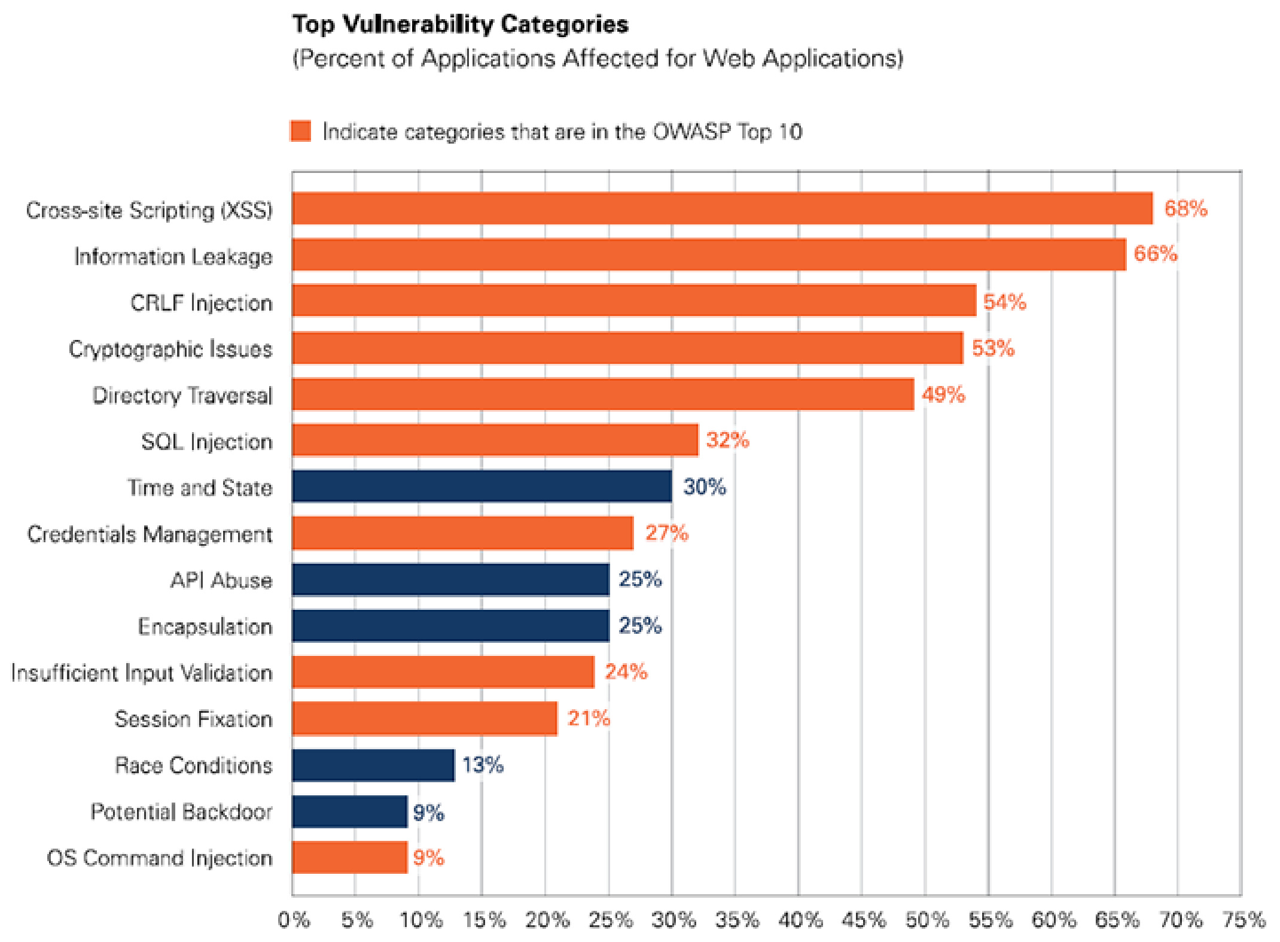
NUS
National University of Singapore

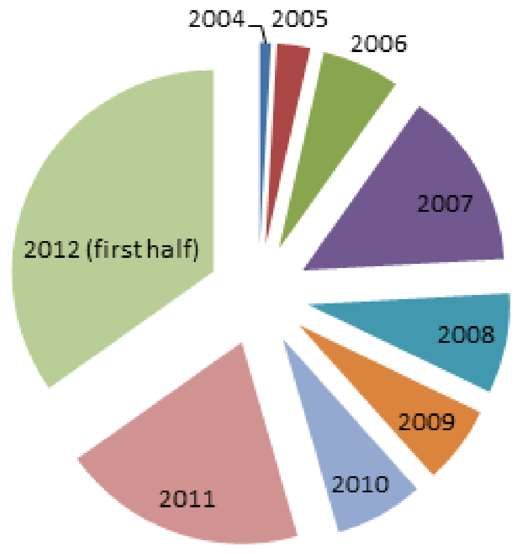
DOM-based XSS Filter

Heryandi, Lu Fangjian, Yang Yuhang, Yang Zhaoyu
School of Computing, National University of Singapore

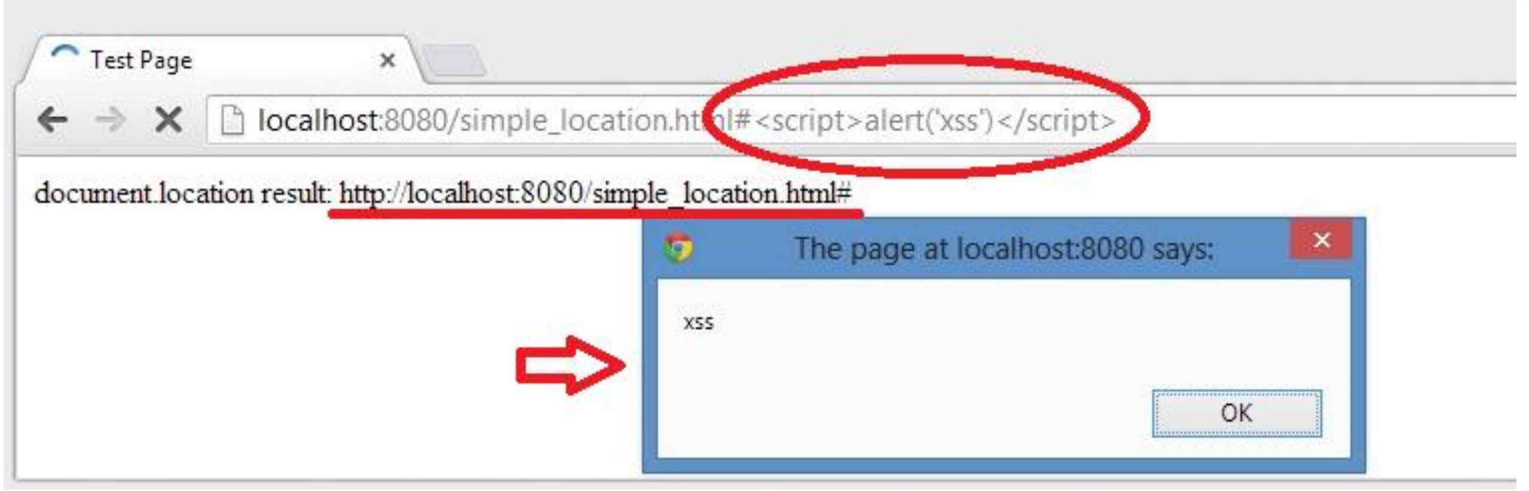
Web Apps Attack Trends


Top Vulnerability Categories
(Percent of Applications Affected for Web Applications)

Percentage of MSRC cases identified as XSS



DOM-based XSS is different from stored XSS and reflected XSS



localhost:8080/simple_location.html#<script>alert('xss')</script>

document.location result: http://localhost:8080/simple_location.html#

The page at localhost:8080 says:

xss

OK

Attack is executed entirely within the browser!

