

# 입문자를 위한 FOSSLight 소개

LG전자 김경애




LG Open Source

# 기업의 오픈소스 관리 방안




# FOSSLight Open Source Project



## FOSSLight

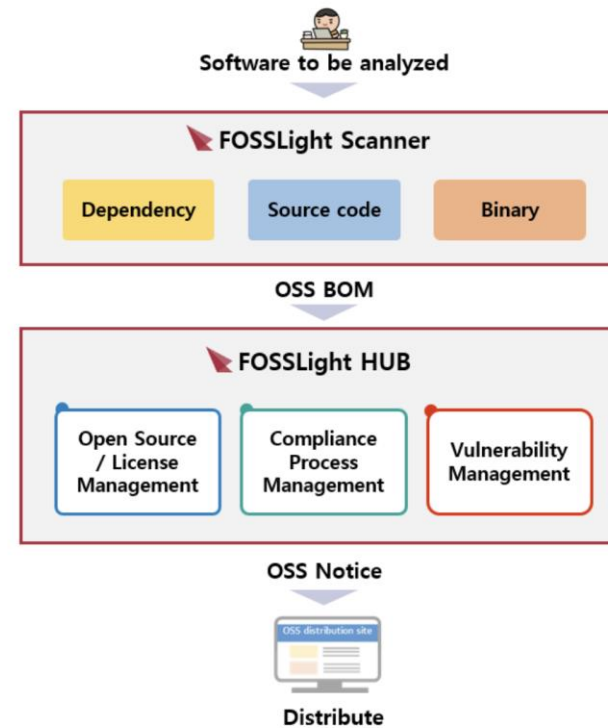
FOSSLight으로 완성하는 Open Source Governance

- [HUB](#)
- [SCANNER](#)
- [GUIDE](#)
- [DEMO](#)
- [NEWS](#)

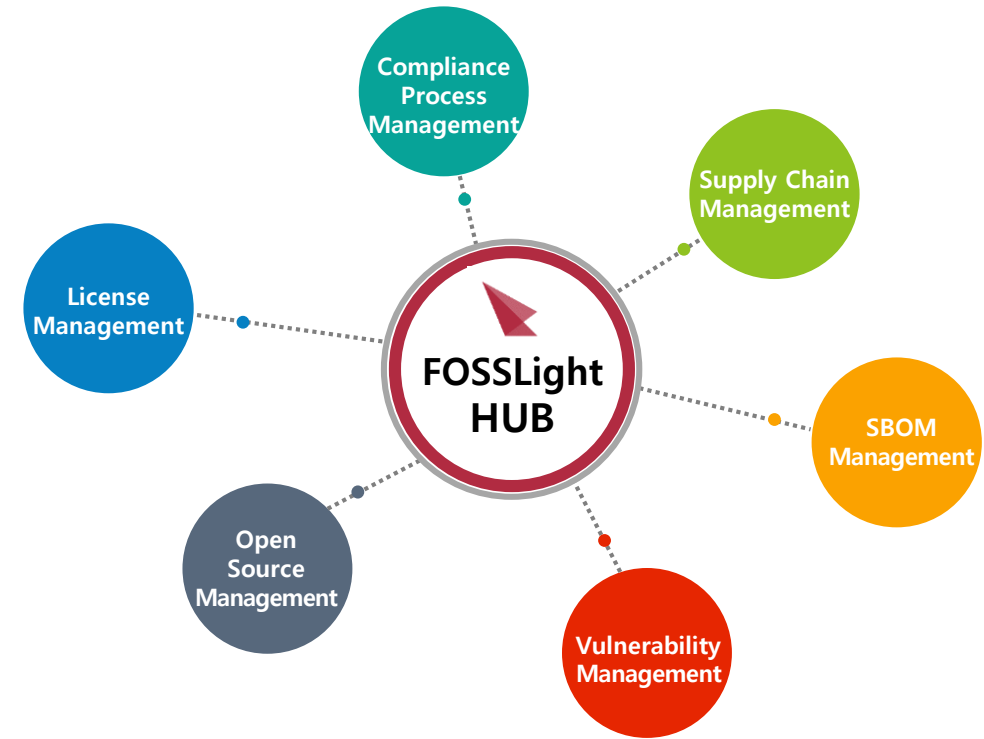
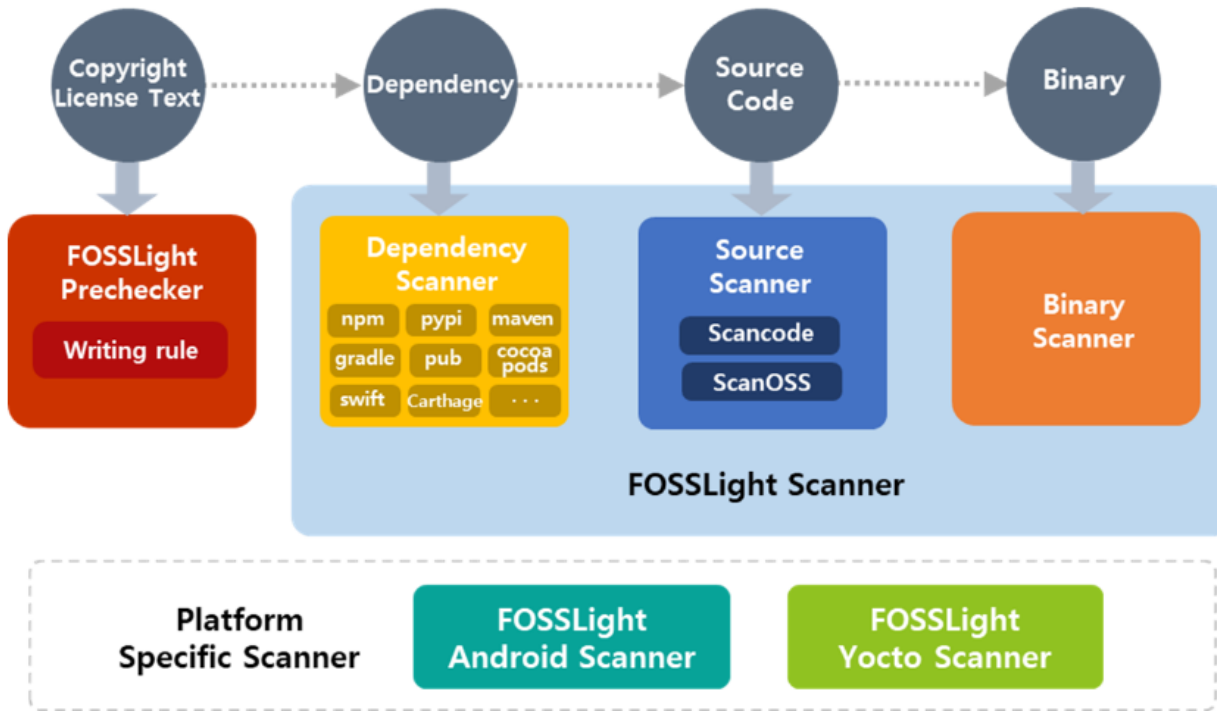


## FOSSLight

오픈 소스를 사용하여 소프트웨어를 개발하고 배포할 때,  
오픈 소스 거버넌스를 위해 FOSSLight을 활용하실 수 있습니다.



# FOSSLight



# 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

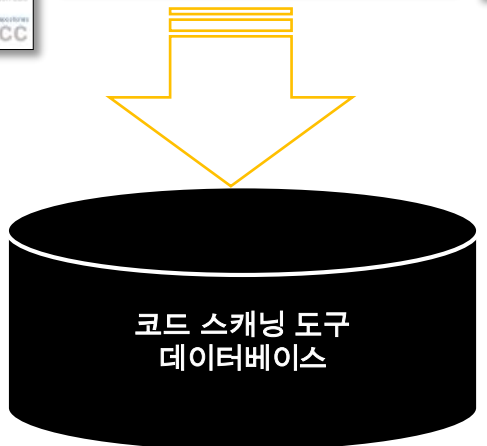
- 소스 코드 내 라이선스 문구가 변경 혹은 삭제되었다면?

