SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Web Security- IE2062

(HSTS) Policy Not Enabled

Danuka Nuwan

IT22349842

Title – HTTP Strict Transport Security (HSTS) Policy Not Enabled

Vulnerability: The application falls short to execute HTTP Strict Transportation Protection (HSTS) plan leaving it prone to different assaults, consisting of SSL-stripping strikes and also man-in-the-middle strikes. Without HSTS customers might be prone to downgrade strikes, where a foe can require using troubled HTTP as opposed to HTTPS compromising the privacy as well as honesty of sent information.

Website-www.cargo.indrive.com

Affected Components:

- Web server configurations
- HTTPS implementation
- Browser security features

Impact Assessment:

High: Failure to execute HSTS subjects individuals to prospective dangers of information interception and also control by enemies. The absence of HSTS threatens the efficiency of HTTPS security endangering the safety of the application as well as individual information.

Instructions to Replicate:

Examine the application's HTTP feedback headers to identify if the Strict-Transport-Security header is missing or misconfigured.

Evaluate the efficiency of HTTPS security by assessing network website traffic making use of obstructing proxy devices or web browser designer devices.

Effort to block as well as control HTTPS web traffic to show the lack of HSTS defense as well as its influence on information honesty as well as privacy.

Assess the application's compatibility with HSTS preload checklists as well as the usefulness of sending it for incorporation in significant internet browsers' HSTS preload listings.

Proof of Concept:

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

MEDIUM | 1

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Vulnerabilities

1.1. https://cargo.indrive.com/

Certainty

Request

```
GET / HTTP/1.1
Host: cargo.indrive.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) : 780.6575 Total Bytes Received : 96722 Body Length : 96153 Is Compressed : No

```
HTTP/1.1 200 OK
cache-control: s-maxage=31536000, stale-while-revalidate
content-encoding:
X-Amz-Cf-Id: V7feg3jGYMvMWmsWqdKsD5WFpszHncZFpwWk5U_856b_keCmwDKySA==
server: istio-envoy
x-powered-by: Next.js
Connection: keep-alive
x-envoy-upstream-service-time: 11
Via: 1.1 a7adf71acf6767d8f3fb252f00dfd348.cloudfront.net (CloudFront)
X-Cache: Miss from cloudfront
X-Amz-Cf-Pop: SIN2-P3
vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
date: Sun, 28 Apr 2024 21:17:46 GMT
etag: "4xampkjzwn221e"
x-nextjs-cache: HIT

<!DOCTYPE html><html dir="ltr" lang="en"><head><meta charset="utf-8"/><meta http-equiv="X-UA-Compatibl
e" content="IE=edge"/><meta name="viewport" content="minimum-scale=1, initial-scale=1, width=device-wid
th, shrink-to-fit=no, user-scalable=no, viewport-fit=cover"/><title>Online Cargo Transportation Service
 - cargo.inDrive</title><meta name="robots" content="index,follow"/><meta name="description" content="F
reight deliveries at your price. We verify every driver's basic info and documents in the app. Learn mo
re about inDrive transportation services!"/><meta property="og:title" content="Online Cargo Transportat
ion Service - cargo.inDrive"/><meta property="og:description" content="Freight deliveries at your pric
e. We verify every driver's basic info and documents in the app. Learn more about inDrive transportatio
n services!"/><link rel="canonical" href="https://cargo.indrive.com"/><link rel="preload" as="image" im
agesrcset="/_next/image?url=%2Fassets%2Fhero.jpg&amp;w=640&amp;q=100 640w, /_next/image?url=%2Fassets%2
Fhero.jpg&amp;w=750&amp;q=100 750w, /_next/image?url=%2Fassets%2Fhero.jpg&amp;w=828&amp;q=100 828w, /_n
ext/image?url=%2Fassets%2Fhero.jpg&amp;w=1080&amp;q=100 1080w, /_next/image?url=%2Fassets%2Fhero.jpg&am
p;w=1200&amp;q=100 1200w, /_next/image?url=%2Fassets%2Fhero.jpg&amp;w=1920&amp;q=100 1920w, /_next/imag
e?url=%2Fassets%2Fhero.jpg&amp;w=2048&amp;q=100 2048w, /_next/image?url=%2Fassets%2Fhero.jpg&a
…
```

Remedy

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>
```

External References

- Wikipedia - HTTP Strict Transport Security
- Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx
- HTTP Strict Transport Security (HSTS) HTTP Header
- Mozilla SSL Configuration Generator

Suggested Resolution:

Set up internet server setups to consist of the Strict-Transport-Security header in HTTP reactions with an ample max-age required to apply HSTS plan.

Make use of include Subdomains regulation to prolong HSTS security to all subdomains of the application's domain name.

Make it possible for preload instruction to send the application for incorporation in internet browsers' HSTS preload checklists making sure HSTS plan is enforced upon the very first browse through to the domain name.

Perform normal safety and security analyses consisting of vulnerability scanning and also infiltration screening to confirm the efficiency of HSTS application as well as recognize any kind of misconfigurations or vulnerabilities.

Inform programmers as well as system managers on the significance of executing HSTS to improve the protection of internet applications as well as safeguard versus SSL-stripping assaults and also downgrade assaults.

Display HSTS preload checklist entries as well as updates to make sure the application stays consisted of in significant internet browsers' HSTS preload checklists, supplying lasting defense versus method downgrade strikes.

Additional references

https://portswigger.net/kb/issues/01000300_strict-transport-security-not-enforced

https://developers.cloudflare.com/ssl/edge-certificates/additional-options/http-strict-transport-security/

https://https.cio.gov/hsts/