



ENGINEERS WITH  
SOCIAL RESPONSIBILITY

# IT 314 SOFTWARE ENGINEERING

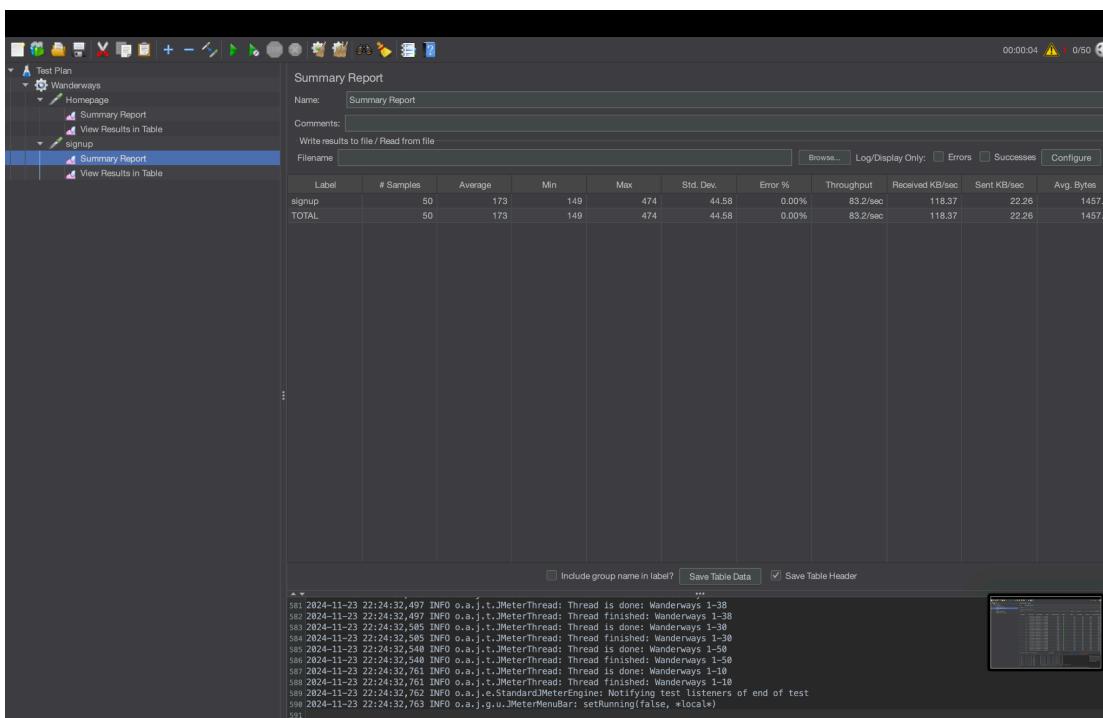
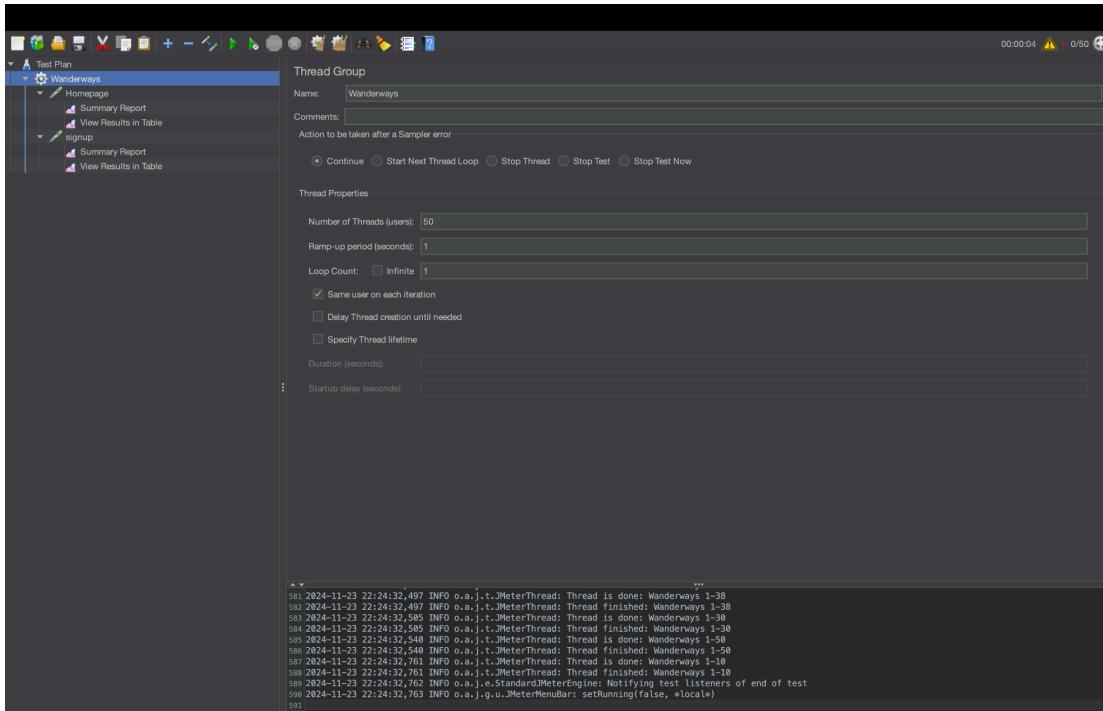
**GROUP - 32**  
**WANDERWAYS**  
**NON-FUNCTIONAL TESTING**

