Metamong: Detecting Render-Update Bugs in Web Browsers through Fuzzing

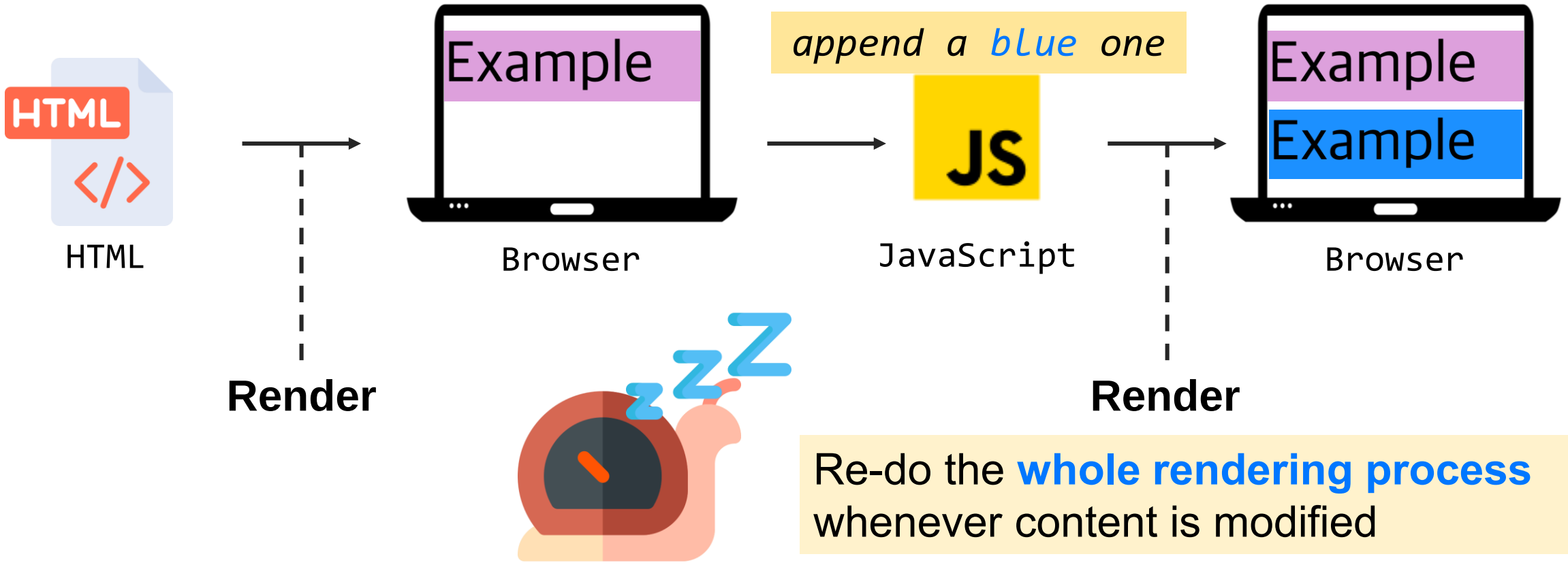
Suhwan Song and Byoungyoung Lee

서 울 대 학 교
SEOUL NATIONAL UNIVERSITY

 : sshkeb96@snu.ac.kr

