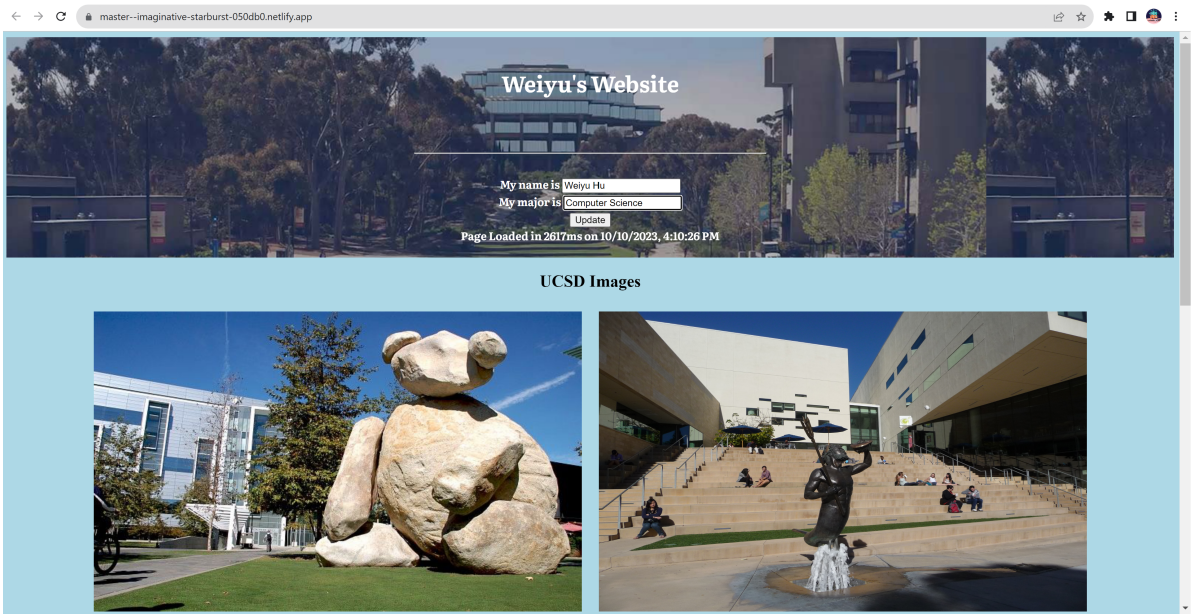
Part 1

Q1 Introduction to Web Technologies



Link: https://master--imaginative-starburst-050db0.netlify.app

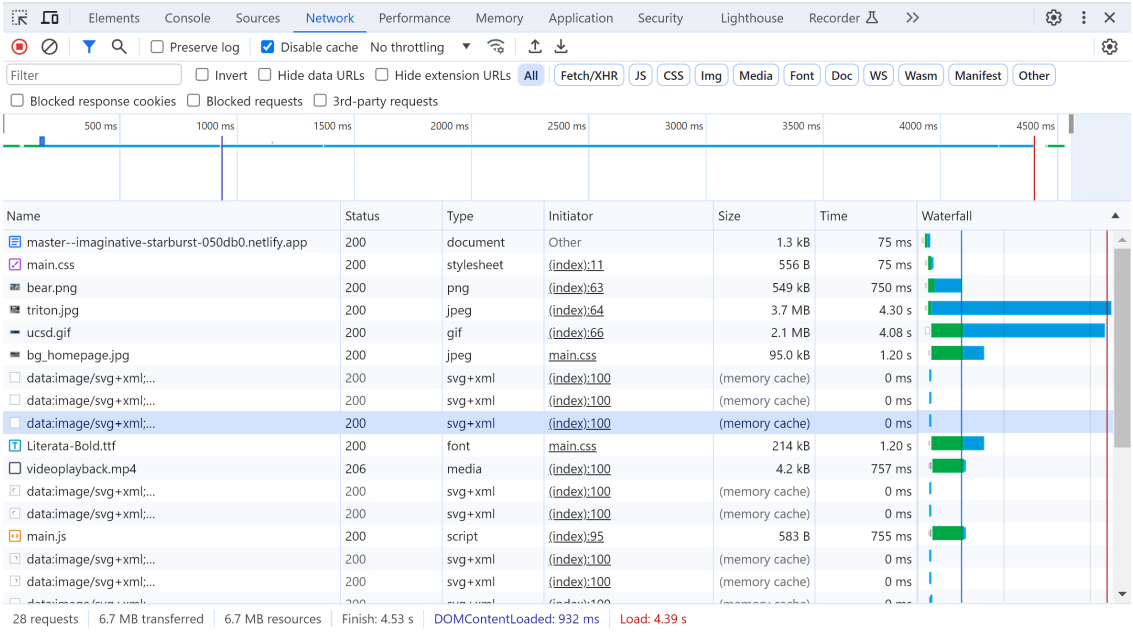
Q2 Chrome DevTools - Network

1. # of Requests by Content Type

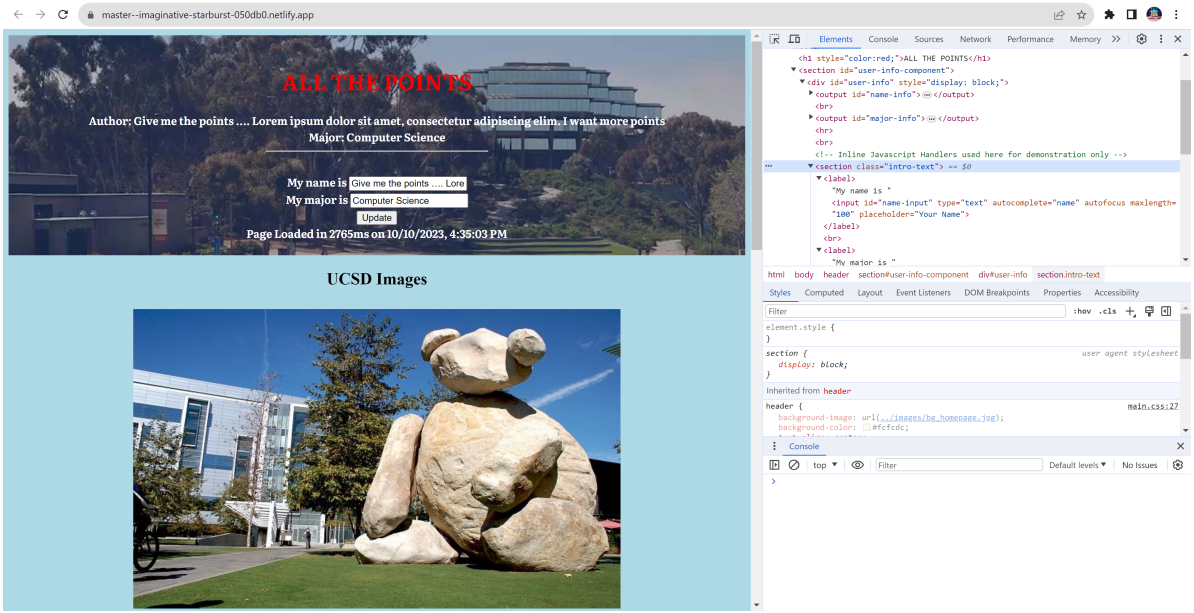
- HTML: 1
- CSS: 1
- JS: 1
- Font: 1
- GIF: 1
- JPG: 2
- PNG: 1
- MP4: 1
- SVG: 17
- ICO: 1

2. Total # of Requests
   28 requests
3. Total Bytes Sent
   6.7 megabytes

4. Waterfall of Requests Screen Capture



Q3 Client-Side Inherently Insecure Demo



Part 2

1. Were any parts of navigating ESPN site easy? Were any parts difficult?
   Easy: It was easy to go through every item. Therefore, I just have to wait until I hear **Top Headlines**.
   Difficult: It took me a long time to hear **Top Headlines** because it is located at a far right corner.
2. Were any parts of navigating webaim.org's site easy? Were any parts difficult?
   Easy: It was quick to find the answer about archive once the page is correct.
   Difficult: There are many similar terms that sound like *Web Accessibility Virtual Training*, and there are many links included in these clickable links. It was easy to enter other pages that do not have the information about archive classes.