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

- 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



“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;
}
```



snippet	OSS name	License
<pre>int divide(int a, int b) {     return a / b; }</pre>	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) 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;
}
  
```

```

* 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 예시

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



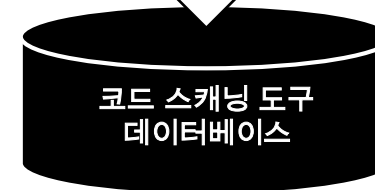
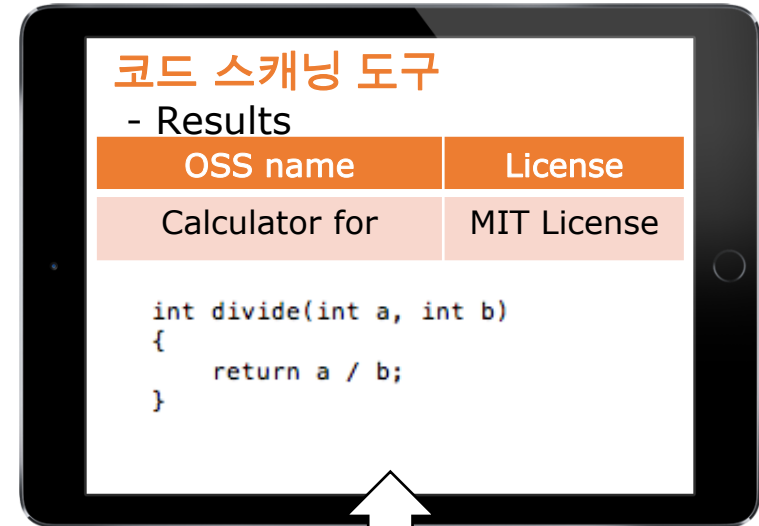
소스 코드 분석

```

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

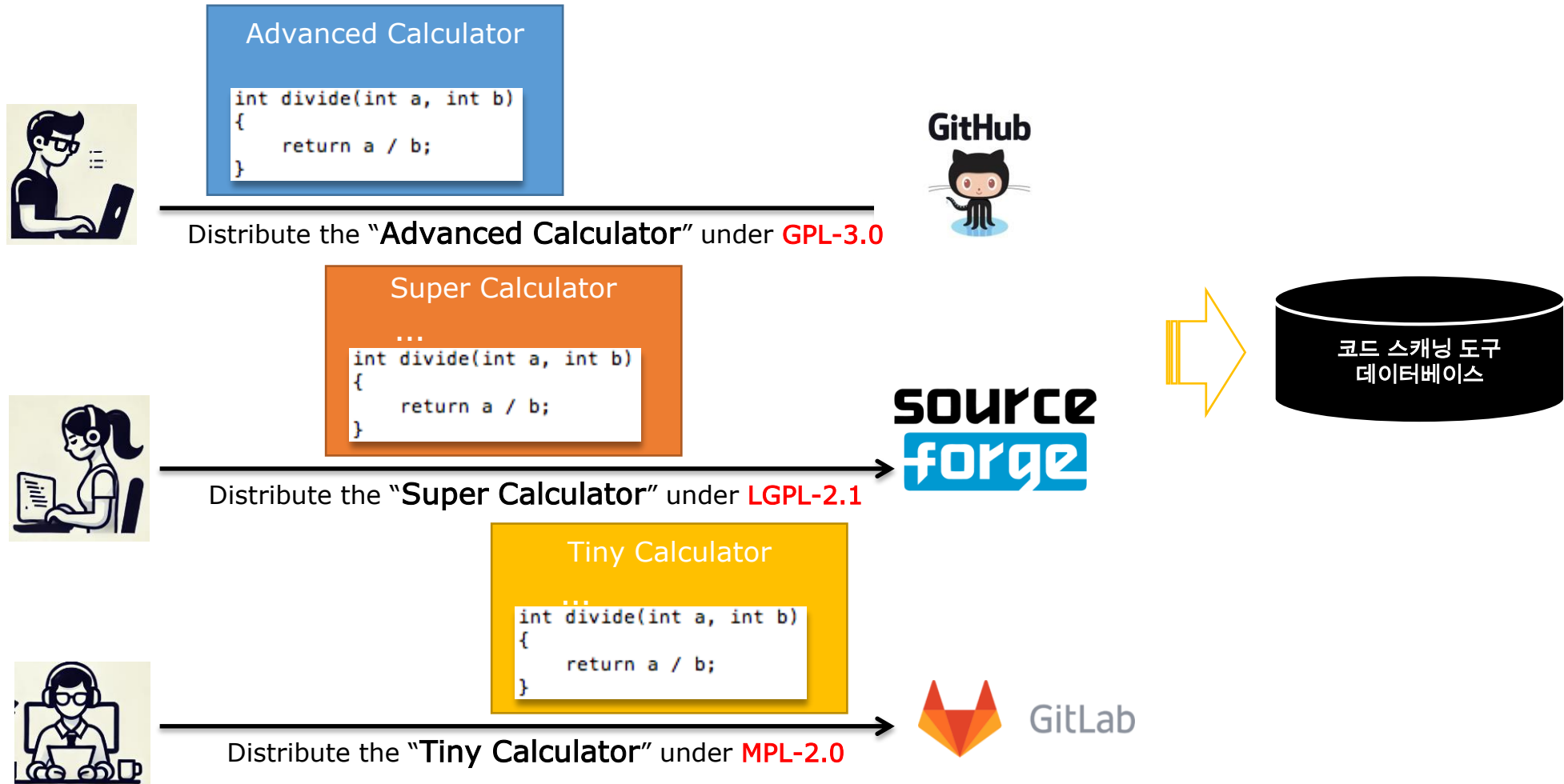
/*
* This is a function from an open source file.
*/
int divide(int a, int b)
{
    return a / b;
}

```



# 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

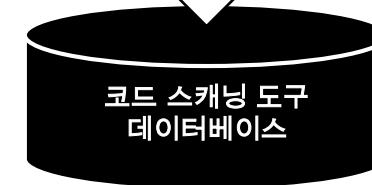
```

* 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;
}

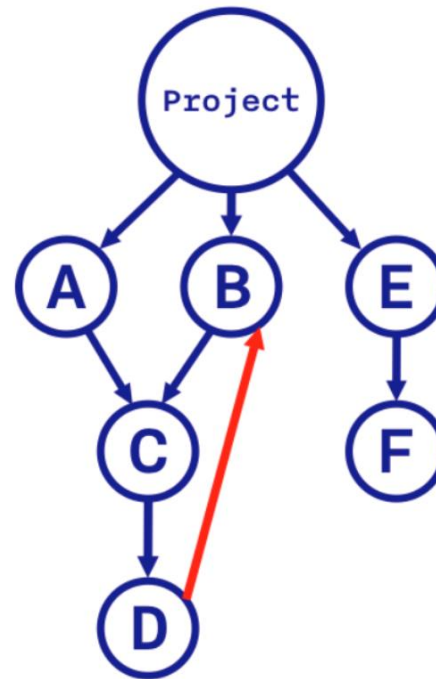
```

OSS name	License
Advanced Calculator	GPL-3.0
Super Calculator	LGPL-2.1
Tiny Calculator	MPL-2.0
Calculator for division	MIT License



## 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",
  "depredate": "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": "*"
},
```

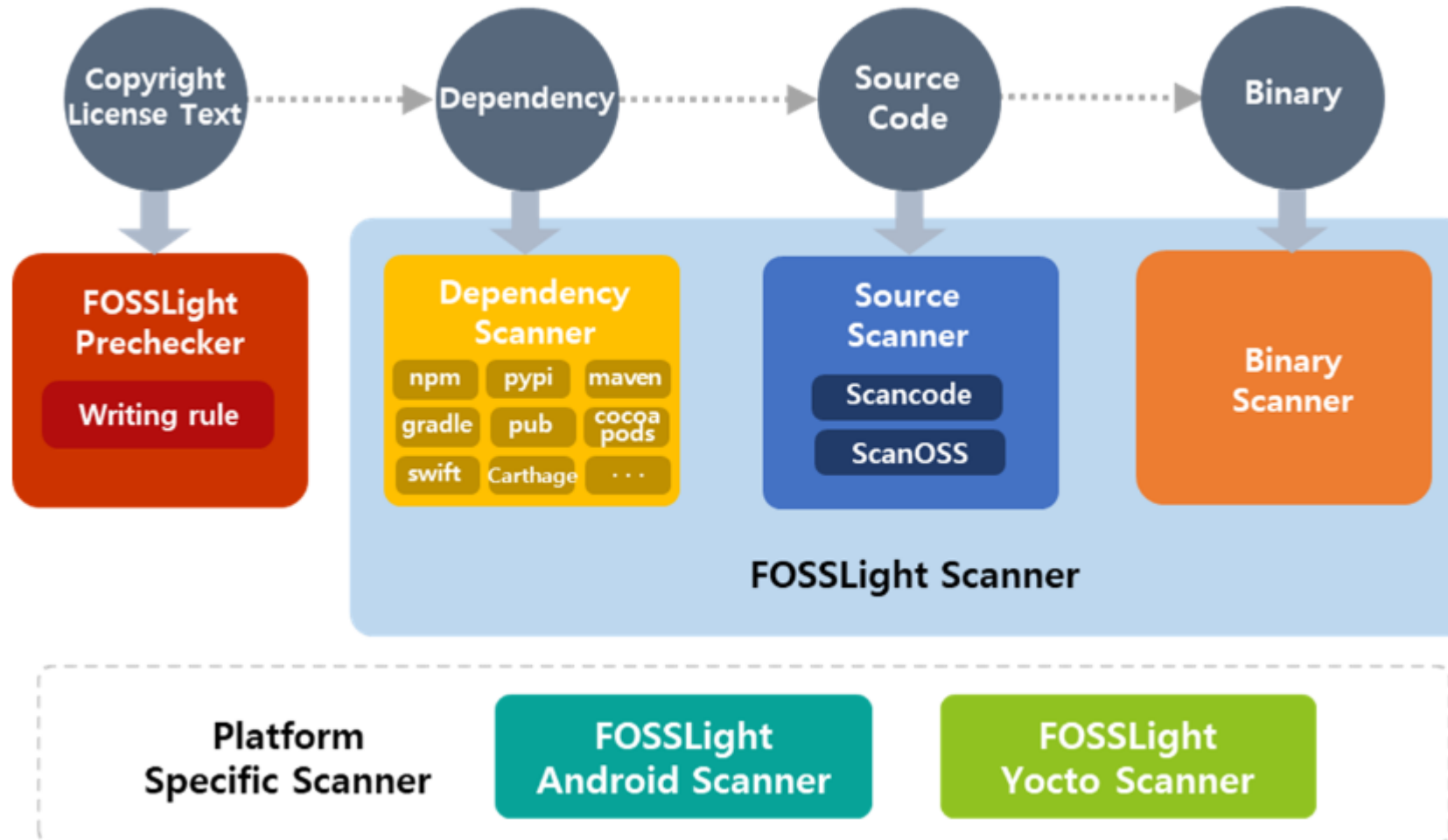
```
@types/body-parser package.json
"dependencies": {
  "@types/connect": "*",
  "@types/node": "*"
},
```



