

Find The Scoreboard Walk-Thru

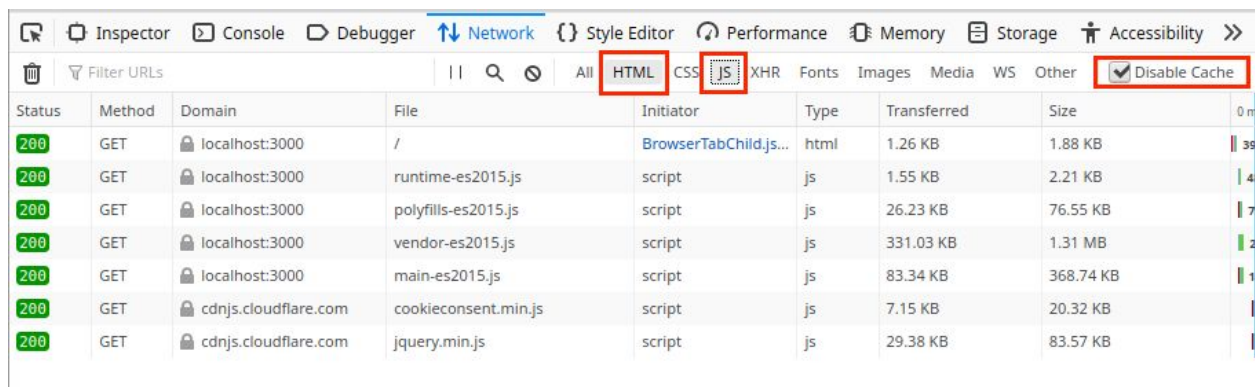
The name of this lab gives a clue: there is a scoreboard somewhere! But it's not something you saw in the initial exploration of the site. How might you find it?

Ideas

1. Check the HTTP traffic (Developer tools, Burp Proxy History) for any references to a scoreboard.
