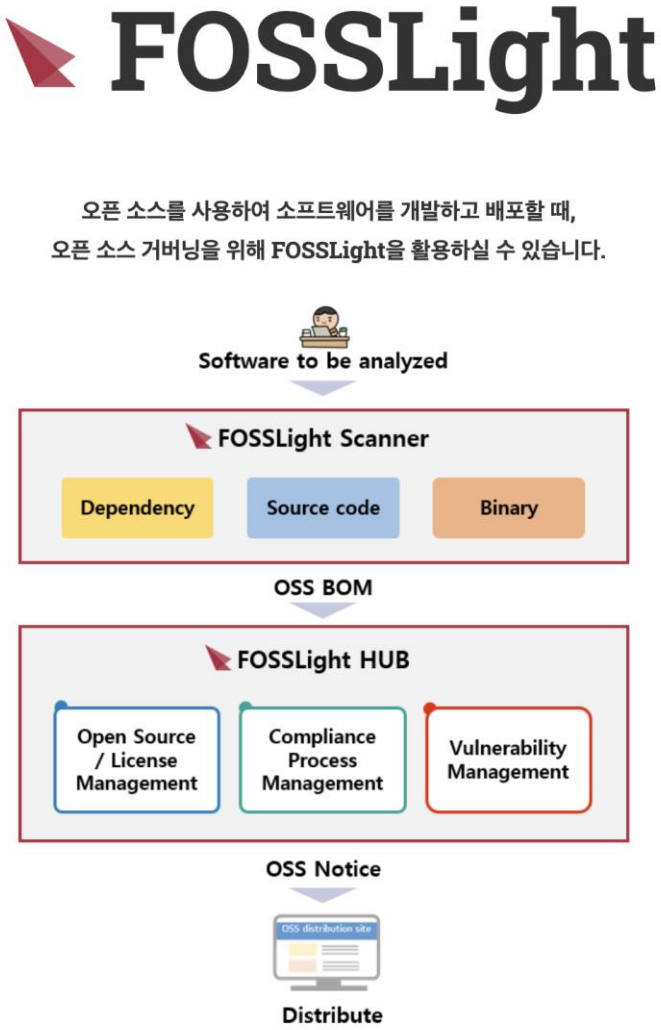
입문자를 위한 FOSSLight 소개

LG전자 김경애

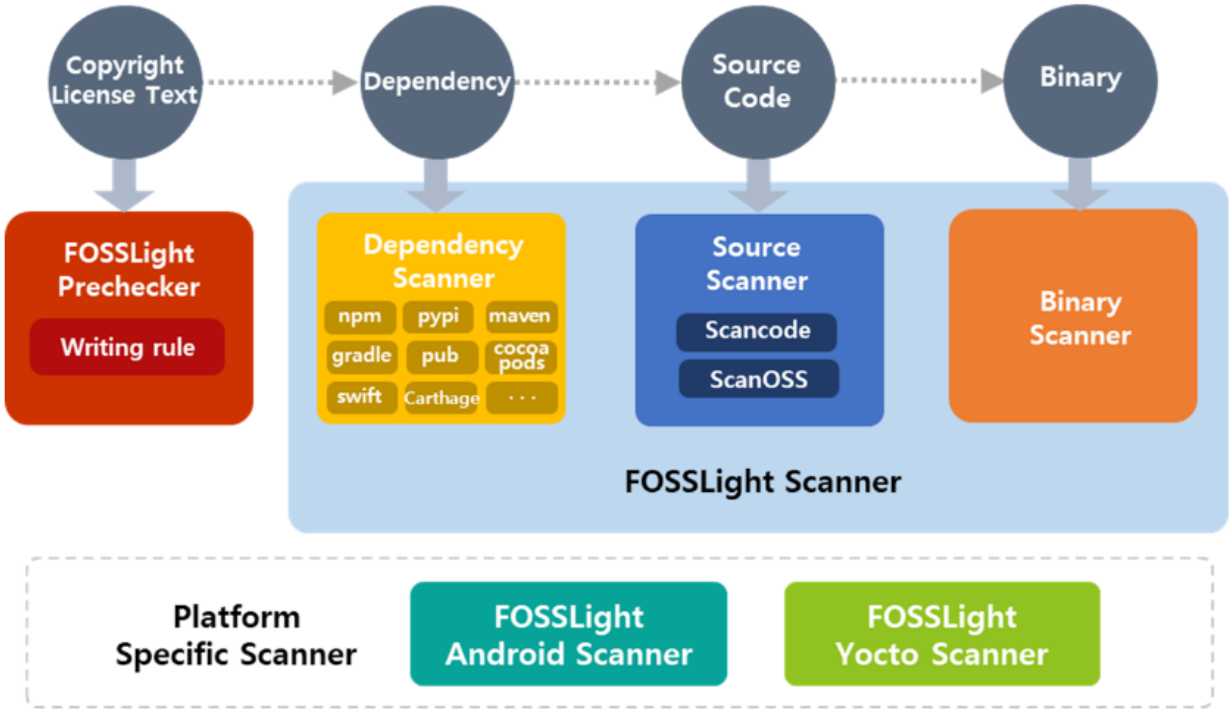
LG Open Source

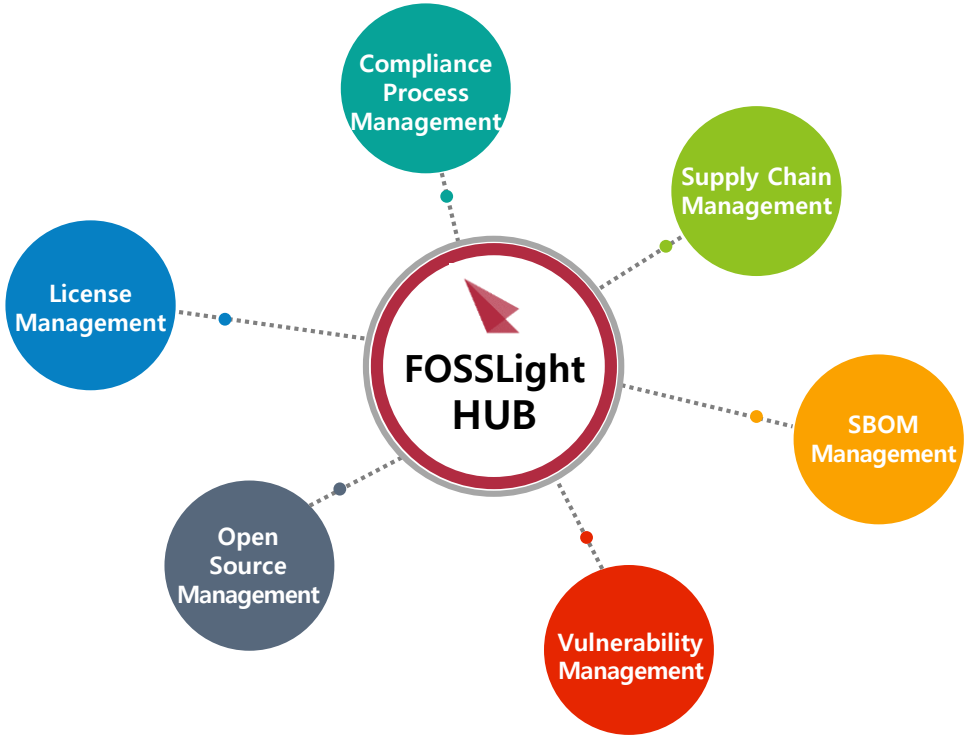
기업의 오픈소스 관리 방안

FOSSLight Open Source Project



FOSSLight





https://fosslight.org/

오픈소스 분석 도구

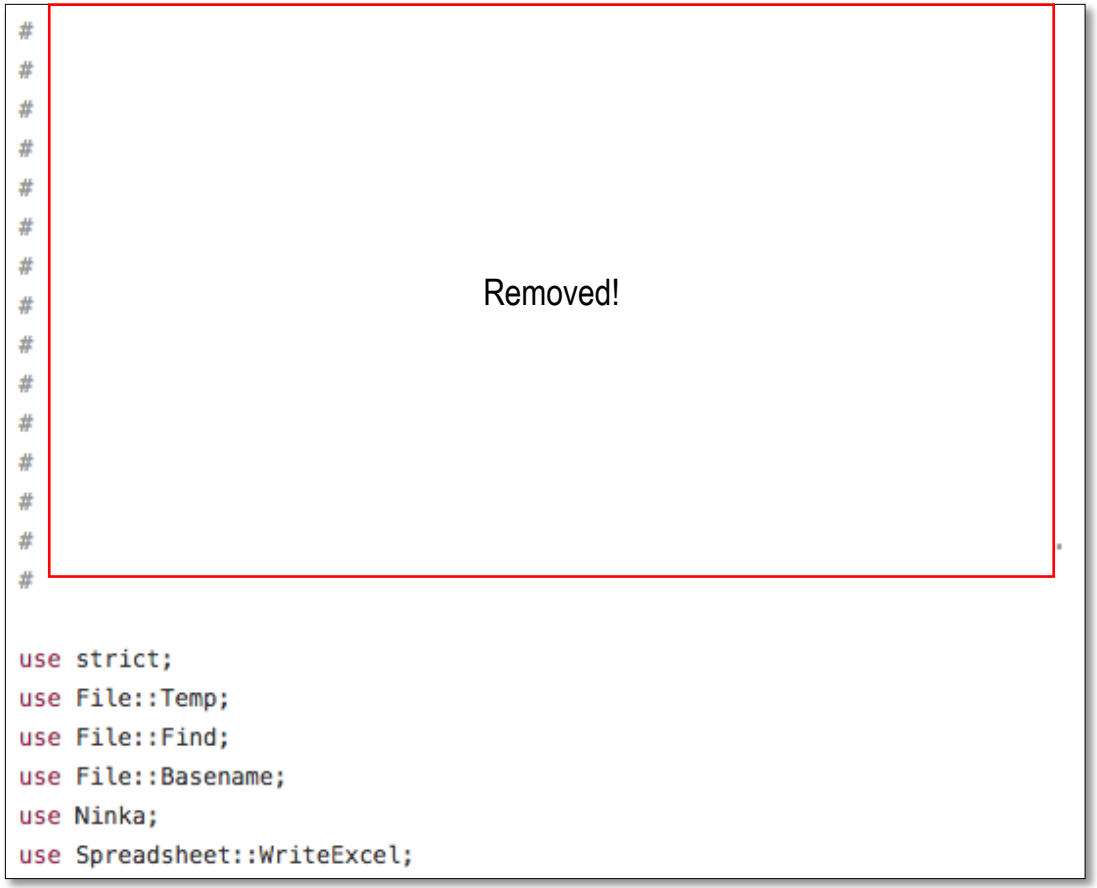
텍스트 스캐닝 도구

- 소스 코드 내 텍스트를 검색하여 자동으로 라이선스 확인

```
#    Copyright (C) 2014,2015  Anthony Kohan and Daniel M. German
#
#    This program is free software; you can redistribute it and/or
#    modify it under the terms of the GNU General Public License as
#    published by the Free Software Foundation; either version 2 of
#    the License, or (at your option) any later version.
#
#    This program is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
#    General Public License for more details.
#
#    You should have received a copy of the GNU General Public License
#    along with this program.  If not, see <http://www.gnu.org/licenses/>.
#

use strict;
use File::Temp;
use File::Find;
use File::Basename;
use Ninka;
use Spreadsheet::WriteExcel;
```

텍스트 스캐닝 도구 약점

- 소스 코드 내 라이선스 문구가 변경 혹은 삭제되었다면?



- 텍스트 검출 도구는 라이선스 문구가 지워진 소스에서는 라이선스 검출을 할 수 없음.

코드 스캐닝 도구

- 오픈소스 데이터베이스 구축
- 사용자의 소스 코드와 데이터베이스의 소스 코드와 비교하여 일치하는 오픈소스 검출

코드 스캐닝 도구의 동작 방식

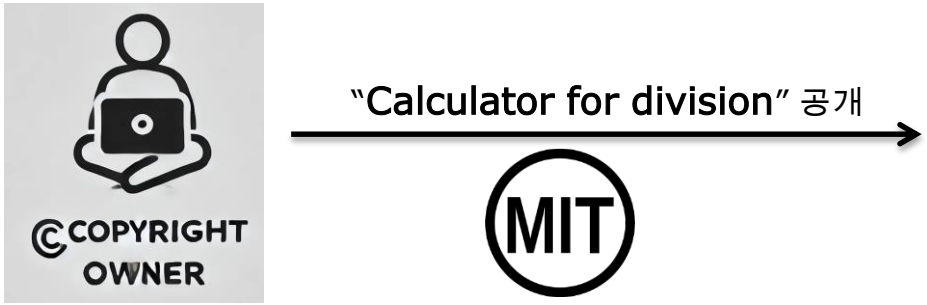
- 한 개발자가 나눗셈용 계산기 프로그램 작성 : “Calculator for division”
- 이를 GitHub에 공개하면서 MIT License 적용함

“Calculator for division” 공개


```
 * Copyright(c) 2014 example,
 *
 * License : MIT
 */

#include <stdio.h>
#include <string.h>

#define NUMSIZE 16
#define OPERSIZE 5

int divide(int a, int b)
{
    return a / b;
}
```

코드 스캐닝 도구의 동작 방식

- 코드 스캐닝 도구는 해당 Code를 취득하여 데이터베이스에 저장함




```
 * Copyright(c) 2014 example,
 *
 * License : MIT
 */

#include <stdio.h>
#include <string.h>

#define NUMSIZE 16
#define OPERSIZE 5

int divide(int a, int b)
{
    return a / b;
}
```

snippet	OSS name	License

`int divide(int a, int b)`
`{`
`  return a / b;`
`}`
	Calculator for division	MIT License

코드 스캐닝 도구의 동작 방식

- 어떤 개발자가 Project 개발에 "Calculator for division"의 소스 코드를 사용
  - 라이선스 텍스트는 삭제하고 필요한 함수만 복사해왔다고 가정

"Calculator for division" 복사


```
 * Copyright(c) 2014 example,
 *
 * License : MIT
 */

#include <stdio.h>
#include <string.h>

#define NUMSIZE 16
#define OPERSIZE 5

int divide(int a, int b)
{
    return a / b;
}
```

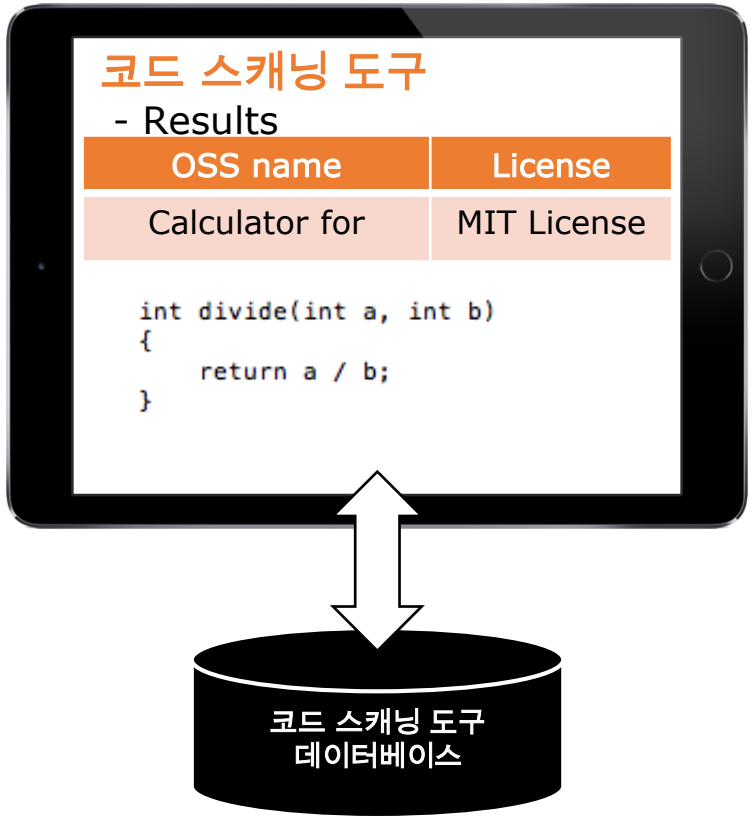
```
 * Copyright (c) 2016 by ABC Electronics Inc.
 * This is core algorism of ABC Electronics.
 */
int sumoper(int a, int b)
{
    return a + b;
}


/*
 * This is a function from an open source file.
 */
int divide(int a, int b)
{
    return a / b;
}
```

코드 스캐닝 도구의 동작 방식 예시

- 라이선스 텍스트가 없기 때문에 텍스트 스캐닝 도구로는 검출 불가
- 코드 스캐닝 도구는 데이터베이스와 소스 코드를 비교하여 일치하는 오픈소스를 찾을 수 있음

