Sri Lanka Institute of Information Technology

Bug Bounty Report 018

mi

IE2062 – Web Security

Submitted by:

IT22199508 – Athapaththu A.M.M.I.P

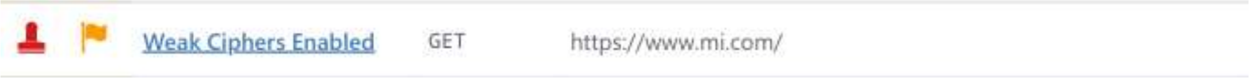
Date of submission

2024.05.04

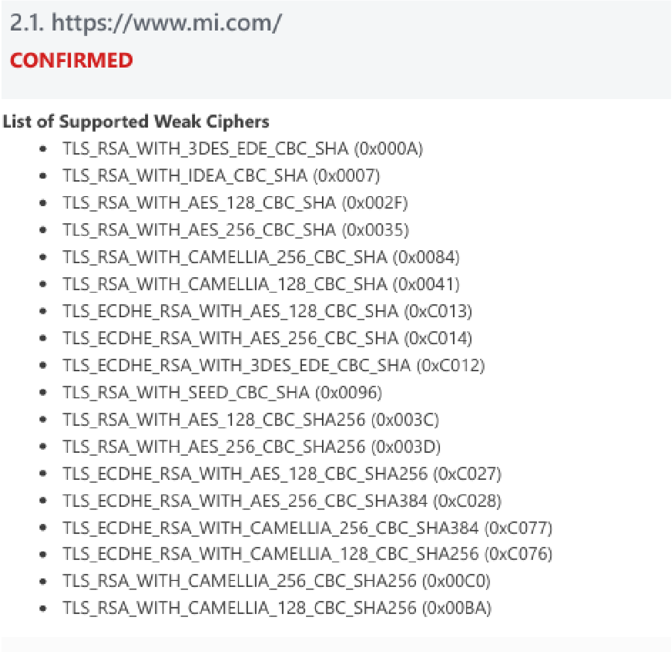
Table of Contents

Vulnerability

1) Weak Ciphers Enabled



Weak Ciphers Enabled GET https://www.mi.com/



2.1. https://www.mi.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
- TLS_RSA_WITH_IDEA_CBC_SHA (0x0007)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xC012)
- TLS_RSA_WITH_SEED_CBC_SHA (0x0096)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xC077)
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xC076)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0x00C0)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0x00BA)

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, http://mi.com/ . (A02) 2021: Cryptographic Failures shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often comes up to sensitive data exposure or system compromise. This may lead to several risks of 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 give a gap that can be exploited by hostile actors since they are not complicated enough or strong enough to survive present 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.

• Impact Assessment

Under the OWASP category connected to poor Cipher Enabled vulnerabilities within the domain of **http://mi.com**/, various potential security threats have been found due to the usage of poor encryption protocols or ciphers. The impact of not addressing this vulnerability is considerable and includes the following potential,

consequences:

1. Data Breaches: The use of weak ciphers raises the risk of data breaches. If attackers successfully infiltrate the website, they may obtain access to a goldmine of sensitive user information, leading to potential data breaches and associated legal and financial penalties.

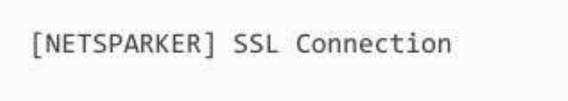
2. Regulatory Non-Compliance: Using weak ciphers may put Starbucks at variance with data protection rules and industry norms, potentially leading to legal and financial implications for non-compliance.

3. Loss of User Trust: Users expect their data to be handled securely. When weak ciphers are employed, it erodes trust in the website's security. This loss of trust can significantly damage the reputation and credibility of Starbucks and may lead to a reduction in customer confidence.

4. Enhanced Attack Surface: Weak ciphers may offer an enhanced attack surface for cybercriminals, making it easier for them to exploit weaknesses and gain unauthorized access to the website, its servers, and underlying systems.

