웹 앱 정적 결함 검출기의 정확도를 동적 정보를 활용하여 향상하기

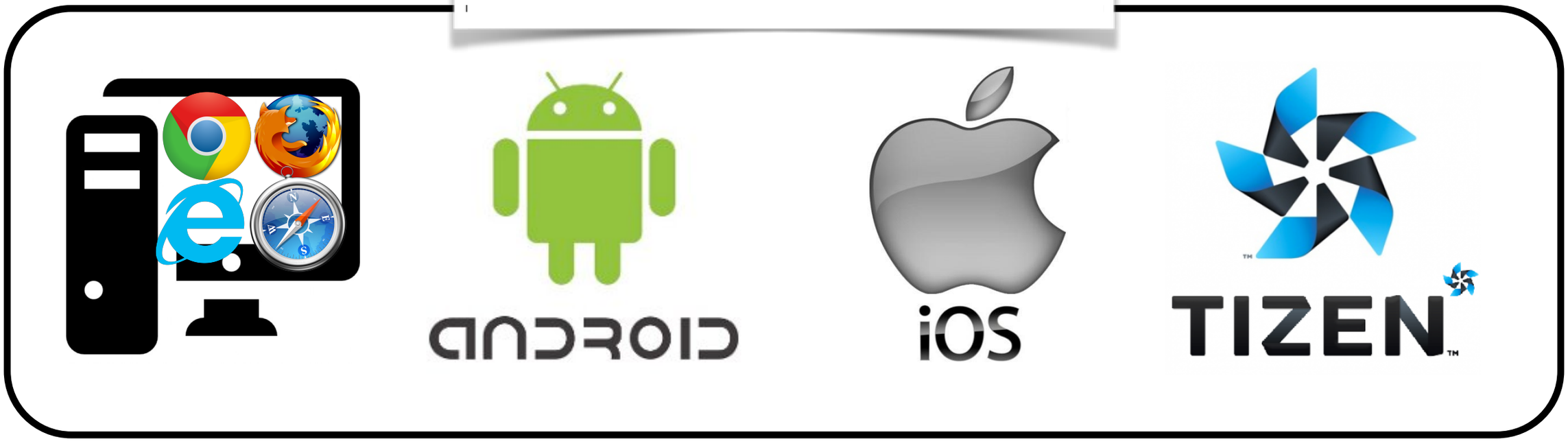
박준영
KAIST

임인호
삼성전자

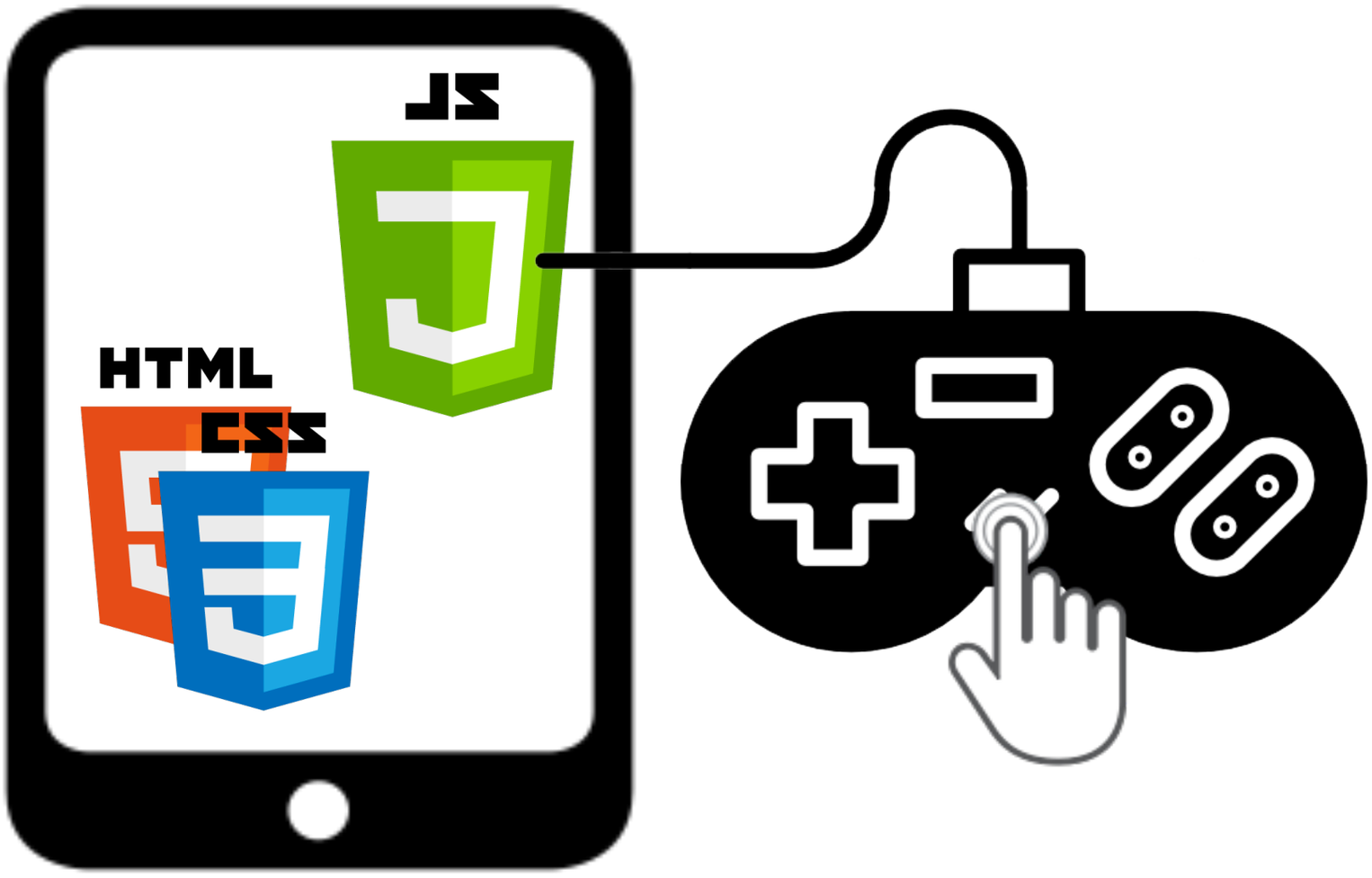
류석영
KAIST

2017-08-09
(ICSE'16)