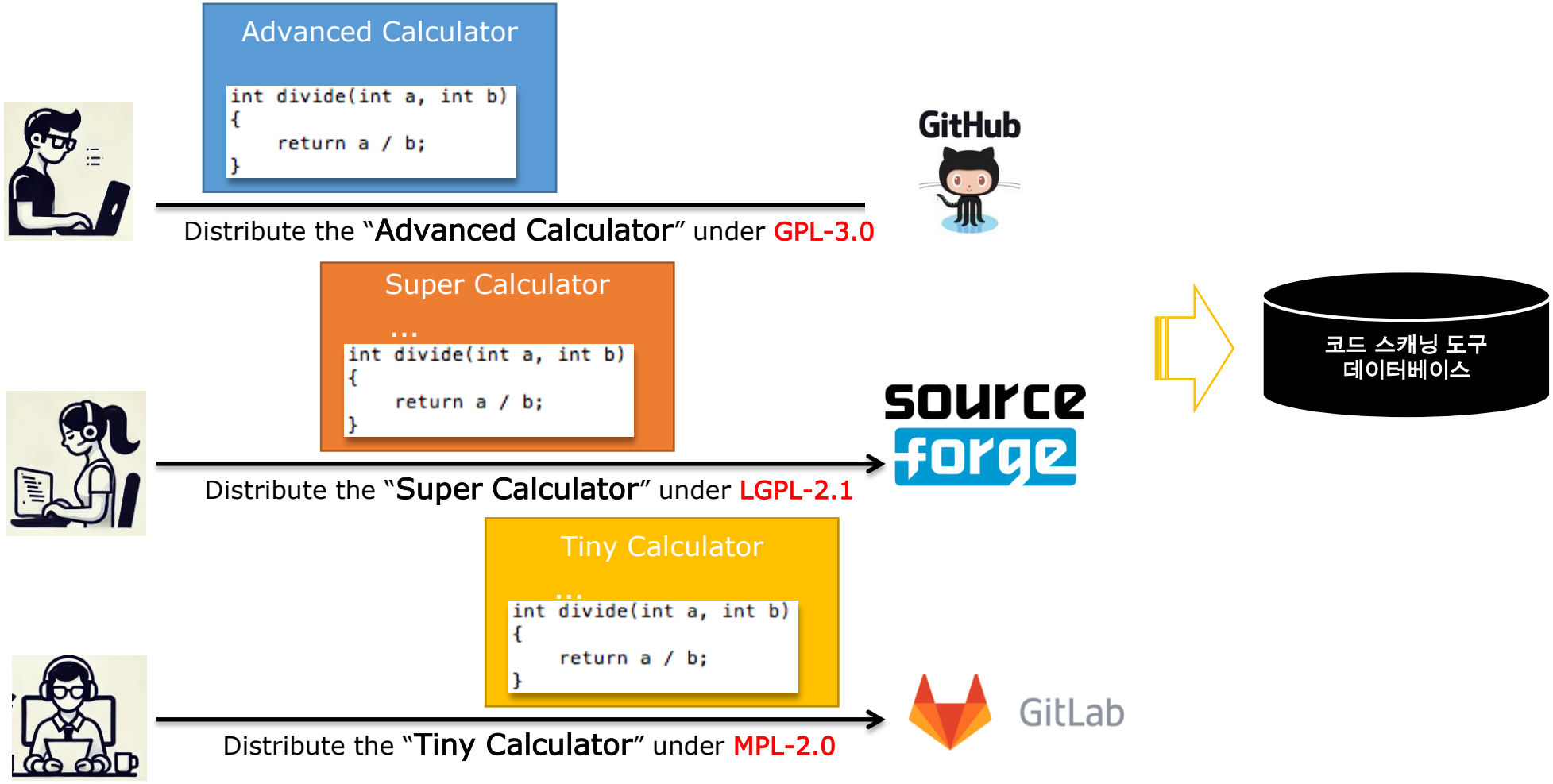
소스 코드 분석

```
 * Copyright (c) 2016 by ABC Electronics Inc.
 * This is core algorism of ABC Electronics.
 */
int sumoper(int a, int b)
{
    return a + b;
}


/*
 * This is a function from an open source file.
 */
int divide(int a, int b)
{
    return a / b;
}
```



코드 스캐닝 도구 약점

- 한 개발자가 MIT 라이선스로 "Calculator for division"을 공개한 후..

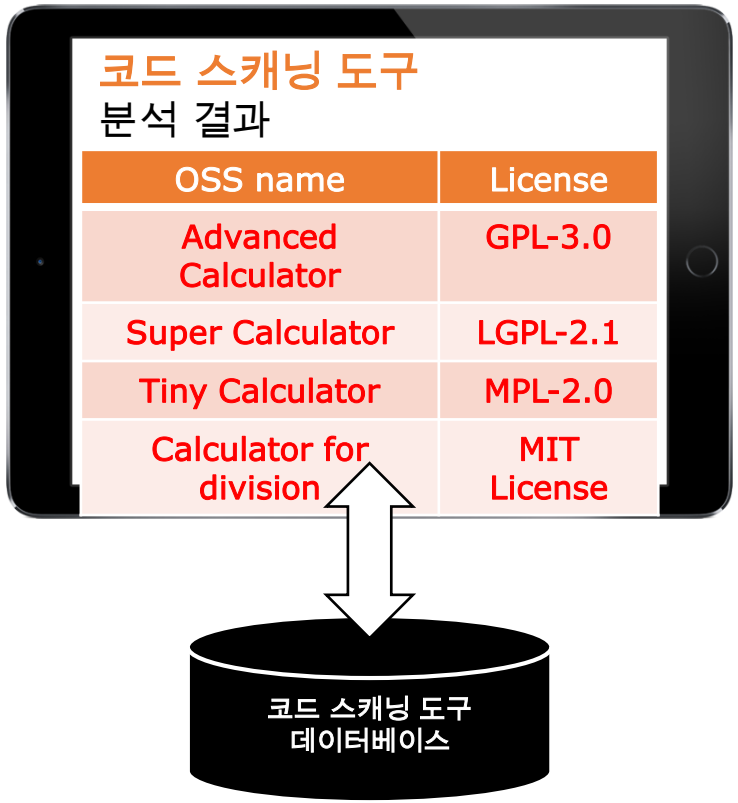


코드 스캐닝 도구 약점

- 사용자가 원 출처를 찾아내야 함

소스 코드 분석

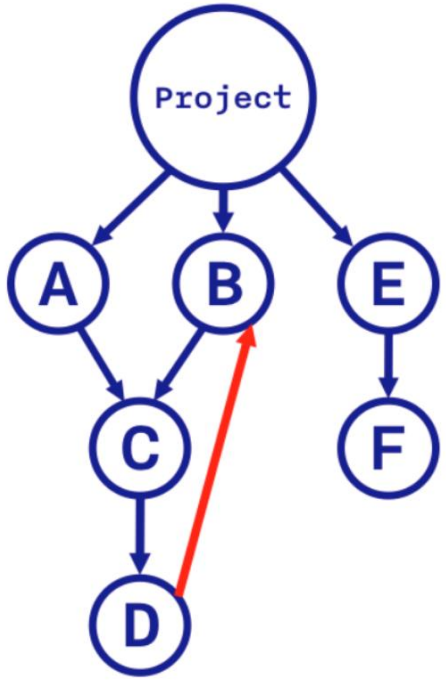
```
 * Copyright (c) 2016 by ABC Electronics Inc.
 * This is core algorism of ABC Electronics.
 */
int sumoper(int a, int b)
{
    return a + b;
}


/*
 * This is a function from an open source file.
 */
int divide(int a, int b)
{
    return a / b;
}
```



디펜던시 분석 (1/2)

- Package Manager에 대한 디펜던시 분석을 지원하는 도구
- Package Manager의 Manifest 파일 자동 감지하여 오픈 소스 정보 분석

- Direct / Transitive Dependency 모두에 대한 오픈 소스 분석이 필요함



디펜던시 분석 (2/2)

twilio-node package.json

```
"dependencies": {
  "@types/express": "^4.11.1",
  "deprecate": "1.0.0",
  "jsonwebtoken": "^8.1.0",
  "lodash": "^4.17.10",
  "moment": "2.19.3",
  "q": "2.0.x",
  "request": "^2.87.0",
  "rootpath": "0.1.2",
  "scmp": "2.0.0",
  "xmlbuilder": "9.0.1"
},
```

@types/express package.json

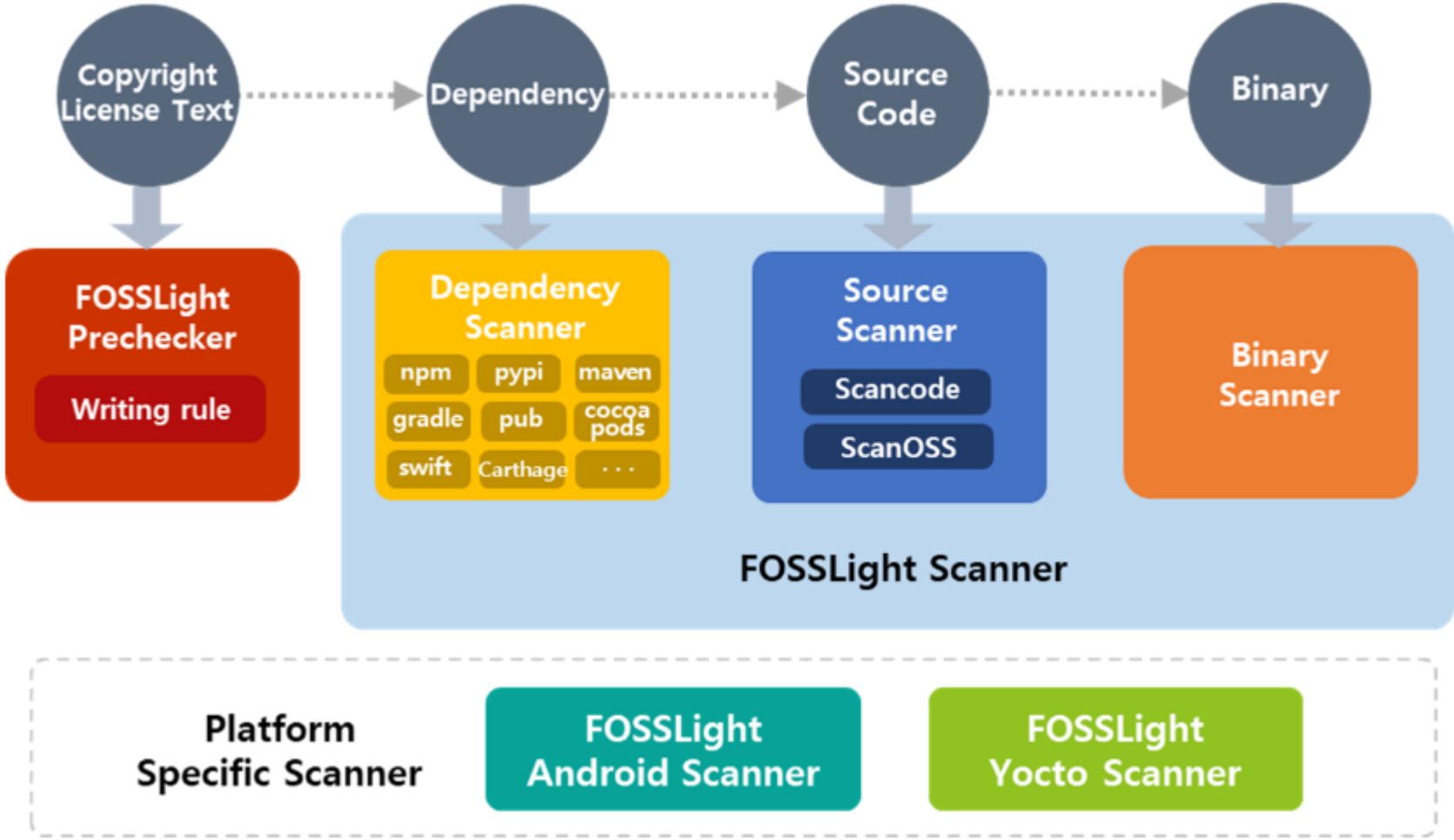
```
"dependencies":{
  "@types/body-parser": "*",
  "@types/express-serve-static-core": "*",
  "@types/serve-static": "*"
},
```

@types/body-parser package.json

```
"dependencies": {
  "@types/connect": "*",
  "@types/node": "*"
},
```

FOSSLight Scanner

FOSSLight Scanner



https://fosslight.org/ko/scanner/

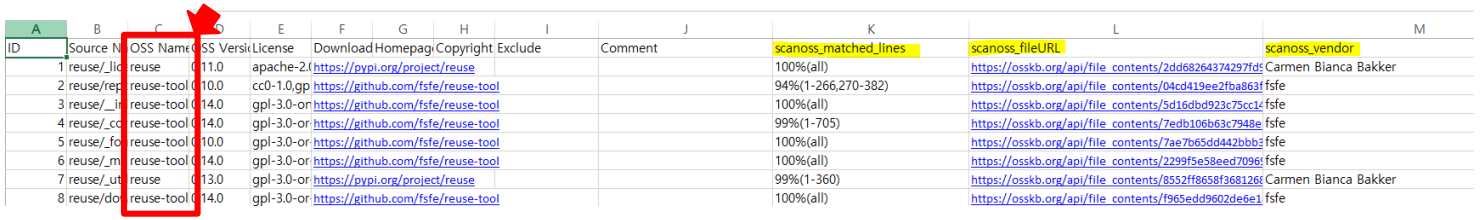
FOSSLight Scanner – Dependency

- Transitive Dependency까지 확인하여 오픈소스 이름 및 버전, 라이선스를 검출함
- 지원 패키지 매니저 : Gradle, Maven, NPM, PIP, Pub, Cocoapods, Swift, Carthage, Go 등

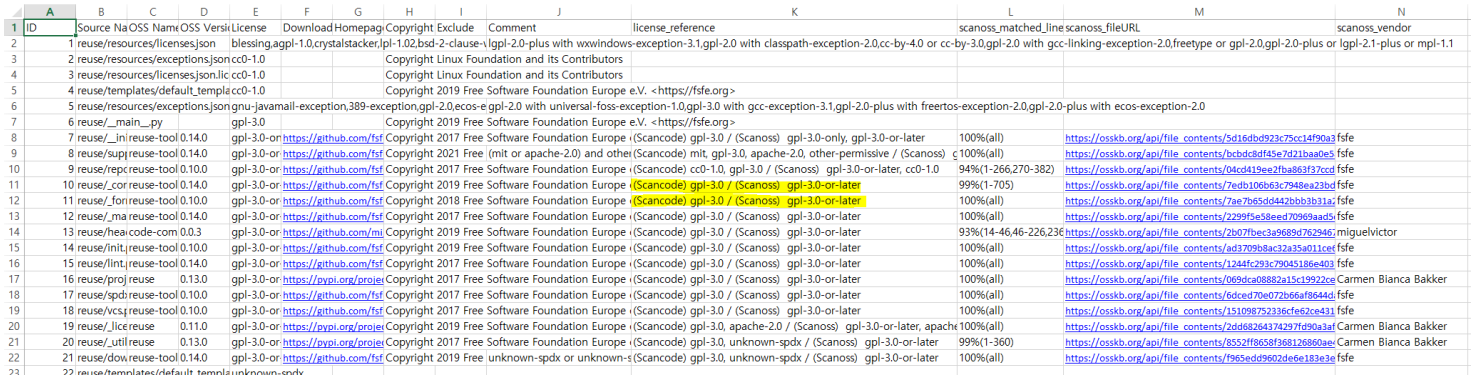
ID	Source Name or	OSS Name	OSS Version	License	Download Location	Homepage
-	[Name of the Sc	[Name of the OSS used i	[Version Number	[License of the C	[Download URL or a specific location within a VCS for the OSS]	[Web site that serves as the OSS's home page]
1	pubspec.yaml	pub:ansicolor	1.0.5	Apache-2.0	https://pub.dev/packages/pub:ansicolor/versions/1.0.5	https://github.com/google/ansicolor-dart
2	pubspec.yaml	pub:async	2.5.0-nullsafety.1	BSD-3-Clause	https://pub.dev/packages/pub:async/versions/2.5.0-nullsafety.1	https://www.github.com/dart-lang/async
3	pubspec.yaml	pub:cached_network_ima	2.3.2+1	MIT	https://pub.dev/packages/pub:cached_network_image/versions/2.3.2+1	https://github.com/Baseflow/flutter_cached_netwo
4	pubspec.yaml	pub:characters	1.1.0-nullsafety.3	BSD-3-Clause	https://pub.dev/packages/pub:characters/versions/1.1.0-nullsafety.3	https://www.github.com/dart-lang/characters
5	pubspec.yaml	pub:charcode	1.2.0-nullsafety.1	BSD-3-Clause	https://pub.dev/packages/pub:charcode/versions/1.2.0-nullsafety.1	https://github.com/dart-lang/charcode
6	pubspec.yaml	pub:clock	1.1.0-nullsafety.1	Apache-2.0	https://pub.dev/packages/pub:clock/versions/1.1.0-nullsafety.1	https://github.com/dart-lang/clock
7	pubspec.yaml	pub:collection	1.15.0-nullsafety.3	BSD-3-Clause	https://pub.dev/packages/pub:collection/versions/1.15.0-nullsafety.3	https://www.github.com/dart-lang/collection
8	pubspec.yaml	pub:console_log_handler	1.1.6	Apache-2.0	https://pub.dev/packages/pub:console_log_handler/versions/1.1.6	https://github.com/MikeMitterer/dart-console_log
9	pubspec.yaml	pub:convert	2.1.1	BSD-3-Clause	https://pub.dev/packages/pub:convert/versions/2.1.1	https://github.com/dart-lang/convert
10	pubspec.yaml	pub:crypto	2.1.5	BSD-3-Clause	https://pub.dev/packages/pub:crypto/versions/2.1.5	https://www.github.com/dart-lang/crypto
11	pubspec.yaml	pub:ffi	0.1.3	BSD-3-Clause	https://pub.dev/packages/pub:ffi/versions/0.1.3	https://github.com/dart-lang/ffi
12	pubspec.yaml	pub:file	5.2.1	BSD-3-Clause	https://pub.dev/packages/pub:file/versions/5.2.1	https://github.com/google/file.dart
13	pubspec.yaml	pub:flutter	1.22.0	BSD-3-Clause	https://pub.dev/packages/pub:flutter/versions/1.22.0	http://flutter.dev
14	pubspec.yaml	pub:flutter_blurhash	0.5.0	MIT	https://pub.dev/packages/pub:flutter_blurhash/versions/0.5.0	https://github.com/fluttercommunity/flutter_blurh
15	pubspec.yaml	pub:flutter_cache_manage	1.4.2	MIT	https://pub.dev/packages/pub:flutter_cache_manager/versions/1.4.2	https://github.com/Baseflow/flutter_cache_manage

FOSSLight Scanner – Source

- 소스 코드를 분석하여 오픈소스 및 버전, 라이선스를 검출
- 여러 스캐너 지원을 통해 String Search뿐만 아니라 Snippet 매칭 지원