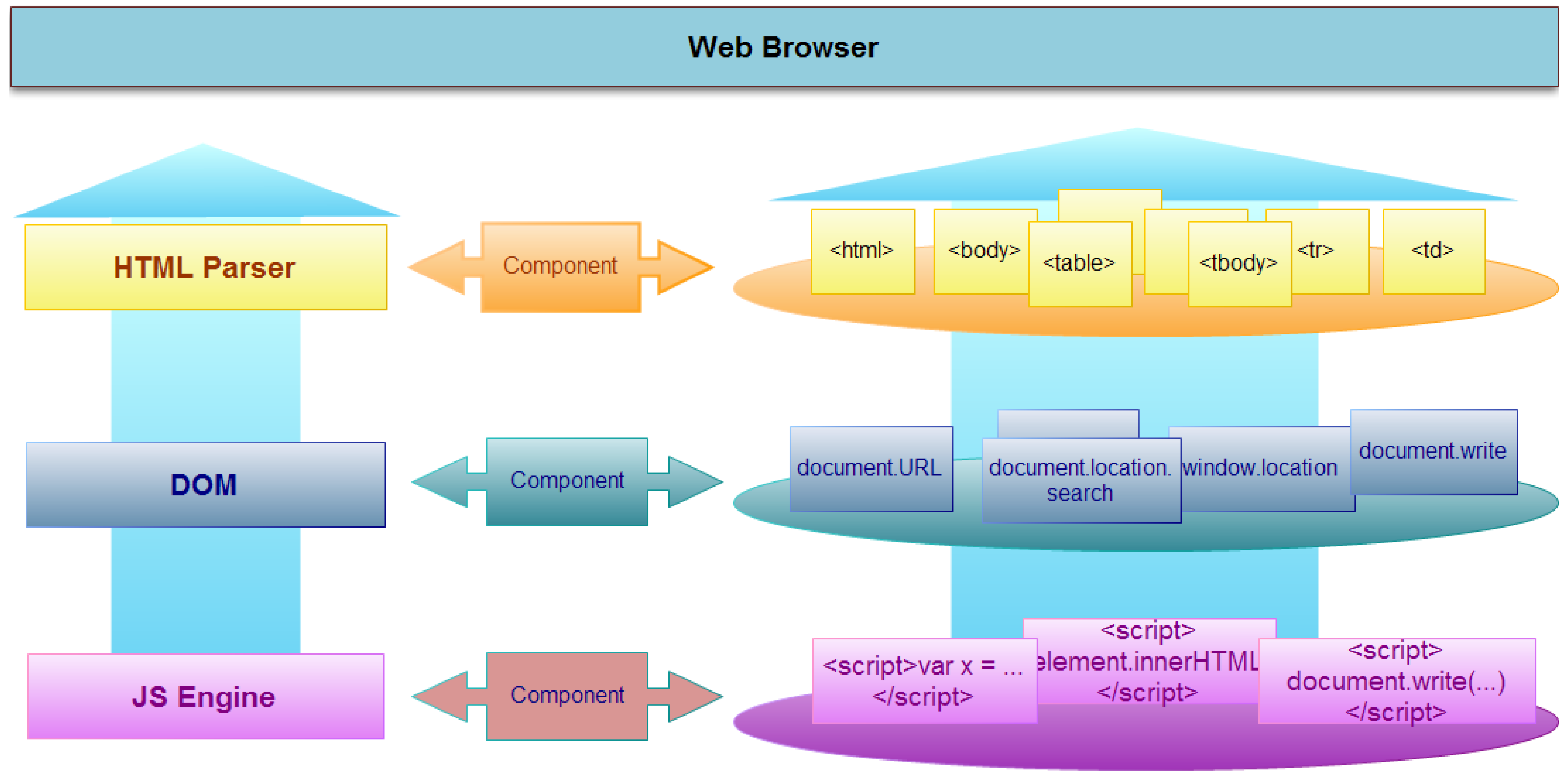
Page makes use of unsafe input!

Goal

Intercept and handle potential vulnerability with minimal impact on user experience.

