Sri Lanka Institute of Information Technology

Journal

IE2062 – Web Security

Submitted by:

IT22199508 – Athapaththu A.M.M.I.P

Date of submission

2024.05.11

Table of Contents

Acknowledgement

Foremost, as a second year second semester Cyber Security student I would like to convey my sincere gratitude to Ms. Chethana, the Lecture in Charge of the Web Security module. Her support, guidance and advice helped us to complete this web audit/ bug bounty task successfully. Her constant guidance also helped us during the time of writing this report.

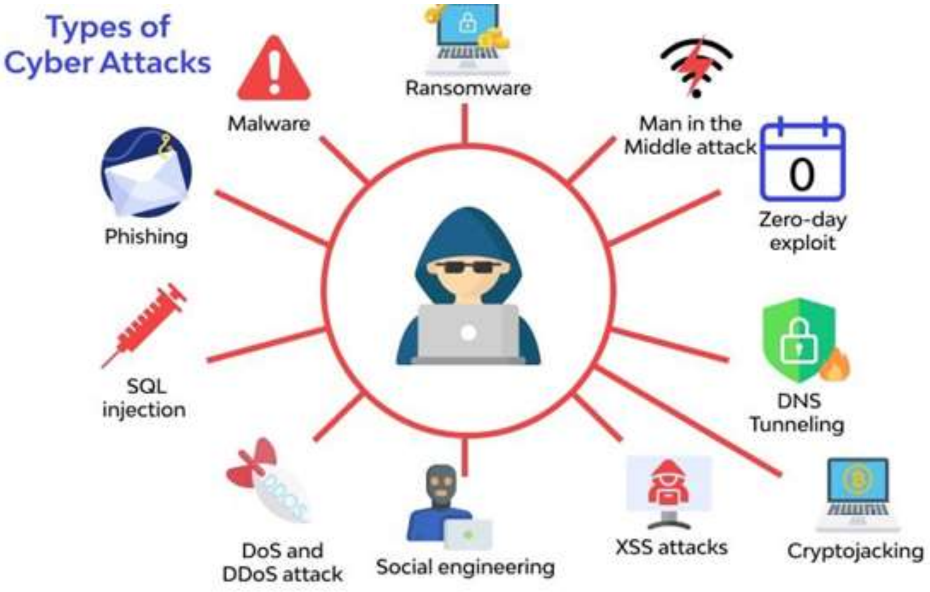
And also, I would like to express my sincere gratitude to our Lab Instructor who guided us and helped us in the Labs that made it easier to complete this bug bounty/ web audit. I appreciate the advice and assistance you provided so that I could complete the task successfully.

Abstract

Cybercrimes, data breaches, and misrepresentation are all dangerous risks that any Company or an organization might face. A large amount of information has been lost, and now organizations need to find out the steps to take to stop the danger from getting worse and to avoid more bad things happening. An investigation was conducted to investigate the processes related to IT security web audits. How they can assist businesses in improving their IT security. This study looks at the impact of the understanding of the threats posed by cybercrime. This investigation shows the web application vulnerabilities that are possessed by a company by evaluating the remediations to be taken to get rid of the security risks. This study has a detailed description about the vulnerabilities that the specific domains of the website possess. This study was done to learn more about cybercrime and gather more data on it. The aim is to put together more extensive information about the vulnerabilities of the website and help the company to mitigate them in order to get rid of the security issues. The investigation clearly showed that IT security audits are more critical for growth of every organization which uses Information Technology.

Introduction

Cybercrime is a problem that all organizations have to face, and it is becoming more common. Every day, cybercrime causes chaos and damage to information. This means that when the organization's systems are not working properly, it can cause the organization to lose a lot of money and harm its reputation.



There are several types of cyber-attacks that an organization can face such as malware, ransomware, SQL injection, DOS/DDOS attacks. With the advancement of technology and globalization of organizations most of the companies uses web applications, with the increase of web applications Cyber-attacks has been increased in the latter years.

- Nearly 1 billion emails were exposed in a single year, affecting 1 in 5 internet users.
- Data breaches cost businesses an average of $4.35 million in 2022.
- Around 236.1 million ransomware attacks occurred globally in the first half of 2022.
- 1 in 2 American internet users had their accounts breached in 2021.
- 39% of UK businesses reported suffering a cyber-attack in 2022.
- Around 1 in 10 US organizations have no insurance against cyber-attacks.
- 53.35 million US citizens were affected by cybercrime in the first half of 2022.

• Cybercrime cost UK businesses an average of £4200 in 2022.

To keep an organization's information system safe from cybercrime, fraud, and unauthorized access to data, it is important to have a strong security system for storing and organizing data. Every organization must make sure that their information is safe, private, and reliable. The actions of the customer, the item itself, and the way data is handled are all important for an organization's security. Although some writing argues that conducting web security auditing is crucial for protecting an organization's data system against cybercrime, fraud, and data breaches, regular checks should be performed to identify weaknesses in the organization's IT system. These checks should be conducted by an independent expert to ensure compliance and to identify any vulnerabilities. Can an IT security check help a company improve data safety and lower network security risks. This report will explain how and why an effective web security audit is done, and if it helps to increase IT security. To reach this objective, I will examine the audits of various Linux frameworks on the preferred international websites.

Then, according to the rules and regulations of the business, a program is set up to check the IT systems used for websites. After the program is completed, a report is made that includes the discoveries and advice on what should be done to lower possible risks to the data's security. Actually, IT auditing requires a lot of time and money. No matter what happens, cybercrimes, lies, or data breaches can be very expensive. So, it's better not to do it. The main purpose of this investigation is to show how important it is to check online security and to see how IT security checks can help improve things. The protection of an organization's information. The investigation also checks how much importance the organization gives to cybercrime risks, how well they follow global security norms and rules, and how often they conduct IT security audits.

Objective

A web audit's objective is to find vulnerabilities in websites by employing different approaches and scans. These audits' main goal is to fix vulnerabilities that, if ignored, can result in online security breaches and jeopardize the confidentiality, integrity, and availability (CIA) of the company's data. As second-year students, our goal is to find vulnerabilities in websites that exist in the real world by applying the information we learned in our web security course throughout the second semester. As undergraduate students, we want to learn more, thus we want to chronicle these weaknesses.

I used a variety of scanning programs to find any potential security holes in the websites I was looking at in order to complete this work. Sublist3r, nikto, nmap, Nessus, OWASP Zap, subfinder, and invicti are some of the tools used. By using various approaches and strategies to find potential flaws in the targeted websites, each tool adds to the total evaluation.

We were able to do in-depth evaluations of the websites and find possible vulnerabilities by employing these scanning technologies. These results are given in the form of a paper that includes a thorough description of the vulnerabilities found, their possible consequences, and suggested mitigation steps.

This exercise's primary goal is to improve our undergraduate students' knowledge and comprehension of online security. Through proactive participation in real-world online audits and thorough documentation of our results, we enhance our understanding of the possible hazards connected to web applications and obtain hands-on experience in detecting vulnerabilities. In the area of online security, this exercise is an invaluable teaching tool that closes the knowledge gap between theory and practice.

Daily Journal-(12.04.2024)

Objectives:

- Learn About what is OWASP TOP 10 Vulnerabilities.
- Learn the vulnerabilities.
- What are the impacts and the solutions for those vulnerabilities.

Sources Used:

- Google.
- OWASP Website.
- Portswigger.

This took me several days to complete. It was not easier to learn about all the vulnerabilities in a limited period of time.

Owasp Top 10 Security Risks and Vulnerabilities

OWASP (Open Web Application Security Project) top 10 vulnerabilities are the widely recognized web application security threats that are faced by the web applications which are critical. These vulnerabilities are updated every three to four years. The Open Web Application Security Project is a non-profit organization which is dedicated to improving the security of the internet. These vulnerabilities help the companies and developers to prioritize their efforts towards web application security. This list is updated by group of security specialists.

Why OWASP Top 10 is important?

- Helps in Mitigation of risks.
- Guidance to Prioritize Security concerns.
- Awareness and gain knowledge about Web Application vulnerabilities.
- Improvement of the security of organization’s web applications.
- To improve the security Design of the web applications.

1. Broken Authentication

Broken authentication is a big problem in web apps and services. It shows that strong user login and session management are very important. This problem happens when these systems don't work correctly, making them easy to be taken advantage of by Hackers. Some common problems are having weak passwords, not managing sessions well, and not protecting against brute-force attacks well enough.

Weak password policies allow users to use easy to guess or commonly used passwords, which makes it easier for attackers to take over accounts. If session management is not done properly, it can lead to session IDs being discovered or easily guessed, which can allow unauthorized people to access user accounts. Furthermore, when there is not enough security against brute-force attacks, attackers can keep trying different login information until they gain access, which is a big security problem.

Countermeasures

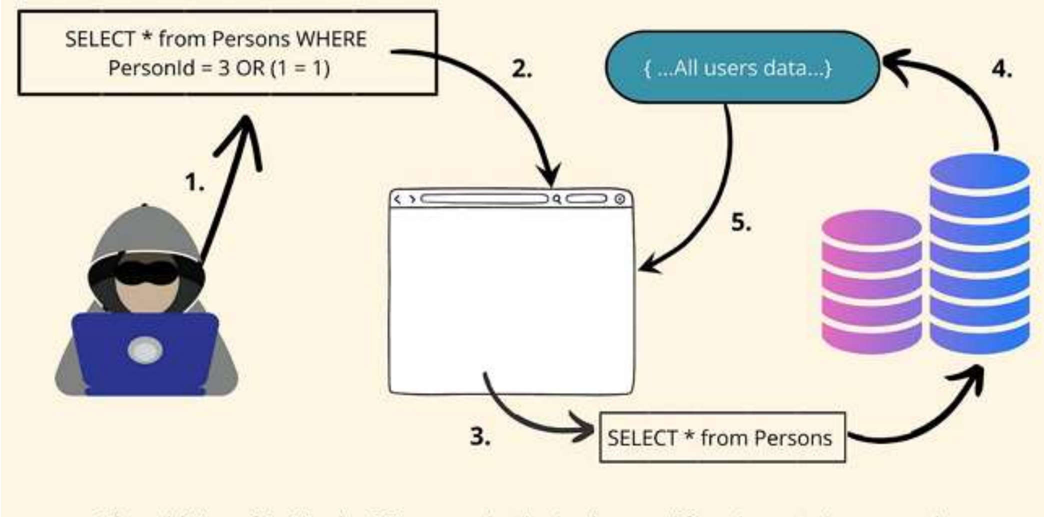
- Use of Strong Passwords.
- Session Management.
- Brute Force Detection and Monitoring.
- API Security.