ID	Source N	OSS Name	OSS Versi	License	Download	Homepag	Copyright	Exclude	Comment	scanoss_matched_lines	scanoss_fileURL	scanoss_vendor
1	reuse/_lic	reuse	0.11.0	apache-2.(	https://pypi.org/project/reuse					100%(all)	https://osskb.org/api/file_contents/2dd68264374297fd	Carmen Bianca Bakker
2	reuse/rep	reuse-tool	0.10.0	cc0-1.0,gp	https://github.com/fsfe/reuse-tool					94%(1-266,270-382)	https://osskb.org/api/file_contents/04cd419ee2fba863f	fsfe
3	reuse/__in	reuse-tool	0.14.0	gpl-3.0-or	https://github.com/fsfe/reuse-tool					100%(all)	https://osskb.org/api/file_contents/5d16dbd923c75cc14	fsfe
4	reuse/_co	reuse-tool	0.14.0	gpl-3.0-or	https://github.com/fsfe/reuse-tool					99%(1-705)	https://osskb.org/api/file_contents/7edb106b63c7948e	fsfe
5	reuse/_fo	reuse-tool	0.10.0	gpl-3.0-or	https://github.com/fsfe/reuse-tool					100%(all)	https://osskb.org/api/file_contents/7ae7b65dd442bbb3	fsfe
6	reuse/_ma	reuse-tool	0.14.0	gpl-3.0-or	https://github.com/fsfe/reuse-tool					100%(all)	https://osskb.org/api/file_contents/2299f5e58eed7096	fsfe
7	reuse/_ut	reuse	0.13.0	gpl-3.0-or	https://pypi.org/project/reuse					99%(1-360)	https://osskb.org/api/file_contents/8552ff8658f368126	Carmen Bianca Bakker
8	reuse/do	reuse-tool	0.14.0	gpl-3.0-or	https://github.com/fsfe/reuse-tool					100%(all)	https://osskb.org/api/file_contents/f965edd9602de6e1	fsfe



ID	Source Na	OSS Name	OSS Versi	License	Download	Homepag	Copyright	Exclude	Comment	license_reference	scanoss_matched_line	scanoss_fileURL	scanoss_vendor
1	reuse/resources/licenses.json			blessing,a	gpl-1.0,crystalstacker,	lpl-1.02,bsd-2-clause-\	lgpl-2.0-plus with wxwindows-exception-3.1,gpl-2.0 with classpath-exception-2.0,cc-by-4.0 or cc-by-3.0,gpl-2.0 with gcc-linking-exception-2.0,freetype or gpl-2.0,gpl-2.0-plus or					lgpl-2.1-plus or mpl-1.1
2	reuse/resources/exceptions.json			cc0-1.0			Copyright Linux Foundation and its Contributors						
3	reuse/resources/licenses.json.lic			cc0-1.0			Copyright Linux Foundation and its Contributors						
4	reuse/templates/default_templa			cc0-1.0			Copyright 2019 Free Software Foundation Europe e.V. <https://fsfe.org>						
5	reuse/resources/exceptions.json			gnu-javamail-exception,389-exception,gpl-2.0,ecos-e			gpl-2.0 with universal-foss-exception-1.0,gpl-3.0 with gcc-exception-3.1,gpl-2.0-plus with freertos-exception-2.0,gpl-2.0-plus with ecos-exception-2.0						
6	reuse/__main__.py			gpl-3.0			Copyright 2019 Free Software Foundation Europe e.V. <https://fsfe.org>						
7	reuse/__in	reuse-tool	0.14.0	gpl-3.0-or	https://github.com/fsf		Copyright 2017 Free Software Foundation Europe		(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-only, gpl-3.0-or-later		100%(all)	https://osskb.org/api/file_contents/5d16dbd923c75cc14f90a3	fsfe
8	reuse/sup	reuse-tool	0.14.0	gpl-3.0-or	https://github.com/fsf		Copyright 2021 Free		(mit or apache-2.0) and othe		(Scancode) mit, gpl-3.0, apache-2.0, other-permissive / (Scanoss) c	100%(all)	https://osskb.org/api/file_contents/bcbdc8df45e7d21baa0e5	fsfe
9	reuse/rep	reuse-tool	0.10.0	gpl-3.0-or	https://github.com/fsf		Copyright 2017 Free Software Foundation Europe		(Scancode) cc0-1.0, gpl-3.0 / (Scanoss) gpl-3.0-or-later, cc0-1.0		94%(1-266,270-382)	https://osskb.org/api/file_contents/04cd419ee2fba863f37ccd	fsfe
10	reuse/_co	reuse-tool	0.14.0	gpl-3.0-or	https://github.com/fsf		Copyright 2019 Free Software Foundation Europe		(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later		99%(1-705)	https://osskb.org/api/file_contents/7edb106b63c7948ea23bd	fsfe
11	reuse/_fo	reuse-tool	0.10.0	gpl-3.0-or	https://github.com/fsf		Copyright 2018 Free Software Foundation Europe		(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later		100%(all)	https://osskb.org/api/file_contents/7ae7b65dd442bbb3b31a2	fsfe
12	reuse/_ma	reuse-tool	0.14.0	gpl-3.0-or	https://github.com/fsf		Copyright 2017 Free Software Foundation Europe		(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later		100%(all)	https://osskb.org/api/file_contents/2299f5e58eed70969aad5	fsfe
13	reuse/hea	code-com	0.0.3	gpl-3.0-or	https://github.com/mi		Copyright 2019 Free Software Foundation Europe		(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later		93%(14-46,46-226,236	https://osskb.org/api/file_contents/2b07fbec3a9689d762946	miguelvictor
14	reuse/init	reuse-tool	0.10.0	gpl-3.0-or	https://github.com/fsf		Copyright 2019 Free Software Foundation Europe		(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later		100%(all)	https://osskb.org/api/file_contents/ad3709b8ac32a35a011ce	fsfe
15	reuse/lint	reuse-tool	0.14.0	gpl-3.0-or	https://github.com/fsf		Copyright 2017 Free Software Foundation Europe		(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later		100%(all)	https://osskb.org/api/file_contents/1244fc293c79045186e403	fsfe
16	reuse/proj	reuse	0.13.0	gpl-3.0-or	https://pypi.org/projec		Copyright 2017 Free Software Foundation Europe		(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later		100%(all)	https://osskb.org/api/file_contents/069dca08882a15c19922ce	Carmen Bianca Bakker
17	reuse/spdx	reuse-tool	0.10.0	gpl-3.0-or	https://github.com/fsf		Copyright 2017 Free Software Foundation Europe		(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later		100%(all)	https://osskb.org/api/file_contents/6dced70e072b66af8644d	fsfe
18	reuse/vcs	reuse-tool	0.10.0	gpl-3.0-or	https://github.com/fsf		Copyright 2017 Free Software Foundation Europe		(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later		100%(all)	https://osskb.org/api/file_contents/151098752336cfe62ce431	fsfe
19	reuse/_lice	reuse	0.11.0	gpl-3.0-or	https://pypi.org/projec		Copyright 2019 Free Software Foundation Europe		(Scancode) gpl-3.0, apache-2.0 / (Scanoss) gpl-3.0-or-later, apache		100%(all)	https://osskb.org/api/file_contents/2dd68264374297fd90a3a	Carmen Bianca Bakker
20	reuse/_util	reuse	0.13.0	gpl-3.0-or	https://pypi.org/projec		Copyright 2017 Free Software Foundation Europe		(Scancode) gpl-3.0, unknown-spdx / (Scanoss) gpl-3.0-or-later		99%(1-360)	https://osskb.org/api/file_contents/8552ff8658f368126860ae	Carmen Bianca Bakker
21	reuse/dow	reuse-tool	0.14.0	gpl-3.0-or	https://github.com/fsf		Copyright 2019 Free		unknown-spdx or unknown-s	(Scancode) gpl-3.0, unknown-spdx / (Scanoss) gpl-3.0-or-later	100%(all)	https://osskb.org/api/file_contents/f965edd9602de6e183e3e	fsfe
22	reuse/templates/default_templa			unknown-spdx									

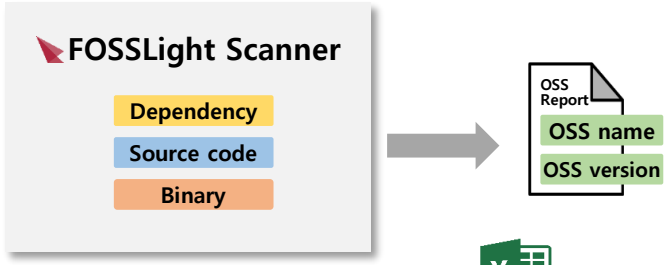
FOSSLight Scanner - Binary

- 바이너리 목록 추출하여 Database에서 오픈소스 정보 확인
- Jar 파일에 대하여 보안 취약점 확인도 가능

	A	B	C	D	E	F	G	H	I	J	K
1	ID	Source Na	OSS Name	OSS Versi	License	Download Location	Homepage	Copyright Text	Exclude	Comment	Vulnerability Link
2	22	lib/aho-cc	hankcs:ah	1.2.3	Apache License Version 2.0	hankcs/AhoCorasickDoubleArrayTrie				OWASP Result.	
3	23	lib/androi	vaadin.ext	0.0.201311	Apache License 2.0	http://developer.android.com/sdk				OWASP Result.	
4	24	lib/annota	jetbrains:a	22.0.0	The Apache Software License V	JetBrains/java-annotations				OWASP Result.	
5	25	lib/ant-1.1	apache.an	1.10.12		https://ant.apache.org/				OWASP Result.	https://nvd.nist.gov/vuln/search/results?form_type=Ad
6	26	lib/checke	checkerfra	3.12.0	The MIT License	https://checkerframework.org				OWASP Result.	
7	27	lib/comm	commons-	1.9.4	https://www.apache.org/licenses/	https://commons.apache.org/proper/commons-beanutils/				OWASP Result.	https://nvd.nist.gov/vuln/search/results?form_type=Ad
8	28	lib/comm	commons-	1.5.0	https://www.apache.org/licenses/	https://commons.apache.org/proper/commons-cli/				OWASP Result.	
9	29	lib/comm	commons-	1.15	https://www.apache.org/licenses/	https://commons.apache.org/proper/commons-codec/				OWASP Result.	
10	30	lib/comm	commons-	3.2.2	http://www.apache.org/licenses/	http://commons.apache.org/collections/				OWASP Result.	https://nvd.nist.gov/vuln/search/results?form_type=Ad
11	31	lib/comm	apache.co	1.21	https://www.apache.org/licenses/	https://commons.apache.org/proper/commons-compress/				OWASP Result.	https://nvd.nist.gov/vuln/search/results?form_type=Ad
12	32	lib/comm	apache.co	2.9.0	https://www.apache.org/licenses/	https://commons.apache.org/dbcp/				OWASP Result.	
13	33	lib/comm	commons-	2.1	http://www.apache.org/licenses/	http://commons.apache.org/digester/				OWASP Result.	
14	34	lib/comm	commons-	2.11.0	https://www.apache.org/licenses/	https://commons.apache.org/proper/commons-io/				OWASP Result.	https://nvd.nist.gov/vuln/search/results?form_type=Ad
15	35	lib/comm	apache.co	2.2.1	https://www.apache.org/licenses/	LICENSE-2.0.txt				OWASP Result.	
16	36	lib/comm	apache.co	3.12.0	https://www.apache.org/licenses/	https://commons.apache.org/proper/commons-lang/				OWASP Result.	
17	37	lib/comm	commons-	1.2	http://www.apache.org/licenses/	http://commons.apache.org/proper/commons-logging/			Exclude	OWASP Result. Excluded due to Binary DB.	
18	38	lib/comm	commons-	1.2	Apache-2.0					Binary DB Result	

FOSSLight Scanner를 통한 SBOM 생성

- FOSSLight Scanner 실행하여 오픈소스 분석 보고서 생성



	Source Name or Path	OSS Name	OSS Version	License	Download Location	Homepage	opyright Tex	Exclude	Comment	ependencie
1	package.json	npm:lge-example	1.0.0	Apache-2.0	https://github.com/LGE-OSS/example	https://www.npmjs.com/package/lge-example			root packa	npm:copy-.
2	package.json	npm:copy-anything	2.0.6	MIT	https://github.com/mesqueeb/copy-anything	https://www.npmjs.com/package/copy-anything			direct	npm:is-wha
3	package.json	npm:is-what	3.14.1	MIT	https://github.com/mesqueeb/is-what	https://www.npmjs.com/package/is-what			transitive	
4	requirements.txt	pypi:CacheControl	0.12.11	Apache Software License	https://pypi.org/project/CacheControl/0.12.11	https://github.com/ionrock/cachecontrol			transitive	pypi:msgpa
5	requirements.txt	pypi:Deprecated	1.2.14	MIT License	https://pypi.org/project/Deprecated/1.2.14	https://github.com/tantale/deprecated			transitive	pypi:wrapt(
6	requirements.txt	pypi:Jinja2	3.1.2	BSD License	https://pypi.org/project/Jinja2/3.1.2	https://palletsprojects.com/p/jinja/			transitive	pypi:Marku
7	requirements.txt	pypi:MarkupSafe	2.1.3	BSD License	https://pypi.org/project/MarkupSafe/2.1.3	https://palletsprojects.com/p/markupsafe/			transitive	
8	requirements.txt	pypi:PyGithub	2.1.1	GNU Library or Lesser Gen	https://pypi.org/project/PyGithub/2.1.1	https://github.com/pygithub/pygithub			transitive	pypi:Depre
9	requirements.txt	pypi:PyJWT	2.8.0	MIT License	https://pypi.org/project/PyJWT/2.8.0	https://github.com/jpadilla/pyjwt			transitive	
10	requirements.txt	pypi:PyNaCl	1.5.0	Apache License 2.0	https://pypi.org/project/PyNaCl/1.5.0	https://github.com/pyca/pynacl/			transitive	pypi:cffi(1.1
11	requirements.txt	pypi:PyYAML	6.0.1	MIT License	https://pypi.org/project/PyYAML/6.0.1	https://pyyaml.org/			transitive	
12	requirements.txt	pypi:XlsxWriter	3.1.8	BSD License	https://pypi.org/project/XlsxWriter/3.1.8	https://github.com/jmcnamara/XlsxWriter			transitive	
13	requirements.txt	pypi:appdirs	1.4.4	MIT License	https://pypi.org/project/appdirs/1.4.4	http://github.com/ActiveState/appdirs			transitive	
14	requirements.txt	pypi:attrs	23.1.0	MIT License	https://pypi.org/project/attrs/23.1.0	https://www.attrs.org/en/stable/changelog.html			transitive	
15	requirements.txt	pypi:beautifulsoup4	4.12.2	MIT License	https://pypi.org/project/beautifulsoup4/4.12.2	https://www.crummy.com/software/BeautifulSoup/bs4/			transitive	pypi:soupsi
16	requirements.txt	pypi:binaryornot	0.4.4	BSD License	https://pypi.org/project/binaryornot/0.4.4	https://github.com/audreyr/binaryornot			transitive	pypi:charde
17	requirements.txt	pypi:boolean.py	4.0	BSD-2-Clause	https://pypi.org/project/boolean.py/4.0	https://github.com/bastikr/boolean.py			transitive	
18	requirements.txt	pypi:certifi	2023.7.22	Mozilla Public License 2.0	https://pypi.org/project/certifi/2023.7.22	https://github.com/certifi/python-certifi			transitive	
19	requirements.txt	pypi:cffi	1.16.0	MIT License	https://pypi.org/project/cffi/1.16.0	http://cffi.readthedocs.org			transitive	pypi:pycpa
20	requirements.txt	pypi:chardet	5.2.0	GNU Lesser General Public	https://pypi.org/project/chardet/5.2.0	https://github.com/chardet/chardet			transitive	

SRC_FL_Source | SRC_FL_Dependency | BIN_FL_Binary

설치 및 사용 방법

- FOSSLight Scanner 설치 방법
  - Python 3.8 ~ 3.11
  - Open JDK

```
$ pip install fosslight_scanner
```

