

SonarQube Project 메뉴 - Security Reports

이 문서는 SonarQube Project 메뉴 중 Security Reports에 대한 가이드를 공유하기 위해 작성되었다.

도구명	Sonarqube Enterprise
버전	9.5
비고	

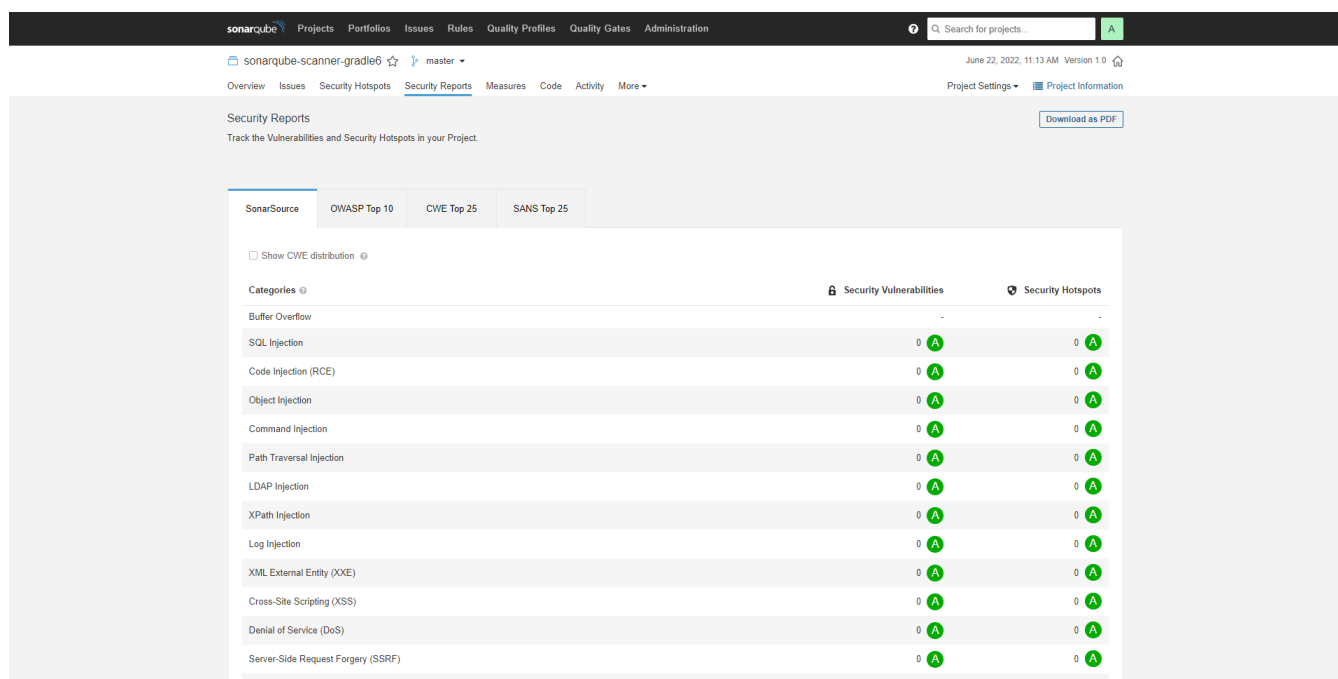
- [SonarQube Project 메뉴 - Security Reports](#)
 - [Security Reports](#)
 - [각 화면 설명](#)
- [참조](#)

 해당 기능은 Enterprise 버전부터 사용가능하다.

SonarQube Project 메뉴 - Security Reports

Security Reports

프로젝트의 취약점 및 보안 핫스팟을 확인하고 PDF로 다운 받을 수 있다.



The screenshot shows the SonarQube Security Reports page for a project named 'sonarqube-scanner-gradle6'. The page has a dark header with navigation links: Projects, Portfolios, Issues, Rules, Quality Profiles, Quality Gates, and Administration. A search bar is on the right. Below the header, the 'Security Reports' tab is selected, showing a table of security vulnerabilities and hotspots. The table has columns for 'Security Vulnerabilities' and 'Security Hotspots'. The 'Security Vulnerabilities' column shows a list of categories like Buffer Overflow, SQL Injection, Code Injection (RCE), Object Injection, Command Injection, Path Traversal Injection, LDAP Injection, XPath Injection, Log Injection, XML External Entity (XXE), Cross-Site Scripting (XSS), Denial of Service (DoS), and Server-Side Request Forgery (SSRF). Each category has a count of 0 and a grade of 'A'. The 'Security Hotspots' column also shows a count of 0 and a grade of 'A'. A 'Download as PDF' button is visible in the top right corner of the report area.

