

**Dhirubhai Ambani
Institute of Information and Communication Technology**

**IT314 – Software Engineering
GROUP – 9**

Non-Functional Requirement Testing



STAYEAZY – HOTEL BOOKING SYSTEM

Instructor: Prof. Saurabh T.

December 02, 2024

Performance testing:

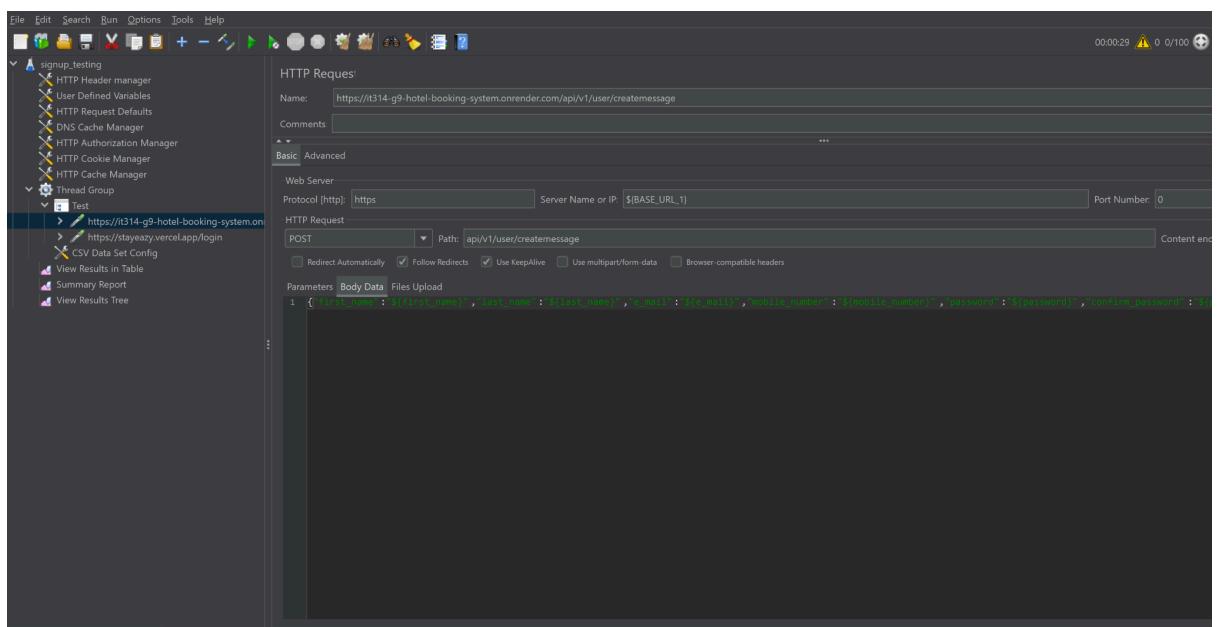
Overview

Test Name: Performance Test of Hotel Booking System

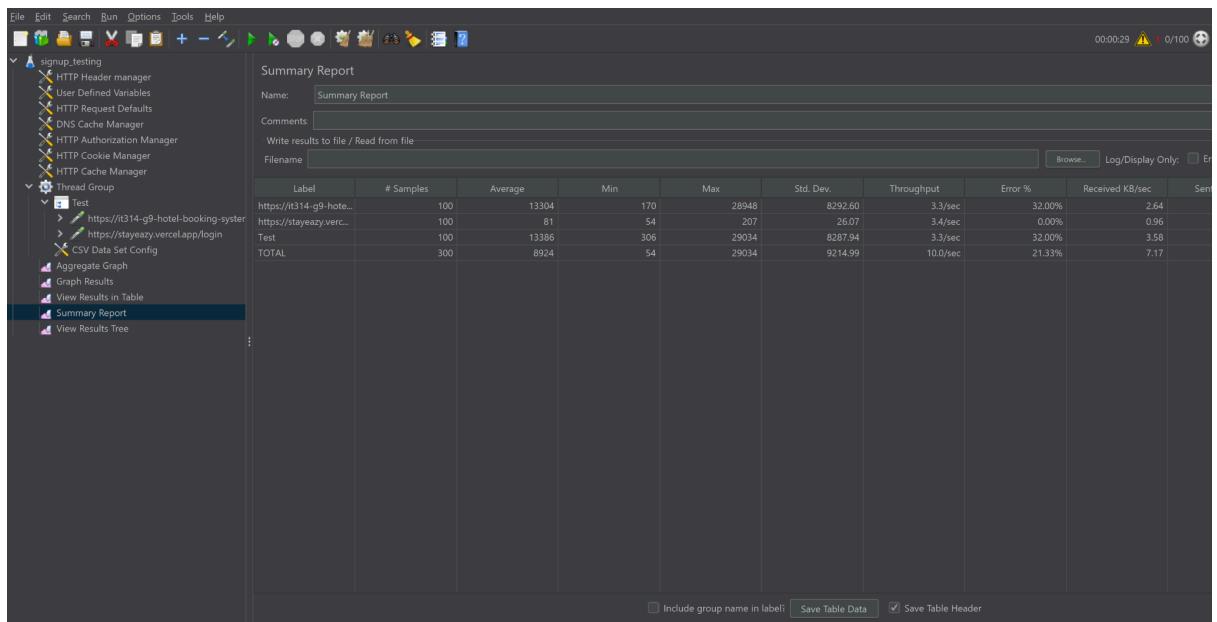
Tool Used: JMeter (via BlazeMeter)