# 1. LOAD BALANCE TESTING

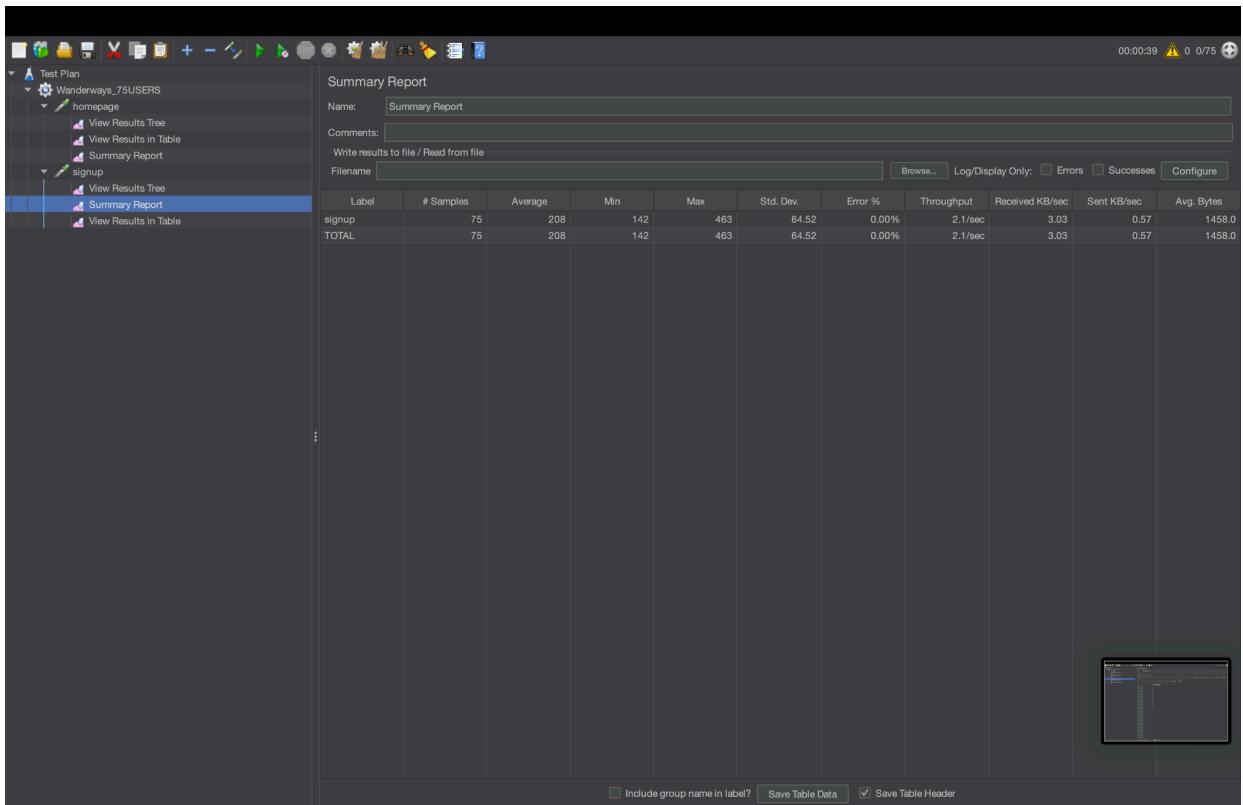
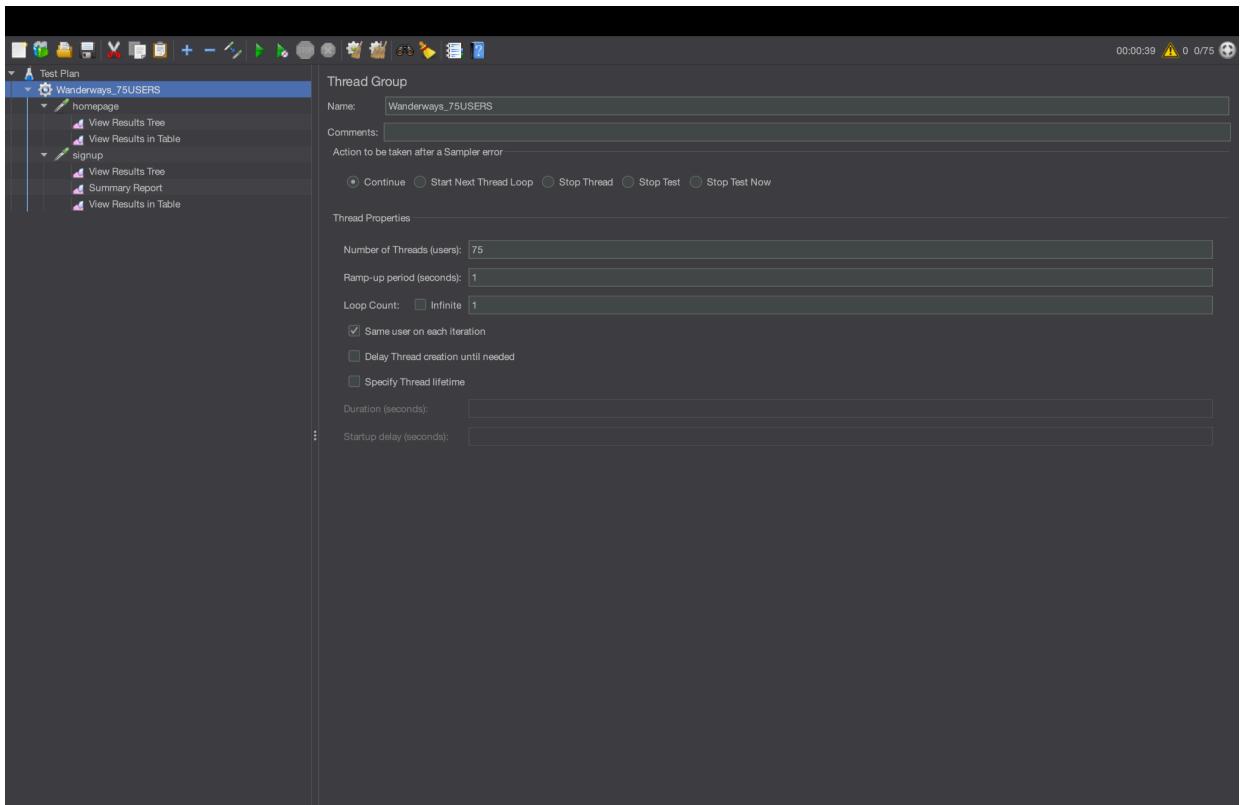
Using JMeter and PostMan, we tested the homepage of our website for how many concurrent users it can handle for GET and POST requests respectively.