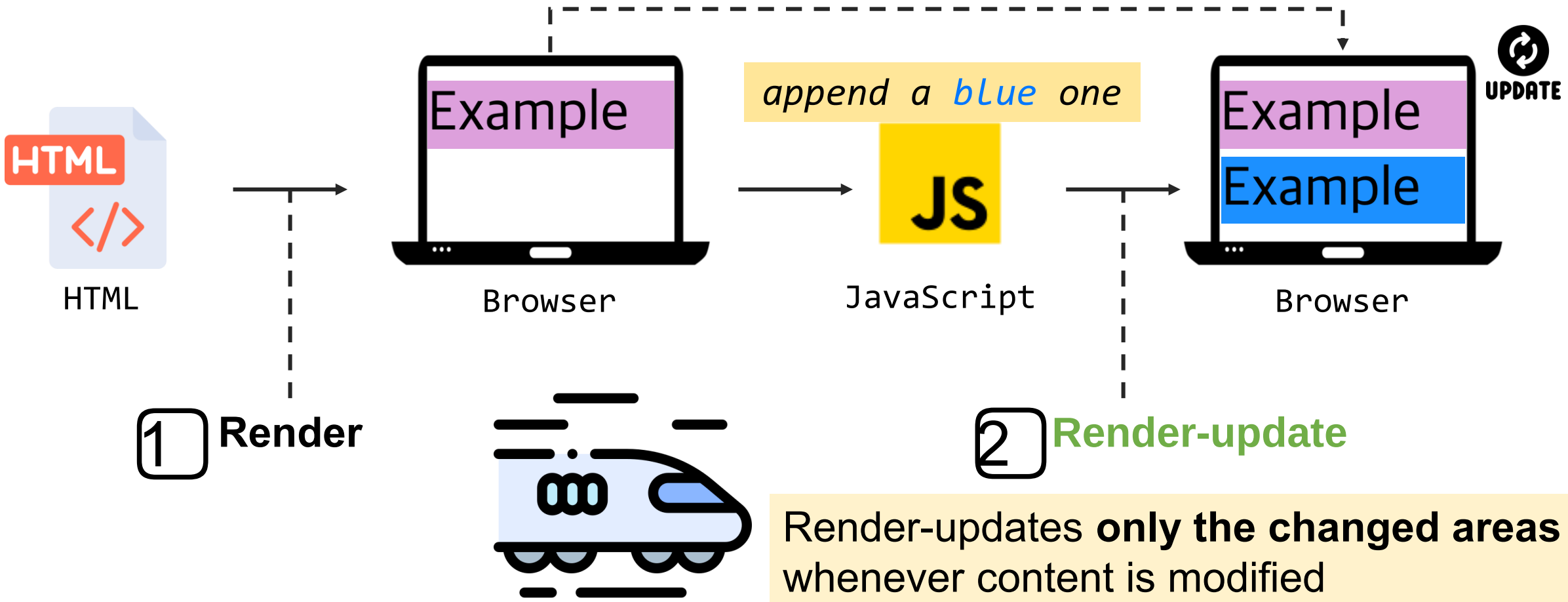
 : https://suhwansong.github.io/

Rendering process of browsers



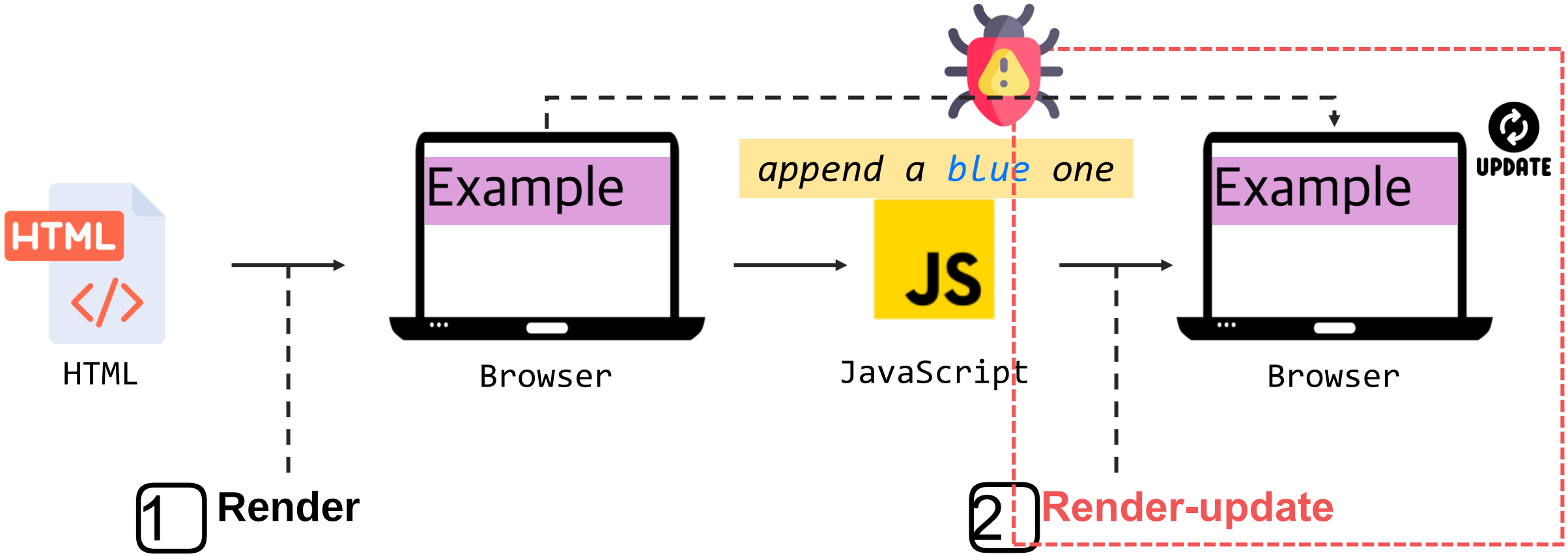
Re-do the **whole rendering process** whenever content is modified

