate the "/manager/html" web application. If you wish to use this app, you must define such a user - the username and password are arbitrary. -- <!-- <user username="admin" password="<must-be-changed>" roles="manager-gui"/> <user username="robot" password="<must-be-changed>" roles="manager-script"/> --> -- <role rolename="role1"/> <user username="tomcat" password="<must-be-changed>" roles="tomcat"/> <user username="both" password="<must-be-changed>" roles="tomcat,role1"/> <user username="role1" password="<must-be-changed>" roles="role1"/> --> <role rolename="manager-gui"/> <user username="infra-was" password="Qkrtnclndir!" roles="manager-gui"/> </tomcat-users> secu-was@jwp-was-01:~\$
	4	패스워드 파일 권한 설정	양호 - 전용 WAS 계정 소유이고, 700(-rwx-----) 또는 600(-rw-----) 권한인 경우 취약 - 전용 WAS 계정 소유가 아니거나, 700(-rwx-----) 또는 600(-rw-----) 권한이 아닌 경우	양호 secu-was@jwp-was-01:~\$ sudo ls -al /home/admin/Desktop/apache-tomcat-9.0.107/\> conf/tomcat-users.xml -rw---r-x 1 admin admin 2851 8월 14일 16:56 /home/admin/Desktop/apache-tomcat-9.0.107/conf/tomcat-users.xml secu-was@jwp-was-01:~\$ tomcat-users.xml 확인 결과 전용 WAS 계정 소유가 아니고 other 사용자에게 읽기 권한과 실행 권한이 존재함	secu-was@jwp-was-01:~\$ sudo ls -al /home/admin/Desktop/\apache-tomcat-9.0.107/conf/tomcat-users.xml -rw----- 1 infra-was infra-was 2851 8월 14일 16:56 /home/admin/Desktop/apache-tomcat-9.0.107/conf/tomcat-users.xml secu-was@jwp-was-01:~\$
	점검결과			1.0	
	보안 적용율 (양호항목 / 진단항목) %		95.0%		