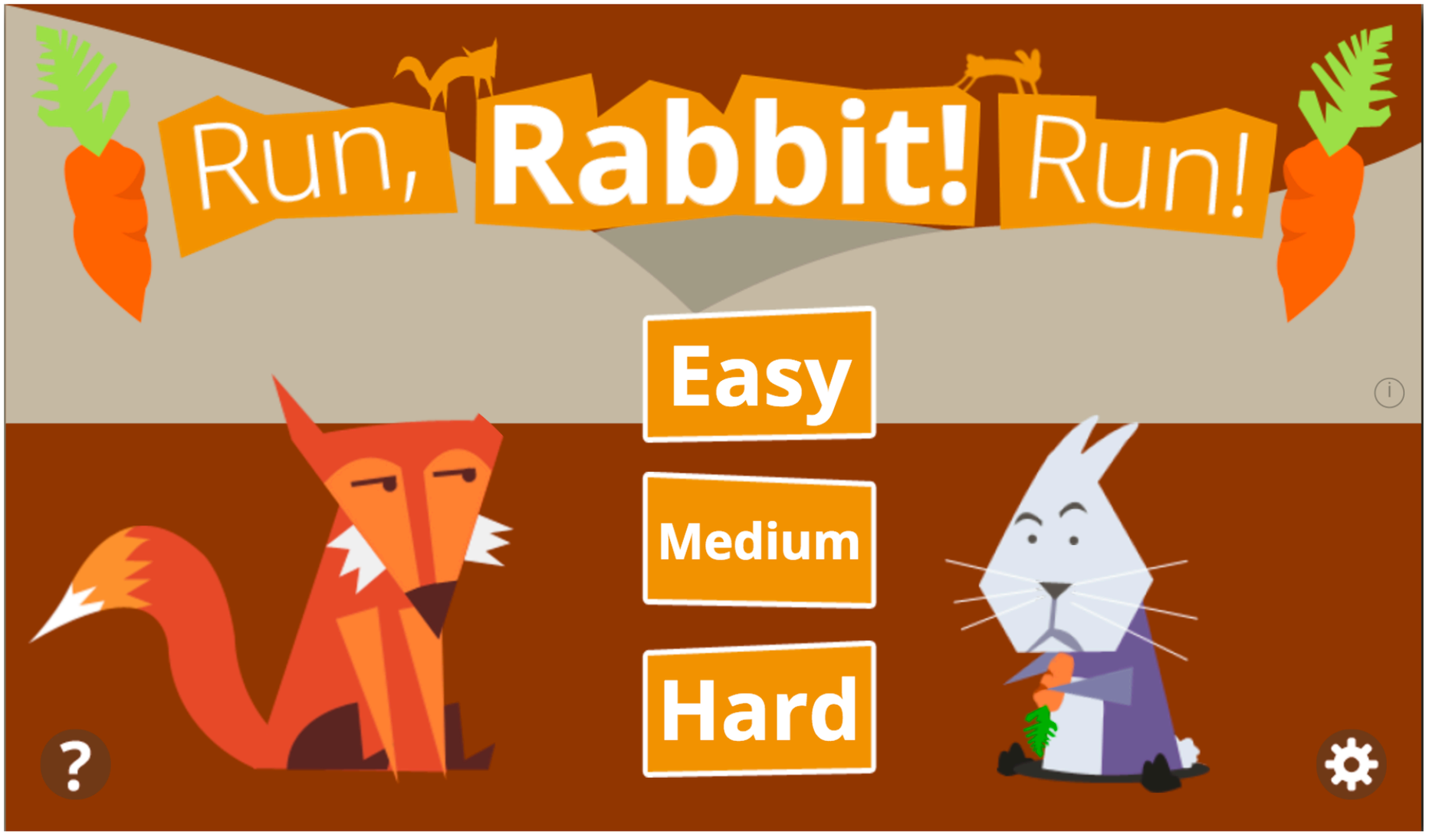
웹 애플리케이션



JavaScript



웹 앱 결함

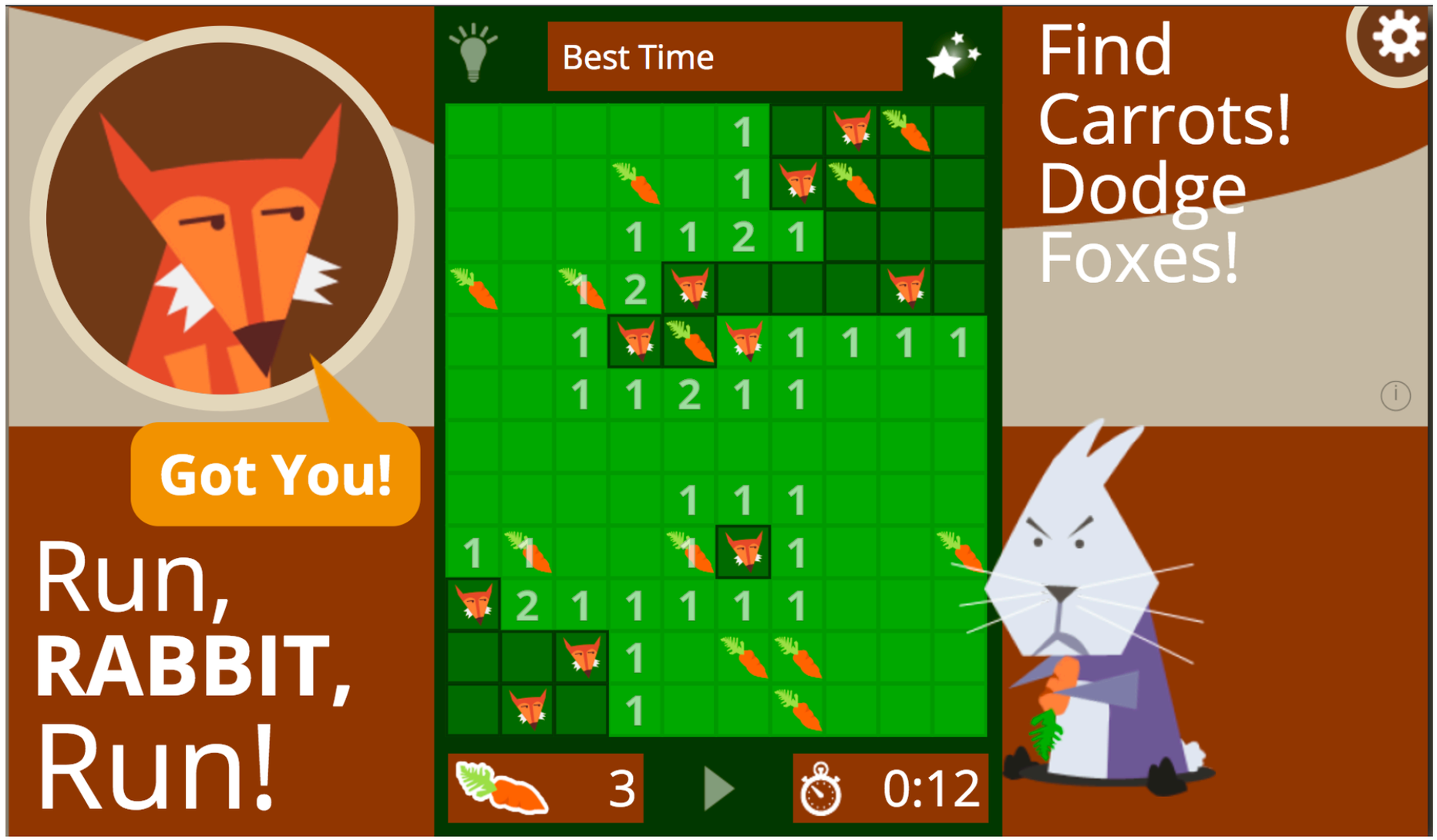


RunRabbitRun의 메인 메뉴

웹 앱 결함

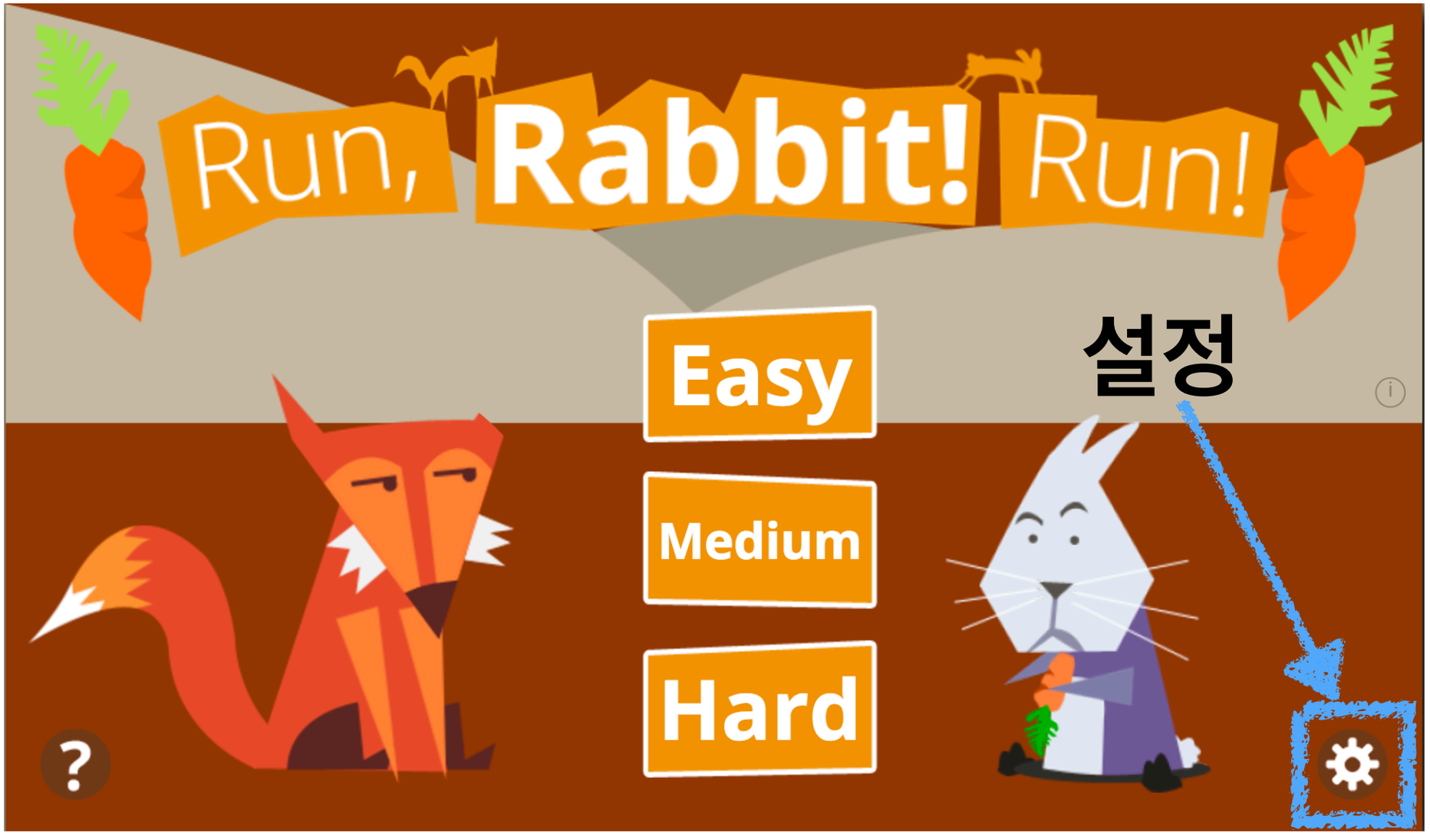
RunRabbitRun의 메인 메뉴

웹 앱 결함


Best Time
Find Carrots! Dodge Foxes!
Got You!
Run, RABBIT, Run!
3
0:12

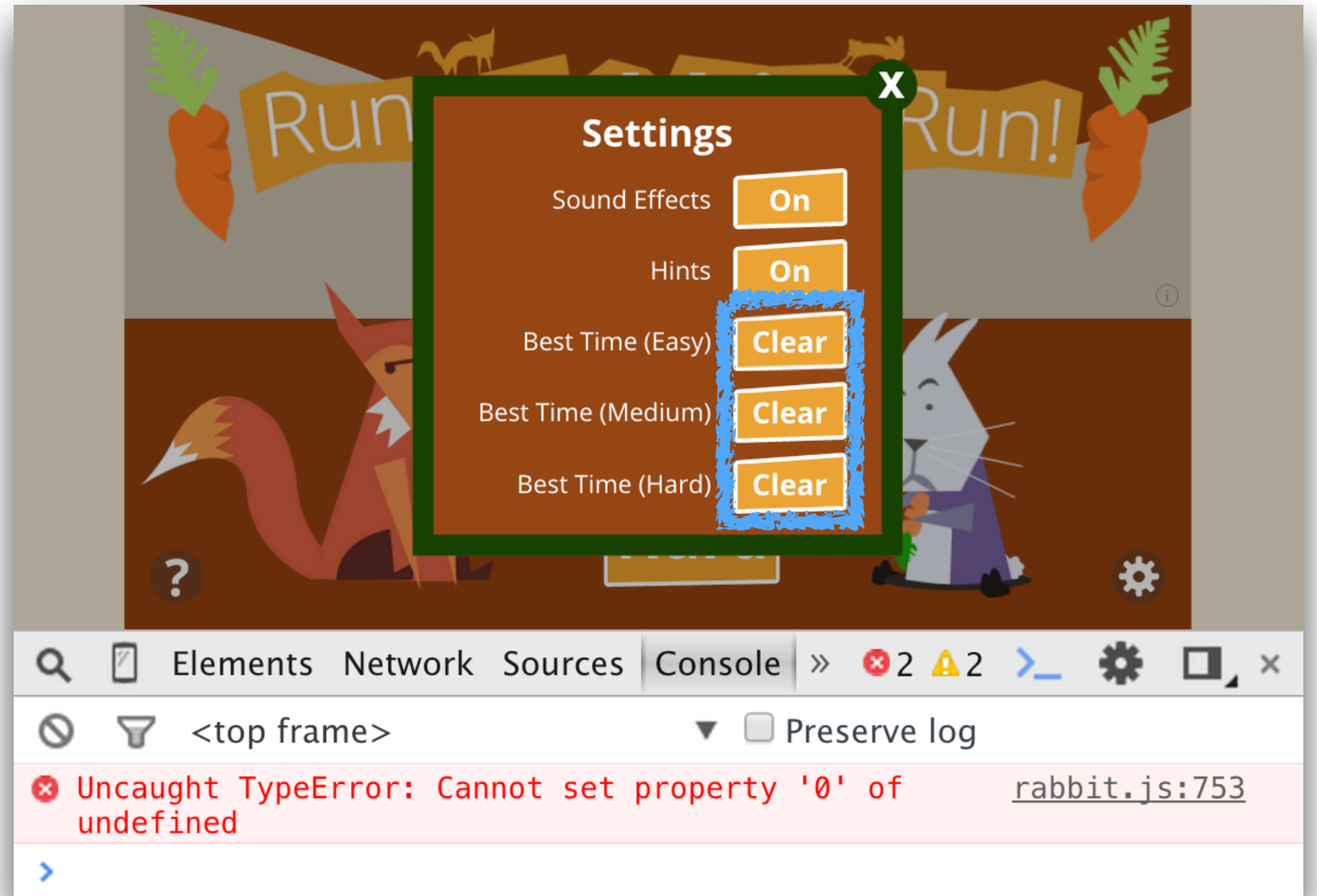
게임 화면

웹 앱 결함



