한양대학교 컴퓨터공학과

Programming Language bAsed Software Security and Engineering

지식베이스를 이용한 보안취약점 정적탐지

프로그래밍언어연구실 홍성문

ROSAEC center 11th
Research On Software Analysis for Error-free Computing
소프트웨어 무결점 연구센터 NRF ERC

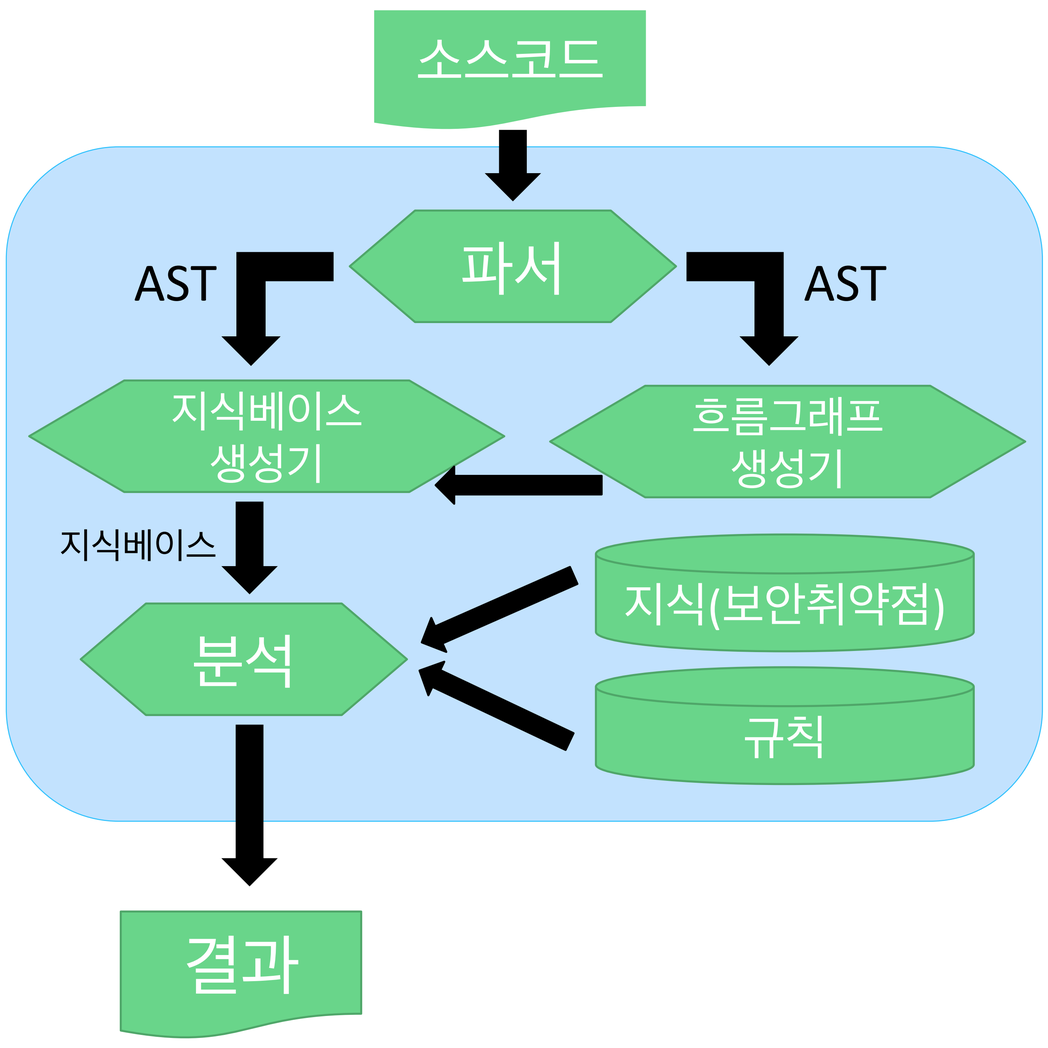
소스코드 보안안취약점 탐지 목적

✓보안취약점이 내포된 SW는 해커의 공격목표가 되어 심각한 보안위협 초래

✓정보시스템 운영 이전 개발단계부터 보안성 고려 및 잔존 취약점 제거 필요

✓운영단계에서의 취약점 제거 비용은 개발단계보다 60 ~ 100배의 비용 소모

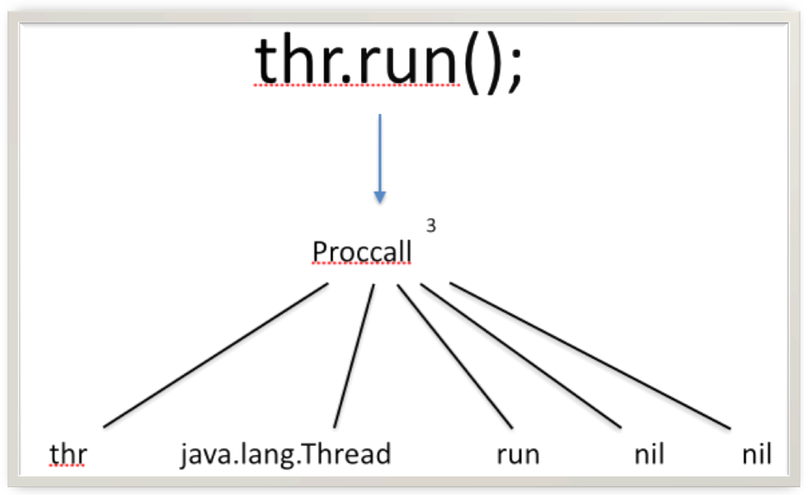
지식베이스 탐지기 전체구성도



Thread 객체에 run 메소드 호출 금지(CWE-572) 예시

```
…
Thread thr = new Thread();
thr.run();
…
```

✓ 소스코드



✓ 핵심구문트리

```
proccall(3,thr,javalangThread,run,[],[]).
```

✓ 지식베이스 정보

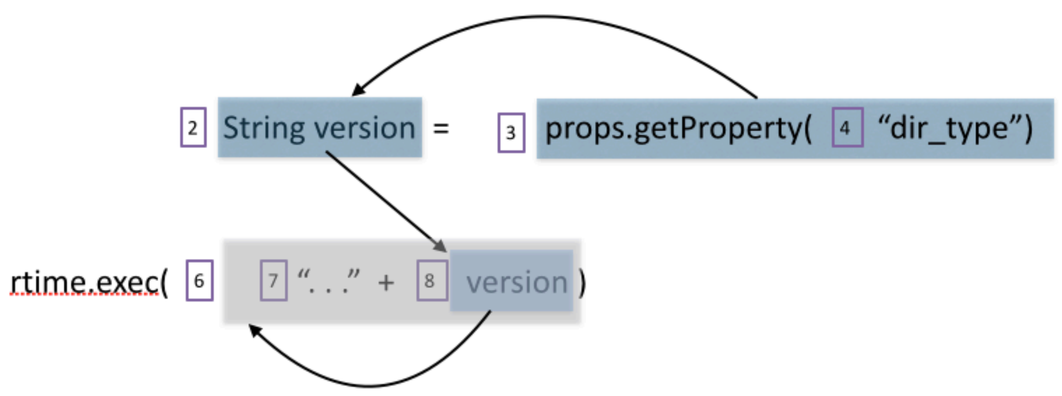
```
proccall(_,_,javalangThread,run,_,_).
```

✓ 지식베이스 탐지 질문

운영체제 명령어 삽입(CWE-78) 예시

```
…
String version =props.getProperty(“dir_type”);
rtime.exec(“ c:\\prog_cmd\\” + version);
…
```

✓ 소스코드



✓ 흐름그래프

```
funccall(3,string,props,javautilproperties,
