KOREA UNIVERSITY
Center for Software Security and Assurance

IoTcube 2.0 Hatbom

사용자 메뉴얼

V0.0.3

2025-09-25

KOREA UNIVERSITY
Center for Software Security and Assurance

[도구별 지원언어]

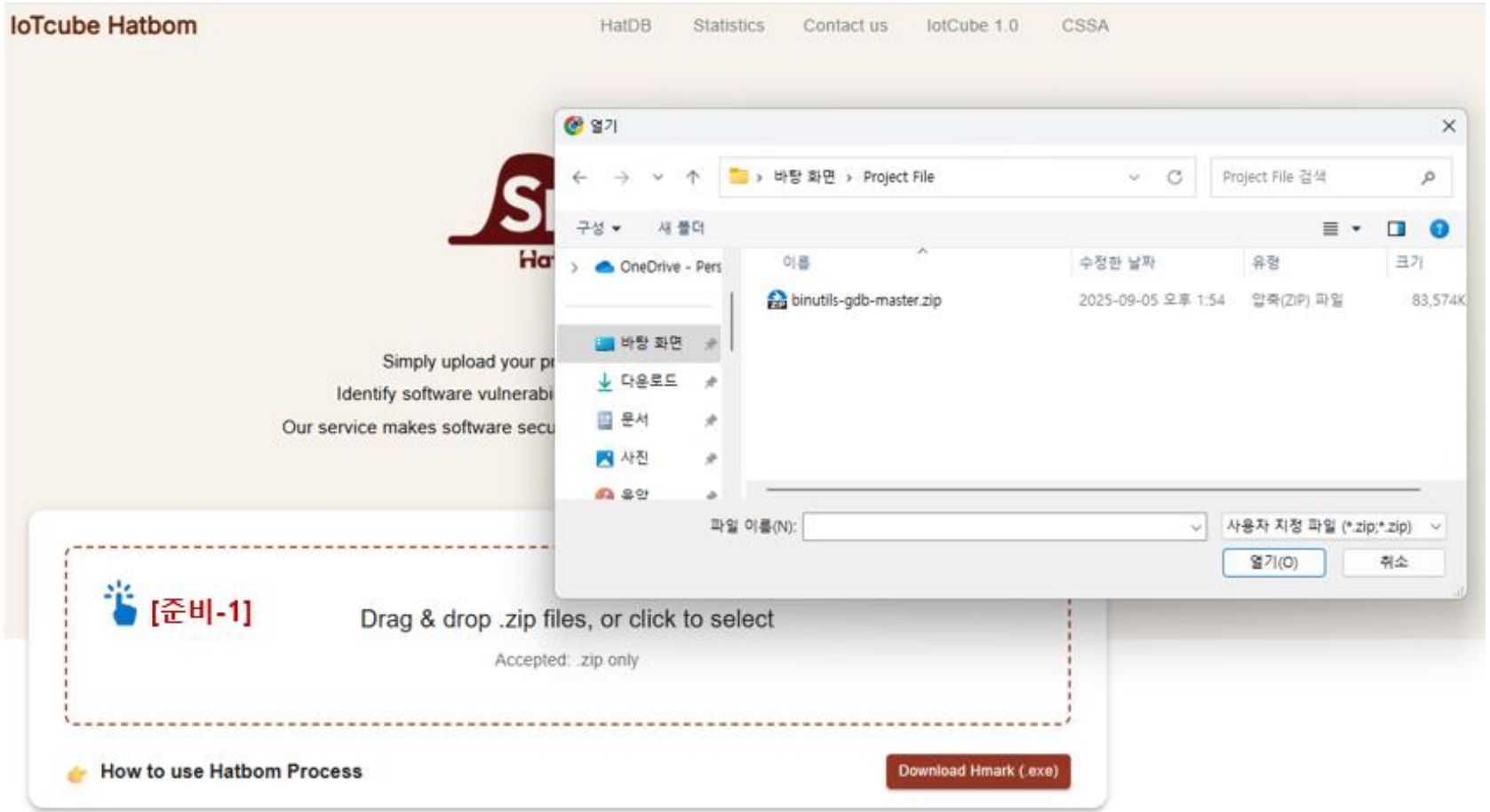
※ 도구 별 지원 언어(2025.9.8 현재) → 도구별 지원 언어는 점진적으로 확대 적요예정임

SBOM	OSS Dependency Graph	Vulnerability	Static Analysis
C/C++, java, python, go, php	C/C++	C/C++, java, python	C/C++