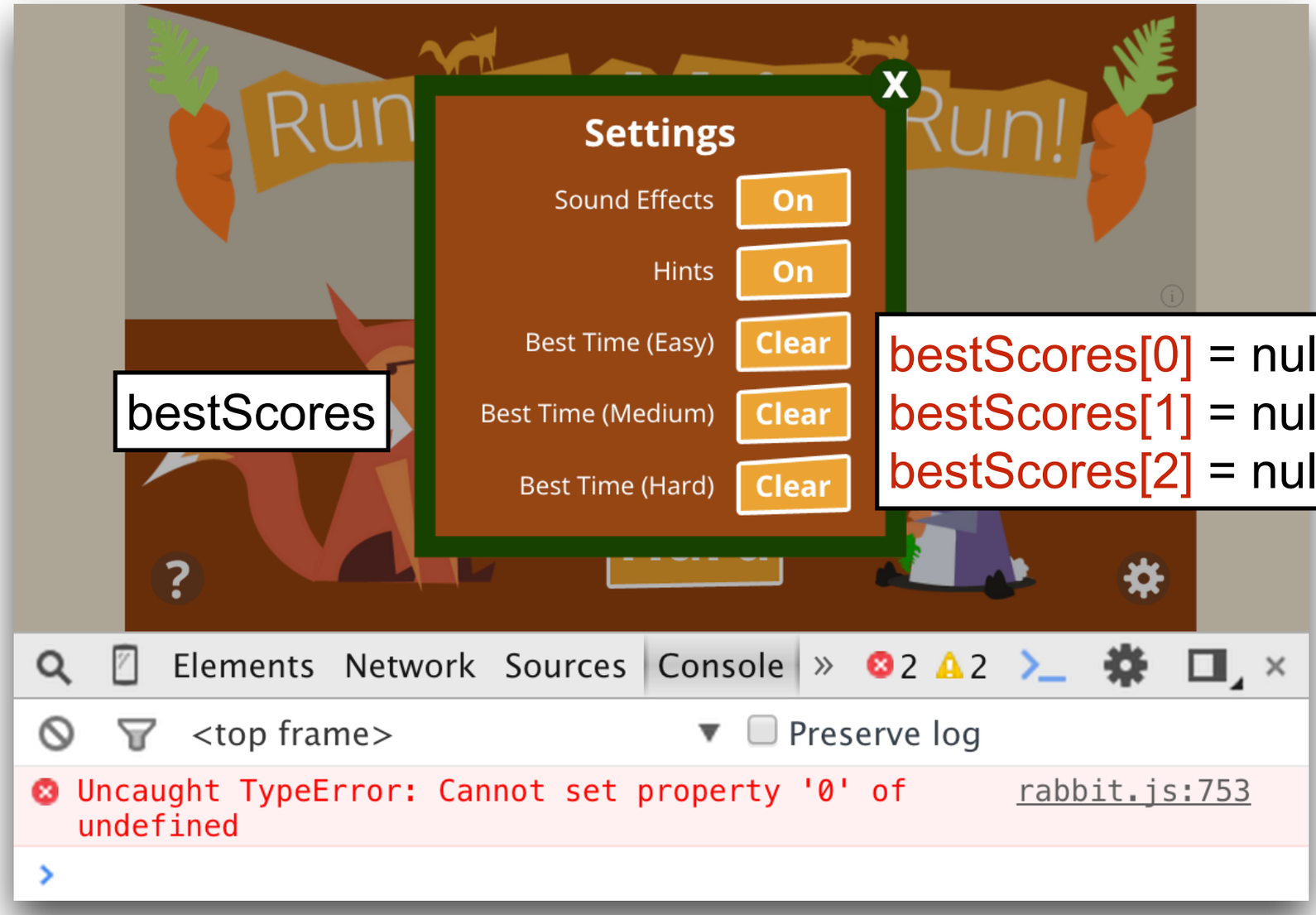
RunRabbitRun의 메인 메뉴

웹 앱 결함



Uncaught TypeError 발생 경고문

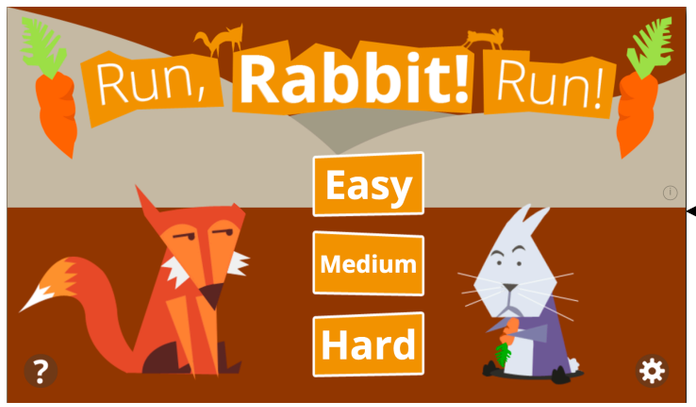
웹 앱 결함



Uncaught TypeError 발생 경고문

웹 앱 결함

메뉴



게임

bestScores = undefined;

if(!bestScores) bestScores = [null, null, null]

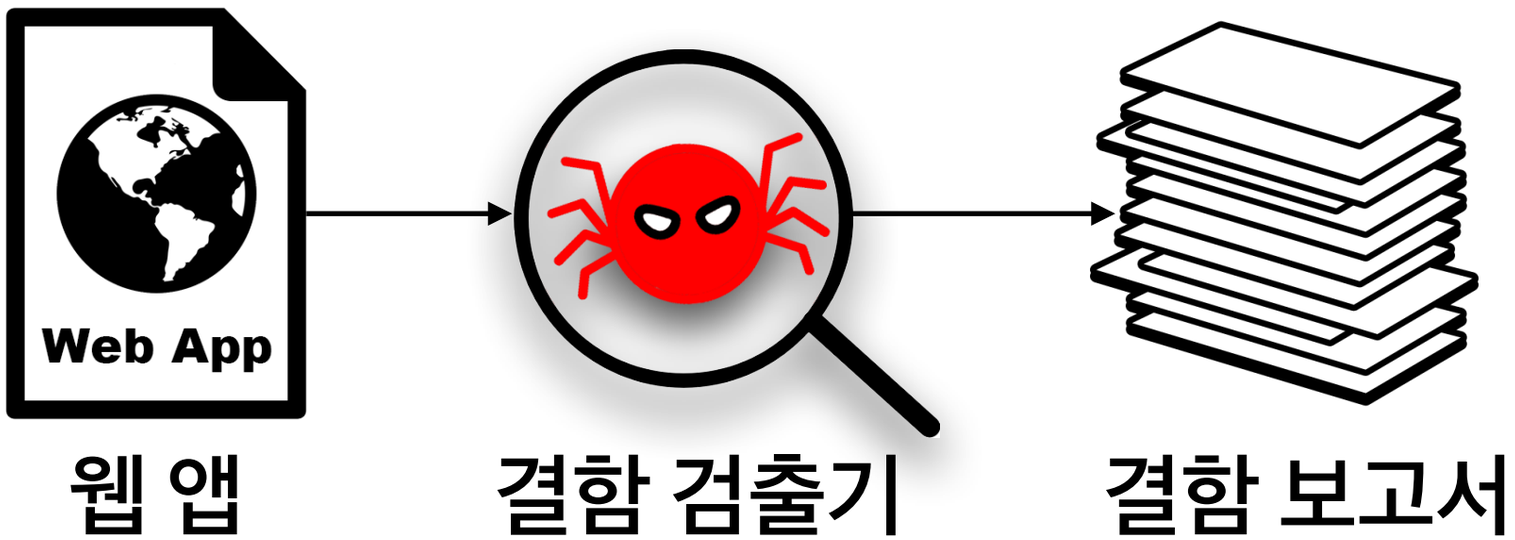
설정

메뉴 (게임 메뉴)+ 설정 Clear : OK

메뉴 설정 Clear : Error!