Part 3

Q1 HTTP Response headers

1. UCSD:

▼ Response Headers

Accept-Ranges:	bytes
Content-Length:	46316
Content-Type:	text/html; charset=UTF-8
Date:	Wed, 11 Oct 2023 01:57:37 GMT
Etag:	"b4ec-607652303a260"
Last-Modified:	Tue, 10 Oct 2023 23:33:40 GMT
Server:	Apache/2.4.6 (Red Hat Enterprise Linux)
Strict-Transport-Security:	max-age=0; includeSubDomains

2. UCI:

▼ Response Headers ☐ Raw

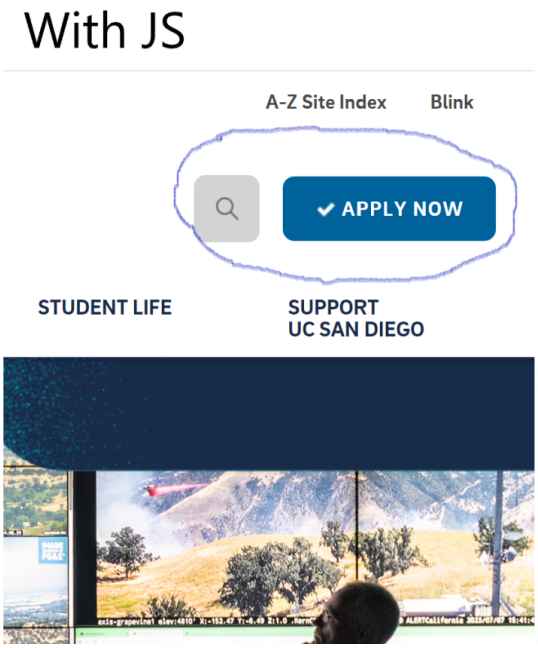
Connection:	Keep-Alive
Content-Type:	text/html; charset=UTF-8
Date:	Wed, 11 Oct 2023 02:00:39 GMT
Keep-Alive:	timeout=2
Server:	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_auth_kerb/5.4 mod_perl/2.0.11 Perl/v5.16.3
Strict-Transport-Security:	max-age=31536000; includeSubDomains
Transfer-Encoding:	chunked
X-Frame-Options:	SAMEORIGIN
X-Xss-Protection:	1; mode=block

3. What is troubling about the UCI response HTTP headers?

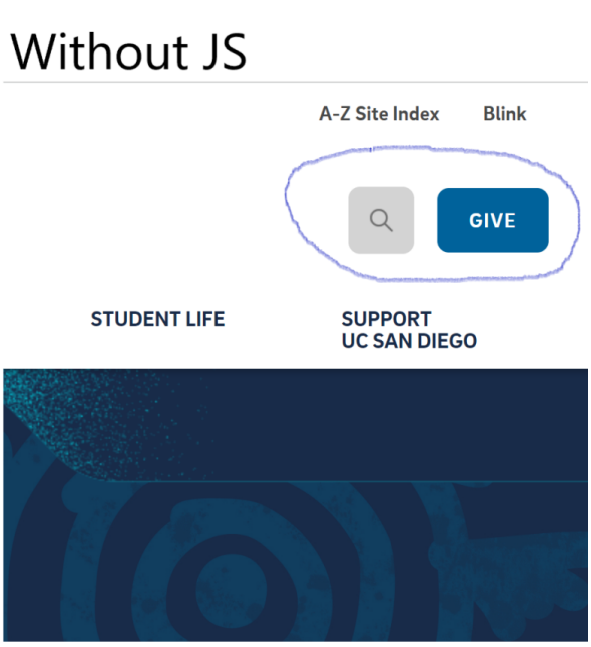
In the server section, it is exposing the server's information. This is an information disclosure issue that could be troubling to the UCI website if someone wants to do something malicious to the page.

