IT22199508

Sri Lanka Institute of Information Technology

Bug Bounty Report 06

Trip

IE2062 – Web Security

Submitted by:

IT22199508 – Athapaththu A.M.M.I.P

Date of submission

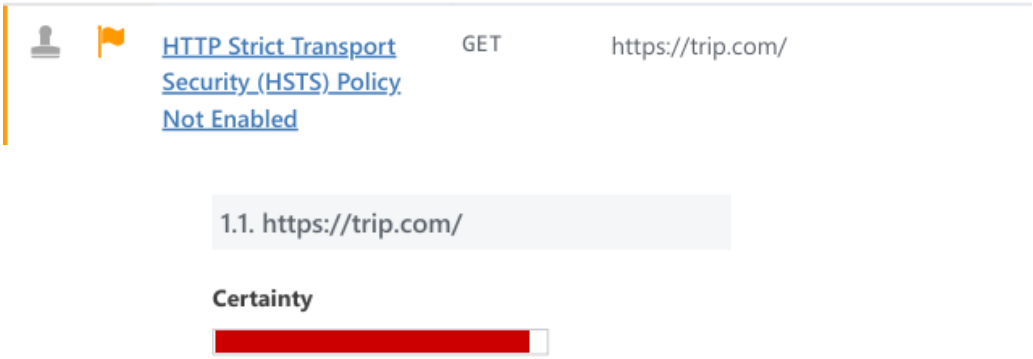
2024.05.04

Table of Contents

IT22199508

Vulnerability

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



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://trip.com/. 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.

- **Proof of Concept**

Request

```
GET / HTTP/1.1
Host: us.trip.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) : 1972.5146 Total Bytes Received : 103877 Body Length : 99128 Is Compressed : No

```
HTTP/1.1 200 OK
Server-Timing: cdn-cache; desc=MISS, edge; dur=0, origin; dur=169
x-readtime: 95
Cache-Control: no-cache, no-store, must-revalidate
ETag: W/"18338-JZ/GzfMP3fgOlMn+CtZwRW2OL4M"
Set-Cookie: UBT_VID=1714682598758.b7b3g84T2DhO;domain=.trip.com;path=/;expires=Fri, 06 Jun 2025 20:43:1
8 GMT
Set-Cookie: ibu_online_home_language_match={"isRedirect":false,"isShowSuggestion":true,"lastVisited":tr
ue,"region":"lk","redirectSymbol":false,"site_url":[],"suggestion":["en-us",""]}; Domain=trip.com; Expi
res=Fri, 02 May 2025 20:43:18 GMT
Set-Cookie: ibulanguage=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: ibulanguage=EN; Max-Age=2592000; Domain=trip.com; Path=/
Set-Cookie: ibulocale=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: ibulocale=en_us; Max-Age=2592000; Domain=trip.com; Path=/
Set-Cookie: cookiePricesDisplayed=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: cookiePricesDisplayed=USD; Max-Age=2592000; Domain=trip.com; Path=/
Set-Cookie: _abtest_userid=417941c8-44fb-46d3-a5f9-f93f74fd8093; domain=.trip.com; max-age=86400000; pa
th=/; SameSite=None; Secure
Transfer-Encoding: chunked
Server: nginx/1.20.1
unique-request-id: a7255a6f
x-trip-app-version: 2.61.0
x-xss-protection: 1; mode=block
Connection: keep-alive
Connection: Transfer-Encoding
x-download-options: noopen
Expires: 0
x-frame-options: SAMEORIGIN
Vary: Accept-Encoding
Vary: User-Agent
x-content-type-options: nosniff
x-cdn-cache: MISS
x-trip-app-idc: SHAXY
Content-Security-Policy-Report-Only: default-src * data: blob:; connect-src  https://*.tripcdn.com *.c-
ctrip.com https://*.trip.com   https://*.ctrip.com https://*.doubleclick.net https://*.google.com http
s://*.tiktok.com https://*.bing.com https://*.mapbox.com https://*.skyscanner.net https://*.tripcdn.cn
 https://*.google-analytics.com https://*.braze.com https://*.yandex.ru https://*.googleapis.com http
s://*.facebook.com https://*.googletagmanager.com https://*.gstatic.com https://wcs
…
```

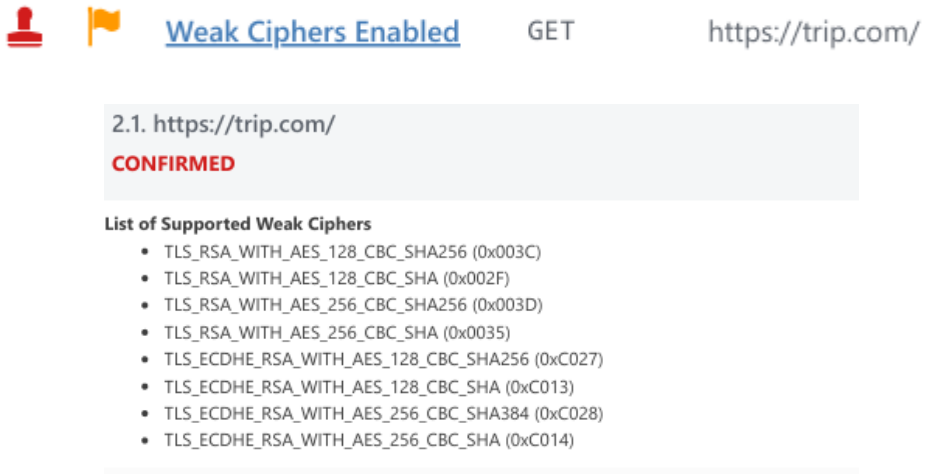
- ## Remediation

- 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>
```