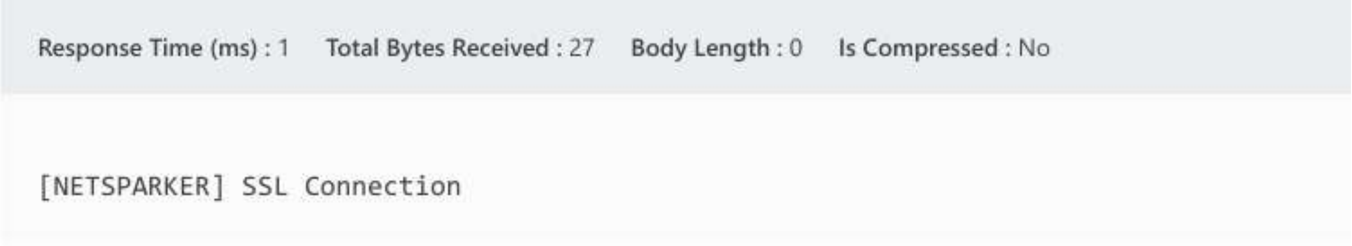
It is vital to fix this Weak Cipher Enabled issue swiftly by adopting strong encryption methods and ciphers. Failure to do so not only expose users to potential security concerns but also damages Starbucks' reputation, legal compliance, and general corporate integrity. The repercussions of the vulnerability will depend on the actions taken by hostile actors and the level of the website's security flaws.

Request



```
[NETSPARKER] SSL Connection
```

Response

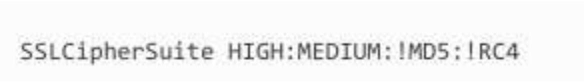


Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

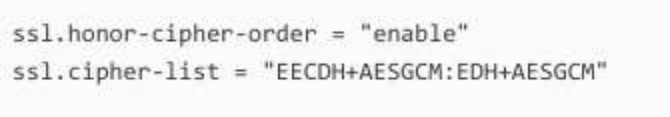
Steps to Reproduce

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



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

2. Lighttpd:



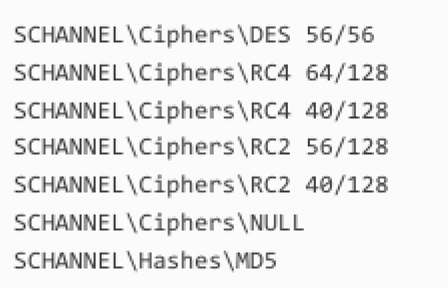
```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

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.Click Start, click Run, type regedt32or type regedit, and then click OK.

b.In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

c.Set "Enabled" DWORD to "0x0" for the following registry keys:

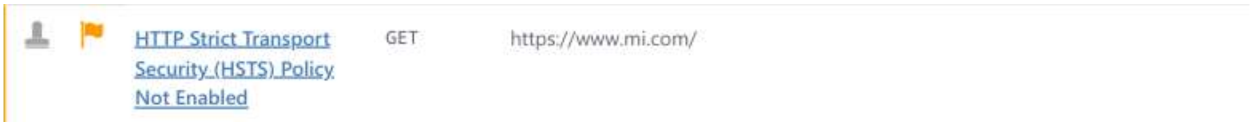


```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

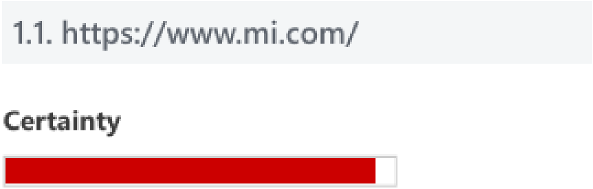
- **Remediation**

Configure your web server to disallow using weak ciphers.

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



HTTP Strict Transport Security (HSTS) Policy Not Enabled GET https://www.mi.com/



1.1. https://www.mi.com/

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://mi.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.mi.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.

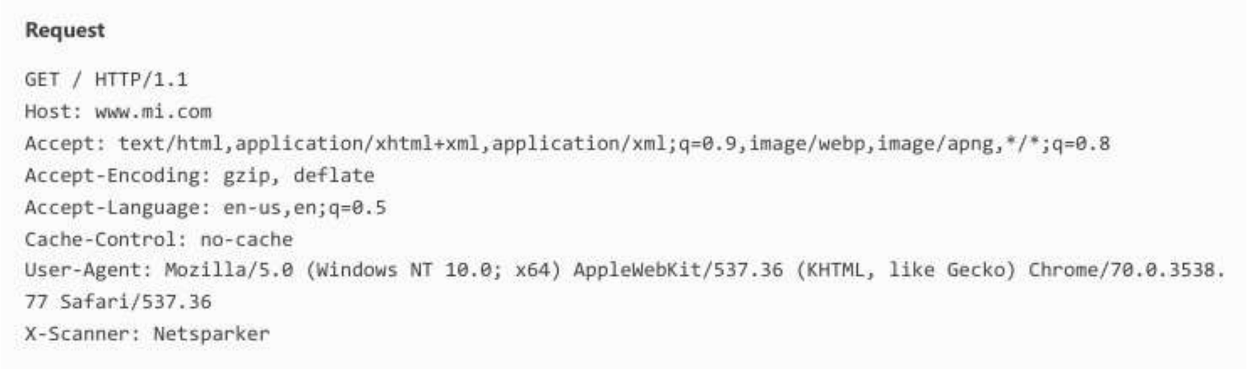
3. Phishing and Data Theft: By pretending to be www.echobox.com, cybercriminals may leverage this vulnerability to conduct phishing attacks and fool victims into disclosing sensitive information such login passwords, personal information, or bank account information. Financial losses and data theft may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

