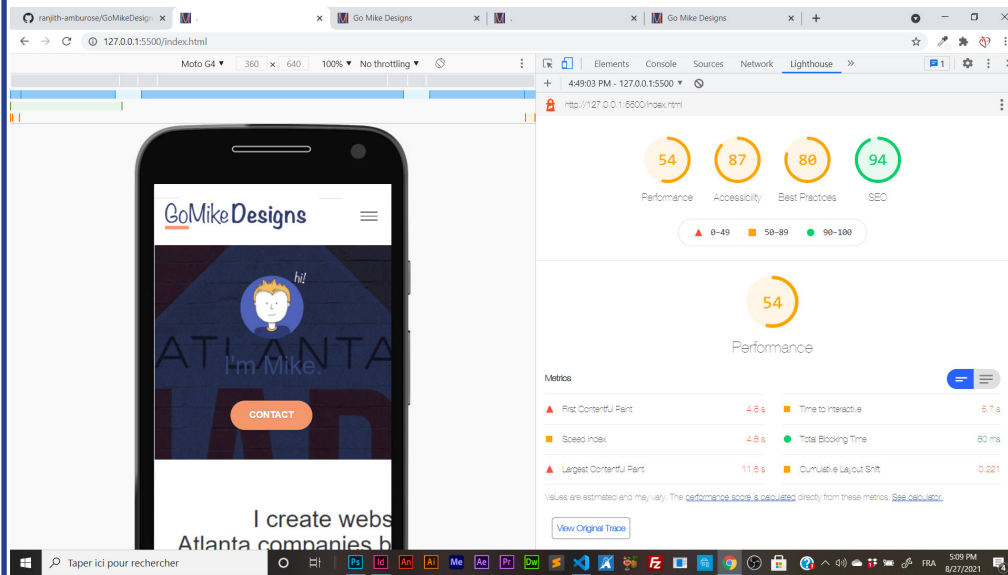
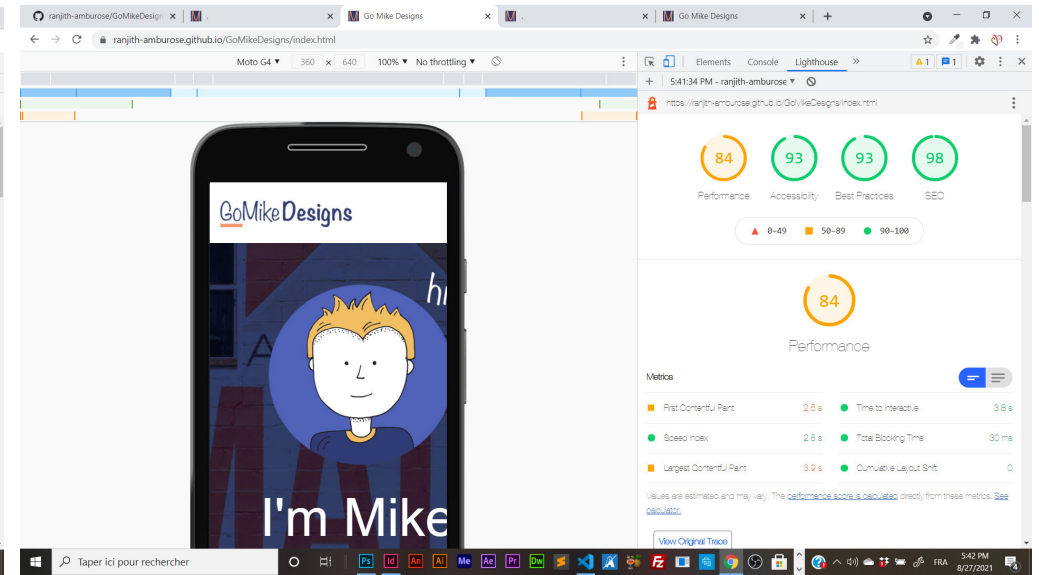


