Sri Lanka Institute of Information Technology

Bug Bounty Report 04

skale

IE2062 – Web Security

Submitted by:

IT22199508 – Athapaththu A.M.M.I.P

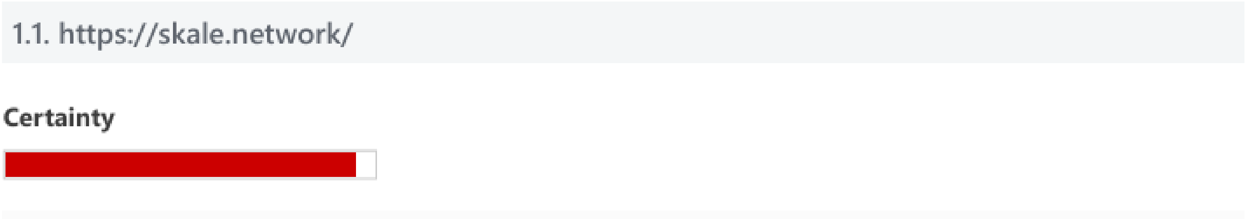
Date of submission

2024.05.04

Table of Contents

Vulnerability

1) HTTP Strict Transport Security (HSTS) Policy Not Enabled



1.1. https://skale.network/

Certainty

Date of Discovery: 20/04/2024

Date of Reporting: 21/04/2024

I am writing to inform you of a vulnerability that I have found in your website, https://skale.network/ . This vulnerability belongs to Cryptographic Failures (A02) 2021 of the OWASP top 10 vulnerabilities. This may lead to several risks of the website. You can see the detailed report of this vulnerability below.

- ## Description

Web servers can declare that all interactions by web browsers and other user agents must take place over HTTPS connections and not unsecured HTTP connections by utilizing the HTTP Strict Transport Security (HSTS) web security policy mechanism. "Strict-Transport-Security" is an HTTP response header field that the server uses to transmit the HSTS Policy to the user agent. The HSTS Policy establishes a time frame for the user agent to exclusively employ secure methods of server access. An application that does not use HSTS may be vulnerable to downgrade, SSL-stripping, man-in-the middle, and cookie-hijacking attacks.

• Impact Assessment

The following are some possible outcomes and hazards associated with the vulnerability relating to the domain www.floqast.com's lack of an activated HTTP Strict Transport Security (HSTS) policy:

1. Security Weakness: Downgrading attacks are possible in the absence of a HSTS policy, which gives hostile actors the ability to intercept or alter unprotected connections between users and the website. This may lead to security flaws that jeopardize user information.

2. Man-in-the-Middle Attacks: The website is vulnerable to man-in-the-middle (MitM) attacks in the absence of HSTS, which allow hackers to intercept and perhaps alter user-website communication. Data theft, illegal access, and other nefarious acts may result from this.

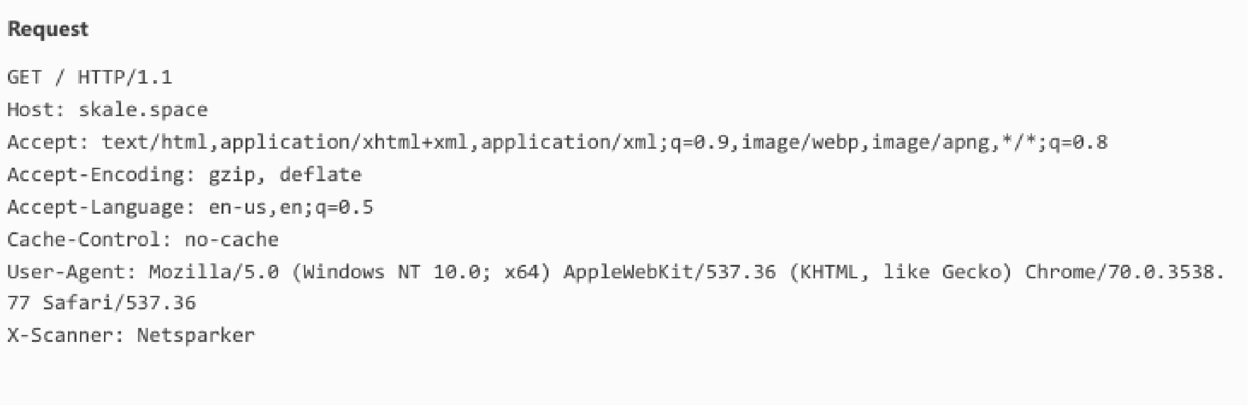
3. Phishing and Data Theft: By pretending to be www.echobox.com, cybercriminals may leverage this vulnerability to conduct phishing attacks and fool victims into disclosing sensitive information such login passwords, personal information, or bank account information. Financial losses and data theft may come from this.

