

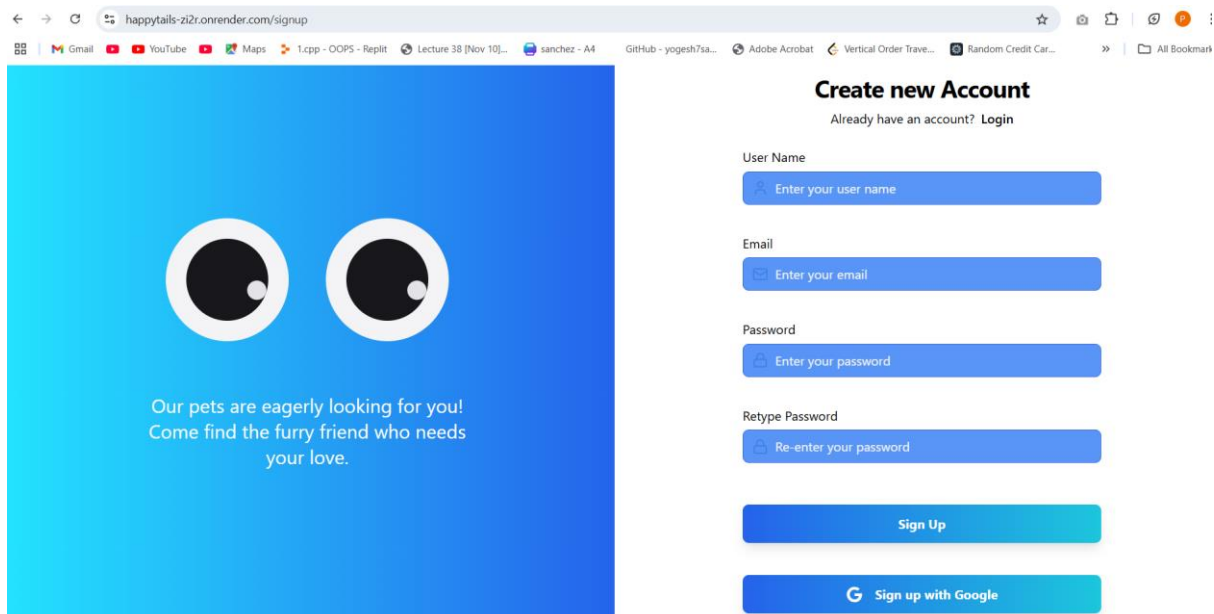
G1 : Pet Adoption System

Non-Functional Testing :

1) Compatibility check:

Compatibility Check refers to the process of ensuring that a software application or system works correctly across different environments, platforms, devices, and configurations. This testing aims to verify that the software behaves as expected under various conditions, ensuring a seamless user experience.

Windows:



The screenshot shows a web browser window with the URL `happytails-z12r.onrender.com/signup`. The page has a blue gradient background on the left with two large white eyes and the text "Our pets are eagerly looking for you! Come find the furry friend who needs your love." On the right, there is a "Create new Account" form. The form includes a link "Already have an account? Login", input fields for "User Name", "Email", "Password", and "Retype Password", a "Sign Up" button, and a "Sign up with Google" button.

Mobile view:



The screenshot shows the same "Create new Account" form on a mobile device. The form is centered and takes up most of the screen. It includes the same "Already have an account? Login" link, input fields for "User Name", "Email", "Password", and "Retype Password", a "Sign Up" button, and a "Sign up with Google" button. The mobile interface shows a status bar at the top with the time 9:51 and a home indicator at the bottom.

2) Load Testing using Jmeter:

Load Testing with JMeter is a process of evaluating the performance of a system by simulating multiple users accessing it simultaneously. Apache JMeter is a popular open-source tool for load testing, especially for web applications and APIs.

