SonarQube 행자부 보안취약점 대응표

소나큐브는 다양한 룰을 포함하고 있다. 이 페이지는 행안부의 보안취약점에 대응하는 SonaQube 대응룰을 정리한다.

- FB: FindBugs
- FSB: FindSecurityBugs
- SQ: SonarQube 자체 지원

소나큐브 룰 = https://rules.sonarsource.com

도구 측정 불가 항목

No.		행자부 SW 보안약점	FB	FSB	PMD	SQ	
1	입력데이터 검증 및 표현	SQL 삽입	O	O		CWE-89	
2		경로 조작 및 자원 삽입	O	O		CWE-99	
3		크로스사이트 스크립트	O	O		CWE-79, RSPEC-5131	
4		운영체제 명령어 삽입		O		CWE-78	
5		위험한 형식 파일 업로드				CWE-434	
6		신뢰되지 않는 URL 주소로 자동접속 연결		O		CWE-601	
7		XQuery 삽입				CWE-652	
8		XPath 삽입		O		CWE-643	
9		LDAP 삽입		O		CWE-90	
10		크로스사이트 요청 위조				CWE-352	
		디렉토리 경로 조작				CWE-22(23,36)	
11		HTTP 응답분할	O	O		CWE-113	
12		정수형 오버플로우				CWE-190	
13		보안기능 결정에 사용되는 부적절한 입력값		O		CWE-807	
14		메모리 버퍼 오버플로우 (C-Language)		O		CWE-119	
15		포맷 스트링 삽입				CWE-134	
16	보안기능	적절한 인증 없는 중요기능 허용				CWE-306	
17		부적절한 인가				CWE-285	
18		중요한 자원에 대한 잘못된 권한 설정				CWE-732	
19		취약한 암호화 알고리즘 사용		O		CWE-327	
20		중요정보 평문저장		O		CWE-312	
21		취약한 암호화 알고리즘 사용		O	x		
22		하드코드된 비밀번호	O	O		CWE-798, CWE-259	
23		충분하지 않은 키 길이 사용		O		CWE-326, Link	
24		적절하지 않은 난수값 사용	O	O		CWE-330	
25		하드코드된 암호화 키		O		CWE-798, CWE-259	
26		취약한 비밀번호 허용				CWE-521	
27		사용자 하드디스크 저장되는 쿠키를 통한 정보노출				CWE-539 ✗	
28		주석문 안에 포함된 시스템 주요정보				CWE-615	
29		솔트 없이 일방향 해쉬 함수 사용				CWE-759	
30		무결성 검사없는 코드 다운로드				CWE-494 ✗	
31		반복된 인증시도 제한 기능 부재				CWE-307 ✗	
32	시간 및 상태	경쟁조건: 검사시점과 사용시점 (TOCTOU)				CWE-367 ✗	
33		종료되지 않은 반복문 또는 재귀 함수	O			CWE-835 ✗	
34	에러처리	오류 메시지를 통한 정보노출			O	CWE-209 ✗	
35		오류 상황 대응 부재			O	CWE-390 ✗	
36		부적절한 예외 처리	O		O	CWE-754	
37	코드오류	Null Pointer 역참조	O		O	CWE-476	
38		부적절한 자원 해제	O		O	CWE-404 ✗	
39		해제된 자원 사용				CWE-416 (C language)	
40		초기화되지 않은 변수 사용				CWE-457 (C language)	
41	캡슐화	잘못된 세션에 의한 데이터 정보노출				CWE-488, CWE-543 ✗	
42		제거되지 않고 남은 디버그 코드				CWE-489 ✗	

43		시스템 데이터 정보노출				CWE-497	System.err.print(e.getMessage())
44		Public 메소드부터 반환된 Private 배열	O		O	CWE-495	
45		Private 배열에 Public 데이터 할당			O	CWE-496	
46	API 오용	DNS Lookup에 의존한 보안결정				CWE-247	
47		취약한 API 사용				CWE-676	