# 행정안전부 소프트웨어 보안약점 진단 for SonarQube 소개

이 문서는 커브(CURVC)에서 개발한 행정안전부 소프트웨어 보안약점 진단 플러그인 정보를 공유하기 위해 작성되었다.



## 행정안전부 소프트웨어 보안약점 진단

커브(CURVC)에서 개발한 행정안전부 소프트웨어 보안 취약점 진단 플러그인은 총 47개의 보안 약점 중 소프트웨어 도구로 찾을 수 있는 33개의 보안 약점을 지원하고 있습니다. 플러그인에서 제공되는 모든 룰에 대한 설명은 한글화 지원으로 보다 쉽게 파악이 가능합니다.

### 주요기능

커브(CURVC)에서 개발한 행정안전부 소프트웨어 보안약점 진단 플러그인의 주요 기능은 다음과 같습니다.

- Java 33개의 룰 지원
  행정안전부 소프트웨어 보안약점 47개 중 33개의 보안 약점을 지원합니다.
- 한국어 지원
  SonarQube로 검출된 행정안전부 소프트웨어 보안약점의 한글 100% 지원합니다.
- 보안약점 진단 보고서
  SonarQube로 검출된 행정안전부 소프트웨어 보안약점 PDF 파일을 제공합니다.

### 세부설명

#### 행정안전부 소프트웨어 보안약점 Java 33개 룰(Rule) 지원

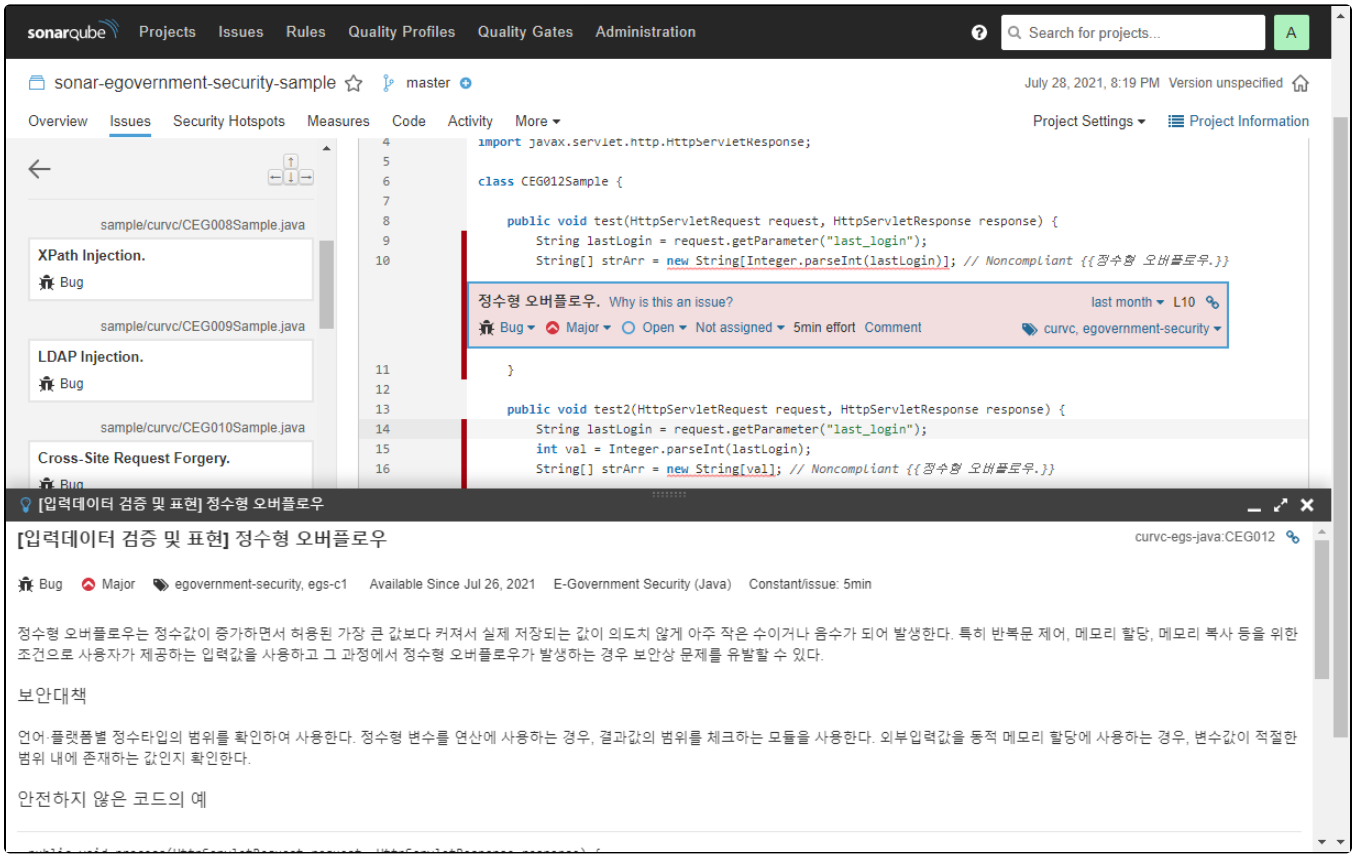
행정안전부 소프트웨어 보안약점 진단 플러그인은 총 47 개의 보약 약점 중 소프트웨어 도구로 찾을 수 있는 33개의 보안 약점을 지원하고 있습니다. 다음은 플러그인에서 행정안전부 소프트웨어 보안약점 지원 룰셋을 보여주고 있습니다.