We used JMeter to test GET request for the home page for:

- 50 users:



b) 75 users:



c) 125 users:

The image displays two screenshots of the JMeter interface. The top screenshot shows the 'Test Plan' window with a 'Thread Group' configuration for 125 users. The bottom screenshot shows the 'Summary Report' window displaying performance metrics for the test.

**Test Plan (Top Window):**

- Thread Group:**
  - Name: Twanderways
  - Comments:
  - Action to be taken after a Sampler error:
    - Continue (radio button selected)
    - Start Next Thread Loop
    - Stop Thread
    - Stop Test
    - Stop Test Now
- Thread Properties:**
  - Number of Threads (users): 125
  - Ramp-up period (seconds): 2
  - Loop Count:  Infinite 1
  - Same user on each iteration
  - Delay Thread creation until needed
  - Specify Thread lifetime
  - Duration (seconds):
  - Startup delay (seconds):

**Summary Report (Bottom Window):**

- Summary Report:**
  - Name: Summary Report
  - Comments: Write results to file / Read from file
  - Filename:
  - Log/Display Only:  Errors  Successes  Configure
- Performance Data Table:**

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
homepage	125	46633	37176	73681	14577.50	0.00%	1.7/sec	2.38	0.43	1446.3
TOTAL	125	46633	37176	73681	14577.50	0.00%	1.7/sec	2.38	0.43	1446.3

d) 500 users:

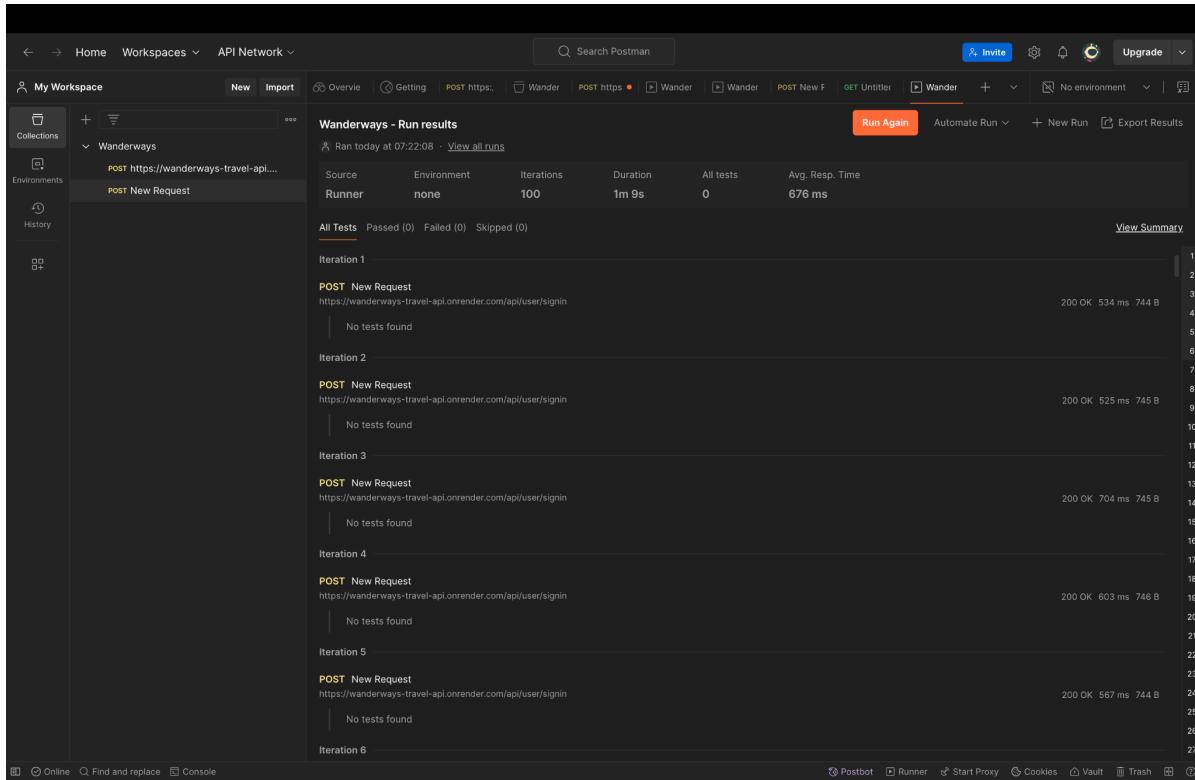
The image displays two screenshots of the JMeter interface. The top screenshot shows the 'Test Plan' window with a 'wanderways' test plan. It contains a 'Thread Group' configuration with 500 threads, a ramp-up period of 2 seconds, and a loop count of 1. The bottom screenshot shows the 'Summary Report' window for the 'homepage' sampler, which has been run 500 times. The summary table provides detailed performance metrics:

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
homepage	500	144455	106608	213490	33140.63	41.20%	2.3/sec	4.60	0.42	2010.4
TOTAL	500	144455	106608	213490	33140.63	41.20%	2.3/sec	4.60	0.42	2010.4

We can see here that as the number of concurrent users increases, the throughput decreases at first and then it increases.

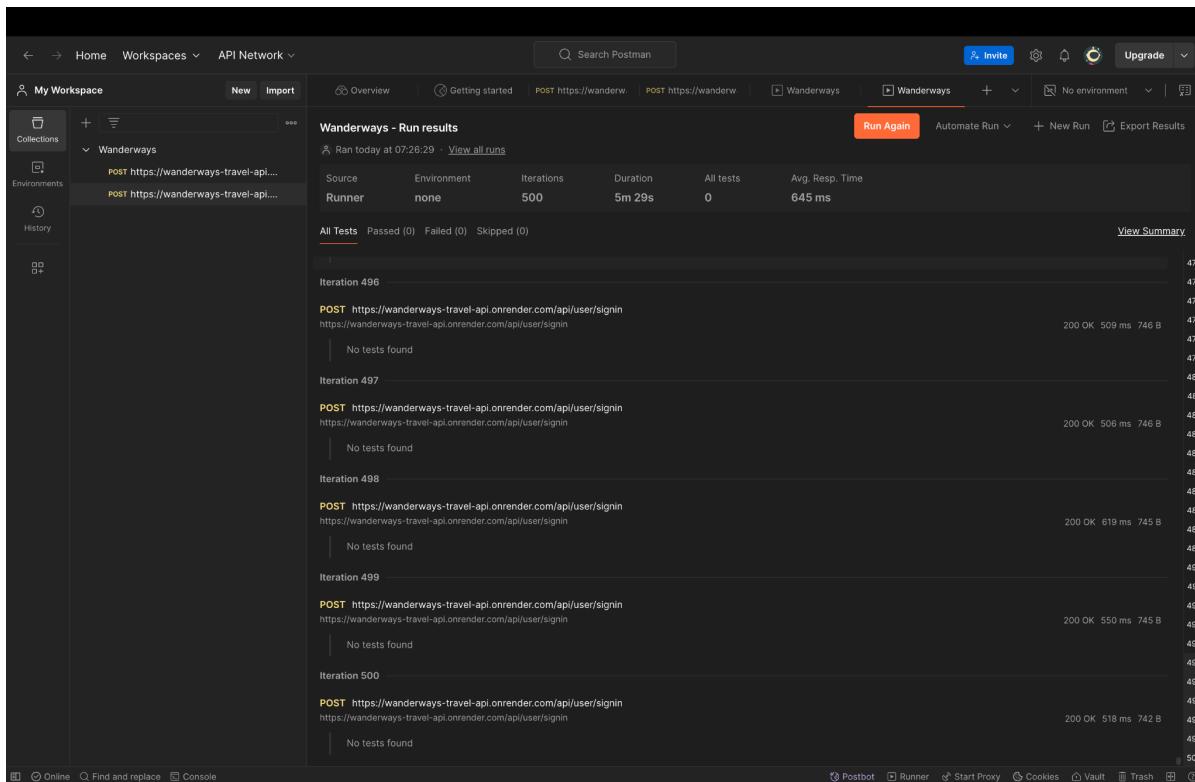
We used PostMan to test POST request for Sign-in Page for:

a) 100 users



The screenshot shows the Postman interface with a collection named "Wanderways". A single POST request is listed under the "Wanderways" collection. The request is directed to <https://wanderways-travel-api.onrender.com/api/user/signin>. The "Iterations" field is set to 100. The "Duration" is 1m 9s, and the "Avg. Resp. Time" is 676 ms. The "All Tests" section shows 0 failed tests. The results are presented in six iterations, each containing one POST request. The response for each iteration is 200 OK with a duration of 534 ms and a body size of 744 B.

