Finding browser bugs, the easy way
Quick WPT introduction

- Shared test suite across all major browser engines.
- Different test kinds:
  - testharness tests.
  - reftests
  - webdriver tests
  - visual / manual tests
Most new tests in Gecko go to WPT

- There’s spec ambiguity.
- They test some browser-specific/non-content-observable functionality.
- Crashtests.
But...

- Sometimes you can do better than a crash test.
- But sometimes there's actually no clear "correct" output.
- Or the correct behavior is already covered.
- Thus WPT gets no coverage for very tricky edge cases 😞
Can we have crashtests?

- RFC for load tests exists: web-platform-tests/rfcs#33
- There’s people still skeptic of their value.
Let’s get some data!

- Local debug builds of Firefox, Chromium, WebKit.
- Extremely crappy test manifest parser / test runner.
- Berlin is cold 😊.
Chromium

• Six different bugs found by running Gecko’s crashtest suite.
  • 1009830, 1009827, 1009825, 1009821, 1009817, 1009806.
• DOM, SVG, layout, media, paint and canvas.
• Mostly but **not only** debug assertion failures.
• Surprisingly no editing crashes.
Gecko

- Two bugs found by running Chromium’s crashtests: 1585226, 1585303.
- One leak caught by a debug assertion (which I fixed myself), one editing bug.
WebKit

• Ran the most tests (both Chromium’s and Gecko’s).
• 20+ bugs found: 202915, 202914, 202913, 202912, 202910, 202909, 202908, 202906, 202905, 202904, 202903, 202902, 202901, 202900, 202899, 202897, 202803, 202804, 202805, 202807, 202809, 202811, 202812.
• Most of them editing, but also SVG, CSS, layout and graphics bugs.
• Several release-build crashes.
# In a nutshell

<table>
<thead>
<tr>
<th>Run / From</th>
<th>Gecko</th>
<th>WebKitGTK+</th>
<th>Chromium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gecko</td>
<td>N/A</td>
<td>TODO</td>
<td>2/0/0</td>
</tr>
<tr>
<td>WebKitGTK+</td>
<td>7/0/1</td>
<td>N/A</td>
<td>16/3/1</td>
</tr>
<tr>
<td>Chromium</td>
<td>6/0/1</td>
<td>TODO</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Follow-up work

- Run WebKit tests on Gecko and Chromium.
- Run the tests with ASAN enabled ( █ ).
- Improve the heuristic to determine whether a Chromium or WebKit test-case is a crashtest.
Conclusions

- I think crashtests would be useful in WPT.
- Browsers are hard.
- Editing is pretty broken.