①SBOM Step ② Vulnerability Step ③VEX Step

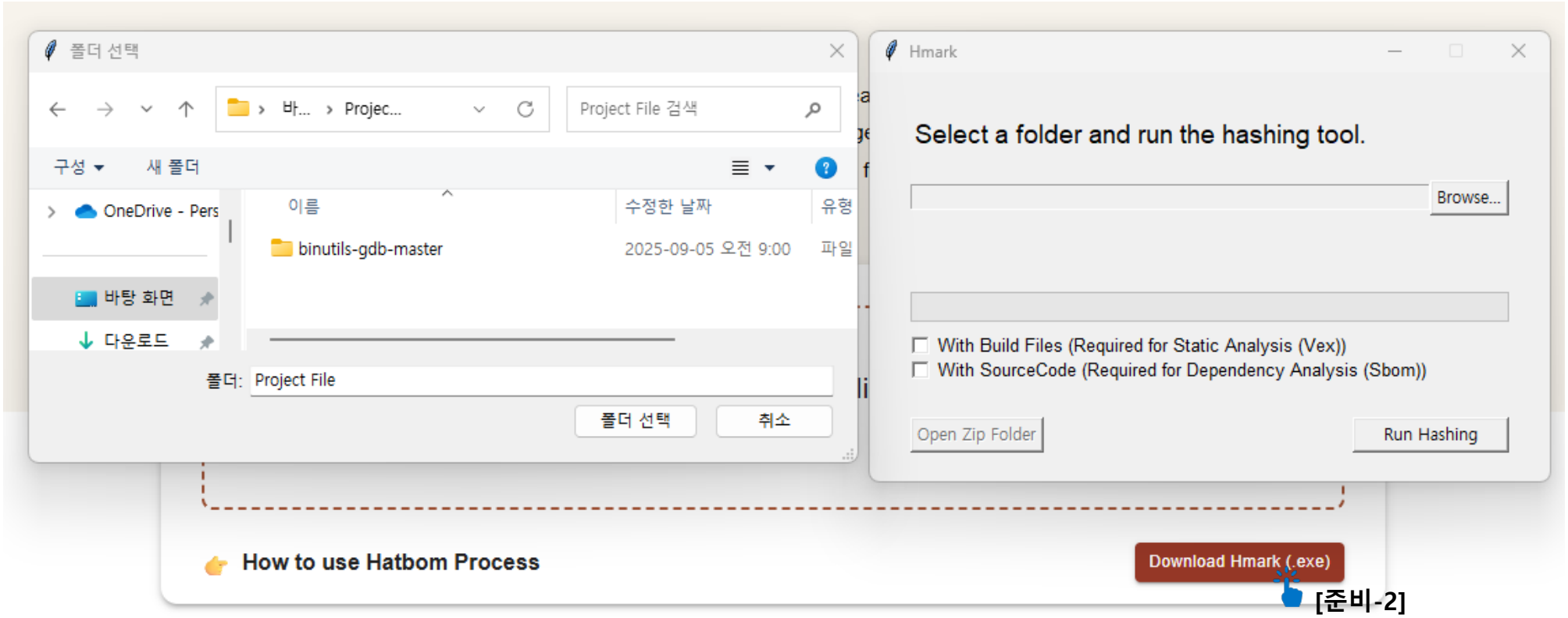
[준비]프로젝트 zip 파일 Drag&Drop

[준비-1] 프로젝트 코드가 있는 프로젝트 파일을 .zip 파일로 압축해서 Drag&Drop



[준비]프로젝트 zip 파일 Drag&Drop

[준비-2] Download Hmark로 Hashing 진행 후 나온 .zip 파일을 Drag&Drop

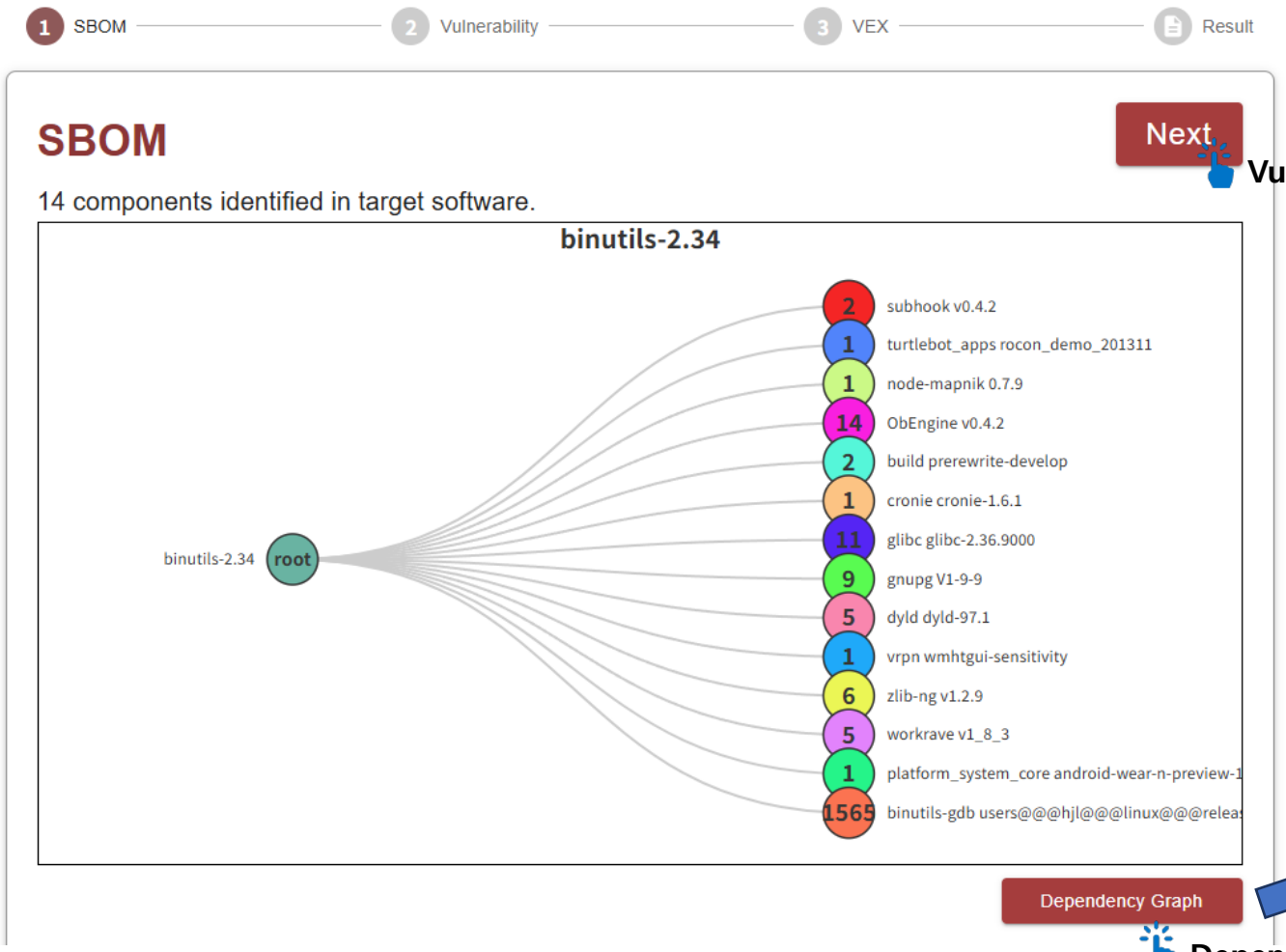


- Hmark는 로컬에서 Hashing 하는 프로그램으로 소스코드를 플랫폼에 제공하지 않아도 되는 장점이 있습니다**(코드 프라이버시)**
- With Build Files를 체크하시면 정적분석에 필요한 바이너리 파일이 포함됩니다.(C/C++ build 완료된 프로젝트 전용)
- With SourceCode를 체크하시면 종속성 그래프 생성에 필요한 **소스코드도 포함**이 됩니다.(C/C++ 전용)

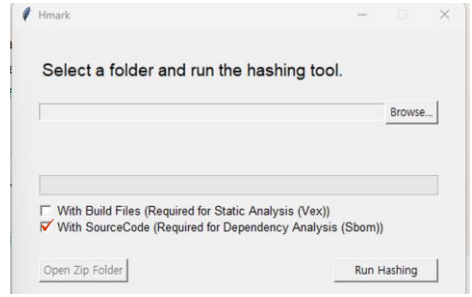
1. SBOM Step

SBOM Step은 OSS탐지와 그에 따른 SBOM 문서 자동생성 Step입니다.
하단의 다운로드 버튼을 통해서 SBOM 문서를 받을 수 있습니다.