Rendering process of modern browsers



Render-updates **only the changed areas** whenever content is modified

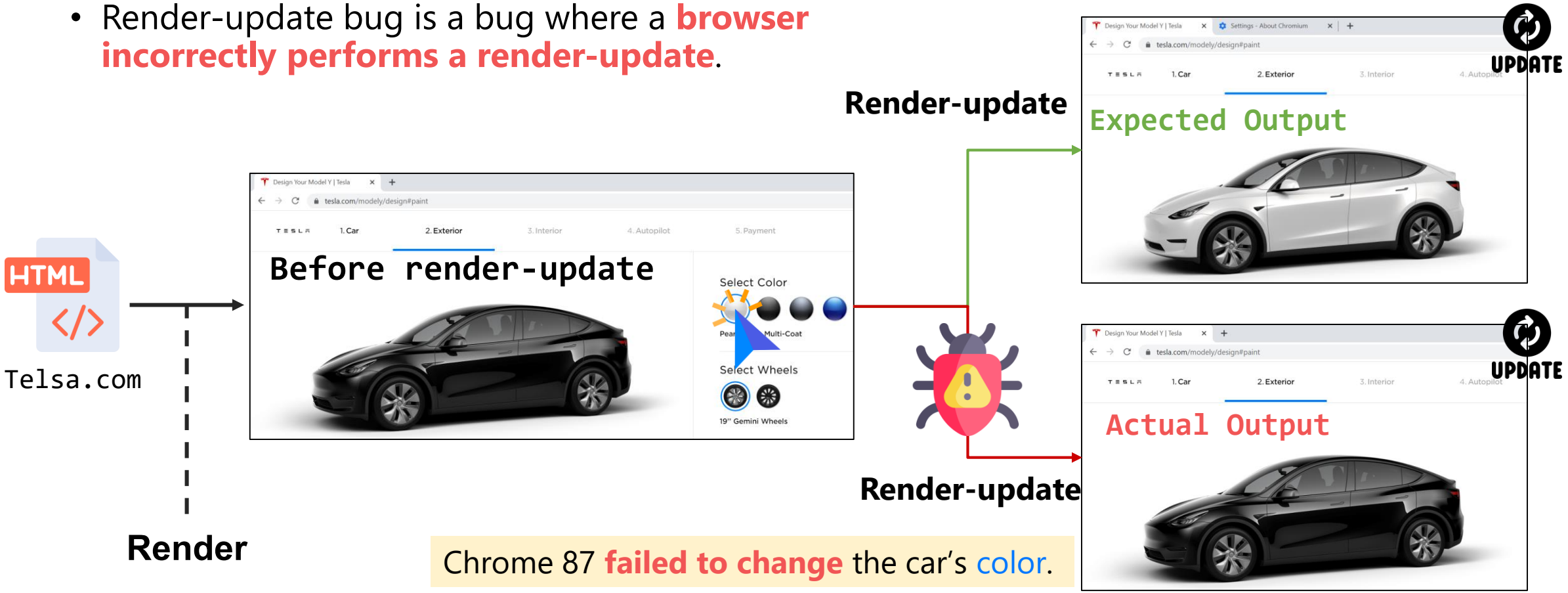
Optimization can introduce a bug!