| Categories | Rule | Type | Severity |
|---|---|---|---|
| 입력데이터 검증 및 표현 | 1.1 SQL 삽입 | Bug | Major |
| | 1.2 경로 조작 및 자원 삽입 | Bug | Major |
| | 1.3 크로스사이트 스크립트 | Bug | Major |
| | 1.4 운영체제 명령어 삽입 | Bug | Major |
| | 1.6 신뢰되지 않는 URL 주소로 자동접속 연결 | Bug | Major |
| | 1.7 XQuery 삽입 | Bug | Major |
| | 1.8 XPath 삽입 | Bug | Major |
| | 1.9 LDAP 삽입 | Bug | Major |
| | 1.10 크로스사이트 요청위조 | Bug | Major |
| | 1.11 HTTP 응답분할 | Bug | Major |
| | 1.12 정수형 오버플로우 | Bug | Major |
| | 1.15 포맷 스트링 삽입 | Bug | Major |
| 보안기능 | 2.3 중요한 자원에 대한 잘못된 권한 설정 | Bug | Major |
| | 2.4 취약한 암호화 알고리즘 사용 | Bug | Major |
| | 2.6 중요정보 평문전송 | Bug | Major |
| | 2.7 하드코드된 비밀번호 | Bug | Major |

| | | | |
|---|---|---|---|
| | 2.8 충분하지 않은 키 길이 사용 | Bug | Major |
| | 2.9 적절하지 않은 난수값 사용 | Bug | Major |
| | 2.10 하드코드된 암호화 키 | Bug | Major |
| | 2.12 사용자 하드디스크 저장되는 쿠키를 통한 정보노출 | Bug | Major |
| | 2.13 주석문 안에 포함된 시스템 주요정보 | Bug | Major |
| | 2.14 솔트 없이 일방향 해쉬 함수 사용 | Bug | Major |
| | 2.15 무결성 검사없는 코드 다운로드 | Bug | Major |
| 시간 및 상태 | 3.2 종료되지 않은 반복문 또는 재귀 함수 | Bug | Major |
| 에러처리 | 4.1 오류 메시지를 통한 정보노출 | Bug | Major |
| | 4.2 오류 상황 대응 부재 | Bug | Major |
| | 4.3 부적절한 예외 처리 | Bug | Major |
| 캡슐화 | 6.2 제거되지 않고 남은 디버그 코드 | Bug | Major |
| | 6.3 시스템 데이터 정보노출 | Bug | Major |
| | 6.4 Public 메소드부터 반환된 Private 배열 | Bug | Major |
| | 6.5 Private 배열에 Public 데이터 할당 | Bug | Major |
| API 오용 | 7.1 DNS Lookup에 의존한 보안결정 | Bug | Major |
| | 7.2 취약한 API 사용 | Bug | Major |