4. Loss of User Trust : People anticipate private and safe internet communication. Users' confidence in the website's security may drop if HSTS isn't implemented, which may even lead them to stop visiting it altogether.

5. Regulatory Non-Compliance: Failure to implement HSTS may lead to violations of cybersecurity and data protection laws. Penalties and reputational harm are among the financial and legal repercussions that may result from this.

Turning on HSTS is essential to fixing this vulnerability. This security feature prevents downgrading attacks and improves overall security by guaranteeing that all communications with the website are encrypted and safe. Quick HSTS implementation can help the website comply with legal obligations, preserve user confidence, and protect user data. The precise consequences of this vulnerability are contingent upon the activities and potential attacks of malevolent individuals.

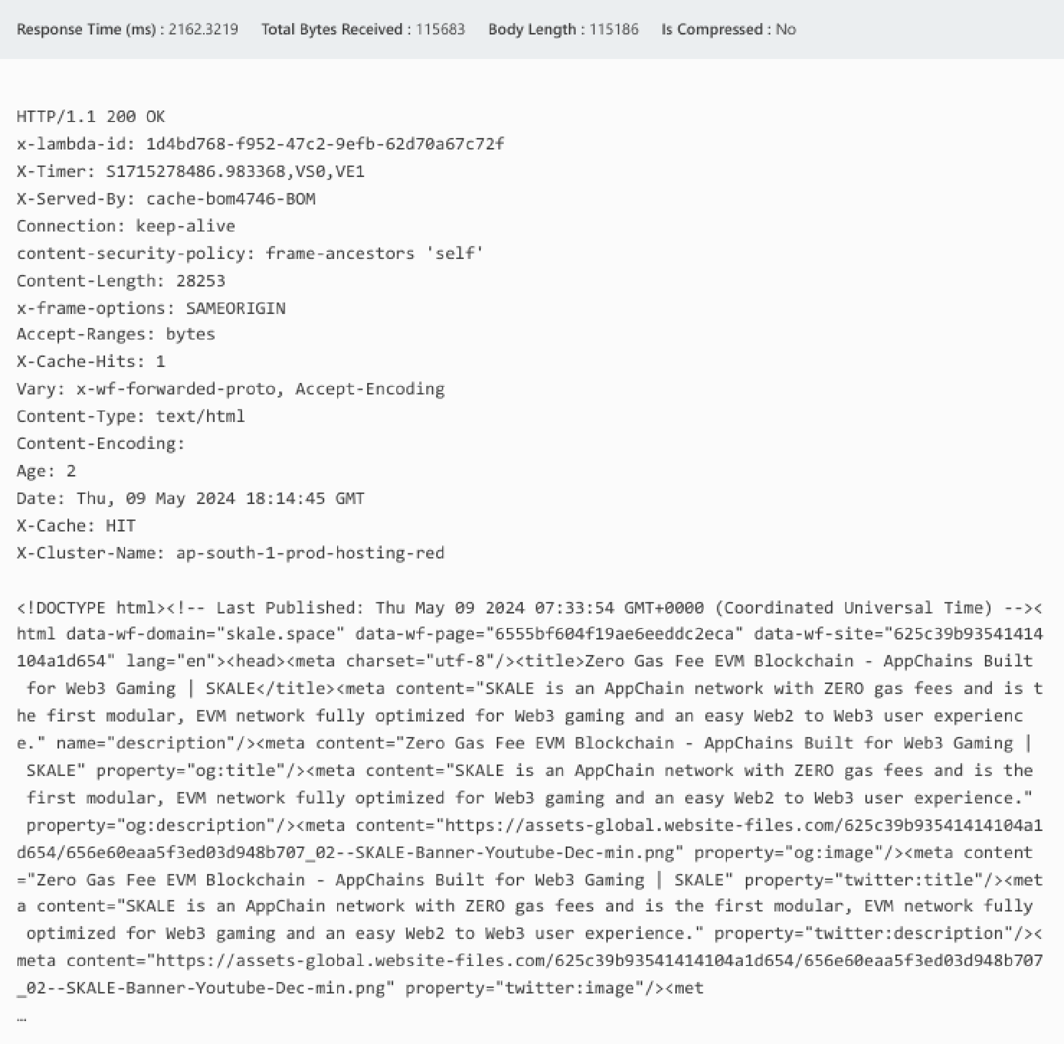
- ## Request



Request

```
GET / HTTP/1.1
Host: skale.space
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

- ## Response

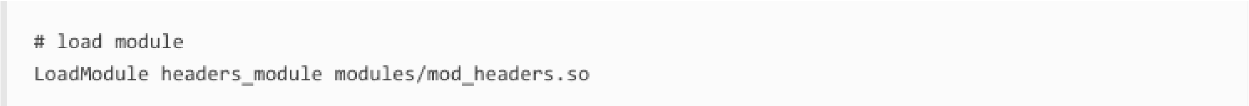


Response Time (ms) : 2162.3219 **Total Bytes Received** : 115683 **Body Length** : 115186 **Is Compressed** : No

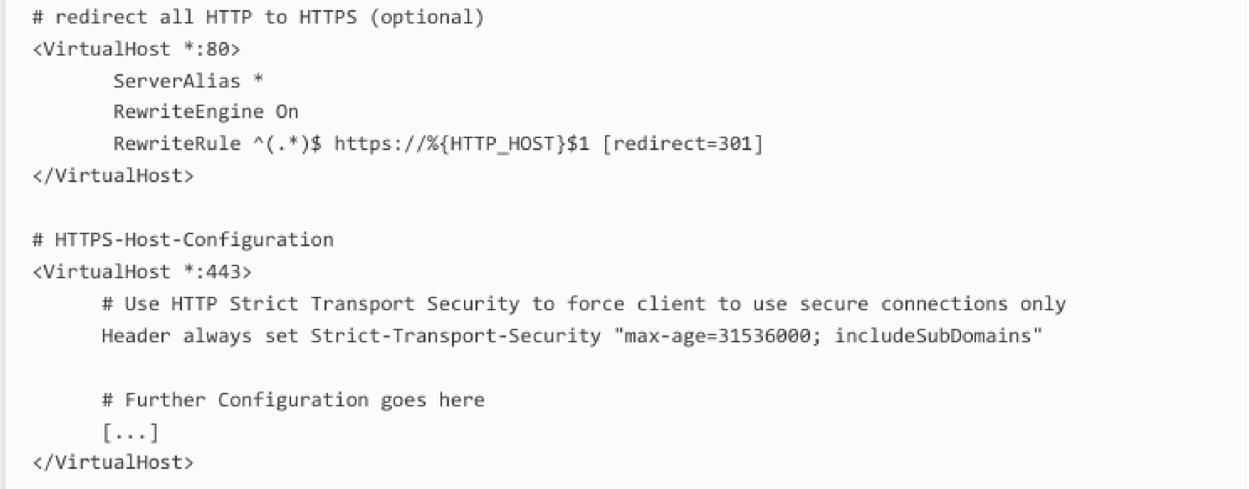
```
HTTP/1.1 200 OK
x-lambda-id: 1d4bd768-f952-47c2-9efb-62d70a67c72f
X-Timer: S1715278486.983368,VS0,VE1
X-Served-By: cache-bom4746-BOM
Connection: keep-alive
content-security-policy: frame-ancestors 'self'
Content-Length: 28253
x-frame-options: SAMEORIGIN
Accept-Ranges: bytes
X-Cache-Hits: 1
Vary: x-wf-forwarded-proto, Accept-Encoding
Content-Type: text/html
Content-Encoding:
Age: 2
Date: Thu, 09 May 2024 18:14:45 GMT
X-Cache: HIT
X-Cluster-Name: ap-south-1-prod-hosting-red