# FOSSLight Scanner

---

# FOSSLight Scanner



# 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 in	[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_image	2.3.2+1	MIT	https://pub.dev/packages/pub:cached_network_image/versions/2.3.2+1	https://github.com/Baseflow/flutter_cached_network_image	
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_handler	
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_blurhash	
15	pubspec.yaml pub:flutter_cache_manager	1.4.2	MIT	https://pub.dev/packages/pub:flutter_cache_manager/versions/1.4.2	https://github.com/Baseflow/flutter_cache_manager	

# FOSSLight Scanner – Source

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

A	B	C	D	E	F	G	H	I	J	K	L	M
ID	Source Name	OSS Name	OSS Version	License	Download	Homepage	Copyright	Exclude	Comment	scanoss_matched_lines	scanoss_fileURL	scanoss_vendor
1	reuse/_lic	reuse	0.11.0	apache-2.0	<a href="https://pypl.org/project/reuse">https://pypl.org/project/reuse</a>					100%(all)	<a href="https://osskb.org/api/file_contents/2dd68264374297fd5">https://osskb.org/api/file_contents/2dd68264374297fd5</a>	Carmen Bianca Bakker
2	reuse/repr	reuse-tool	0.10.0	cc0-1.0, gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>					94%(1-266,270-382)	<a href="https://osskb.org/api/file_contents/04cd419ee2fba863f37cd">https://osskb.org/api/file_contents/04cd419ee2fba863f37cd</a>	fsfe
3	reuse/_in	reuse-tool	0.14.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>					100%(all)	<a href="https://osskb.org/api/file_contents/5d16dbd923c75cc14f90a3">https://osskb.org/api/file_contents/5d16dbd923c75cc14f90a3</a>	fsfe
4	reuse/_cc	reuse-tool	0.14.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>					99%(1-705)	<a href="https://osskb.org/api/file_contents/7edb106b63c7948e23bd">https://osskb.org/api/file_contents/7edb106b63c7948e23bd</a>	fsfe
5	reuse/_fo	reuse-tool	0.10.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>					100%(all)	<a href="https://osskb.org/api/file_contents/7ae7b65dd442bbb31a">https://osskb.org/api/file_contents/7ae7b65dd442bbb31a</a>	fsfe
6	reuse/_m	reuse-tool	0.14.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>					100%(all)	<a href="https://osskb.org/api/file_contents/2299f5e58eed70969aad">https://osskb.org/api/file_contents/2299f5e58eed70969aad</a>	fsfe
7	reuse/_ut	reuse	0.13.0	gpl-3.0-or-later	<a href="https://pypl.org/project/reuse">https://pypl.org/project/reuse</a>					99%(1-360)	<a href="https://osskb.org/api/file_contents/8552ff8658f368126860ae">https://osskb.org/api/file_contents/8552ff8658f368126860ae</a>	Carmen Bianca Bakker
8	reuse/dow	reuse-tool	0.14.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>					100%(all)	<a href="https://osskb.org/api/file_contents/f965edd9602de6e183e3e">https://osskb.org/api/file_contents/f965edd9602de6e183e3e</a>	fsfe

A	B	C	D	E	F	G	H	I	J	K	L	M	N
ID	Source Name	OSS Name	OSS Version	License	Download	Homepage	Copyright	Exclude	Comment	license_reference	scanoss_matched_line	scanoss_fileURL	scanoss_vendor
1	reuse/resources/licenses	json		blissing, gpl-1.0, crystalstacker, mpl-1.0, 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	template	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-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				Copyright 2017 Free Software Foundation Europe (Scancode) gpl-3.0 / (Scanoss) gpl-3.0-only, gpl-3.0-or-later	100%(all)	<a href="https://osskb.org/api/file_contents/5d16dbd923c75cc14f90a3">https://osskb.org/api/file_contents/5d16dbd923c75cc14f90a3</a>	fsfe	
8	reuse/suppl	reuse-tool	0.14.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				Copyright 2021 Free (mit or apache-2.0) and other (Scancode) mit, gpl-3.0, apache-2.0, other-permissive / (Scanoss) gpl-3.0-or-later	100%(all)	<a href="https://osskb.org/api/file_contents/bcbdbdf45e7d21baa0e3">https://osskb.org/api/file_contents/bcbdbdf45e7d21baa0e3</a>	fsfe	
9	reuse/repr	reuse-tool	0.10.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				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)	<a href="https://osskb.org/api/file_contents/04cd419ee2fba863f37cd">https://osskb.org/api/file_contents/04cd419ee2fba863f37cd</a>	fsfe	
10	reuse/_cor	reuse-tool	0.14.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				Copyright 2019 Free Software Foundation Europe (Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later	99%(1-705)	<a href="https://osskb.org/api/file_contents/7edb106b63c7948e23bd">https://osskb.org/api/file_contents/7edb106b63c7948e23bd</a>	fsfe	
11	reuse/_for	reuse-tool	0.10.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				Copyright 2018 Free Software Foundation Europe (Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later	100%(all)	<a href="https://osskb.org/api/file_contents/7ae7b65dd442bbb31a">https://osskb.org/api/file_contents/7ae7b65dd442bbb31a</a>	fsfe	
12	reuse/_ma	reuse-tool	0.14.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				Copyright 2017 Free Software Foundation Europe (Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later	100%(all)	<a href="https://osskb.org/api/file_contents/2299f5e58eed70969aad">https://osskb.org/api/file_contents/2299f5e58eed70969aad</a>	fsfe	
13	reuse/hea	code-com	0.0.3	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				Copyright 2019 Free Software Foundation Europe (Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later	93%(14-46,46-226,236)	<a href="https://osskb.org/api/file_contents/2b07fbc3a9689d762946">https://osskb.org/api/file_contents/2b07fbc3a9689d762946</a>	miguelvictor	
14	reuse/init	reuse-tool	0.10.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				Copyright 2019 Free Software Foundation Europe (Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later	100%(all)	<a href="https://osskb.org/api/file_contents/ad3709b8ac32a35a011cef">https://osskb.org/api/file_contents/ad3709b8ac32a35a011cef</a>	fsfe	
15	reuse/lint	reuse-tool	0.14.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				Copyright 2017 Free Software Foundation Europe (Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later	100%(all)	<a href="https://osskb.org/api/file_contents/1244fc293c79045186e403">https://osskb.org/api/file_contents/1244fc293c79045186e403</a>	fsfe	
16	reuse/proj	reuse	0.13.0	gpl-3.0-or-later	<a href="https://pypl.org/project/reuse">https://pypl.org/project/reuse</a>				Copyright 2017 Free Software Foundation Europe (Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later	100%(all)	<a href="https://osskb.org/api/file_contents/069dca08882a15c19922ce">https://osskb.org/api/file_contents/069dca08882a15c19922ce</a>	Carmen Bianca Bakker	
17	reuse/spd	reuse-tool	0.10.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				Copyright 2017 Free Software Foundation Europe (Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later	100%(all)	<a href="https://osskb.org/api/file_contents/6dced70e072b66af8644d">https://osskb.org/api/file_contents/6dced70e072b66af8644d</a>	fsfe	
18	reuse/vcs	reuse-tool	0.10.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				Copyright 2017 Free Software Foundation Europe (Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later	100%(all)	<a href="https://osskb.org/api/file_contents/151098752336cfe62ce431">https://osskb.org/api/file_contents/151098752336cfe62ce431</a>	fsfe	
19	reuse/_lic	reuse	0.11.0	gpl-3.0-or-later	<a href="https://pypl.org/project/reuse">https://pypl.org/project/reuse</a>				Copyright 2019 Free Software Foundation Europe (Scancode) gpl-3.0, apache-2.0 / (Scanoss) gpl-3.0-or-later, apache-2.0	100%(all)	<a href="https://osskb.org/api/file_contents/2dd68264374297fd50a3a1">https://osskb.org/api/file_contents/2dd68264374297fd50a3a1</a>	Carmen Bianca Bakker	
20	reuse/_util	reuse	0.13.0	gpl-3.0-or-later	<a href="https://pypl.org/project/reuse">https://pypl.org/project/reuse</a>				Copyright 2017 Free Software Foundation Europe (Scancode) gpl-3.0, unknown-spdx / (Scanoss) gpl-3.0-or-later	99%(1-360)	<a href="https://osskb.org/api/file_contents/8552ff8658f368126860ae">https://osskb.org/api/file_contents/8552ff8658f368126860ae</a>	Carmen Bianca Bakker	
21	reuse/dow	reuse-tool	0.14.0	gpl-3.0-or-later	<a href="https://github.com/fsfe/reuse-tool">https://github.com/fsfe/reuse-tool</a>				Copyright 2019 Free Software Foundation Europe (Scancode) gpl-3.0, unknown-spdx or unknown-spdx / (Scanoss) gpl-3.0-or-later	100%(all)	<a href="https://osskb.org/api/file_contents/f965edd9602de6e183e3e">https://osskb.org/api/file_contents/f965edd9602de6e183e3e</a>	fsfe	
22	reuse/templates/default	template	unknown-cv						Copyright 2019 Free Software Foundation Europe (Scancode) gpl-3.0, unknown-spdx or unknown-spdx / (Scanoss) gpl-3.0-or-later				