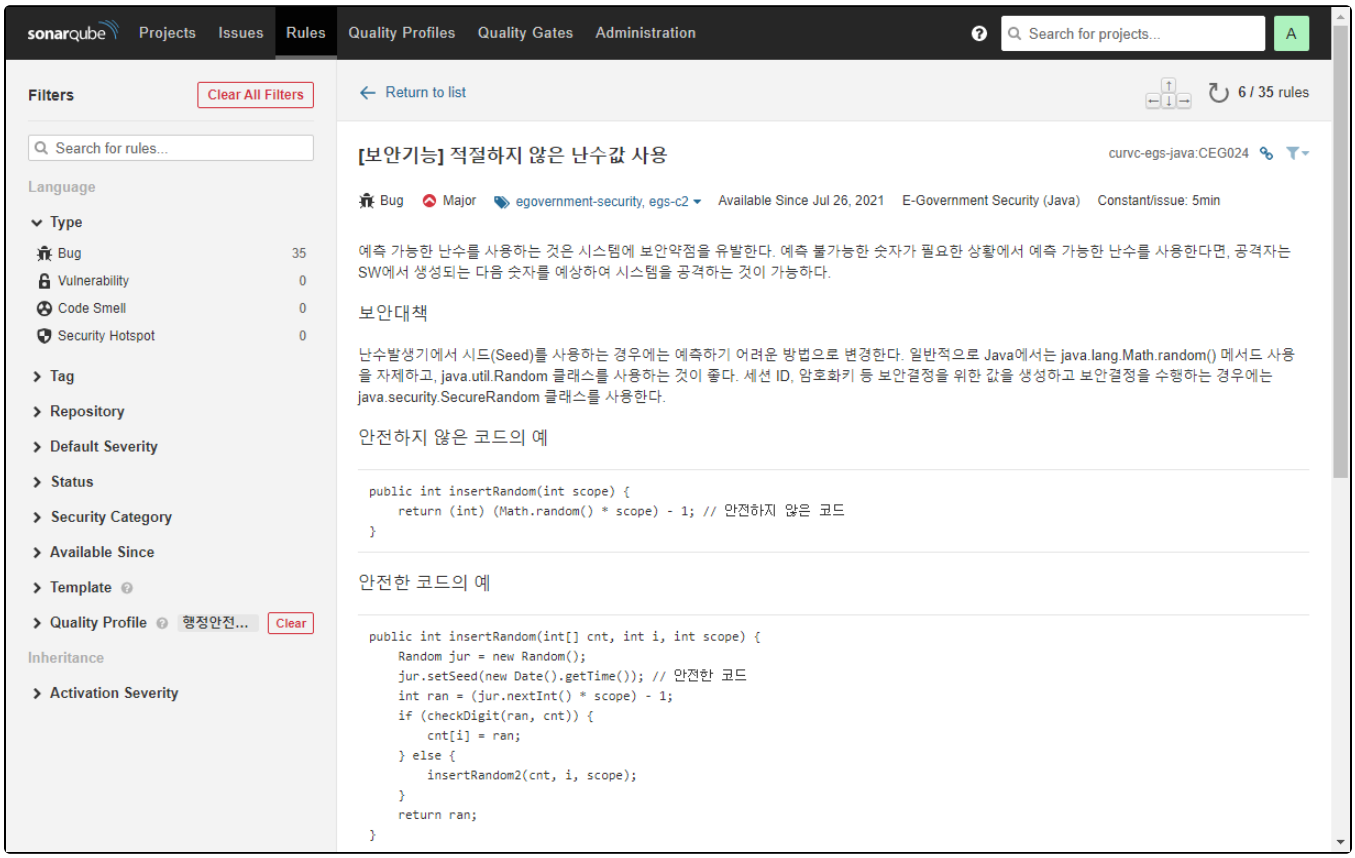
## 행정안전부 소프트웨어 보안약점 진단 수행

행정안전부 소프트웨어 보안약점은 진단은 플러그인 설치시 자동으로 만들어지는 "행정안전부 보안약점" 프로파일을 프로젝트로 설정 후 Sonar Scanner 를 수행하면 됩니다.