2. Injection

Injection attacks are one of the most significant and famous web security threats. There are several types of injection attacks such as:

- SQL Injection (The most common Injection attack)
- Command Injection.
- XML Injection.

These attacks happen when harmful codes or commands are inserted into the insert fields and the parameters of web applications. Through SQL injections the attackers could be able to access databases unauthorizedly and steal important information from the databases and change the information.



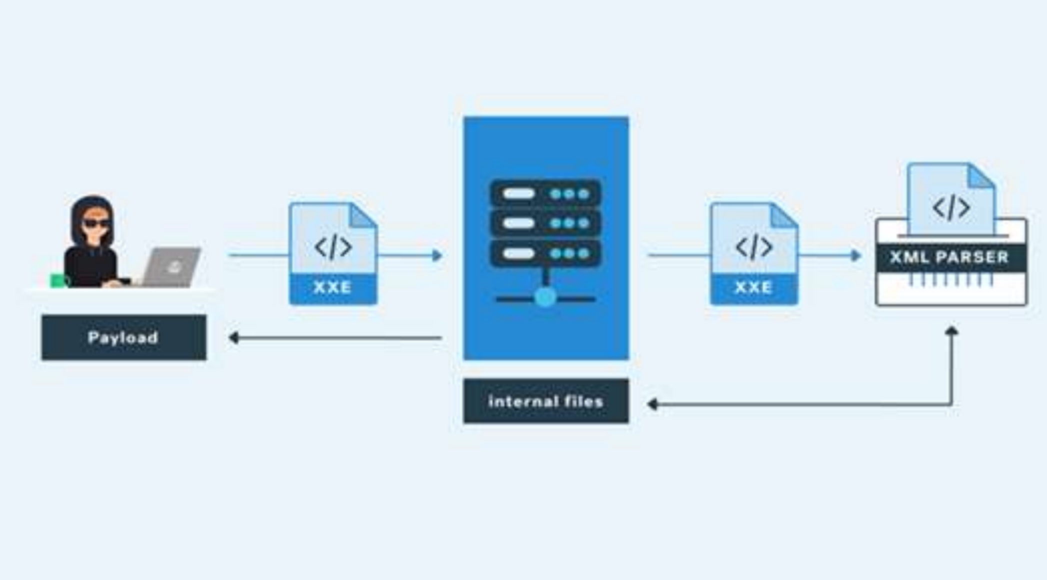
The addition of 1=1 in the SQL query by the hacker modifies the actual query and all the user data is fetched as 1=1 always holds true

Countermeasures

- Use stored Procedures.
- Least Privilege.
- Use Object Relational Mapping.
- Use Prepared Statements.
- Input Validation.

3. XML External Entities

XML External Entities (XXE) is a weakness in the way web applications handle XML files. This happens when a hacker can change or insert malicious things into a computer program that reads XML. These outside sources can point to files on your computer or other computers, which can cause problems with keeping information private, stopping services from working, and even letting someone run code on your computer from a distance. XXE attacks are really worrying because they can take advantage of XML data transfer, which is commonly used in web services and communication between API.

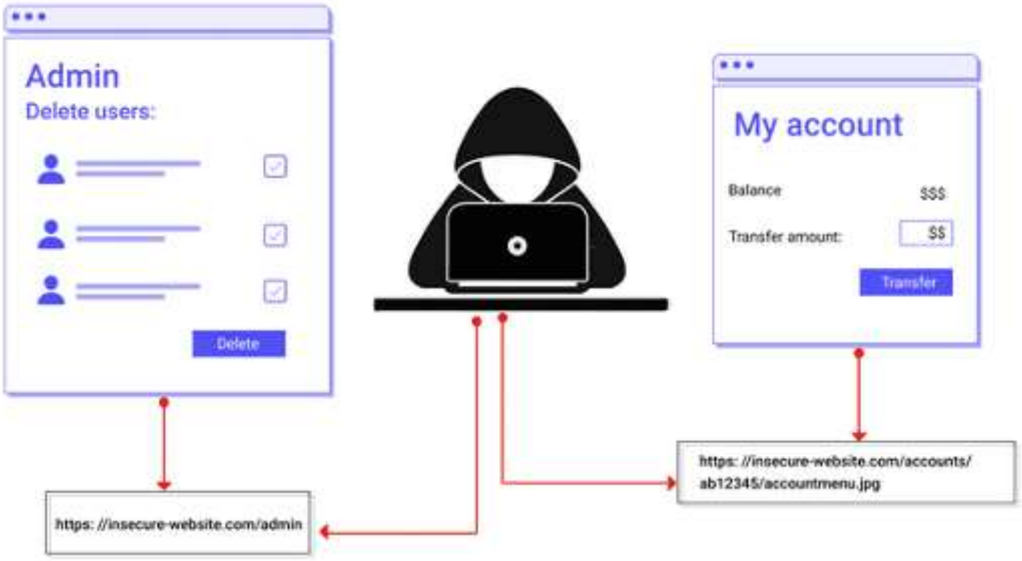


Countermeasures

- Input Validation and Sanitization.
- Use of Firewalls.
- Update and Patch Software.
- Access Controls.
- Use Modern and secure parsers.

4. Broken Access Control

Broken Access Control is a big problem in web applications. It happens when the system doesn't properly check who can access certain things. It lets people who shouldn't be able to access certain places or do certain things in a computer program, do those things anyway. This weakness usually happens when there are mistakes in how a person is identified and given permission to access something. It can also be caused by not managing a person's session properly. When access control is broken, attackers can use it to look at private information, change data, or even get control over the system.

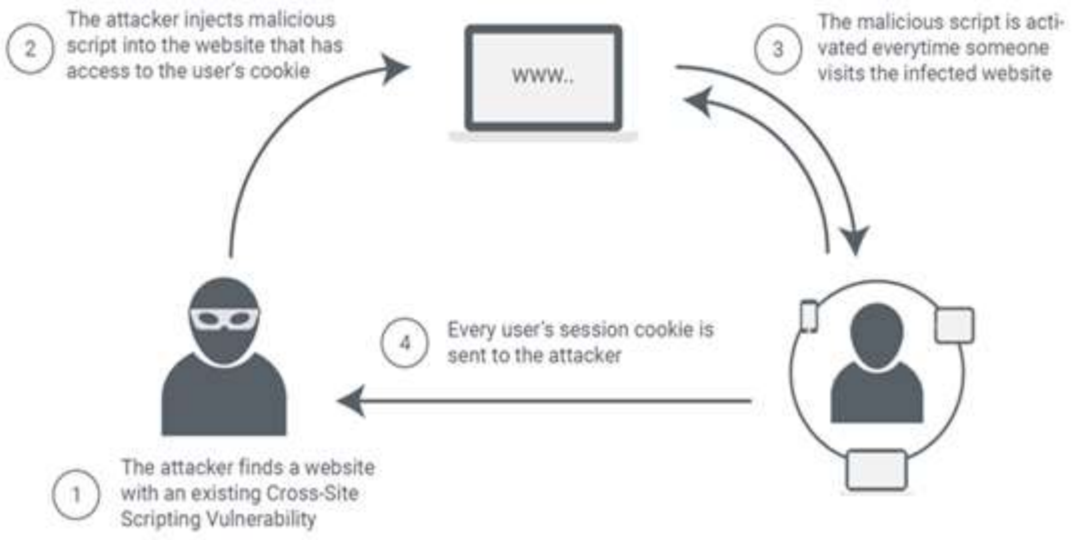

Admin
Delete users:
Delete
My account
Balance
$$$
Transfer amount:
$$
Transfer
https: //insecure-website.com/accounts/ ab12345/accountmenu.jpg
https: //insecure-website.com/admin

Countermeasures

- Explicit Authorization Checks.
- Session Management.
- Access Control Testing.
- Authentication Tokens.
- Error- Handling.

5. Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) is a common and risky security problem on websites. It happens when a person puts harmful scripts or code into web pages that other people look at. These codes are run on the victim's web browser and can cause various harmful actions like stealing sensitive information, taking over user sessions, changing the appearance of websites, or spreading harmful software. XSS vulnerabilities happen when web applications don't properly check and clean up the information that users enter or display on the website. This makes it possible for attackers to add harmful code into fields where users enter information, website addresses, or other content that users create


2
The attacker injects malicious script into the website that has access to the user's cookie
www..
3
The malicious script is activated everytime someone visits the infected website
4
Every user's session cookie is sent to the attacker
1
The attacker finds a website with an existing Cross-Site Scripting Vulnerability

Countermeasures

- Content Security Policy.
- Regular Security Testing.
- Browser Security Features.
- Use trusted Frameworks and Libraries.
- Output Encoding.
- Security Headers.

Bug Bounty Methodologies

OWASP Testing Guide

The Web Security Testing Guide (WSTG) Project produces the premier cybersecurity testing resource for web application developers and security professionals. The WSTG is a comprehensive guide to testing the security of web applications and web services. Created by the collaborative efforts of cybersecurity professionals and dedicated volunteers, the WSTG provides a framework of best practices used by penetration testers and organizations all over the world.

The main phases of OWASP Testing guide are:

- Information Gathering
- Configuration and Deployment Management Testing.
- Web Application Security Testing.
- Reporting.

Penetration Testing Execution Standard (PTES)

A framework and approach for doing penetration testing, often known as ethical hacking or security testing, is the Penetration Testing Execution Standard (PTES). PTES offers an organized and consistent method for creating, carrying out, and reporting on penetration tests. It was developed to provide thorough and efficient security evaluations of systems, networks, and applications by penetration testers and security experts. PTES is a set of rules that covers several stages of the penetration testing process rather than a single standard.

Daily Journal-(16.04.2024)

This was one of the more hard days of journaling this.

Objectives:

- Find the tools used for Bug Bounty Program.
- Learn how to use them.
- Install the Tools.