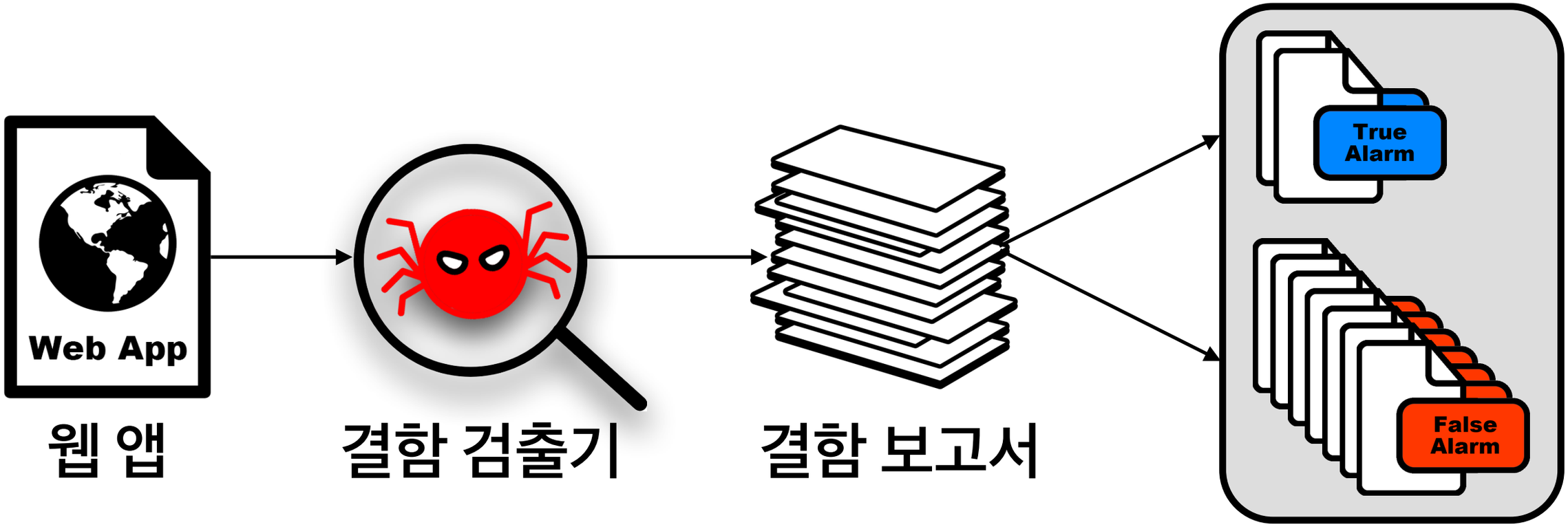
정적 결함 검출기

정적 결함 검출기

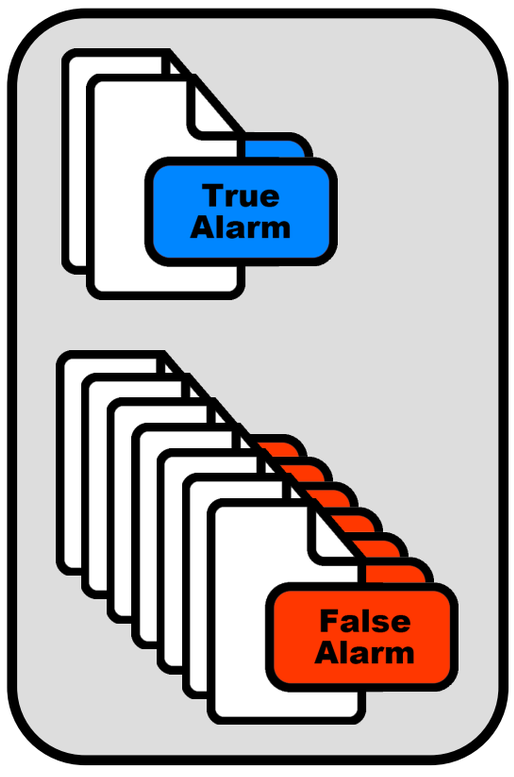


TypeError
ReferenceError
오류 발생이 쉬운 유형

정적 결함 검출기



결함 보고서 조사



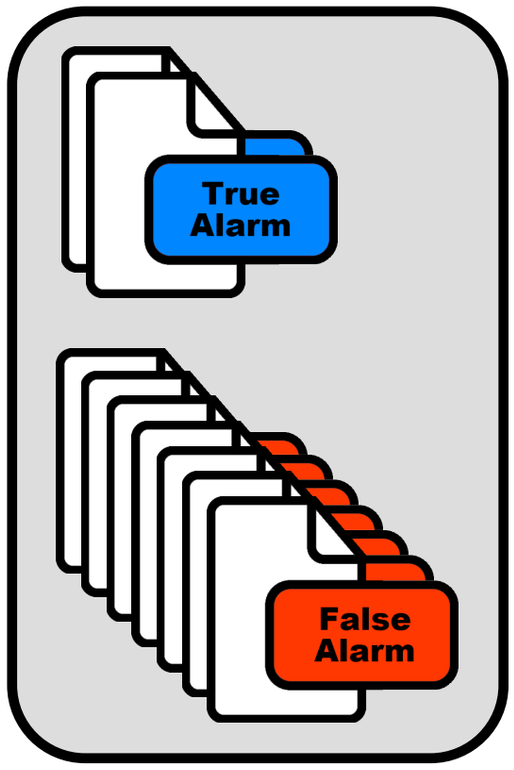
55

334

Causes	#FPs
W3C APIs	160
Browser-specific APIs	19
JavaScript library APIs	36
Dynamic file loading	24
Dynamic code generation	6
Asynchronous calls	89
Others	0

30개 Tizen 웹 앱에서 검출된 결함

결함 보고서 조사



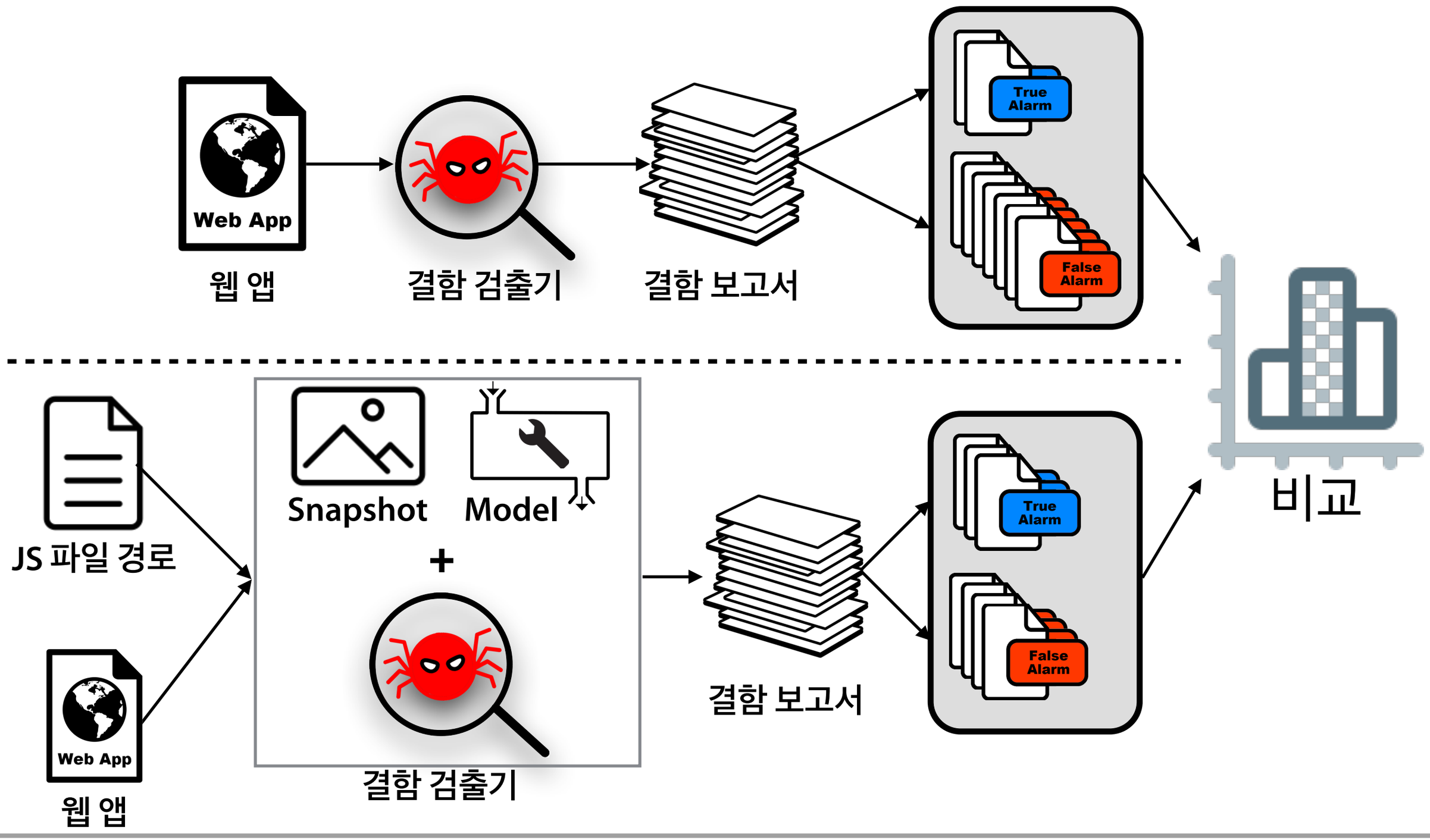
55

334

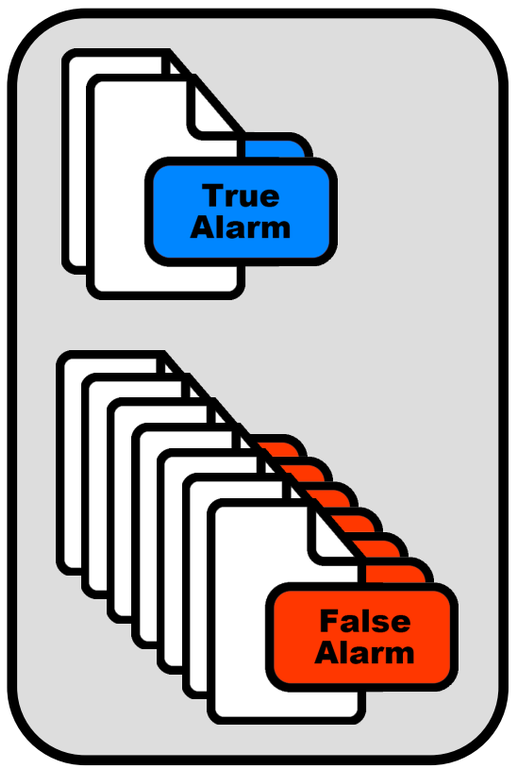
Causes	#FPs
W3C APIs	160
Browser-specific APIs	19
JavaScript library APIs	36
Dynamic file loading	24
Dynamic code generation	6
Asynchronous calls	89
Others	0

30개 Tizen 웹 앱에서 검출된 결함

큰 그림


Web App
웹 앱
결함 검출기
결함 보고서
True Alarm
False Alarm
비교
JS 파일 경로
Web App
웹 앱
Snapshot
Model
+
결함 검출기
결함 보고서
True Alarm
False Alarm