Fail to draw the blue one due to the render-update bug

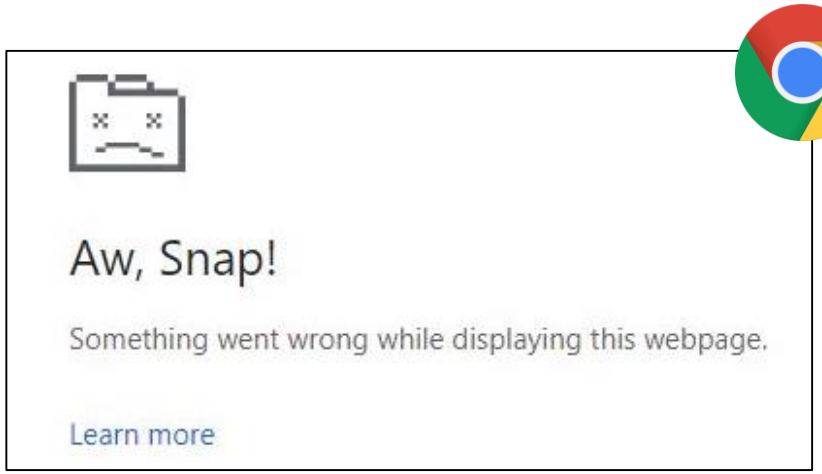
Render-update bug on a real website!

- Render-update bug is a bug where a **browser incorrectly performs a render-update**.



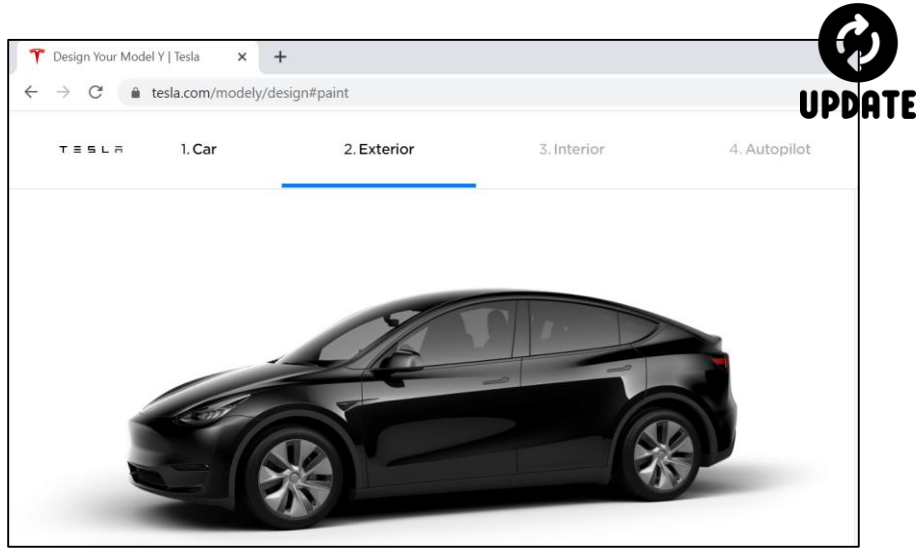
Chrome 87 **failed to change** the car's color.

