



Gestión de Riesgos del Software Libre

Primer plataforma SCA libre



Julian Coccia, CTO

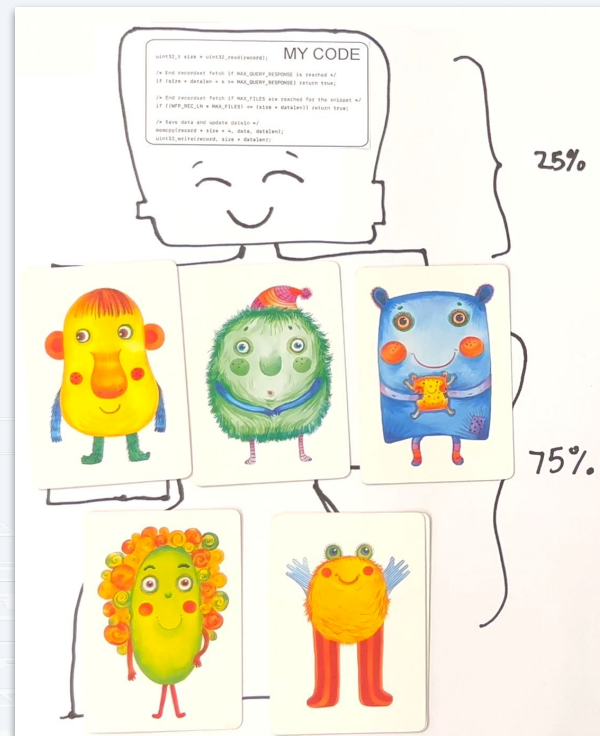
Nada menos que Frankies

- 75% del software es libre

The Forrester Wave™,
Software Composition Analysis
Q3 2021

- 85-90% del software es libre

Github, 2022



Riesgos del Software Libre

- Cumplimiento de licencias
- Vulnerabilidades
- Riesgo técnico
- Análisis de la Composición del Software (SCA)
 - Generación del SBOM (inventario)

Línea de tiempo

- 2002: Primer solución SCA para fusiones y adquisiciones
- 2007: Nacen los smartphones
- 2008: HP lanza FOSSology
- 2015: Linux Foundation lanza OpenChain
- 2020: Solarwinds hack
- 2020: OpenChain ISO/IEC 5230:2020 publicada
- 2021: Orden ejecutiva de Biden: SBOM obligatorio
- 2021: Lanzamiento SCANOSS
- 2021: LOG4J caos

Grandes empresas



PyMES

Tipos de detección

Detección de declaraciones

- Metadata que acompaña al código
- Declaraciones de copyright
- Encabezados y ficheros de licencia
- Declaraciones de dependencia

Detección de lo no declarado (requiere KB)

- Ficheros sin encabezado
- Dependencias incluídas
- Detección de plagiarismo
- Crítico para C/C++
- Importante para TODOS los lenguajes

Comparación de huellas

```
urepath = ''
for basis in ( 'basis-link', 'basis', '' ):
    for ure in ( 'ure-link', 'ure', 'URE', '' ):
        if os.path.isfile(realpath(basepath, basis, ure, 'lib', 'unorc')):
            urepath = realpath(basepath, basis, ure)
            info(3, "Found %s in %s" % ('unorc', realpath(urepath, 'lib')))
            # Break the inner loop...
            break
        # Continue if the inner loop wasn't broken.
        else:
            continue
    # Inner loop was broken, break the outer.
    break
```



Your code fingerprint

```
file=24e35278ad5d4d3babe7379dc34d5bce,439,pasted.wfp
5=369450fc
6=bf7226a9
8=b04dd861
9=9727e3cd
11=2152ba16
```



```
{
  "snippet.py": [
    {
      "id": "snippet",
      "status": "pending",
      "lines": "1-10",
      "oss_lines": "165-174",
      "matched": "90%",
      "purl": [
        "pkg:github/unoconv/unoconv",
        "pkg:deb/unoconv",
        "pkg:pypi/unoconv"
      ],
      "vendor": "unoconv",
      "component": "unoconv",
      "version": "0.8.2",
      "latest": "0.8.2",
      "url": "https://github.com/unoconv/unoconv",
      "release_date": "2017-12-07",
      "file": "unoconv",
      "url_hash": "c36074c3996ba9d7d85f4a57787b5645",
      "file_hash": "0f55e083dcc72a11334eb1a77137e2c4",
      "source_hash": "aff32ef2847f81abc62da076b9ff43f",
      "file_url": "https://osskb.org/api/file_contents/0f55e083dcc72a11334eb1a77137e2c4",
      "licenses": [
        {
          "name": "GPL-2.0-only",
          "obligations": "https://www.osadl.org/fileadmin/checklists/unreflicenses/GPL-2.0-only.txt",
          "copyright": "yes",
          "patent_hints": "yes",
          "incompatible_with": "Apache-1.0, Apache-1.1, Apache-2.0, BSD-4-Clause, BSD-4-Clause-UC, FTL, IJG, OpenSSL, Python-2.0, zlib-acknowledgement, XFree86-1.1",
          "source": "component_declared"
        }
      ]
    }
  ]
}
```