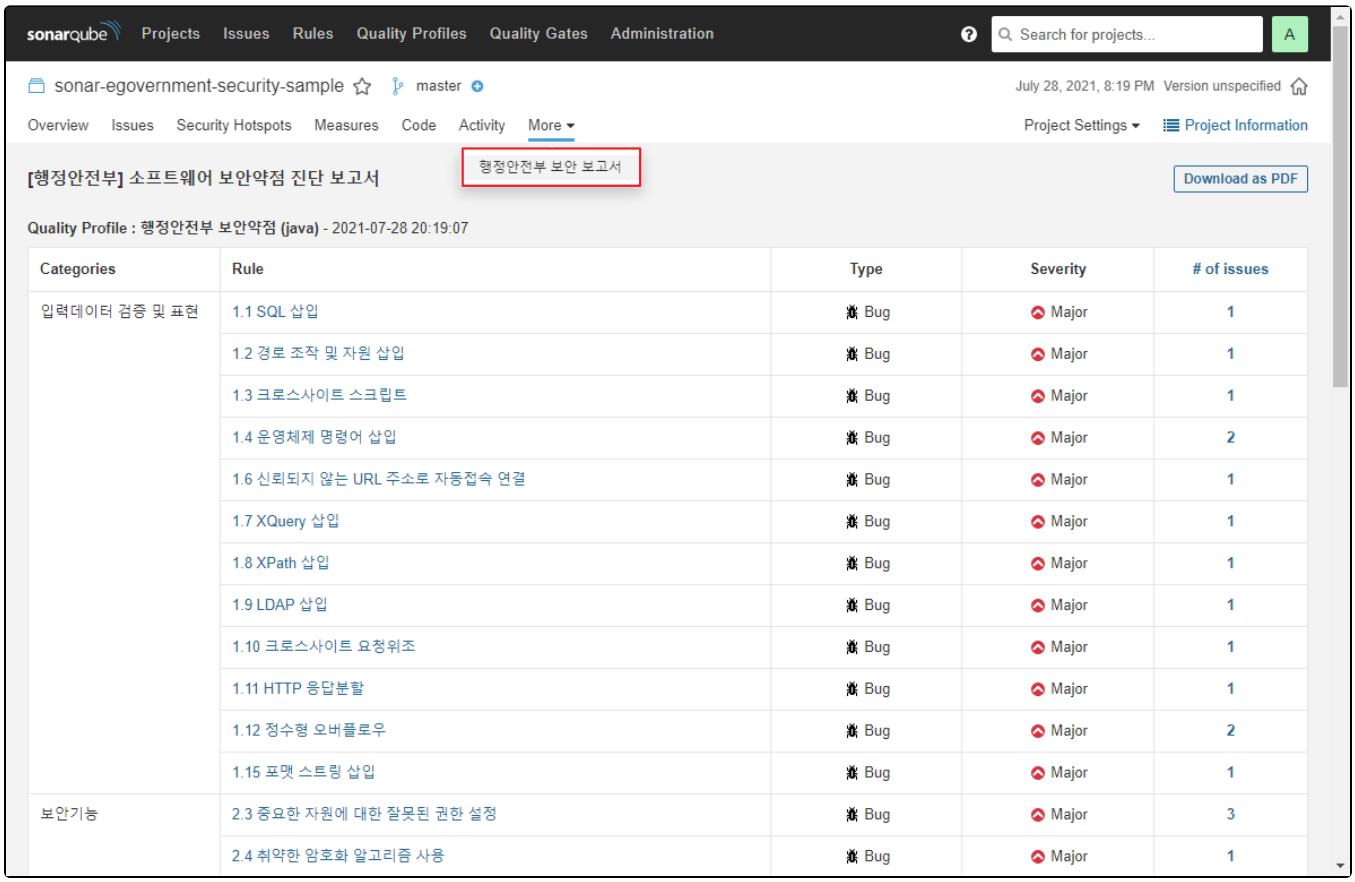

## 소프트웨어 보안약점 설명 한글화 지원

플러그인에서 제공되는 모든 룰 명 및 룰에 대한 설명은 100% 한글화가 지원됩니다.