        getProperty,[string],[4])
proccall(5,rtime,javalangRuntime,exec,[string],[6])
```

```
Control_flow(1,5)
Data_flow(4,3)
Data_flow(8,6)
Data_flow(7,6)
Data_flow(3,2)
Data_flow(2,8)
Data_flow(2,6)
```

✓ 지식베이스 정보

```
path(Node, Node, _, [Node]).
path(Start, Finish, Visited, [Start | Path]) :-
    data_flow(Start, X),
     not(member(X, Visited)),
     path(X, Finish, [X | Visited], Path).
```

✓ 그래프 검색 규칙

```
funccall(X,_,_,javautilProperties,getProperty,_,_) ,
proccall(_,_,javalangRuntime,exec,[H|_],_) ,
path(X,H,[X],Path).
```

✓ 지식베이스 탐지 질문

규칙명세언어와 지식베이스 비교

Filename	lines	Analysis time(s) (RDL)	#detection (RDL)	Analysis time(s) (Knowledge -Base)	#detection (Knowledge -Base)
AccessLogValue	1144	0.860	1	0.416	1
ASCIIReader	204	0.795	0	0.377	0
ContextConfig	1359	1.038	4	0.522	4
JkMX	395	1.265	0	0.659	0
JspC	1406	1.294	6	0.676	5
ProxyDirContext	1621	1.339	2	0.703	2
SetNextRule	215	1.181	0	0.608	0