



# SLIIT

---

*Discover Your Future*

---

Sri Lanka Institute of Information Technology

## Bug Bounty Report 10

Arkose labs

**IE2062 – Web Security**

Submitted by:

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

Date of submission

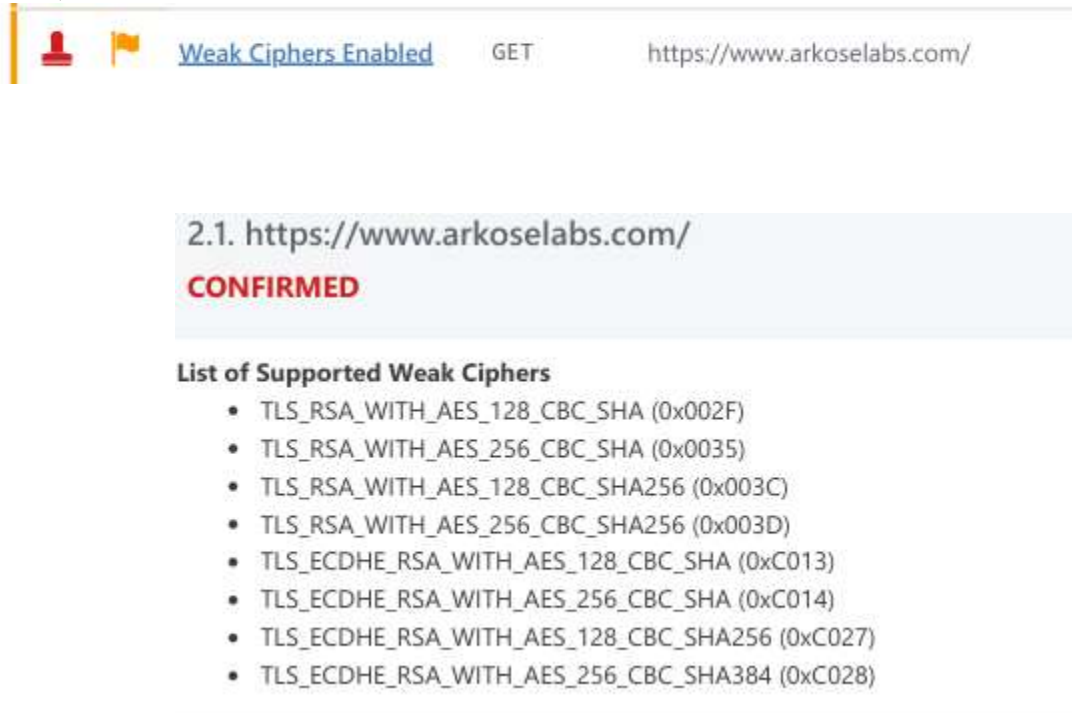
2024.05.04

## Table of Contents

Vulnerability .....	3
1) Weak Ciphers Enabled .....	<b>Error! Bookmark not defined.</b>
• Description .....	<b>Error! Bookmark not defined.</b>
• Impact Assessment .....	<b>Error! Bookmark not defined.</b>
• Steps to Reproduce .....	<b>Error! Bookmark not defined.</b>
• Proof of Concept .....	<b>Error! Bookmark not defined.</b>
• Remediation .....	<b>Error! Bookmark not defined.</b>
2) HTTP Strict Transport Security (HSTS) Policy Not Enabled.....	<b>Error! Bookmark not defined.</b>
• Description .....	<b>Error! Bookmark not defined.</b>
• Impact Assessment .....	<b>Error! Bookmark not defined.</b>
• Steps to Reproduce.....	<b>Error! Bookmark not defined.</b>
• Proof of Concept .....	<b>Error! Bookmark not defined.</b>
• Remediation .....	<b>Error! Bookmark not defined.</b>

# Vulnerability

## 1) Weak Ciphers Enabled



The screenshot shows a vulnerability report interface. At the top, there is a header bar with a red pushpin icon, a yellow flag icon, the title 'Weak Ciphers Enabled', the HTTP method 'GET', and the URL 'https://www.arkoselabs.com/'. Below this, the specific vulnerability is identified as '2.1. https://www.arkoselabs.com/' with a status of 'CONFIRMED'. A section titled 'List of Supported Weak Ciphers' contains a bulleted list of eight TLS cipher suites.

2.1. https://www.arkoselabs.com/  
**CONFIRMED**

**List of Supported Weak Ciphers**

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002F)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003C)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003D)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xC013)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xC014)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xC027)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xC028)

**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://arkoselabs.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://arkoselabs.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 regedt32 or 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



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://arkoselabs.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.arkoselabs.com](http://www.arkoselabs.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](http://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.arkoselabs.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) : 1092.5675    Total Bytes Received : 6953    Body Length : 6388    Is Compressed : No

HTTP/1.1 502 Bad Gateway  
Set-Cookie: cf\_ob\_info=502:88226b8cdc2392f5:CMB; path=/; expires=Sat, 11-May-24 13:12:52 GMT  
Set-Cookie: cf\_use\_ob=443; path=/; expires=Sat, 11-May-24 13:12:52 GMT  
Expires: Thu, 01 Jan 1970 00:00:01 GMT  
Referrer-Policy: same-origin  
Server: cloudflare  
Connection: keep-alive  
Content-Length: 6388  
X-Frame-Options: SAMEORIGIN  
CF-RAY: 88226b8cdc2392f5-CMB  
Content-Type: text/html; charset=UTF-8  
Date: Sat, 11 May 2024 13:12:22 GMT  
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
  
<!DOCTYPE html>  
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->  
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->  
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->  
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif-->  
<head>  
<meta http-equiv="refresh" content="0">  
  
<title>www.arkoselabs.com | 502: Bad gateway</title>  
<meta charset="UTF-8" />  
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />  
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />  
<meta name="robots" content="noindex, nofollow" />  
<meta name="viewport" content="width=device-width,initial-scale=1" />  
<link rel="stylesheet" id="cf\_styles-css" href="/cdn-cgi/styles/main.css" />  
  
</head>  
<body>  
<div id="cf-wrapper">  
<div id="cf-error-details" class="p-0">  
<header class="mx-auto pt-10 lg:pt-6 lg:px-8 w-240 lg:w-full mb-8">  
<h1 class="inline-block sm:block sm:mb-2 font-light text-60 lg:text-4xl text-black-dark leading-tight m  
r-2">  
<span class="inline-block">Bad gateway</span>  
<span class="code-label">Error code 502</span>  
</h1>  
<div>  
Visit <a href="https://www.cloudflare.com/5xx-error-landing?utm\_source=errorcode\_502&utm\_campaign=www.a  
rkoselabs.com" target="\_blank" rel="noopener noreferrer">cloudflare.com</a> for more information.  
</div>  
...

- **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