Sources Used:

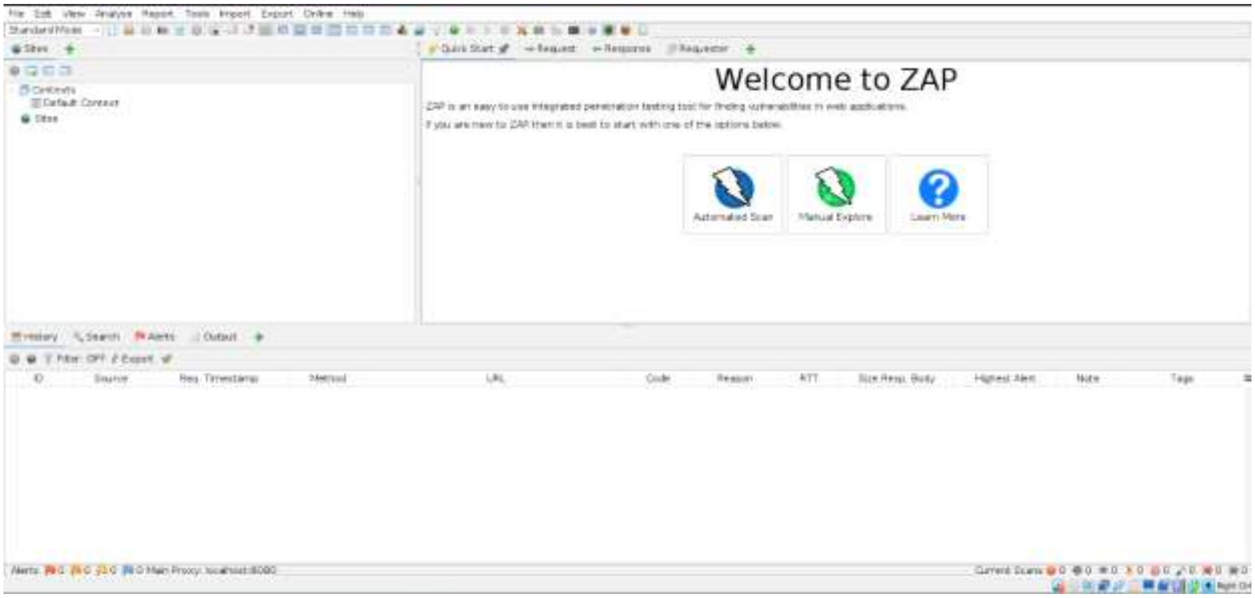
- OWASP.
- Portswigger.
- Youtube.
- Google.

I faced many challenges during this phase. It was harder to install the tools. Some tools were not installing, and some were outdated. It was harder to learn how to these tools.

Key Tools Used for Bug Bounty Hunting

1) OWASP Zap

A well-known open-source security testing tool for identifying and fixing vulnerabilities in online applications is called OWASP ZAP (Zed Attack Proxy). Users may intercept, examine, and change online traffic for security research with this tool, which serves as both a scanner and a proxy. ZAP aids programmers and security experts in locating typical online application flaws including Cross-Site Scripting (XSS), SQL Injection, and Cross-Site Request Forgery (CSRF). It is used by both novice and expert security testers because to its user-friendly interface and automatic scanning features. ZAP is continuously updated as part of the OWASP project to stay on top of new threats, ensuring that it continues to be an effective tool in the battle against web application vulnerabilities.



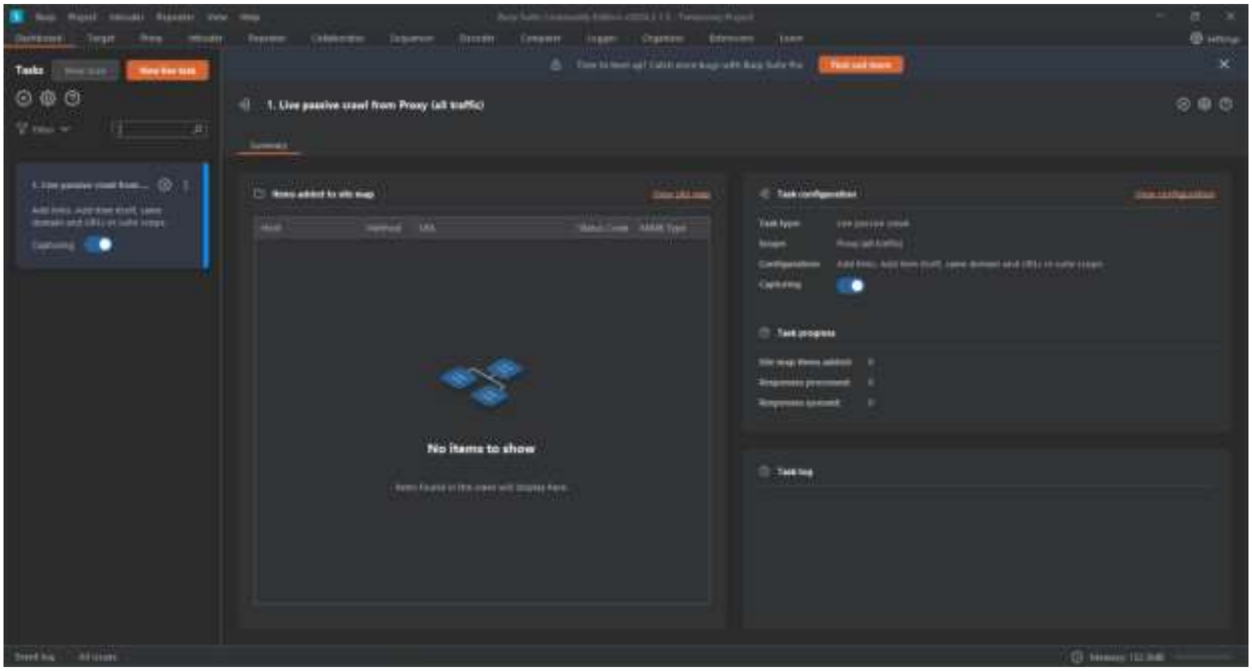
Welcome to ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

2) Burp Suite

Burp Suite is a popular and effective web application security testing tool made for locating and repairing vulnerabilities in online applications. The proxy, scanner, repeater, intruder, and sequencer are just a few of the crucial security testing components included in this integrated platform. Burp Suite is used by security experts, ethical hackers, and developers to find common online application flaws including Cross-Site Scripting (XSS), SQL Injection, and security configuration errors. People who are interested in penetration testing and security assessments appreciate it because of its interactive and straightforward user interface. The tool's rich feature set and frequent upgrades guarantee its leadership in web application security testing and enable the defense of digital assets against potential attacks.



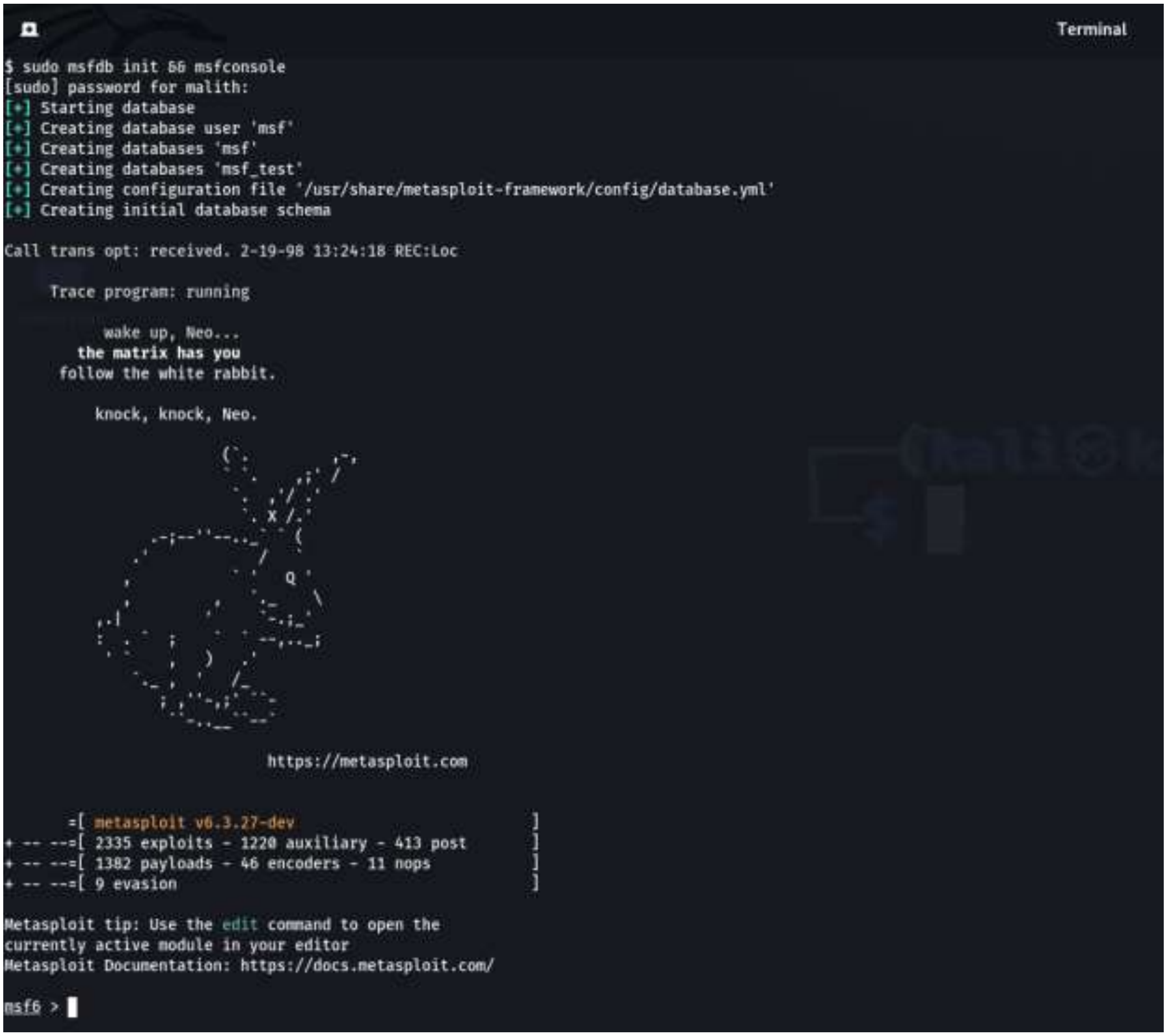
1. Live passive crawl from Proxy (all traffic)

Task type: Live passive crawl
Scope: Proxy (all traffic)
Configuration: Add links. Add item itself, same domain and URLs in suite scope.
Capturing