각 화면 설명

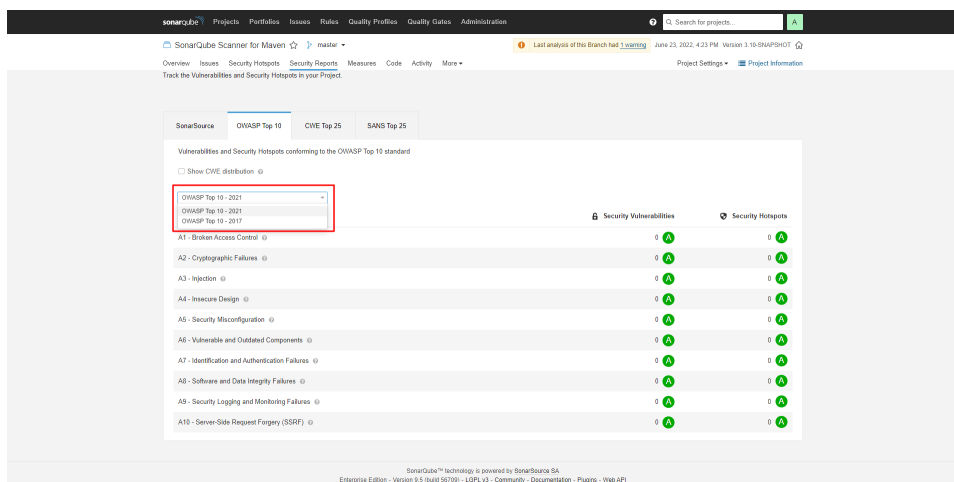
1. SonarSource: Quality Gate를 토대로 취약점 및 보안 핫스팟을 보여준다.



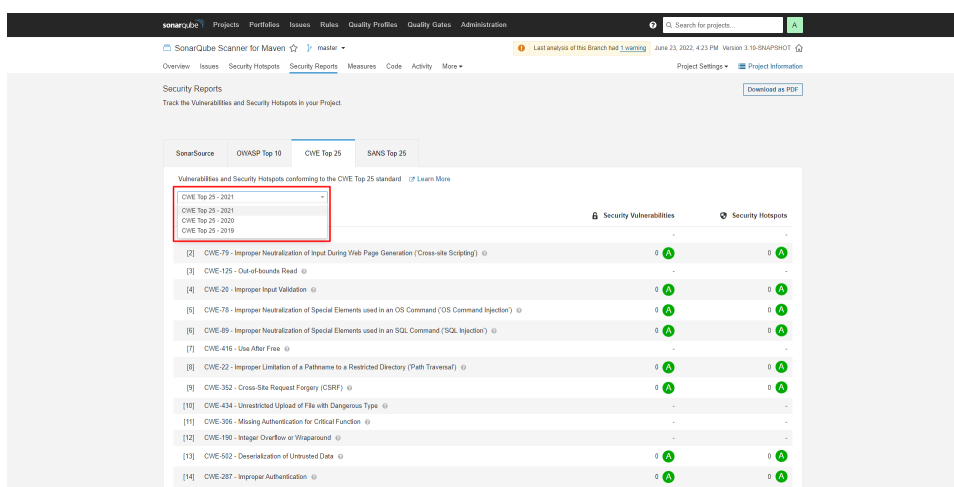
Security Reports는 Quality Profile에 의존한다. Quality Profile에서 활성화된 특정 OWASP,CWE 범주에 해당하는 규칙이 없는 경우 표시되는 등급은 A

Quality Profile에서 더 많은 Rule을 활성화해야한다.

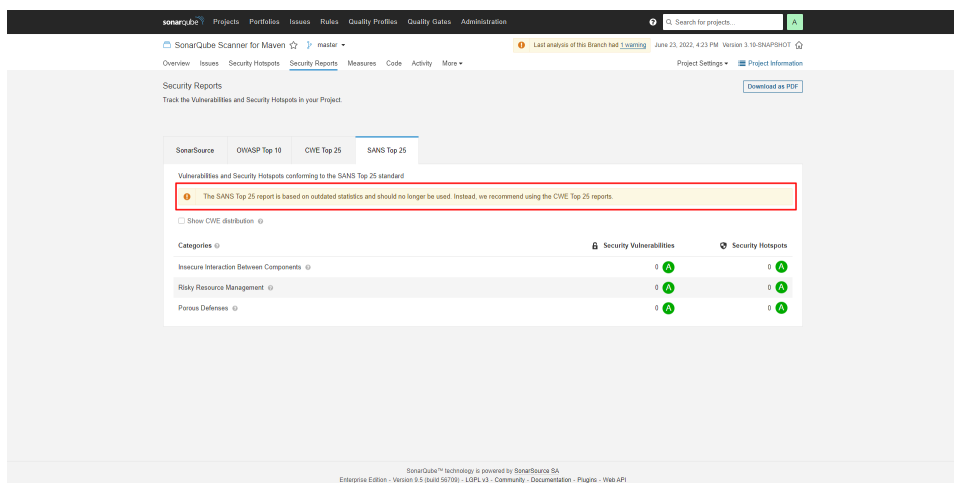
2. OWASP Top 10: 악용가능성, 탐지가능성 및 영향에 대해 빈도수가 높고 보안상 영향을 크게 줄 수 있는 10가지 웹 애플리케이션 보안 취약점 목록 연도를 선택 할 수 있다.



3. CWE Top 25: SANS 연구소에서 발표한 25대 소프트웨어 주요 취약점 연도를 선택 할 수 있다.



4. SANS Top 25: 오래된 자료, CWE Top 25 사용 오래된 자료로 추천하지 않는다.



Sonarqube

- [Sonarqube Docs-Security Reports](#)