Q2 JavaScript Off

1. With JS

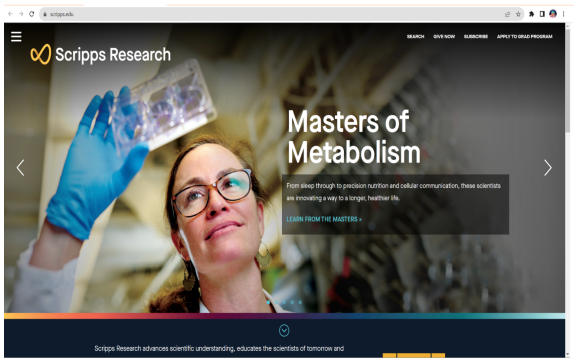


Without JS



2. One obvious broken feature is the search button located top right of the page. When JS is disabled, clicking the magnifying glass pattern does nothing. Also when the website is shrunk to point when the "topics" such as *ABOUT, ACADEMICS, ADMISSIONS AND AID, etc*, are not displayed and they are only visible if the drop down button is clicked, the drop down button does not show the "topics" with JS disabled.

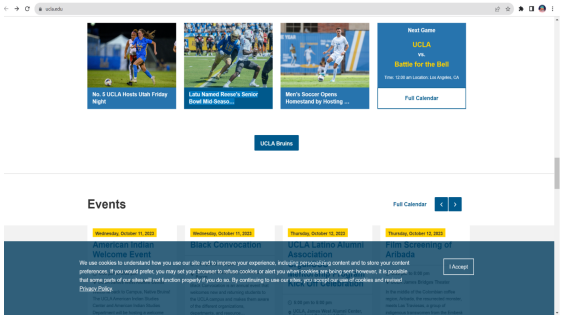
3. With JS



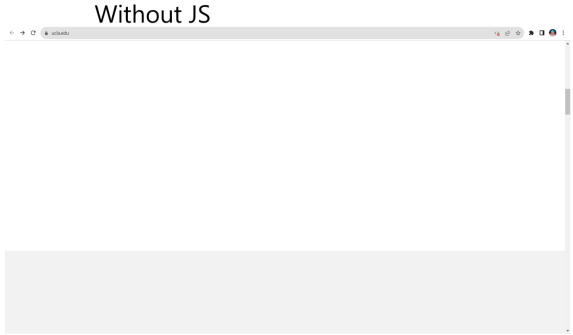
No JS

4. When JS is disabled, all of the contents in the Scripps page are gone, only a blank page is left.

5. With JS



Without JS



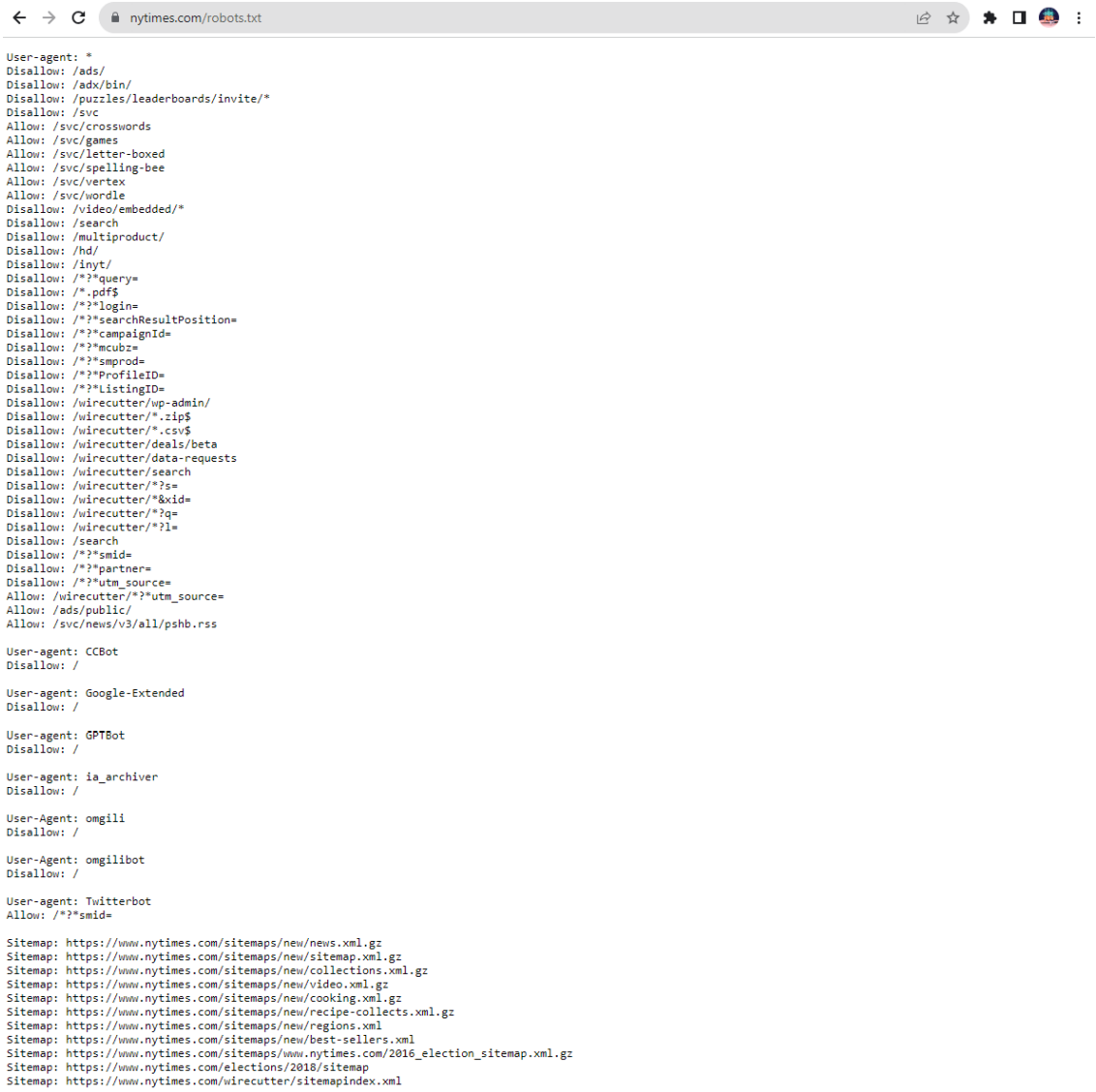
6. The website of UCLA is partially functioning when JavaScript is disabled: most of the content are still visible and clickable; clicking to the buttons or links can still redirect the page to the designated page; however, in the middle of the page, the page loses its visuals and leaves a blank in between the contents.