GO MIKE DESIGNS

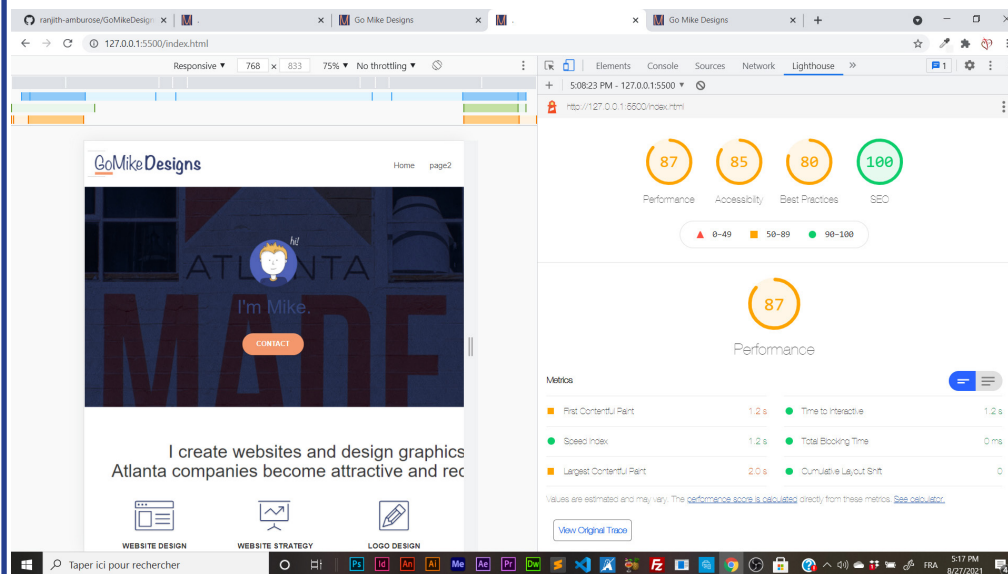
MOBILE VERSION BEFORE



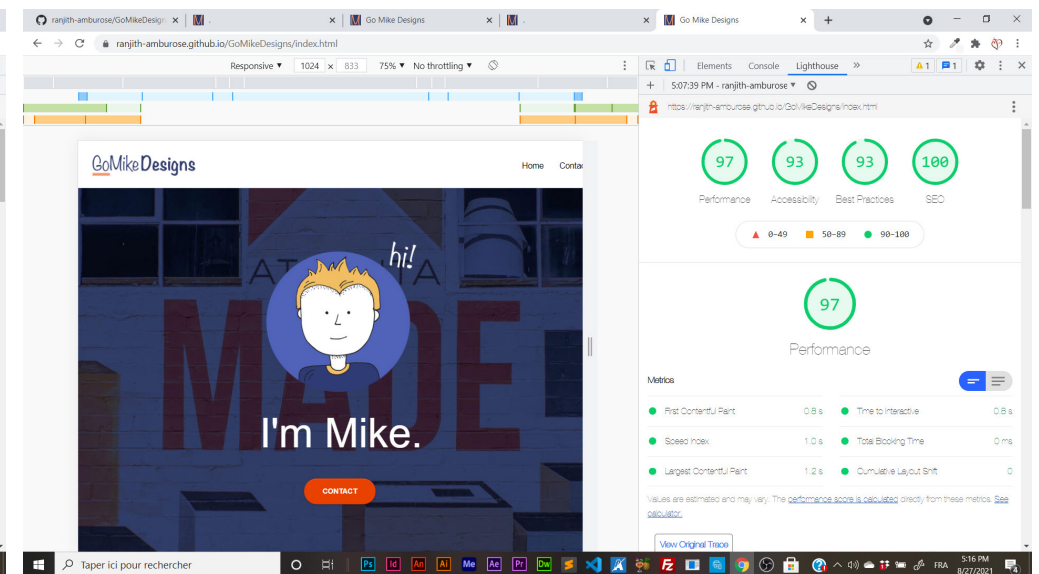
MOBILE VERSION AFTER



DESKTOP VERSION BEFORE



DESKTOP VERSION AFTER



GO MIKE DESIGNS

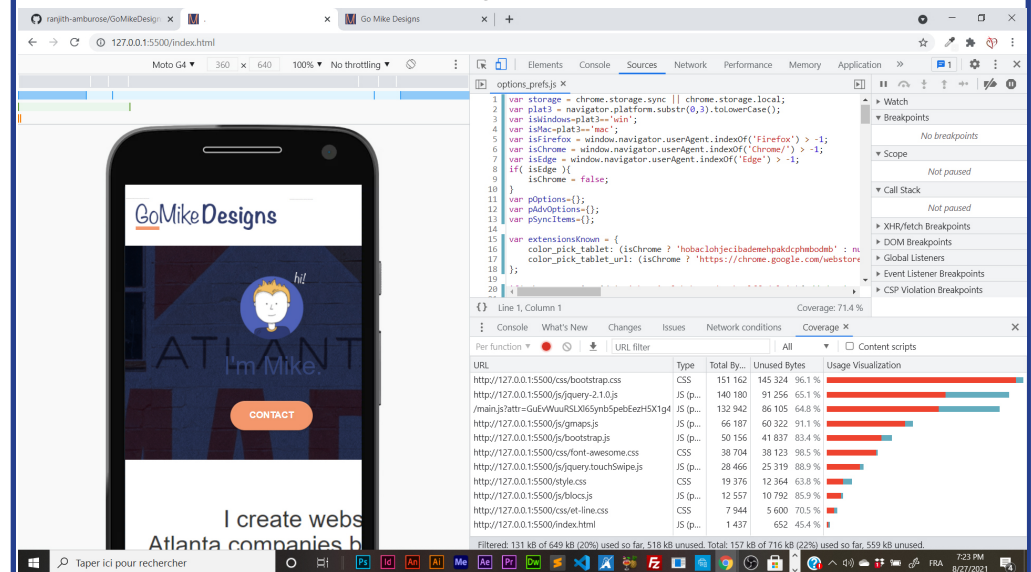
BEFORE

1. <html> element does not have a valid value for its [lang] attribute.
2. Properly size images.
3. Eliminate render-blocking resources

4. Preload key request

AFTER

1. <html> [lang] attribute was default. I have fixed to <html lang=en></html>. This information helps search engines return language specific results
2. Actual Image size and the rendering image size had larger difference which fails the audit and slows down the page load time. Which has been corrected to the required rendering image size and the i have also reduced the file size using <https://tinypng.com/>
3. To identify the critical render-blocking, i used Coverage Tab in Chrome Dev Tools . To eliminate render-blocking scripts i used 'async' so that the scripts can be executed afte the page has been loaded.



4. Preloading requests can make the web pages load faster.
I have declared the preload links in the HTML to instruct the browser to download the key resources as soon as possible.

GO MIKE DESIGNS

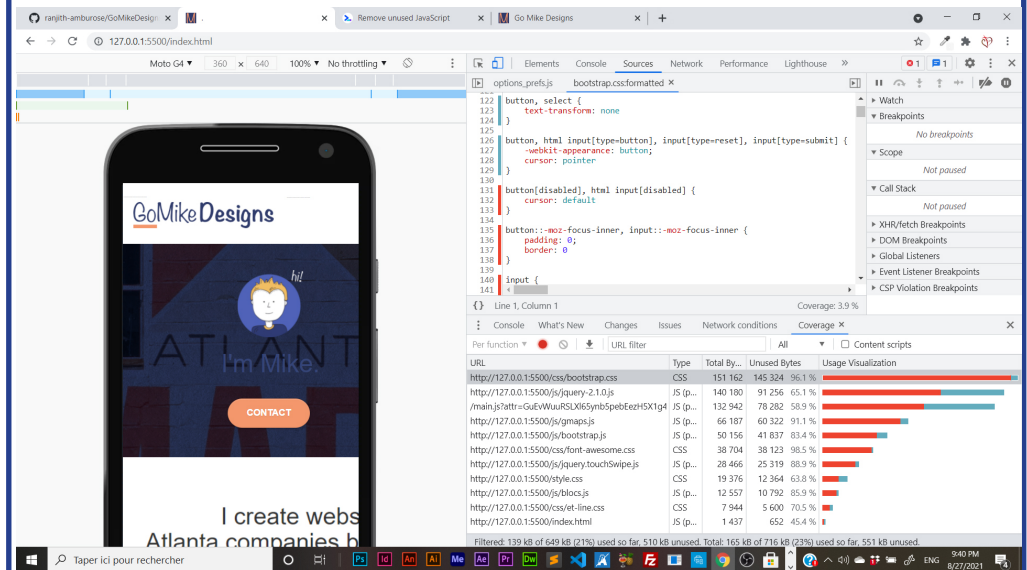
5. Reduce unused JavaScript & CSS

6. Ensure text remains visible during webfont load

7. Image elements do not have explicit width and height

8. Does not use HTTPS

5. I detected unused JS code line-by-line by using coverage tab in Chrome Dev Tools and deleted the unused JS codes.



6. To avoid showing invisible text while custom font loads is to temporarily show a system font. By including 'font-display:swap;' in my @font-face style.

7. Images without dimensions, width and height attributes has failed the audit. I have determined the width and the height attributes for the browser to know the aspect ratio to calculate and reserve sufficient space for the images.

8. All websites should be protected with HTTPS, even ones that don't handle sensitive data. HTTPS prevents intruders from tampering with or passively listening in on the communications between your site and your users. We should consider to host our site on a CDN. Most CDNs are secure by default.

GO MIKE DESIGNS

9. Includes front-end JavaScript libraries with known security vulnerabilities

10. Tap targets are not sized appropriately

9. I have updated the released newer version libraries to fix the vulnerability.

10. To fix the tap targets, i have increased the size of tap targets and also increased the space between the tap targets.