동적인 파일 로딩



55

334

Causes	#FPs
W3C APIs	160
Browser-specific APIs	19
JavaScript library APIs	36
Dynamic file loading	24
Dynamic code generation	6
Asynchronous calls	89
Others	0

30개 Tizen 웹 앱에서 검출된 결함

동적인 파일 로딩

- 파일 경로를 입력하면 소스 코드로 로딩하는 기능이 존재

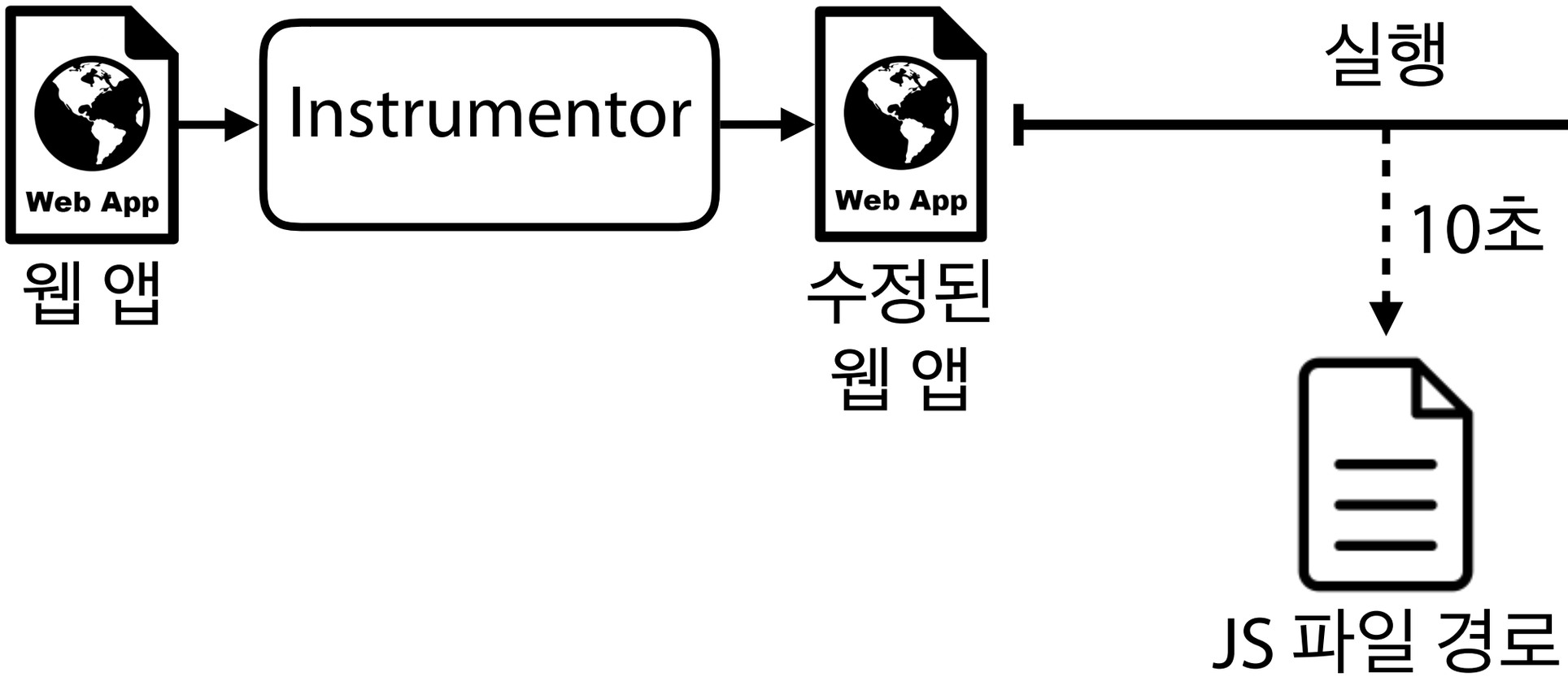
```
<script src="file.js"></script>
```

- 사용자에게 빠르게 페이지를 보여주기 위해, JavaScript를 이용하여 일부 자원의 로딩을 미루는 경우가 흔함

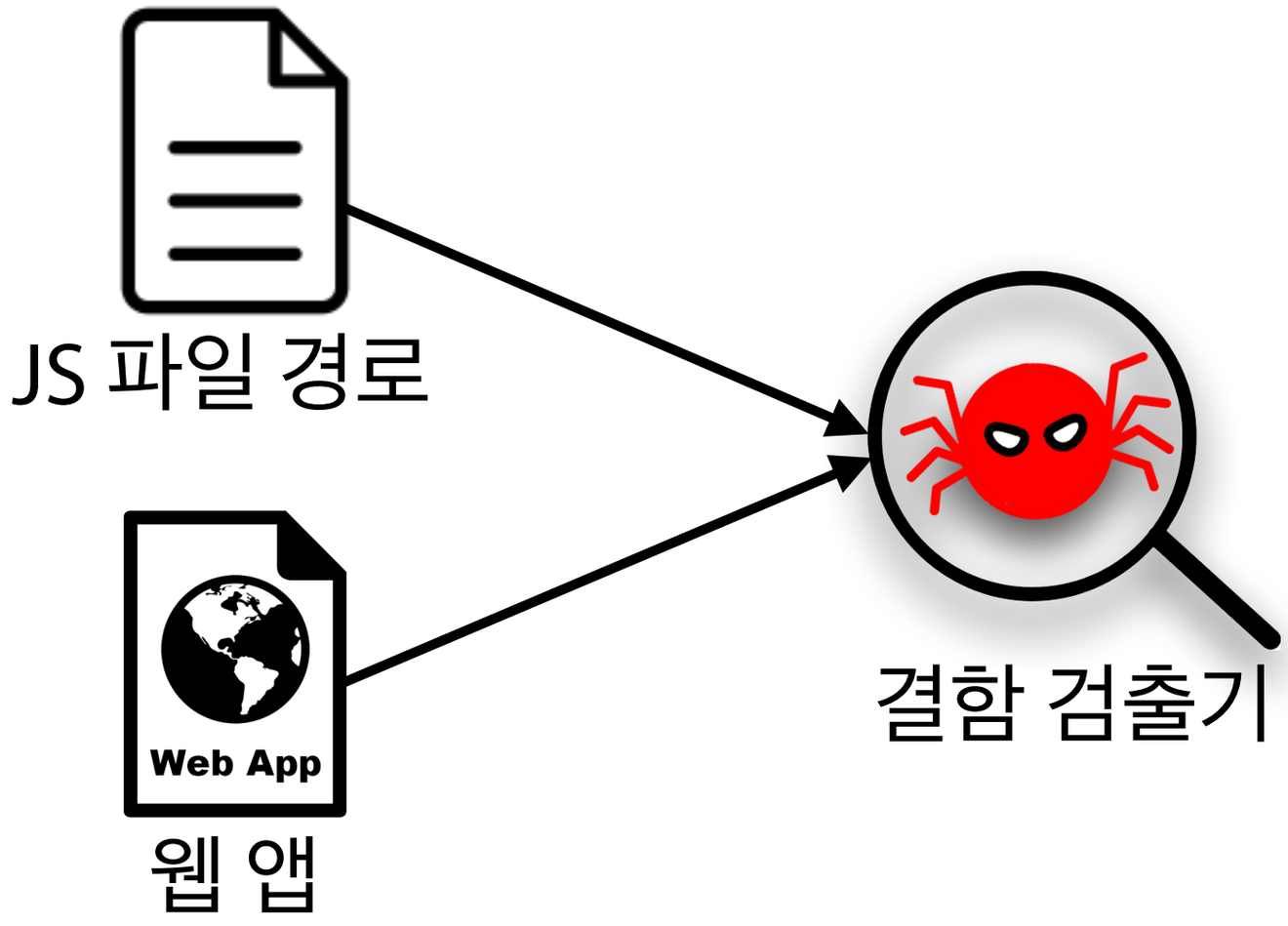
```
document.write('<script src="file.js"></script>');
```

- 파일 경로(String)값을 정확하게 정적 분석하기 어려움

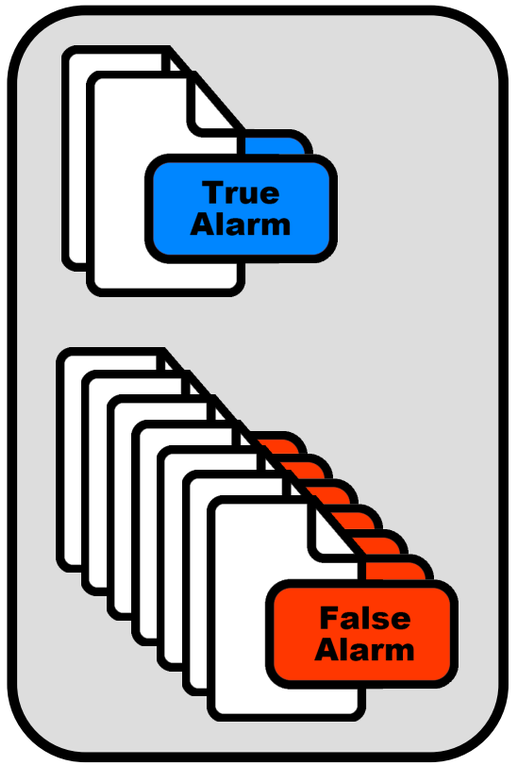
JS 파일 경로



JS 파일 경로



부정확하거나 누락된 API



55

334

Causes	#FPs
W3C APIs	160
Browser-specific APIs	19
JavaScript library APIs	36
Dynamic file loading	24
Dynamic code generation	6
Asynchronous calls	89
Others	0