<!DOCTYPE html><!-- Last Published: Thu May 09 2024 07:33:54 GMT+0000 (Coordinated Universal Time) --><
html data-wf-domain="skale.space" data-wf-page="6555bf604f19ae6eeddc2eca" data-wf-site="625c39b93541414
104a1d654" lang="en"><head><meta charset="utf-8"/><title>Zero Gas Fee EVM Blockchain - AppChains Built
 for Web3 Gaming | SKALE</title><meta content="SKALE is an AppChain network with ZERO gas fees and is t
he first modular, EVM network fully optimized for Web3 gaming and an easy Web2 to Web3 user experienc
e." name="description"/><meta content="Zero Gas Fee EVM Blockchain - AppChains Built for Web3 Gaming |
 SKALE" property="og:title"/><meta content="SKALE is an AppChain network with ZERO gas fees and is the
 first modular, EVM network fully optimized for Web3 gaming and an easy Web2 to Web3 user experience."
 property="og:description"/><meta content="https://assets-global.website-files.com/625c39b93541414104a1
d654/656e60eaa5f3ed03d948b707_02--SKALE-Banner-Youtube-Dec-min.png" property="og:image"/><meta content
="Zero Gas Fee EVM Blockchain - AppChains Built for Web3 Gaming | SKALE" property="twitter:title"/><met
a content="SKALE is an AppChain network with ZERO gas fees and is the first modular, EVM network fully
 optimized for Web3 gaming and an easy Web2 to Web3 user experience." property="twitter:description"/><
meta content="https://assets-global.website-files.com/625c39b93541414104a1d654/656e60eaa5f3ed03d948b707
_02--SKALE-Banner-Youtube-Dec-min.png" property="twitter:image"/><met
…
```

- **Remediation**

- Configure your webserver to redirect HTTP requests to HTTPS.
- i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.



```
# load module
LoadModule headers_module modules/mod_headers.so
```



```
# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
       ServerAlias *
       RewriteEngine On
       RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

