자바스크립트 웹 어플리케이션의 동적 테인트 분석

박준영
공동 연구 : 이성호, 류석영 교수님
Programming Language Research Group
한국과학기술원

목표

- 자바스크립트로 구현한 웹 어플리케이션에서 개인정보를 유출하는지 판별/흐름 확인

  ⇒ 사용자가 실제로 어플리케이션을 사용하는 도중에 개인정보가 유출되는 때를 테인트 분석을 통하여 감지

출발점

- Jalangi
  ⇒ 범용적 자바스크립트 동적 분석 프레임워크

- Jalangi의 필요한 부분만을 이용하여
  테인트 분석에 특화

Jalangi

- 6개 중 하나의 분석 예제

  ⇒ 간단한 테인트 분석

- 핵심 기법

  ⇒ 선택적 record-replay

instrument ➔ record ➔ replay(analyze)

테인트 분석에 특화

- record-replay 통합

  instrument ➔ record ➔ replay(analyze)

  instrument ➔ run(analyze)

- higher-level source/sink 정의

  low-level hard coding

  테이블로 관리하여 쉽게 추가/제거

예제

App.	eBook Reader(modified)
Source	document.cookie
Sink	XMLHttpRequest.send()

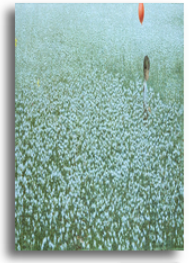
1. instrument
2. 실행

확장 프로그램 | Readium 라이브러리

chrome-extension://fepbnnnkkadjhjahcafoaglimekefifl/views/library_taint_.html

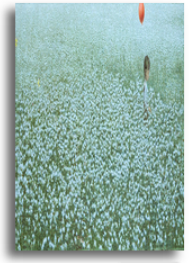
Readium

메밀 꽃 필 무렵
이효석



읽기 | 세부 항목

메밀 꽃 필 무렵
이효석



읽기 | 세부 항목

Elements Network Sources Timeline Profiles Resources Audits Console

<top frame>

```
event.returnValue is deprecated. Please use the standard event.preventDefault() instead.
'window.webkitStorageInfo' is deprecated. Please use 'navigator.webkitTemporaryStorage' or 'navigator.webkitPersistentStorage' instead.   d69bf
found sink
Data is leaked at : (tests/taint_tests/fepbnnnkkadjhjahcafoaglimekefifl/0.9.1_0/scripts/libs/plugins.js:720:45)
----
taint flow :
      at : (tests/taint_tests/fepbnnnkkadjhjahcafoaglimekefifl/0.9.1_0/scripts/d69bf62ca57fdbe0151f90a245536dd6.js:2947:17) => function (name)
           at : (tests/taint_tests/fepbnnnkkadjhjahcafoaglimekefifl/0.9.1_0/scripts/d69bf62ca57fdbe0151f90a245536dd6.js:2794:30) <= function (c_name)
source at : (tests/taint_tests/fepbnnnkkadjhjahcafoaglimekefifl/0.9.1_0/scripts/d69bf62ca57fdbe0151f90a245536dd6.js:616:26)
====================Timer Report=======================
595
====================Timer Report=======================
```

끝