b) 500 users



The screenshot shows the Postman interface with a collection named "Wanderways". A single POST request is listed under the "Wanderways" collection. The request is directed to <https://wanderways-travel-api.onrender.com/api/user/signin>. The "Iterations" field is set to 500. The "Duration" is 5m 29s, and the "Avg. Resp. Time" is 645 ms. The "All Tests" section shows 0 failed tests. The results are presented in 500 iterations, each containing one POST request. The response for each iteration is 200 OK with a duration of 509 ms and a body size of 746 B.

We used PostMan to also test POST request for Sign-up Page for:

c) 100 users

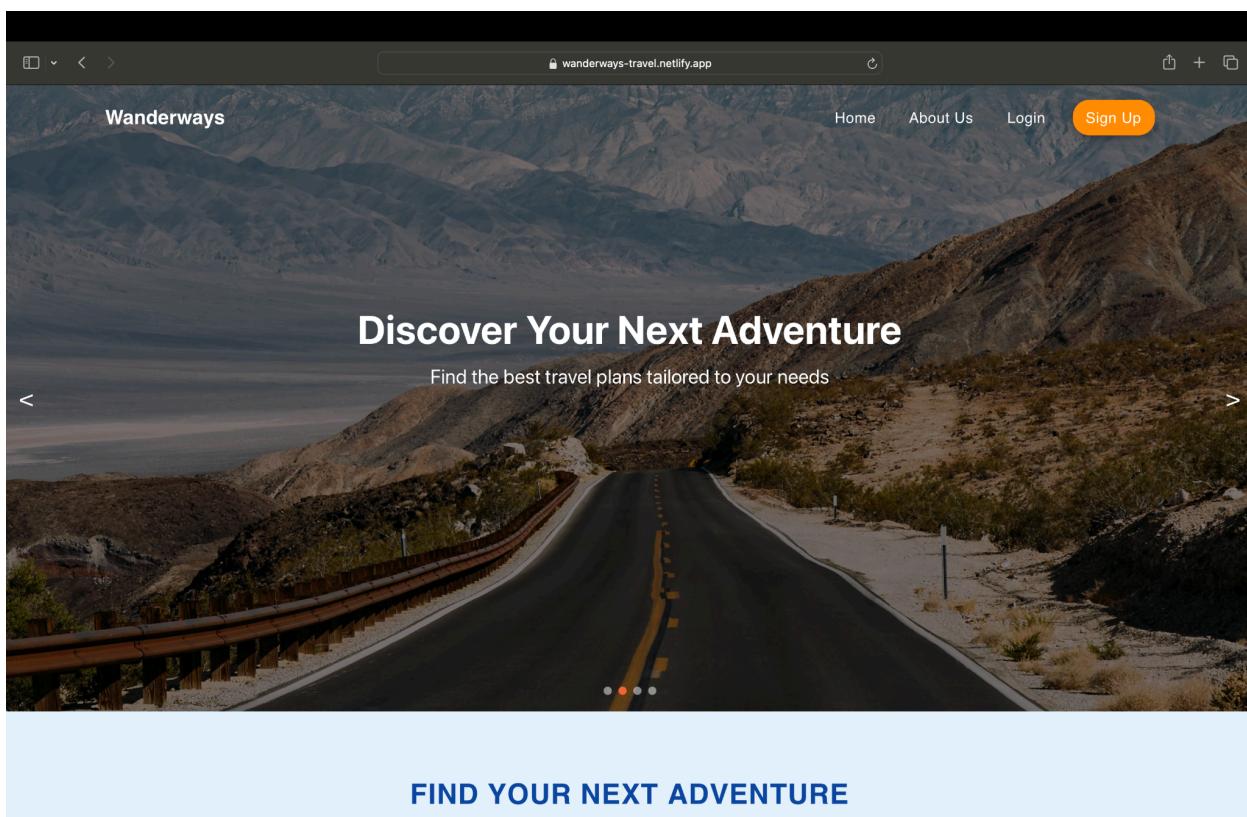
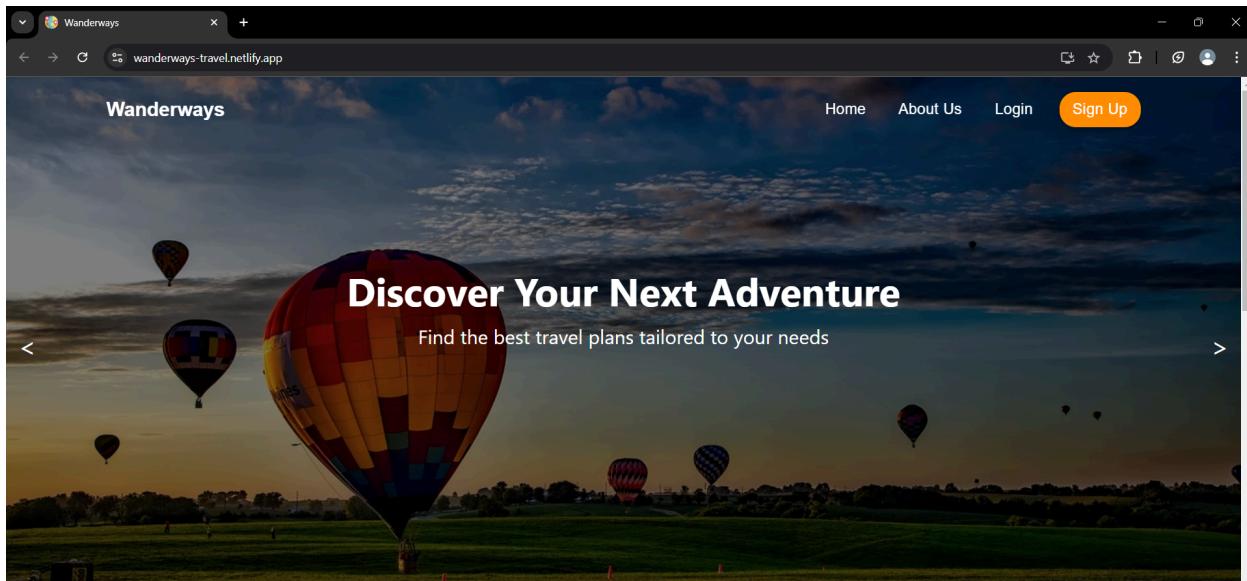
The screenshot shows the Postman interface with a 'Wanderways - Run results' section. The run was completed at 07:05:22. The summary indicates 100 iterations, 1m 3s duration, 0 failed tests, and an average response time of 616 ms. The results table lists 100 iterations, each showing a successful POST request to `https://wanderways-travel-api.onrender.com/api/user/signup` with a 200 OK status, 1103 ms duration, and 505 B size. All iterations show 'No tests found'.