No items to show

3) Metasploit

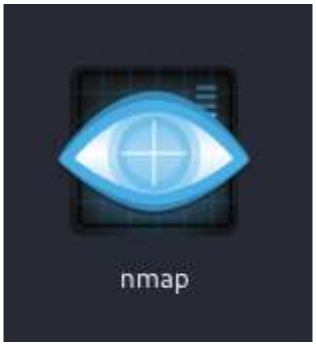
A well-known and flexible penetration testing tool, Metasploit helps security experts and ethical hackers evaluate and improve the security of systems and networks. It was created by Rapid7 and offers a full range of tools, exploits, and payloads for finding, using, and fixing vulnerabilities in a controlled setting. With its modular design, Metasploit's extensive library of known vulnerabilities allows for customization and automation of security assessments. Its effectiveness in finding weak spots, presenting actual assault scenarios, and assisting in the creation of strong defense methods is the reason for its appeal. Those that are devoted to protecting digital assets continue to have Metasploit as a key tool in their toolbox.



```
$ sudo msfdb init && msfconsole
[sudo] password for malith:
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` ` (
              .'            /   `
             ,           ` '   Q '
             ,         ,   `._    \
          ,.|         '     `-.;_'
          :  . `  ;    `  ` --,.._;
           ' `    ,   )   .'
              `._ ,  '   /_
                 ; ,''-,;' ``-
                  ``-..__``--`

                             https://metasploit.com


       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1382 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the edit command to open the
currently active module in your editor
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

4) Nmap

Network administrators and security experts use the well-known open-source network scanning application Nmap, also known as Network Mapper, to find and examine hosts and services on networks. Users may use this flexible tool to map network topologies, find available ports, and acquire crucial data about distant systems. Nmap includes a wide range of scanning methods, such as OS identification and version enumeration, and is very flexible. It helps identify possible vulnerabilities and enables businesses to guarantee the integrity of their network infrastructure, making it a crucial tool for network security evaluations. Nmap is a crucial tool for preserving and strengthening network security because of its ongoing development and community support.



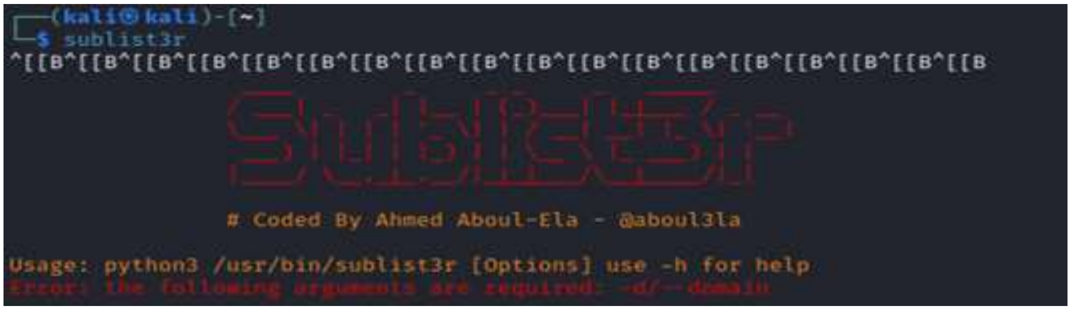
5) Nikto

Nikto is a well-known open-source web server vulnerability scanner that helps security experts find possible security problems in web servers and applications. Nikto, created by CIRT (Center for Internet Security), does thorough scans, evaluating a variety of typical online vulnerabilities and misconfigurations, including out-of-date software, known vulnerabilities, and server-specific problems. It is a command-line program that generates thorough results, making it appropriate for both human testing and automated security evaluations. Nikto is a significant addition to any security professional's toolset since it strengthens web server defenses by identifying and fixing vulnerabilities before bad actors can take advantage of them.

nikto

6) Sublist3r

A Python-based open-source program called Sublist3r is made specifically for subdomain enumeration and reconnaissance. It is used by penetration testers and security experts to find the subdomains connected to a target domain, assisting in the discovery of possible security issues and attack vectors. Sublist3r gathers a list of subdomains connected to the target domain using search engines like Google, Bing, and Yahoo as well as numerous DNS databases. This knowledge can be essential for calculating the assault surface and finding hidden assets that could otherwise go unnoticed. For experts working in online application security and penetration testing, Sublist3r is a useful tool because of its simplicity, speed, and interaction with other tools.



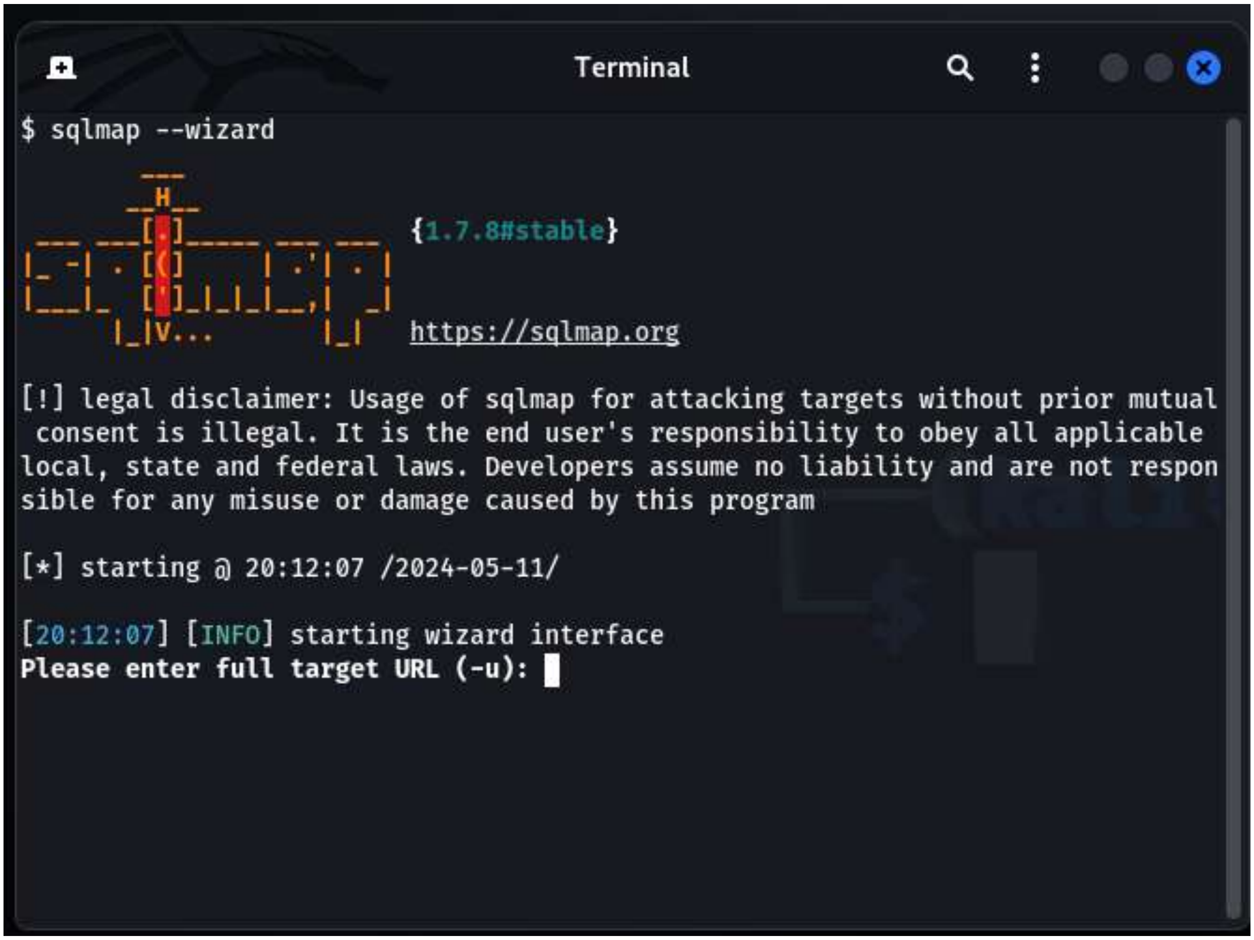
```
┌──(kali㉿kali)-[~]
└─$ sublist3r
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B

                       # Coded By Ahmed Aboul-Ela - @aboul3la

Usage: python3 /usr/bin/sublist3r [Options] use -h for help
Error: the following arguments are required: -d/--domain
```

7) Netsparker

Netsparker is a well-known online application security scanner and vulnerability assessment tool that businesses rely on to find and fix web-based security vulnerabilities. This automatic scanner, created by Netsparker Ltd., specializes in identifying a variety of vulnerabilities, such as SQL injection, Cross-Site Scripting (XSS), and more. Because it is not only identifies vulnerabilities but also verifies their presence, Proof-Based Scanning technology from Netsparker avoids false positives. It appeals to developers and security experts alike because to its automation features, user-friendly interface, and connection with development environments. In order for enterprises to properly safeguard their digital assets, Netsparker plays a crucial role in increasing web application security.

8) SQL Map

SQLMap is a popular open-source penetration testing tool specifically designed for detecting and exploiting SQL injection vulnerabilities in web applications and databases. Developed in Python, it streamlines the process of identifying and assessing SQL injection vulnerabilities, which can be a severe security risk. SQLMap automates the process of fingerprinting the database, enumerating tables, and extracting data, making it a valuable asset for ethical hackers and security professionals. Its extensive feature set and user-friendly command-line interface enable users to uncover and address these vulnerabilities, helping organizations secure their web applications against potentially devastating data breaches and manipulation attacks.



```
$ sqlmap --wizard
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.8#stable}
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 20:12:07 /2024-05-11/

