

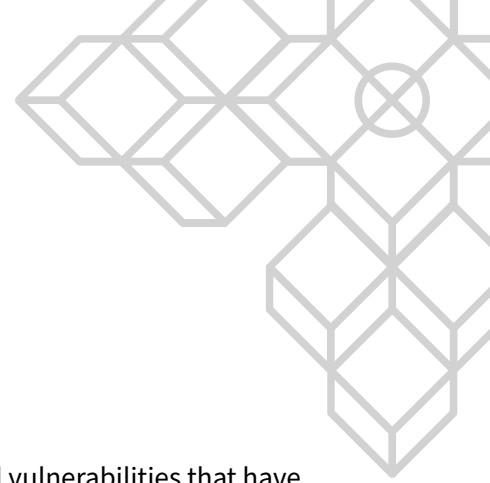


# **Terraformer Web Penetration Test Report**

Prepared for Terraformer, 8 April 2022

# Table of Contents

<b>Introduction</b>	<b>3</b>
Scope . . . . .	3
Conclusion . . . . .	3
Methodologies . . . . .	4
<b>Vulnerabilities Summary</b>	<b>5</b>
<b>Detailed Vulnerabilities</b>	<b>6</b>
Vulnerability 1: Leaking email addresses from newsletter subscribers . . . . .	6
Vulnerability 2: Additional web server exposed . . . . .	9
Vulnerability 3: HSTS not enforced on URL path . . . . .	10
Vulnerability 4: Lack of WAF - Web Application Firewall . . . . .	11
Vulnerability 5: Depending on Terra's public infrastructure to operate . . . . .	12
Vulnerability 6: Server headers information disclosure . . . . .	13
<b>Document control</b>	<b>14</b>
<b>Appendices</b>	<b>15</b>
Appendix A: Report Disclaimer . . . . .	15
Appendix B: Risk assessment methodology . . . . .	16



## Introduction

SCV was engaged by Terraformer to assist in identifying security threats and vulnerabilities that have the potential to affect their security posture. Additionally, SCV will assist the team in understanding the risks and identifying potential mitigations.

Terraformer is a protocol that offers aggregated solutions for DeFi and NFT. This includes trading, yield farming, data and analytics, launchpad, and NFT marketplace, built on the Terra ecosystem.

## Scope

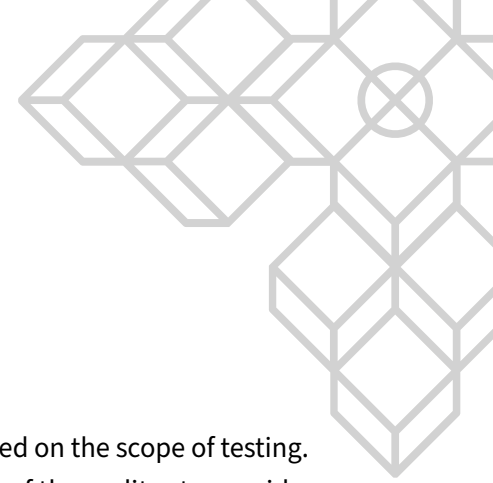
SCV performed the security assessment on the following items:

- [ftm.com](https://ftm.com)
- [terraroutes.com](https://terraroutes.com)

The KYC 3rd party provider and related endpoints ([api.ftm.com](https://api.ftm.com)) were not part of the scope and were excluded from this testing engagement.

## Conclusion

The identified vulnerabilities pose a *low* to *none* level of technical risk to Terraformer and users. Remediations were effectively applied by Terraformer team and reviewed by SCV.



## Methodologies

SCV performed a combination of automated and manual security testing based on the scope of testing. The testing performed is based on the extensive experience and knowledge of the auditor to provide the greatest coverage and value to Terraformer.

This will include the identification and enumeration of the application, identifying vulnerabilities, exploiting identified vulnerabilities, and then analysing and reporting on the results.

Our methodology is based on multiple industry recognised methodologies including OWASP but is not limited to the following:

- Broken Access Control;
- Cryptographic Failures;
- Injection;
- Insecure Design;
- Security Misconfiguration;
- Vulnerable and Outdated Components;
- Identification and Authentication Failures;
- Software and Data Integrity Failures;
- Security Logging and Monitoring Failures;
- Server-Side Request Forgery.

