Sri Lanka Institute of Information Technology

IT21299902 (ZAKEY M.S.M.A)

Bug bounty Report 01.

Domain: MalwareBytes.com

Web security – IE2062

B.Sc. (Hons) in Information Technology Specialization in cyber security.

Declaration:

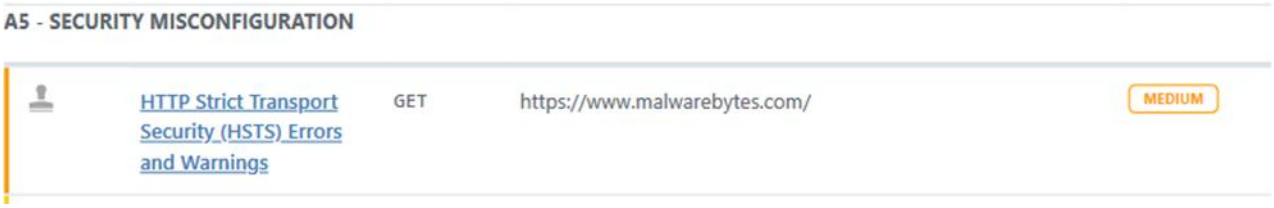
- I hereby certify that no part of this assignment has been copied from any other work or any other source. No part of this assignment has been written/produced for me by another person.

- I hold a copy of this assignment that I can produce if the original is lost or damaged.

1. Security misconfiguration.

- **HTTP strict transport security (HSTS) errors and warnings**

I hope this message finds you well. I am writing to report a vulnerability I discovered under the domain of https://www.malwarebytes.com during my participation in the bug bounty program. Please find below the details of the vulnerability for your review and further action.



Vulnerability title: HTTP strict transport security (HSTS) errors and warnings

Severity: Medium

OWASP classification 2013: A5

Effected components: CDN and proxy servers.

Subdomains */Malwarebytes.com

Date of Discovery: 2023/05/10

Date of Report: 2023/05/12

2. Vulnerability Description.

I have identified a misconfigured HTTP strict transport security header vulnerability within the affected system. This vulnerability allows an attacker to do man-in-the-middle attack or protocol downgrade attacks. By exploiting this vulnerability, an attacker could potentially steal sensitive user information, manipulate website content, or perform other malicious activities.

3. Impact assessment.

1. HSTS faults or warnings indicate that an HTTPS connection is not being properly enforced by the web application. Insecure connections. As a result, users may access the application over insecure HTTP connections, increasing the risk of attackers listening in, meddling with, or intercepting their communications.

2. HSTS failures or warnings can make the web application susceptible to MITM attacks. Attackers can force the browser to communicate over insecure HTTP rather than HTTPS by intercepting the initial HTTP request and altering the response to delete or change the HSTS headers.

3. The website may be unable to create secure connections with compliant browsers due to HSTS issues. Users may get browser errors or warnings as a result, indicating that the connection might not be secure. Users can feel deterred from using the application or think it's less reliable.

4. HSTS faults or warnings may make SSL/TLS's (Secure Sockets Layer/Transport Layer Security) defense against SSL/TLS-stripping attacks less effective. These attacks seek to switch the connection from HTTPS to HTTP, which would enable attackers to eavesdrop on or alter user-app communication.

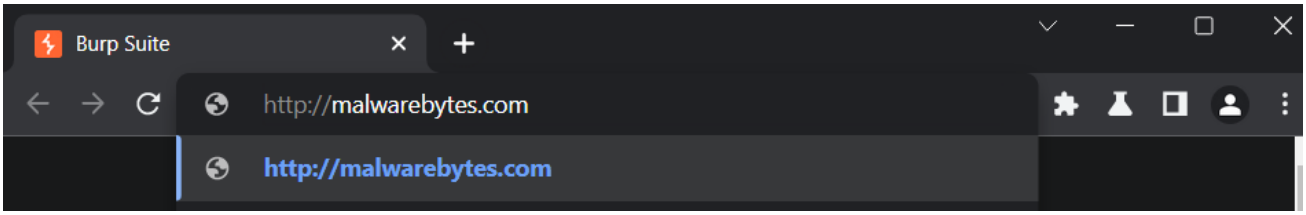
4. Steps to Reproduce.