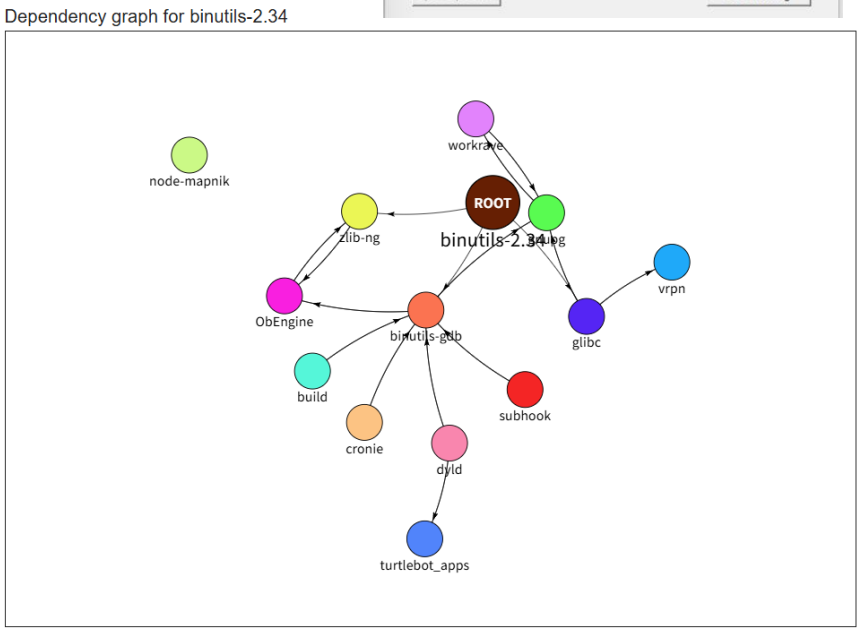
- C/C++의 경우 소스코드 제공시 OSS의 Dependency도 확인 할 수 있습니다.