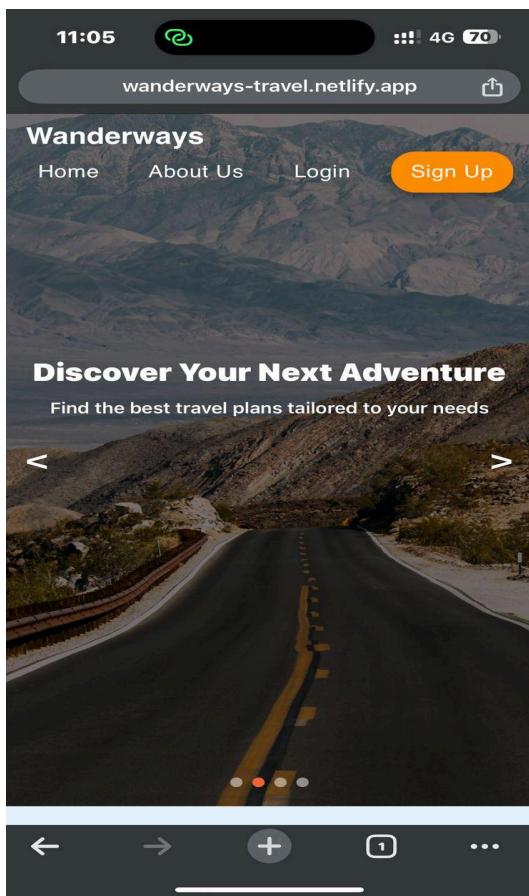
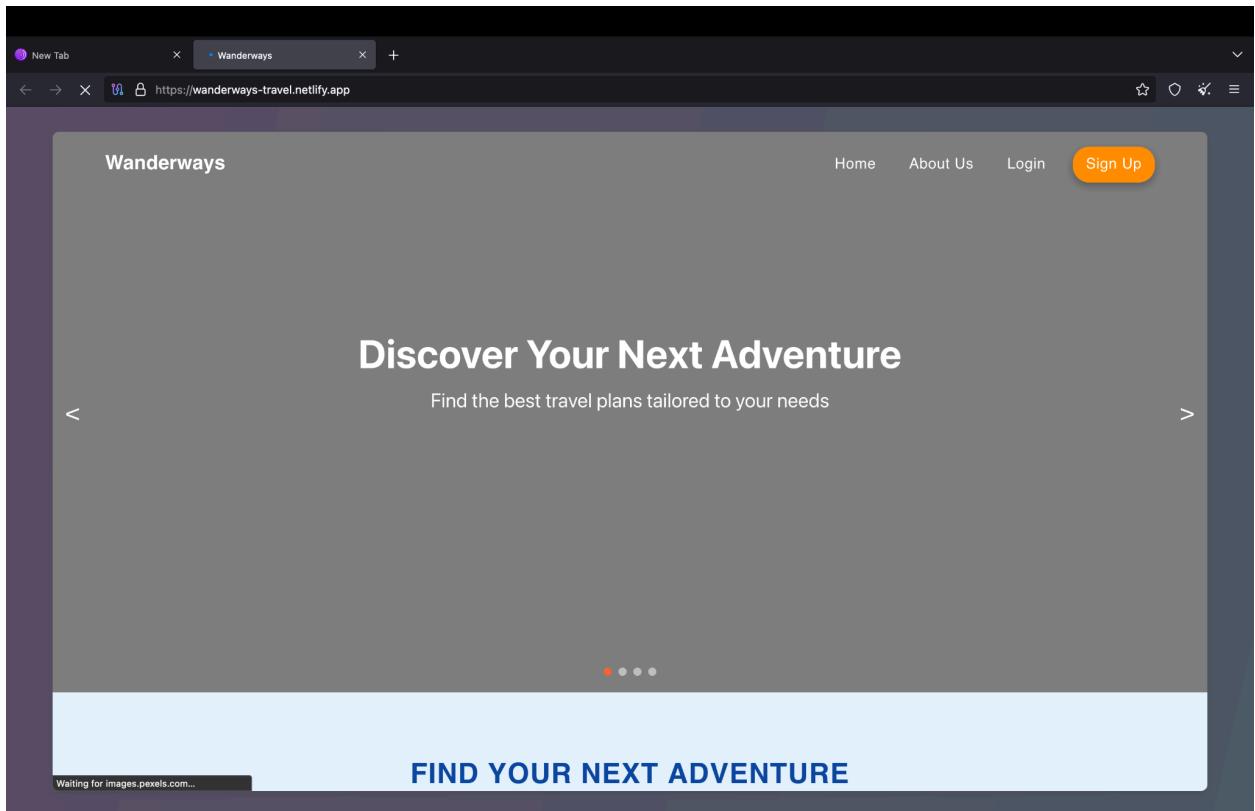
d) 500 users