[20:12:07] [INFO] starting wizard interface
Please enter full target URL (-u): 
```

Risk Level Information

High:

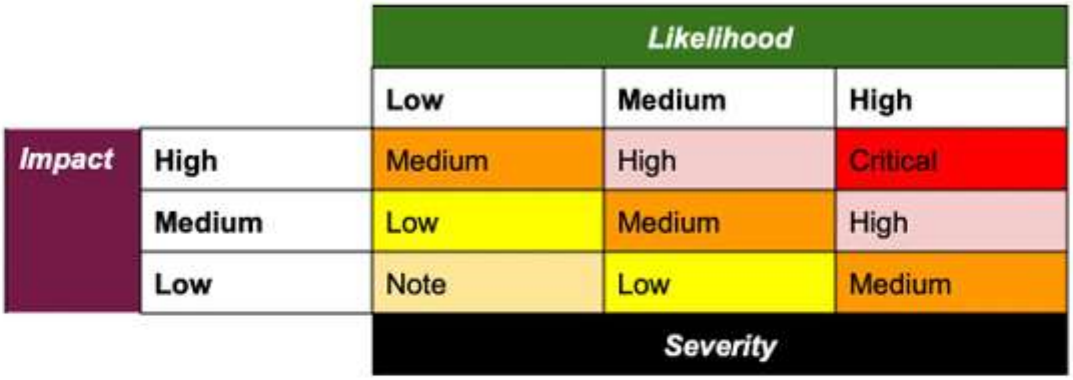
The high-risk rating displays the greatest danger connected to a particular vulnerability. The target application can be effectively exploited by an attacker, and the application data may be compromised partially or whole. An attacker may cause the web application's data to be modified or deleted.

Medium:

The medium risk level denotes a significant risk in conjunction with a particular vulnerability. An attacker can obtain low-level information about the program by taking advantage of a medium vulnerability. Medium risk vulnerabilities should be addressed after high-risk vulnerabilities.

Low:

The low-risk level denotes the danger that is least likely to be connected to a certain vulnerability. Gaining knowledge about the web application that was not meant to be known otherwise may result from this.



		Likelihood		
		Low	Medium	High
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Severity		

Daily Journal-(20.04.2024)

This phase is the vast area of the bug bounty program. I had to spend several hours learning how to find new bugs and how to use the tools to find the bugs. With the limited time had It was so much harder to allocate time for my other work.

Objectives:

- How to use the tools properly.
- How to use Automated Tools.
- How to Identify Vulnerabilities.
- Find Open ports.
- Find Subdomains.
- Find Vulnerabilities.
- Create Reports.

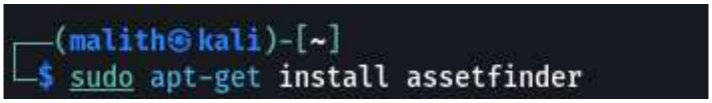
Sources Used:

- Youtube.
- Portswigger.
- Hackerone.
- Bugcrowd.
- Linkedin.
- Facebook (Bug Bounty Groups)
- Google.

Bug Bounty 1 (freshworks)

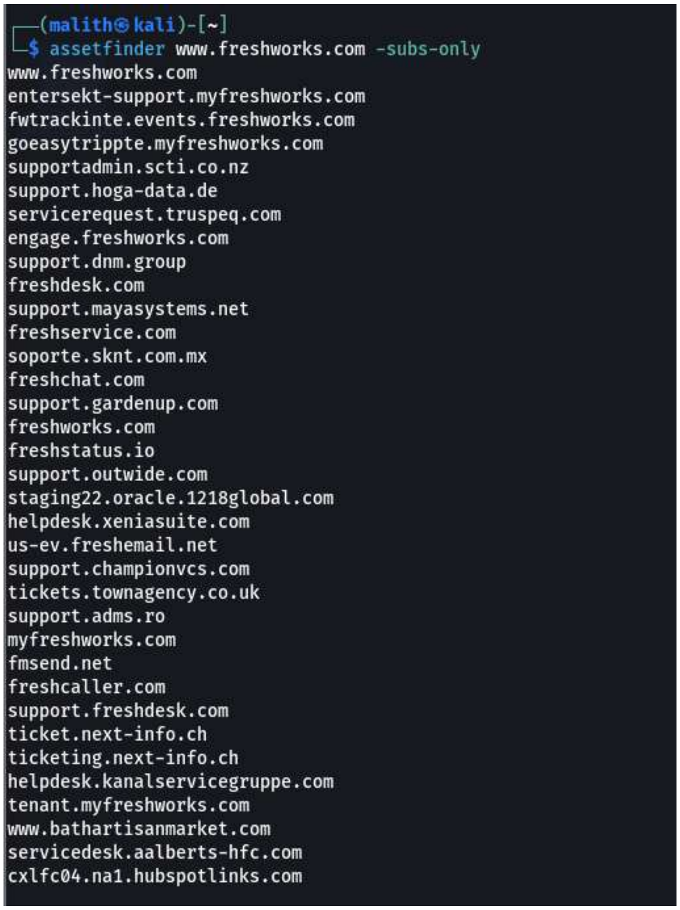
Reconnaissance

Firstly, I used the Assetfinder tool to find the subdomains of the freshworks website. Assetfinder tool is used to find the subdomains of a website. To install the Assetfinder we must use the command:



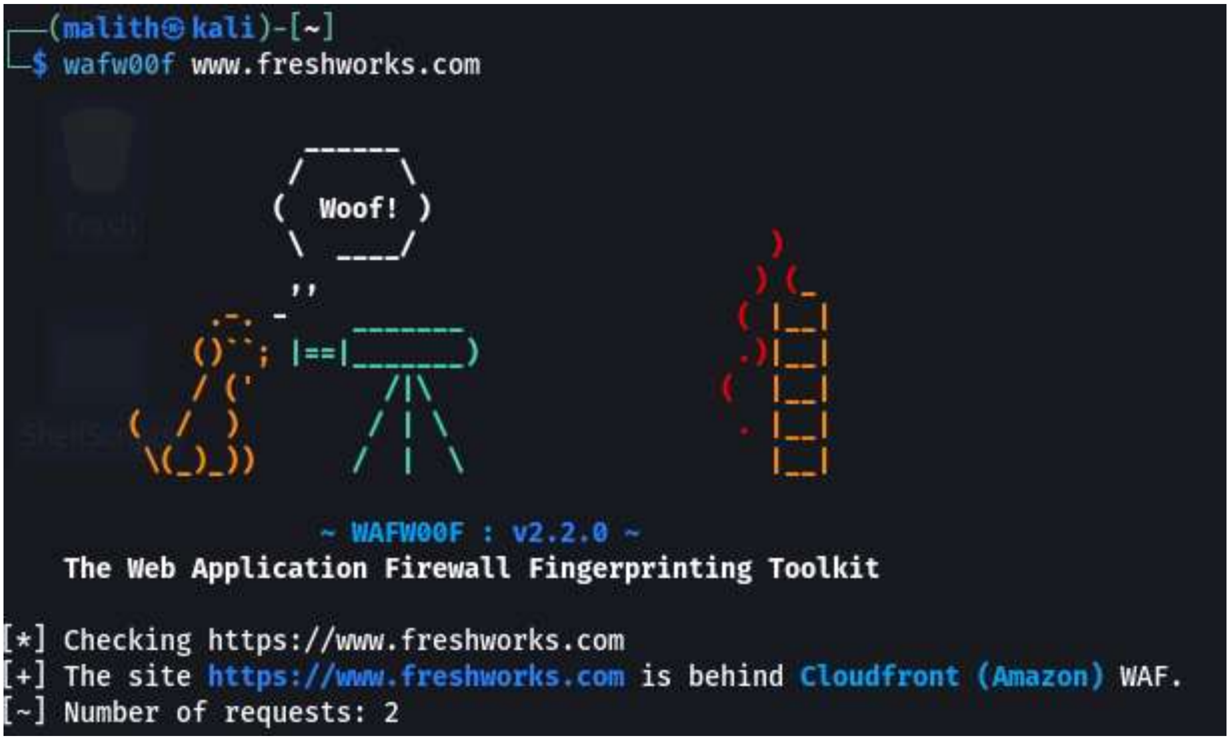
```
┌──(malith㉿kali)-[~]
└─$ sudo apt-get install assetfinder
```

Then, I got the subdomains list as below.



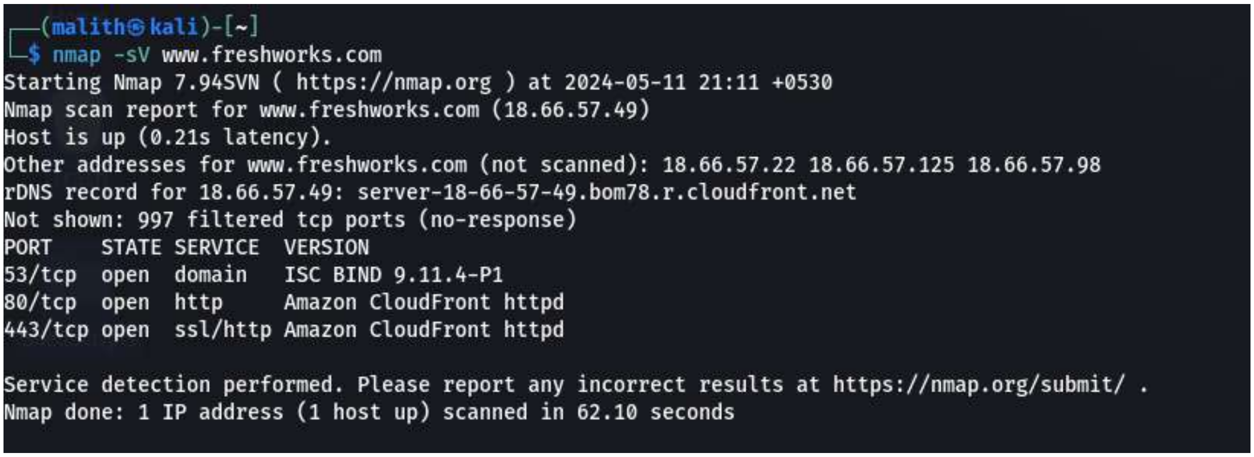
```
┌──(malith㉿kali)-[~]
└─$ assetfinder www.freshworks.com -subs-only
www.freshworks.com
entersekt-support.myfreshworks.com
fwtrackinte.events.freshworks.com
goeasytrippte.myfreshworks.com
supportadmin.scti.co.nz
support.hoga-data.de
servicerequest.truspeq.com
engage.freshworks.com
support.dnm.group
freshdesk.com
support.mayasystems.net
freshservice.com
soporte.sknt.com.mx
freshchat.com
support.gardenup.com
freshworks.com
freshstatus.io
support.outwide.com
staging22.oracle.1218global.com
helpdesk.xeniasuite.com
us-ev.freshemail.net
support.championvcs.com
tickets.townagency.co.uk
support.adms.ro
myfreshworks.com
fmsend.net
freshcaller.com
support.freshdesk.com
ticket.next-info.ch
ticketing.next-info.ch
helpdesk.kanalservicegruppe.com
tenant.myfreshworks.com
www.bathartisanmarket.com
servicedesk.aalberts-hfc.com
cxlfc04.na1.hubspotlinks.com
```

I also found that freshworks website is running behind a firewall “Azure Front Door (Microsoft)”. To find the firewall I used the wafw00f tool. The commands and the results are shown from the below screenshots.



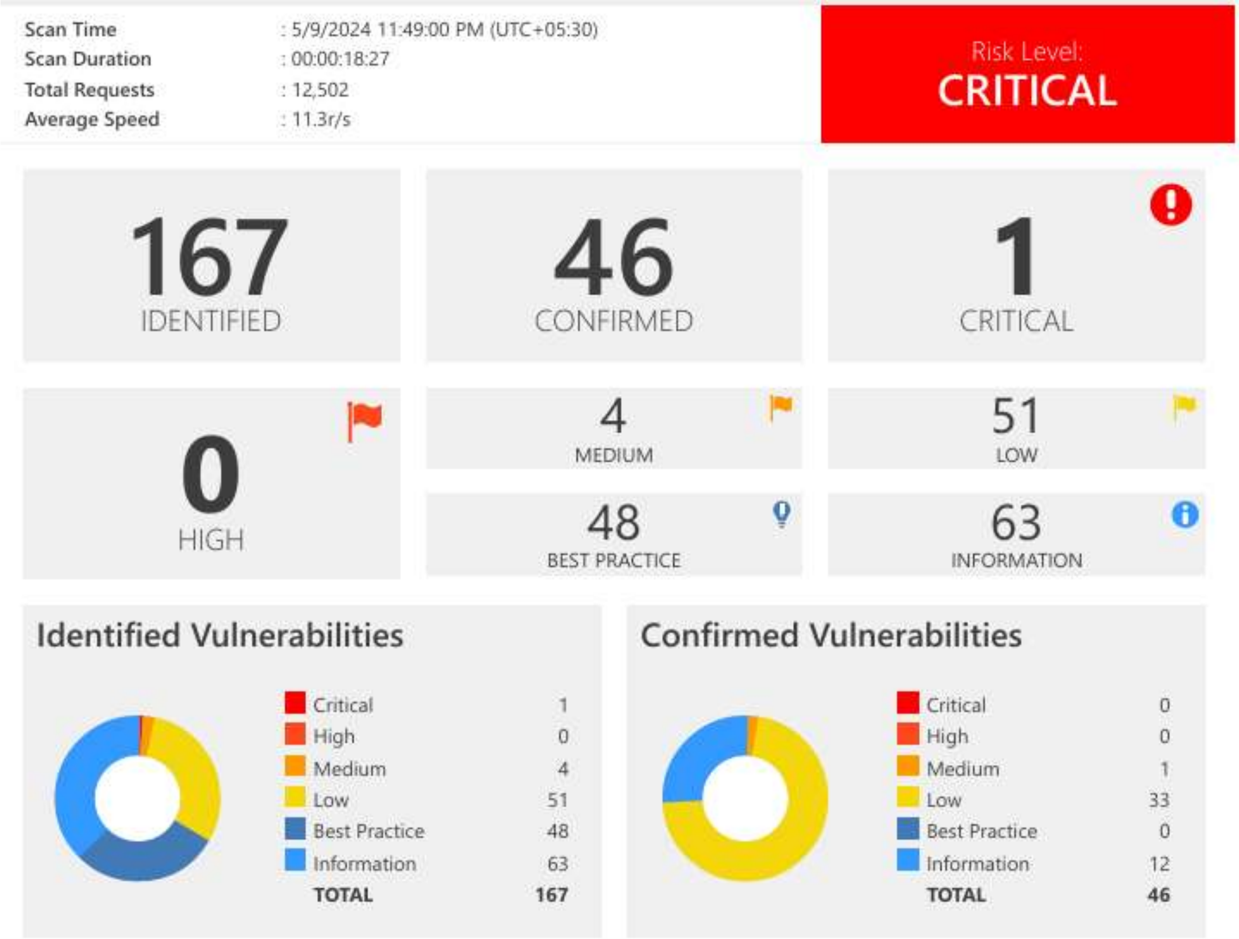
```
┌──(malith㉿kali)-[~]
└─$ wafw00f www.freshworks.com