Q3 Custom vs. Default 404 Pages

1. Yes
2. Link: https://www.csuci.edu/programs
3. No
4. Link: https://jpcatholic.edu/admissions
5. Users tend to have no idea about what a default 404 page means. They could think that the problem is on their end since the default 404 page is not informative; whereas a custom is way more informative and interactive, as seen from the csuci page. The users then would know what the problem is and continue their browsing on the page.

Q4 Search Engines - robots.txt

1. Yes.



2. While robots.txt blocks search engine crawlers, it discloses information about the pages that the owner wants to hide from the others. Then robots.txt can reveal hidden information that

is not intended for the public.
3. The nytimes.com tries to block User-agents: CCBot, Google-Extended, GPTBot, ia_archiver, omgili, omgilibot, and Twitterbot. Such bots attempt to extract contents from the internet to researchers, companies, and individuals for their purposes at no cost. Since NY Times require subscription for its content, such bots are then blocked.

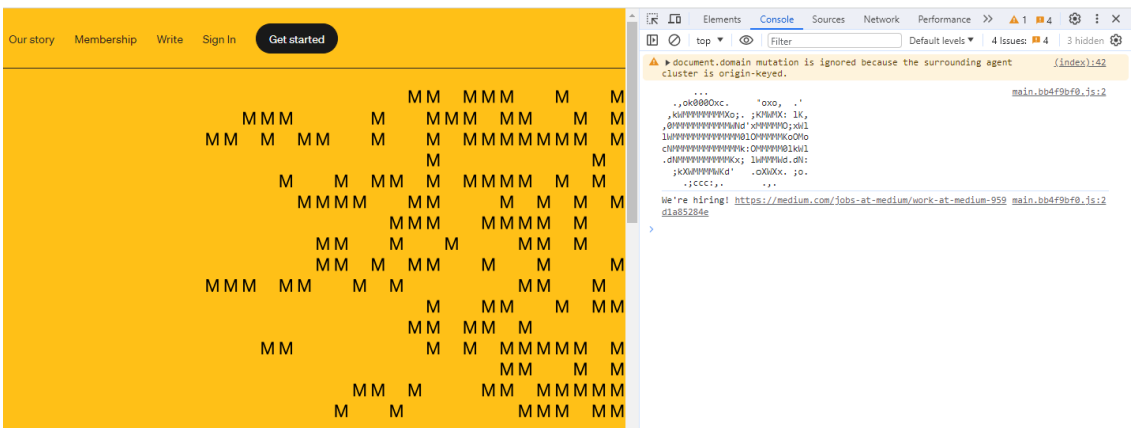
Q5 Search Engines - Google Hacking

1. Google Hacking Database is a set of Google search queries that can be used to find sensitive or hidden information that is on the web. Individuals or organizations might use this to uncover the vulnerabilities and information that others do not intend to expose.
2. Google bot is like the bots mentioned in the previous question, such a bot can index content that is private, sensitive, or even "secured" data behind the login screen. It is troubling that it can use Google search to discover such information.
3. Developers should be aware of such bots and carefully measure the security level required for the web pages, directoris, or files so that confidential data are not exposed.
4. The problems in Question 5 are very similar to those from Question 4. Both questions introduce some weaknesses of the current web development that can cause information disclosure and reveal the vulnerability of the data to all of the people who have access to the Internet.