## Vulnerabilities Summary

	Title and Summary	Risk	Status
1	Leaking email addresses from newsletter subscribers	High	Remediated
2	Additional web server exposed	Low	Remediated
3	HSTS not enforced on URL path	Low	Remediated
4	Lack of WAF - Web Application Firewall	Low	Acknowledged
5	Depending on Terra's public infrastructure to operate	Informational	Acknowledged
6	Server headers information disclosure	Informational	Remediated

## Detailed Vulnerabilities

### Vulnerability 1: Leaking email addresses from newsletter subscribers

Likelihood	Impact	Risk
Likely	Severe	High

#### Description

Users have the ability to subscribe to a newsletter using an email address to receive updates.


The design implementation is not secure as it fails to protect subscribers data due a vulnerability caused by an insecure implementation of **Google Spreadsheets** that is used to track email subscriptions requests.

An attacker can reuse the *Bearer Token* from *Google Spreadsheets* response and self-grant reading and writing permissions to the spreadsheet using the following IAM account:

- `googlesheetseditor@terraformer-331708.iam.gserviceaccount.com`.

Bad actors could use the data to perform spear phishing (phishing emails) attacks aiming to steal funds from others users by impersonation or lure them to a scam web site.

## Request

Pretty Raw Hex  \n 

[illegible]

ⓘ ⚙ ⬅ ➡ Search...

## Response

Pretty Raw Hex Render **≡** ↻ ≡

```
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=UTF-8
3 Vary: Origin
4 Vary: X-Origin
5 Vary: Referer
6 Date: Tue, 29 Mar 2022 12:04:28 GMT
7 Server: ESF
8 Cache-Control: private
9 Content-Length: 130911
10 X-Xss-Protection: 0
11 X-Frame-Options: SAMEORIGIN
12 X-Content-Type-Options: nosniff
13 Access-Control-Allow-Origin: https://tfm.com
14 Access-Control-Expose-Headers: vary,vary,vary,content-encoding,date,server,content-length
15 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"
16
17 {
18   "range": "Newsletter!A2:A3422",
19   "majorDimension": "ROWS",
20   "values": [
```

### Figure 1: Requests and Response

## **Recommendations**

Consider moving the data from *Google Spreadsheets* also to the already solution in-use *Mailjet*.



## Vulnerability 2: Additional web server exposed

Likelihood	Impact	Risk
Rare	Low	Low

### Description

The *terraroutes.com* host has another web server running into the *8083/TCP* that appears to have no functionality.

Server header also exposes software versions as per figure below:

```
> curl -I terraroutes.com:8083
HTTP/1.0 404 NOT FOUND
Content-Type: text/html; charset=utf-8
Content-Length: 232
Access-Control-Allow-Origin: *
Server: Werkzeug/2.0.3 Python/3.8.10
Date: Fri, 01 Apr 2022 03:17:08 GMT
```

**Figure 2:** Server header response

Exposed versions could facilitate an attack in case a public exploit is known for the particular running version.

### Recommendations

If the web server is no longer required remove it from the public access.

## Vulnerability 3: HSTS not enforced on URL path

Likelihood	Impact	Risk
Rare	Moderate	Low

### Description

By the definition, the HTTP **Strict-Transport-Security** response header informs browsers that the site should only be accessed using HTTPS, and that any future attempts to access it using HTTP should automatically be converted to HTTPS.

HSTS could also prevent in the *MiTM* (Man-in-the-Middle) attacks from being exploitable.

The host *terraformer.com* does not enforce the use of HSTS on the following paths:

- /swap
- /route

### Recommendations

Ensure the HSTS is well configured across the entire website. For more information on its implementation, can be found the following link:

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>

## Vulnerability 4: Lack of WAF - Web Application Firewall

Likelihood	Impact	Risk
Rare	Low	Low

### Notes

Resource will be moved to Cloudflare in the neat future or next releases Terraformer team advices.

### Description

The *terrارoutes.com* host resolves to the following IP address *157.230.105.20* that seems to be hosted by **Digital Ocean** in the *Europe/Berlin* pod.

Since there is no protection when reaching *terrارoutes.com*, an attacker could potentially overload the server by sending a large number of requests that would likely cause some network disruptions and consequentially would impact the server and services it offers.

### Recommendations

Ensure the endpoint is not exposed directly to the internet by deploying a WAF in front.