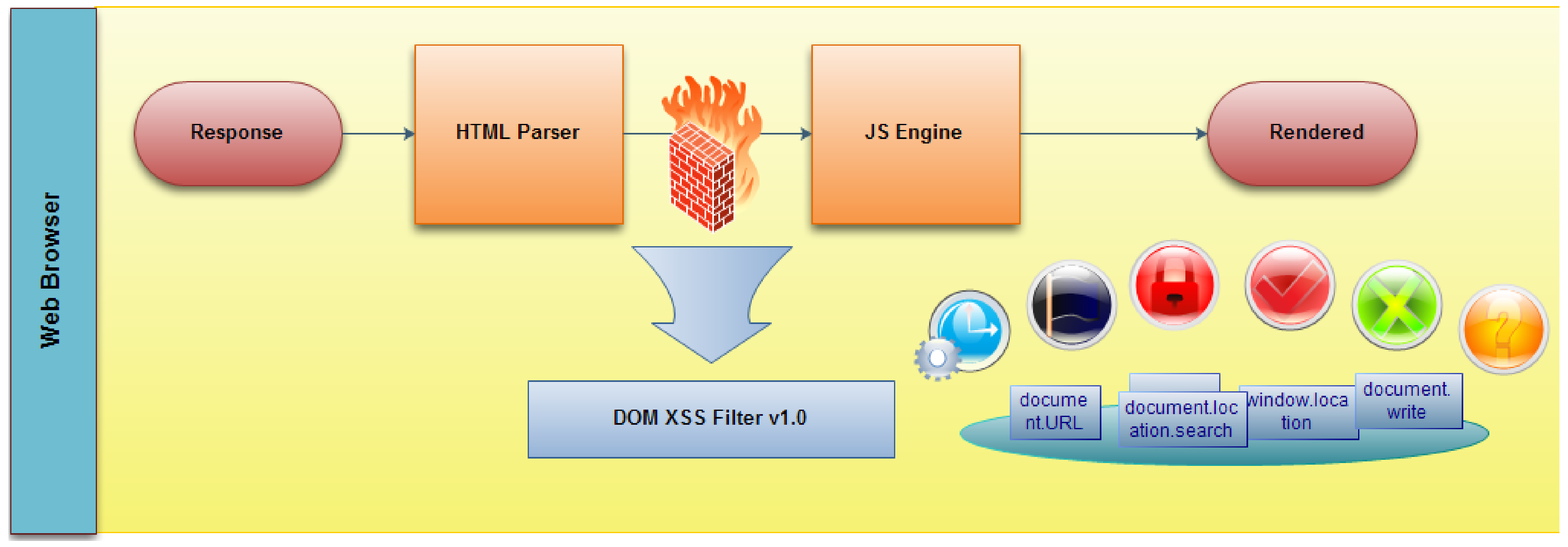
- **Efficiency: No significant overhead**
- **Flexibility: Easy to maintain**
- **Compatibility: Compatible with most websites**
- **Effectiveness: Protection from DOM-based XSS**

Approach Overview



Our Solution: Protect access to unsafe inputs!

- **Remove Referer from HTTP header**
  - **Intercept and remove by chrome.webRequest API**
- **Protection: encode return value**