- Load Testing on user signup:

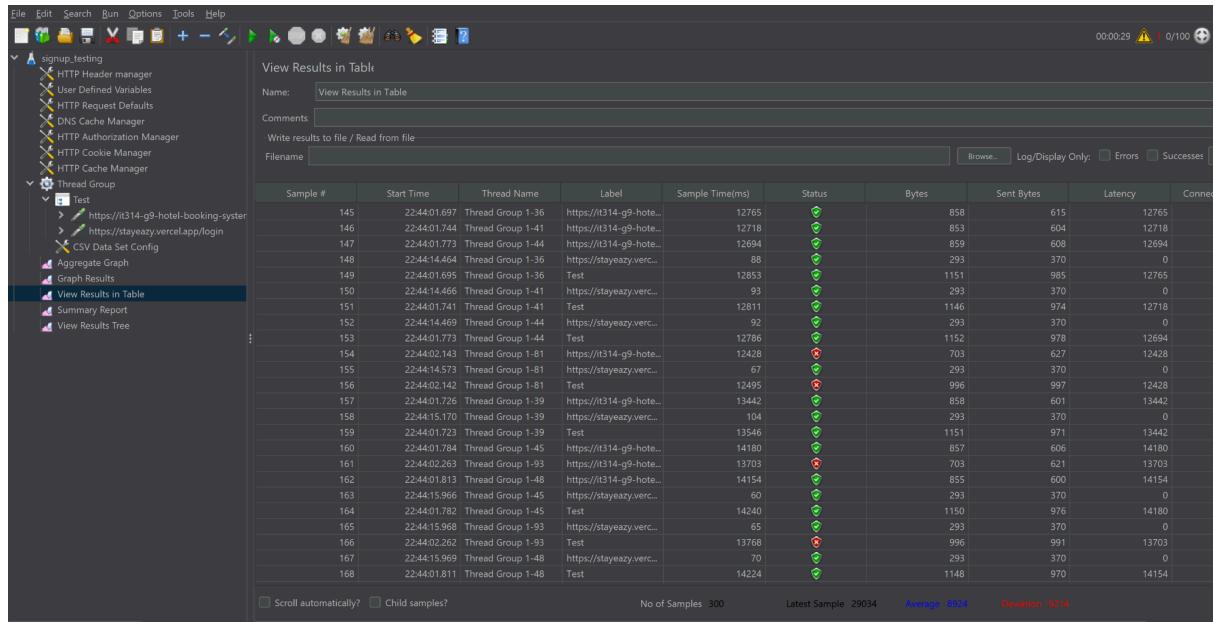
Create Request:



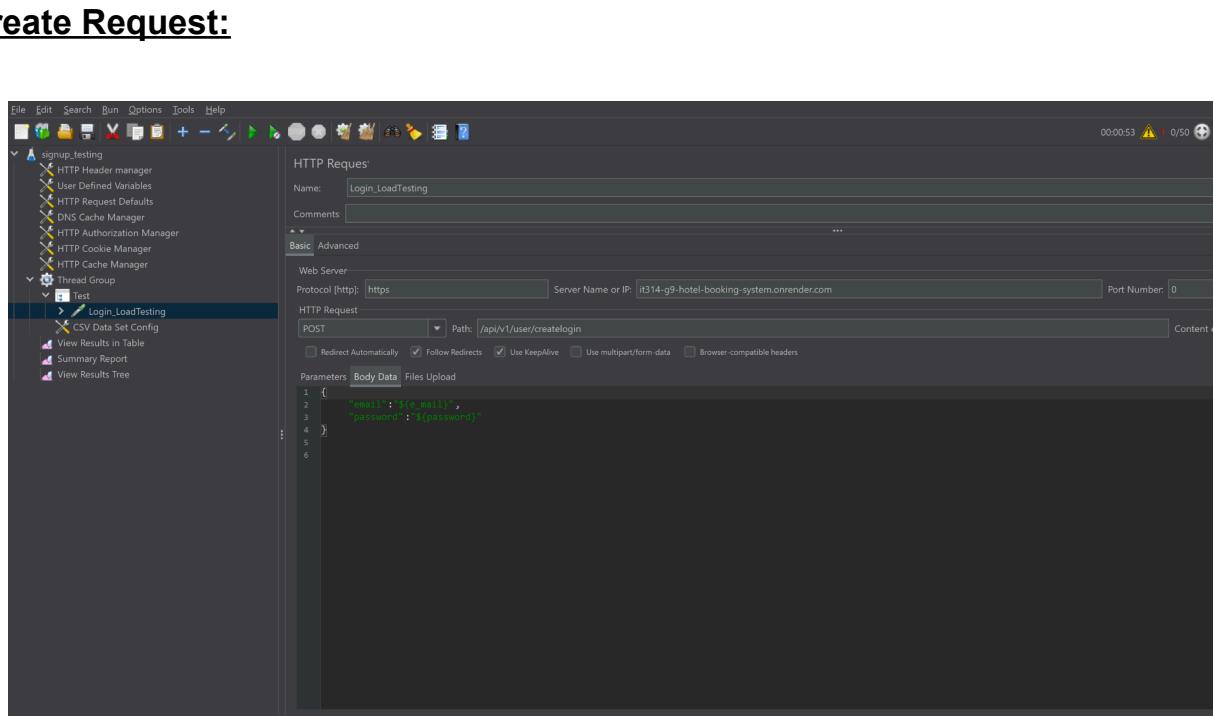
Summary Report:



Result in Table:



- Load Testing on user login:



Summary Report:

The screenshot shows the JMeter interface with the 'Summary Report' tab selected. The left sidebar shows a tree structure with 'signup_testing' expanded, containing 'HTTP Header manager', 'User Defined Variables', 'HTTP Request Defaults', 'DNS Cache Manager', 'HTTP Authorization Manager', 'HTTP Cookie Manager', and 'HTTP Cache Manager'. Below this is a 'Thread Group' node with a child 'Test' node, which has a 'CSV Data Set Config' child. Other options like 'View Results in Table', 'Summary Report', and 'View Results Tree' are also listed. The main panel displays a 'Summary Report' table with the following data:

Label	# Samples	Average	Min	Max	Std. Dev.	Throughput	Error %	Received KB/sec
login_LoadTesting	50	10815	195	19606	5201.60	2.4/sec	32.00%	2.2
Test	50	10815	195	19606	5201.60	2.4/sec	32.00%	2.2
TOTAL	100	10815	195	19606	5201.60	4.9/sec	32.00%	4.5

At the bottom of the table, there are checkboxes for 'Include group name in label', 'Save Table Data', and 'Save Table Header'. The status bar at the bottom right shows '00:00:20 1/50'.

Result in Table:

The screenshot shows the JMeter interface with the 'View Results in Table' tab selected. The left sidebar is identical to the previous screenshot, showing the 'signup_testing' tree structure. The main panel displays a 'View Results in Table' table with the following data:

Sample #	Start Time	Thread Name	Label	Sample Time(ms)	Status	Bytes	Sent Bytes	Latency
1	23:49:31.905	Thread Group 1-7	login_LoadTesting	195	🔴	703	489	2
2	23:49:31.904	Thread Group 1-7	Test	195	🔴	703	489	2
3	23:49:31.787	Thread Group 1-1	login_LoadTesting	2674	🟢	1077	478	26
4	23:49:31.785	Thread Group 1-1	Test	2674	🟢	1077	478	26
5	23:49:31.924	Thread Group 1-8	login_LoadTesting	2949	🟢	1084	494	29
6	23:49:31.924	Thread Group 1-8	Test	2949	🟢	1084	494	29
7	23:49:31.865	Thread Group 1-5	login_LoadTesting	3008	🟢	1084	498	30
8	23:49:31.864	Thread Group 1-5	Test	3008	🟢	1084	498	30
9	23:49:31.884	Thread Group 1-6	login_LoadTesting	2998	🔴	703	492	29
10	23:49:31.884	Thread Group 1-6	Test	2998	🔴	703	492	29
11	23:49:31.965	Thread Group 1-10	login_LoadTesting	3897	🟢	1084	493	36
12	23:49:31.964	Thread Group 1-10	Test	3897	🟢	1084	493	36
13	23:49:31.985	Thread Group 1-11	login_LoadTesting	4276	🟢	1094	493	42
14	23:49:31.984	Thread Group 1-11	Test	4276	🟢	1094	493	42
15	23:49:32.105	Thread Group 1-17	login_LoadTesting	4657	🔴	703	492	46
16	23:49:32.104	Thread Group 1-17	Test	4657	🔴	703	492	46
17	23:49:31.807	Thread Group 1-2	login_LoadTesting	4961	🟢	1082	493	49
18	23:49:31.807	Thread Group 1-2	Test	4961	🟢	1082	493	49
19	23:49:31.845	Thread Group 1-4	login_LoadTesting	5317	🟢	1084	493	55
20	23:49:31.844	Thread Group 1-4	Test	5317	🟢	1084	493	55
21	23:49:32.085	Thread Group 1-16	login_LoadTesting	5993	🟢	1089	499	59
22	23:49:32.084	Thread Group 1-16	Test	5993	🟢	1089	499	59
23	23:49:32.065	Thread Group 1-15	login_LoadTesting	6018	🟢	1087	496	60
24	23:49:32.064	Thread Group 1-15	Test	6018	🟢	1087	496	60

At the bottom of the table, there are checkboxes for 'Scroll automatically?' and 'Child samples?'. The status bar at the bottom right shows 'No of Samples 100', 'Latest Sample 19606', 'Average 10815', 'Deviation 5201', and 'Latency 55ms'.