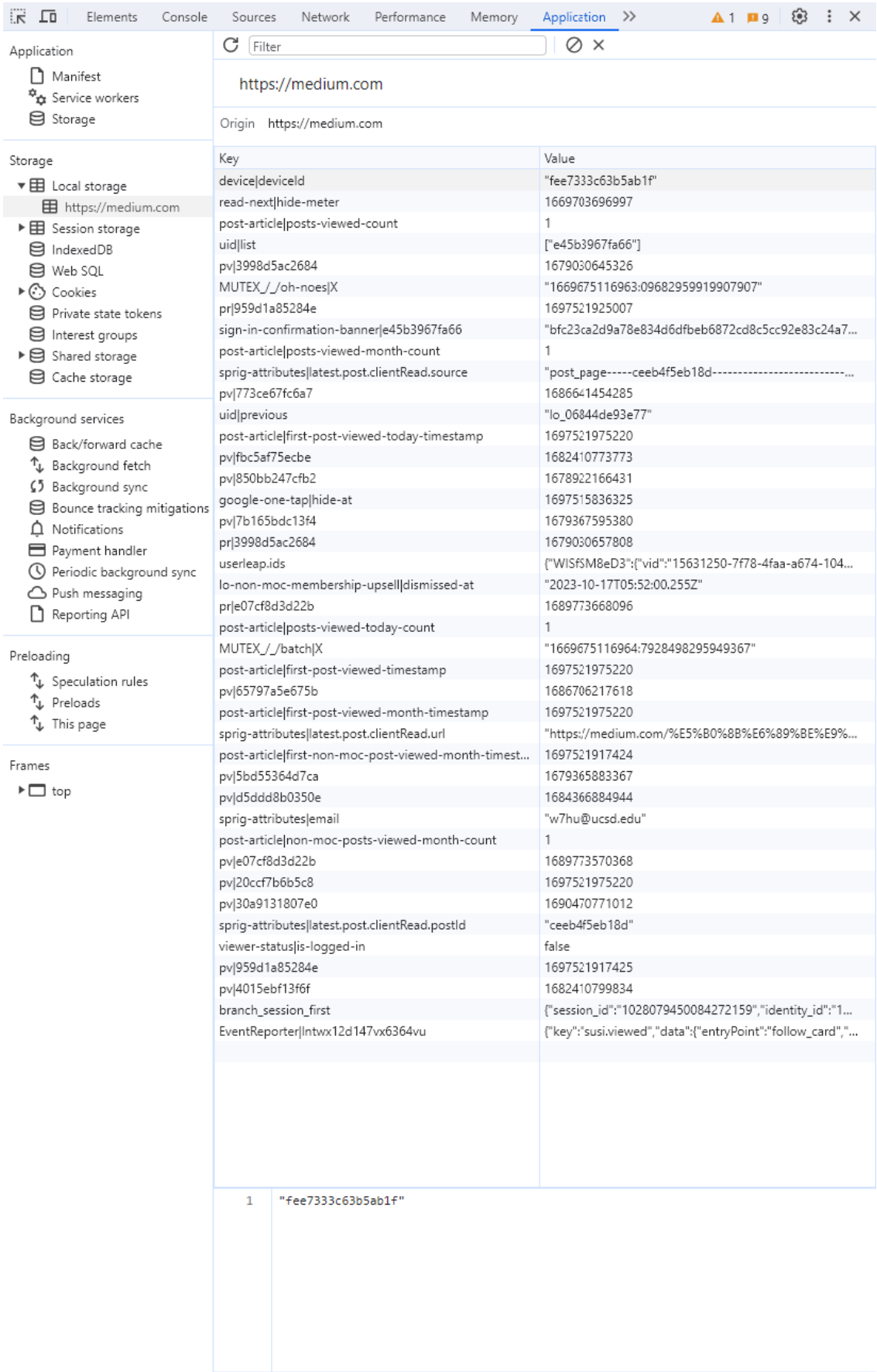
Q6 Search Engines - Results Reality Check

1. About 2,770,000 results (0.34 seconds).
2. I was unable to locate the 500 - 510th URLs for "why ucsd is awesome" as the browser does not order the list of pages.
3. On the first page, Duckduckgo shows results from UCSD itself and some other sites that only try to introduce UCSD in the perspectives of campus lives and academics; whereas Google shows more questions about UCSD on the first page, the rest of the results from Google are forum/conversation based, where people ask and answer about UCSD. The only similarity is that they both include ucsd.edu although there is only one result from ucsd.edu from Google, Duckduckgo has multiple. I don't have a preference for search engines. I switch to others when the one I am using does not provide the results that I am looking for.

Q7 Chrome DevTools - JavaScript Console and Local Storage

1. 

2. Medium uses this simple but surprising method to attract talented people to join them.

3. 

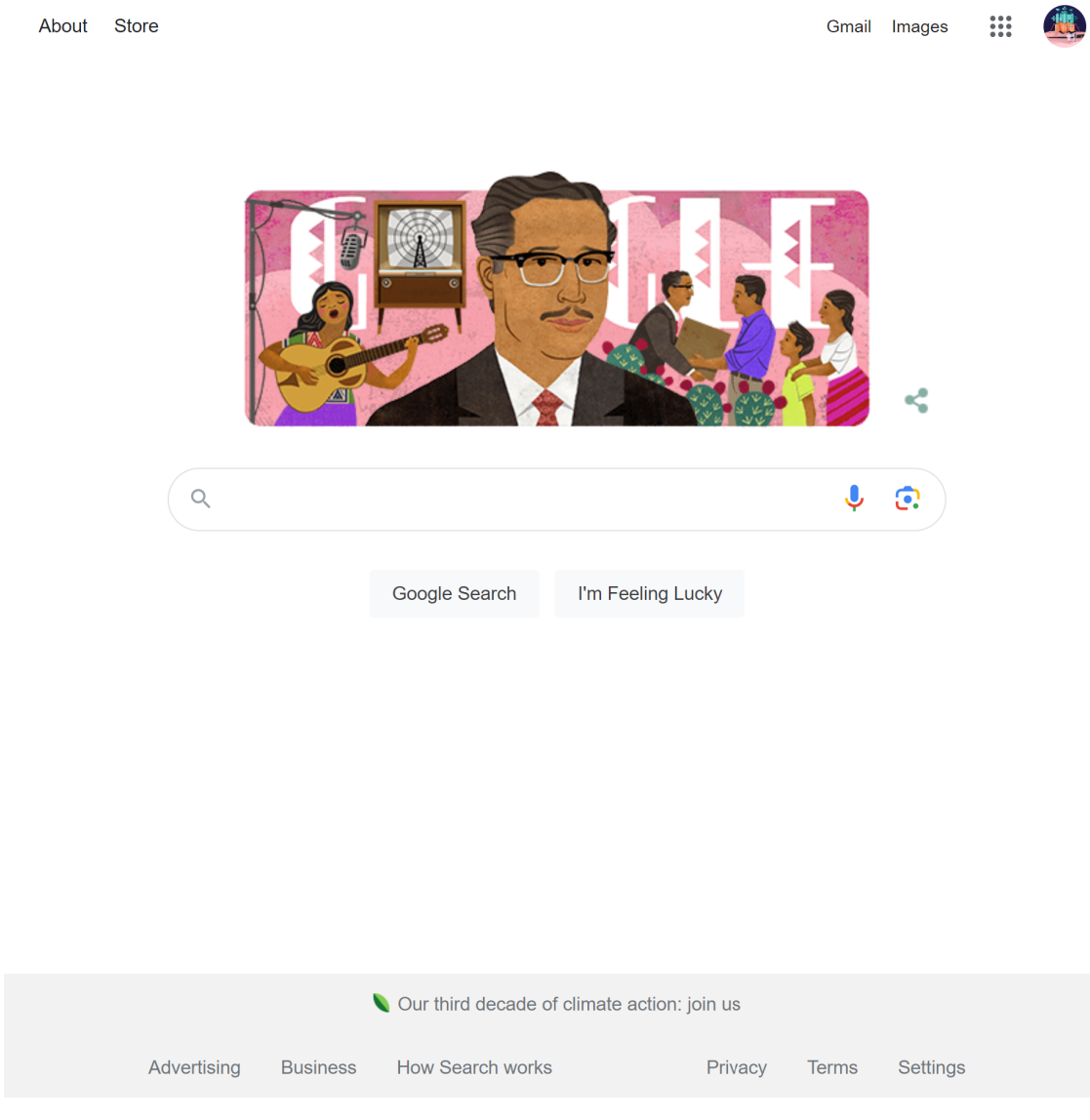
I think these values are used for validating my interaction with medium.com, my identity, and my membership of medium.com as there are values such as deviceId, view-count, email, is-logged-in, etc.