JSON response

Base de datos de Software Libre

- 154M URLs descargadas (>2Pb)
- 100.000.000.000 de ficheros
- 3.000.000.000.000 de líneas de código
- Acceso gratuito
 - Fundación para la Transparencia del Software



- **Adopción** masiva de SBOM
- **Notarización** de SBOMs
- Validación de **integridad**
- Enlazado y **Trazabilidad**

Proyectos de la Fundación

Get in touch

**Public SCA Service,
free SBOM.
No strings attached.**

Snippet-level software identification against a public knowledgebase.

141 million
URLs indexed

The Status

At the moment we have **141,490,922** URLs indexed in the OSSKB.

We are constantly working to grow our OSSKB. If you wish to help, please don't hesitate to [contact us](#).

OSSKB.ORG

SBOM Broadcasting

Your generated JSON file

```
{
  "type": "sbom",
  "parent_sboms": [],
  "sbom_data": {
    "checksum":
      "e8312db4b3ea35838dae38097ca7824f88421f6506
      2045243cd0288b29ae0dea"
    "algorithm": "SHA256"
  }
}
```

Parent SBOM (optional)

Add Hash + Add TXID +

SBOM Data*

SBOM hash

e8312db4b3ea35838dae38097ca7824f88421f65062045243cd0288b29ae0dea

Hash type

SHA224 SHA256 SHA384

Add Hash +

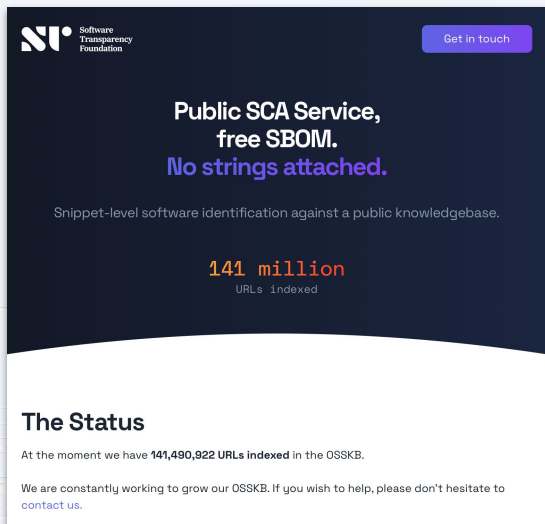