2) Internal Server Error

2.1. https://skale.network/

CONFIRMED

Date of Discovery: 20/04/2024

Date of Reporting: 21/04/2024

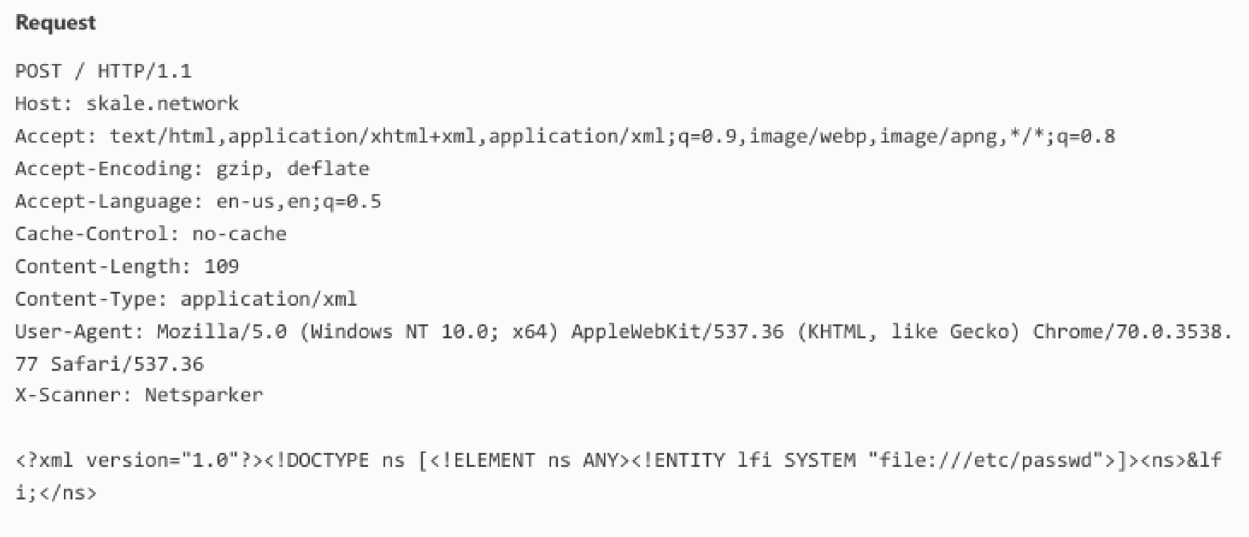
- ### Description

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

- ### Impact

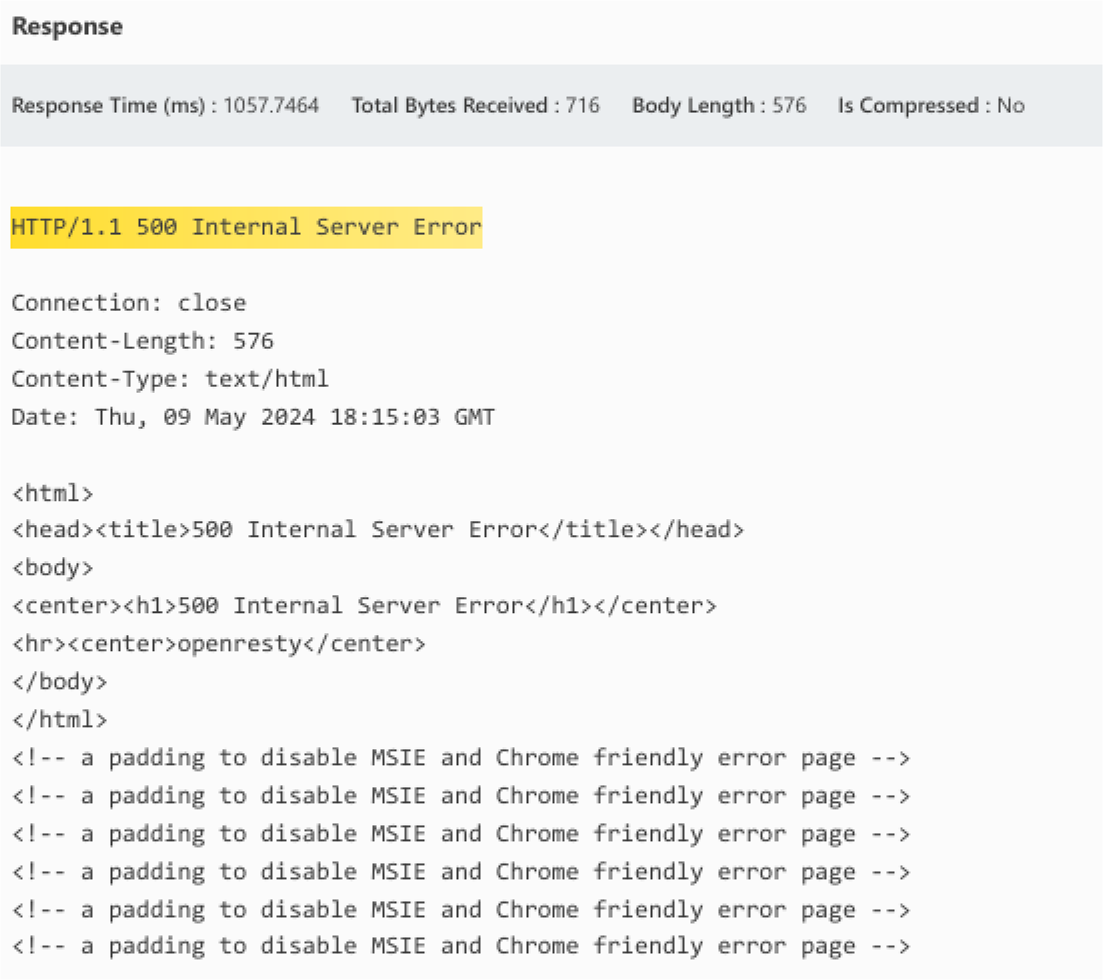
The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

- ## Proof of Concept



Request

```
POST / HTTP/1.1
Host: skale.network
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 109
Content-Type: application/xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "file:///etc/passwd">]><ns>&lf
i;</ns>
```



Response

Response Time (ms) : 1057.7464   Total Bytes Received : 716   Body Length : 576   Is Compressed : No

```
HTTP/1.1 500 Internal Server Error

Connection: close
Content-Length: 576
Content-Type: text/html
Date: Thu, 09 May 2024 18:15:03 GMT

<html>
<head><title>500 Internal Server Error</title></head>
<body>
<center><h1>500 Internal Server Error</h1></center>
<hr><center>openresty</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

- ## Remediation

- Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.