Janus: Detecting Rendering Bugs in Web Browsers via Visual Delta Consistency

Chijin Zhou[1], Quan Zhang[1], Bingzhou Qian[2], Yu Jiang[1]

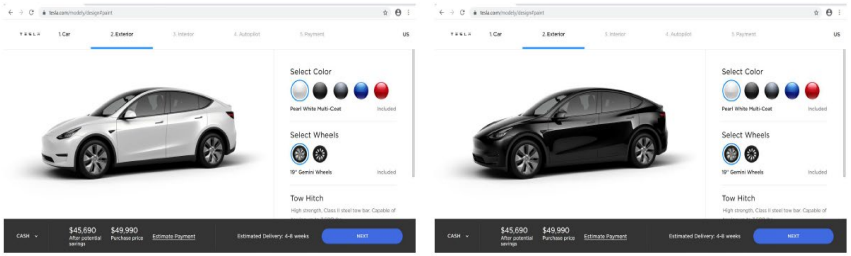
[1]Tsinghua University, China
[2]NUDT, China

Why focus on *rendering bugs*?

rendering bugs are ...

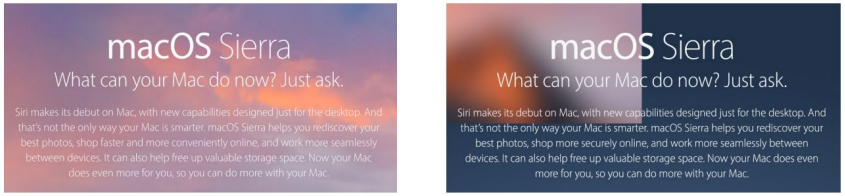
- ***Important***: rendering lies at the heart of our web experience
- ***Unavoidable***: standards evolve rapidly causing frequent browser updates
- ***Numerous***: 20,000+ rendering bugs were filed in the last 5 years

Chrome 87.0.4274.0



(a) Expected rendered page. (b) Actual rendered page.

Chrome 55.0.2852.0



(a) Expected rendered page. (b) Actual rendered page.

Motivation: why not *differential testing*?

Case 1: Support of styles varies across browsers

Rendered Page

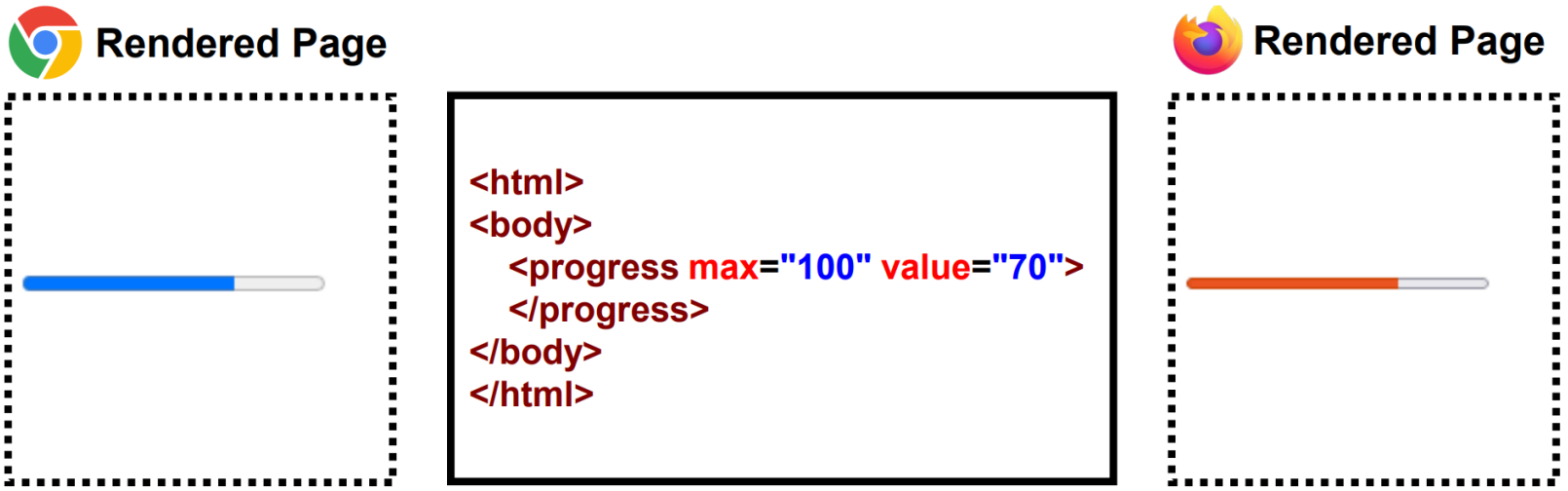
```
<html>
<body>
   <textarea style="content-visibility:
hidden">TEXT</textarea>
   <img src="img.png"
  style="-webkit-box-reflect: below;">
</body>
</html>
```