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.freshworks.com
[+] The site https://www.freshworks.com is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

I used the nmap tool to find whether there are any unusual ports are opened but there weren’t any unusual ports opened.



```
┌──(malith㉿kali)-[~]
└─$ nmap -sV www.freshworks.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 21:11 +0530
Nmap scan report for www.freshworks.com (18.66.57.49)
Host is up (0.21s latency).
Other addresses for www.freshworks.com (not scanned): 18.66.57.22 18.66.57.125 18.66.57.98
rDNS record for 18.66.57.49: server-18-66-57-49.bom78.r.cloudfront.net
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   ISC BIND 9.11.4-P1
80/tcp  open  http     Amazon CloudFront httpd
443/tcp open  ssl/http Amazon CloudFront httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.10 seconds
```

Vulnerabilities Found.



Scan Time	: 5/9/2024 11:49:00 PM (UTC+05:30)
Scan Duration	: 00:00:18:27
Total Requests	: 12,502
Average Speed	: 11.3r/s

Risk Level:
CRITICAL

167	IDENTIFIED
46	CONFIRMED
1	CRITICAL
0	HIGH
4	MEDIUM
51	LOW
48	BEST PRACTICE
63	INFORMATION

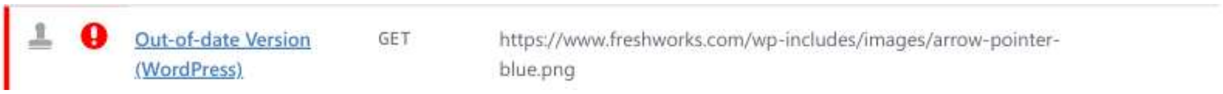
Identified Vulnerabilities

🟥	Critical	1
🟧	High	0
🟧	Medium	4
🟨	Low	51
🟦	Best Practice	48
🟦	Information	63
	TOTAL	**167**

Confirmed Vulnerabilities

🟥	Critical	0
🟧	High	0
🟧	Medium	1
🟨	Low	33
🟦	Best Practice	0
🟦	Information	12
	TOTAL	**46**

Out-of-date Version (WordPress)



Out-of-date Version (WordPress) GET https://www.freshworks.com/wp-includes/images/arrow-pointer-blue.png

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.freshworks.com . This vulnerability belongs to Vulnerable and Outdated components (A06-2021) 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

The "Out-of-Date Version (OpenSSL) vulnerability" is a big security problem because it uses old and possibly not safe versions of the software called OpenSSL. OpenSSL is commonly used to safely send information over computer networks and is important for many online services and applications. Using an old version of OpenSSL can make your systems vulnerable to cyber threats like data breaches, attacks where someone secretly listens or changes your messages, and hackers being able to control your system from a distance. It is very important to fix this problem to keep digital messages and data safe and secure. Regularly updating OpenSSL to the latest secure versions, making sure to fix any problems, and checking for vulnerabilities are important steps to reduce the risk and protect sensitive information from being used by bad people.

Impact Assessment

The following are some possible risks and effects for www.echobox.com that could arise from the vulnerability caused by using an outdated version of OpenSSL:

1. **Security Weakness:** Older versions of OpenSSL can have known flaws that are exploitable by hostile parties. This produces a security vulnerability that can allow unwanted access to private information or jeopardize the security of the website.

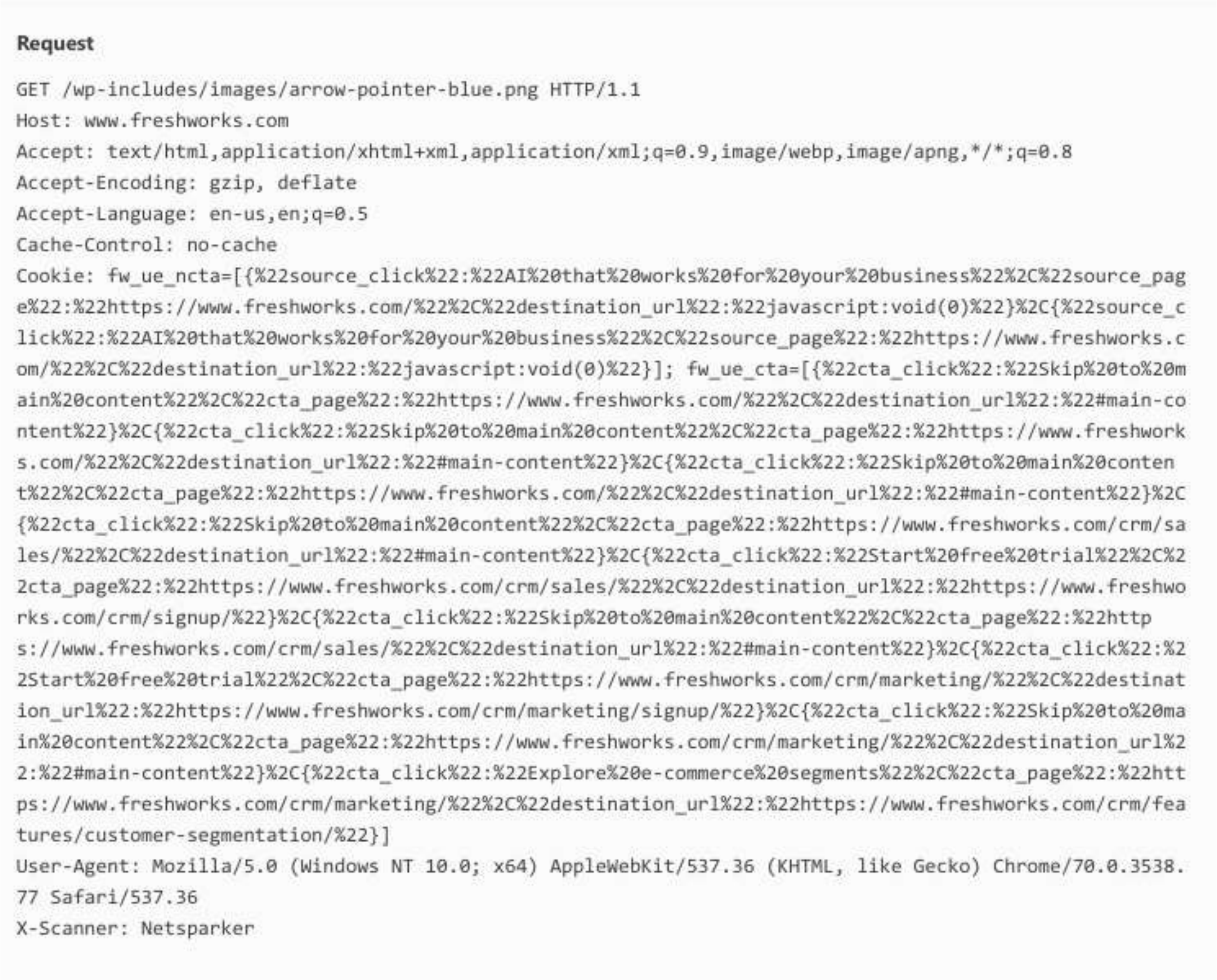
2. **Inaccurate Data:** Data breaches are more likely when OpenSSL is being used obsoletely. Cybercriminals may take use of well-known weaknesses in the OpenSSL version to obtain private user data, including payment information, login passwords, and personal information. Financial and legal repercussions may follow a data breach.

3. **Disagreement with Users:** Users anticipate a secure handling of their information. Users' trust and confidence in www.echobox.com's security procedures may be damaged if it is discovered that the website is employing obsolete and unsafe versions of OpenSSL. Users may become less engaged with the platform as a result and the website's reputation may suffer.