Identifying render-update bugs is challenging



Memory Bug

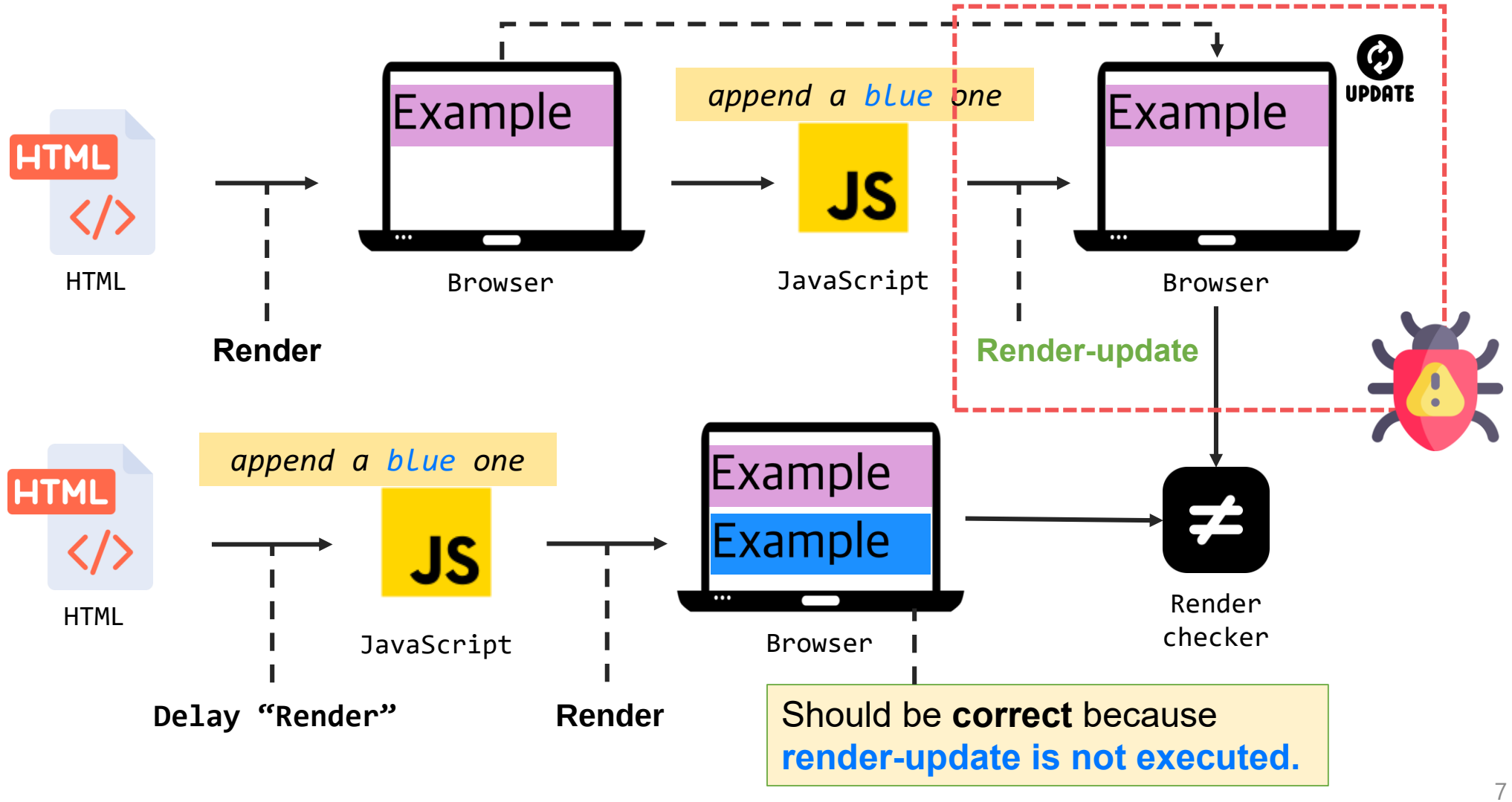
Crash can be detected



Render-update Bug

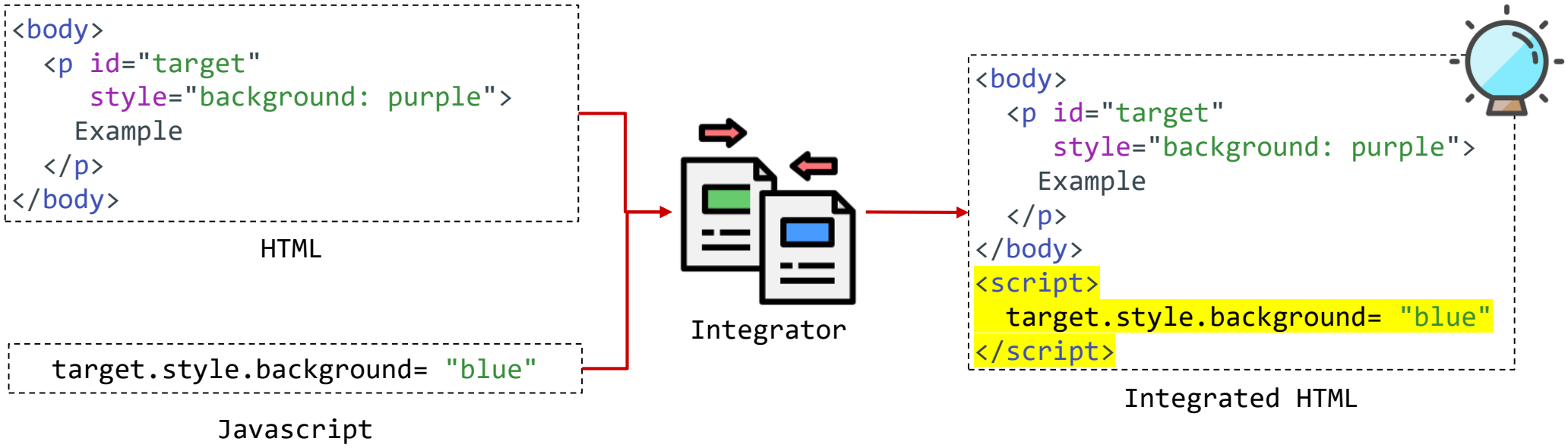