The screenshot shows the Postman interface with a 'Wanderways - Run results' section. The run was completed at 07:07:08. The summary indicates 500 iterations, 5m 20s duration, 0 failed tests, and an average response time of 627 ms. The results table lists 500 iterations, each showing a successful POST request to `https://wanderways-travel-api.onrender.com/api/user/signup` with a 200 OK status, 1099 ms duration, and 505 B size. All iterations show 'No tests found'.

## 2. COMPATIBILITY TESTING

We have made sure that our website is accessible and fully working with the latest web browsers, both on PC/Desktop and Mobile Phone. To test this, we used Google Chrome, Safari, Torr, and also Safari on Mobile Phone.





### 3. SECURITY TESTING

We conducted Vulnerability Testing on our website using a third party "<https://pentest-tools.com/>". Here is the result for the test which ran for 30 minutes.



#### Website Vulnerability Scanner Report

✓ <https://wanderways-travel.netlify.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:



Scan information:

Start time:	Dec 01, 2024 / 16:08:45 UTC+0530
Finish time:	Dec 01, 2024 / 16:38:59 UTC+0530
Scan duration:	30 min, 14 sec
Tests performed:	37/37
Scan status:	Finished

##### Findings

■ Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
<a href="https://wanderways-travel.netlify.app/">https://wanderways-travel.netlify.app/</a>	Response does not include the HTTP Content-Security-Policy security header or meta tag <a href="#">Request / Response</a>

▼ 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://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

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

CONFIRMED

URL	Evidence
<a href="https://wanderways-travel.netlify.app/">https://wanderways-travel.netlify.app/</a>	Response headers do not include the X-Content-Type-Options HTTP security header <a href="#">Request / Response</a>

▼ 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](#)

## Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
<a href="https://wanderways-travel.netlify.app/">https://wanderways-travel.netlify.app/</a>	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/Referrer\\_header:\\_privacy\\_and\\_security\\_concerns](https://developer.mozilla.org/en-US/docs/Web/Security/Referrer_header:_privacy_and_security_concerns)

**Classification:**  
CWE : [CWE-693](#)  
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)  
OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

## Robots.txt file found

CONFIRMED

URL
<a href="https://wanderways-travel.netlify.app/robots.txt">https://wanderways-travel.netlify.app/robots.txt</a>

▼ Details

**Risk description:**  
There is no particular security risk in having a robots.txt file. However, it's important to note that adding endpoints in it should not be considered a security measure, as this file can be directly accessed and read by anyone.

**Recommendation:**  
We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

**References:**  
<https://www.theregister.co.uk/2015/05/19/robotstxt/>

**Classification:**  
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)  
OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