Rendered Page

content-visibility	√	content-visibility	×
-webkit-box-reflect	√	-webkit-box-reflect	×

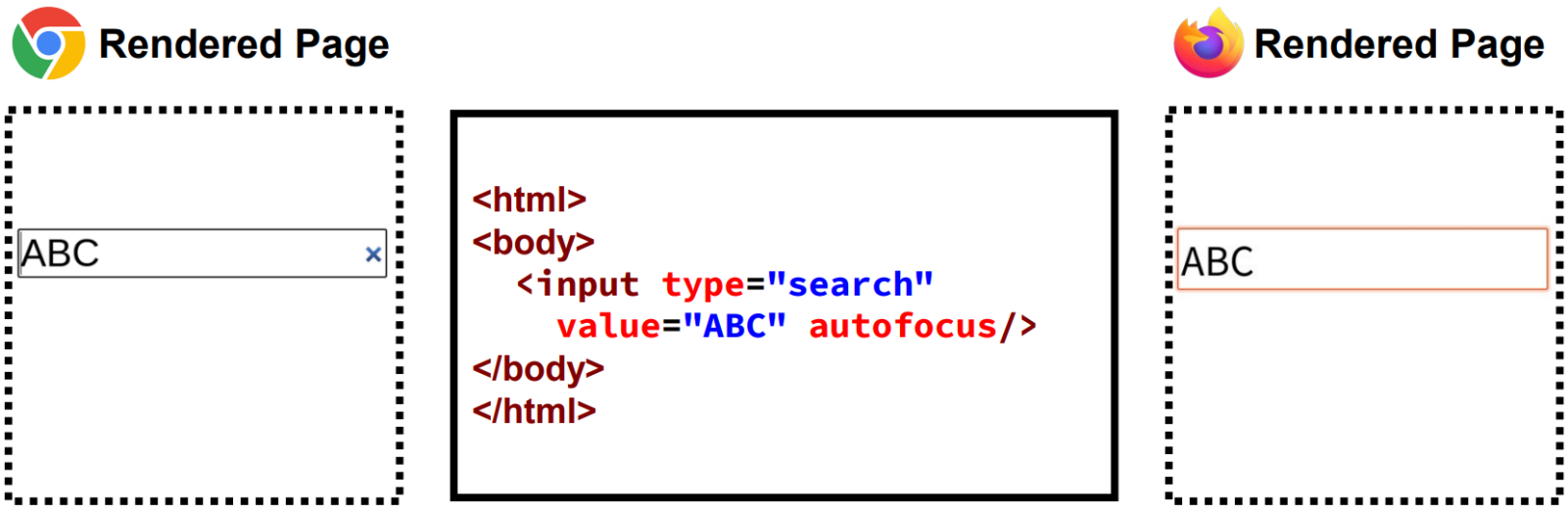
Motivation: why not *differential testing*?

Case 2: Default style for some elements varies across browsers



Motivation: why not *differential testing*?

Case 3: Rendered appearance for some elements varies across browsers



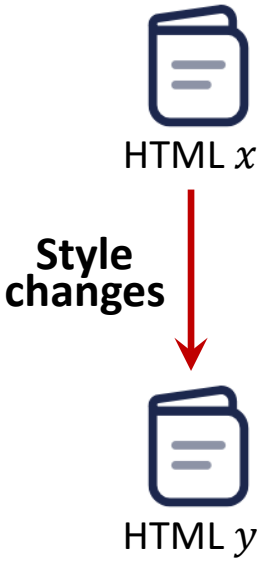
Motivation: why not *differential testing*?