No crash at all…

Render-update oracle

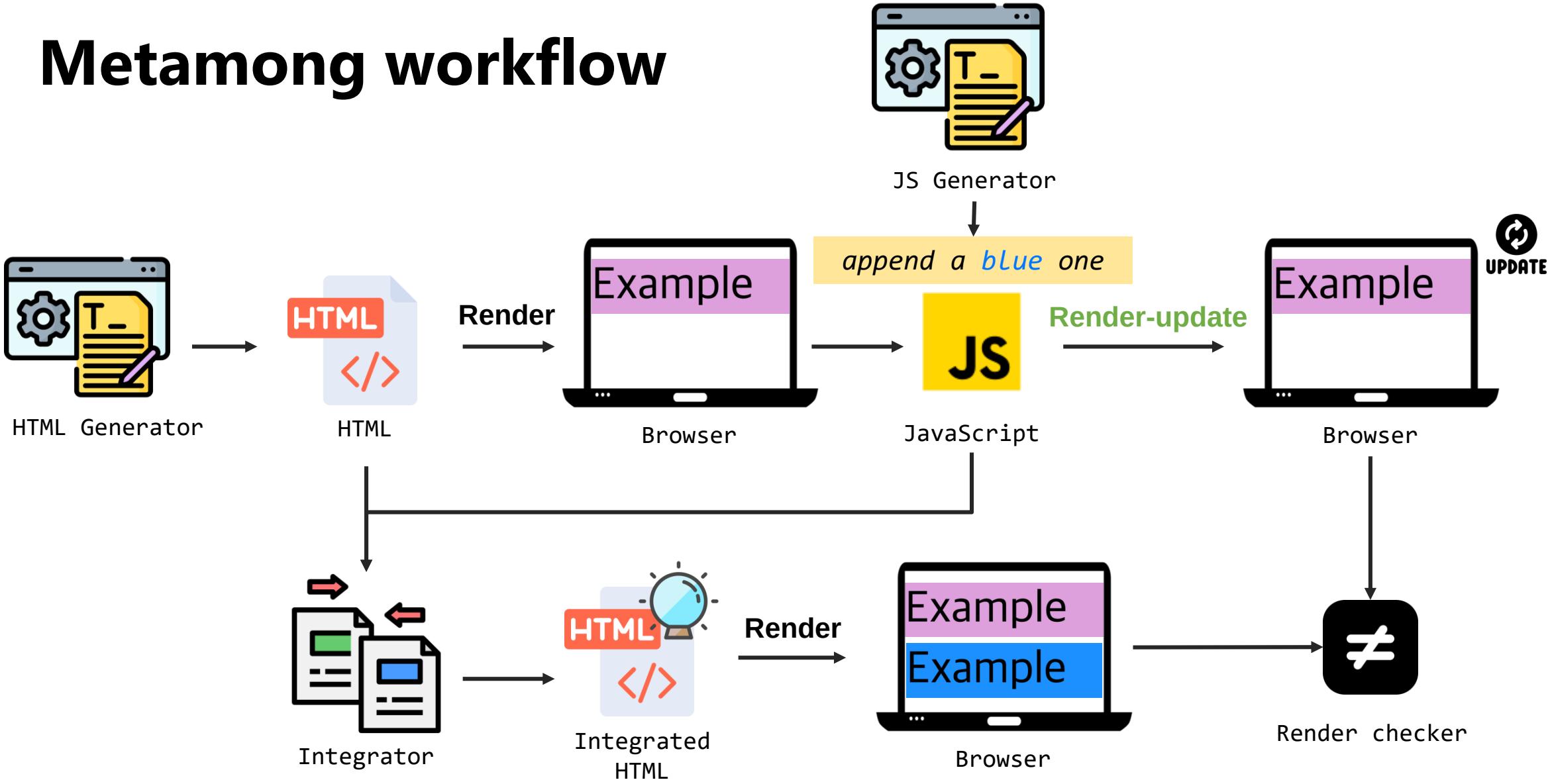


How to delay “Render”

- Wraps the mutation primitive with <script> tag and append it.