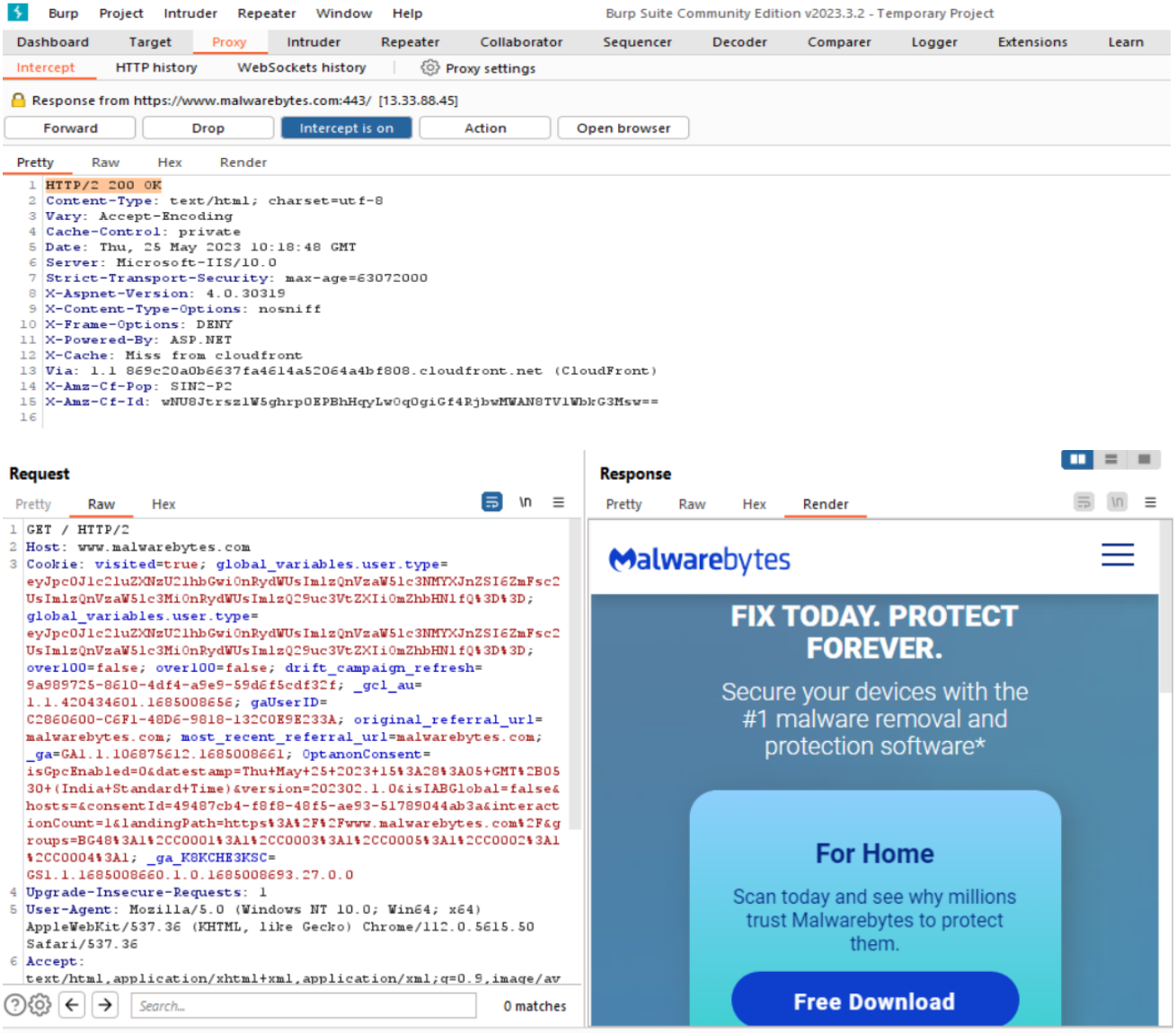
1. Ensure the website has HSTS enabled: Verify that the website has HTTP Strict Transport Security (HSTS) enabled. This can be done by checking the website's response headers. Look for the presence of the "Strict-Transport-Security" header in the HTTP response.
2. Clear browser HSTS cache: If you have previously visited the website, your browser may have cached the HSTS policy. Clear your browser's HSTS cache to start fresh for testing purposes. The process for clearing the cache varies depending on the browser you are using.
3. Attempt to access the website using HTTP: Instead of accessing the website using HTTPS, intentionally try to access it using HTTP. Enter the URL using the "http://" protocol instead of "https://".
4. Observe the error or warning: Depending on the browser and its HSTS implementation, you may encounter different behaviors when attempting to access the website over HTTP. Common scenarios include:

    a. Error page: The browser may display an error page indicating that the website cannot be accessed because it enforces HTTPS. The error message may vary depending on the browser.
    b. Warning message: The browser may display a warning message, typically in the form of a notification or a bar at the top of the page, indicating that the website should be accessed using HTTPS instead of HTTP.
    c. Automatic redirection: In some cases, the browser may automatically redirect the HTTP request to HTTPS, without displaying an error or warning. This behavior depends on the browser's HSTS implementation.

5. Proof of concept.

1. Access web application through HTTP.





2. HSTS scan report by SSLLabs

SSL Report: malwarebytes.com

Assessed on: Thu, 25 May 2023 10:17:27 UTC | Hide | Clear cache

Scan Another >>

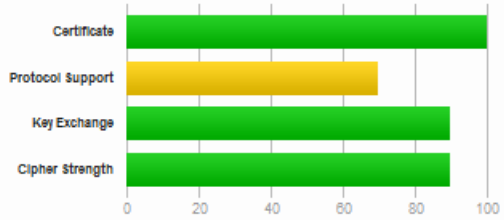
	Server	Test time	Grade
1	99.84.238.97 server-99-84-238-97.sfo5.r.cloudfront.net Ready	Thu, 25 May 2023 09:59:47 UTC Duration: 262.355 sec	B
2	99.84.238.177 server-99-84-238-177.sfo5.r.cloudfront.net Ready	Thu, 25 May 2023 10:04:09 UTC Duration: 267.374 sec	B
3	99.84.238.194 server-99-84-238-194.sfo5.r.cloudfront.net Ready	Thu, 25 May 2023 10:08:36 UTC Duration: 266.71 sec	B
4	99.84.238.172 server-99-84-238-172.sfo5.r.cloudfront.net Ready	Thu, 25 May 2023 10:13:02 UTC Duration: 264.250 sec	B

SSL Report v2.1.10

Summary

Overall Rating

B

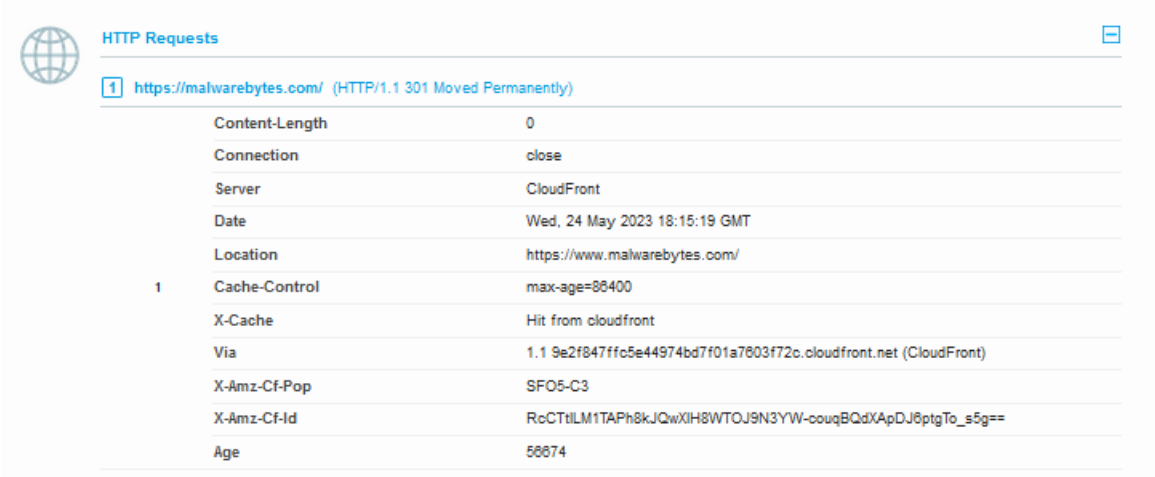


Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This site works only in browsers with SNI support.

This server supports TLS 1.3.