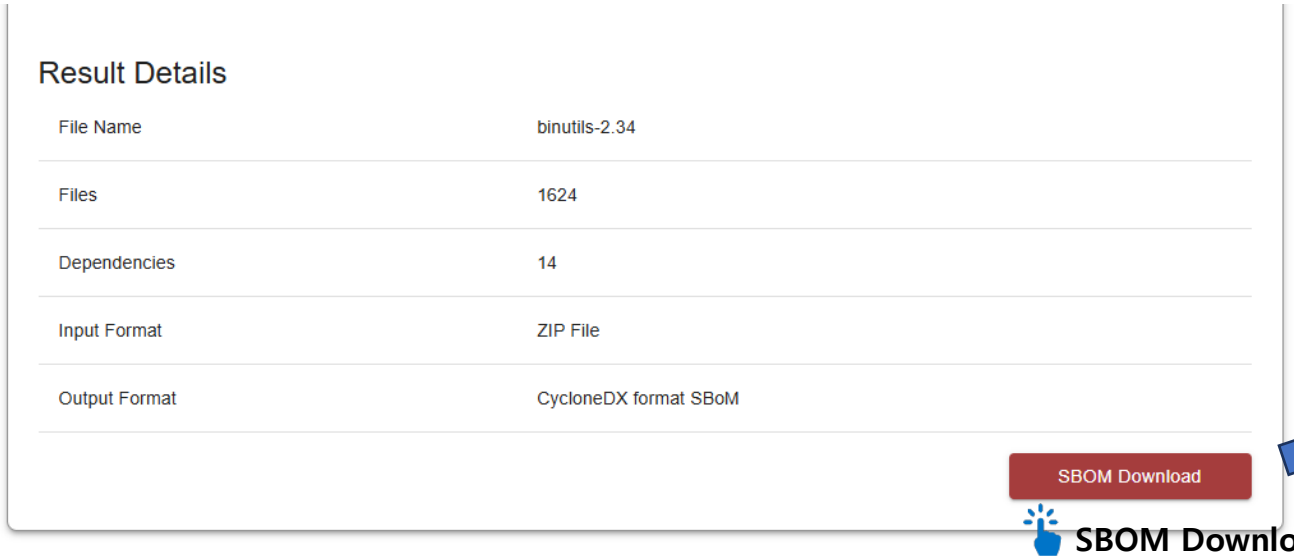
Vulnerability Step



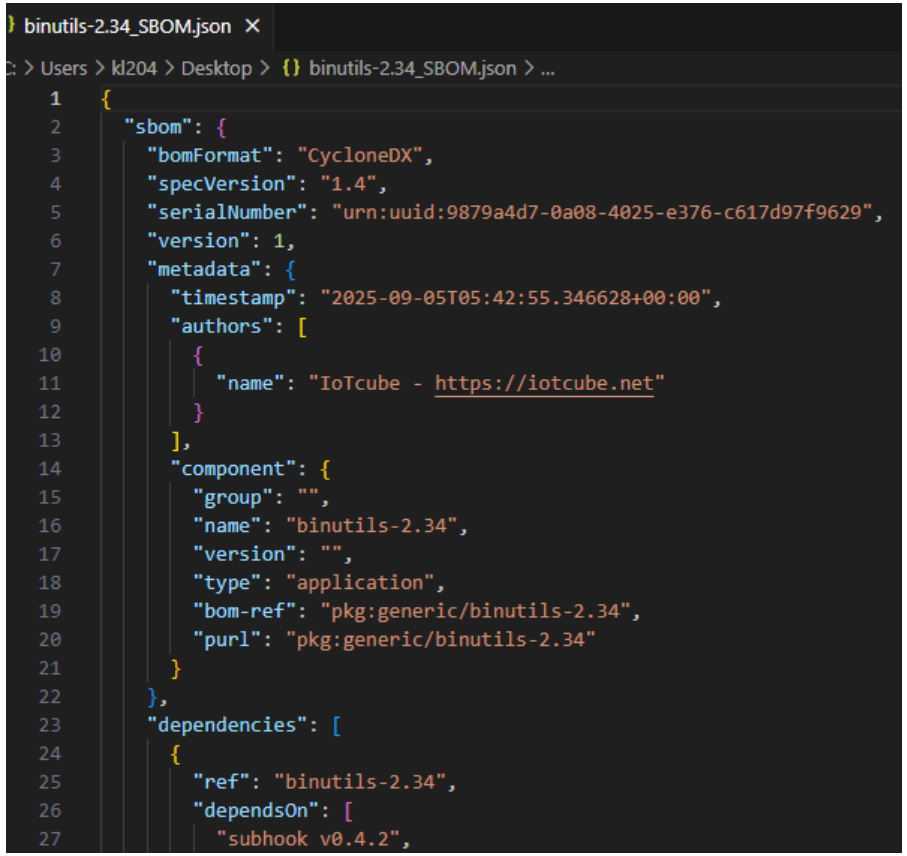
Dependency Graph



1. SBOM Step



SBOM Download