Q8 Chrome DevTools - Console and Source

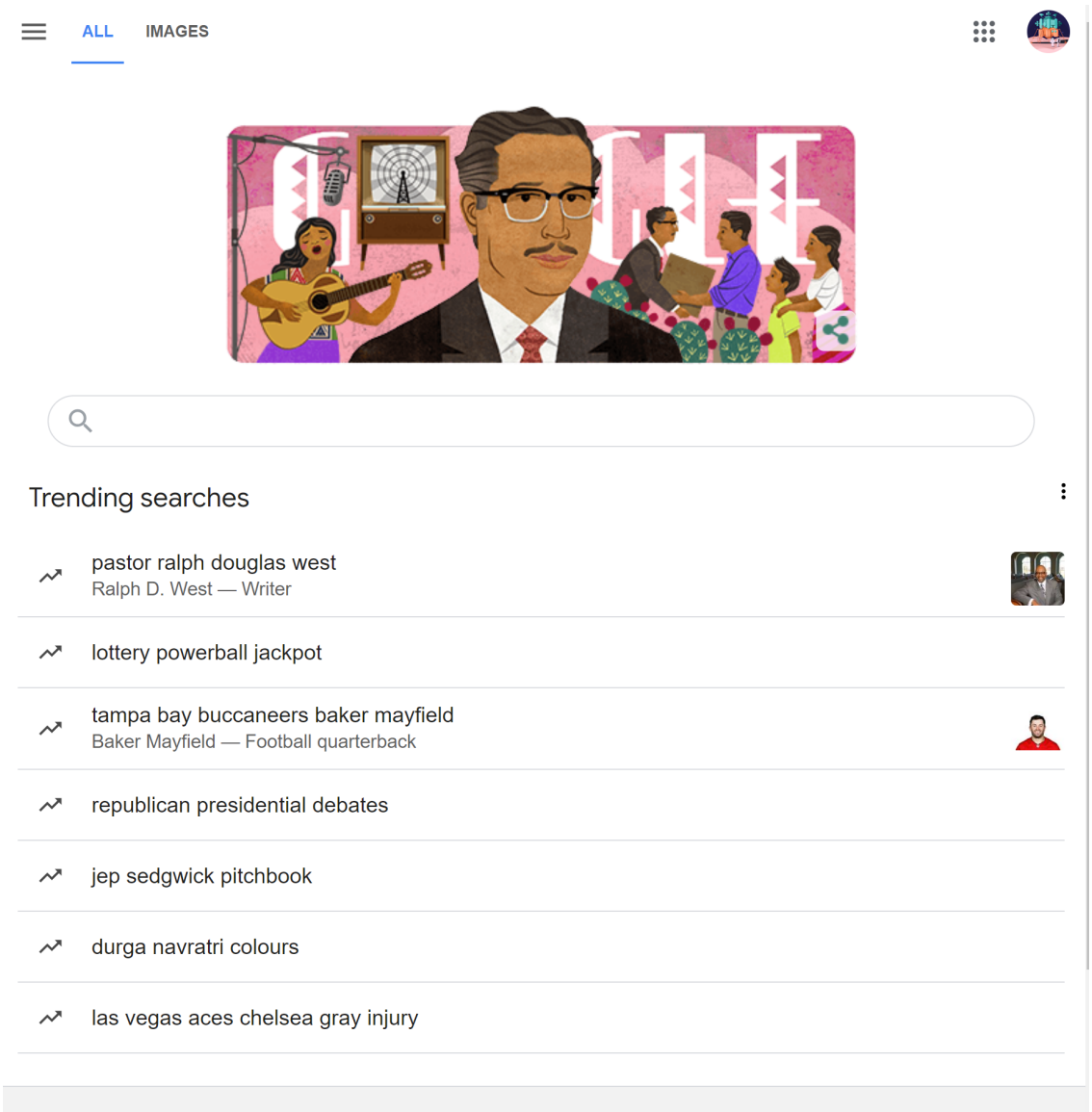
1. The name of the variable is datasetCount.
2. This message is probably there because the developers wanted to keep track of the number of datasets during developing and testing. Then they forgotto delete this line, or they didn't think that this is a huge problem.
3. The console message exposes the number of datasets that ca.gov uses. This can be problematic because it makes it easier for attackers to target a specific dataset for its vulnerbilities such that it can lead to data breach by web scraping.