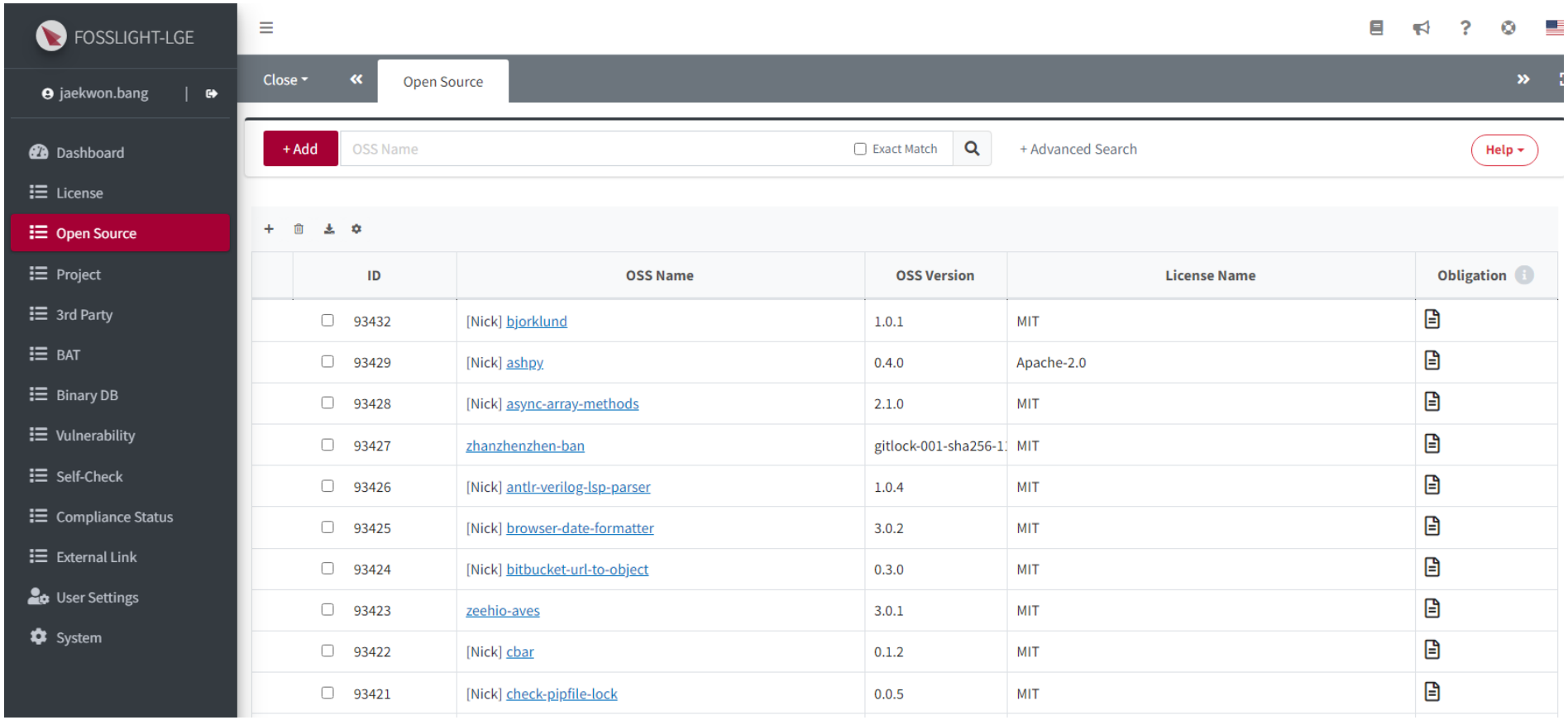
- FOSSLight Scanner 사용 방법
  - 명령어 fosslight 를 호출
  - fosslight –h 를 입력시, parameter 확인 가능

```
$ fosslight
```

FOSSLight Hub

오픈소스 관리

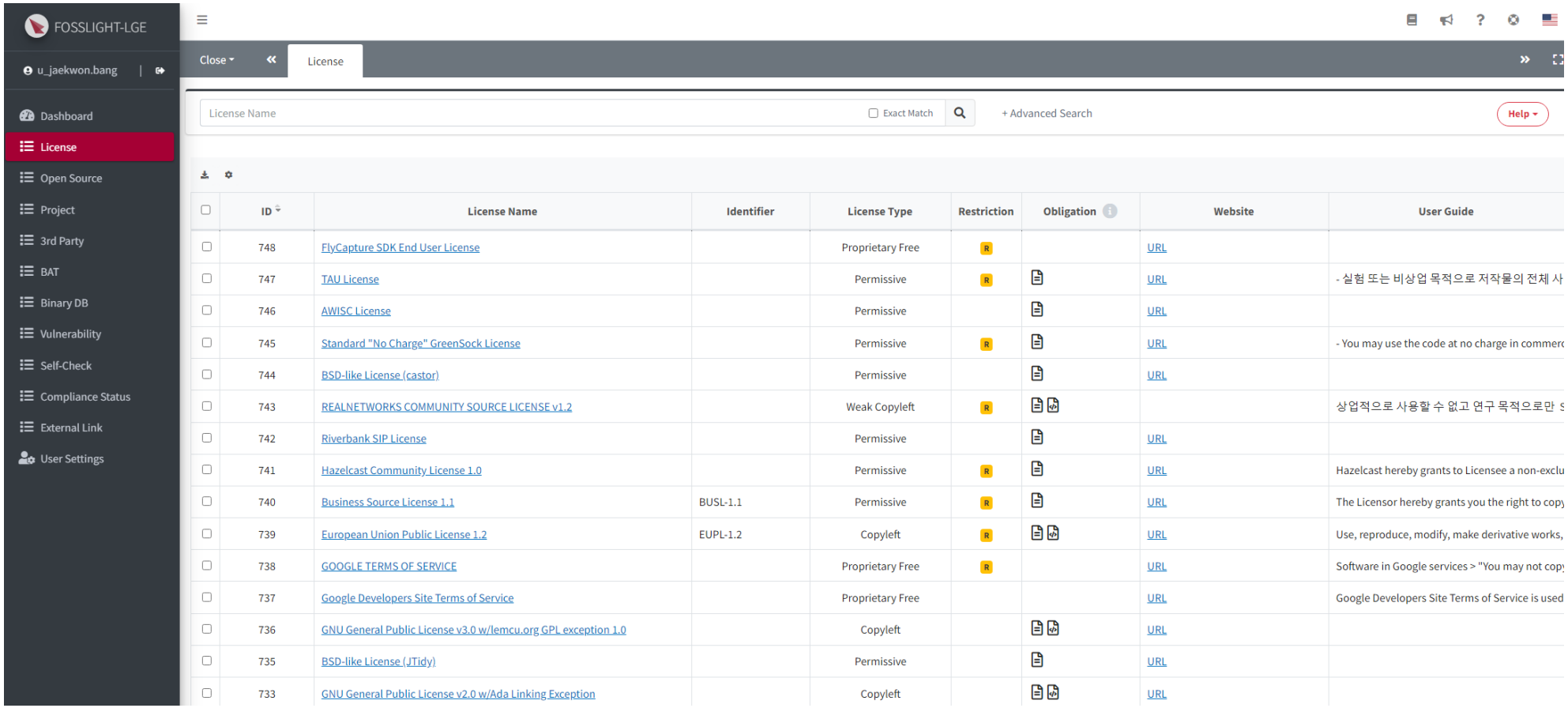
- 오픈소스 버전별로 라이선스 및 의무 사항 관리



ID	OSS Name	OSS Version	License Name	Obligation
93432	[Nick] bjorklund	1.0.1	MIT	
93429	[Nick] ashpy	0.4.0	Apache-2.0	
93428	[Nick] async-array-methods	2.1.0	MIT	
93427	zhanzhenzhen-ban	gitlock-001-sha256-1	MIT	
93426	[Nick] antlr-verilog-lsp-parser	1.0.4	MIT	
93425	[Nick] browser-date-formatter	3.0.2	MIT	
93424	[Nick] bitbucket-url-to-object	0.3.0	MIT	
93423	zeehio-aves	3.0.1	MIT	
93422	[Nick] cbar	0.1.2	MIT	
93421	[Nick] check-pipfile-lock	0.0.5	MIT	

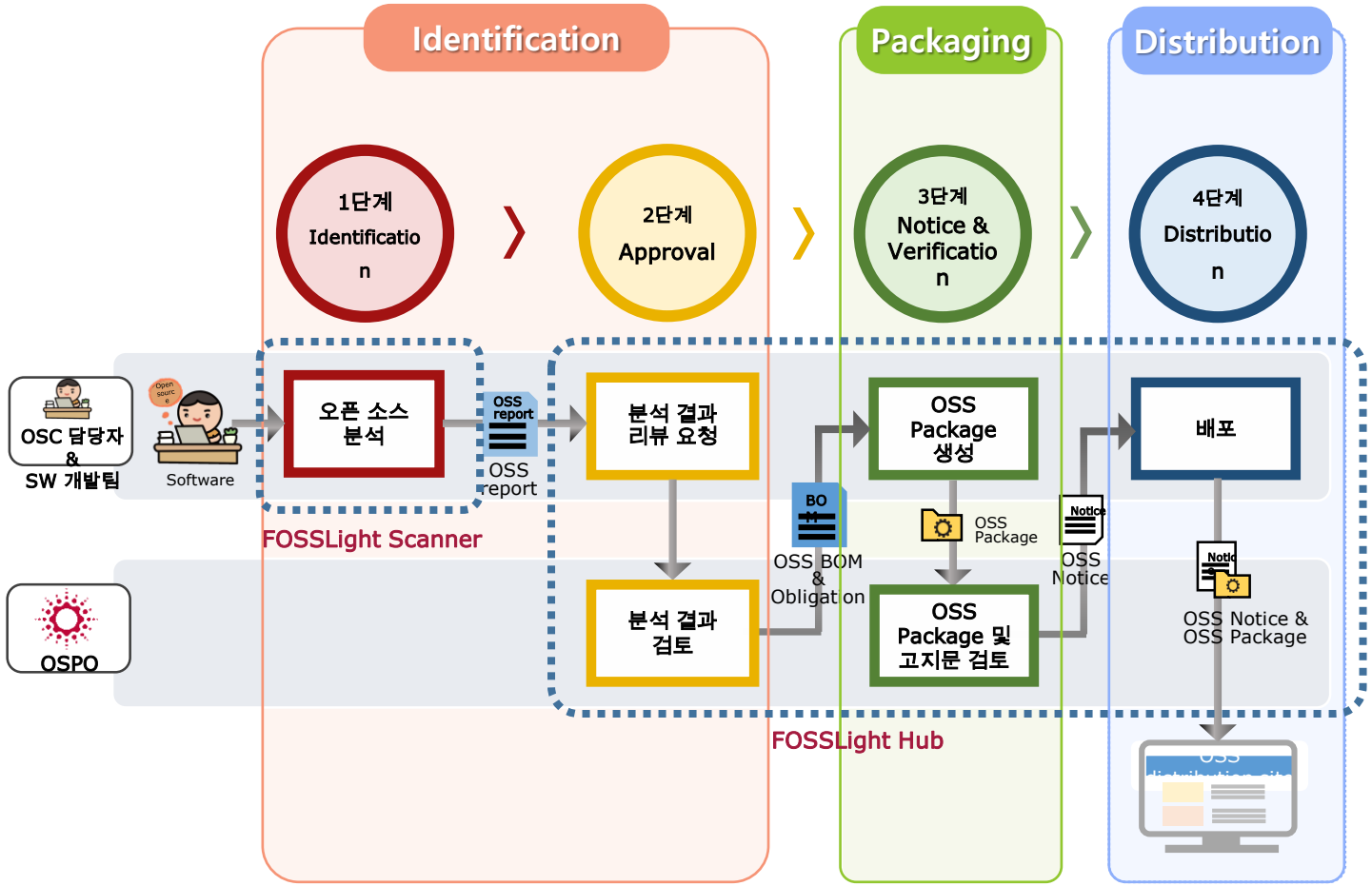
라이선스 관리

- 라이선스별로 의무사항, 제약사항, 준수사항 관리



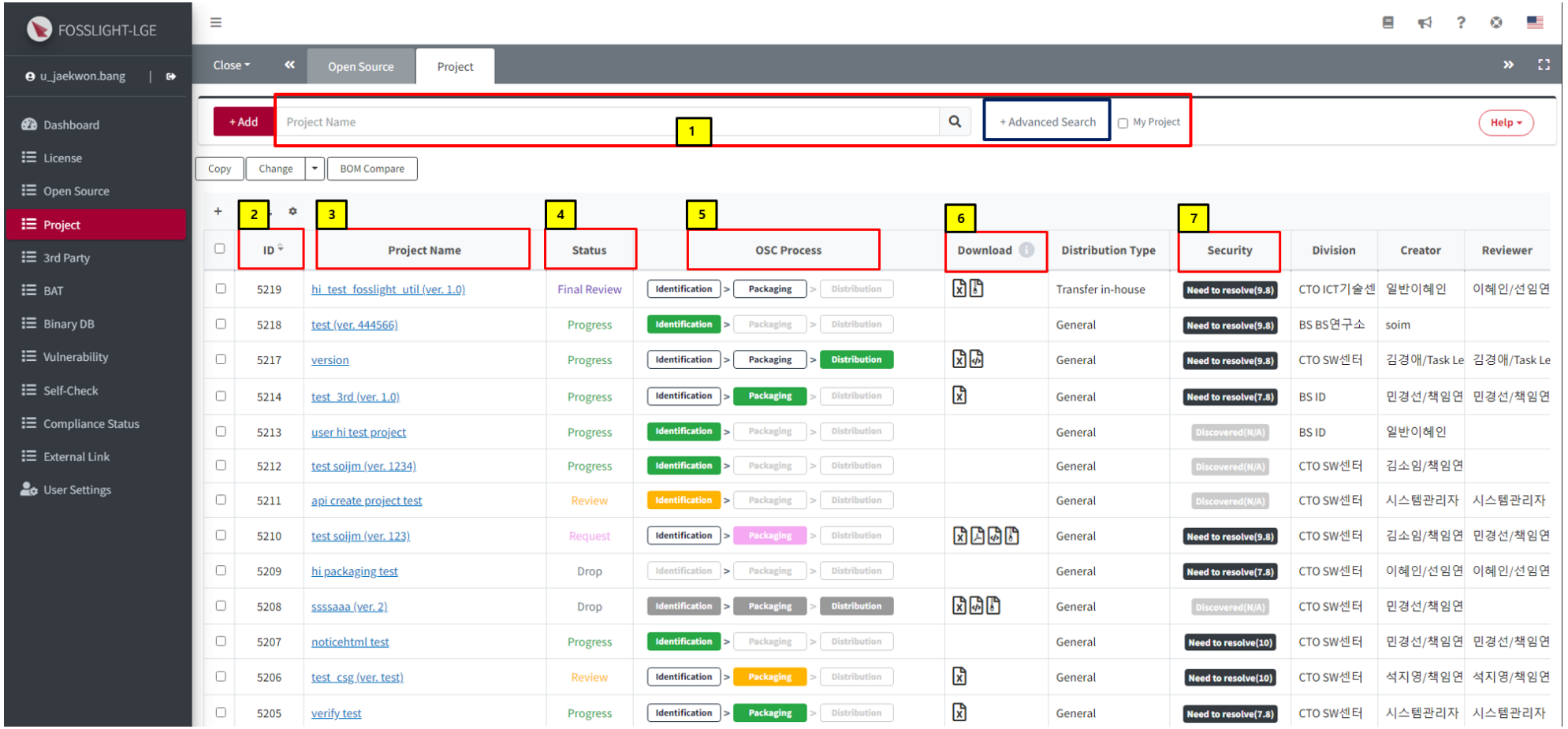
ID	License Name	Identifier	License Type	Restriction	Obligation	Website	User Guide
748	FlyCapture SDK End User License		Proprietary Free	R		URL	
747	TAU License		Permissive	R		URL	- 실험 또는 비상업 목적으로 저작물의 전체 사
746	AWISC License		Permissive			URL	
745	Standard "No Charge" GreenSock License		Permissive	R		URL	- You may use the code at no charge in commerc
744	BSD-like License (castor)		Permissive			URL	
743	REALNETWORKS COMMUNITY SOURCE LICENSE v1.2		Weak Copyleft	R			상업적으로 사용할 수 없고 연구 목적으로만
742	Riverbank SIP License		Permissive			URL	
741	Hazelcast Community License 1.0		Permissive	R		URL	Hazelcast hereby grants to Licensee a non-exclu
740	Business Source License 1.1	BUSL-1.1	Permissive	R		URL	The Licensor hereby grants you the right to copy
739	European Union Public License 1.2	EUPL-1.2	Copyleft	R		URL	Use, reproduce, modify, make derivative works,
738	GOOGLE TERMS OF SERVICE		Proprietary Free	R		URL	Software in Google services > "You may not copy
737	Google Developers Site Terms of Service		Proprietary Free			URL	Google Developers Site Terms of Service is used
736	GNU General Public License v3.0 w/lemcu.org GPL exception 1.0		Copyleft			URL	
735	BSD-like License (JTidy)		Permissive			URL	
733	GNU General Public License v2.0 w/Ada Linking Exception		Copyleft			URL	

참고) LG전자 오픈소스 컴플라이언스 프로세스



컴플라이언스 프로세스 관리

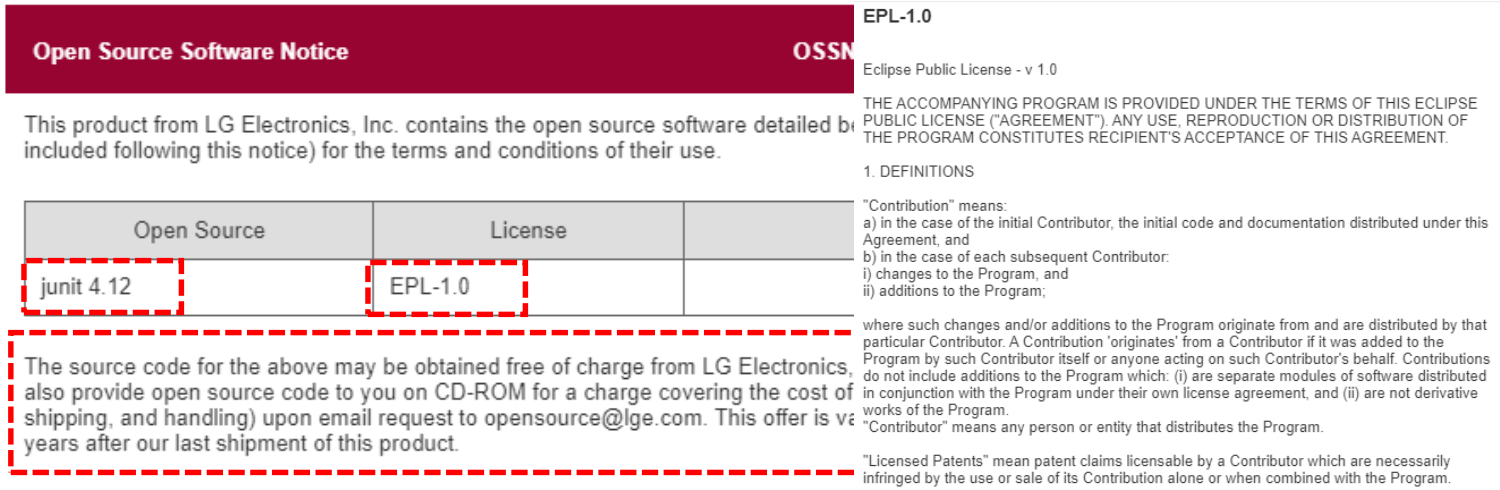
- 단계별 프로세스 진행 및 이력 조회
- 프로젝트 검색, 부서별 검색, 오픈소스별 검색



OSS 고지문 발급

- 사용된 Open Source 및 저작권, License를 고지하기 위한 OSS 고지문 발급
- 공개할 소스코드 취합한 OSS Package 리뷰

- 지원 포맷 : HTML, TEXT, SPDX



Open Source Software Notice OSSN

This product from LG Electronics, Inc. contains the open source software detailed b
included following this notice) for the terms and conditions of their use.