The *same* HTML file is likely to yield *different* rendered pages across browsers

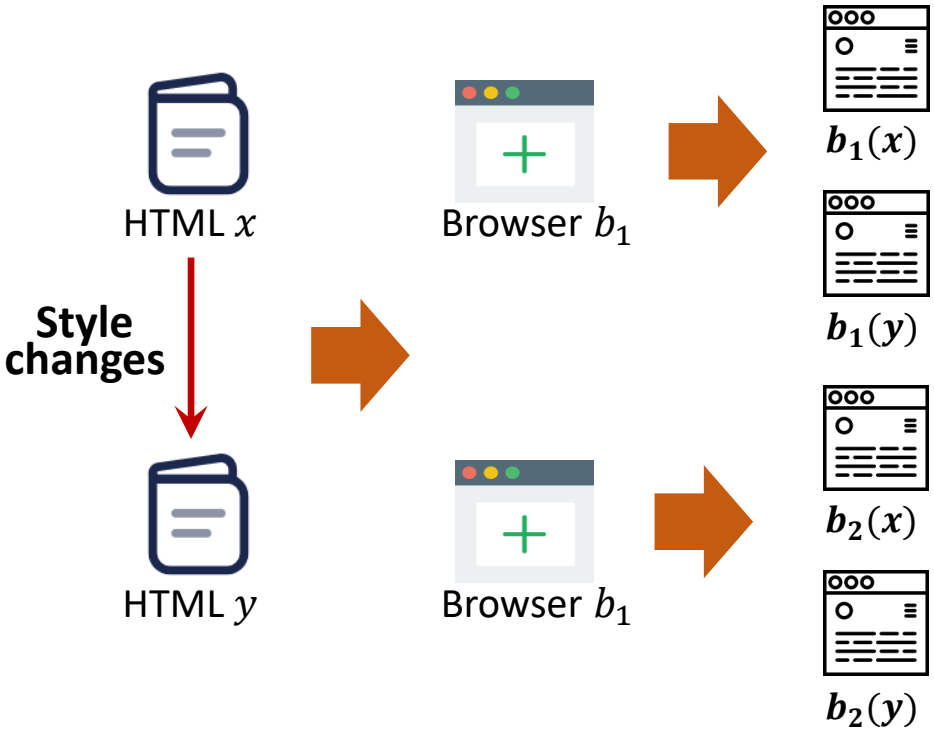
Basic idea of ***Janus***

HTML x

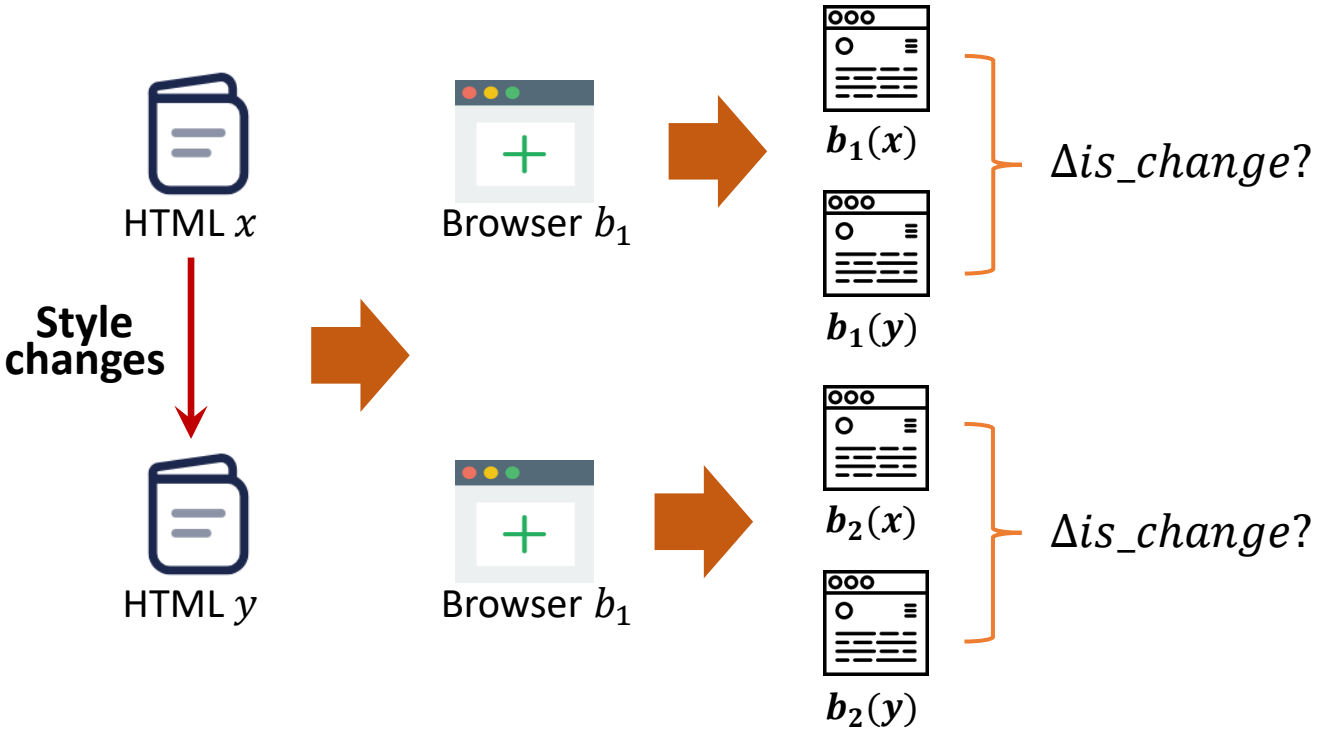
Basic idea of ***Janus***



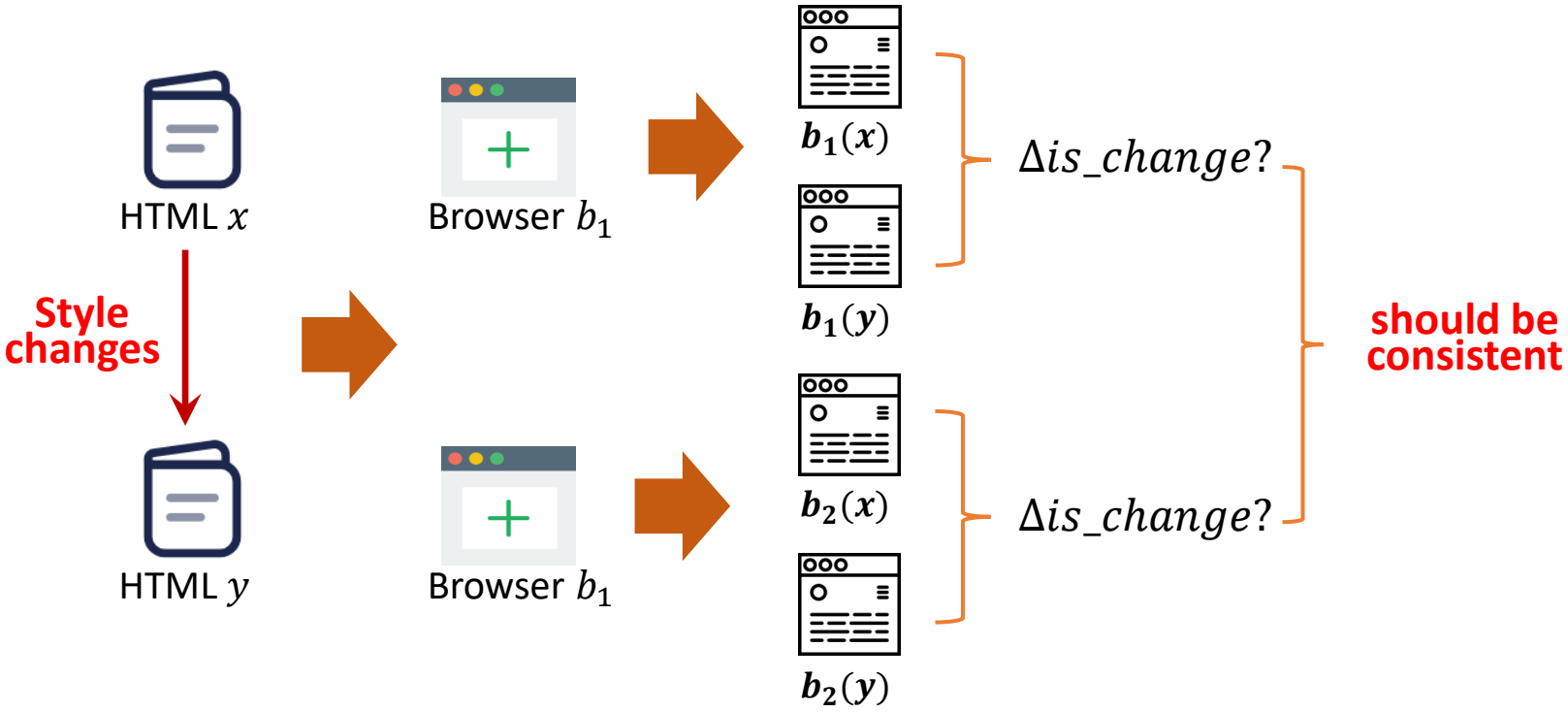
Basic idea of ***Janus***



Basic idea of ***Janus***



Basic idea of ***Janus***