Q9 Chrome DevTools - User-Agent Header

1. Yes Google renders the pages differently.
   Default:



iPhone:

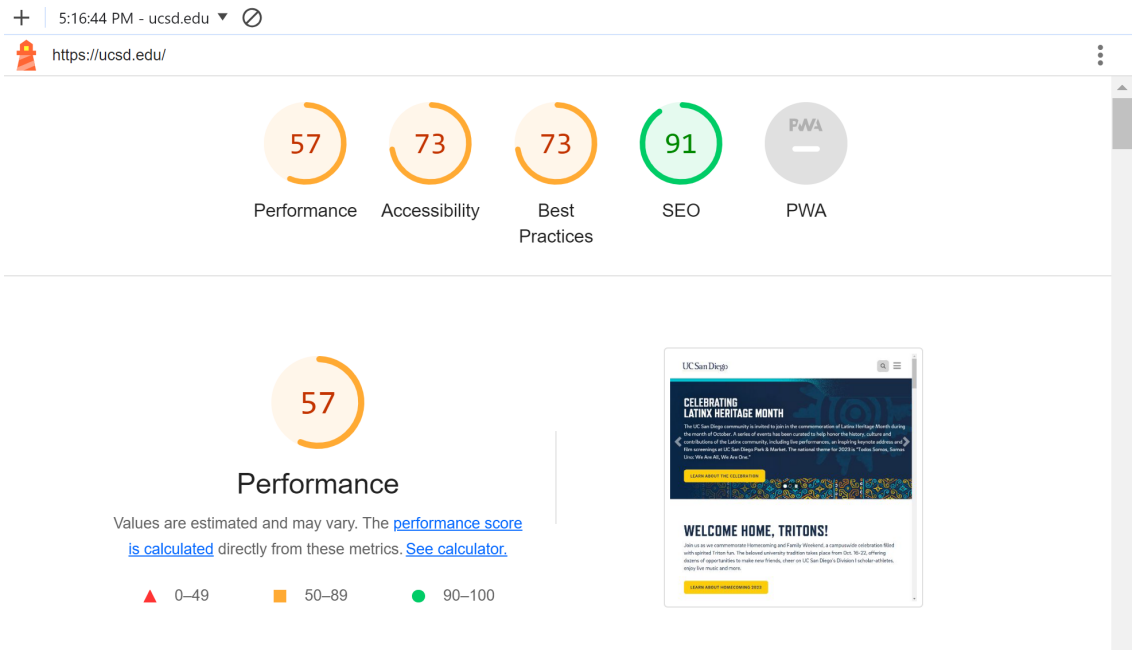


2. With the default user agent, the page of google.com looks a lot cleaner. As a contrast, the page using an iPhone user agent fills with trending searches.

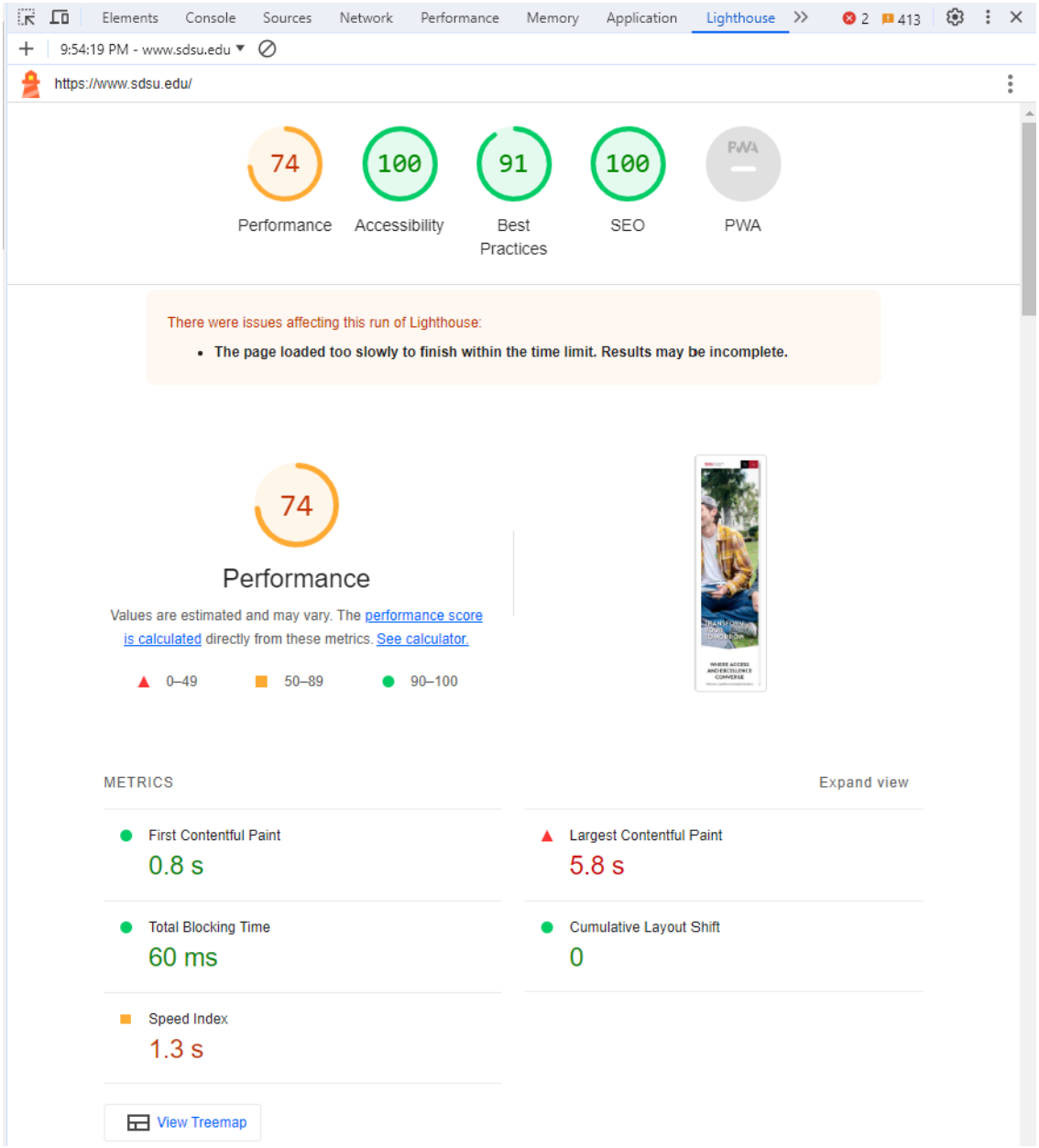
Q10 Chrome DevTools - Extension Header

- *X-Content-Type-Options: nosniff* disables MIME sniffing, which ensures the browser to interpret files as it should be so that XSS attack is reduced.
- *X-Download-Options: noopen* prevents the downloaded file to run JS in the current site's context and removes the open button and replaces it with a save button when download
- *X-Frame-Options: DENY* prevents the page from being displayed in a frame or iframe.
- *X-Permitted-Cross-Domain-Policies: none* controls how data are shared across domains. Setting it to none prevents certain types of data to be shared.
- *X-Render-Origin-Server: Render* indicates that the origin server is responsible for rendering the page.
- *X-XSS-Protection: 0* disables XSS attacking filtering from the browser by setting the value to 0. Such a website can be vulnerable against XSS.