Open Source	License	
junit 4.12	EPL-1.0	

The source code for the above may be obtained free of charge from LG Electronics,
also provide open source code to you on CD-ROM for a charge covering the cost of
shipping, and handling) upon email request to opensource@lge.com. This offer is va
years after our last shipment of this product.

EPL-1.0

Eclipse Public License - v 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS ECLIPSE PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

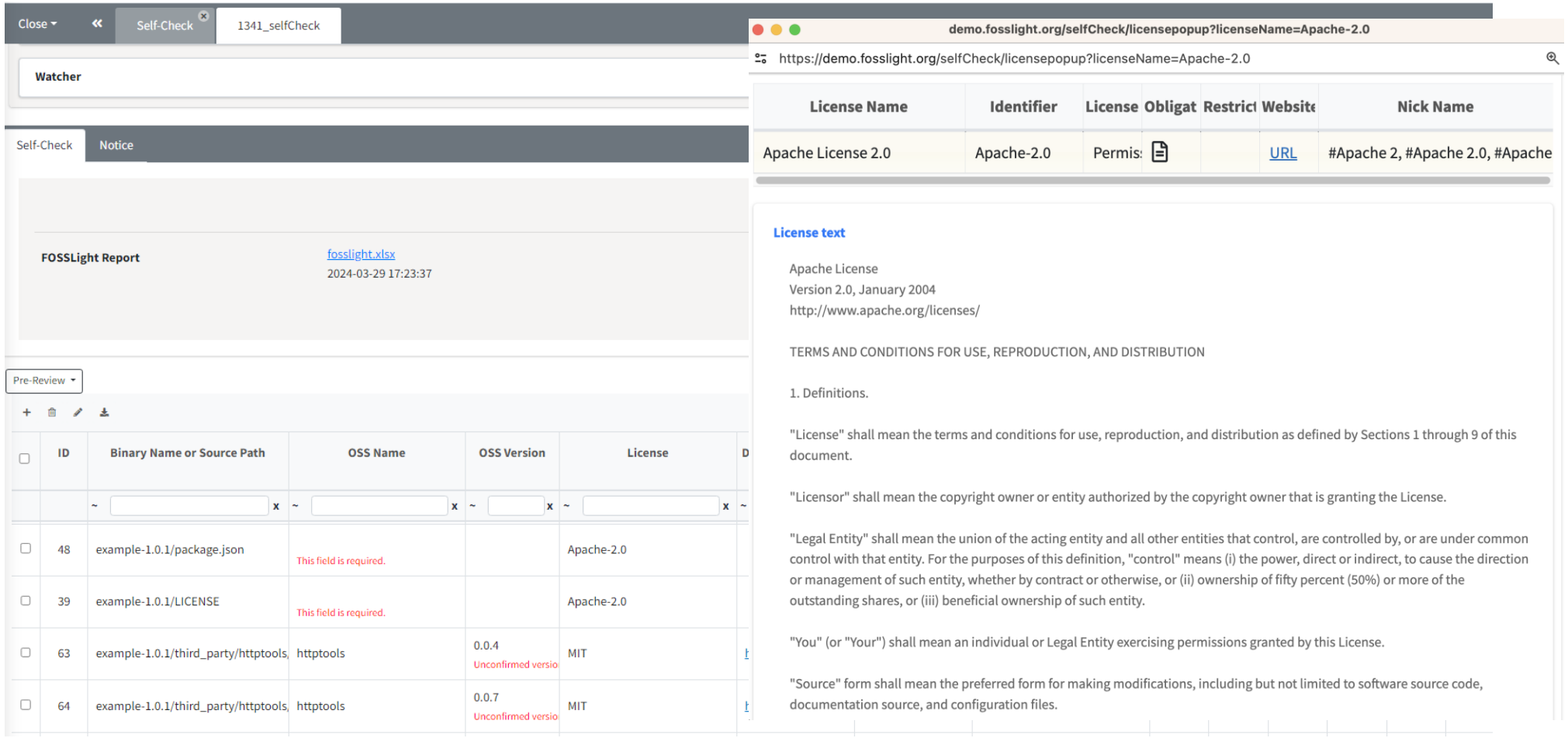
"Contribution" means:
a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
b) in the case of each subsequent Contributor:
i) changes to the Program, and
ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.
"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

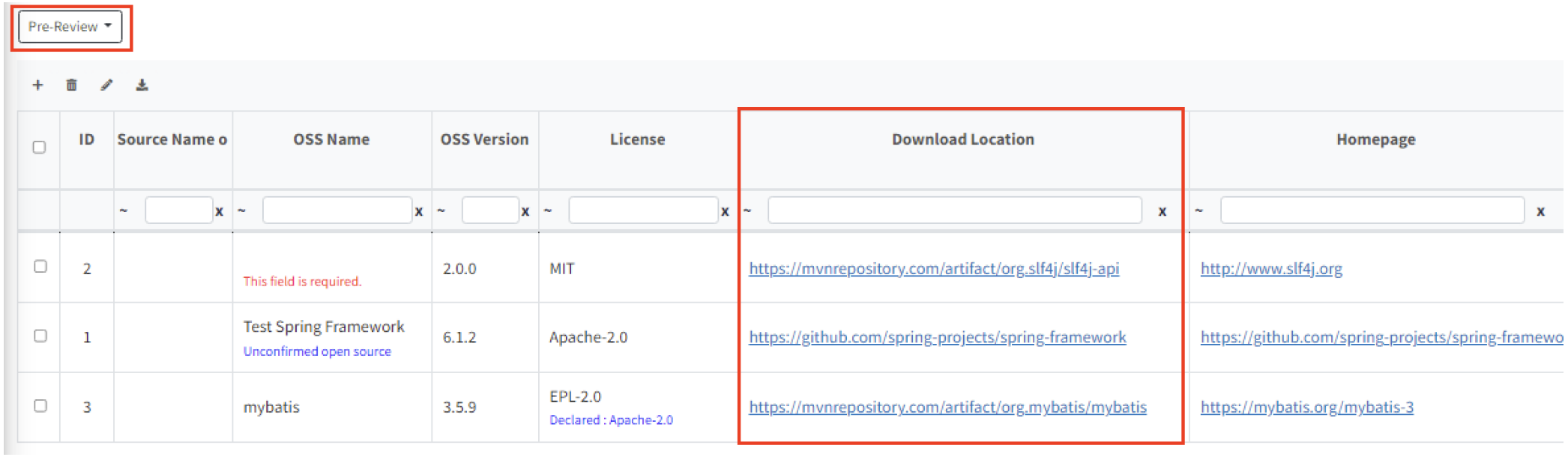
사전 점검

- 프로젝트에서 사용할 오픈소스와 라이선스 리스트를 업로드하여
  각각의 의무 사항 및 보안취약점 정보를 확인할 수 있음



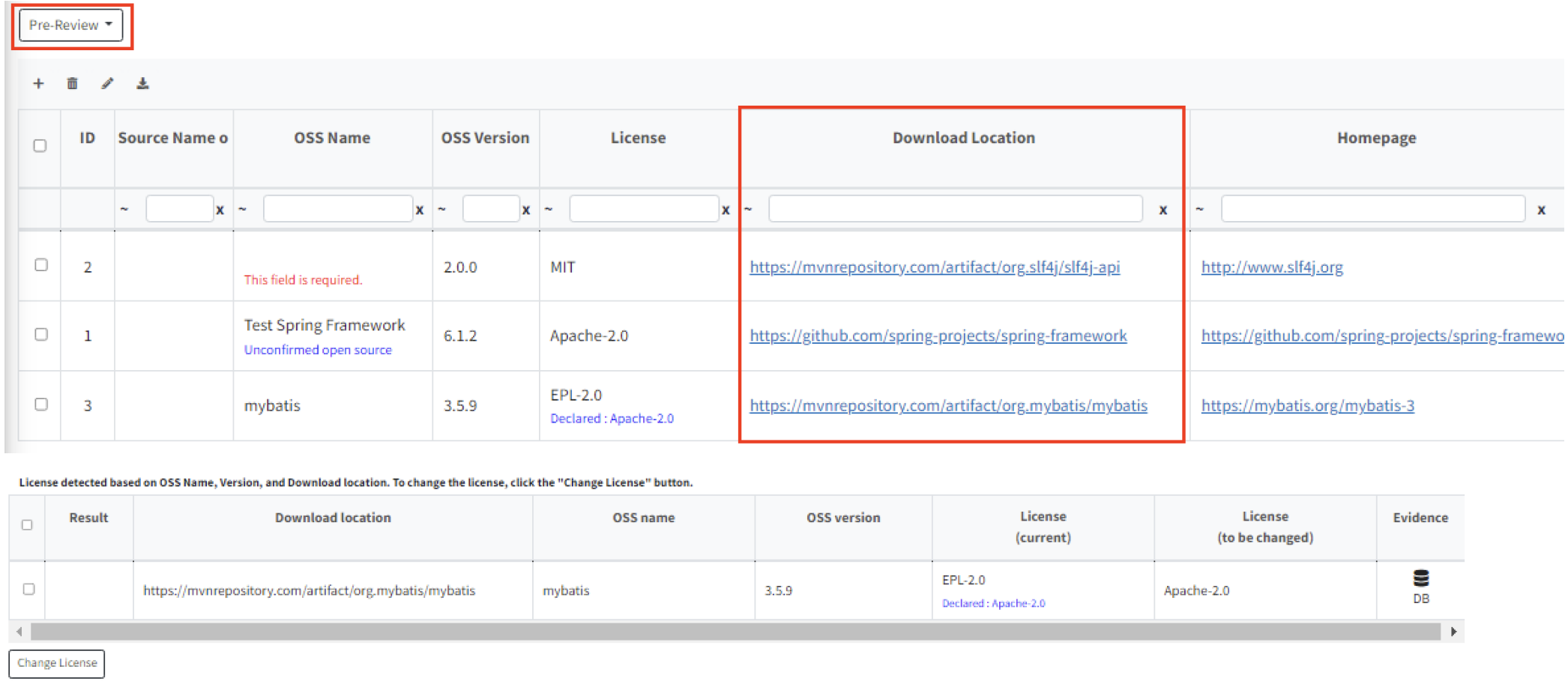
사전 점검 (Pre-Review)

- 오픈소스를 다운로드한 URL만 알아도 오픈소스와 라이선스 정보를 확인할 수 있음



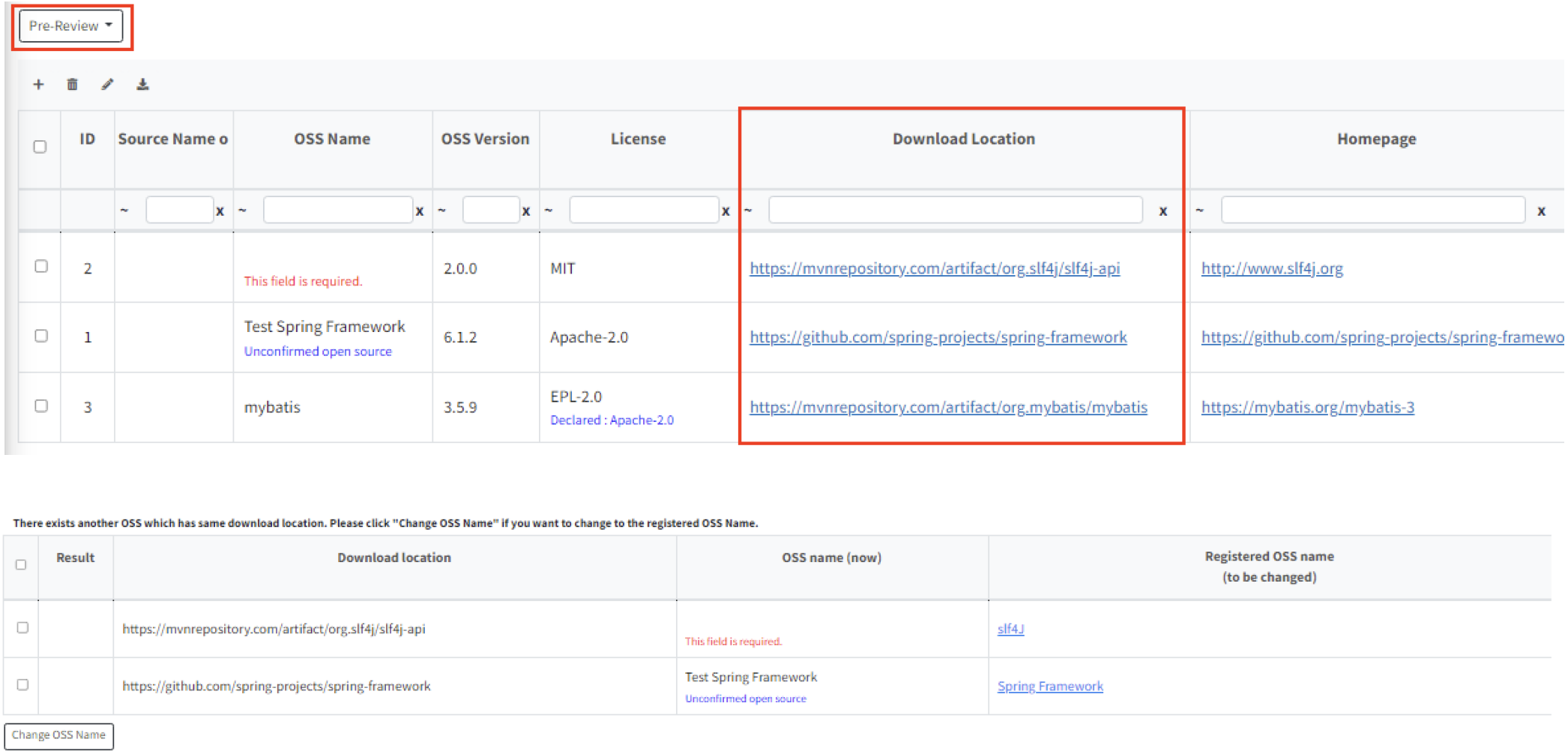
사전 점검 (Pre-Review)

- 오픈소스를 다운로드한 URL만 알아도 라이선스 정보를 확인할 수 있음



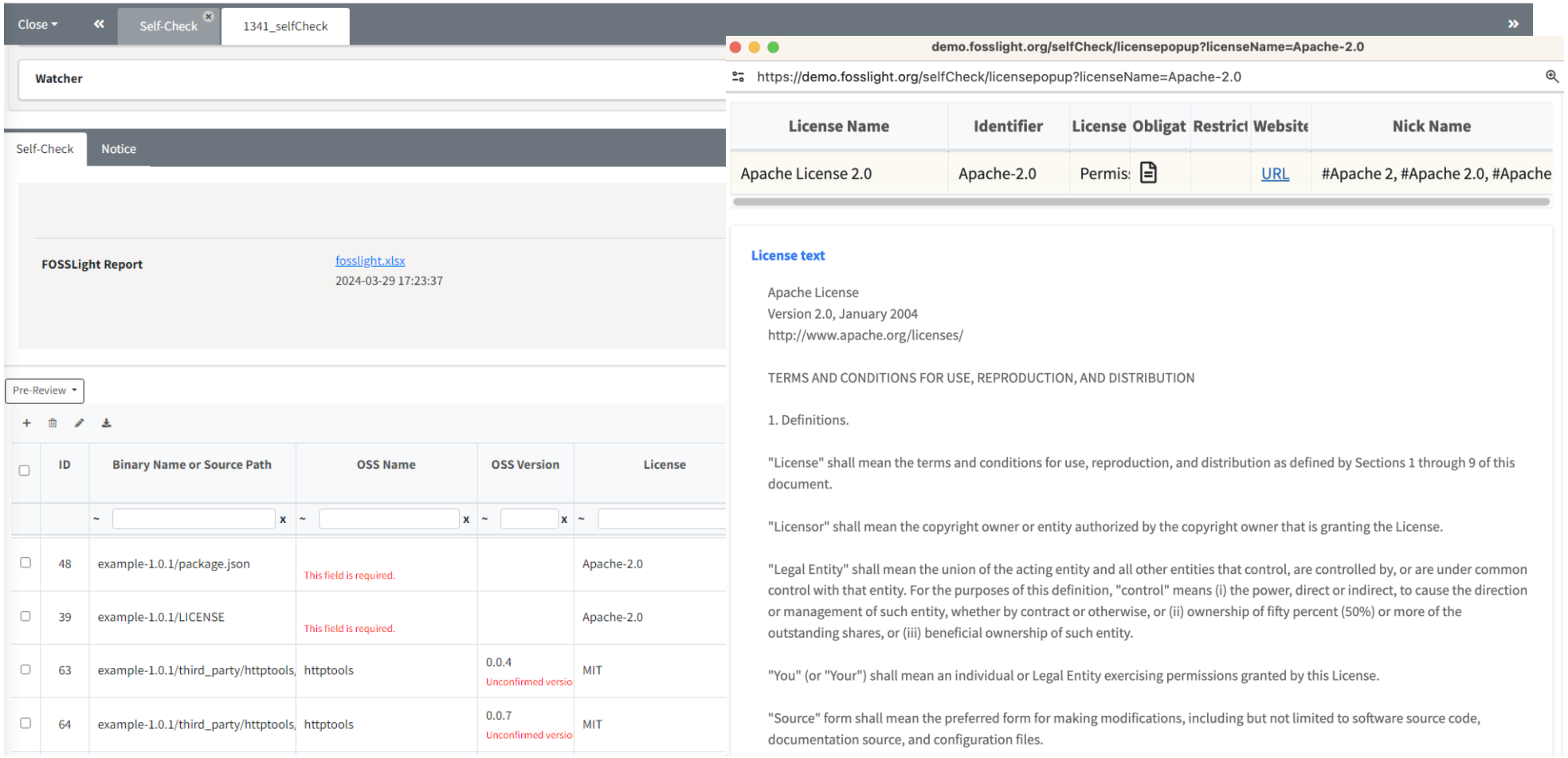
사전 점검 (Pre-Review)