Your Token Id

Token id

Publish to Blockchain

SBOM.INFO

Fundación para la Transparencia del Software



- Perpétuo
- Gratuito
- Seguro
- Anónimo
- Sin estado

OSSKB.ORG

Presencia en repositorios públicos

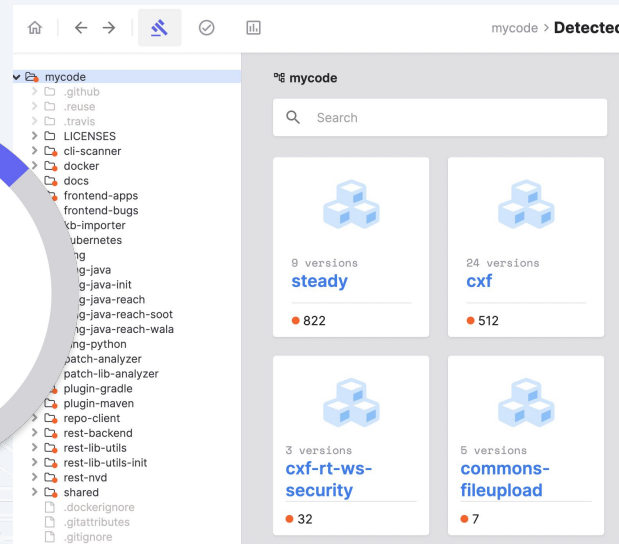
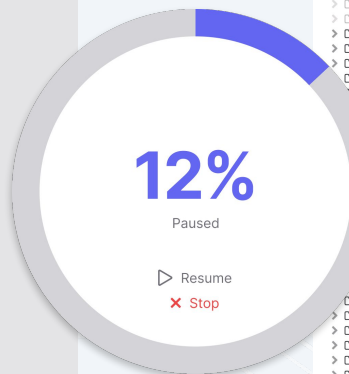
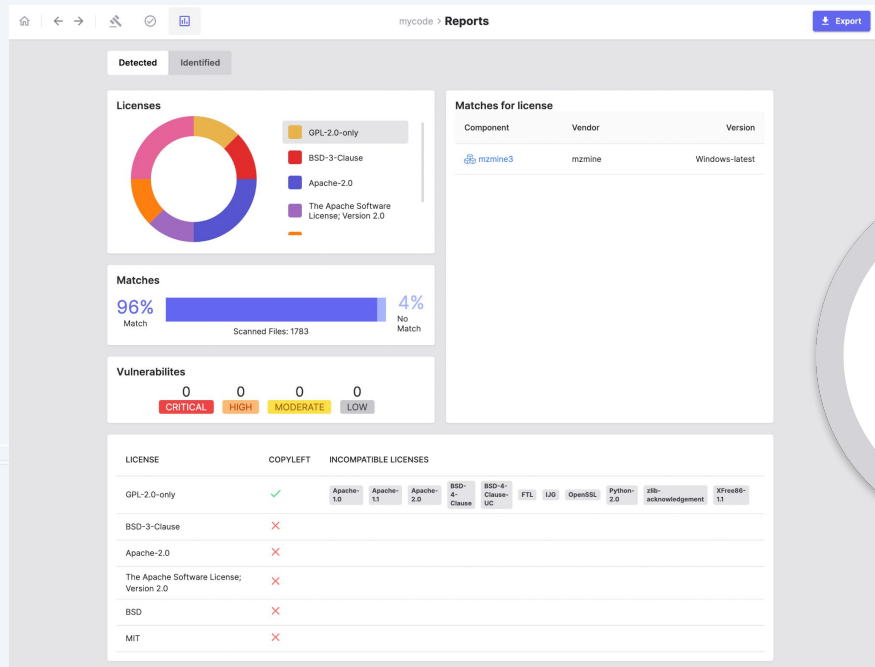
```
$ pip3 install scanoss  
$ scanoss-py scan mycode/
```

```
$ npm install -g scanoss  
$ scanoss-js scan mycode/
```



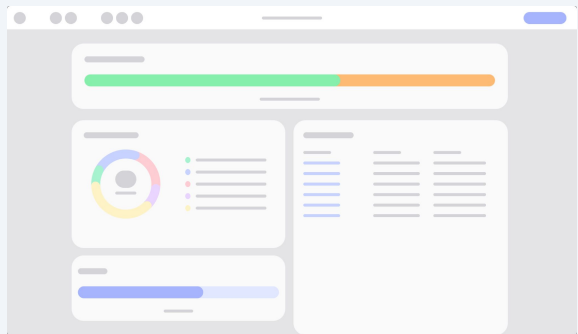
<https://github.com/scanoss>

App de auditoría de software multiplataforma

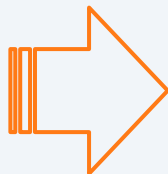


<https://github.com/scanoss/audit-workbench>

API público de la Base de Conocimiento de Software Libre



```
$ scanoss-py scan  
$ scanoss-js scan
```



<https://osskb.org/api>

Ecosistema en constante crecimiento

Herramientas libres



OSS
Review Toolkit

FOSSLight



fossology

Proveedores SCA

Abogados

Universidades

Audidores

Requerimientos
a proveedores



Resolviendo el SBOM entrante



Resolviendo el SBOM entrante



Cómo encontrarnos?

- <https://github.com/scanoss>
- <https://scanoss.com>
- <https://st.foundation>





Gracias



Julian Coccia, CTO

<https://scanoss.com>