# FOSSLight Scanner - Binary

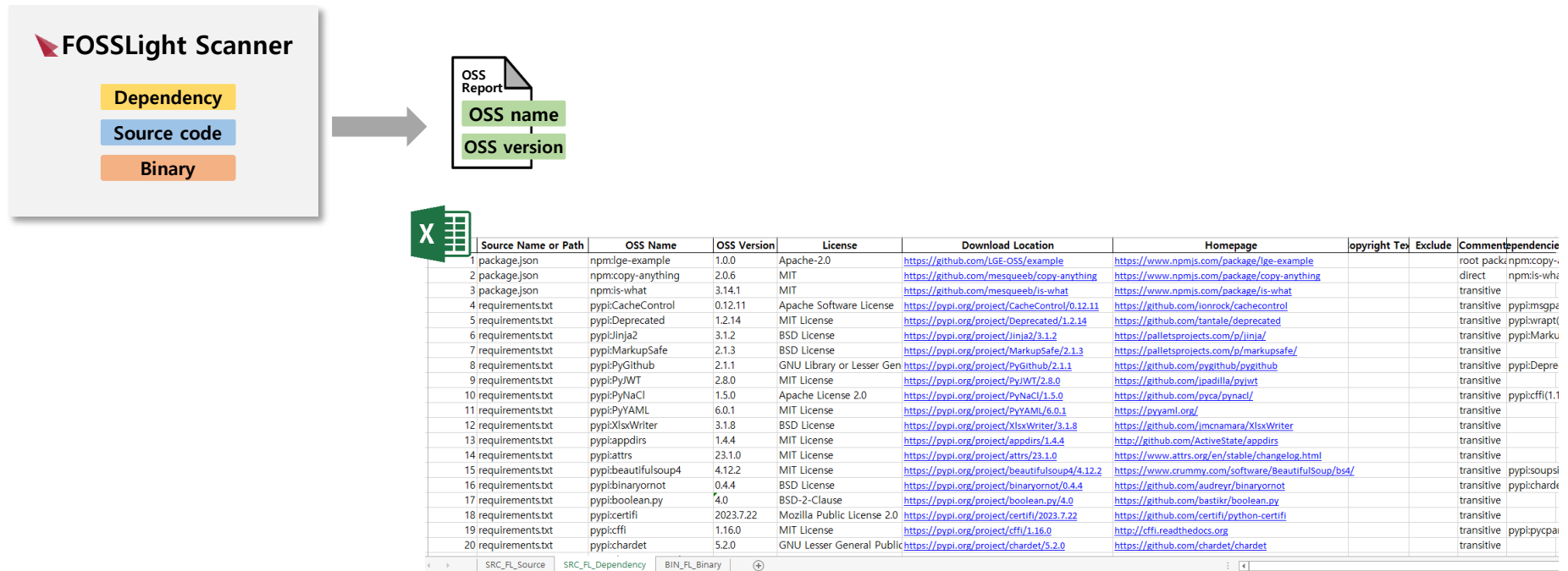
- 바이너리 목록 추출하여 Database에서 오픈소스 정보 확인
- Jar 파일에 대하여 보안 취약점 확인도 가능



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

# FOSSLight Scanner를 통한 SBOM 생성

- FOSSLight Scanner 실행하여 오픈소스 분석 보고서 생성



# 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

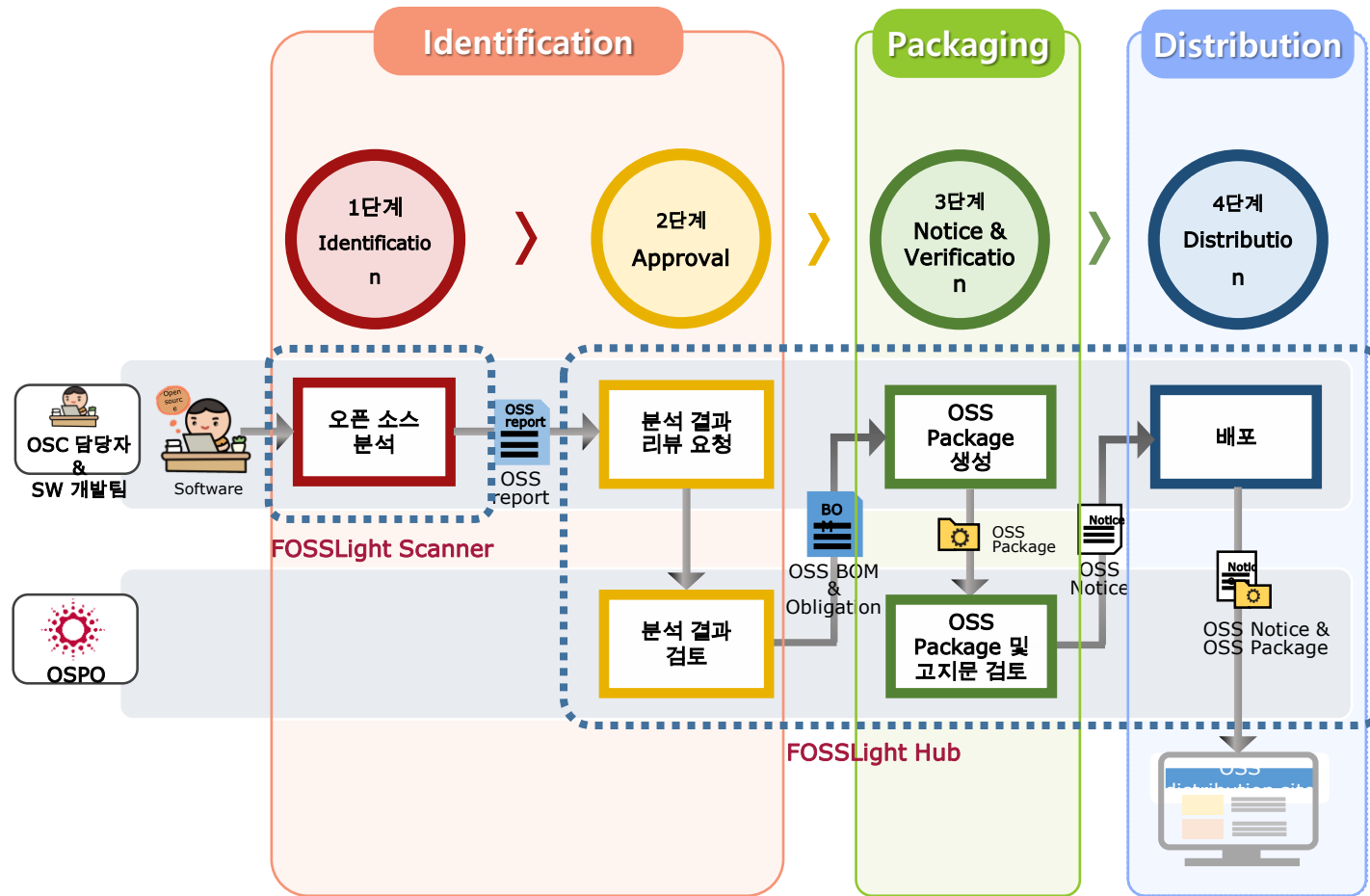
	ID	OSS Name	OSS Version	License Name	Obligation <span>i</span>
<input type="checkbox"/>	93432	[Nick] <a href="#">bjorklund</a>	1.0.1	MIT	
<input type="checkbox"/>	93429	[Nick] <a href="#">ashpy</a>	0.4.0	Apache-2.0	
<input type="checkbox"/>	93428	[Nick] <a href="#">async-array-methods</a>	2.1.0	MIT	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