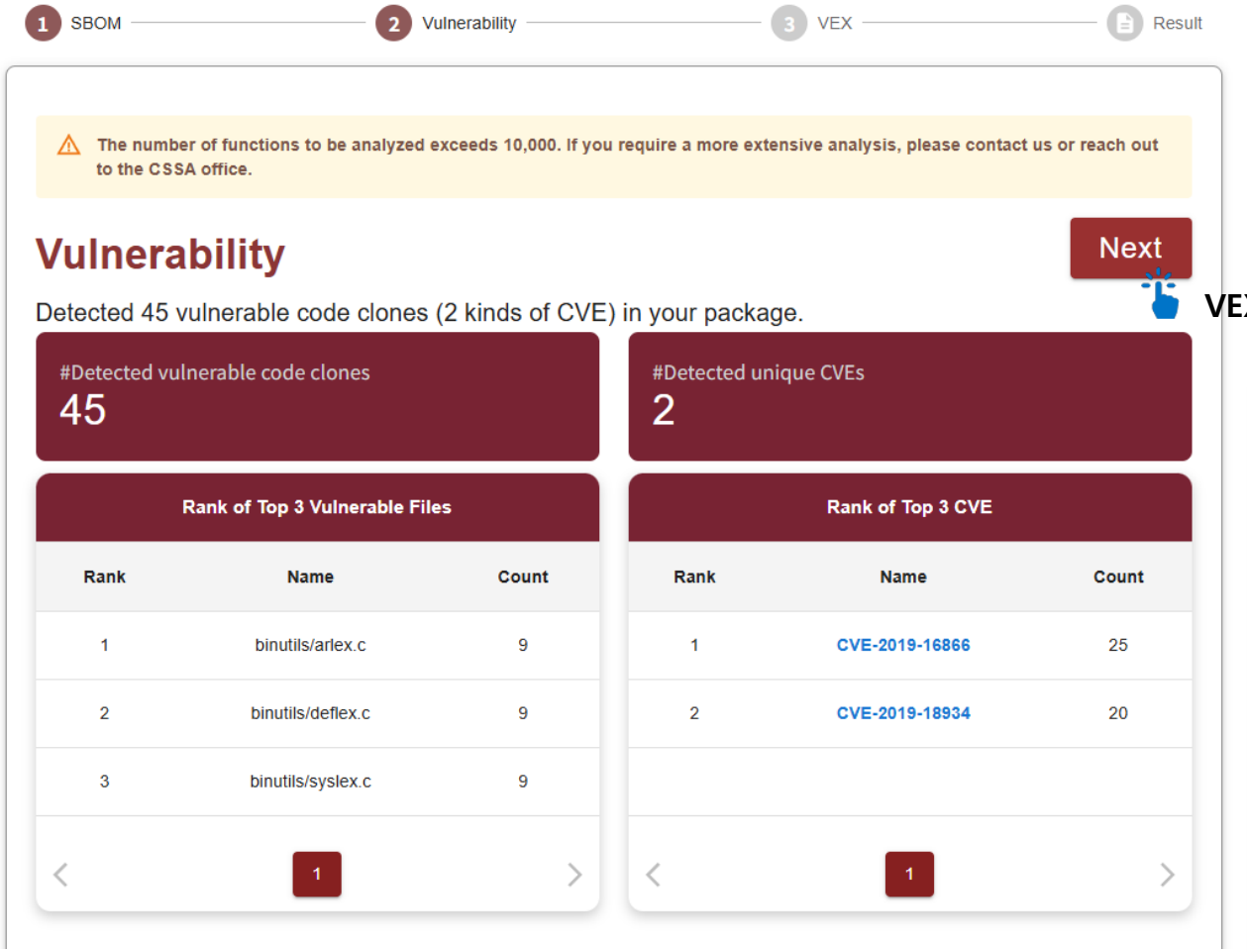


2. Vulnerability Step

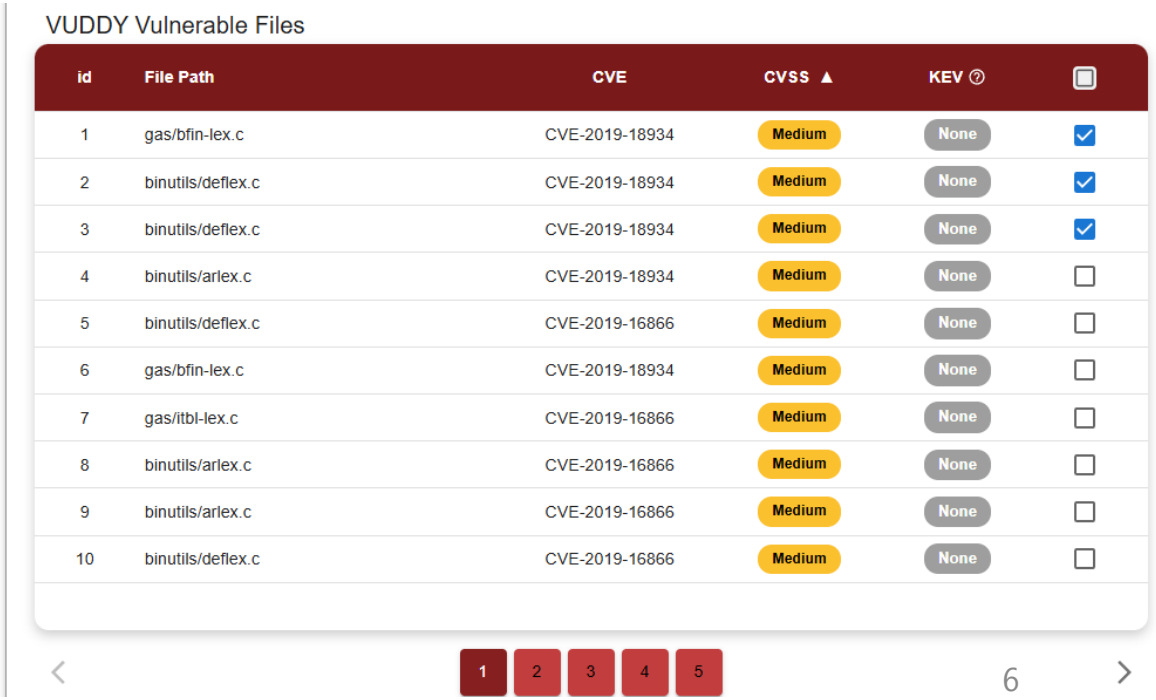
Vulnerability Step은 취약점을 탐지하는 Step 입니다.
제공한 프로젝트에 어떤 취약점이 있는지 확인 할 수 있습니다.