## Vulnerability 5: Depending on Terra's public infrastructure to operate

Likelihood	Impact	Risk
Rare	Informational	Informational

### Notes

Terraformer team is planning to deploy their own node and infrastructure that does not depending on the TFL public nodes.

### Description

The Terraformer frontend depends on the public **LCD** and **FCD** to operate while interacting with Terra chain.

Terra's public infrastructure is a well known and receives a significant amount of demand causing performance issues on occasion.

Terraformer could experience downtime and/or significant delays using this public node, affecting their user's perception of the service.

### Recommendations

It is recommended that Terraformer deploys the required infrastructure exclusively for their needs and use the public ones from Terra as a fallback.

By using a dedicate node, Terraformer will have greater control over the performance of their service. Which will also contribute to the further decentralization of the Terra ecosystem they rely on.

## Vulnerability 6: Server headers information disclosure

Likelihood	Impact	Risk
Rare	Informational	Informational

### Description

The *terrارoutes.com* host appears to be running behind a reverse proxy using Nginx to fetch the upstream backend.

When requested, the server response carry a header containing the running version of Nginx (*nginx/1.18.0*).

While this poses no directly risk impact to Terraformer, it could facilitate an exploit attempt by knowing exactly what version to target and consequentially increases the attack surface.

### Recommendations

Configure the reverse proxy to hide it's version by setting the `server_tokens` parameter to `off` at the `nginx.conf` file.

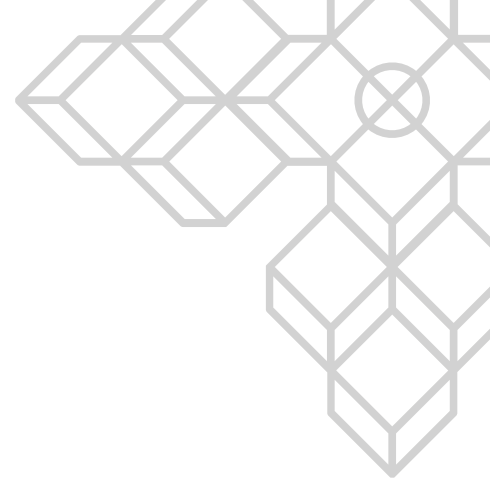
# Document control

## Document changes

Version	Date	Name	Changes
0.1	2022-04-05	Vinicius Marino	Initial report
0.2	2022-04-06	Vinicius Marino	Team communication and Pre-Release
1.0	2022-04-08	Vinicius Marino	Final Document Release

## Document contributors

Name	Role	Email address
Vinicius Marino	Security Specialist	vini@scv.services



# Appendices

## Appendix A: Report Disclaimer

The content of this audit report is provided “As is”, without representations and warranties of any kind.

The author and their employer disclaim any liability for damage arising out of, or in connection with, this audit report.

Copyright of this report remains with the author.

## Appendix B: Risk assessment methodology

A qualitative risk assessment is performed on each vulnerability to determine the impact and likelihood of each.

Risk rate will be calculated on a scale. As per criteria Likelihood vs Impact table below:

<b>Likelihood</b>	<b>Rare</b>	<b>Unlikely</b>	<b>Possible</b>	<b>Likely</b>
<b>Impact</b>				
<b>Critical</b>	<b>Medium</b>	<b>High</b>	<b>Critical</b>	<b>Critical</b>
<b>Severe</b>	<b>Low</b>	<b>Medium</b>	<b>High</b>	<b>High</b>
<b>Moderate</b>	<b>Low</b>	<b>Medium</b>	<b>Medium</b>	<b>High</b>
<b>Low</b>	<b>Low</b>	<b>Low</b>	<b>Low</b>	<b>Medium</b>
<b>Informational</b>	<b>Informational</b>	<b>Informational</b>	<b>Informational</b>	<b>Informational</b>

### LIKELIHOOD:

- **Likely:** likely a security incident will occur;
- **Possible:** It is possible a security incident can occur;
- **Unlikely:** Low probability a security incident will occur;
- **Rare:** In rare situations, a security incident can occur;

### IMPACT:

- **Critical:** May cause a significant and critical impact;
- **Severe:** May cause a severe impact;
- **Moderate:** May cause a moderated impact;
- **Low:** May cause low or none impact;
- **Informational:** May cause very low impact or none.