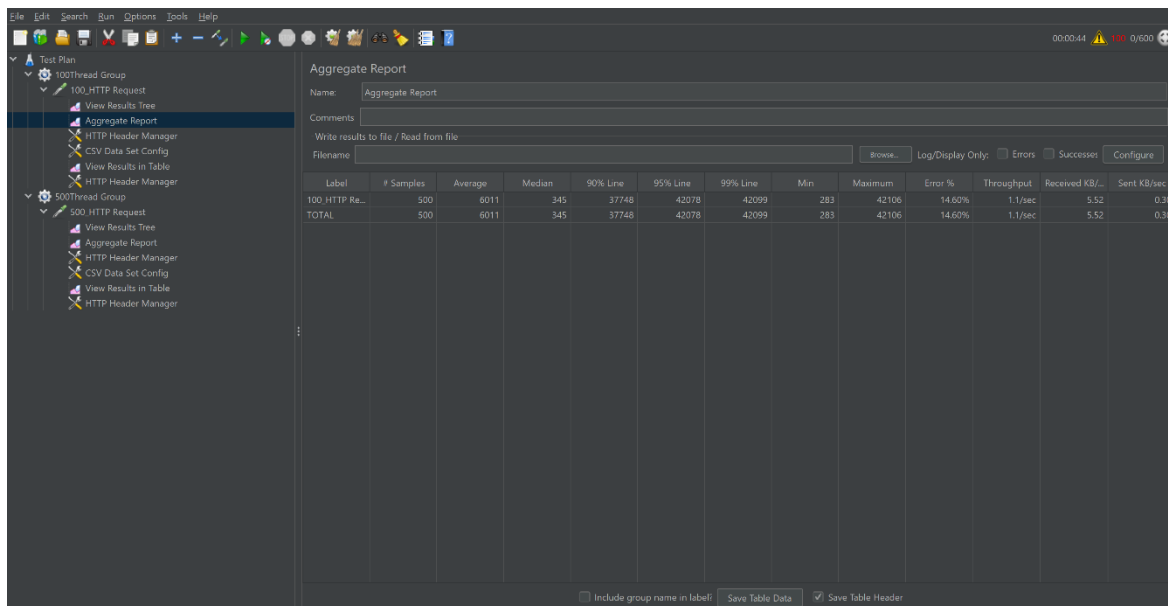
Here I use it using the JDK and apache Jmeter 5.6.3

Here I consider some of the post method which are no dependent on the authentication and token things. So in all the get user in backend we use the only Post methos which are not token dependent.

I use the different post method for it like:

1) Sign Up:

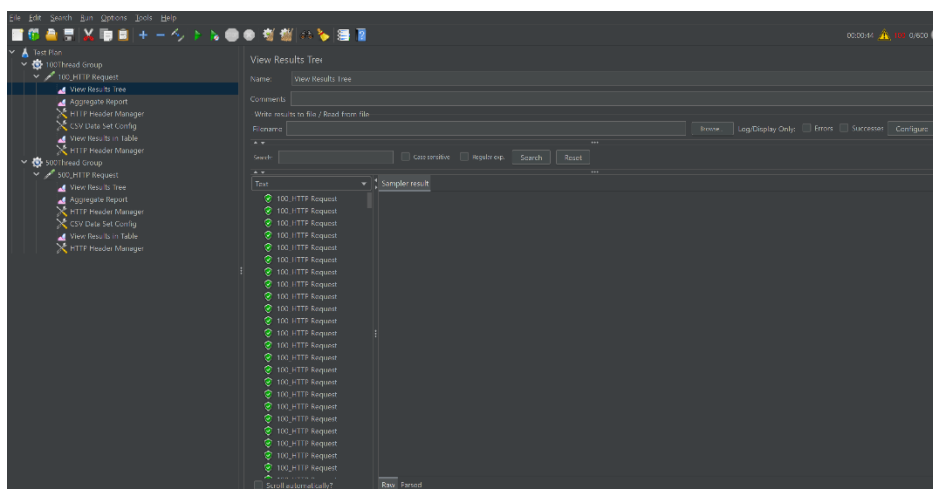
100 user:



The screenshot shows the Apache JMeter 5.6.3 interface. The left sidebar displays a test plan with a '100Thread Group' containing a '100 HTTP Request' element. The main panel shows the 'Aggregate Report' for this test. The report includes a table with the following data:

Label	# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Maximum	Error %	Throughput	Received KB/s	Sent KB/sec
100 HTTP Re...	500	6011	345	37748	42078	42099	283	42106	14.60%	1.1/sec	5.52	0.30
TOTAL	500	6011	345	37748	42078	42099	283	42106	14.60%	1.1/sec	5.52	0.30

At the bottom of the report, there are checkboxes for 'Include group name in label', 'Save Table Data', and 'Save Table Header'.