## 행정안전부 소프트웨어 보안약점 진단 보고서

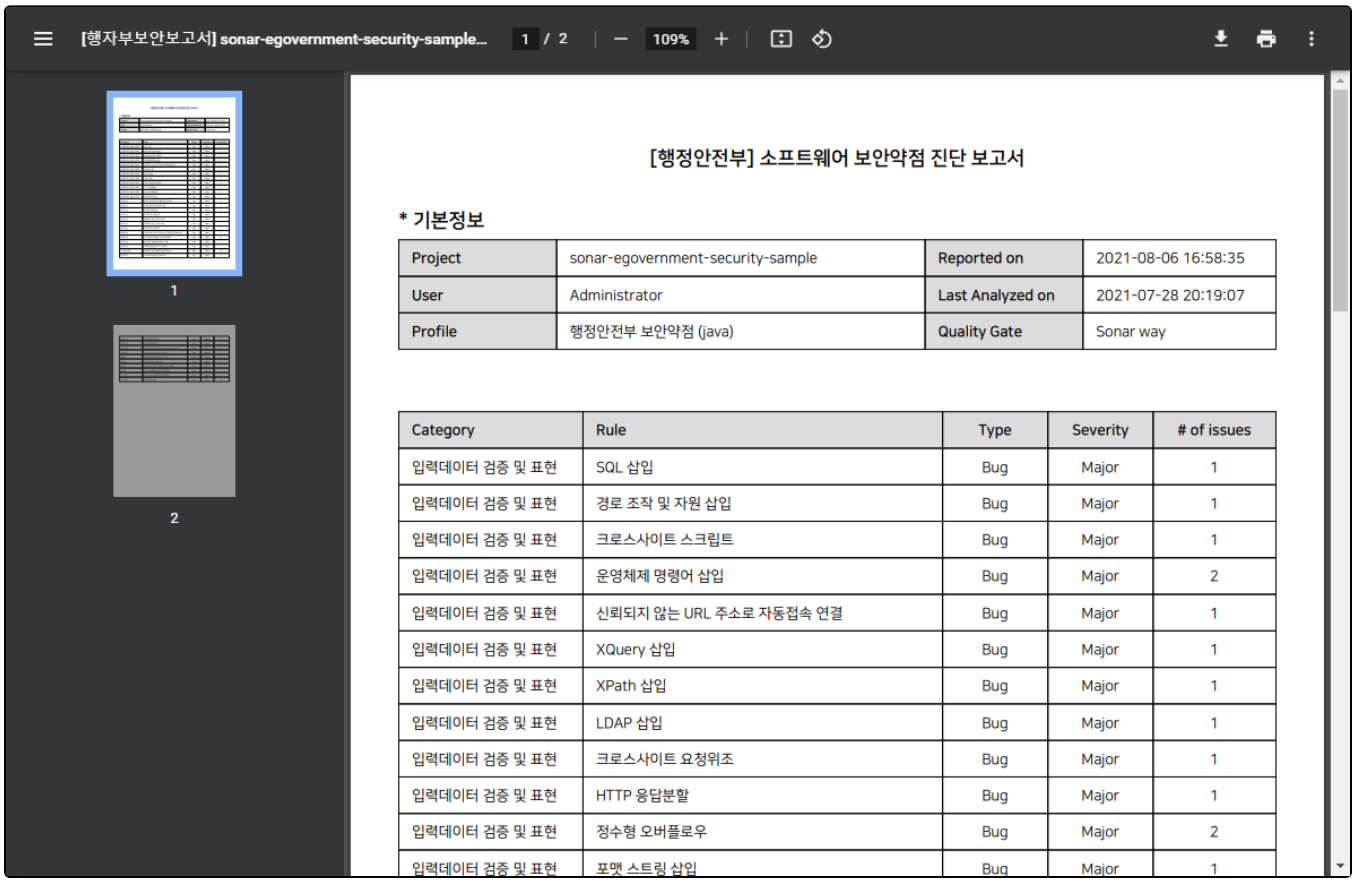
특정 프로젝트 진입 후 상단 More 메뉴에서 행정안전부 보안 보고서를 선택하면 다음과 그림같이 진단 보고서를 확인할 수 있습니다.