# 라이선스 관리

- 라이선스별로 의무사항, 제약사항, 준수사항 관리

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

# 참고) LG전자 오픈소스 컴플라이언스 프로세스



# 컴플라이언스 프로세스 관리

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

ID	Project Name	Status	OSC Process	Download	Distribution Type	Security	Division	Creator	Reviewer
5219	hi_test_fosslight_util(ver_1.0)	Final Review	Identification > Packaging > Distribution	[X] [D]	Transfer in-house	Need to resolve(9.8)	CTO ICT기술센	일반이혜인	이혜인/선임연
5218	test(ver_444566)	Progress	Identification > Packaging > Distribution		General	Need to resolve(9.8)	BS BS연구소	soim	
5217	version	Progress	Identification > Packaging > Distribution	[X] [D]	General	Need to resolve(9.8)	CTO SW센터	김경애/Task Le	김경애/Task Le
5214	test_3rd(ver_1.0)	Progress	Identification > Packaging > Distribution	[X]	General	Need to resolve(7.8)	BS ID	민경선/책임연	민경선/책임연
5213	user hi test project	Progress	Identification > Packaging > Distribution		General	Discovered(N/A)	BS ID	일반이혜인	
5212	test_soijm(ver_1234)	Progress	Identification > Packaging > Distribution		General	Discovered(N/A)	CTO SW센터	김소임/책임연	
5211	api_create_project test	Review	Identification > Packaging > Distribution		General	Discovered(N/A)	CTO SW센터	시스템관리자	시스템관리자
5210	test_soijm(ver_123)	Request	Identification > Packaging > Distribution	[X] [D] [D] [D]	General	Need to resolve(9.8)	CTO SW센터	김소임/책임연	민경선/책임연
5209	hi_packaging test	Drop	Identification > Packaging > Distribution		General	Need to resolve(7.8)	CTO SW센터	이혜인/선임연	이혜인/선임연
5208	ssssaaa(ver_2)	Drop	Identification > Packaging > Distribution	[X] [D] [D]	General	Discovered(N/A)	CTO SW센터	민경선/책임연	
5207	noticehtml test	Progress	Identification > Packaging > Distribution		General	Need to resolve(10)	CTO SW센터	민경선/책임연	민경선/책임연
5206	test_csg(ver_test)	Review	Identification > Packaging > Distribution	[X]	General	Need to resolve(10)	CTO SW센터	석지영/책임연	석지영/책임연
5205	verify_test	Progress	Identification > Packaging > Distribution	[X]	General	Need to resolve(7.8)	CTO SW센터	시스템관리자	시스템관리자

# 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
<p>This product from LG Electronics, Inc. contains the open source software detailed below (including the source code included following this notice) for the terms and conditions of their use.</p>		
Open Source	License	
junit 4.12	EPL-1.0	

The source code for the above may be obtained free of charge from LG Electronics, Inc. (including the source code 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](mailto:opensource@lge.com). This offer is valid for 90 days 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:

- in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- in the case of each subsequent Contributor:
  - changes to the Program, and
  - 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

The screenshot displays the FOSSLight self-check interface. On the left, a 'Self-Check' window shows a 'FOSSLight Report' for '1341\_selfCheck' dated 2024-03-29 17:23:37. Below the report is a 'Pre-Review' section with a table of detected licenses.

ID	Binary Name or Source Path	OSS Name	OSS Version	License
48	example-1.0.1/package.json	This field is required.		Apache-2.0
39	example-1.0.1/LICENSE	This field is required.		Apache-2.0
63	example-1.0.1/third_party/httpptools	httpptools	0.0.4 Unconfirmed versio	MIT
64	example-1.0.1/third_party/httpptools	httpptools	0.0.7 Unconfirmed versio	MIT

On the right, a browser window shows the 'License text' for Apache License 2.0. The license text includes the title 'License text', version 'Version 2.0, January 2004', and the URL 'http://www.apache.org/licenses/'. It also includes the title 'TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION' and the section '1. Definitions.' with definitions for 'License', 'Licensor', 'Legal Entity', 'You', and 'Source'.

# 사전 점검 (Pre-Review)

- 오픈소스를 다운로드한 URL만 알아도 오픈소스와 라이선스 정보를 확인할 수 있음

Pre-Review ▾

	ID	Source Name o	OSS Name	OSS Version	License	Download Location	Homepage
		~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x
<input type="checkbox"/>	2		This field is required.	2.0.0	MIT	<a href="https://mvnrepository.com/artifact/org.slf4j/slf4j-api">https://mvnrepository.com/artifact/org.slf4j/slf4j-api</a>	<a href="http://www.slf4j.org">http://www.slf4j.org</a>
<input type="checkbox"/>	1		Test Spring Framework Unconfirmed open source	6.1.2	Apache-2.0	<a href="https://github.com/spring-projects/spring-framework">https://github.com/spring-projects/spring-framework</a>	<a href="https://github.com/spring-projects/spring-framewo">https://github.com/spring-projects/spring-framewo</a>
<input type="checkbox"/>	3		mybatis	3.5.9	EPL-2.0 Declared : Apache-2.0	<a href="https://mvnrepository.com/artifact/org.mybatis/mybatis">https://mvnrepository.com/artifact/org.mybatis/mybatis</a>	<a href="https://mybatis.org/mybatis-3">https://mybatis.org/mybatis-3</a>


# 사전 점검 (Pre-Review)

- 오픈소스를 다운로드한 URL만 알아도 라이선스 정보를 확인할 수 있음

Pre-Review ▾

ID	Source Name o	OSS Name	OSS Version	License	Download Location	Homepage
	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x
<input type="checkbox"/>	2	This field is required.	2.0.0	MIT	<a href="https://mvnrepository.com/artifact/org.slf4j/slf4j-api">https://mvnrepository.com/artifact/org.slf4j/slf4j-api</a>	<a href="http://www.slf4j.org">http://www.slf4j.org</a>
<input type="checkbox"/>	1	Test Spring Framework <small>Unconfirmed open source</small>	6.1.2	Apache-2.0	<a href="https://github.com/spring-projects/spring-framework">https://github.com/spring-projects/spring-framework</a>	<a href="https://github.com/spring-projects/spring-framewo">https://github.com/spring-projects/spring-framewo</a>
<input type="checkbox"/>	3	mybatis	3.5.9	EPL-2.0 <small>Declared : Apache-2.0</small>	<a href="https://mvnrepository.com/artifact/org.mybatis/mybatis">https://mvnrepository.com/artifact/org.mybatis/mybatis</a>	<a href="https://mybatis.org/mybatis-3">https://mybatis.org/mybatis-3</a>

License detected based on OSS Name, Version, and Download location. To change the license, click the "Change License" button.

Result	Download location	OSS name	OSS version	License (current)	License (to be changed)	Evidence
<input type="checkbox"/>	<a href="https://mvnrepository.com/artifact/org.mybatis/mybatis">https://mvnrepository.com/artifact/org.mybatis/mybatis</a>	mybatis	3.5.9	EPL-2.0 <small>Declared : Apache-2.0</small>	Apache-2.0	 DB

Change License



# 사전 점검 (Pre-Review)

- 오픈소스를 다운로드한 URL만 알아도 오픈소스 정보를 확인할 수 있음

Pre-Review ▾

+ ✖ ✎ ⏴

<input type="checkbox"/>	ID	Source Name o	OSS Name	OSS Version	License	Download Location	Homepage
		~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x
<input type="checkbox"/>	2		This field is required.	2.0.0	MIT	<a href="https://mvnrepository.com/artifact/org.slf4j/slf4j-api">https://mvnrepository.com/artifact/org.slf4j/slf4j-api</a>	<a href="http://www.slf4j.org">http://www.slf4j.org</a>
<input type="checkbox"/>	1		Test Spring Framework Unconfirmed open source	6.1.2	Apache-2.0	<a href="https://github.com/spring-projects/spring-framework">https://github.com/spring-projects/spring-framework</a>	<a href="https://github.com/spring-projects/spring-framewo">https://github.com/spring-projects/spring-framewo</a>
<input type="checkbox"/>	3		mybatis	3.5.9	EPL-2.0 Declared : Apache-2.0	<a href="https://mvnrepository.com/artifact/org.mybatis/mybatis">https://mvnrepository.com/artifact/org.mybatis/mybatis</a>	<a href="https://mybatis.org/mybatis-3">https://mybatis.org/mybatis-3</a>

There exists another OSS which has same download location. Please click "Change OSS Name" if you want to change to the registered OSS Name.