- CVSS(Common Vulnerability Scoring System)는 취약점의 점수입니다.
등급 구간: None(0), Low(0.1–3.9), Medium(4.0–6.9), High(7.0–8.9),
Critical(9.0–10.0) 으로 산출됩니다.

- VEX문서 생성을 위해서는 탐지된 cve 들을 체크해주어야 합니다.



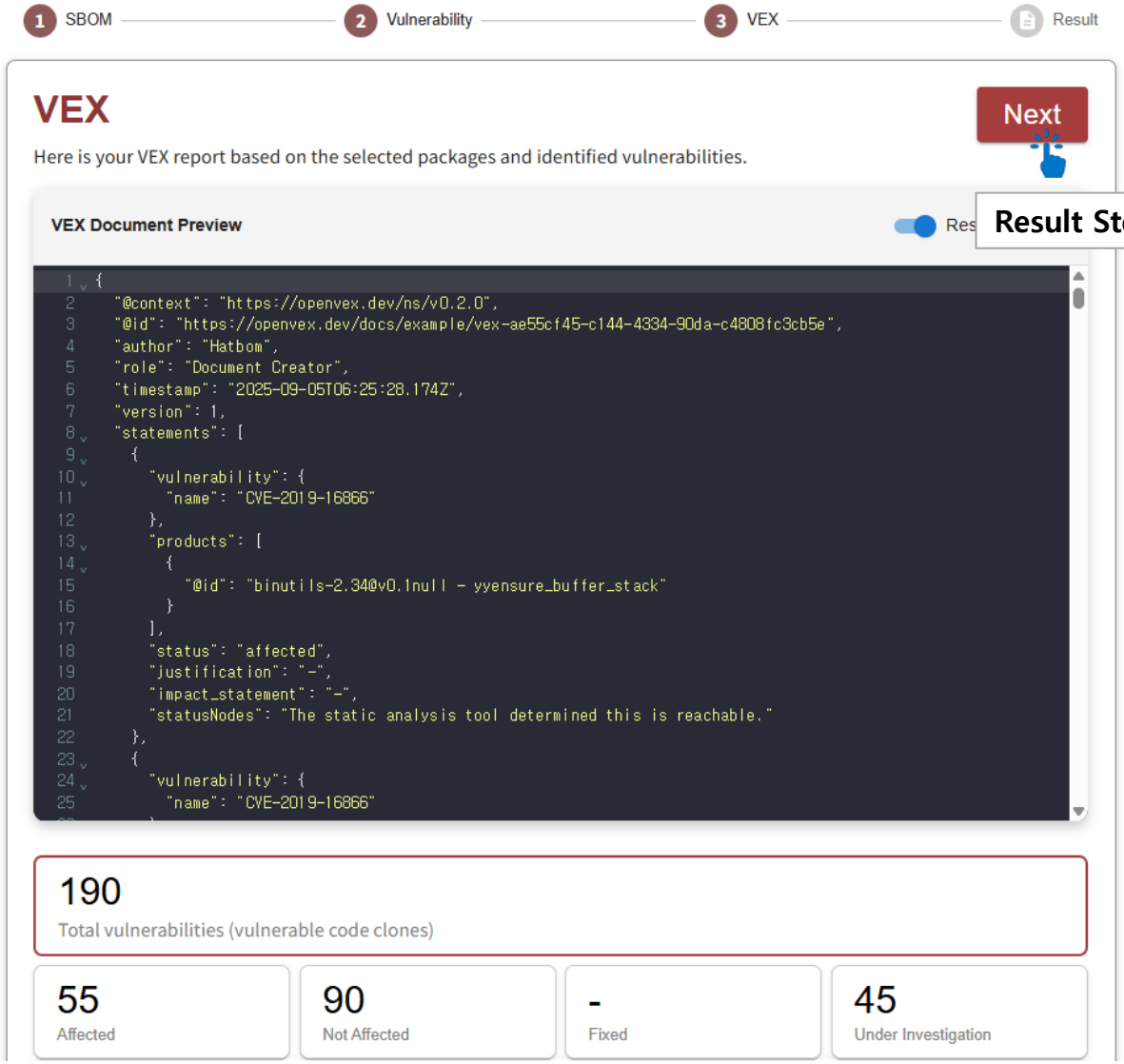
VEX Step

