



# SLIIT

---

*Discover Your Future*

---

Sri Lanka Institute of Information Technology

## Bug Bounty Report 07

**8x8**

**IE2062 – Web Security**

Submitted by:

**IT22199508 – Athapaththu A.M.M.I.P**

Date of submission



2024.05.04

## **Table of Contents**

Vulnerability .....	3
1) HTTP Strict Transport Security (HSTS) Errors and Warnings.....	3
• Description .....	3
• Proof of Concept .....	4
• Remediation .....	5
2) Insecure Frame (External).....	6
• Description & impact Assessment .....	6
• Steps to Reproduce .....	8
• Remediation .....	9

# Vulnerability

## 1) HTTP Strict Transport Security (HSTS) Errors and Warnings

 [HTTP Strict Transport Security \(HSTS\) Errors and Warnings](#) GET <https://www.8x8.com/>

1.1. <https://www.8x8.com/>

Error	Resolution
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

Date of Discovery: 20/04/2024

Date of Reporting: 21/04/2024

- **Description**

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

● Proof of Concept

**Request**

GET / HTTP/1.1  
Host: www.8x8.com  
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) : 521.896    Total Bytes Received : 1910782    Body Length : 1910067    Is Compressed : No

HTTP/1.1 200 OK  
Age: 9213  
Cache-Control: public,max-age=0,must-revalidate  
Access-Control-Allow-Origin: \*  
Strict-Transport-Security: max-age=31536000; includeSubDomains  
X-Nf-Request-Id: 01HXGC97ZNPXTS9T725S08GMMR  
Server: Netlify  
X-Content-Type-Options: nosniff, nosniff  
X-Xss-Protection: 1; mode=block  
Vary: Accept-Encoding  
Cache-Status: "Netlify Edge"; hit  
Referrer-Policy: no-referrer-when-downgrade  
Accept-Ranges: bytes  
Content-Length: 226346  
Content-Type: text/html; charset=UTF-8  
Etag: "ce4d41f82cbe02801afdc17bf8e2da58-ssl-df"  
Content-Security-Policy: default-src 'self' \* data: blob: 'unsafe-inline' 'unsafe-eval'; object-src 'none'  
Date: Fri, 10 May 2024 04:30:49 GMT  
Content-Encoding:

<!DOCTYPE html><html lang="en"><head><meta charSet="utf-8"/><meta http-equiv="x-ua-compatible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/><script src="https://8x8.fides-cdn.ethyca.com/fides.js"></script><script>Fides.gtm()</script><script rel="preload" type="text/javascript" src="/\_scripts/dadf3a0e00c10dd096135c2af0e10e27.qualifiedPreLoad.js" data-ssr-inserted="true" pop-some="tags"></script><script async="" rel="preload" type="text/javascript" src="/\_scripts/4cb2324bfbba0f2deb9472e4fe57baf0.floodlightTagSrc.js" data-ssr-inserted="true" pop-some="tags"></script><script rel="preload" type="text/javascript" src="/\_scripts/2a42928d47374ef2138098c0dba6e9b9.floodlightTag.js" data-ssr-inserted="true" pop-some="tags"></script><script async="" rel="preload" type="text/javascript" src="/\_scripts/0a43dde06b404c49d748cec792e9de63.qualified.js" data-ssr-inserted="true" pop-some="tags"></script><meta name="generator" content="Gatsby 4.23.1"/><meta data-react-helmet="true" name="description" content="The 8x8 unified platform for contact center, business phone, video, chat, and APIs helps companies of any size deliver differentiated customer experiences."/><meta data-react-helmet="true" name="copyright" content="© 202

...