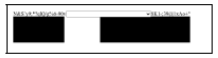
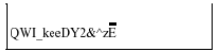
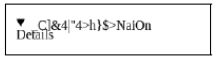
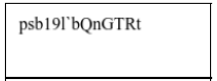
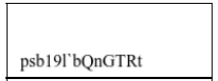
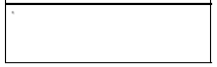
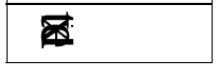
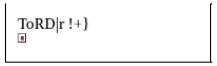
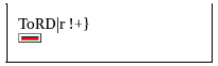


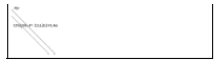
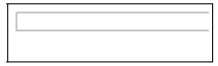
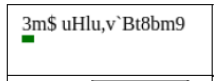
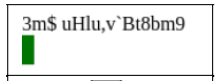
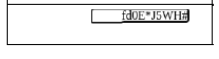
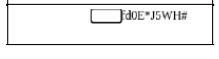
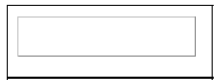
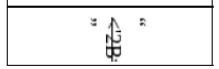
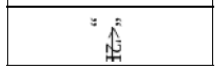
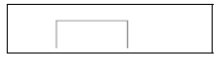
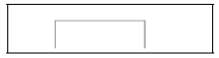
Metamong workflow



New render-update bugs

We found **19** new render-update bugs without false positive issues and **five** of them were fixed.

Browser	Issue ID	Correct	Incorrect	New	Fixed	Description
Chrome (89.0.4329.0)	#1154662			✓		The dashed underline is incorrect after removing an
Chrome (89.0.4329.0)	#1162740			✓		
Chrome (89.0.4329.0)	#1163006			✓	✓	
Chrome (89.0.4329.0)	#1163031			✓		
Chrome (89.0.4329.0)	#1164643			✓	✓	
Chrome (108.0.5305.0)	#1364376			✓		
Chrome (108.0.5305.0)	#1365243			✓	✓	
Chrome (108.0.5305.0)	#1365244			✓		
Chrome (108.0.5305.0)	#1365252			✓		

Browser	Issue ID	Correct	Incorrect	New	Fixed	Description
Chrome (108.0.5305.0)	#1365255			✓	✓	The border line of <fieldset> is not updated after removing a CSS rule "offset-path".
Chrome (108.0.5305.0)	#1365746			✓		The height of <fieldset> does not decrease after removing a CSS rule "margin-right".
Chrome (108.0.5305.0)	#1366233			✓	✓	The shape of <q> is incorrect after removing a CSS rule "font-weight".
Chrome (108.0.5305.0)	#1366280			✓		The height of <th> is incorrect after removing a CSS rule "margin-left".
Chrome (108.0.5305.0)	#1370936			✓		The border line is incorrect after removing a CSS rule "-webkit-border-end".
Chrome (108.0.5305.0)	#1370962			✓		The size of <table> is incorrect after removing a CSS rule "@font-face".
Chrome (108.0.5305.0)	#1370987			✓		The position of quote is incorrect after removing an element.
Chrome (108.0.5305.0)	#1371003			✓		The location of text is incorrect after adding an element.
Firefox (85.0a1)	#1680232			✓		The line moves to a wrong position after adding a CSS rule "display".
Firefox (85.0a1)	#1683814			✓		The size of <dir> is bigger unexpectly after adding an element.

Conclusion

- This paper proposed Metamong, a framework tailored for detecting render-update bugs in web browsers without false positives.
- Metamong consists of two key components: a page mutator and a render-update oracle to trigger and detect the render-update bugs.
- Metamong has found 19 new bugs in Chrome and Firefox.