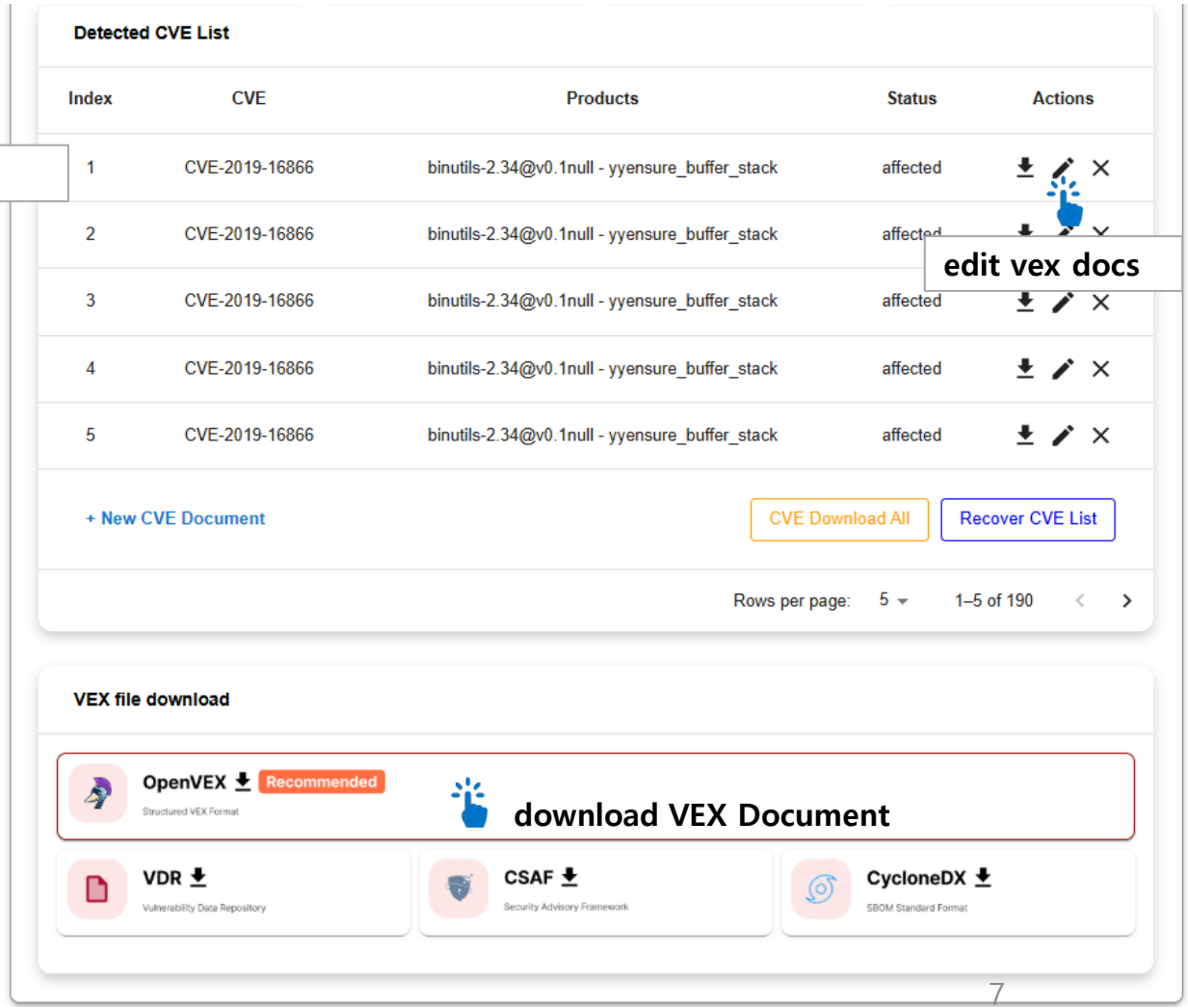


3. VEX Step

VEX Step은 취약점의 유효성을 문서화시키는 Step입니다. 수정할 수 있는 곳이 있어 각 취약점의 디테일한 내용들을 추가 할 수 있습니다.

- C/C++의 프로젝트의 경우 build가 된 프로젝트이면 정적 분석이 자동으로 실행됩니다.





4. Result Step

전체적인 step 요약을 확인 할 수 있습니다.