4. **Non-compliance with regulations:** Violating cybersecurity and data protection laws may result from using obsolete and insecure versions of OpenSSL. The reputation of the website could be harmed in addition to possible financial and legal repercussions.

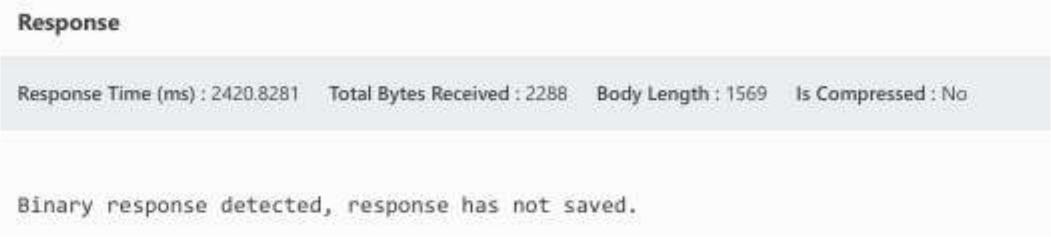
The most recent secure version of OpenSSL should be quickly updated and patched by www.echobox.com to solve this vulnerability. To reduce these risks, it's crucial to routinely check for OpenSSL updates and implement security patches. The website will be able to improve security, preserve user confidence, guarantee regulatory compliance, and safeguard sensitive data by doing this. The precise consequences of this vulnerability are contingent upon the activities of possible aggressors and the vulnerabilities present in the obsolete version of OpenSSL.

- ## Proof of Concept



Request

```
GET /wp-includes/images/arrow-pointer-blue.png HTTP/1.1
Host: www.freshworks.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
Cookie: fw_ue_ncta=[{%22source_click%22:%22AI%20that%20works%20for%20your%20business%22%2C%22source_pag
e%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22javascript:void(0)%22}%2C{%22source_c
lick%22:%22AI%20that%20works%20for%20your%20business%22%2C%22source_page%22:%22https://www.freshworks.c
om/%22%2C%22destination_url%22:%22javascript:void(0)%22}]; fw_ue_cta=[{%22cta_click%22:%22Skip%20to%20m
ain%20content%22%2C%22cta_page%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22#main-co
ntent%22}%2C{%22cta_click%22:%22Skip%20to%20main%20content%22%2C%22cta_page%22:%22https://www.freshwork
s.com/%22%2C%22destination_url%22:%22#main-content%22}%2C{%22cta_click%22:%22Skip%20to%20main%20conten
t%22%2C%22cta_page%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22#main-content%22}%2C
{%22cta_click%22:%22Skip%20to%20main%20content%22%2C%22cta_page%22:%22https://www.freshworks.com/crm/sa
les/%22%2C%22destination_url%22:%22#main-content%22}%2C{%22cta_click%22:%22Start%20free%20trial%22%2C%2
2cta_page%22:%22https://www.freshworks.com/crm/sales/%22%2C%22destination_url%22:%22https://www.freshwo
rks.com/crm/signup/%22}%2C{%22cta_click%22:%22Skip%20to%20main%20content%22%2C%22cta_page%22:%22http
s://www.freshworks.com/crm/sales/%22%2C%22destination_url%22:%22#main-content%22}%2C{%22cta_click%22:%2
2Start%20free%20trial%22%2C%22cta_page%22:%22https://www.freshworks.com/crm/marketing/%22%2C%22destinat
ion_url%22:%22https://www.freshworks.com/crm/marketing/signup/%22}%2C{%22cta_click%22:%22Skip%20to%20ma
in%20content%22%2C%22cta_page%22:%22https://www.freshworks.com/crm/marketing/%22%2C%22destination_url%2
2:%22#main-content%22}%2C{%22cta_click%22:%22Explore%20e-commerce%20segments%22%2C%22cta_page%22:%22htt
ps://www.freshworks.com/crm/marketing/%22%2C%22destination_url%22:%22https://www.freshworks.com/crm/fea
tures/customer-segmentation/%22}]
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) : 2420.8281 **Total Bytes Received** : 2288 **Body Length** : 1569 **Is Compressed** : No

```
Binary response detected, response has not saved.
```

- ## Remediation

Please upgrade your installation of WordPress to the latest stable version

Missing X-Frame-Options Header

Missing X-Frame-Options Header GET https://www.freshworks.com/apps/

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.freshworks.com . This vulnerability belongs to the Security Misconfigurations (A05)-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

In online applications, the lack of an X-Frame-Options header poses a serious risk. This header is necessary to stop clickjacking attacks, in which malevolent parties try to insert a weak site inside an iframe on a different domain with the intention of inflicting damage. In the event that the X-Frame-Options header is incorrectly set, private data might be accessed or compromised. Web developers should always provide this header in the response of their application, indicating whether or not the page may be framed by other websites, in order to lessen the risk of this happening. This precaution is essential for maintaining the reliability and security of online material, thereby shielding consumers from potential security flaws and invasions of privacy.

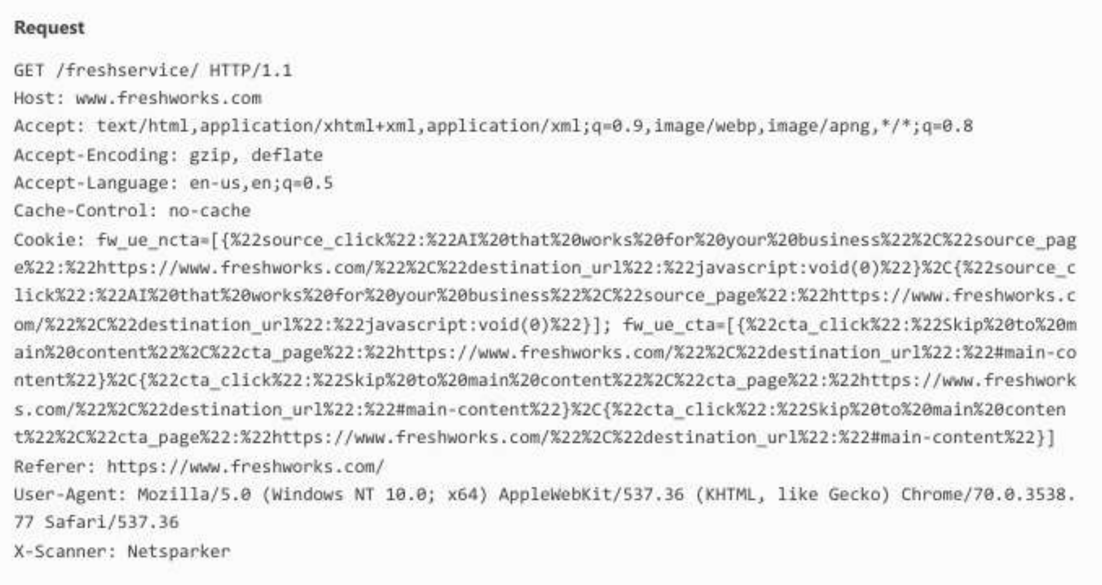
Impact Assessment

The Missing of the X-Frame-Options header on www.starbucks.com presents multiple vulnerabilities in the context of the OWASP category. If this security precaution isn't taken, bad actors could use Clickjacking and other attacks to undermine the integrity of the web application and possibly do a lot of damage. Should attackers be successful in using this vulnerability, the following situations might occur:

- Unauthorized Data Access: By deceiving visitors into inadvertently interacting with a website using Clickjacking, attackers can obtain sensitive user data, including financial information, login passwords, and personal information.
- Service Disruption: An attacker can interfere with the Starbucks website's operation by inserting a malicious frame into it, rendering it inaccessible to users for a short while or permanently. Financial losses as well as a bad user experience may result from this disruption.
- Malicious Use of Starbucks Domain: Phishing, denial-of-service, and malware distribution are just a few of the ways malicious actors may use the compromised Starbucks domain. This could hurt innocent customers in addition to damaging Starbucks' reputation.

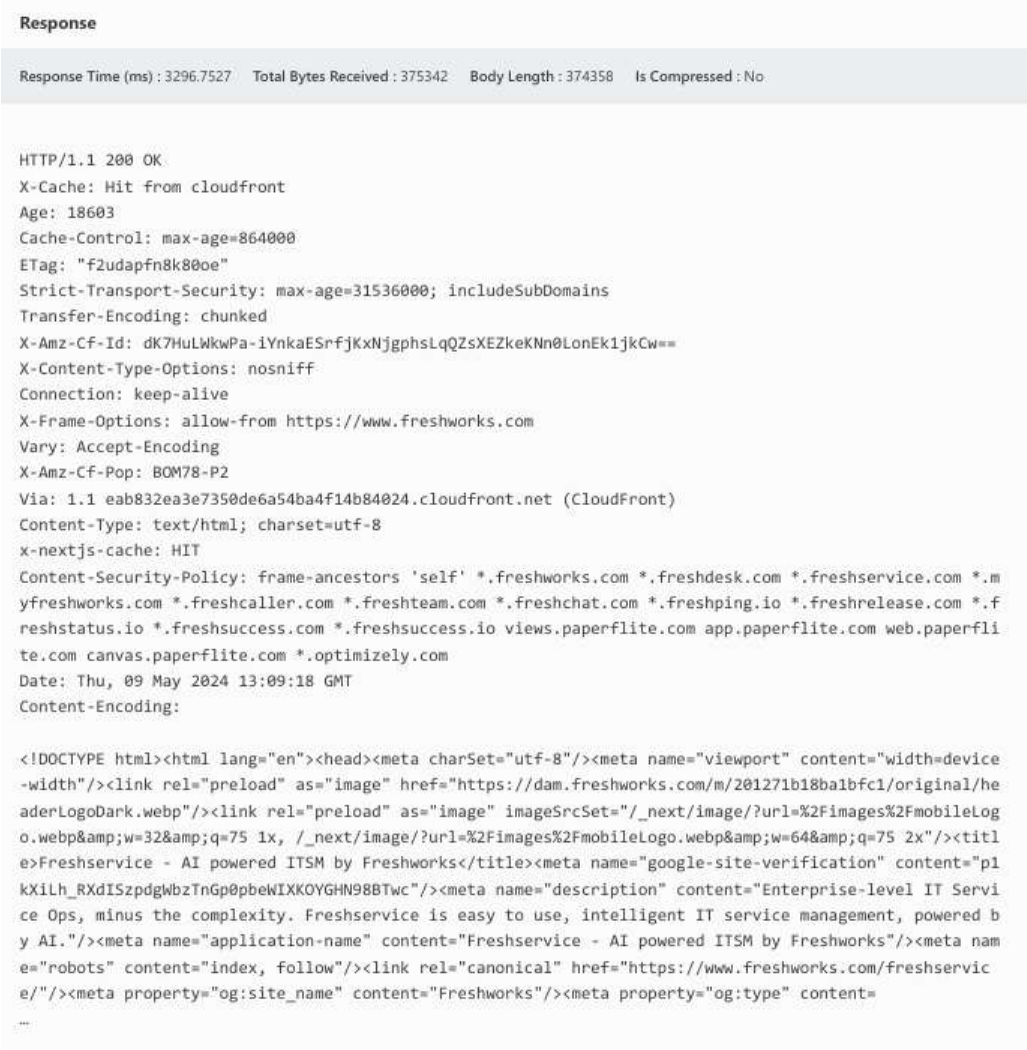
It's crucial to remember that these are merely a few possible outcomes of taking advantage of this weakness. The precise strategies used by hostile actors and the weaknesses they take advantage of may determine the true effect of the attack. Starbucks must employ the X-Frame-Options header and other security steps to guard its web application and users in order to reduce these risks.

- ## Proof of Concept



Request