HTTP Requests

1 https://malwarebytes.com/ (HTTP/1.1 301 Moved Permanently)

	Content-Length	0
	Connection	close
	Server	CloudFront
	Date	Wed, 24 May 2023 18:15:19 GMT
	Location	https://www.malwarebytes.com/
1	Cache-Control	max-age=86400
	X-Cache	Hit from cloudfront
	Via	1.1 9e2f847ffc5e44974bd7f01a7603f72c.cloudfront.net (CloudFront)
	X-Amz-Cf-Pop	SFO5-C3
	X-Amz-Cf-Id	RcCTtlLM1TAPh8kJQwXlH8WTOJ9N3YW-couqBQdXApDJ6ptgTo_s5g==
	Age	56674

3. Scan report by net sparker.

Vulnerabilities

3.1. https://www.malwarebytes.com/

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

Certainty

Request

```
GET / HTTP/1.1
Host: www.malwarebytes.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) : 394.9114 Total Bytes Received : 99524 Body Length : 98932 Is Compressed : No

```
HTTP/1.1 200 OK
X-Cache: Miss from cloudfront
Cache-Control: private
Strict-Transport-Security: max-age=63072000
Transfer-Encoding: chunked
X-Powered-By: ASP.NET
Server: Microsoft-IIS/10.0
X-Amz-Cf-Id: atIflY-iXNub1rOSkvyNvvPxhzhZrm-We6nwj5RTD_8IBClGuho51A==
X-Content-Type-Options: nosniff
X-AspNet-Version: 4.0.30319
Connection: keep-alive
X-Frame-Options: DENY
Vary: Accept-Encoding
X-Amz-Cf-Pop: SIN2-C1
Via: 1.1 c8c43b7bd0e92cbb9fbe171dc985f060.cloudfront.net (CloudFront)
Content-Type: text/html; charset=utf-8
Date: Mon, 15 May 2023 10:15:59 GMT
Content-Encoding:
```

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">

<title>Cyber Security Software & Anti-Malware | Malwarebytes</title>
<meta name="description" content="Protect your home and business PCs, Macs, iOS and Android devices fro
m the latest cyber threats and malware, including ransomware."/>
<link rel="canonical" href="https://www.malwarebytes.com/"/></link>

<link rel="alternate" hreflang="x-default" href="https://www.malwarebytes.com"/>
<link rel="alternate" href="https://www.malwarebytes.com" hreflang="en-us"/>
<link rel="alternate" href="https://es.malwarebytes.com" hreflang="es-es"/>
<link rel="alternate" href="https://de.malwarebytes.com" hreflang="de-de"/>
<link rel="alternate" href="https://it.malwarebytes.com" hreflang="it-it"/>
<link rel="alternate" href="https://fr.malwarebytes.com" hreflang="fr-fr"/>
<link rel="alternate" href="https://nl.malwarebytes.com" hreflang="nl-nl"/>
<link rel="alternate" href="https://br.malwarebytes.com" hreflang="pt-br"/>
<link rel="alternate" href="https://pt.malwarebytes.com" hreflang="pt-pt"/>
<link rel="alternate" href="https://pl.malwarebytes.com" hreflang="pl-pl"/>
<link rel="alternate" href="https://ru.malwarebytes.com" hreflang="ru-ru"/>
<link rel="alternate" href="https://www.malwarebytes.com/jp" hreflang="ja-jp"/>
<link rel="alternate" href="https://www.malwarebytes.com/se" hreflang="sv-se"/>
<script type=
…
```

6. Proposed mitigation/fix.

The first step is to identify the error codes and resolve those problems. The domain must be added to the HSTS preload list after the issues with the HSTS header have been resolved. Browsers automatically connect to the website via HTTPS when the domain is added to the HSTS preload list, preventing users from making HTTPS requests to the server.

The web application needs to be set in accordance with the following requirements before being added to the preload list of the browser.

1. Present a legitimate certificate.
2. If you are listening on port 80, switch all HTTP domains on the same host to HTTPS. Serve every subdomain using HTTPS.
   - If a DNS record for the www subdomain exists, you must support HTTPS for that subdomain.
3. Provide a HSTS header for HTTPS queries on the base domain:
   - The maximum age requirement is 31536000 seconds (one year).
   - It is necessary to specify the included Subdomains directive.
   - Preload directive needs to be mentioned.
   - The HSTS header must be included on the additional redirection that is being served from your HTTPS site, not on the destination page.