The screenshot shows the Apache JMeter 5.6.3 interface. The left sidebar displays a test plan with a '100Thread Group' containing a '100 HTTP Request' element. The main panel shows the 'View Results Tree' for this test. The tree displays a list of 100 HTTP requests, each with a green status icon and a 'Sample result' label. The bottom of the tree shows a 'Raw Panel' with a 'Start/End Automatically?' checkbox.

[illegible]

2) **NewPassword** post method:-

FileEditSearchRunOptionsToolsHelp

Test Plan

Thread Group

HTTP Request

View Results Tree

Aggregate Report

HTTP Header Manager

CSV Data Set Config

View Results in Table

00:00:03

0

0/100

Aggregate Report

Name:Aggregate Report

Comments

Write results to file / Read from file

Filename

Browser

Log/Display Only

Errors

Successes

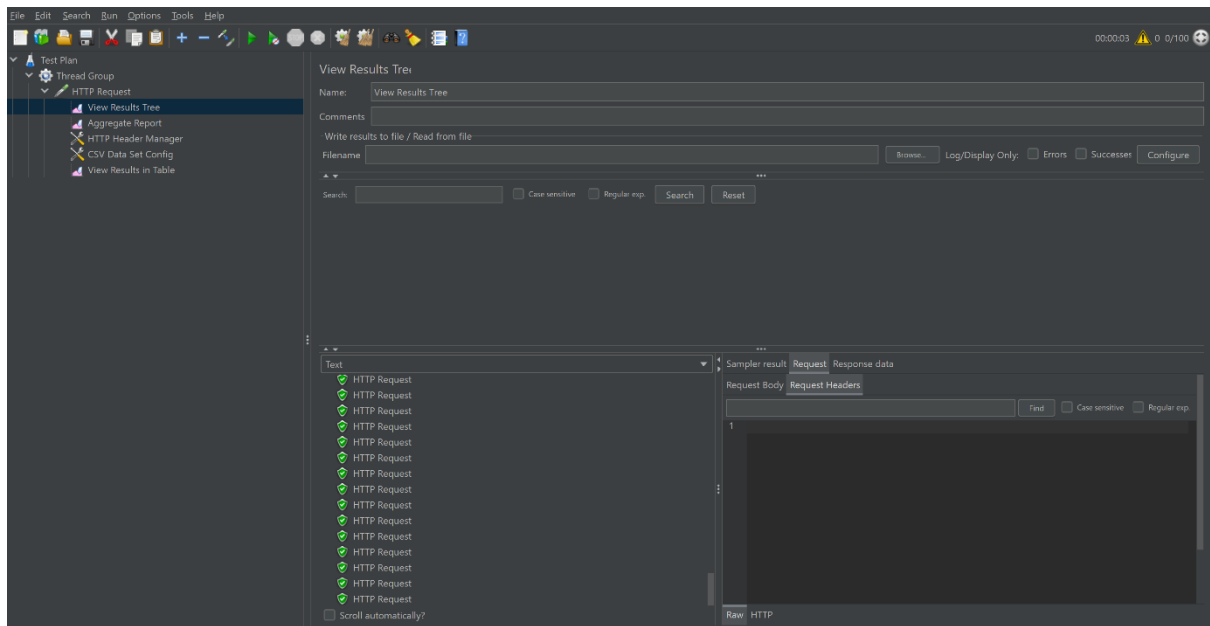
Configure

Label	# Samples ↑	Average	Median	90% Line	95% Line	99% Line	Min	Maximum	Error %	Throughput	Received KB/sec	Sent KB/sec
HTTP Request	100	376	336	526	620	698	291	924	0.00%	28.0/sec	8.75	8.86
TOTAL	100	376	336	526	620	698	291	924	0.00%	28.0/sec	8.75	8.86