**Screenshot:**

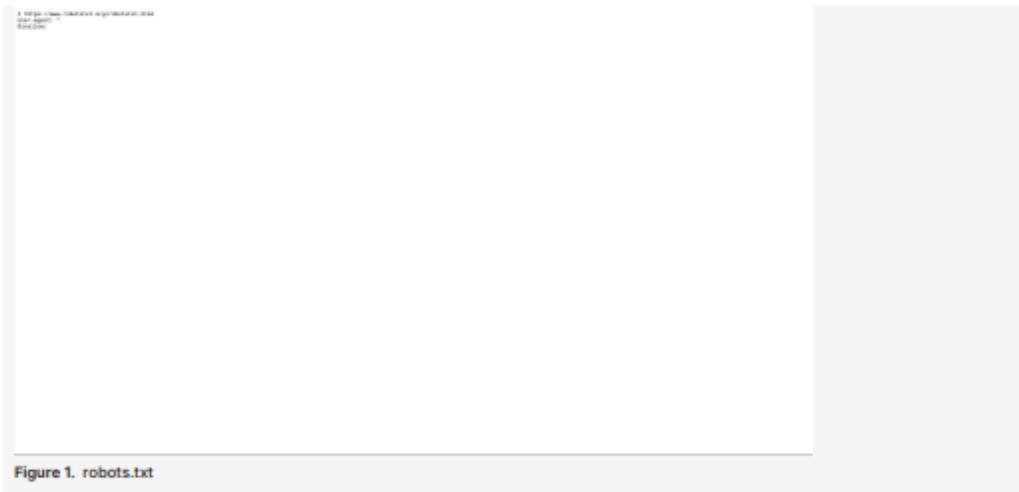


Figure 1. robots.txt

## ■ Server software and technology found

UNCONFIRMED

Software / Version	Category
<input type="checkbox"/> Emotion	JavaScript frameworks, Development
<input type="checkbox"/> Font Awesome	Font scripts
<input type="checkbox"/> Goober	JavaScript libraries
 MUI	UI frameworks
 React	JavaScript frameworks
 favicon	JavaScript frameworks
 React Router 6	JavaScript frameworks
 PWA	Miscellaneous
 Webpack	Miscellaneous
 Module Federation	Miscellaneous
 DigiCert	SSL/TLS certificate authorities
 Netlify	PaaS, CDN
 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-Fingerprint\\_Web\\_Server.html](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 - 2017 : A6 - Security Misconfiguration  
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

#### Screenshot:

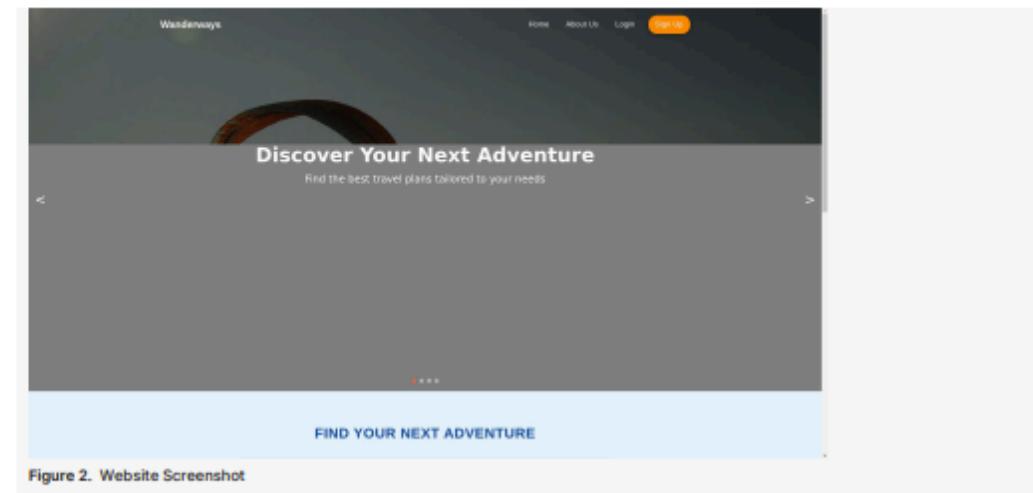


Figure 2. Website Screenshot

### Spider results

URL	Method	Page Title	Page Size	Status Code
<a href="https://wanderways-travel.netlify.app/">https://wanderways-travel.netlify.app/</a>	GET	Wanderways	650 B	200
<a href="https://wanderways-travel.netlify.app/manifest.json">https://wanderways-travel.netlify.app/manifest.json</a>	GET		492 B	200
<a href="https://wanderways-travel.netlify.app/static">https://wanderways-travel.netlify.app/static</a>	GET	Wanderways	650 B	200
<a href="https://wanderways-travel.netlify.app/static/">https://wanderways-travel.netlify.app/static/</a>	GET	Wanderways	650 B	200
<a href="https://wanderways-travel.netlify.app/static/css">https://wanderways-travel.netlify.app/static/css</a>	GET	Wanderways	650 B	200
<a href="https://wanderways-travel.netlify.app/static/css/">https://wanderways-travel.netlify.app/static/css/</a>	GET	Wanderways	650 B	200
<a href="https://wanderways-travel.netlify.app/static/js">https://wanderways-travel.netlify.app/static/js</a>	GET	Wanderways	650 B	200
<a href="https://wanderways-travel.netlify.app/static/js/">https://wanderways-travel.netlify.app/static/js/</a>	GET	Wanderways	650 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)

### Website is accessible.

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

### Nothing was found for client access policies.

### 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 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 (37/37)

- ✓ Starting the scan...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ 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 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://wanderways-travel.netlify.app/
scan_type: Light
authentication: False
```

**Scan stats**

Unique Injection Points Detected:	2
URLs spidered:	8
Total number of HTTP requests:	39
Average time until a response was received:	163ms