2. Look at the URLs you've seen so far to see what kinds of words and phrases are used.
3. Search for likely strings

Walk-Thru

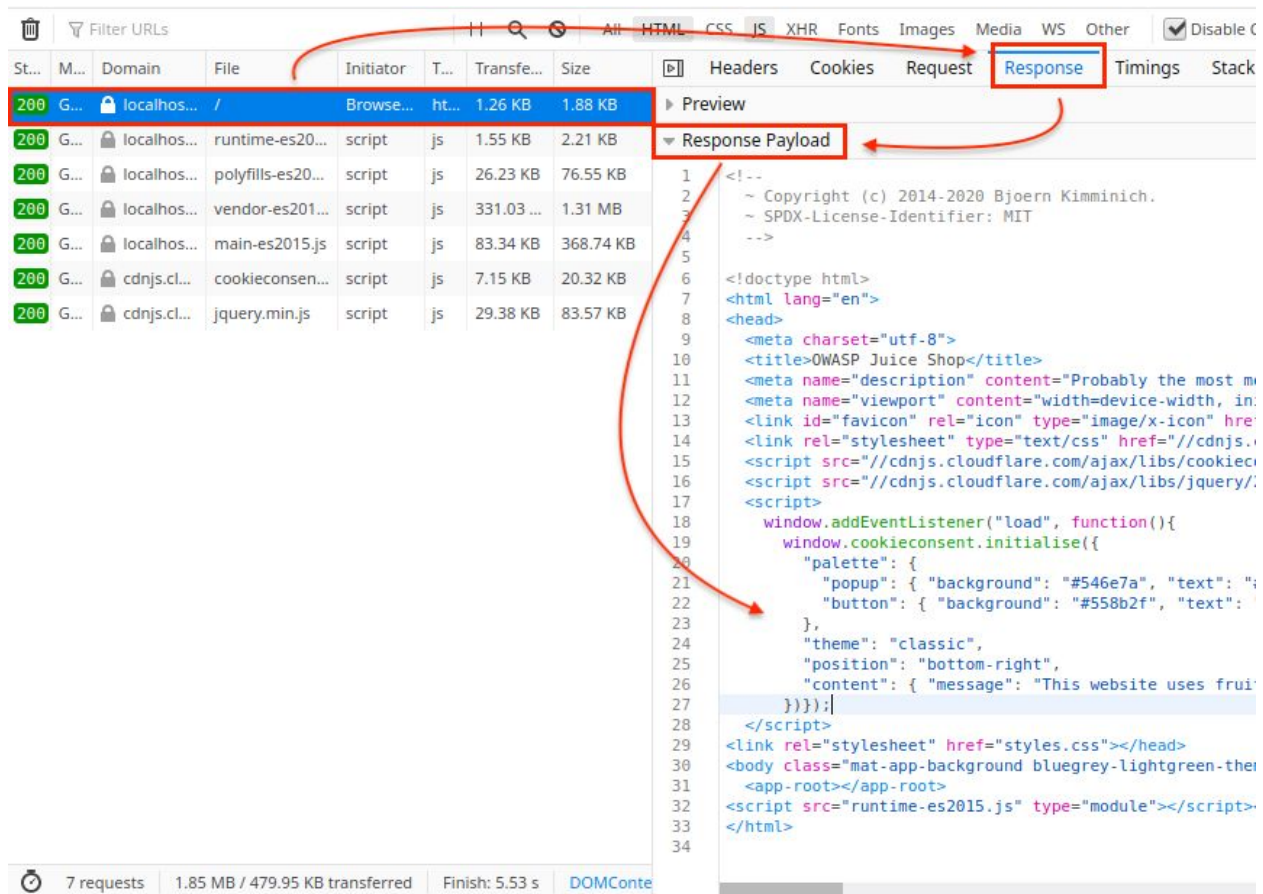
1. Developer Tools > Network. Check "Disable Cache" and reload the page to get full content.
2. Notice the "type" of all the responses. Focus on "html" and "js" items by clicking "HTML" and "JS" in the filter bar.



Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 m
200	GET	localhost:3000	/	BrowserTabChild.js...	html	1.26 KB	1.88 KB	39
200	GET	localhost:3000	runtime-es2015.js	script	js	1.55 KB	2.21 KB	4
200	GET	localhost:3000	polyfills-es2015.js	script	js	26.23 KB	76.55 KB	7
200	GET	localhost:3000	vendor-es2015.js	script	js	331.03 KB	1.31 MB	2
200	GET	localhost:3000	main-es2015.js	script	js	83.34 KB	368.74 KB	1
200	GET	cdnjs.cloudflare.com	cookieconsent.min.js	script	js	7.15 KB	20.32 KB	
200	GET	cdnjs.cloudflare.com	jquery.min.js	script	js	29.38 KB	83.57 KB	

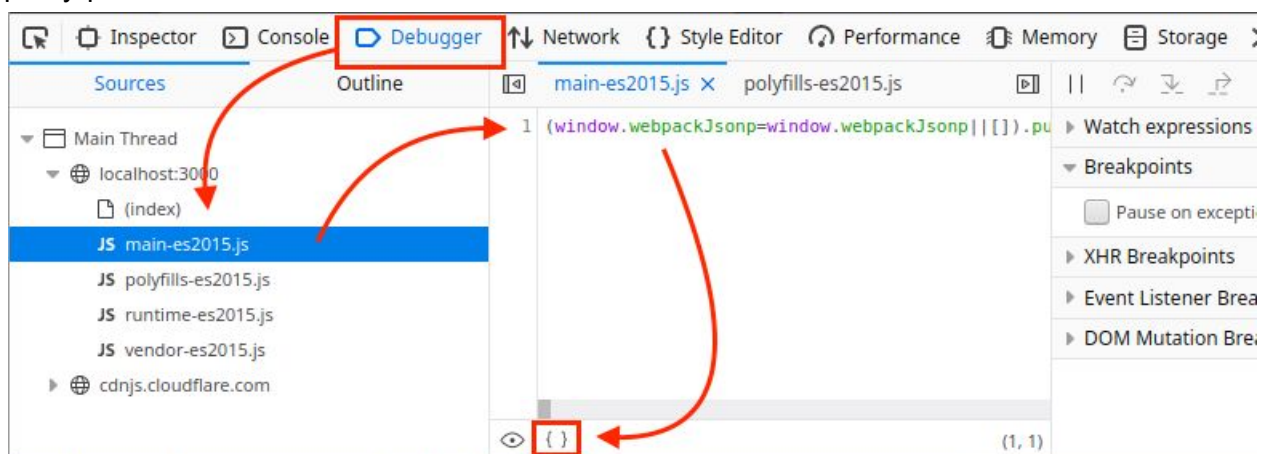
Developer Tools, Network Tab Settings

3. Check the only HTML response you see for any obvious menu bars or other link targets (HTML "A" tags). Notice the response "preview" is blank, and the "response payload" is pretty small - this app is rendered by client-side Javascript, so there's not much to see here.



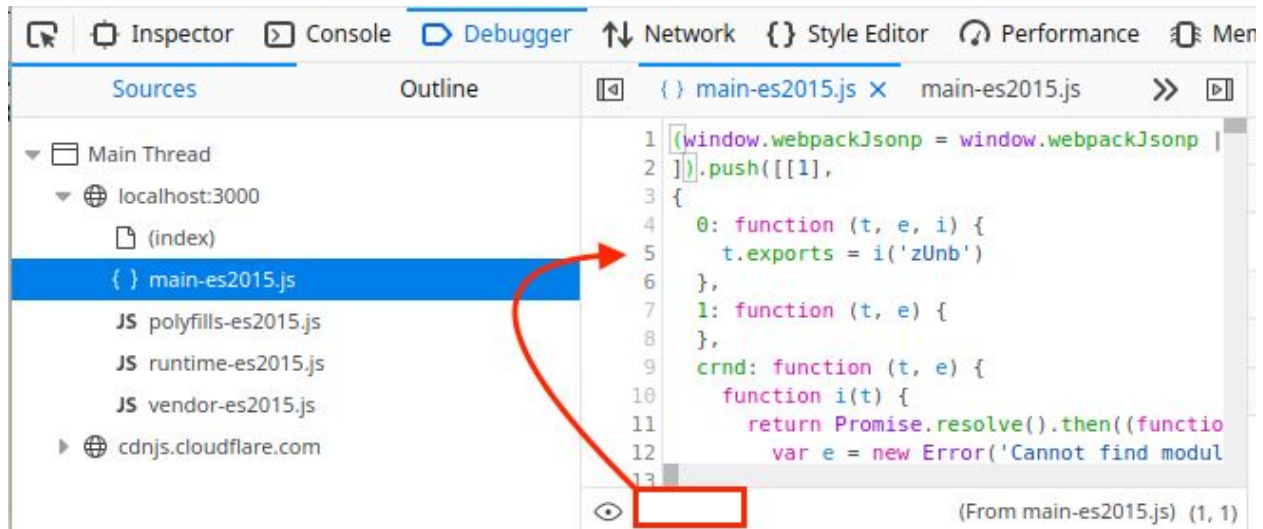
Viewing the Response Payload

- Look at the Javascript files. The one with "main" in its name seems promising. But when you click on it from the Network pane, it's just one long line, so try it in the Debugger pane instead.
- In the debugger pane, it's still one long line, but there's a '{}' button at the bottom to pretty-print it:



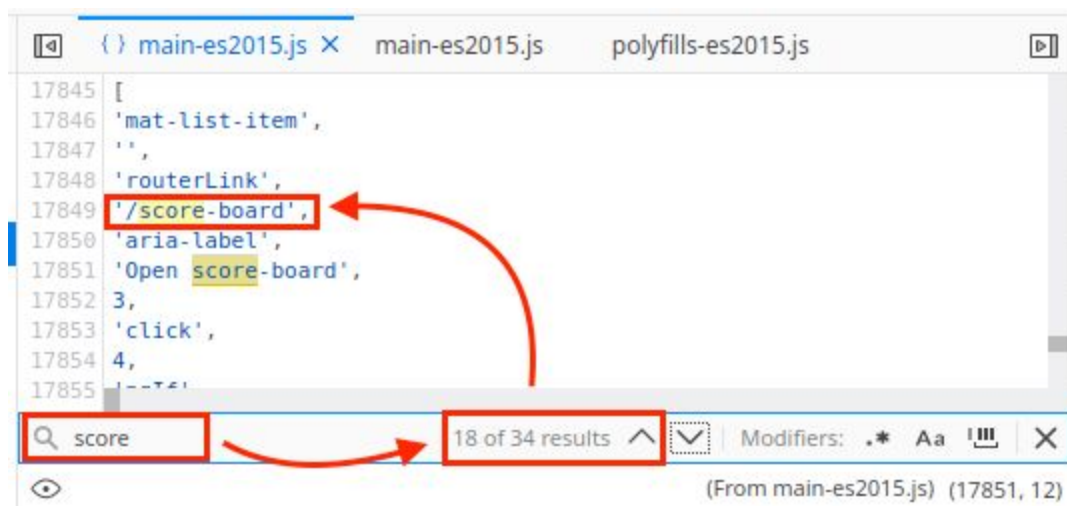
Viewing the "main" Javascript File

Click the braces and ...



Built-in Javascript Beautifier!

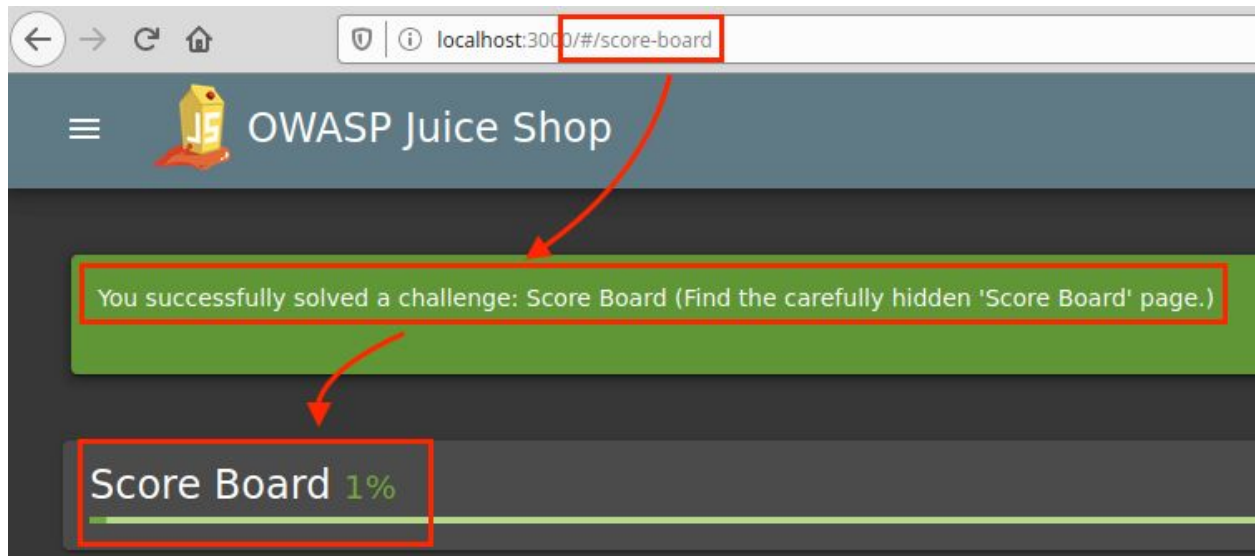
6. search (Ctrl-F or Ctrl-Shift F) after clicking in the window showing the Javascript) for "score"



RouterLink to "score-board" Resource

7. In your browser, type `"/#/score-board"` as the path in the address bar so that the URL is `http://localhost:3000/#/score-board`

8. Win!



Alternative win:

Visit <http://localhost:3000/.well-known/security.txt>

See the scoreboard mentioned right there.