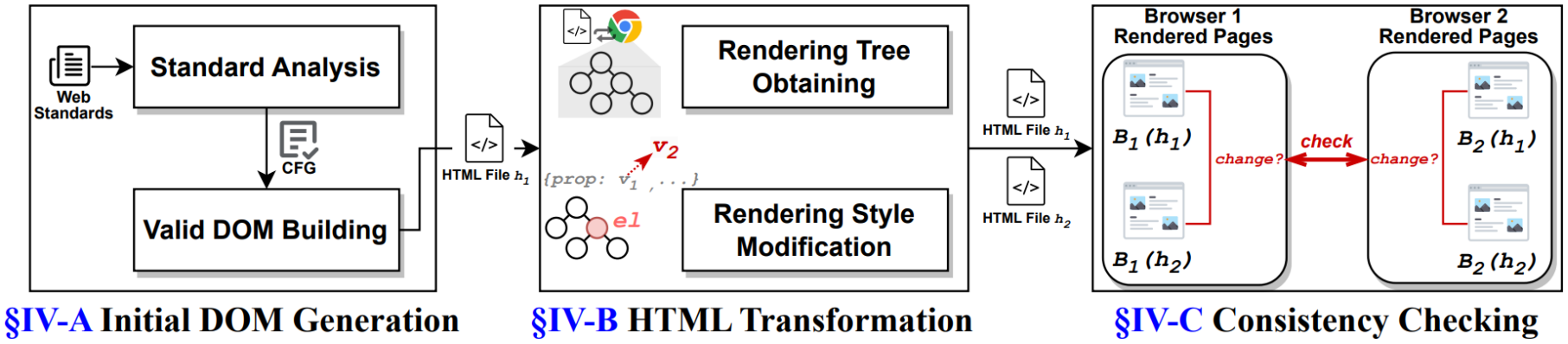


Visual Delta Consistency: If all rendering features used in x and y are supported by b_1 and b_2,the visual delta should be consistent.

See the paper for proof

Design

- Approach:
  - analyze web standards to randomly construct a valid HTML file
  - modify a node in the rendering tree with a valid value
  - check if the change status of rendered pages is consistent



Evaluation

highlight

- Janus found **31** non-crash rendering bugs in mainstream browsers, with **24** confirmed by developers.
- Bugs affect all kinds of rendering-related components.
- Janus only introduces **13%** overhead in the browser fuzzing process.