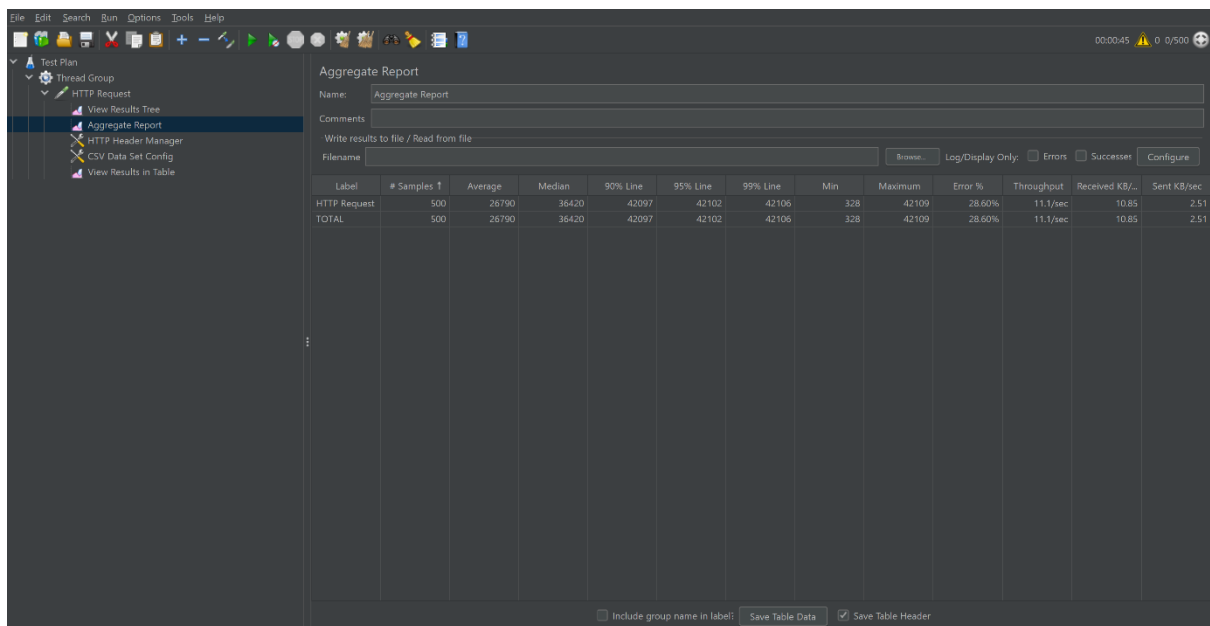
Include group name in label:

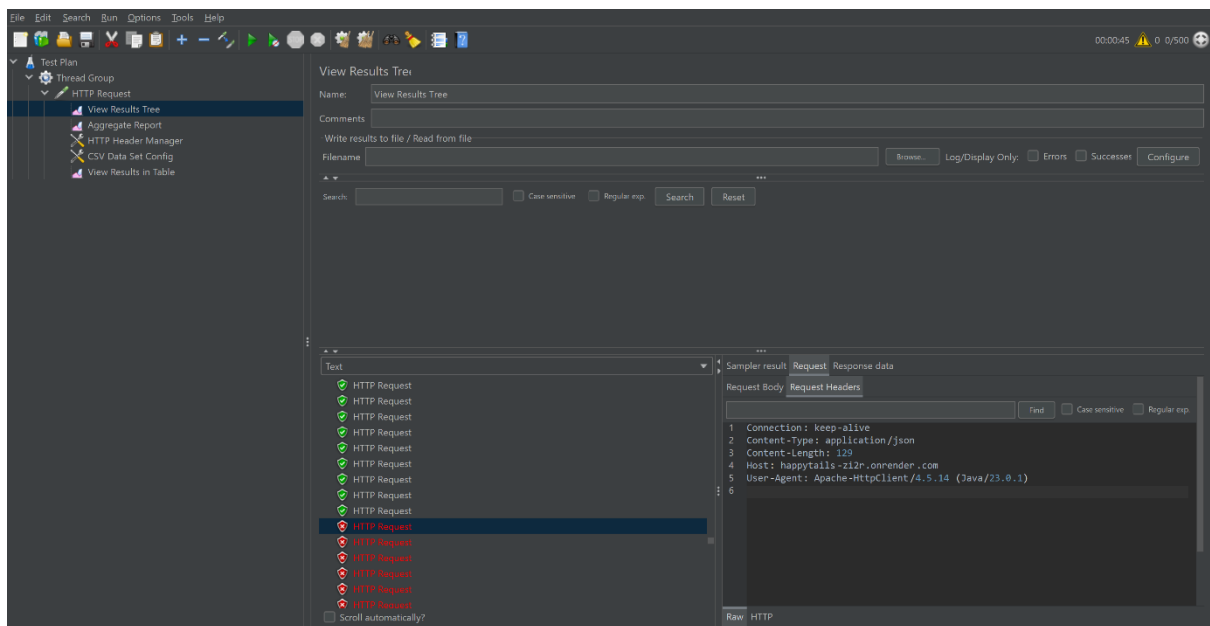
Save Table Data

Save Table Header



500 users:

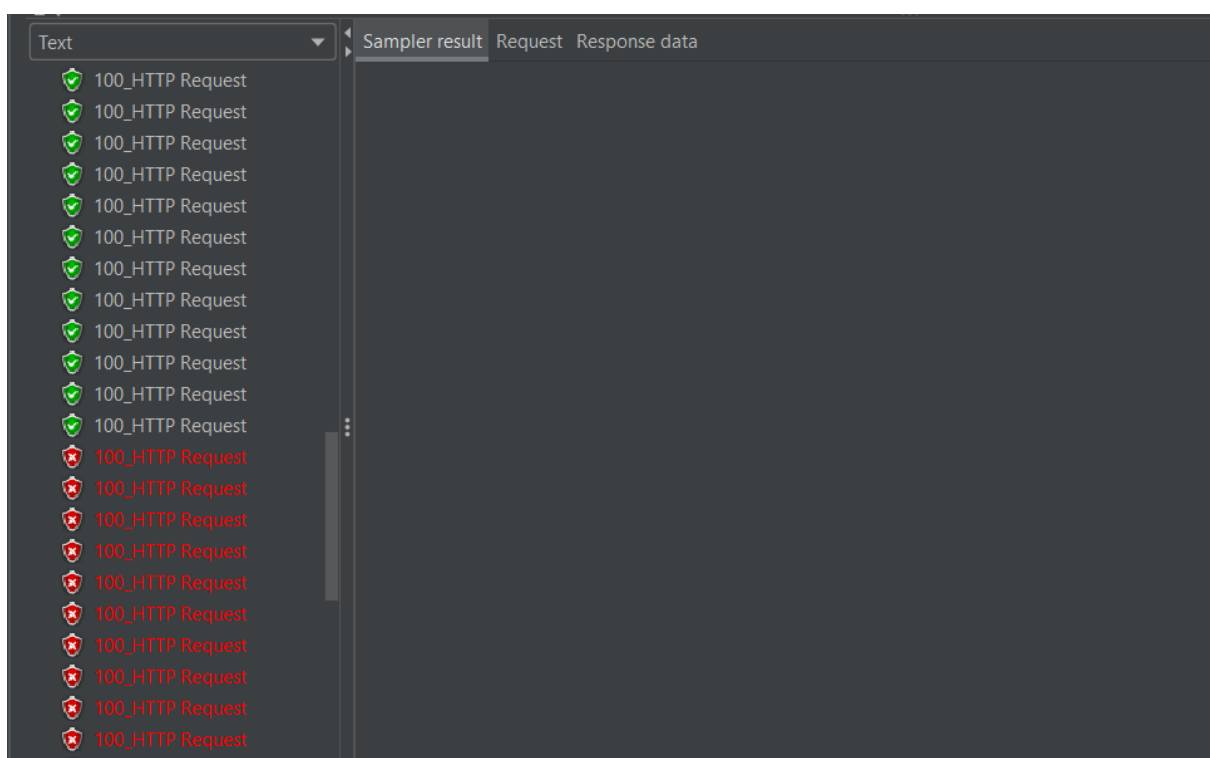




3) VarifyOTP:

100 users:

Label	# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Maximum	Error %	Throughput	Received KB/...	Sent KB/sec
100_HTTP Re...	100	29146	36433	42081	42087	42094	435	42095	41.00%	2.2/sec	2.81	0.31
TOTAL	100	29146	36433	42081	42087	42094	435	42095	41.00%	2.2/sec	2.81	0.31



500 users:

[illegible]

FileEditSearchRunOptionsToolsHelp

Test Plan

Thread Group

View Results Tree

Aggregate Report

HTTP Header Manager

CSV Data Set Config

View Results in Table

00:00:44

0/500

View Results in Table

Name:

View Results in Table

Comments

Write results to file / Read from file

Filename

Browse...