<input type="checkbox"/>	Result	Download location	OSS name (now)	Registered OSS name (to be changed)
<input type="checkbox"/>		<a href="https://mvnrepository.com/artifact/org.slf4j/slf4j-api">https://mvnrepository.com/artifact/org.slf4j/slf4j-api</a>	This field is required.	<a href="#">slf4j</a>
<input type="checkbox"/>		<a href="https://github.com/spring-projects/spring-framework">https://github.com/spring-projects/spring-framework</a>	Test Spring Framework Unconfirmed open source	<a href="#">Spring Framework</a>

Change OSS Name

# 사전 점검 (Pre-Review)

- 오픈소스 라이선스 의무 사항 확인 가능함

The screenshot displays the FOSSlight self-check interface. On the left, a 'Pre-Review' table lists items for review. On the right, a browser window shows the license details for Apache-2.0.

ID	Binary Name or Source Path	OSS Name	OSS Version	License
<input type="checkbox"/>	~ [ ] x ~ [ ] x ~ [ ] x ~ [ ]			
<input type="checkbox"/>	example-1.0.1/package.json	This field is required.		Apache-2.0
<input type="checkbox"/>	example-1.0.1/LICENSE	This field is required.		Apache-2.0
<input type="checkbox"/>	example-1.0.1/third_party/httptools	httptools	0.0.4 Unconfirmed version	MIT
<input type="checkbox"/>	example-1.0.1/third_party/httptools	httptools	0.0.7 Unconfirmed version	MIT

License Name	Identifier	License Obligat	Restrict	Website	Nick Name
Apache License 2.0	Apache-2.0	Permis:		<a href="#">URL</a>	#Apache 2, #Apache 2.0, #Apache

**License text**

Apache License  
Version 2.0, January 2004  
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

# 사전 점검 (오픈소스 분석)

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

Self-Check
Notice
🔗 🗑️ ↺ 🔒 -

Upload Analysis Result
  URL

---

Enter the link of the source to be analyzed

Pre-Review ▾

+
🗑️
✎
📄

	ID	Binary Name or So	OSS Name	OSS Ver:	License	Download	Homepage	Copyright Text	OSS   Licen	User Vuln	Oblig	Restri	☐
	~	<input style="width: 80%;" type="text" value=""/>	x ~	<input style="width: 80%;" type="text" value=""/>	x ~	<input style="width: 80%;" type="text" value=""/>	x ~	<input style="width: 80%;" type="text" value=""/>	x ~	<input style="width: 80%;" type="text" value=""/>	x ~	<input style="width: 80%;" type="text" value=""/>	x ~

# FOSSLight Hub로 보안 취약점 관리하기

---

# 보안 취약점 조회

- 오픈소스 버전에 따른 보안 취약점 점수 및 내용 확인 가능

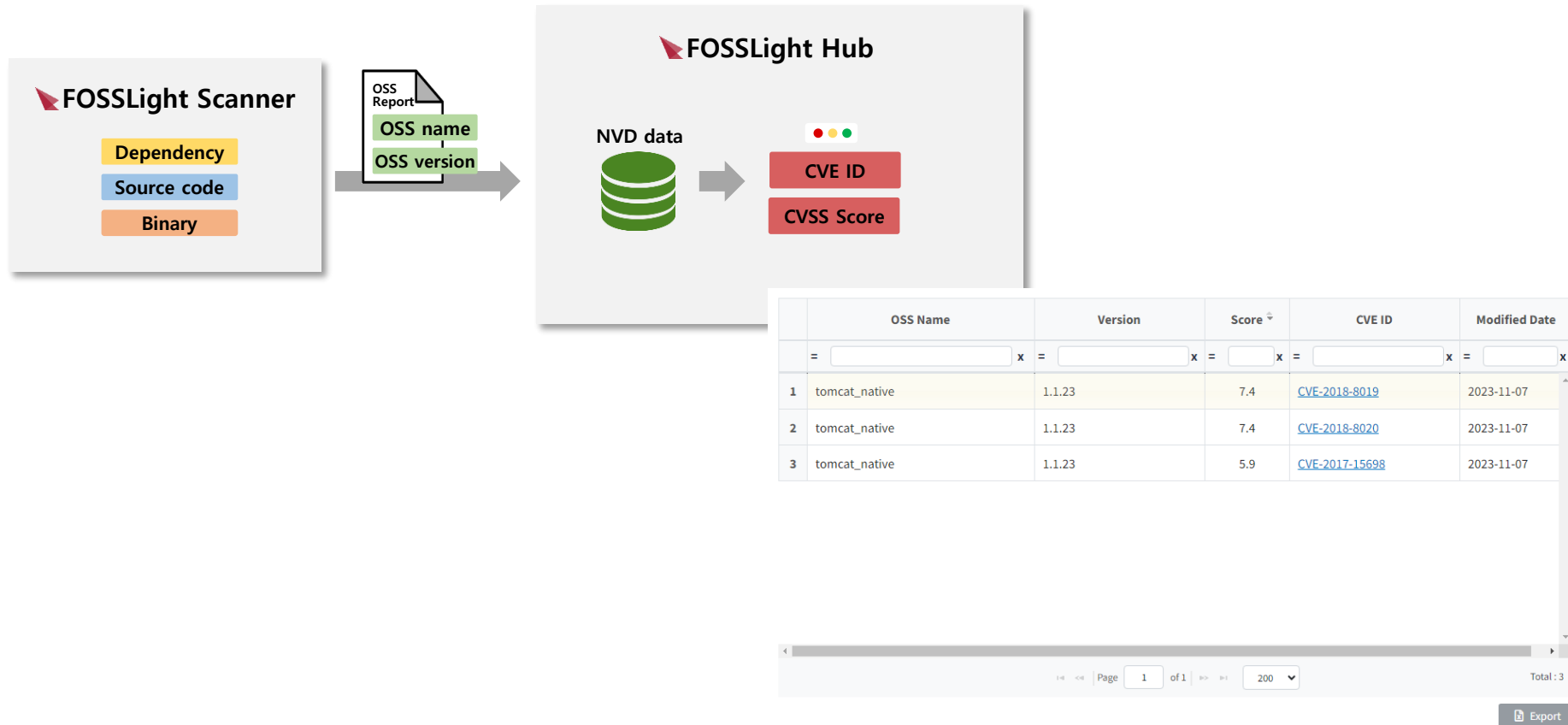
	OSS Name	Version	Score	CVE ID	Modified Date
1	tomcat_native	1.1.23	7.4	<a href="#">CVE-2018-8019</a>	2023-11-07
2	tomcat_native	1.1.23	7.4	<a href="#">CVE-2018-8020</a>	2023-11-07
3	tomcat_native	1.1.23	5.9	<a href="#">CVE-2017-15698</a>	2023-11-07

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 관리

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



1. **CVE ID** : CVE-2018-8019

2. **Description** : When using an OSCP 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 OSCP checks are not affected by this vulnerability. Al emplear un responder OSCP, 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 OSCP no se han visto afectados por esta vulnerabilidad.

# 보안 취약점 확인

- 개발 제품별 프로젝트 등록하여 프로젝트별 보안 취약점 확인 가능

The screenshot displays a web application interface for managing project security vulnerabilities. The interface is divided into two main sections: a project list on the left and a detailed BOM (Bill of Materials) view on the right.