- 오픈소스를 다운로드한 URL만 알아도 오픈소스 정보를 확인할 수 있음



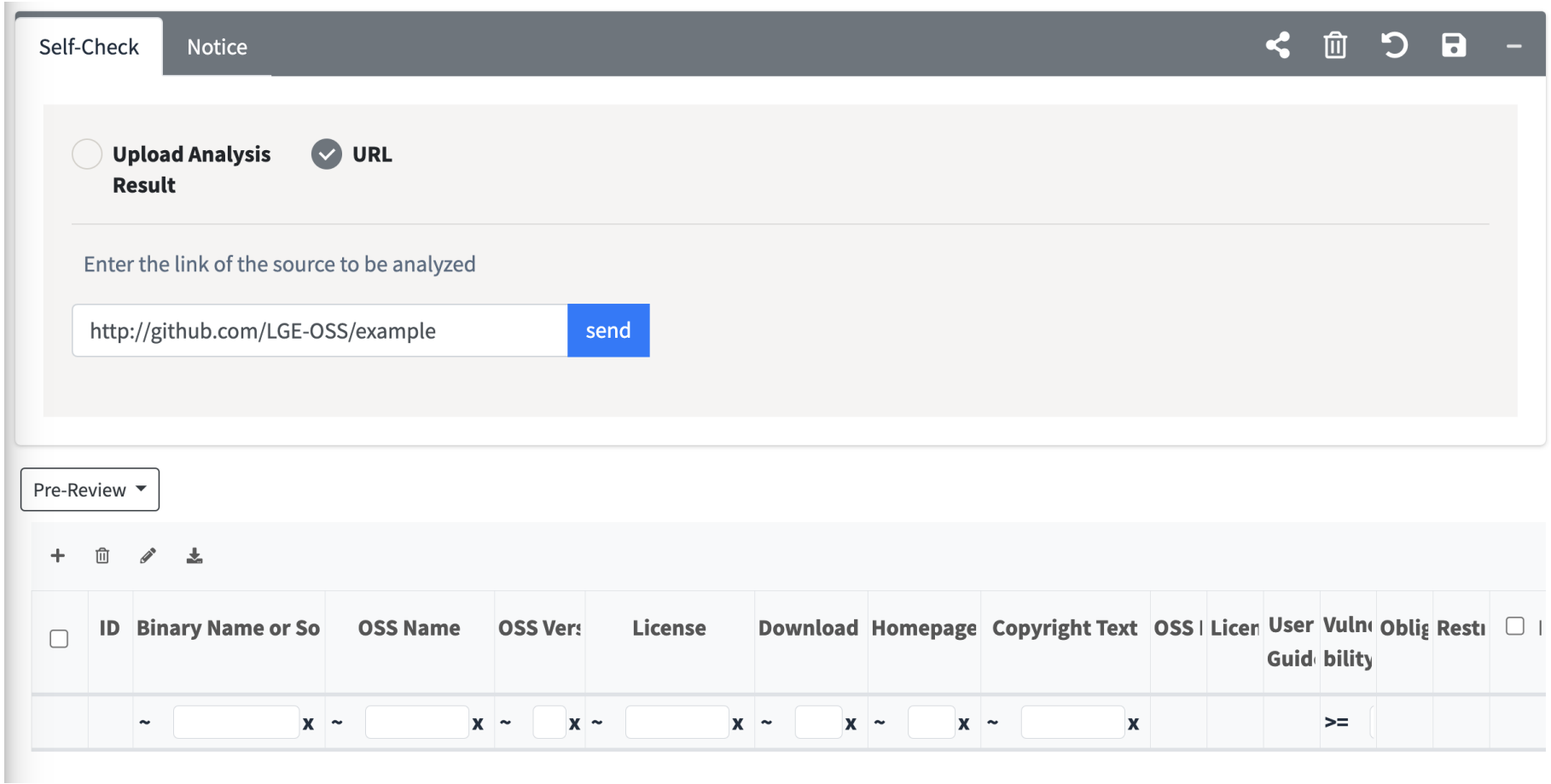
사전 점검 (Pre-Review)

- 오픈소스 라이선스 의무 사항 확인 가능함



사전 점검 (오픈소스 분석)

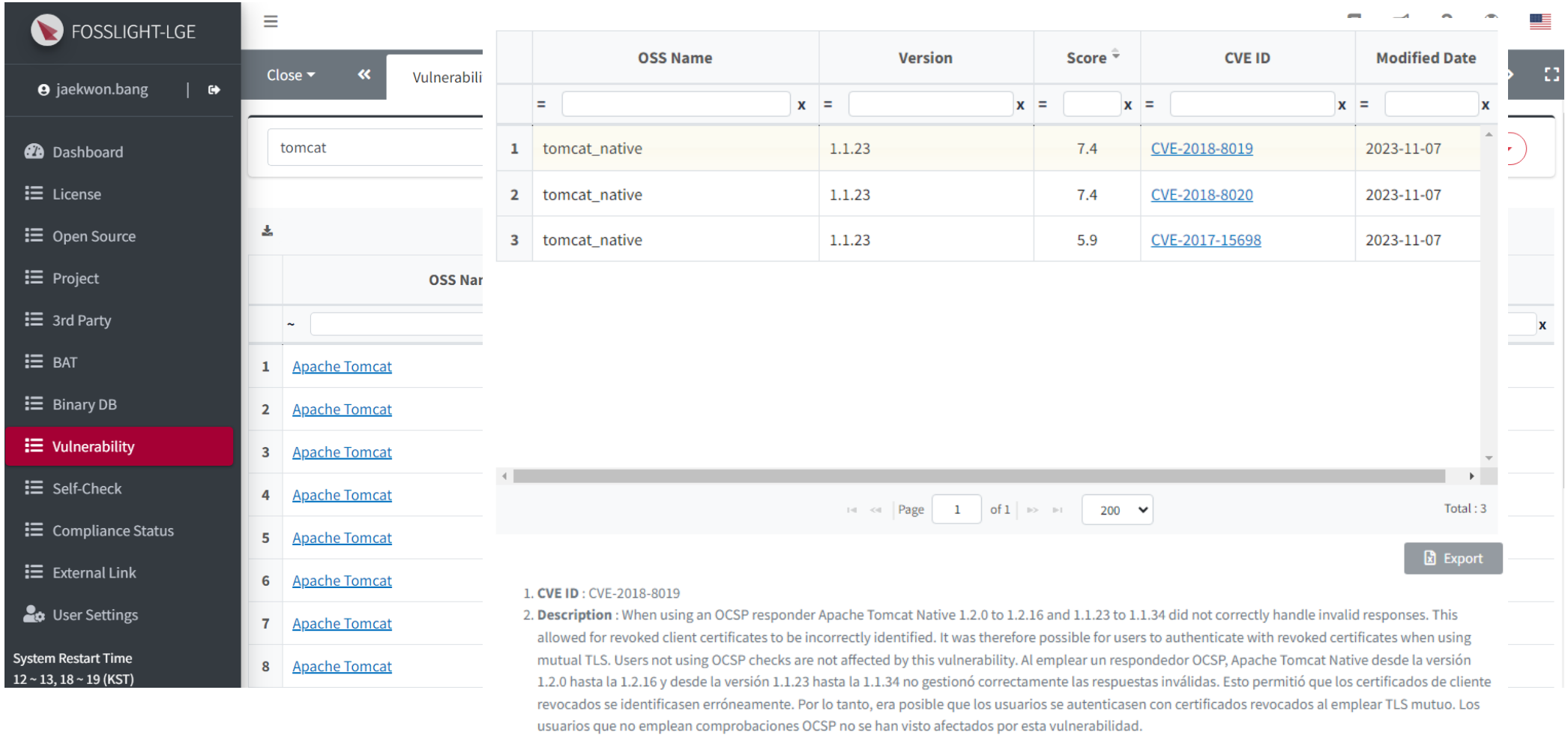
- Self-Check에 스캐닝 도구를 연동하여 소스 레파지토리 주소를 입력으로 오픈소스 라이선스 의무 사항 확인 가능



FOSSLight Hub로 보안 취약점 관리하기

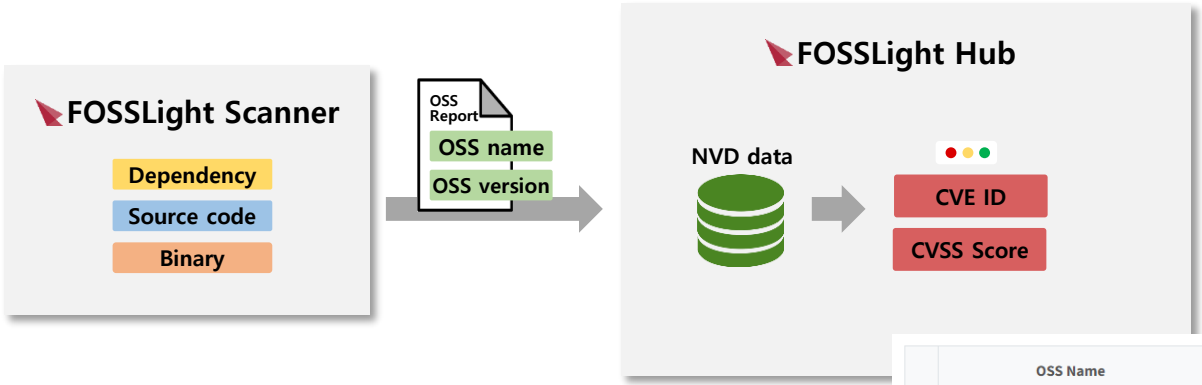
보안 취약점 조회

- 오픈소스 버전에 따른 보안 취약점 점수 및 내용 확인 가능



보안 취약점 관리

- 오픈소스 분석한 결과를 FOSSLight Hub 업로드하여 보안취약점 조회 및 관리 가능



	OSS Name	Version	Score	CVE ID	Modified Date
1	tomcat_native	1.1.23	7.4	CVE-2018-8019	2023-11-07
2	tomcat_native	1.1.23	7.4	CVE-2018-8020	2023-11-07
3	tomcat_native	1.1.23	5.9	CVE-2017-15698	2023-11-07

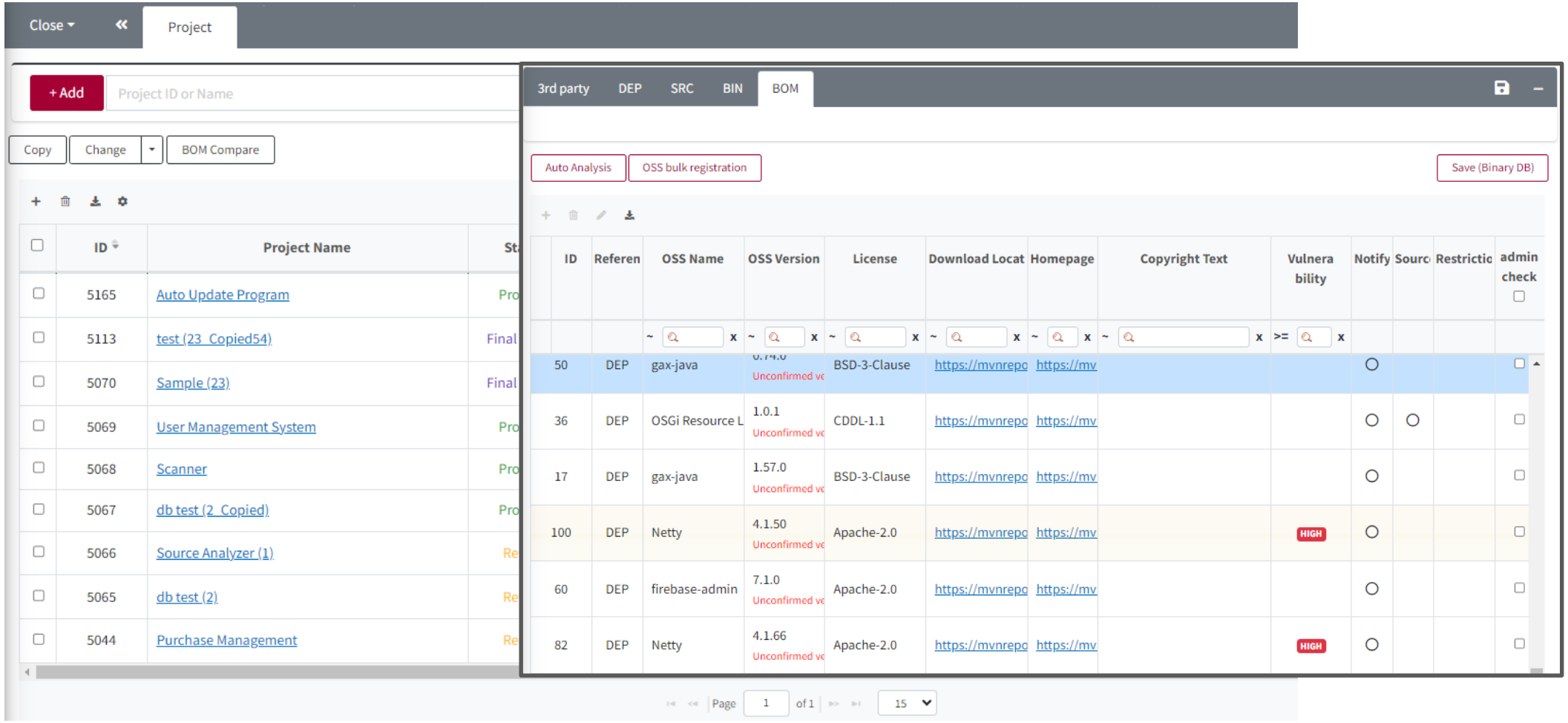
Page 1 of 1 200 Total : 3

Export

1. **CVE ID** : CVE-2018-8019
2. **Description** : When using an OCSP responder Apache Tomcat Native 1.2.0 to 1.2.16 and 1.1.23 to 1.1.34 did not correctly handle invalid responses. This allowed for revoked client certificates to be incorrectly identified. It was therefore possible for users to authenticate with revoked certificates when using mutual TLS. Users not using OCSP checks are not affected by this vulnerability. Al emplear un respondedor OCSP, Apache Tomcat Native desde la versión 1.2.0 hasta la 1.2.16 y desde la versión 1.1.23 hasta la 1.1.34 no gestionó correctamente las respuestas inválidas. Esto permitió que los certificados de cliente revocados se identificasen erróneamente. Por lo tanto, era posible que los usuarios se autenticasen con certificados revocados al emplear TLS mutuo. Los usuarios que no emplean comprobaciones OCSP no se han visto afectados por esta vulnerabilidad.

보안 취약점 확인

- 개발 제품별 프로젝트 등록하여 프로젝트별 보안 취약점 확인 가능



보안취약점 실시간 알림

- 보안 취약점 변경 사항에 대해 관리자 및 프로젝트 담당자에게 메일 알림

FOSSLight Hub Notification

[OSC] Vulnerability Discovered

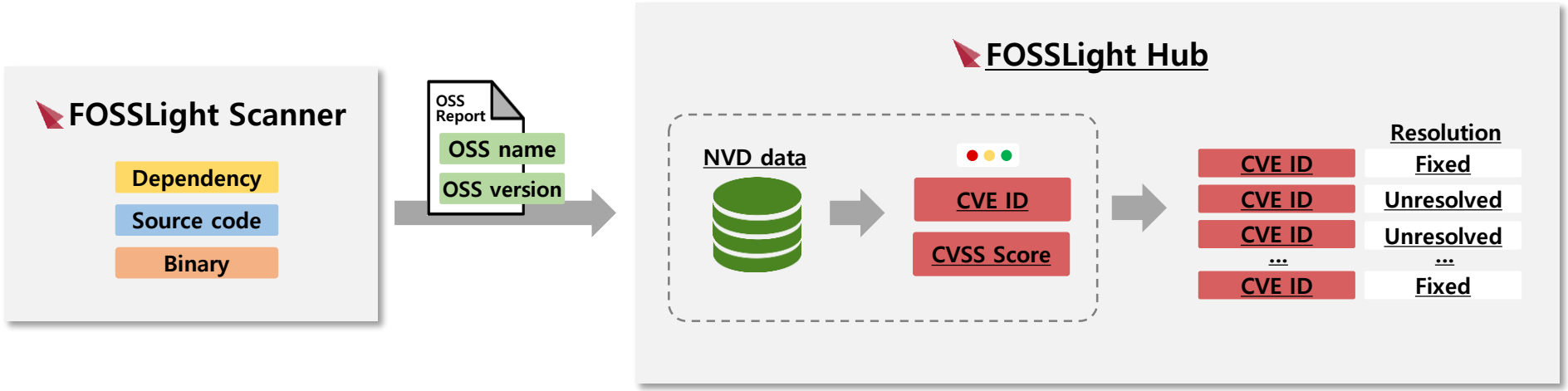
« Vulnerability Information »

OSS ID	OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
22869	json-smart-v2	2.2.1	CVE-2021-27568	9.1	An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as demonstrated by NumberFormatException. When it is not caught, it may cause programs using the library to crash or expose sensitive information.	2021-02-23	2022-05-12
15690	json-smart-v2	2.3	CVE-2021-27568	9.1	An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as demonstrated by NumberFormatException. When it is not caught, it may cause programs using the library to crash or expose sensitive information.	2021-02-23	2022-05-12