Log/Display Only:

☐ Errors
☐ Successes

Configure

Sample #	Start Time	Thread Name	Label	Sample Time(ms)	Status	Bytes	Sent Bytes	Latency	Connect Time(ms)
351	04:58:08.081	Thread Group 1-3..	HTTP Request	36453		321	258	36453	36077
352	04:58:07.860	Thread Group 1-3..	HTTP Request	36674		321	258	36674	36064
353	04:58:07.891	Thread Group 1-3..	HTTP Request	36667		321	258	36667	36062
354	04:58:08.159	Thread Group 1-3..	HTTP Request	36422		321	258	36422	36073
355	04:58:07.991	Thread Group 1-3..	HTTP Request	36670		321	258	36670	36057
356	04:58:08.057	Thread Group 1-3..	HTTP Request	36702		321	258	36702	36084
357	04:58:08.118	Thread Group 1-3..	HTTP Request	36678		321	258	36678	36081
358	04:58:08.142	Thread Group 1-3..	HTTP Request	42079		2711	0	0	42079
359	04:58:08.147	Thread Group 1-3..	HTTP Request	42074		2711	0	0	42074
360	04:58:08.123	Thread Group 1-3..	HTTP Request	42098		2711	0	0	42098
361	04:58:08.154	Thread Group 1-3..	HTTP Request	42067		2711	0	0	42067
362	04:58:08.170	Thread Group 1-3..	HTTP Request	42067		2711	0	0	42067
363	04:58:08.165	Thread Group 1-3..	HTTP Request	42088		2711	0	0	42088
364	04:58:08.182	Thread Group 1-3..	HTTP Request	42086		2711	0	0	42086
365	04:58:08.176	Thread Group 1-3..	HTTP Request	42092		2711	0	0	42092
366	04:58:08.190	Thread Group 1-3..	HTTP Request	42076		2711	0	0	42076
367	04:58:08.194	Thread Group 1-3..	HTTP Request	42090		2711	0	0	42090
368	04:58:08.201	Thread Group 1-3..	HTTP Request	42083		2711	0	0	42083
369	04:58:08.236	Thread Group 1-3..	HTTP Request	42080		2711	0	0	42080
370	04:58:08.230	Thread Group 1-3..	HTTP Request	42086		2711	0	0	42086
371	04:58:08.224	Thread Group 1-3..	HTTP Request	42092		2711	0	0	42092
372	04:58:08.207	Thread Group 1-3..	HTTP Request	42093		2711	0	0	42093
373	04:58:08.213	Thread Group 1-3..	HTTP Request	42087		2711	0	0	42087
374	04:58:08.219	Thread Group 1-3..	HTTP Request	42081		2711	0	0	42081
375	04:58:08.243	Thread Group 1-3..	HTTP Request	42089		2711	0	0	42089

☐ Scroll automatically?
☐ Child samples?

No of Samples 1000

Lastest Sample 42098

Message 32041

Deviation 18389

4) Forgot password post methods:

[illegible]

The screenshot shows the Burp Suite interface with the 'Request' tab selected. The 'Request Body' section displays the following content:

```

1 POST http://happy-tails-o089.onrender.com/forgotpassword
2
3 POST data:
4 {
5     "email": "user1700@example.com",
6     "otp": "${OTP}"
7 }
8
9
10 [no cookies]
11

```

Website Vulnerability Scanner Report

✓ <https://happytails-zi2r.onrender.com/signup>

! 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: 3

Info: 16

Scan information:

Start time: Dec 02, 2024 / 21:51:52 UTC+0530

Finish time: Dec 02, 2024 / 21:52:13 UTC+0530

Scan duration: 21 sec

Tests performed: 19/19

Scan status: **Finished**

Findings

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
https://happytails-zi2r.onrender.com/signup	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](#)

Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
https://happytails-zi2r.onrender.com/signup	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](#)

Server software and technology found

UNCONFIRMED ⓘ

Software / Version	Category
 HTTP/3	Miscellaneous
 Lucide	Font scripts
 React	JavaScript frameworks
 React Router 6	JavaScript frameworks
 Vite	Miscellaneous
 Cloudflare	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

Classification:

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

Security.txt file is missing

CONFIRMED

URL
Missing: https://happytails-zl2r.onrender.com/.well-known/security.txt

▼ Details

Risk description:

There is no particular risk in not having a 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 - 2017 : [A6 - Security Misconfiguration](#)
OWASP Top 10 - 2021 : [A5 - 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 enabled HTTP OPTIONS method.
 - 🚩 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-Content-Type-Options.
 - 🚩 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)

- ✓ Starting the scan...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ 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 enabled HTTP OPTIONS method...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ 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://happytails-zi2r.onrender.com/signup
scan_type: Light
authentication: False

Scan stats

Unique Injection Points Detected:	1
URLs spidered:	1
Total number of HTTP requests:	10
Average time until a response was received:	207ms