| Categories | Rule | Type | Severity | # of issues |
|---|---|---|---|---|
| 입력데이터 검증 및 표현 | 1.1 SQL 삽입 | Bug | Major | 1 |
| | 1.2 경로 조작 및 자원 삽입 | Bug | Major | 1 |
| | 1.3 크로스사이트 스크립트 | Bug | Major | 1 |
| | 1.4 운영체제 명령어 삽입 | Bug | Major | 2 |
| | 1.6 신뢰되지 않는 URL 주소로 자동접속 연결 | Bug | Major | 1 |
| | 1.7 XQuery 삽입 | Bug | Major | 1 |
| | 1.8 XPath 삽입 | Bug | Major | 1 |
| | 1.9 LDAP 삽입 | Bug | Major | 1 |
| | 1.10 크로스사이트 요청위조 | Bug | Major | 1 |
| | 1.11 HTTP 응답분할 | Bug | Major | 1 |
| | 1.12 정수형 오버플로우 | Bug | Major | 2 |
| | 1.15 포맷 스트링 삽입 | Bug | Major | 1 |
| 보안기능 | 2.3 중요한 자원에 대한 잘못된 권한 설정 | Bug | Major | 3 |
| | 2.4 취약한 암호화 알고리즘 사용 | Bug | Major | 1 |

## 소프트웨어 보안약점 진단 보고서 PDF 출력

Downloads as PDF 클릭 시, PDF 본을 다운로드 할 수 있으며, 다음과 같은 소프트웨어 보안약점 진단 보고서를 얻을 수 있습니다.




## [행정안전부] 소프트웨어 보안약점 진단 보고서

### * 기본정보

| | | | |
|---|---|---|---|
| Project | sonar-egovernment-security-sample | Reported on | 2021-08-06 16:58:35 |
| User | Administrator | Last Analyzed on | 2021-07-28 20:19:07 |
| Profile | 행정안전부 보안약점 (java) | Quality Gate | Sonar way |

| Category | Rule | Type | Severity | # of issues |
|---|---|---|---|---|
| 입력데이터 검증 및 표현 | SQL 삽입 | Bug | Major | 1 |
| 입력데이터 검증 및 표현 | 경로 조작 및 자원 삽입 | Bug | Major | 1 |
| 입력데이터 검증 및 표현 | 크로스사이트 스크립트 | Bug | Major | 1 |
| 입력데이터 검증 및 표현 | 운영체제 명령어 삽입 | Bug | Major | 2 |
| 입력데이터 검증 및 표현 | 신뢰되지 않는 URL 주소로 자동접속 연결 | Bug | Major | 1 |
| 입력데이터 검증 및 표현 | XQuery 삽입 | Bug | Major | 1 |
| 입력데이터 검증 및 표현 | XPath 삽입 | Bug | Major | 1 |
| 입력데이터 검증 및 표현 | LDAP 삽입 | Bug | Major | 1 |
| 입력데이터 검증 및 표현 | 크로스사이트 요청위조 | Bug | Major | 1 |
| 입력데이터 검증 및 표현 | HTTP 응답분할 | Bug | Major | 1 |
| 입력데이터 검증 및 표현 | 정수형 오버플로우 | Bug | Major | 2 |
| 입력데이터 검증 및 표현 | 포맷 스트링 삽입 | Bug | Major | 1 |