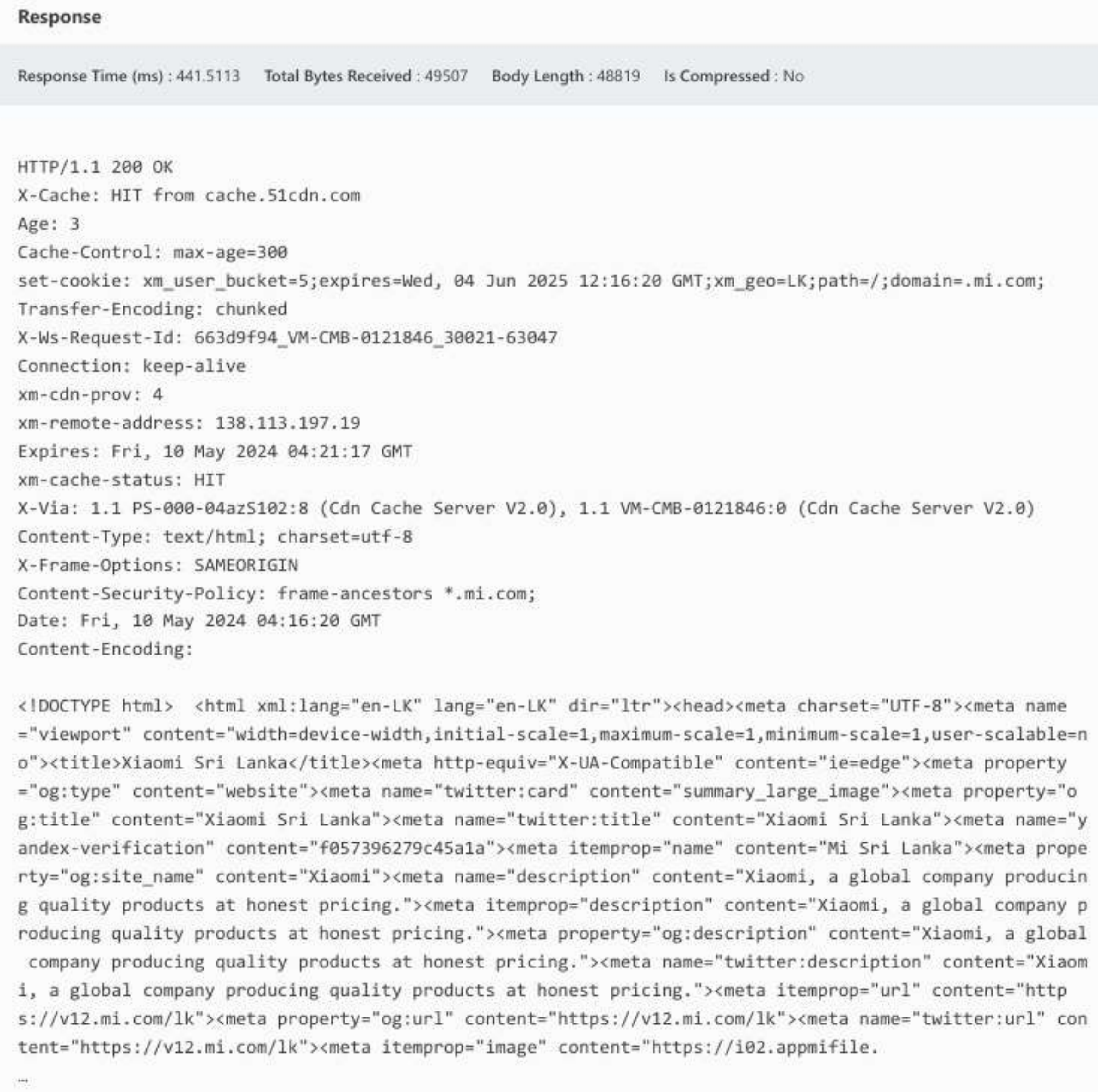
Turning on HSTS is essential to fixing this vulnerability. This security feature prevents downgrading attacks and improves overall security by guaranteeing that all communications with the website are encrypted and safe. Quick HSTS implementation can help the website comply with legal obligations, preserve 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: www.mi.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