**Project List (Left Panel):**

ID	Project Name	Status
5165	<a href="#">Auto Update Program</a>	Pro
5113	<a href="#">test (23_Copied54)</a>	Final
5070	<a href="#">Sample (23)</a>	Final
5069	<a href="#">User Management System</a>	Pro
5068	<a href="#">Scanner</a>	Pro
5067	<a href="#">db test (2_Copied)</a>	Pro
5066	<a href="#">Source Analyzer (1)</a>	Re
5065	<a href="#">db test (2)</a>	Re
5044	<a href="#">Purchase Management</a>	Re

**BOM View (Right Panel):**

3rd party DEP SRC BIN BOM

Auto Analysis OSS bulk registration Save (Binary DB)

ID	Referen	OSS Name	OSS Version	License	Download Locat	Homepage	Copyright Text	Vulnerability	Notify Sourc	Restrictio	admin check
50	DEP	gax-java	0.14.0 Unconfirmed vc	BSD-3-Clause	<a href="https://mvnrepo">https://mvnrepo</a>	<a href="https://mv">https://mv</a>			○		<input type="checkbox"/>
36	DEP	OSGi Resource L	1.0.1 Unconfirmed vc	CDDL-1.1	<a href="https://mvnrepo">https://mvnrepo</a>	<a href="https://mv">https://mv</a>			○ ○		<input type="checkbox"/>
17	DEP	gax-java	1.57.0 Unconfirmed vc	BSD-3-Clause	<a href="https://mvnrepo">https://mvnrepo</a>	<a href="https://mv">https://mv</a>			○		<input type="checkbox"/>
100	DEP	Netty	4.1.50 Unconfirmed vc	Apache-2.0	<a href="https://mvnrepo">https://mvnrepo</a>	<a href="https://mv">https://mv</a>		HIGH	○		<input type="checkbox"/>
60	DEP	firebase-admin	7.1.0 Unconfirmed vc	Apache-2.0	<a href="https://mvnrepo">https://mvnrepo</a>	<a href="https://mv">https://mv</a>			○		<input type="checkbox"/>
82	DEP	Netty	4.1.66 Unconfirmed vc	Apache-2.0	<a href="https://mvnrepo">https://mvnrepo</a>	<a href="https://mv">https://mv</a>		HIGH	○		<input type="checkbox"/>

Page 1 of 1 15

# 보안취약점 실시간 알림

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

## FOSSLight Hub Notification

### [OSC] Vulnerability Discovered

#### « Vulnerability Information »

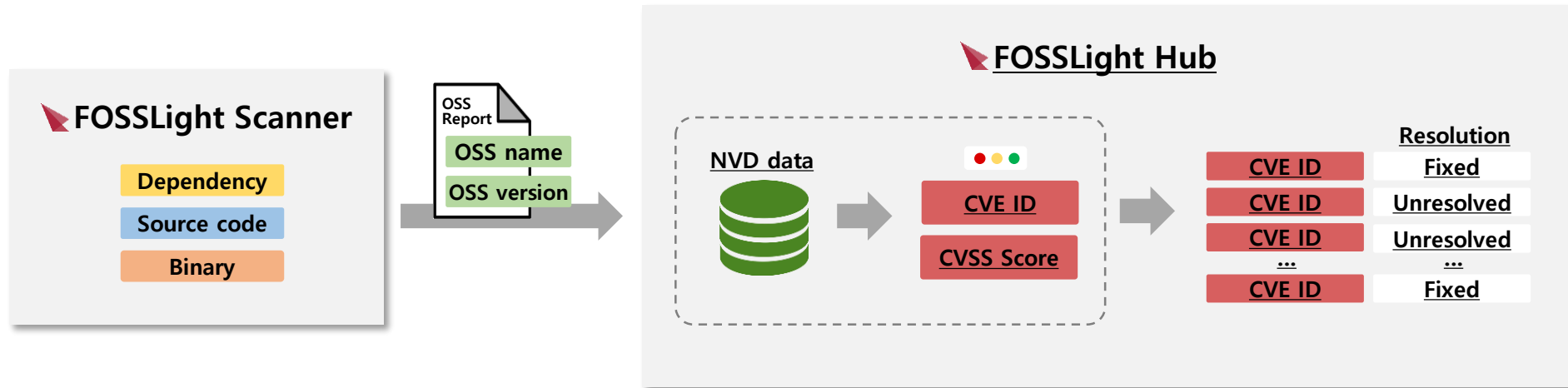
OSS ID	OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
22869	json-smart-v2	2.2.1	<a href="#">CVE-2021-27568</a>	9.1	An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as 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	<a href="#">CVE-2021-27568</a>	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](mailto:osc.lge.com)



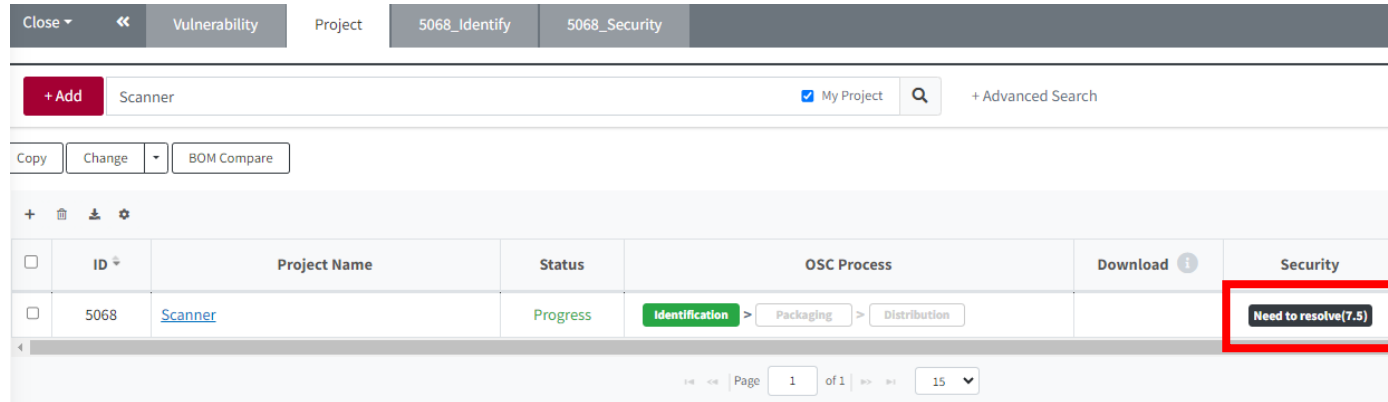
# 제품 보안취약점 수정 여부 관리 기능

- 프로젝트별로 발견된 보안취약점을 확인하고 해결 여부를 관리할 수 있음



# Security탭

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



The screenshot shows a web interface for project management. At the top, there are tabs for 'Vulnerability', 'Project', '5068\_Identify', and '5068\_Security'. Below the tabs, there is a search bar with '+ Add Scanner', a 'My Project' checkbox, and a search icon. Below the search bar, there are buttons for 'Copy', 'Change', and 'BOM Compare'. The main content is a table with the following columns: ID, Project Name, Status, OSC Process, Download, and Security. The table contains one row with ID '5068', Project Name 'Scanner', Status 'Progress', OSC Process 'Identification > Packaging > Distribution', and Security 'Need to resolve(7.5)'. A red arrow points to the 'Need to resolve(7.5)' text.

ID	Project Name	Status	OSC Process	Download	Security
5068	Scanner	Progress	Identification > Packaging > Distribution		Need to resolve(7.5)

# 보안 프로세스 관리

- 프로젝트별로 발견된 보안취약점을 확인하고 해결 여부를 관리할 수 있음

Total Fixed Not Fixed						
<input type="checkbox"/>	OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution
	~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>
<input type="checkbox"/>	appsmith	1.8.1	CVE-2022-4096	6.5	2022-11-21	Unresolved
<input type="checkbox"/>	appsmith	1.8.0	CVE-2022-4096	6.5	2022-11-21	Unresolved
<input type="checkbox"/>	appsmith	1.7.8	CVE-2022-39824	8.9	2022-09-05	Unresolved
<input type="checkbox"/>	appsmith	1.7.8	CVE-2022-4096	6.5	2022-11-21	Unresolved
<input type="checkbox"/>	appsmith	1.7.7	CVE-2022-39824	8.9	2022-09-05	Unresolved
<input type="checkbox"/>	appsmith	1.7.7	CVE-2022-4096	6.5	2022-11-21	Unresolved
<input type="checkbox"/>	appsmith	1.7.6	CVE-2022-39824	8.9	2022-09-05	Unresolved
<input type="checkbox"/>	appsmith	1.7.6	CVE-2022-4096	6.5	2022-11-21	Unresolved
<input type="checkbox"/>	appsmith	1.7.3	CVE-2022-39824	8.9	2022-09-05	Unresolved
<input type="checkbox"/>	appsmith	1.7.3	CVE-2022-4096	6.5	2022-11-21	Unresolved
<input type="checkbox"/>	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

