IT314 SOFTWARE ENGINEERING

Project : Naive Baker

Prof. : Saurabh Tiwari

Group : 13

Testing : Non Functional Requirements TESTING

Done By : Dalwadi Devansh(202101184)

Maru utsav(202101195)

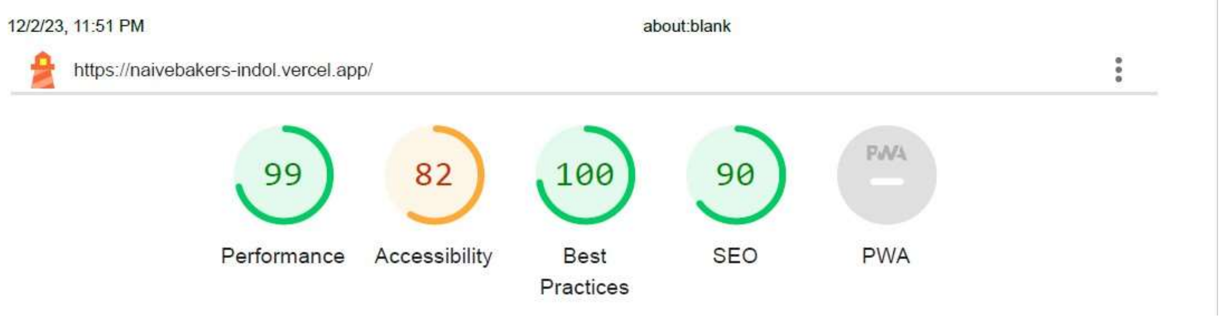
Maintainability:

- Naivebaker, which uses django ,vercel, railway for the backend and JS and CSS for the front, undergoes maintainability testing to make sure the system is simple to update and enhance in the future.
- The code has been reviewed to ensure that it complies with coding standards and is simple to read and understand. We have thorough documentation outlining every step of the process, and the system has undergone testing to ensure it can withstand modifications without malfunctioning. Furthermore, the code may be modified without causing issues in other areas of the system, and the system is designed to introduce new features with ease. All in all, we've made sure that Common Ground is robust and easily extensible without generating problems.

Ease of Use:

Tested with: https://www.webpagetest.org/

Lighthouse Report:

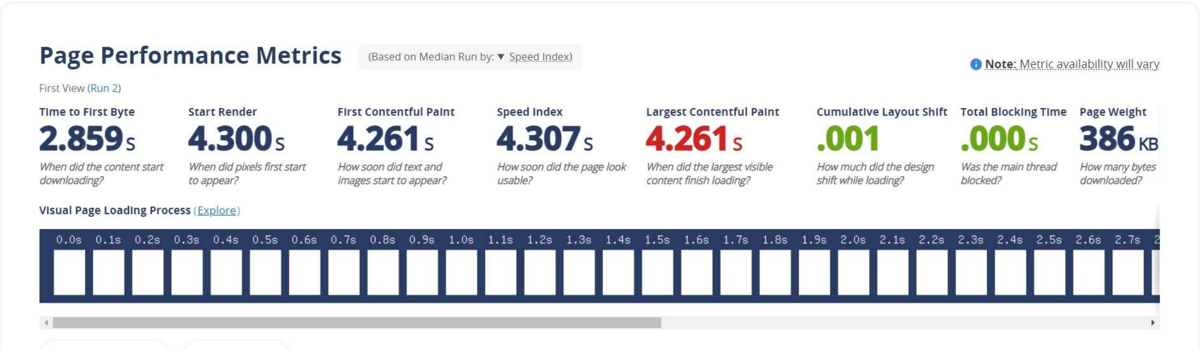


12/2/23, 11:51 PM about:blank

https://naivebakers-indol.vercel.app/

Performance	Accessibility	Best Practices	SEO	PWA
99	82	100	90	–

Performance Report:



Page Performance Metrics (Based on Median Run by: ▼ Speed Index)