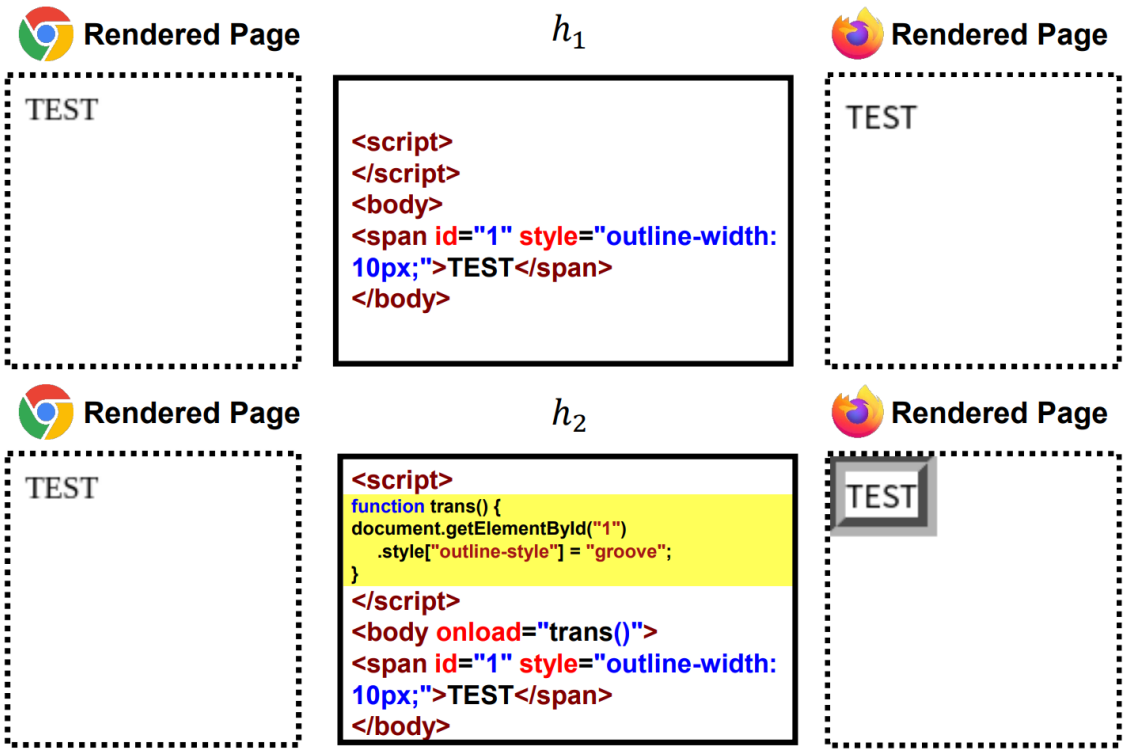
Browser	Reported	Confirmed	Duplicated	Fixed
Chrome	8	6	2	4
Safari	21	16	3	4
Firefox	2	2	0	0
Total	31	24	5	8

Browser	Affected Component				
	Content	DOM	Forms	Layout	Paint
Chrome	1	0	0	5	2
Safari	1	1	7	4	8
Firefox	1	0	0	1	0
Total	3	1	7	10	10

	Initial DOM Generation	HTML Transformation	Browser Execution	Consistency Checking
Time (ms)	1.35	12.88	1286.45	177.45
Percentage	0.09%	0.87%	87.03%	12.01%