Total Fixed Not Fixed								
<input type="checkbox"/>	OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution		
~	<input type="text"/>	x	~ <input type="text"/>	x	~ <input type="text"/>	x	~ <input type="text"/>	x
<input type="checkbox"/>	appsmith	1.8.1	CVE-2022-4096	6.5	2022-11-21	Unresolved		
<input type="checkbox"/>	appsmith	1.8.0	CVE-2022-4096	6.5	2022-11-21	Unresolved		
<input type="checkbox"/>	appsmith	1.7.8	CVE-2022-39824	8.9	2022-09-05	Unresolved		
<input type="checkbox"/>	appsmith	1.7.8	CVE-2022-4096	6.5	2022-11-21	Unresolved		
<input type="checkbox"/>	appsmith	1.7.7	CVE-2022-39824	8.9	2022-09-05	Unresolved		
<input type="checkbox"/>	appsmith	1.7.7	CVE-2022-4096	6.5	2022-11-21	Unresolved		
<input type="checkbox"/>	appsmith	1.7.6	CVE-2022-39824	8.9	2022-09-05	Unresolved		
<input type="checkbox"/>	appsmith	1.7.6	CVE-2022-4096	6.5	2022-11-21	Unresolved		
<input type="checkbox"/>	appsmith	1.7.3	CVE-2022-39824	8.9	2022-09-05	Unresolved		
<input type="checkbox"/>	appsmith	1.7.3	CVE-2022-4096	6.5	2022-11-21	Unresolved		
<input type="checkbox"/>	appsmith	1.7.2	CVE-2022-39824	8.9	2022-09-05	Unresolved		

# 제품 보안 취약점 확인

- 개발 제품별 프로젝트 등록하여 프로젝트별 보안 취약점 확인 가능

<input type="checkbox"/>	ID ↕	Project Name	Status	OSC Process	Download ⓘ	Security
<input type="checkbox"/>	697	<a href="#">3rd party create test 1</a>	Complete	Identification > Packaging		Discovered(N/A)
<input type="checkbox"/>	532	<a href="#">Sample_pro</a>	Complete	Identification > Packaging		Discovered(N/A)
<input type="checkbox"/>	506	<a href="#">AnotherTest Project (0.1)</a>	Complete	Identification > Packaging		Need to resolve(7.8)
<input type="checkbox"/>	480	<a href="#">MoonSangWoong_TRAINING PROJECT (1.0)</a>	Complete	Identification > Packaging		Need to resolve(9.8)
<input type="checkbox"/>	475	<a href="#">mj.prj.(0.1)</a>	Complete	Identification > Packaging		Need to resolve(9.8)
<input type="checkbox"/>	469	<a href="#">jkh test (1.0.0)</a>	Complete	Identification > Packaging		Need to resolve(9.8)
<input type="checkbox"/>	467	<a href="#">DY Training Project (1.0)</a>	Complete	Identification > Packaging		Need to resolve(10.0)

# SBOM 관리

- 특정 오픈소스 버전을 사용하는 프로젝트 조회 가능

The screenshot displays the SBOM management interface. At the top, there are tabs for 'Project', 'Self-Check', '315\_selfCheck', and '324\_selfCheck'. Below the tabs is a search bar with a magnifying glass icon, which is highlighted with a red box. The search bar contains the text 'Project ID or Name' and a checkbox for 'My Project'. To the right of the search bar is a '+ Advanced Search' button with the text 'option selected' below it.

Below the search bar are several filter fields: Status, Created Date, Division, Creator, Reviewer, Watcher, Network Service, Priority, Binary Name, Model Name, Distribution Type, OSS Notice, License Name, and 3rd Party Name. The 'Model Name' field is set to 'openssl' and the 'Distribution Type' field is set to '1.0.0'. These two fields are highlighted with a red box.

At the bottom of the filter section are two buttons: 'save conditions' and 'reset'.

Below the filter section are three buttons: 'Copy', 'Change', and 'BOM Compare'.

At the bottom of the interface is a table with the following columns: ID, Project Name, Status, OSC Process, Download, Creator, and Created Date. The table contains one row with the following data:

ID	Project Name	Status	OSC Process	Download	Creator	Created Date
632	<a href="#">sbom test</a>	Progress	Identification > Packaging		ab	2023-12-06

# SBOM 변경 추적

+ Add new\_project\_from\_api  My Project  + Advanced Search

Copy Change **SBOM Compare**

395 399

Status	OSS_Before	License_Before	OSS_After	License_After
add			npm:copy-anything (2.0.6)	MIT
add			soon	MIT
delete	mesqueeb-copy-anything (2.0.6)	MIT		
delete	mobis_psh	MIT		

Page 1 of 1 15 Count : 4

# 공급망 관리

- 타사에서 전달받은 Software 별 SBOM 관리 가능

**Mobile application (1.2) | Progress**

3rd party

Pre-Review

ID	Binary Name	OSS Name	OSS Version	License	Download	Homepage	Copyright	Tr	Vulnerability
<input type="checkbox"/>	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="checkbox"/> x	~ <input type="checkbox"/> x	~ <input type="text"/> x	>=	<input type="checkbox"/>
<input type="checkbox"/>	1 sample.jar	android-logging-log4j	1.0.3	Apache-2.0	https://c	<a href="https://c">https://c</a>			
<input type="checkbox"/>	2 multi.jar	angularjs-dropdown-multiselect	1.11.8	MIT	https://r	<a href="http://d">http://d</a>	Copyright (c		
<input type="checkbox"/>	3 dbus.so	dbus-java	2.7	AFL-2.1	https://c	<a href="https://v">https://v</a>	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>

The screenshot shows the FOSSLight Guide website. The left sidebar contains a navigation menu with categories like FOSSLIGHT HUB, FOSSLIGHT HUB BASIC TUTORIALS, and FOSSLIGHT HUB ADVANCED. The main content area is titled 'Developer Documentation' and includes a 'Note' section, a 'FOSSLight Hub 소스 다운로드' section, and '설치 및 실행 방법 - 1' (Installation and Execution Method - 1). Below this, there are sections for '개발 환경' (Development Environment) with links to Docker and Docker Compose, '빌드 및 실행' (Build and Execution) with a code block for 'docker-compose up --build', '설치 및 실행 방법 - 2' (Installation and Execution Method - 2), '요구사항' (Requirements) listing Java 11, MariaDB 10.0, and 8GB+ memory, and another '개발 환경' section listing Spring Boot 2.1.x, Gradle 6.x, Git, Spring Tool Suite, and UTF-8 project character set.

# 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 실행가능

## 개발 환경

- [Docker](#)
- [Docker Compose](#)

## 빌드 및 실행

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

plaintext

NVD Data 초기  
다운로드 필요

# DB 백업 및 복구

2. License

3. Open Source

4. Project

5. 3rd Party

6. Binary DB

7. Vulnerability

8. Self-Check

9. System

## FOSSLIGHT HUB BASIC TUTORIALS

Project

Self-Check

## FOSSLIGHT HUB TIPS

- ☐ Tips: Common

- ☐ Tips: Project

- ☐ Tips: Use Case

- ☐ Tips: Vulnerability

## FOSSLIGHT HUB ADVANCED

Developer Documentation

REST API

## ☐ Maintenance

- ☐ DB 백업 및 복구하기

- DB 버전 업그레이드하기

- NVD Data를 2002년 Data부터 다운로드 받

- 🏠 FOSSLight Homepage

## 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
```

```
$ mysqldump -ufossilight -pfossilight fossilight > fossilight_backup.sql
```

plaintext

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

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

```
$ mysqldump -ufossilight -pfossilight fossilight --no-create-info > fossilight_backup.sql
```

plaintext

### 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`

```
$ mysql -ufossilight -pfossilight fossilight < fossilight_backup.sql
```

plaintext

Migration  
Script 제공

# REST API

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

Swagger  
powered by SMART BEAR

Select a definition v2

## FOSSLight Hub Open API <sup>1</sup>

[ Base URL: demo.fosslight.org/ ]  
<https://demo.fosslight.org/v2/api-docs?group=v2>

Authorize

- 1. OSS & License** Api Oss V 2 Controller
  - GET /api/v2/licenses Search License Info
  - GET /api/v2/oss Search OSS List
  - POST /api/v2/oss Register New OSS
- 2. 3rd Party** Api Partner V 2 Controller >
- 3. Project** Api Project V 2 Controller >
- 4. Vulnerability** Api Vulnerability V 2 Controller >
- 5. SelfCheck** Api Self Check V 2 Controller >
- 6. Code v2** Api Code V 2 Controller >
- 7. Binary** Api Bat V 2 Controller >

# System 메뉴

- Admin 권한으로 접속시 확인 가능한 시스템 관리 메뉴

The screenshot shows the FOSSLight web interface. The left sidebar contains a menu with 'System' highlighted. The main content area displays a table of system configuration items under the 'Code management' tab.

Code No	Code Name	Code Description
100	Number of rows per a page	Number of records to be loaded per a page
101	order by cast column	Define cases for converting string to int for grid display
102	email type	
103	email contents	
104	email list contents	
110	email template file path	
111	email default contents	
120	File upload Extension	
121	Download Sample File	Location of sample files
122	Network Server license list	Licenses that has obligations for network server
200	Division	
201	License Type	
203	License Division	
204	License Composition Type	
205	Project Status	



**THANK YOU !**