30개 Tizen 웹 앱에서 검출된 결함

부정확하거나 누락된 API

- W3C API: 브라우저 개발자가 따르는 표준 API

`Node.nodeType`

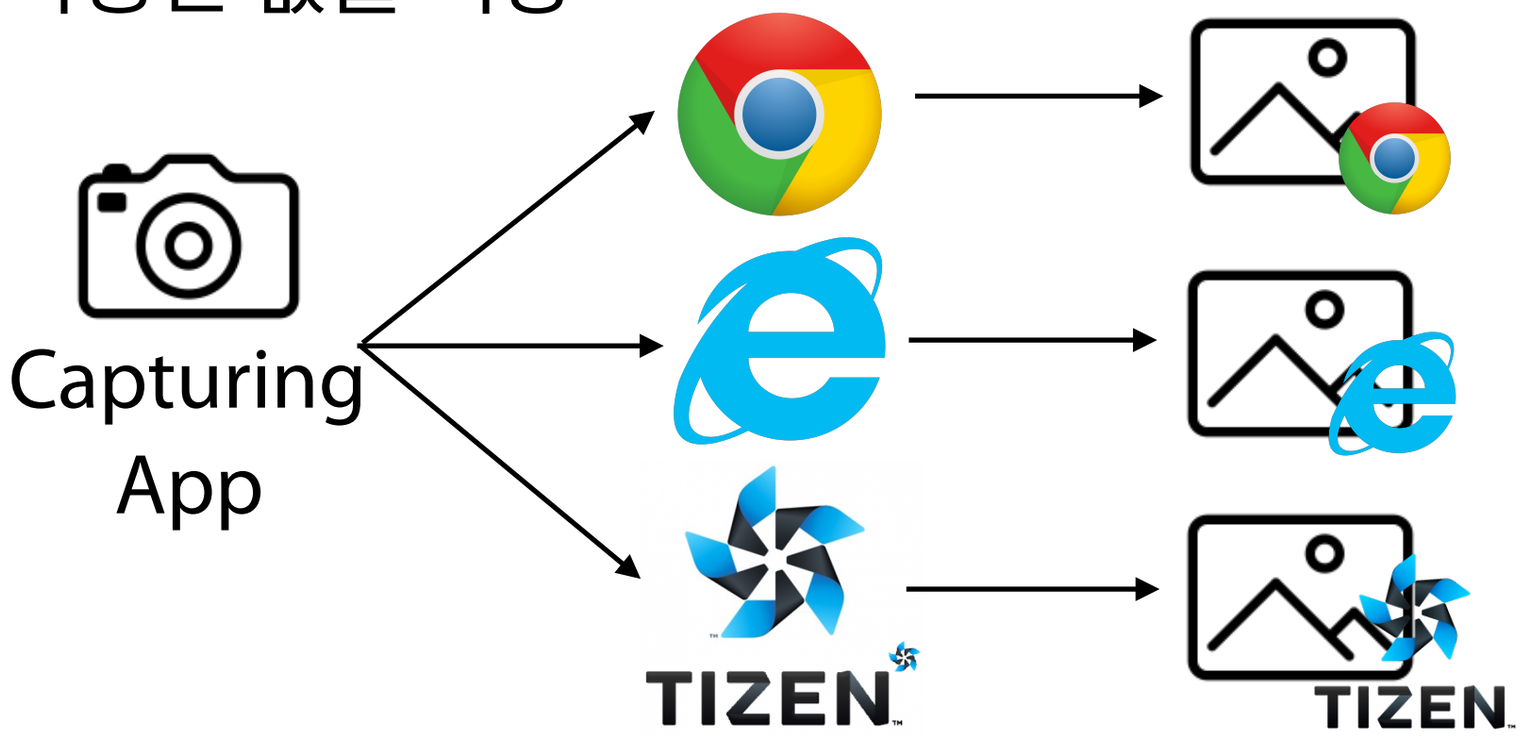
Specification	Status	Comment
DOM The definition of ‘Node.nodeType' in that specification.	Living Standard	Deprecated `ATTRIBUTE_NODE`, `CDATA_SECTION_NODE`, `ENTITY_REFERENCE_NODE` and `NOTATION_NODE` types.
Document Object Model (DOM) Level 3 Core Specification The definition of 'Node.nodeType' in that specification.	Recommendation	No changes.