Compatibility Testing

Overview

- Compatibility testing was conducted on StayEazy website across various browsers on Windows 11 and MacOS. The testing aimed to verify smooth functionality, responsiveness, and consistent performance across all platforms.

Test Environment :

Operating System: Windows 11, MacOS

Browsers Tested:

- Google Chrome
- Safari
- Mozilla Firefox
- Brave

Results:

1. Google Chrome

- Fully compatible with seamless performance. All features rendered correctly without any issues.

2. Safari

- Fully compatible and delivered excellent performance. Behaved similarly to Chrome with no discrepancies observed.

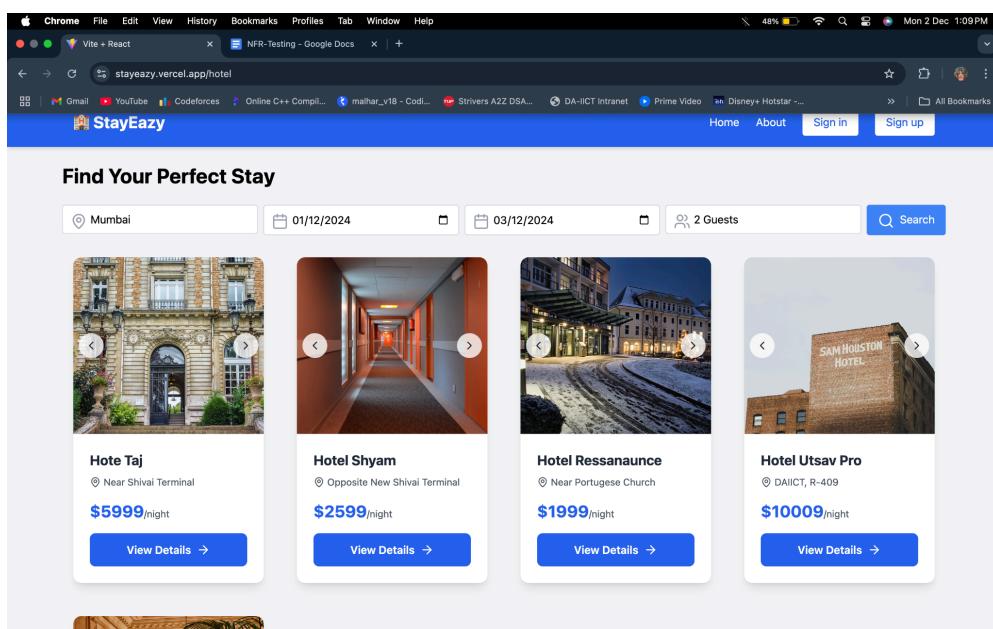
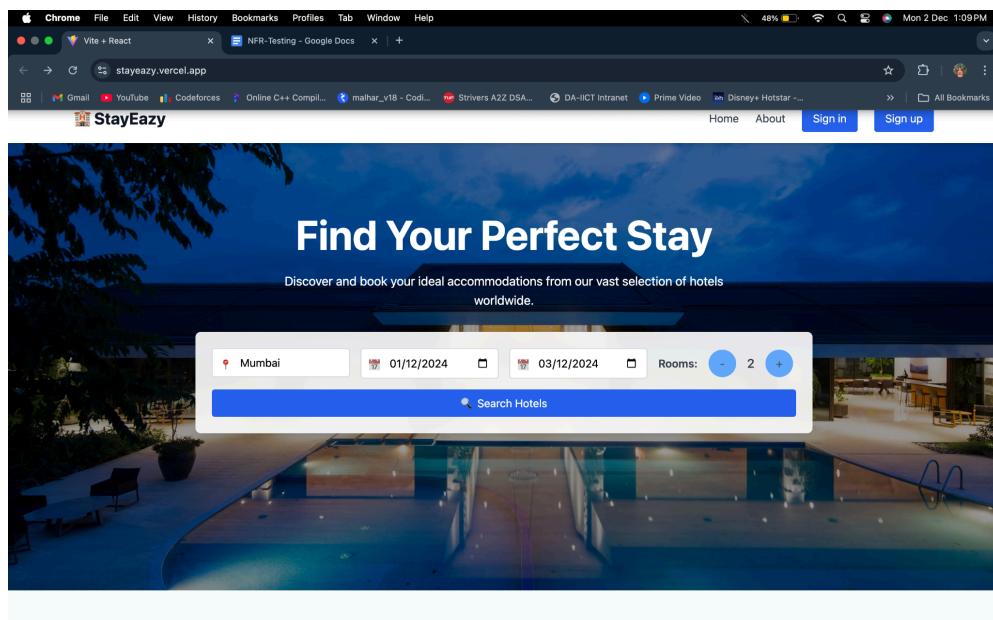
3. Mozilla Firefox

- Fully compatible with smooth operation and consistent feature rendering.