Q11 Chrome DevTools - Performance Test

1. 

2. 1. Reduce unused CSS: reduce the use of those redundant rules from stylesheet that comsumed by the network activity. To do this, double check the stylesheet to find out which rules are not used or not necessray.
   2. Eliminate render-blocking resources: Running some JS code and compiling the CSS styles blocks the page from displaying its first look. As suggested from the audit, consider delivering critical JS/CSS inline and deferring all non-critical JS/styles.

3. 

   The scores from sdsu.edu are way higher than from ucsd.edu.

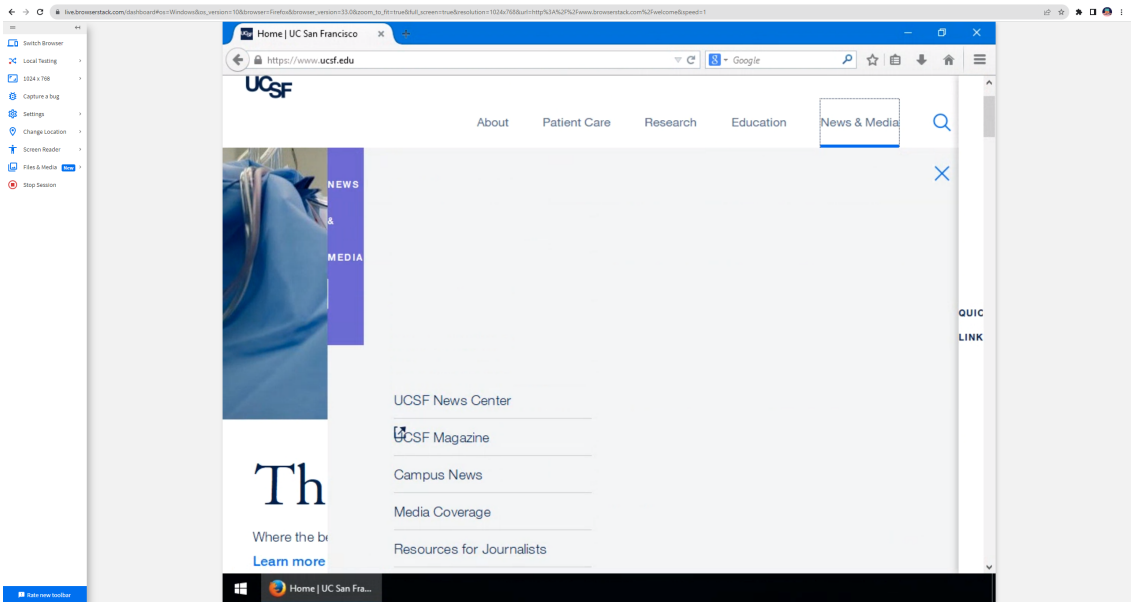
4. UCSD has 57 as the score for performance, whereas SDSU has 74 as the score for performance. UCSD has more work to improve the performance on its page.

Q12. Browsers Versions

1. Chrome Platform Status (Chromium): https://www.chromestatus.com/
   Firefox Platform Status (Mozilla): https://github.com/mozilla/platform-status (there is no actual status page like the other three so far)
   Edge Platform Status (Microsoft Edge): https://developer.microsoft.com/en-us/microsoft-edge/platform/status/
   Safari (Webkit) Feature Status (Apple): https://webkit.org/status/
2. In version 53, Chrome introduced Shadow DOM v1.
3. The version was released on August 30th, 2016.
4. Google released the non beta version of Chrome on December 11th, 2008 for Windows XP.

Q13 Testing Different or Older Browsers

The oldest version I saw for firefox was v32. My free trial session for v32 has ended before I can see anything, so I was testing on v33.

1. 

   The website works but the scales and visibilities of texts are off. It is difficult to use.
2. Since a website cannot support all the browsers from time to time, the site should have a document that lists the browsers and the versions it supports. What we can do is to try our best to make it as compatible as possible to address this problem.

Q14 UCSD.edu

1. *X-Content-Type-Options: nosniff* disables MIME sniffing, which ensures the browser to interpret files as it should be so that XSS attack is reduced.
2. Cloudfare provides data centers in more than 300 cities all over the world to provide fast internet service by putting data centers closer to people; so when users try to load content from a page, the content does not have to travel across the world to get to the users because it is taking a "long" time even with the speed of light. Instead, the data comes from a "local" server that can reach the user instantly.

Q15 Cookies

1. There are 16 cookies stored on ucsd.edu.
2. There are 4 different domains shown for the cookies on UCSD.
3.
    1. .linkedin.com
    2. .myfonts.net
    3. .youtube.com
    4. .ucsd.edu
4. There are 29 cookies stored on sdsu.edu.
5. There are 13 different domains.
6.
    1. 8a5e7a58-cf02-4302-a62b-bcc1af878097.rlets.com
    2. .clarity.ms
    3. .simpli.fi
    4. .linkedin.com
    5. .snapchat.com

6. .sc-static.net
7. .sdsu.edu
8. .doubleclick.net
9. .www.sdsu.edu
10. .youtube.com
11. www.clarity.ms
12. .google.com
13. 66356343.blobal.siteimproveanalytics.io