- Browser-specific API: 특정 브라우저만 제공하는 API

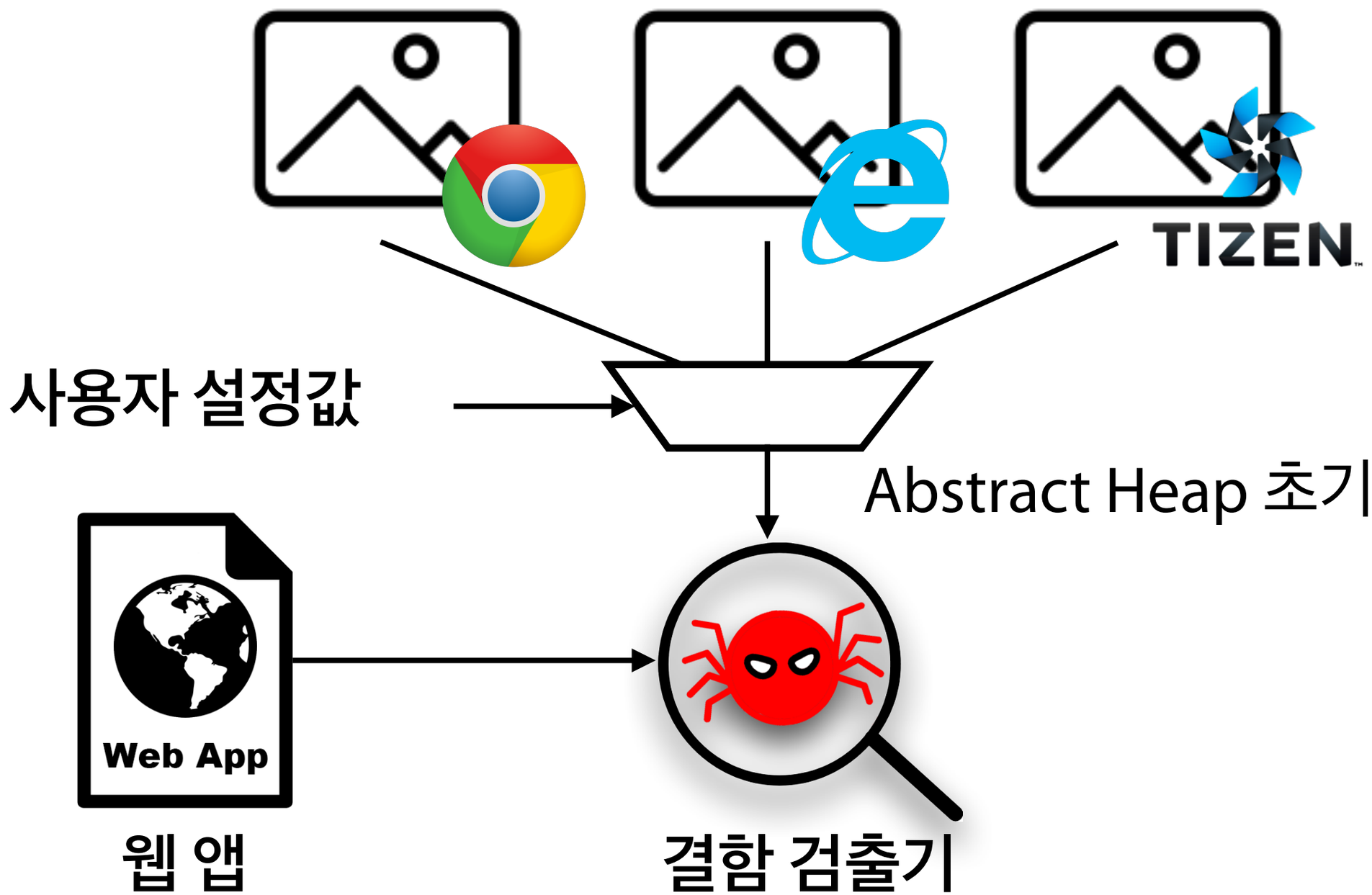
Snapshot

- 실행 환경을 특정하여 동적 정보로 정확한 값을 제공
  `navigator.language = "ko"`

- `window` 객체를 시작으로 재귀적인 property 접근을 통해 도달가능한 값을 저장



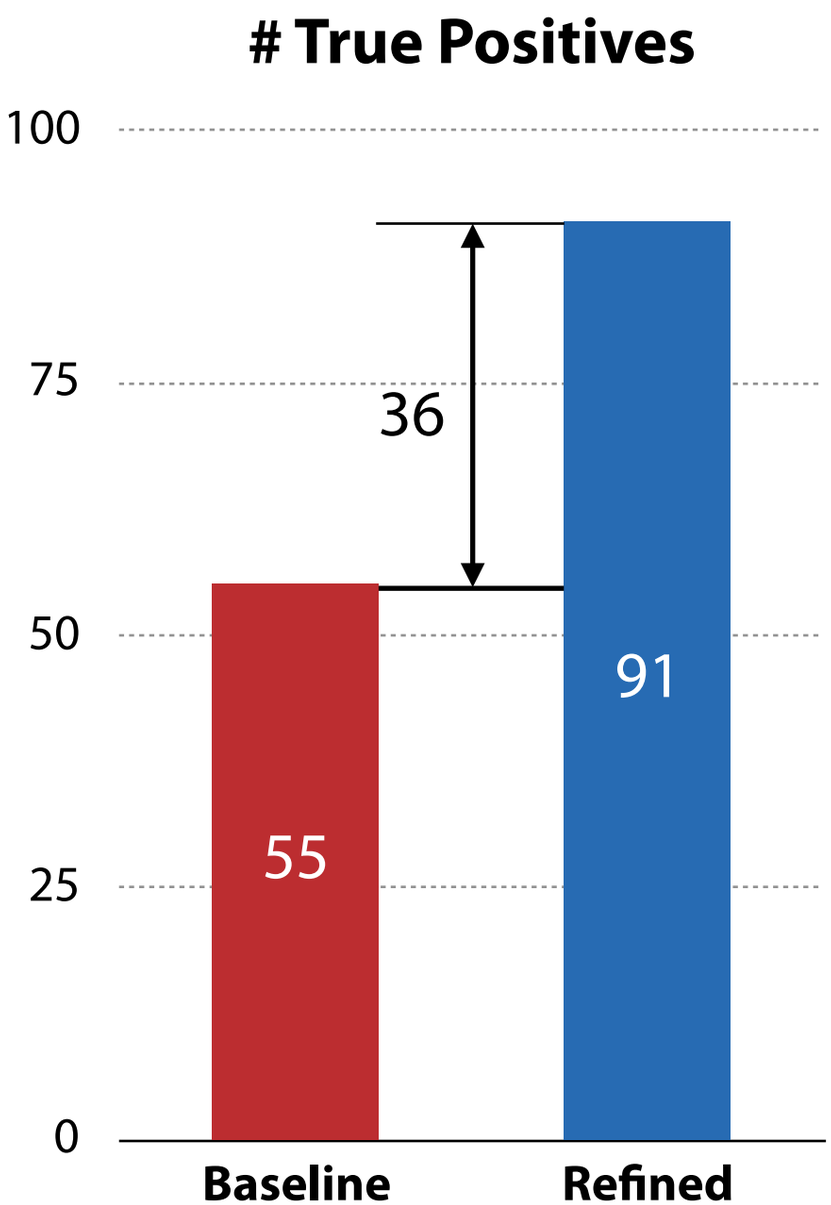
Snapshot

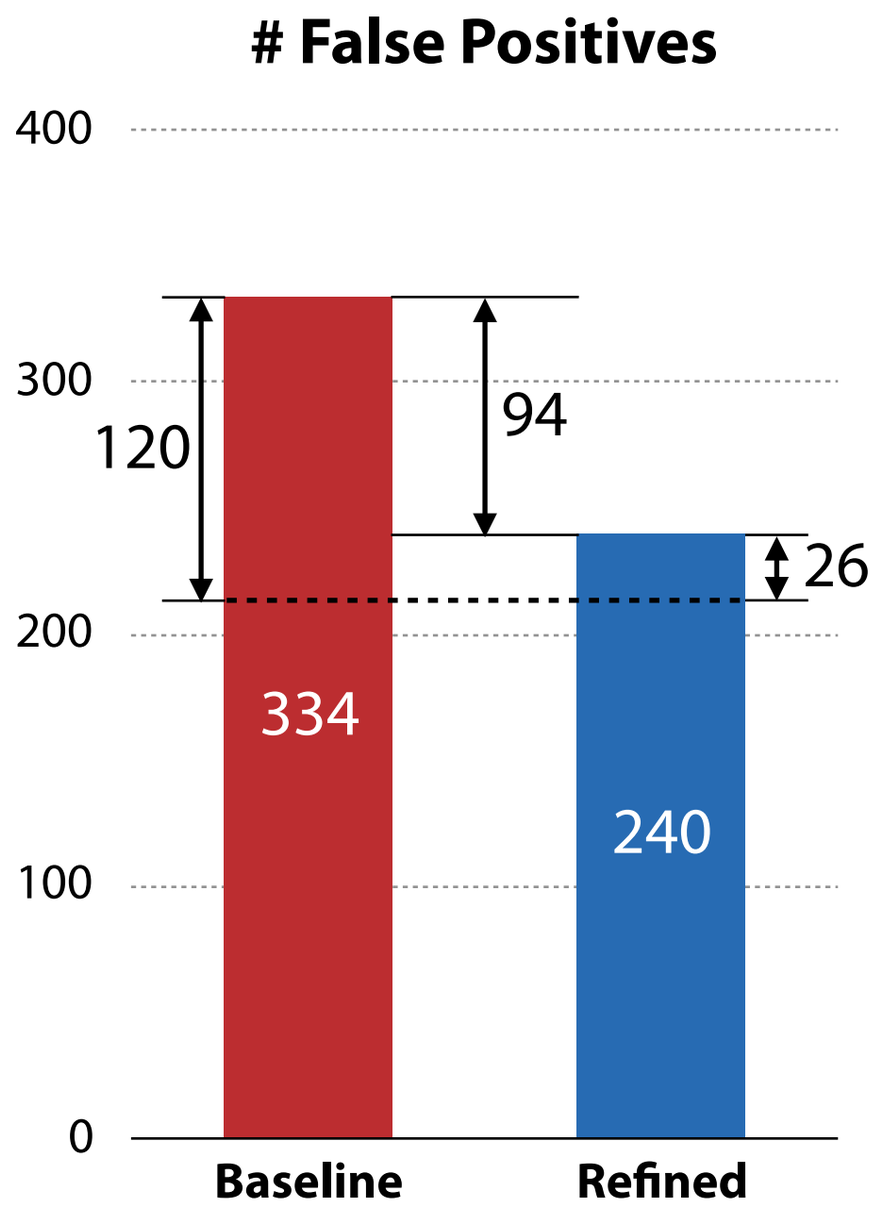


평가

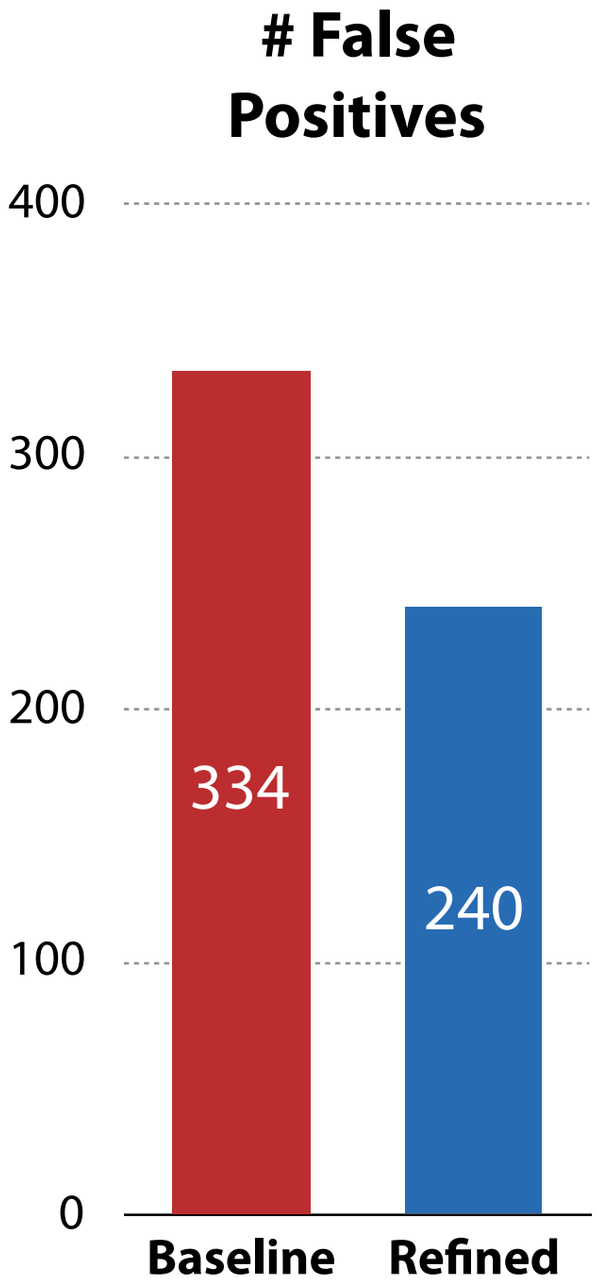
- RQ1: **Precision**. True/false 알람 개수 변화
- RQ2: **Coverage**. 분석된 파일과 함수의 개수 변화
- RQ3: **Scalability**. 분석 시간 변화