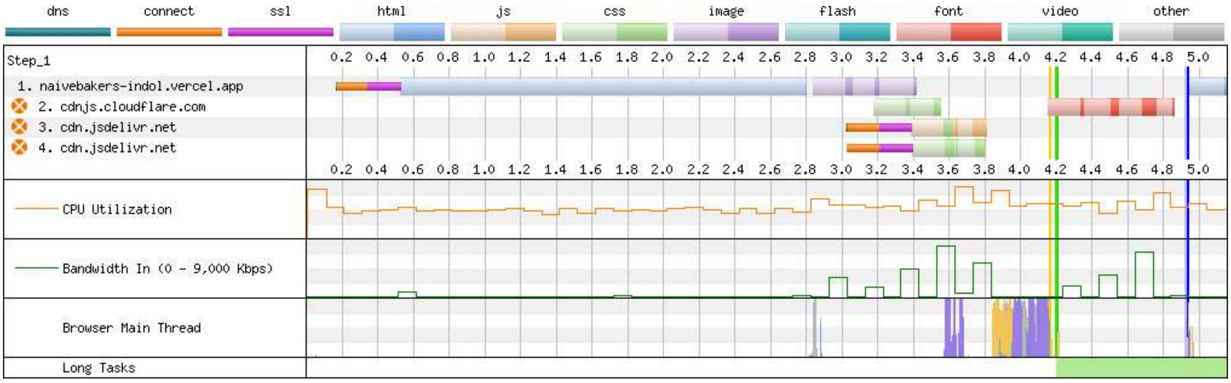
Note: Metric availability will vary

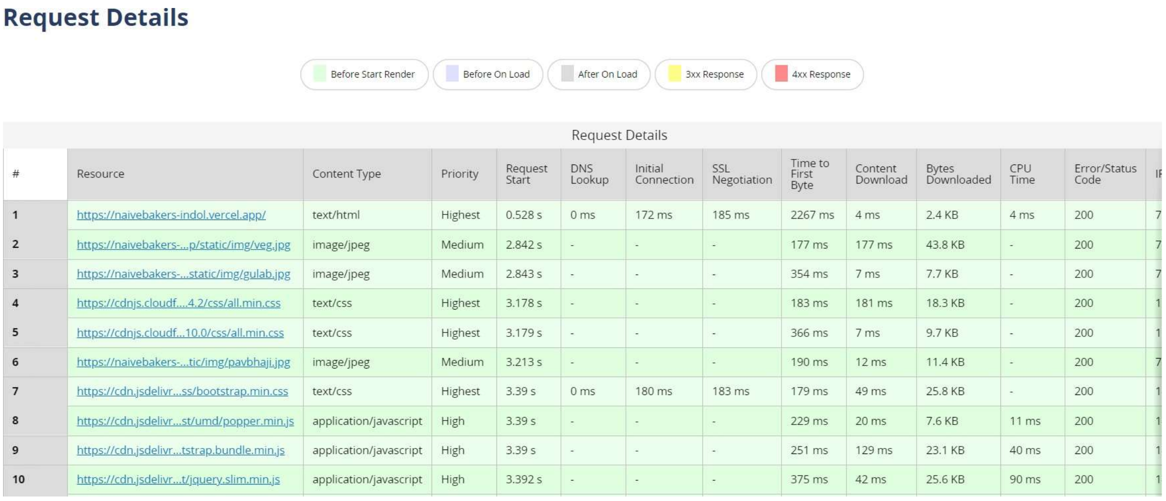
First View (Run 2)

Time to First Byte	Start Render	First Contentful Paint	Speed Index	Largest Contentful Paint	Cumulative Layout Shift	Total Blocking Time	Page Weight
2.859s	4.300s	4.261s	4.307s	4.261s	.001	.000s	386KB
When did the content start downloading?	When did pixels first start to appear?	How soon did text and images start to appear?	How soon did the page look usable?	When did the largest visible content finish loading?	How much did the design shift while loading?	Was the main thread blocked?	How many bytes downloaded?