* This mail was sent by osc.lge.com

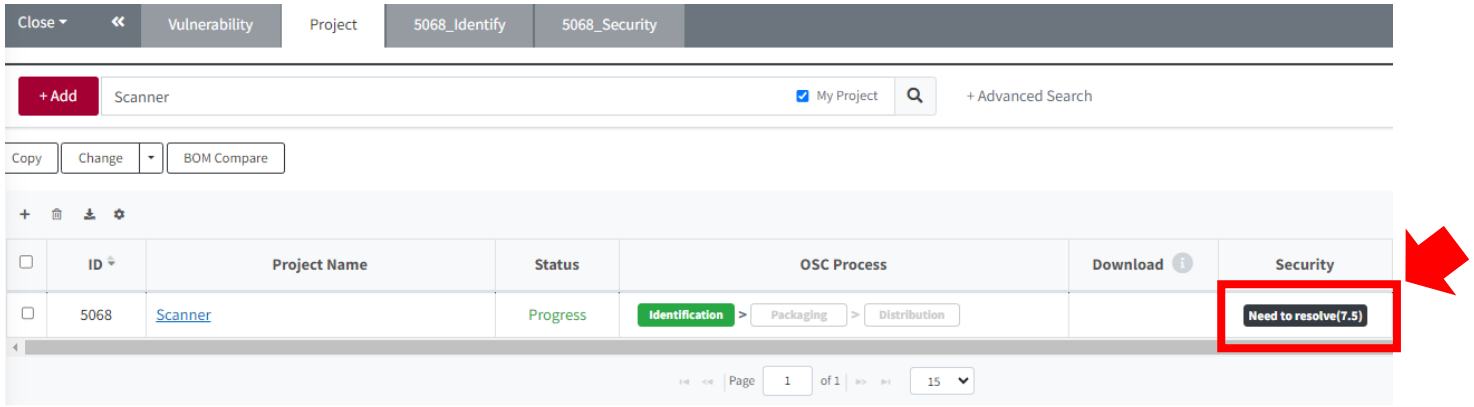
제품 보안취약점 수정 여부 관리 기능

- 프로젝트별로 발견된 보안취약점을 확인하고 해결 여부를 관리할 수 있음



Security탭

- 프로젝트 별 사용된 오픈 소스의 보안취약점 목록을 CVE ID별로 확인 가능



보안 프로세스 관리

- 프로젝트별로 발견된 보안취약점을 확인하고 해결 여부를 관리할 수 있음

OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution
appsmith	1.8.1	CVE-2022-4096	6.5	2022-11-21	Unresolved
appsmith	1.8.0	CVE-2022-4096	6.5	2022-11-21	Unresolved
appsmith	1.7.8	CVE-2022-39824	8.9	2022-09-05	Unresolved
appsmith	1.7.8	CVE-2022-4096	6.5	2022-11-21	Unresolved
appsmith	1.7.7	CVE-2022-39824	8.9	2022-09-05	Unresolved
appsmith	1.7.7	CVE-2022-4096	6.5	2022-11-21	Unresolved
appsmith	1.7.6	CVE-2022-39824	8.9	2022-09-05	Unresolved
appsmith	1.7.6	CVE-2022-4096	6.5	2022-11-21	Unresolved
appsmith	1.7.3	CVE-2022-39824	8.9	2022-09-05	Unresolved
appsmith	1.7.3	CVE-2022-4096	6.5	2022-11-21	Unresolved
appsmith	1.7.2	CVE-2022-39824	8.9	2022-09-05	Unresolved

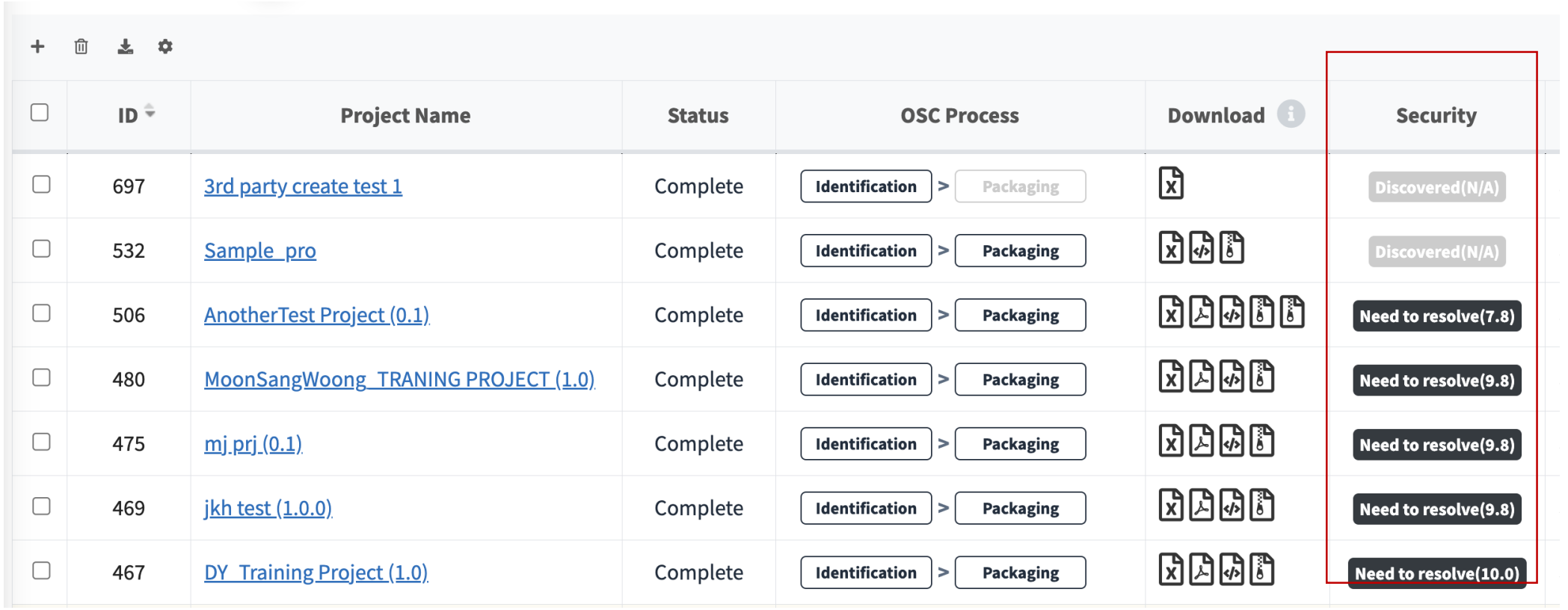
Security탭 – Vulnerability Resolution

- Vulnerability Resolution
  - 수정 여부에 따라 Resolution 값 저장 가능

- Unresolved
- Fixed

제품 보안 취약점 확인

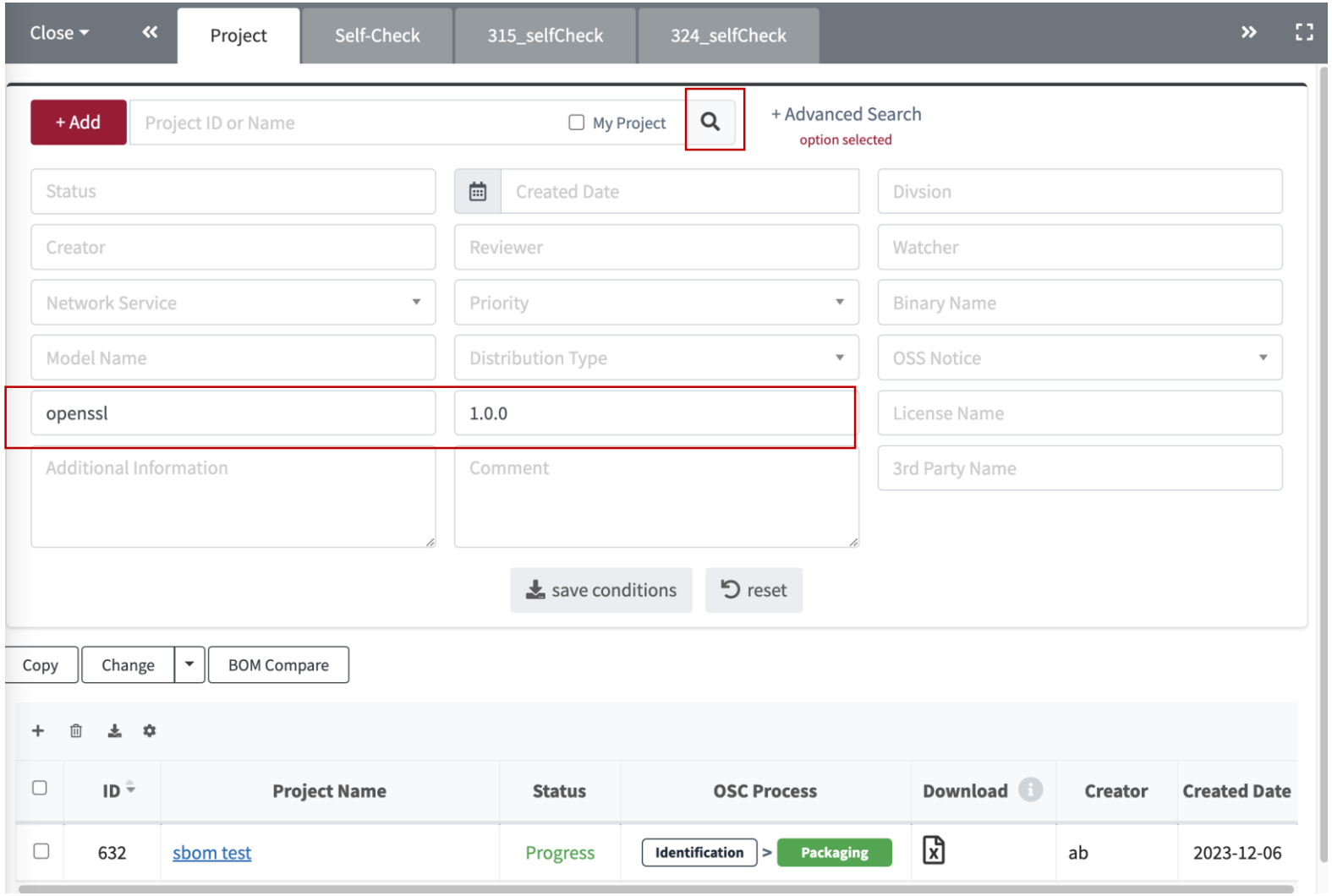
- 개발 제품별 프로젝트 등록하여 프로젝트별 보안 취약점 확인 가능



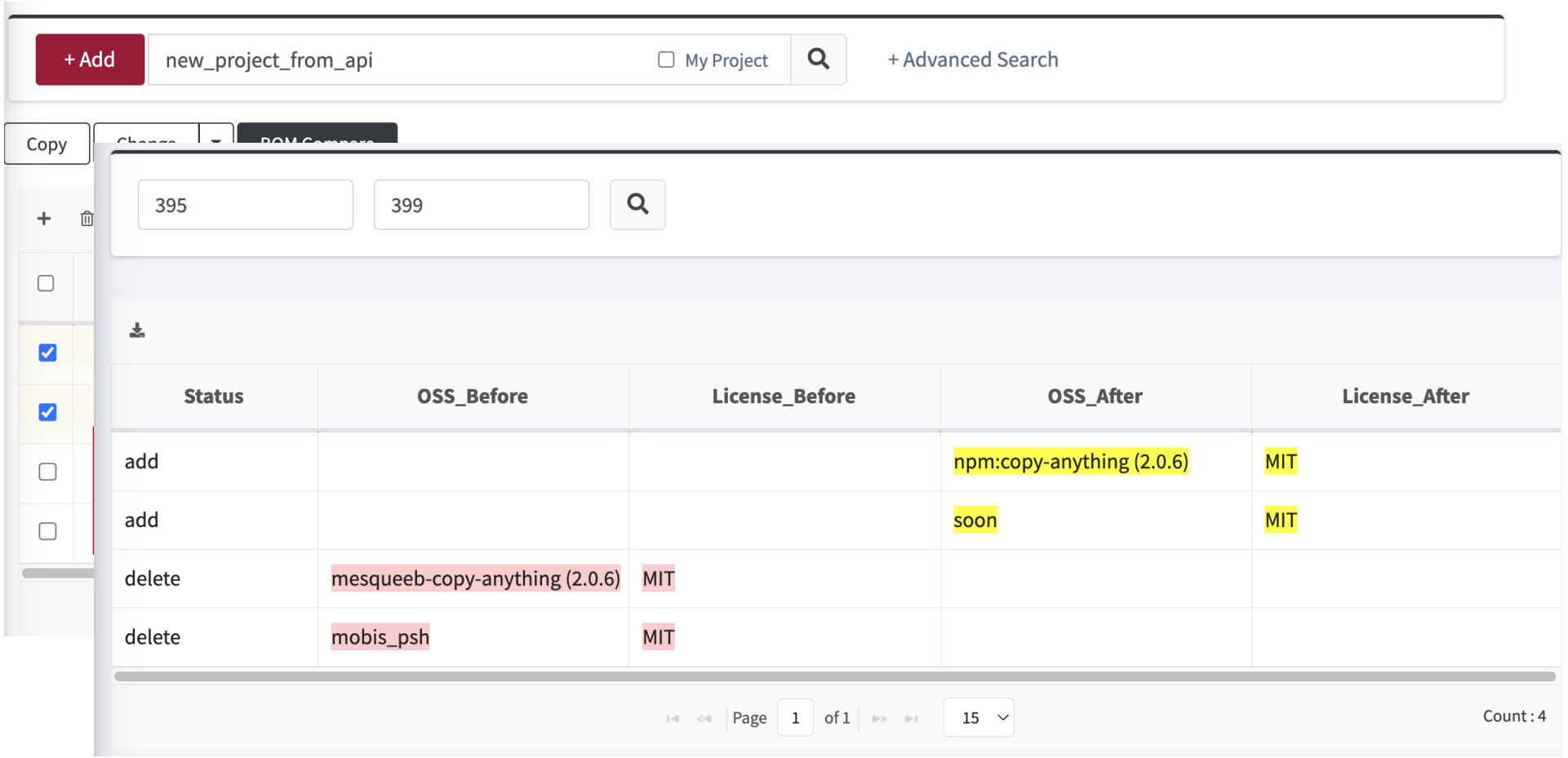
ID	Project Name	Status	OSC Process	Download	Security
697	3rd party create test 1	Complete	Identification > Packaging		Discovered(N/A)
532	Sample_pro	Complete	Identification > Packaging		Discovered(N/A)
506	AnotherTest Project (0.1)	Complete	Identification > Packaging		Need to resolve(7.8)
480	MoonSangWoong_TRANING PROJECT (1.0)	Complete	Identification > Packaging		Need to resolve(9.8)
475	mj prj (0.1)	Complete	Identification > Packaging		Need to resolve(9.8)
469	jkh test (1.0.0)	Complete	Identification > Packaging		Need to resolve(9.8)
467	DY_Training Project (1.0)	Complete	Identification > Packaging		Need to resolve(10.0)

SBOM 관리

- 특정 오픈소스 버전을 사용하는 프로젝트 조회 가능

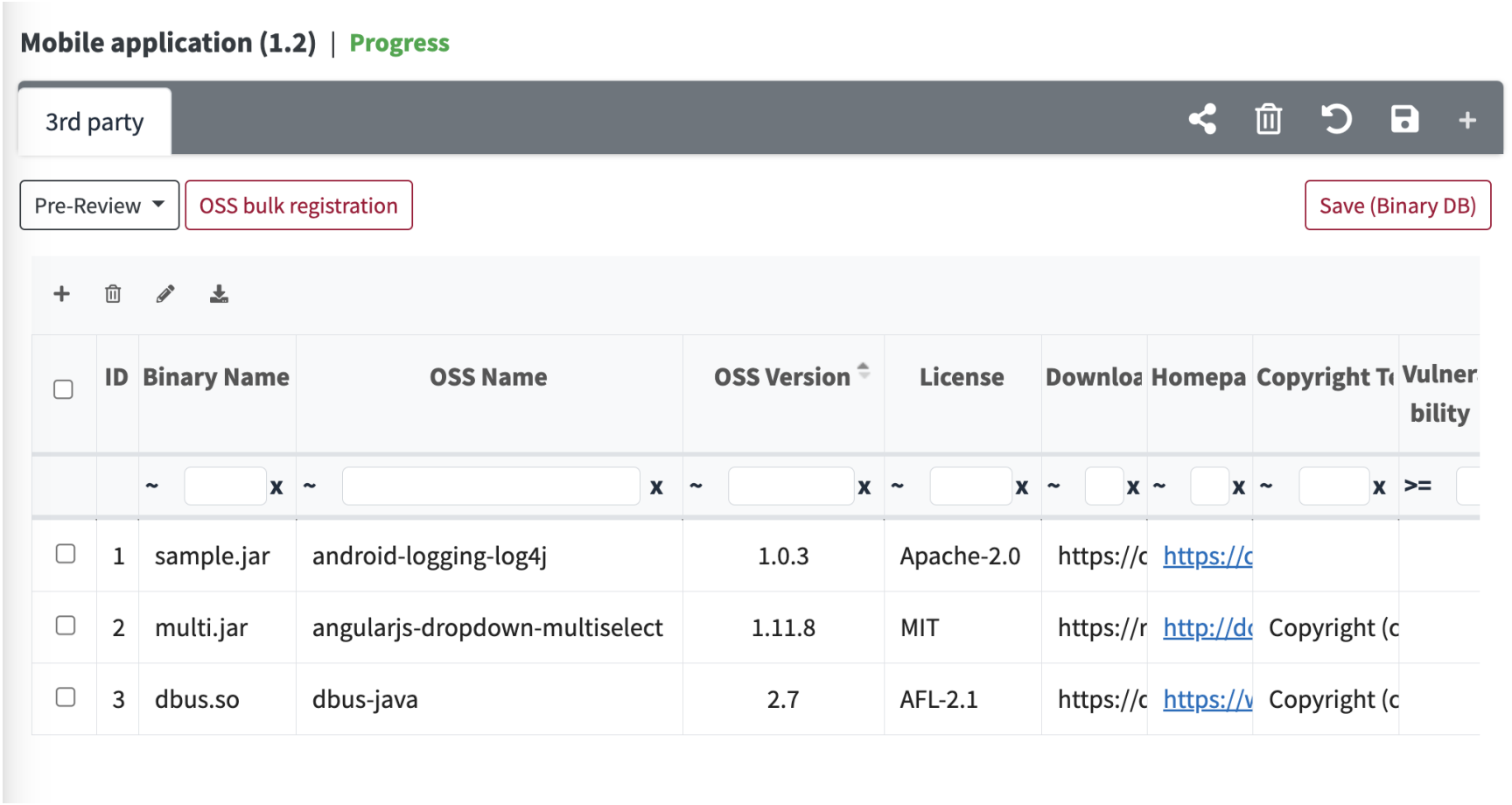


SBOM 변경 추적



공급망 관리

- 타사에서 전달받은 Software 별 SBOM 관리 가능



	ID	Binary Name	OSS Name	OSS Version	License	Downloa	Homepa	Copyright Te	Vulner bility
		~ x	~ x	~ x	~ x	~ x	~ x	~ x	>=
☐	1	sample.jar	android-logging-log4j	1.0.3	Apache-2.0	https://c	https://c		
☐	2	multi.jar	angularjs-dropdown-multiselect	1.11.8	MIT	https://r	http://dc	Copyright (c	
☐	3	dbus.so	dbus-java	2.7	AFL-2.1	https://c	https://v	Copyright (c	

