

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
 - 주요기능
 - 세부설명
 - 행정안전부 소프트웨어 보안약점 Java 33개 룰(Rule) 지원
 - 행정안전부 소프트웨어 보안약점 진단 수행
 - 소프트웨어 보안약점 설명 한글화 지원
 - 행정안전부 소프트웨어 보안약점 진단 보고서
 - 소프트웨어 보안약점 진단 보고서 PDF 출력

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 보안 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 경수형 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 하드코딩된 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.

The screenshot displays the SonarQube web interface. The top navigation bar includes 'sonarqube', 'Projects', 'Issues', 'Rules', 'Quality Profiles', 'Quality Gates', and 'Administration'. A search bar is present on the right. The main content area shows the 'Issues' tab for a project named 'sonar-egovement-security-sample'. A list of issues is shown on the left, including 'XPath Injection.', 'LDAP Injection.', and 'Cross-Site Request Forgery.'. The selected issue is '정수형 오버플로우' (Integer Overflow), which is categorized as a 'Bug' with a 'Major' severity. The issue description explains that integer overflow occurs when a value increases beyond the maximum allowed, leading to unexpected behavior. It also provides a link to the ' CWE-190: Integer Overflow or Underflow ' rule. The code snippet on the right shows the problematic line: `String[] strArr = new String[Integer.parseInt(lastLogin)];`. Below the main content, there is a detailed description of the issue in Korean, including a section for '안전하지 않은 코드의 예' (Example of unsafe code).

소프트웨어 보안약점 설명 한글화 지원

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

Filters [Clear All Filters](#) [Return to list](#) 6 / 35 rules

Search for rules...

Language

Type

- Bug 35
- Vulnerability 0
- Code Smell 0
- Security Hotspot 0

Tag

Repository

Default Severity

Status

Security Category

Available Since

Template

Quality Profile [행정안전...](#) [Clear](#)

Inheritance

Activation Severity

[보안기능] 적절하지 않은 난수값 사용 curvc-egs-java:CEG024

Bug **Major** **egovernment-security, egs-c2** Available Since Jul 26, 2021 E-Government Security (Java) Constant/issue: 5min

예측 가능한 난수를 사용하는 것은 시스템에 보안약점을 유발한다. 예측 불가능한 숫자가 필요한 상황에서 예측 가능한 난수를 사용한다면, 공격자는 SW에서 생성되는 다음 숫자를 예상하여 시스템을 공격하는 것이 가능하다.

보안대책

난수발생기에서 시드(Seed)를 사용하는 경우에는 예측하기 어려운 방법으로 변경한다. 일반적으로 Java에서는 `java.lang.Math.random()` 메서드를 사용하고, `java.util.Random` 클래스를 사용하는 것이 좋다. 세션 ID, 암호화키 등 보안결정을 위한 값을 생성하고 보안결정을 수행하는 경우에는 `java.security.SecureRandom` 클래스를 사용한다.

안전하지 않은 코드의 예

```
public int insertRandom(int scope) {
    return (int) (Math.random() * scope) - 1; // 안전하지 않은 코드
}
```

안전한 코드의 예

```
public int insertRandom(int[] cnt, int i, int scope) {
    Random jur = new Random();
    jur.setSeed(new Date().getTime()); // 안전한 코드
    int ran = (jur.nextInt() * scope) - 1;
    if (checkDigit(ran, cnt)) {
        cnt[i] = ran;
    } else {
        insertRandom2(cnt, i, scope);
    }
    return ran;
}
```

행정안전부 소프트웨어 보안약점 진단 보고서

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

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration ? Search for projects... A

sonar-egovernment-security-sample ☆ master July 28, 2021, 8:19 PM Version unspecified

Overview Issues Security Hotspots Measures Code Activity **More** Project Settings Project Information

[행정안전부] 소프트웨어 보안약점 진단 보고서 행정안전부 보안 보고서 Download as PDF

Quality Profile : 행정안전부 보안약점 (java) - 2021-07-28 20:19:07

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.



1



2