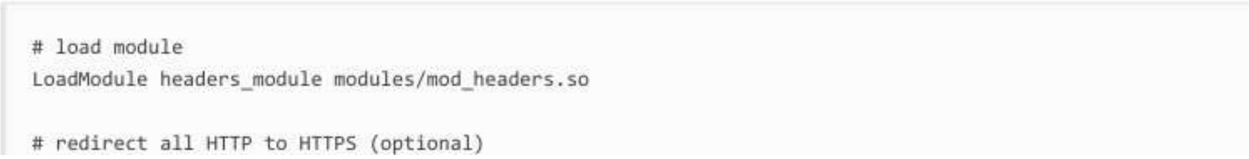
Response Time (ms) : 441.5113 **Total Bytes Received** : 49507 **Body Length** : 48819 **Is Compressed** : No

```
HTTP/1.1 200 OK
X-Cache: HIT from cache.51cdn.com
Age: 3
Cache-Control: max-age=300
set-cookie: xm_user_bucket=5;expires=Wed, 04 Jun 2025 12:16:20 GMT;xm_geo=LK;path=/;domain=.mi.com;
Transfer-Encoding: chunked
X-Ws-Request-Id: 663d9f94_VM-CMB-0121846_30021-63047
Connection: keep-alive
xm-cdn-prov: 4
xm-remote-address: 138.113.197.19
Expires: Fri, 10 May 2024 04:21:17 GMT
xm-cache-status: HIT
X-Via: 1.1 PS-000-04azS102:8 (Cdn Cache Server V2.0), 1.1 VM-CMB-0121846:0 (Cdn Cache Server V2.0)
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors *.mi.com;
Date: Fri, 10 May 2024 04:16:20 GMT
Content-Encoding:

<!DOCTYPE html>  <html xml:lang="en-LK" lang="en-LK" dir="ltr"><head><meta charset="UTF-8"><meta name
="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,minimum-scale=1,user-scalable=n
o"><title>Xiaomi Sri Lanka</title><meta http-equiv="X-UA-Compatible" content="ie=edge"><meta property
="og:type" content="website"><meta name="twitter:card" content="summary_large_image"><meta property="o
g:title" content="Xiaomi Sri Lanka"><meta name="twitter:title" content="Xiaomi Sri Lanka"><meta name="y
andex-verification" content="f057396279c45a1a"><meta itemprop="name" content="Mi Sri Lanka"><meta prope
rty="og:site_name" content="Xiaomi"><meta name="description" content="Xiaomi, a global company producin
g quality products at honest pricing."><meta itemprop="description" content="Xiaomi, a global company p
roducing quality products at honest pricing."><meta property="og:description" content="Xiaomi, a global
 company producing quality products at honest pricing."><meta name="twitter:description" content="Xiaom
i, a global company producing quality products at honest pricing."><meta itemprop="url" content="http
s://v12.mi.com/lk"><meta property="og:url" content="https://v12.mi.com/lk"><meta name="twitter:url" con
tent="https://v12.mi.com/lk"><meta itemprop="image" content="https://i02.appmifile.
…
```

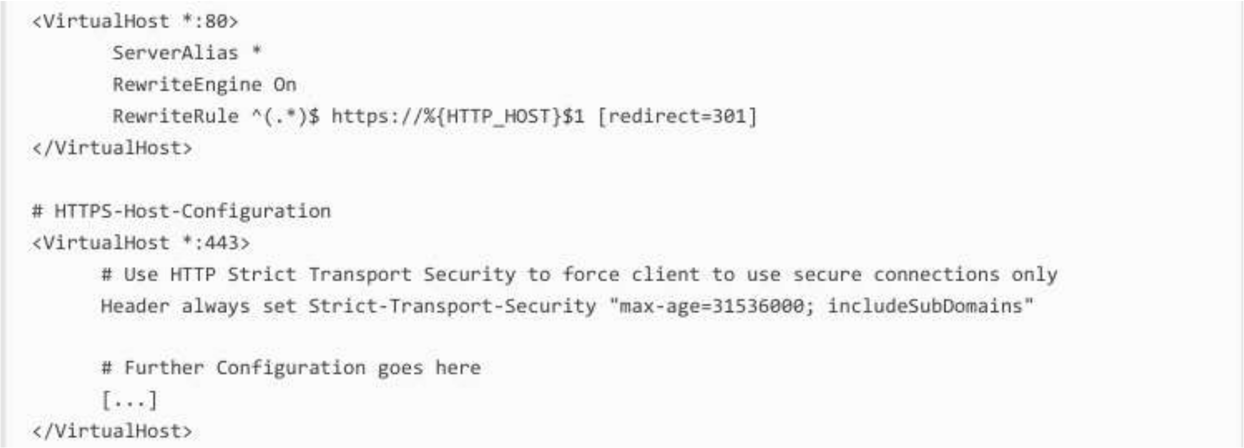
Remediation

- 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>
```