Visual Page Loading Process (Explore)

Web Vitals Report:





Request Details

🟩 Before Start Render · ▨ Before On Load · ▨ After On Load · 🟨 3xx Response · 🟥 4xx Response

Request Details

#	Resource	Content Type	Priority	Request Start	DNS Lookup	Initial Connection	SSL Negotiation	Time to First Byte	Content Download	Bytes Downloaded	CPU Time	Error/Status Code	I
1	https://naivebakers-indol.vercel.app/	text/html	Highest	0.528 s	0 ms	172 ms	185 ms	2267 ms	4 ms	2.4 KB	4 ms	200	7
2	https://naivebakers-...p/static/img/veg.jpg	image/jpeg	Medium	2.842 s	-	-	-	177 ms	177 ms	43.8 KB	-	200	7
3	https://naivebakers-...static/img/gulab.jpg	image/jpeg	Medium	2.843 s	-	-	-	354 ms	7 ms	7.7 KB	-	200	7
4	https://cdnjs.cloudf....4.2/css/all.min.css	text/css	Highest	3.178 s	-	-	-	183 ms	181 ms	18.3 KB	-	200	1
5	https://cdnjs.cloudf...10.0/css/all.min.css	text/css	Highest	3.179 s	-	-	-	366 ms	7 ms	9.7 KB	-	200	1
6	https://naivebakers-...tic/img/pavbhaji.jpg	image/jpeg	Medium	3.213 s	-	-	-	190 ms	12 ms	11.4 KB	-	200	7
7	https://cdn.jsdelivr...ss/bootstrap.min.css	text/css	Highest	3.39 s	0 ms	180 ms	183 ms	179 ms	49 ms	25.8 KB	-	200	1
8	https://cdn.jsdelivr...st/umd/popper.min.js	application/javascript	High	3.39 s	-	-	-	229 ms	20 ms	7.6 KB	11 ms	200	1
9	https://cdn.jsdelivr...tstrap.bundle.min.js	application/javascript	High	3.39 s	-	-	-	251 ms	129 ms	23.1 KB	40 ms	200	1
10	https://cdn.jsdelivr...t/jquery.slim.min.js	application/javascript	High	3.392 s	-	-	-	375 ms	42 ms	25.6 KB	90 ms	200	1

Pentest Tools

Website Vulnerability Scanner Report

✓ https://naivebakers-indol.vercel.app/

Summary

Overall risk level:

Low

Risk ratings:

High:	0
Medium:	0
Low:	2
Info:	17

Scan information:

Start time:	Dec 02, 2023 / 12:54:11
Finish time:	Dec 02, 2023 / 12:54:28
Scan duration:	17 sec
Tests performed:	19/19
Scan status:	Finished

Findings

Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
https://naivebakers-indol.vercel.app/	Response headers do not include the HTTP Content-Security-Policy security header

Details

Risk description:
The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Server software and technology found

UNCONFIRMED

Software / Version	Category
Cloudflare	CDN
jsDelivr	CDN
cdnjs	CDN
Popper	Miscellaneous
Bootstrap 4.6.2	UI frameworks

Vercel	PaaS
jQuery	JavaScript libraries
Font Awesome 5.10.0	Font scripts
HSTS	Security

Details

Risk description:
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Security.txt file is missing

CONFIRMED

URL
Missing: https://naivebakers-indol.vercel.app/.well-known/security.txt

Details

Risk description:
We have detected that the server is missing the security.txt file. There is no particular risk in not creating a valid Security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Website is accessible.

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for robots.txt file.

Nothing was found for use of untrusted certificates.

Nothing was found for enabled HTTP debug methods.

Nothing was found for secure communication.

Nothing was found for directory listing.

Nothing was found for missing HTTP header - Strict-Transport-Security.

Nothing was found for missing HTTP header - X-Frame-Options.

Nothing was found for missing HTTP header - X-Content-Type-Options.

Nothing was found for missing HTTP header - Referrer.

Nothing was found for domain too loose set for cookies.

Nothing was found for HttpOnly flag of cookie.

Nothing was found for Secure flag of cookie.

Nothing was found for unsafe HTTP header Content Security Policy.

Scan coverage information

List of tests performed (19/19)

- ✓ Checking for website accessibility...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for website technologies...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for robots.txt file...
- ✓ Checking for absence of the security.txt file...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for missing HTTP header - X-Frame-Options...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for domain too loose set for cookies...

- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for unsafe HTTP header Content Security Policy...

Scan parameters

Target:	https://naivebakers-indol.vercel.app/
Scan type:	Light
Authentication:	False

Scan stats

Unique Injection Points Detected:	5
URLs spidered:	5
Total number of HTTP requests:	13
Average time until a response was received:	82ms