FOSSLight Hub

오픈소스 및 라이선스 관리

- 오픈소스 정보 통합 관리
- 라이선스 의무사항 및 제약사항 확인
- 오픈소스 일괄 등록

컴플라이언스 프로세스 관리

- 올인원 오픈소스 컴플라이언스 수행
- 고지문 자동 생성 및 공개 소스코드 검증
- 이슈 트래킹

보안취약점 관리

- 보안취약점 조회
- 프로젝트별 보안취약점 모니터링 (자동 메일 알림)

사전점검

- 오픈소스 자동 분석
- 라이선스 자동 검출
- 라이선스 의무사항 및 보안취약점 알림

SBOM 관리

- 오픈소스 및 상용 소프트웨어 목록 관리
- 소프트웨어별 사용 프로젝트 검색
- SPDX, CycloneDX 문서 지원 (ISO 표준)

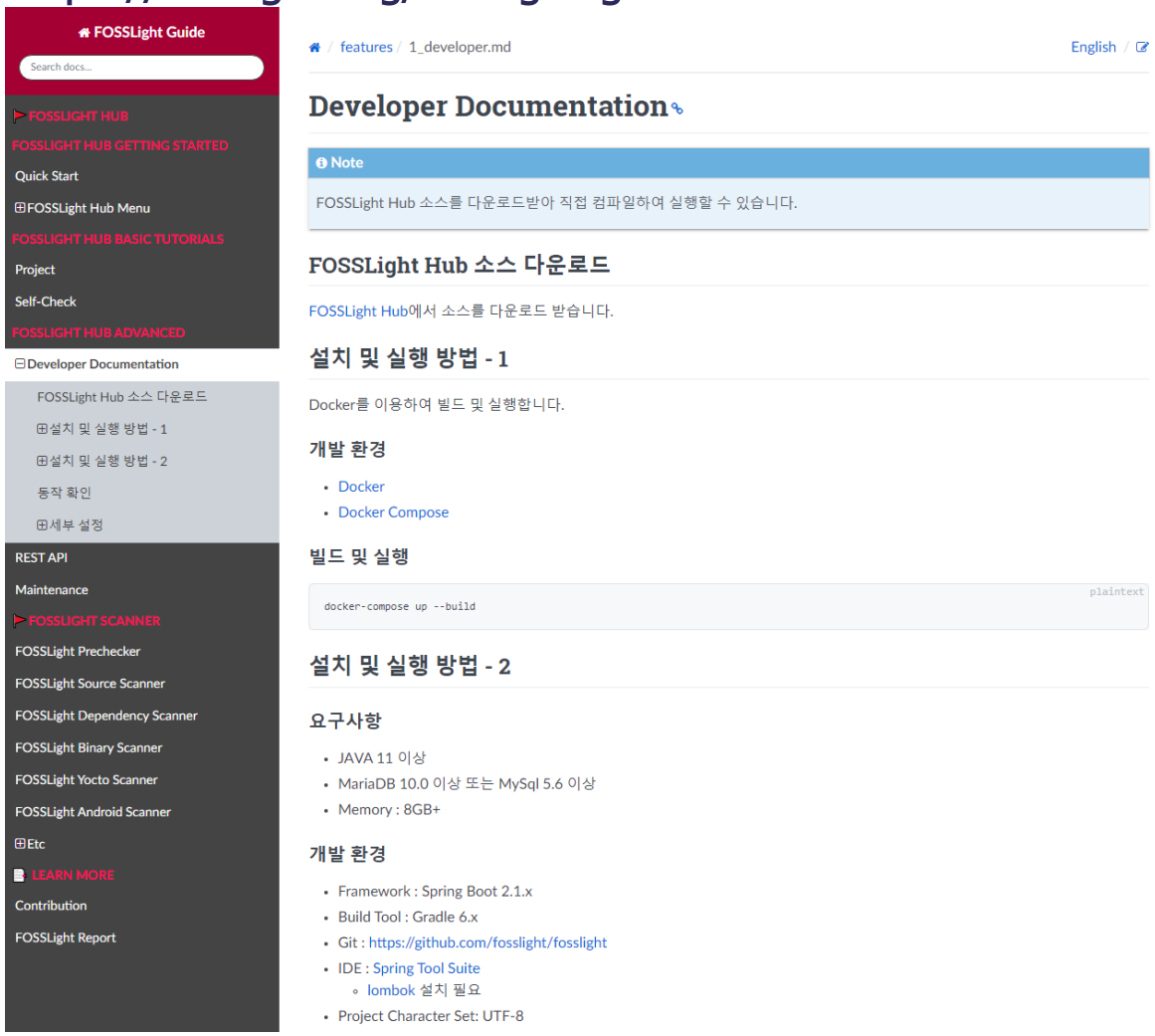
SW 공급망 관리

- 공급받은 타사 소프트웨어 관리
- 오픈 소스 확약서 관리
- 프로젝트 자동 연계

FOSSLight 설치 및 관리

개발 환경 설정

- https://fosslight.org/fosslight-guide



개발 환경 설정

- 소스 코드 빌드 & 실행
  - Java, MariaDB 설치 필요

1. JAVA를 설치합니다.: https://openjdk.java.net
2. DDL : fosslight_create.sql
3. MariaDB 또는 Mysql 설치합니다. : https://mariadb.org/download
4. Database 생성 및 초기 Data 등록

```
mysql -u root -p < fosslight_create.sql
```

More …

- Docker로 빌드 & 실행
  - 자동으로 DB, Java 세팅하여 쉽게 실행 가능

개발 환경

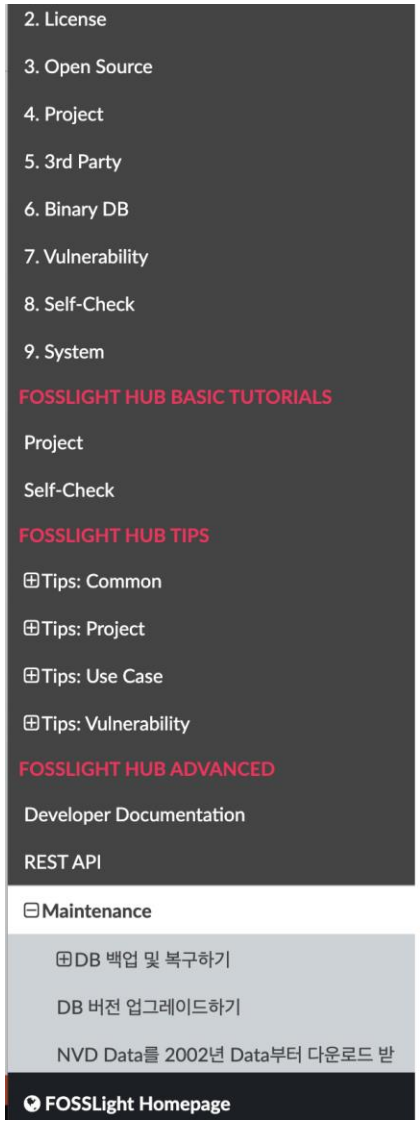
- Docker
- Docker Compose

빌드 및 실행

```
plaintext
docker-compose up --build
```

NVD Data 초기 다운로드 필요

DB 백업 및 복구



Maintenance

Note

FOSSLight Hub를 운영하는 데 유용한 가이드입니다.

DB 백업 및 복구하기

1. 백업

선택1. 전체 백업

mysqldump -u[아이디] -p[패스워드] [데이터베이스명] > [백업파일명].sql

```plaintext
$ mysqldump -ufosslight -pfosslight fosslight > fosslight_backup.sql
```

선택2. FOSSLight 최신 버전으로 업데이트를 위한 DB 백업 (Data만 추출)

mysqldump -u[아이디] -p[패스워드] [데이터베이스명] -no-create-info > [백업파일명].sql

```plaintext
$ mysqldump -ufosslight -pfosslight fosslight --no-create-info > fosslight_backup.sql
```

2. 복구

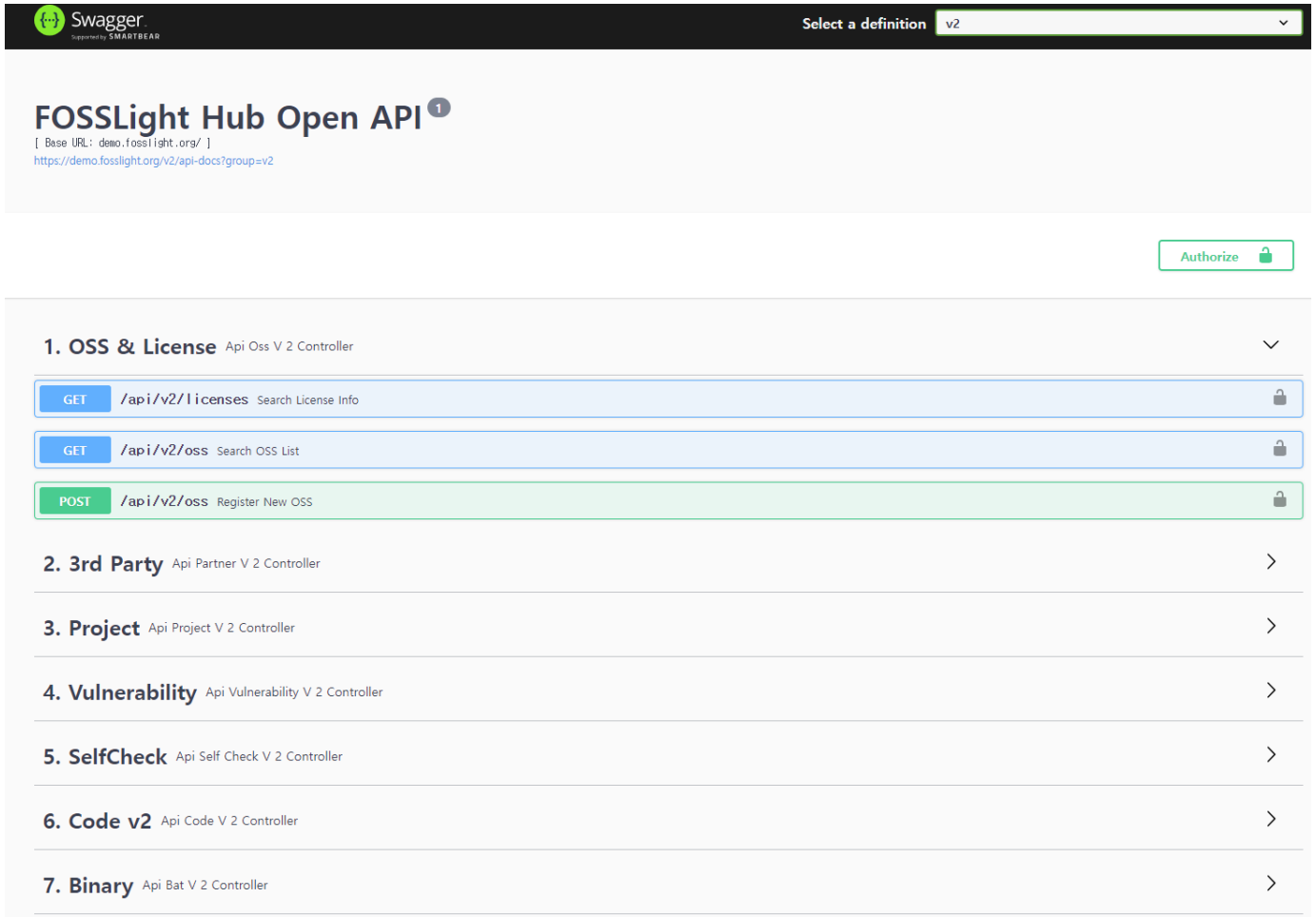
1. 버전에 따른 Table 구조를 반영하기 위해 빈 DB를 새로 만들고 기본 값을 설정합니다. Developer Documentation - 다운로드 & 설치 - 4. Database 생성 및 Data 초기 등록
2. 백업한 파일로 복구합니다. mysql -u[아이디] -p[패스워드] [데이터베이스명] < [백업파일명].sql

```plaintext
$ mysql -ufosslight -pfosslight fosslight < fosslight_backup.sql
```

Migration Script 제공

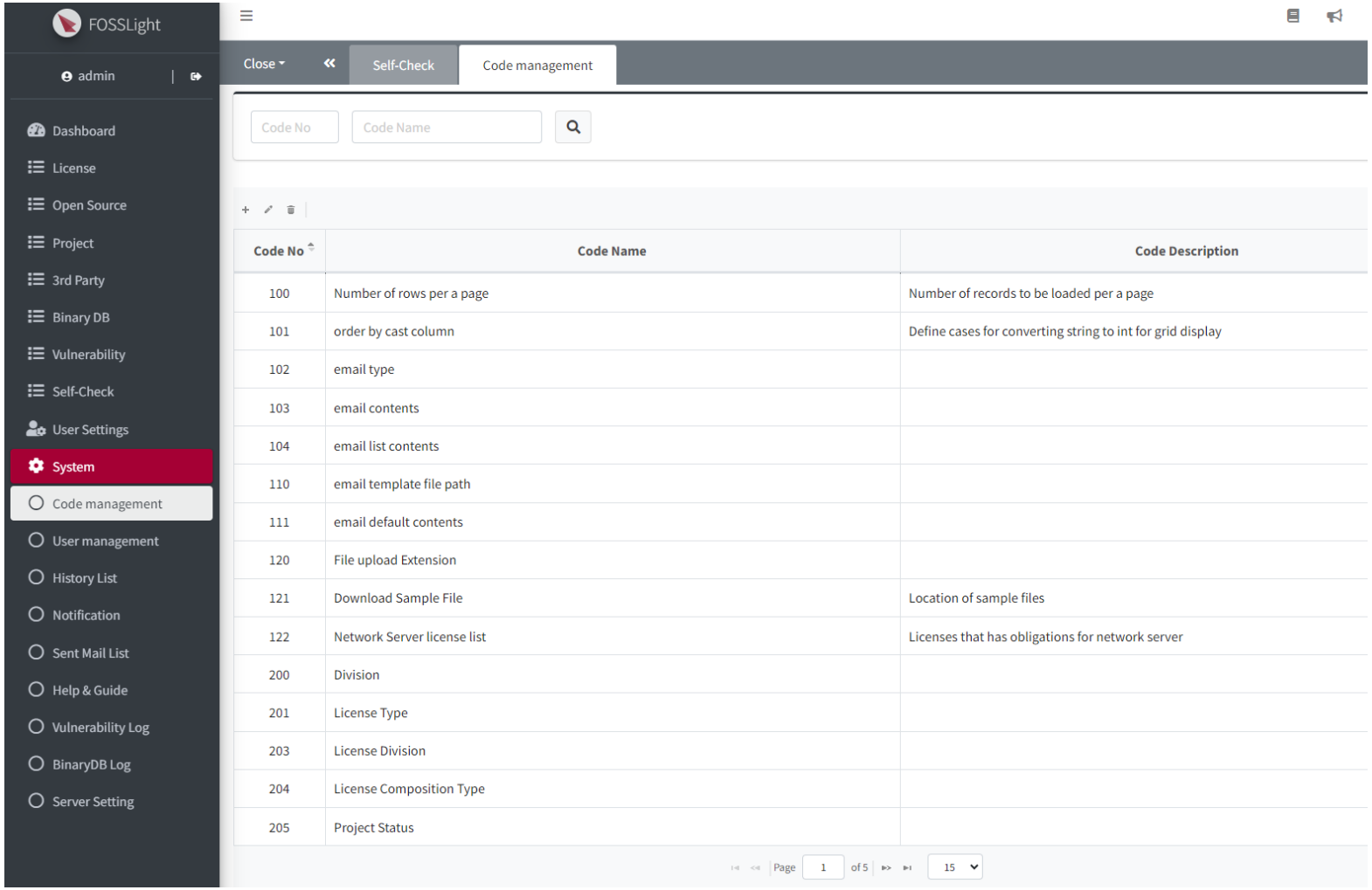
REST API

- 다른 툴과 연동할 수 있도록 REST API를 제공
  - ➢ TOKEN은 User Management에서 발행 가능



System 메뉴

- Admin 권한으로 접속시 확인 가능한 시스템 관리 메뉴



THANK YOU !