IT22199508

2) Weak Ciphers Enabled



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://www.trip.com . This vulnerability belongs to the Cryptographic Failures (A02)-2021 of the OWASP top 10 vulnerabilities. This may lead to several risks to the website. You can see the detailed report of this vulnerability below.

- ## Description

When activated, weak ciphers provide a serious risk to the safety of data and computer systems. These weak encryption methods leave a gap that can be exploited by hostile actors since they are not complicated enough or strong enough to survive todays cyberattacks. Attackers can intercept, decode, and alter data by weakening the encryption used to secure sensitive information, jeopardizing the communication's secrecy and integrity. Given the importance of data security and privacy in today's linked society, this vulnerability is particularly serious. As a result, it is critical that businesses and people maintain vigilance and update their encryption procedures to prevent the security of their systems and the data they contain from ever being compromised by weak ciphers.

- ## Impact Assessment

The Weak Cipher Enabled vulnerability under the OWASP category on www.malwarebyte.com has led to the discovery of a number of potential security vulnerabilities because of the use of insufficient encryption protocols or ciphers. The following possible outcomes are all included in the significant impact of ignoring this vulnerability:

1. Loss of User Trust: Consumers put their trust in e-commerce sites like Traffic Factory to safeguard their private information. This confidence is undermined by weak ciphers that expose users' information to dangers. Traffic Factory's credibility and reputation may suffer greatly as a result, and consumer loyalty and trust may drop.

2. Data Breaches: Data breaches are more likely when ciphers are weak. Attackers may obtain sensitive user data if they are able to take advantage of these vulnerabilities, which could result in data breaches and the related financial and legal repercussions.

3. Enhanced Attack Surface: Cybercriminals can more easily exploit vulnerabilities and obtain illegal access to a website, its servers, and underlying systems when weak ciphers provide them a larger attack surface.

4. Man-in-the-Middle Attacks: Vulnerabilities in ciphers allow attackers to intercept and modify data that users exchange with websites. This poses serious security issues since it might result in data alteration and unauthorized access.

5. Data Breaches: Weak ciphers can break encryption, exposing private customer information and perhaps resulting in legal and financial repercussions for Malware Byte.

It is critical to use strong encryption techniques and ciphers to quickly resolve this Weak Cipher Enabled issue. Failing to do so puts Traffic Factory's brand, legal compliance, and general company integrity in jeopardy in addition to exposing users to potential security risks. The actions of hostile actors and the degree of the website's security flaws will determine the precise impact of this vulnerability.

- ## Proof of Concept

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

- ## Actions to take

1. For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
    a. a.Click Start, click Run, type regedt32or type regedit, and then click OK.
    b. b.In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
    c. c.Set "Enabled" DWORD to "0x0" for the following registry keys

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

- ## Remediation

Configure your web server to disallow using weak ciphers.

IT22199508