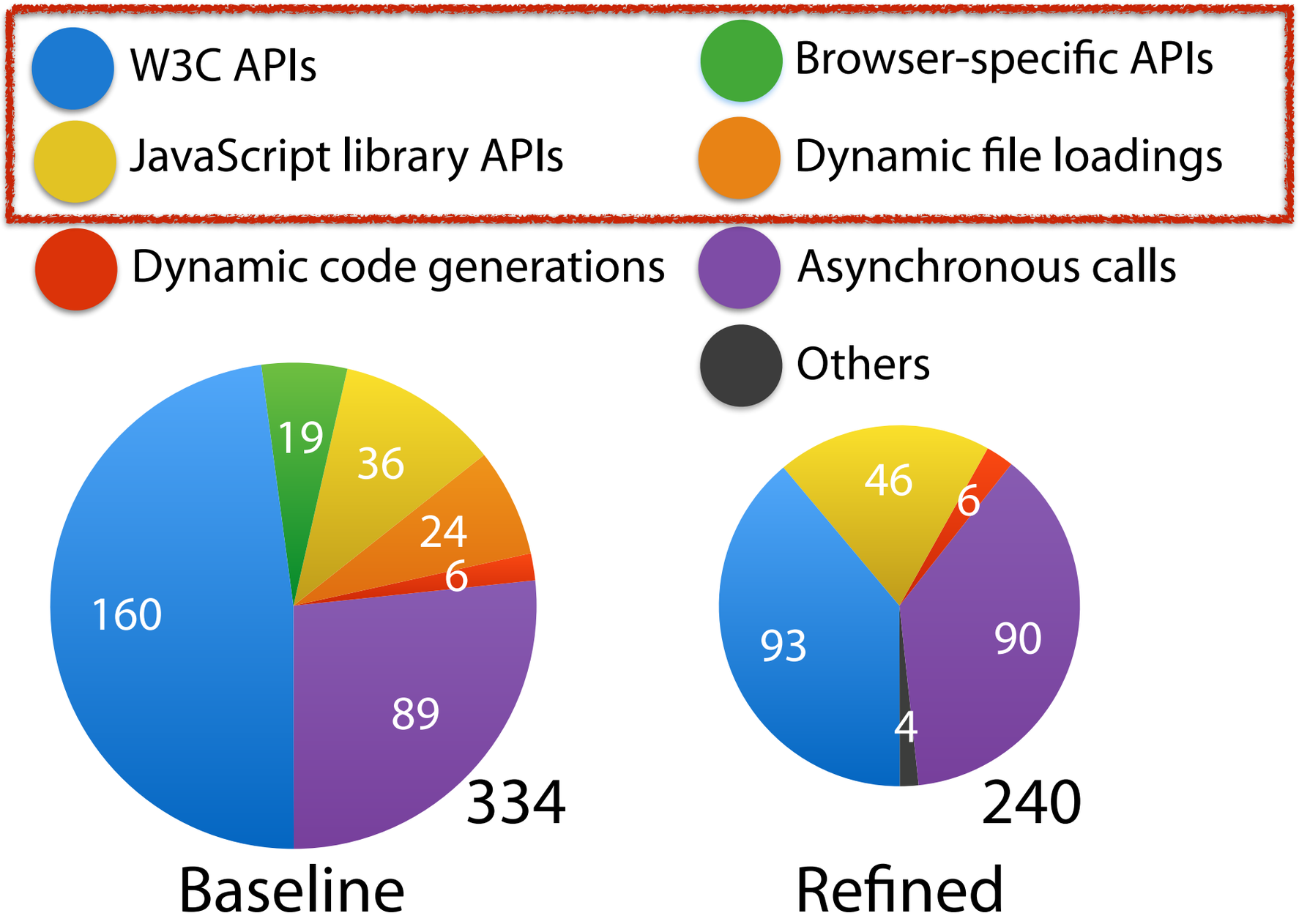
결과: Precision



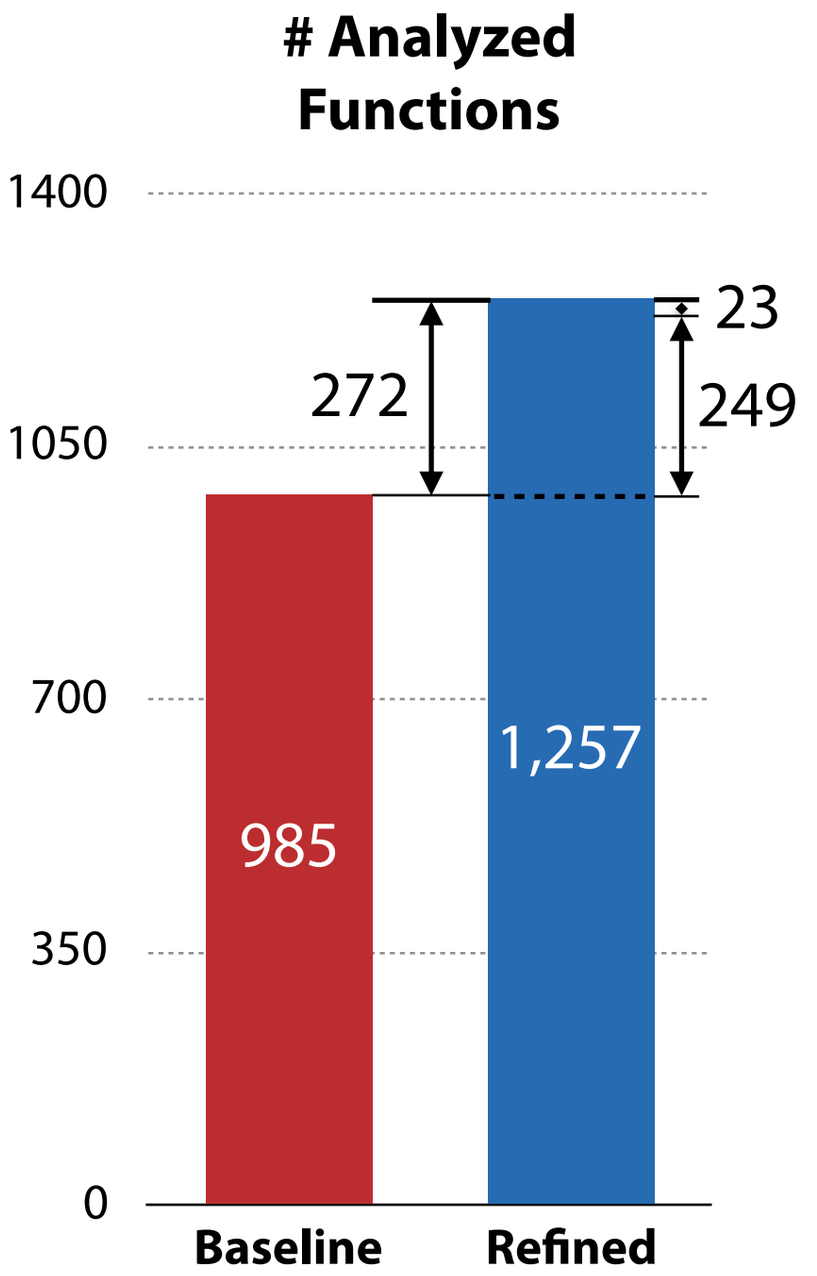


결과: Precision





결과: Coverage



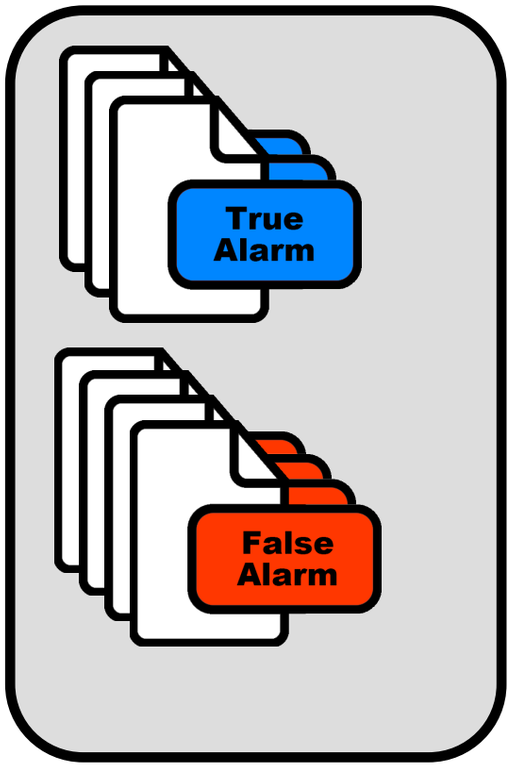
앱 디렉토리에 포함된 JS 파일 개수

Application Type	App ID	# JS files	# Loaded files	
			Baseline	Refined
Tizen/Chrome cross-platform	5)	422	1	10
	10)	13	1	13
	16)	15	1	15
Tizen SDK sample	18)	735	4	16
	19)	730	4	11
	20)	729	4	10
Tizen market	30)	375	14	17

결과: Scalability

분석 범위	평균 분석 시간 변화
변하지 않은 경우	1.28x
함수가 늘어난 경우	1.18x
파일과 함수가 늘어난 경우	4.09x
모든 경우	1.70x

요약



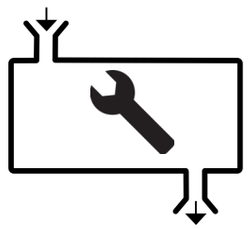
JS 파일 경로

+ 92 파일

+ 272 분석된 함수 (985 → 1257)

Snapshot

+ 새로 찾은 36 TP (55 → 91)

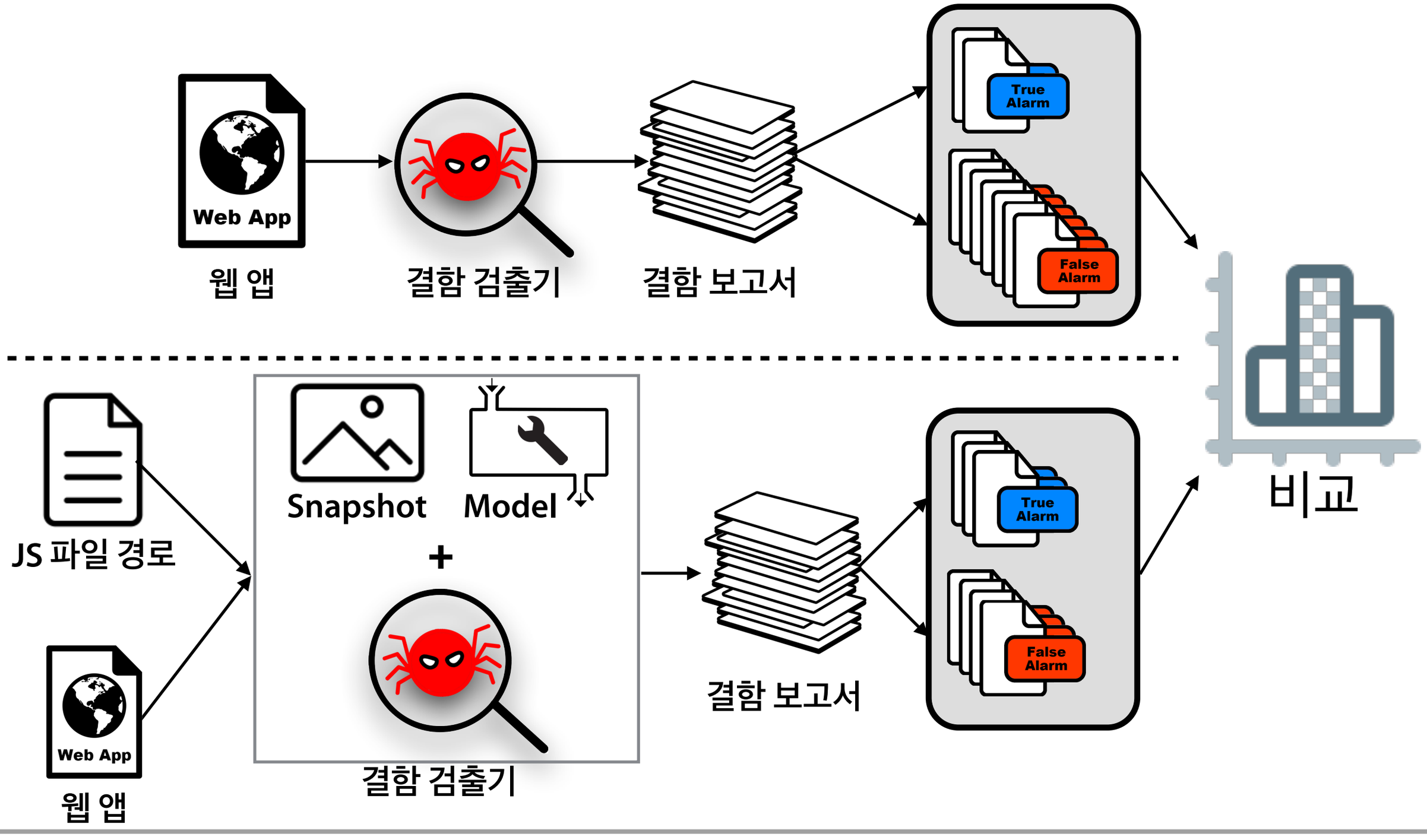


Type-based
JS Lib Model

- 94 FP (334 → 240)

1.70x 분석 시간

Q&A


Web App
웹 앱
결함 검출기
결함 보고서
True Alarm
False Alarm
비교
JS 파일 경로
Web App
웹 앱
Snapshot
Model
+
결함 검출기
결함 보고서
True Alarm
False Alarm