4. Brave

- Compatible for essential features, with good performance given its lightweight nature.

Google Chrome:



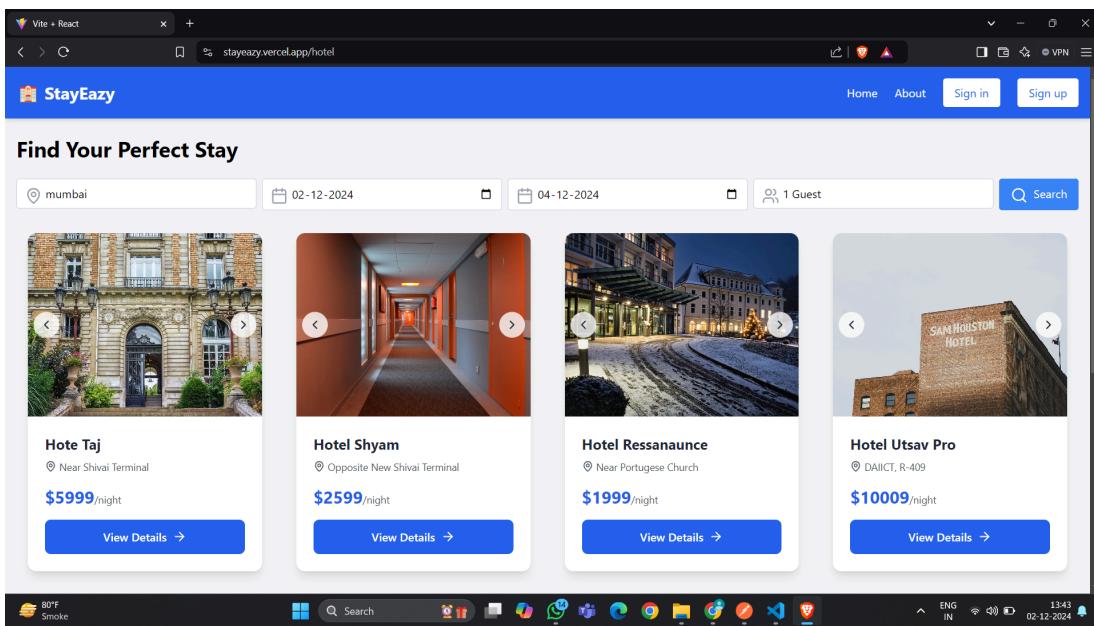
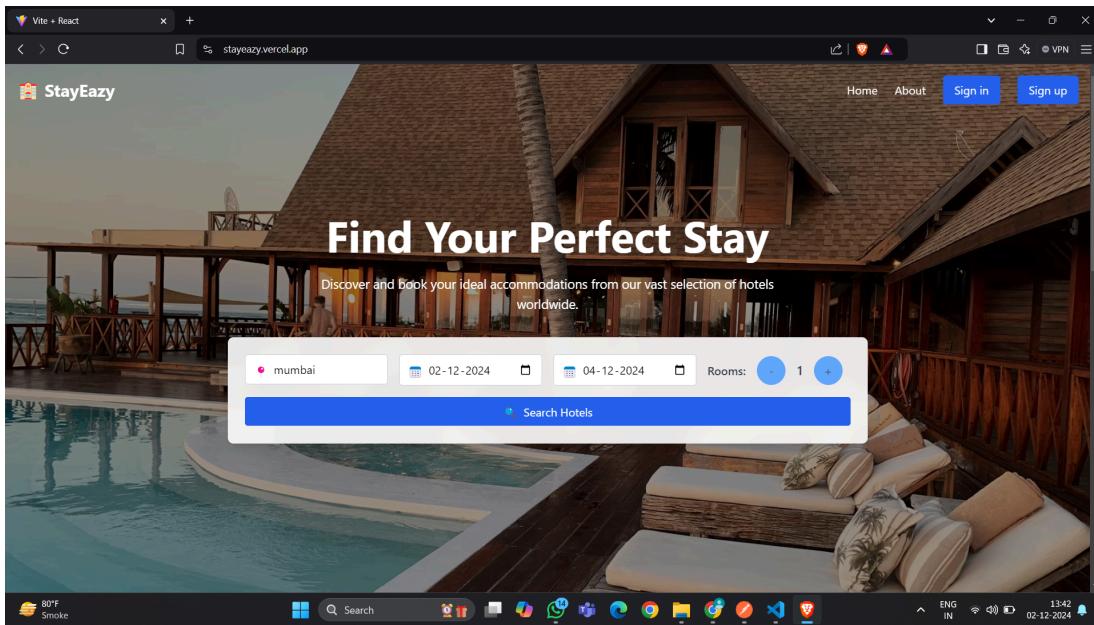
Safari:

The screenshot shows the StayEasy homepage. At the top, there is a navigation bar with links for Home, About, Sign in, and Sign up. Below the navigation bar is a large banner with the text "Find Your Perfect Stay" and a subtext "Discover and book your ideal accommodations from our vast selection of hotels worldwide." A search bar is overlaid on the banner, containing fields for location ("Mumbai"), check-in date ("01/12/2024"), check-out date ("01/12/2024"), and rooms ("1"). A blue "Search Hotels" button is also present. The background of the banner features a photograph of a modern building with a large, illuminated swimming pool at night.

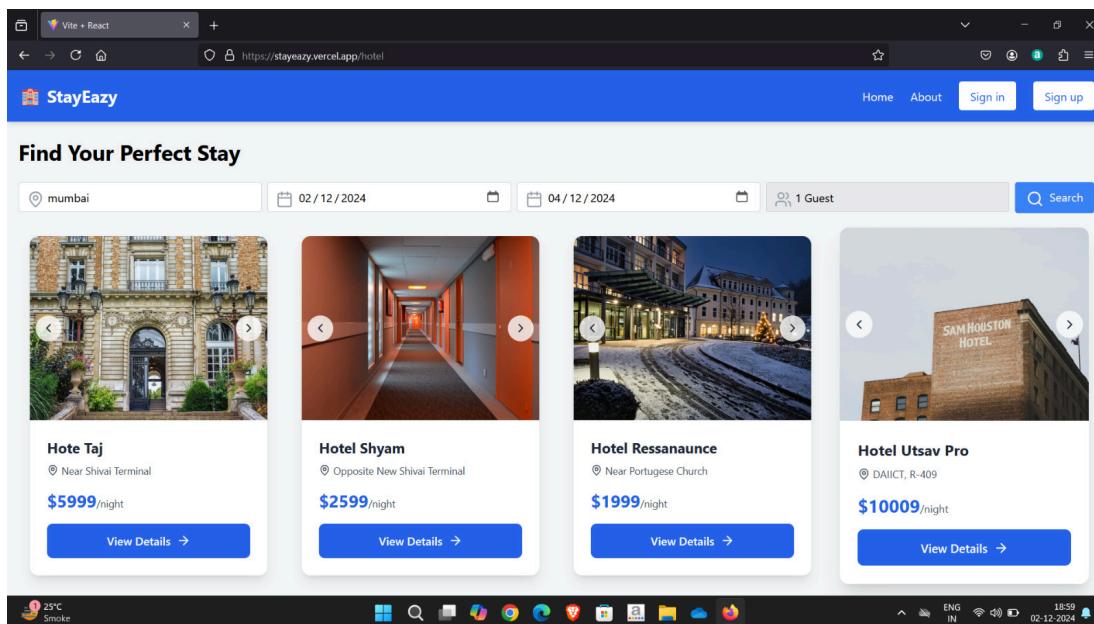
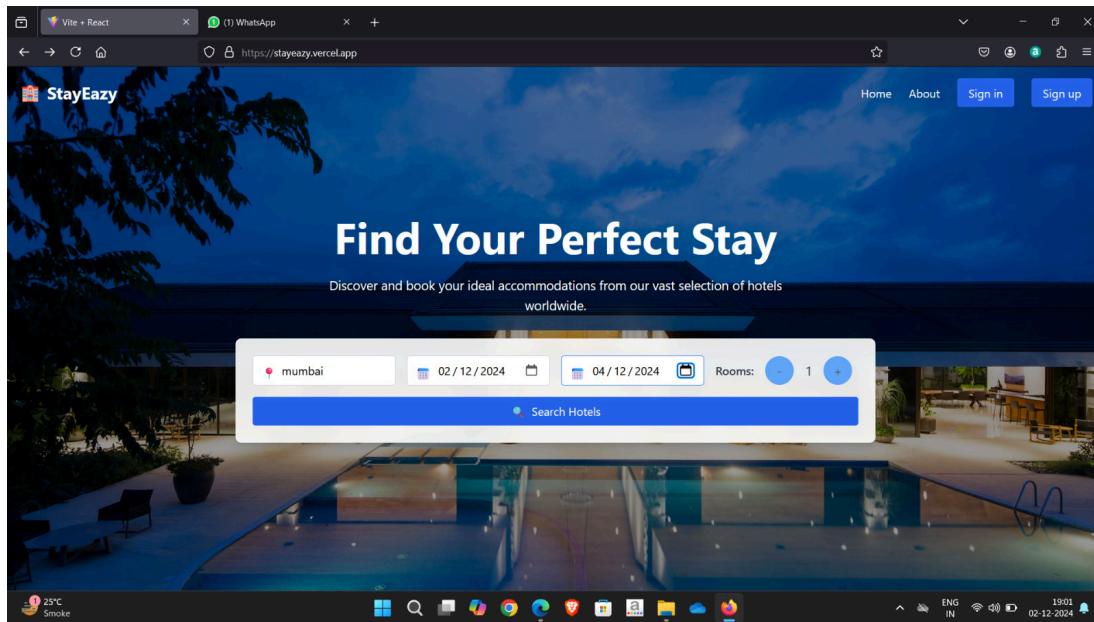
The screenshot shows the search results page for StayEasy. The search parameters are the same as the homepage: location "Mumbai", check-in "01/12/2024", check-out "01/12/2024", and 1 guest. The results are displayed in a grid of four cards:

- Hotel Taj**
Near Shivai Terminal
\$5999/night
[View Details →](#)
- Hotel Shyam**
Opposite New Shivai Terminal
\$2599/night
[View Details →](#)
- Hotel Ressanaunce**
Near Portugese Church
\$1999/night
[View Details →](#)
- Hotel Utsav Pro**
DAIICIT, R-409
\$10009/night
[View Details →](#)

Brave:



Firefox:



Security Testing using Pentest-Tools

Overview of Pentest-Tools

Pentest-Tools is an online platform designed to facilitate penetration testing, focusing on evaluating the security of systems, networks, and web applications. It offers a comprehensive suite of automated tools to identify vulnerabilities, assess configurations, and ensure compliance with security standards.

By simulating cyberattacks, Pentest-Tools helps proactively identify threats, ensuring systems remain robust against unauthorized access and data breaches.

Role in Non-Functional Requirements (NFR) Testing:

Pentest-Tools is particularly valuable in the following areas of NFR testing:

- **Security Testing:** Verifies adherence to security best practices by identifying vulnerabilities like SQL injection and configuration issues.
- **Reliability Testing:** Evaluates the system's resilience to malicious attacks that could disrupt availability or functionality.
- **Data Privacy:** Assesses the mechanisms in place to safeguard sensitive user and donor information.

By incorporating Pentest-Tools into NFR testing, organizations can bolster their security posture, enhance system reliability, and provide a safer platform for end users.

Website Vulnerability Scanner Report

✓ <https://stayeazy.vercel.app/>

! The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. [Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.](#)

Summary

Overall risk level:
Low

Risk ratings:
High: 0
Medium: 0
Low: 4
Info: 34

Scan information:
Start time: Dec 01, 2024 / 23:21:00 UTC+0530
Finish time: Dec 01, 2024 / 23:26:16 UTC+0530
Scan duration: 5 min, 16 sec
Tests performed: 38/38
Scan status: **Finished**

Findings

FLAG Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
https://stayeazy.vercel.app/	Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

▼ Details

Risk description:

The risk is that 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 - 2017 : [A6 - Security Misconfiguration](#)
OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

FLAG Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
https://stayeazy.vercel.app/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response. Request / Response

▼ Details

Risk description:

The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g.

"<https://www.google.com>", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:

The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:

https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

FLAG Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
https://stayeazy.vercel.app/	Response headers do not include the X-Content-Type-Options HTTP security header Request / Response

▼ Details

Risk description:

The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

Recommendation:

We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff`.

References:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>

Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

FLAG Server software and technology found

UNCONFIRMED ⓘ

Software / Version	Category
 Google Sign-in	Authentication
 Lucide	Font scripts
 React	JavaScript frameworks
 React Router 6	JavaScript frameworks
 Tailwind CSS	UI frameworks
 Vercel	PaaS
 Vite	Miscellaneous
 HSTS	Security

▼ Details

Risk description:

The risk is that 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-

Classification:

OWASP Top 10 - 2017 : A6 - Security Misconfiguration
 OWASP Top 10 - 2021 : A5 - Security Misconfiguration

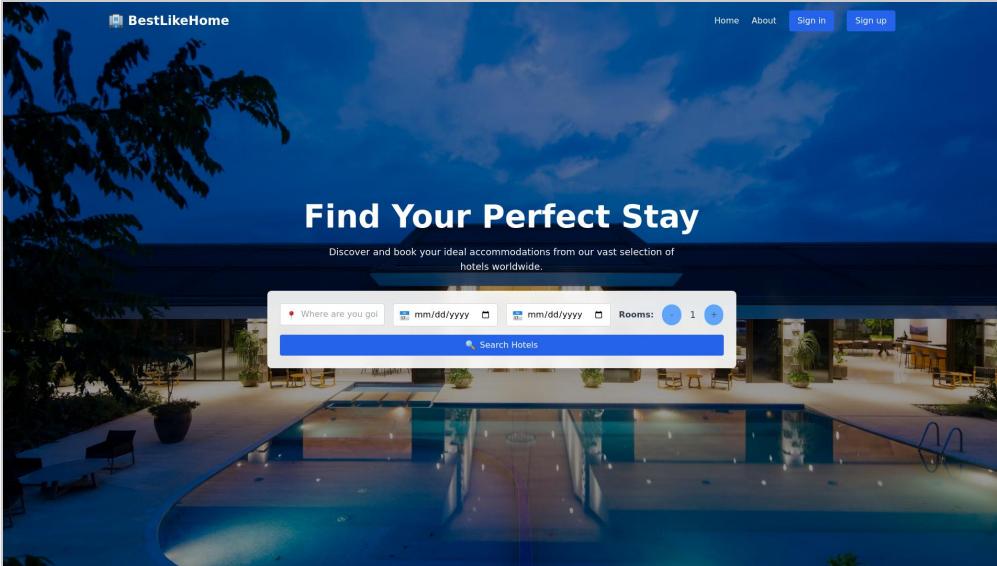
Screenshot:

Figure 1. Website Screenshot

Flag Spider results

URL	Method	Page Title	Page Size	Status Code
https://stayeazy.vercel.app/	GET	Vite + React	515 B	200
https://stayeazy.vercel.app/assets	GET	Vite + React	515 B	200
https://stayeazy.vercel.app/assets/	GET	Vite + React	515 B	200

▼ Details

Risk description:

The table contains all the unique pages the scanner found. The duplicated URLs are not available here as scanning those is considered unnecessary

Recommendation:

We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

References:

[All the URLs the scanner found, including duplicates](#) (available for 90 days after the scan date)

Flag Website is accessible.

Flag Nothing was found for vulnerabilities of server-side software.

Flag Nothing was found for client access policies.

Flag Nothing was found for robots.txt file.

Flag Nothing was found for absence of the security.txt file.

└ Outdated JavaScript libraries were merged into server-side software vulnerabilities.

└ Nothing was found for use of untrusted certificates.

└ Nothing was found for enabled HTTP debug methods.

└ Nothing was found for administration consoles.

└ Nothing was found for information disclosure.

└ Nothing was found for software identification.

└ Nothing was found for sensitive files.

└ Nothing was found for interesting files.

└ Nothing was found for enabled HTTP OPTIONS method.

└ Nothing was found for secure communication.

└ Nothing was found for directory listing.

└ Nothing was found for error messages.

└ Nothing was found for debug messages.

└ Nothing was found for code comments.

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

└ Nothing was found for Insecure Direct Object Reference.

└ Nothing was found for domain too loose set for cookies.

└ Nothing was found for mixed content between HTTP and HTTPS.

└ Nothing was found for internal error code.

- Nothing was found for HttpOnly flag of cookie.

 - Nothing was found for Secure flag of cookie.

 - Nothing was found for login interfaces.

 - Nothing was found for Server Side Request Forgery.

 - Nothing was found for Open Redirect.

 - Nothing was found for Exposed Backup Files.

 - Nothing was found for unsafe HTTP header Content Security Policy.

 - Nothing was found for OpenAPI files.

 - Nothing was found for file upload.
-
- ## Scan coverage information
-
- ### List of tests performed (38/38)
- ✓ Starting the scan...
 - ✓ Checking for missing HTTP header - Content Security Policy...
 - ✓ Checking for missing HTTP header - Referrer...
 - ✓ Checking for missing HTTP header - X-Content-Type-Options...
 - ✓ Spidering target...
 - ✓ 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 outdated JavaScript libraries...
 - ✓ Checking for use of untrusted certificates...
 - ✓ Checking for enabled HTTP debug methods...
 - ✓ Checking for administration consoles...
 - ✓ Checking for information disclosure... (this might take a few hours)
 - ✓ Checking for software identification...
 - ✓ Checking for sensitive files...
 - ✓ Checking for interesting files... (this might take a few hours)
 - ✓ Checking for enabled HTTP OPTIONS method...
 - ✓ Checking for secure communication...
 - ✓ Checking for directory listing...
 - ✓ Checking for error messages...
 - ✓ Checking for debug messages...
 - ✓ Checking for code comments...
 - ✓ Checking for missing HTTP header - Strict-Transport-Security...
 - ✓ Checking for Insecure Direct Object Reference...
 - ✓ Checking for domain too loose set for cookies...
 - ✓ Checking for mixed content between HTTP and HTTPS...
 - ✓ Checking for internal error code...
 - ✓ Checking for HttpOnly flag of cookie...
 - ✓ Checking for Secure flag of cookie...
 - ✓ Checking for login interfaces...
 - ✓ Checking for Server Side Request Forgery...
 - ✓ Checking for Open Redirect...

- ✓ Checking for Exposed Backup Files...
- ✓ Checking for unsafe HTTP header Content Security Policy...
- ✓ Checking for OpenAPI files...
- ✓ Checking for file upload...

Scan parameters

target: https://stayeazy.vercel.app/
scan_type: Light
authentication: False

Scan stats

Unique Injection Points Detected: 1
URLs spidered: 3
Total number of HTTP requests: 16056
Average time until a response was received: 0ms
Total number of HTTP request errors: 282