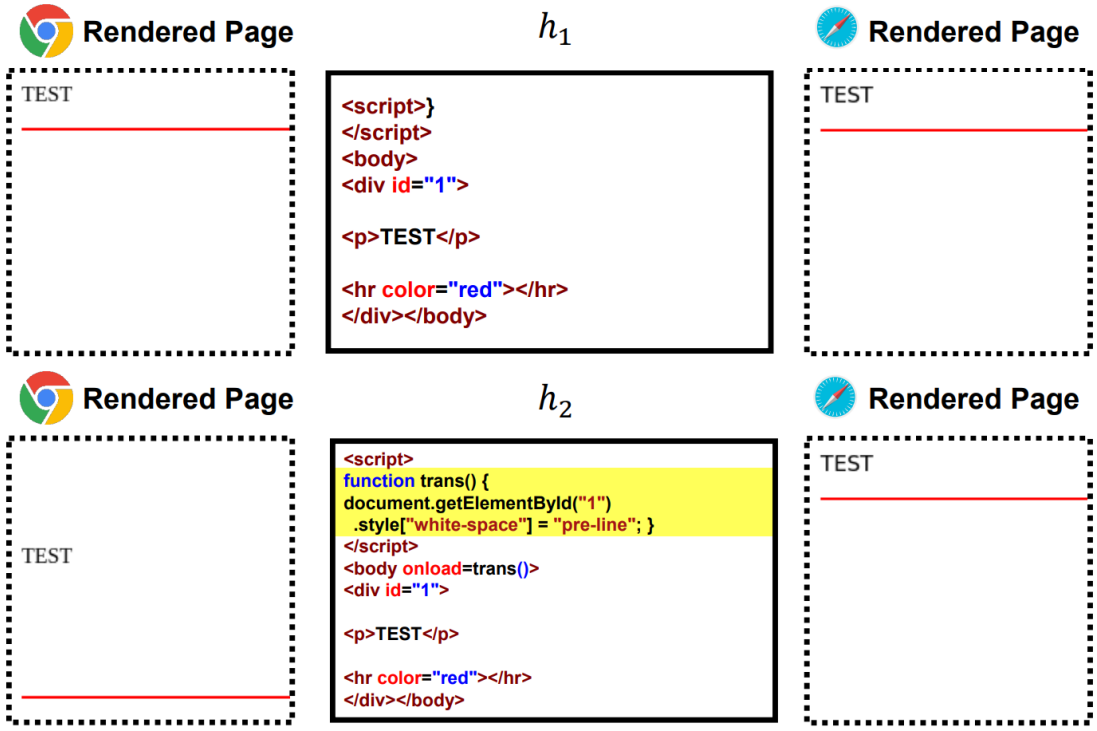
Evaluation

Bug case 1: Chrome incorrectly implemented groove



Evaluation

Bug case 2: Safari fails to render the empty lines



Summary

Prototype: https://github.com/ChijinZ/janus-browser-fuzzer

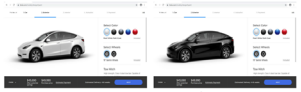
Goal: detecting rendering bugs

Why focus on *rendering bugs*?

rendering bugs are ...

- ***Important***: rendering lies at the heart of our web experience
- ***Inevitable***: standards evolve rapidly causing frequent browser updates
- ***Numerous***: 20,000+ rendering bugs were filed in the last 5 years

Chrome 87.0.4274.0



(a) Expected rendered page. (b) Actual rendered page.

Chrome 55.0.2852.0

(a) Expected rendered page. (b) Actual rendered page.

Motivation: differential testing is not applicable

Motivation: why not *differential testing*?

Case 1: Support of styles varies across browsers

Rendered Page

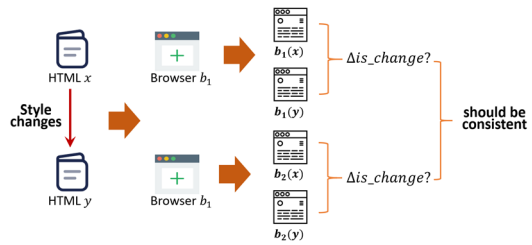
```
<html>
<body>
  <textarea style="content-visibility:
hidden">TEXT</textarea>
    <img src="img.png"
   style="-webkit-box-reflect: below;">
</body>
</html>
```

Rendered Page

content-visibility	√	content-visibility	×
-webkit-box-reflect	√	-webkit-box-reflect	×

Method: visual delta consistency

Basic idea of ***Janus***



Visual Delta Consistency: If all rendering features used in x and y are supported by b_1 and b_2, the visual delta should be consistent.

See the paper for proof

Evaluation: can find real-world bugs

Evaluation

highlight

- Janus found **31** non-crash rendering bugs in mainstream browsers, with **24** confirmed by developers.
- Bugs affect all kinds of rendering-related components.
- Janus only introduces **13%** overhead in the browser fuzzing process.

Browser	Reported	Confirmed	Duplicated	Fixed
Chrome	8	6	2	4
Safari	21	16	3	4
Firefox	2	2	0	0
Total	31	24	5	8

Browser	Affected Component				
	Content	DOM	Forms	Layout	Paint
Chrome	1	0	0	5	2
Safari	1	1	7	4	8
Firefox	1	0	0	1	0
Total	3	1	7	10	10

	Initial DOM Generation	HTML Transformation	Browser Execution	Consistency Checking
Time (ms)	1.35	12.88	1286.45	177.45
Percentage	0.09%	0.87%	87.03%	12.01%