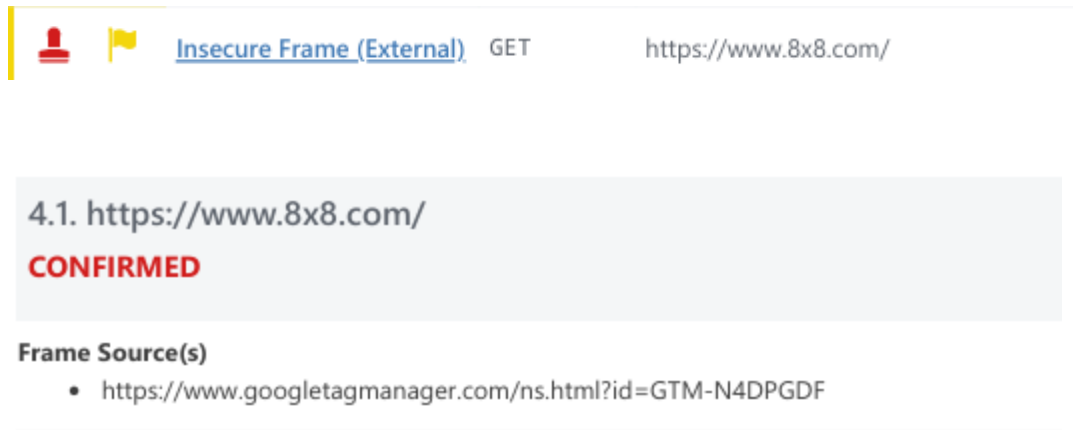
- **Remediation**



Ideally, after fixing the errors and warnings, you should consider adding your domain to the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
  - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
  - The max-age must be at least 31536000 seconds (1 year)
  - The includeSubDomains directive must be specified
  - The preload directive must be specified
  - If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

## 2) Insecure Frame (External)



  [Insecure Frame \(External\)](#) GET <https://www.8x8.com/>

4.1. <https://www.8x8.com/>  
**CONFIRMED**

**Frame Source(s)**

- <https://www.googletagmanager.com/ns.html?id=GTM-N4DPGDF>

Date of Discovery: 20/04/2024

Date of Reporting: 21/04/2024

### • Description & impact Assessment

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly

Here is an example, the URLs below all belong to the same origin as <http://site.com>:

<http://site.com>  
<http://site.com/>  
<http://site.com/my/page.html>

Whereas the URLs mentioned below aren't from the same origin as **<http://site.com>**:

<http://www.site.com> (a sub domain)  
<http://site.org> (different top level domain)  
<https://site.com> (different protocol)  
<http://site.com:8080> (different port)

When the `sandbox` attribute is set, the `iframe` content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the `iframe`.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the `sandbox` attribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure `iframe` might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the `iframe`.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

Sandbox containing a value of :

- `allow-same-origin` will not treat it as a unique origin.
- `allow-top-navigation` will allow code in the `iframe` to navigate the parent somewhere else, e.g. by changing `parent.location`.
- `allow-forms` will allow form submissions from inside the `iframe`.
- `allow-popups` will allow popups.
- `allow-scripts` will allow malicious script execution however it won't allow to create popups.

## • Steps to Reproduce

### Request

```
GET / HTTP/1.1
Host: www.8x8.com
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) : 709.5472    Total Bytes Received : 1910782    Body Length : 1910067    Is Compressed : No

```
HTTP/1.1 200 OK
Age: 9189
Cache-Control: public,max-age=0,must-revalidate
Access-Control-Allow-Origin: *
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Nf-Request-Id: 01HXGC8GF6RNRSDYPFFSME481D
Server: Netlify
X-Content-Type-Options: nosniff, nosniff
X-Xss-Protection: 1; mode=block
Vary: Accept-Encoding
Cache-Status: "Netlify Edge"; hit
Referrer-Policy: no-referrer-when-downgrade
Accept-Ranges: bytes
Content-Length: 226346
Content-Type: text/html; charset=UTF-8
Etag: "ce4d41f82cbe02801afdc17bf8e2da58-ssl-df"
Content-Security-Policy: default-src 'self' * data: blob: 'unsafe-inline' 'unsafe-eval'; object-src 'none'
Date: Fri, 10 May 2024 04:30:25 GMT
Con
...
ides-overlay-primary-active-disabled-color: #FFB6C1 !important;
--fides-overlay-primary-button-background-hover-color: #F13D4F !important;
}
</style></head><body><noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-N4DPGDF" height="0" width="0" style="display: none; visibility: hidden" aria-hidden="true"></iframe></noscript><div id="__gatsby"><div style="outline:none" tabIndex="-1" id="gatsby-focus-wrapper"><div><div><
```



- **Remediation**

- Apply sandboxing in inline frame.

```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of seamless attribute and allow-top-navigation, allow-popups and allow-scripts in sandbox attribute.