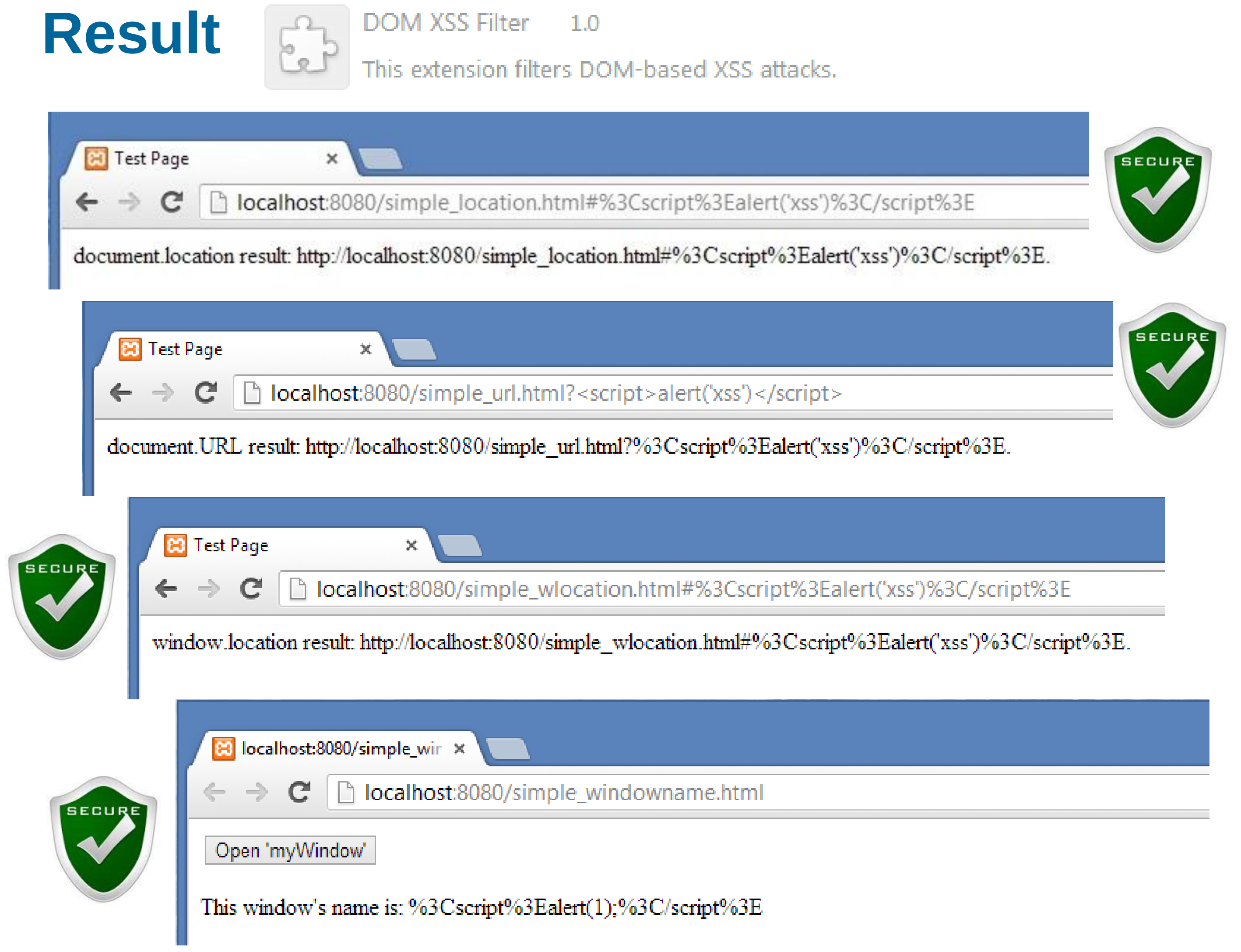


- **Chrome Content Script**
  - **Before complete DOM tree is constructed, inject small amount of JavaScript to…**
    - **Override `document.URL` getter**
    - **Override `document.URLUnencoded` getter**
    - **Protect `document.location`:**
      - **`document.location.search` already encoded**
      - **Override `document.location.hash` getter**
    - **Override `window.name` getter**
    - **Force encode `window.location.hash`**

Implementation

- **Browser**
  - **Google Chrome 26.0.1410.43 m & 27.0.1453.9 m**
- **JavaScript**
- **Chrome Extension API**
  - **chrome.webRequest**
  - **Content Script**

Result



DOM XSS Filter 1.0

This extension filters DOM-based XSS attacks.

localhost:8080/simple_location.html#%3Cscript%3Ealert('xss')%3C/script%3E

document.location result: http://localhost:8080/simple_location.html#%3Cscript%3Ealert('xss')%3C/script%3E.

localhost:8080/simple_url.html?<script>alert('xss')</script>

document.URL result: http://localhost:8080/simple_url.html?%3Cscript%3Ealert('xss')%3C/script%3E.

localhost:8080/simple_wlocation.html#%3Cscript%3Ealert('xss')%3C/script%3E

window.location result: http://localhost:8080/simple_wlocation.html#%3Cscript%3Ealert('xss')%3C/script%3E.

localhost:8080/simple_wir

localhost:8080/simple_windowname.html

This window's name is: %3Cscript%3Ealert(1);%3C/script%3E

Evaluation

- **Efficiency: 1.5 page of un-minified code**
- **Flexibility: Plain JavaScript & Chrome API**
- **Compatibility: Tested with 10 websites**

https://www.google.com	https://mail.google.com
https://www.facebook.com	https://twitter.com
http://www.wikipedia.org	http://slashdot.org
https://news.ycombinator.com	http://www.yahoo.com
http://www.youtube.com	http://www.amazon.com

- **Effectiveness: See Result**