```
GET /freshservice/ HTTP/1.1
Host: www.freshworks.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
Cookie: fw_ue_ncta=[{%22source_click%22:%22AI%20that%20works%20for%20your%20business%22%2C%22source_pag
e%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22javascript:void(0)%22}%2C{%22source_c
lick%22:%22AI%20that%20works%20for%20your%20business%22%2C%22source_page%22:%22https://www.freshworks.c
om/%22%2C%22destination_url%22:%22javascript:void(0)%22}]; fw_ue_cta=[{%22cta_click%22:%22Skip%20to%20m
ain%20content%22%2C%22cta_page%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22#main-co
ntent%22}%2C{%22cta_click%22:%22Skip%20to%20main%20content%22%2C%22cta_page%22:%22https://www.freshwork
s.com/%22%2C%22destination_url%22:%22#main-content%22}%2C{%22cta_click%22:%22Skip%20to%20main%20conten
t%22%2C%22cta_page%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22#main-content%22}]
Referer: https://www.freshworks.com/
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) : 3296.7527 Total Bytes Received : 375342 Body Length : 374358 Is Compressed : No

```
HTTP/1.1 200 OK
X-Cache: Hit from cloudfront
Age: 18603
Cache-Control: max-age=864000
ETag: "f2udapfn8k80oe"
Strict-Transport-Security: max-age=31536000; includeSubDomains
Transfer-Encoding: chunked
X-Amz-Cf-Id: dK7HuLWkwPa-iYnkaESrfjKxNjgphsLqQZsXEZkeKNn0LonEk1jkCw==
X-Content-Type-Options: nosniff
Connection: keep-alive
X-Frame-Options: allow-from https://www.freshworks.com
Vary: Accept-Encoding
X-Amz-Cf-Pop: BOM78-P2
Via: 1.1 eab832ea3e7350de6a54ba4f14b84024.cloudfront.net (CloudFront)
Content-Type: text/html; charset=utf-8
x-nextjs-cache: HIT
Content-Security-Policy: frame-ancestors 'self' *.freshworks.com *.freshdesk.com *.freshservice.com *.m
yfreshworks.com *.freshcaller.com *.freshteam.com *.freshchat.com *.freshping.io *.freshrelease.com *.f
reshstatus.io *.freshsuccess.com *.freshsuccess.io views.paperflite.com app.paperflite.com web.paperfli
te.com canvas.paperflite.com *.optimizely.com
Date: Thu, 09 May 2024 13:09:18 GMT
Content-Encoding:

<!DOCTYPE html><html lang="en"><head><meta charSet="utf-8"/><meta name="viewport" content="width=device
-width"/><link rel="preload" as="image" href="https://dam.freshworks.com/m/201271b18ba1bfc1/original/he
aderLogoDark.webp"/><link rel="preload" as="image" imageSrcSet="/_next/image/?url=%2Fimages%2FmobileLog
o.webp&amp;w=32&amp;q=75 1x, /_next/image/?url=%2Fimages%2FmobileLogo.webp&amp;w=64&amp;q=75 2x"/><titl
e>Freshservice - AI powered ITSM by Freshworks</title><meta name="google-site-verification" content="p1
kXiLh_RXdISzpdgWbzTnGp0pbeWIXKOYGHN98BTwc"/><meta name="description" content="Enterprise-level IT Servi
ce Ops, minus the complexity. Freshservice is easy to use, intelligent IT service management, powered b
y AI."/><meta name="application-name" content="Freshservice - AI powered ITSM by Freshworks"/><meta nam
e="robots" content="index, follow"/><link rel="canonical" href="https://www.freshworks.com/freshservic
e/"/><meta property="og:site_name" content="Freshworks"/><meta property="og:type" content=
…
```

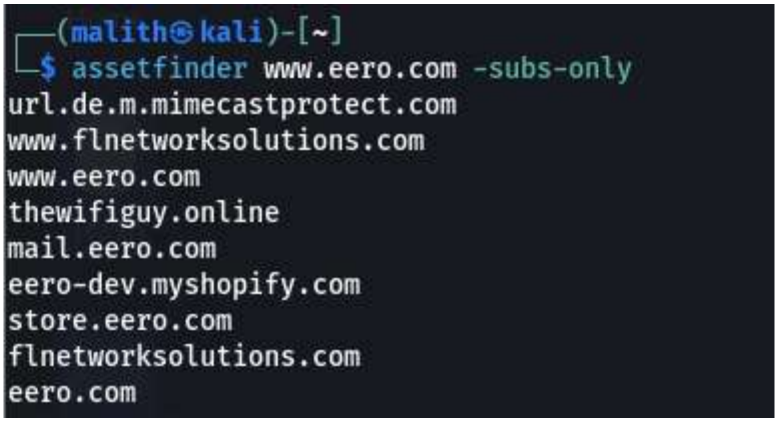
- **Remediation**

Either use the DENYor SAMEORIGINheader value to support the majority of browsers. Additionally, you can define the frame ancestorsContent-Security-Policy directive.

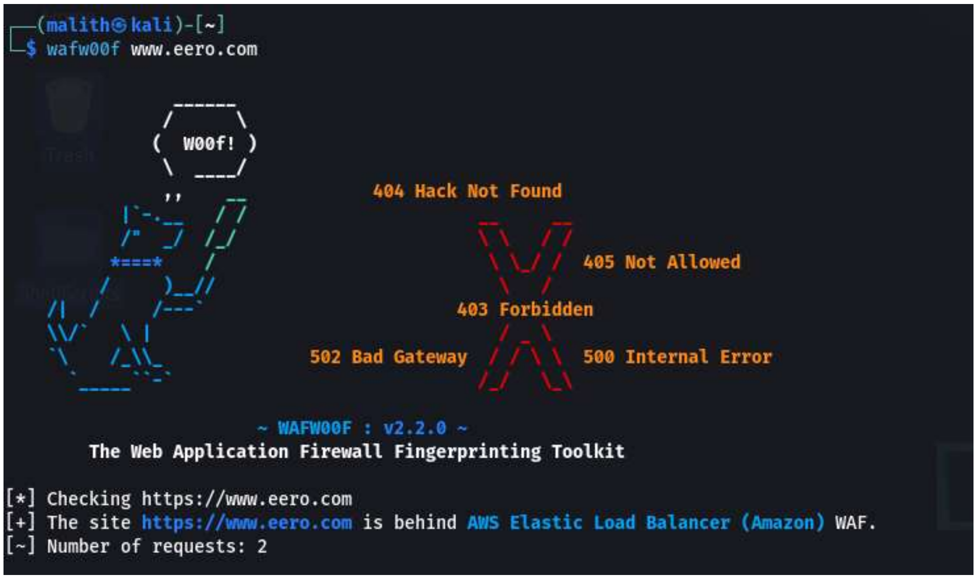
Bug Bounty 2 (eero)

Reconnaissance

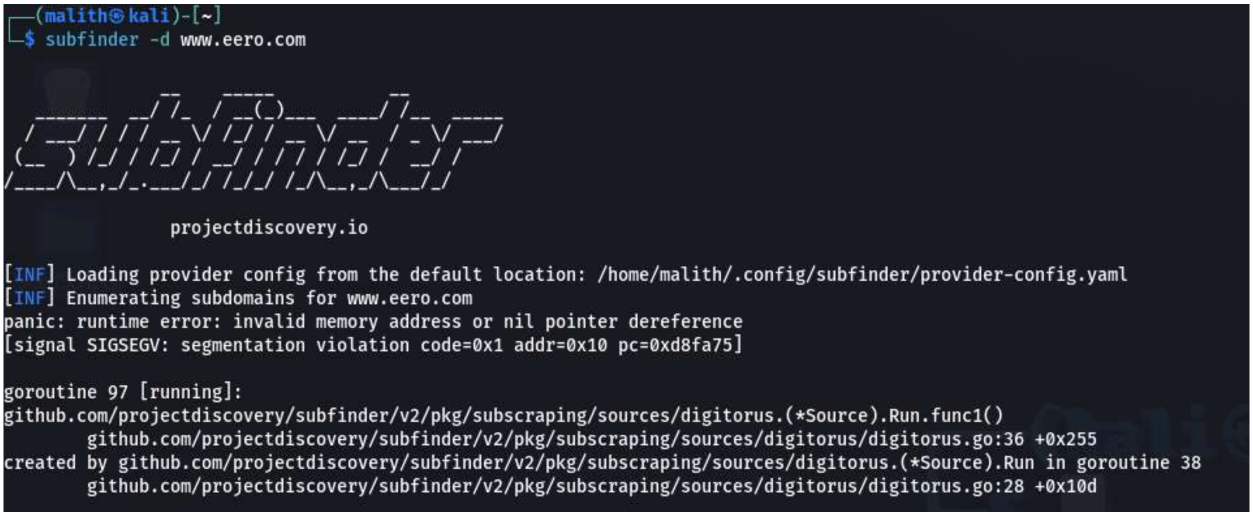
Firstly, I used the Assetfinder tool to find the subdomains of the eero website. Assetfinder tool is used to find the subdomains of a website.



```
┌──(malith㉿kali)-[~]
└─$ assetfinder www.eero.com -subs-only
url.de.m.mimecastprotect.com
www.flnetworksolutions.com
www.eero.com
thewifiguy.online
mail.eero.com
eero-dev.myshopify.com
store.eero.com
flnetworksolutions.com
eero.com
```

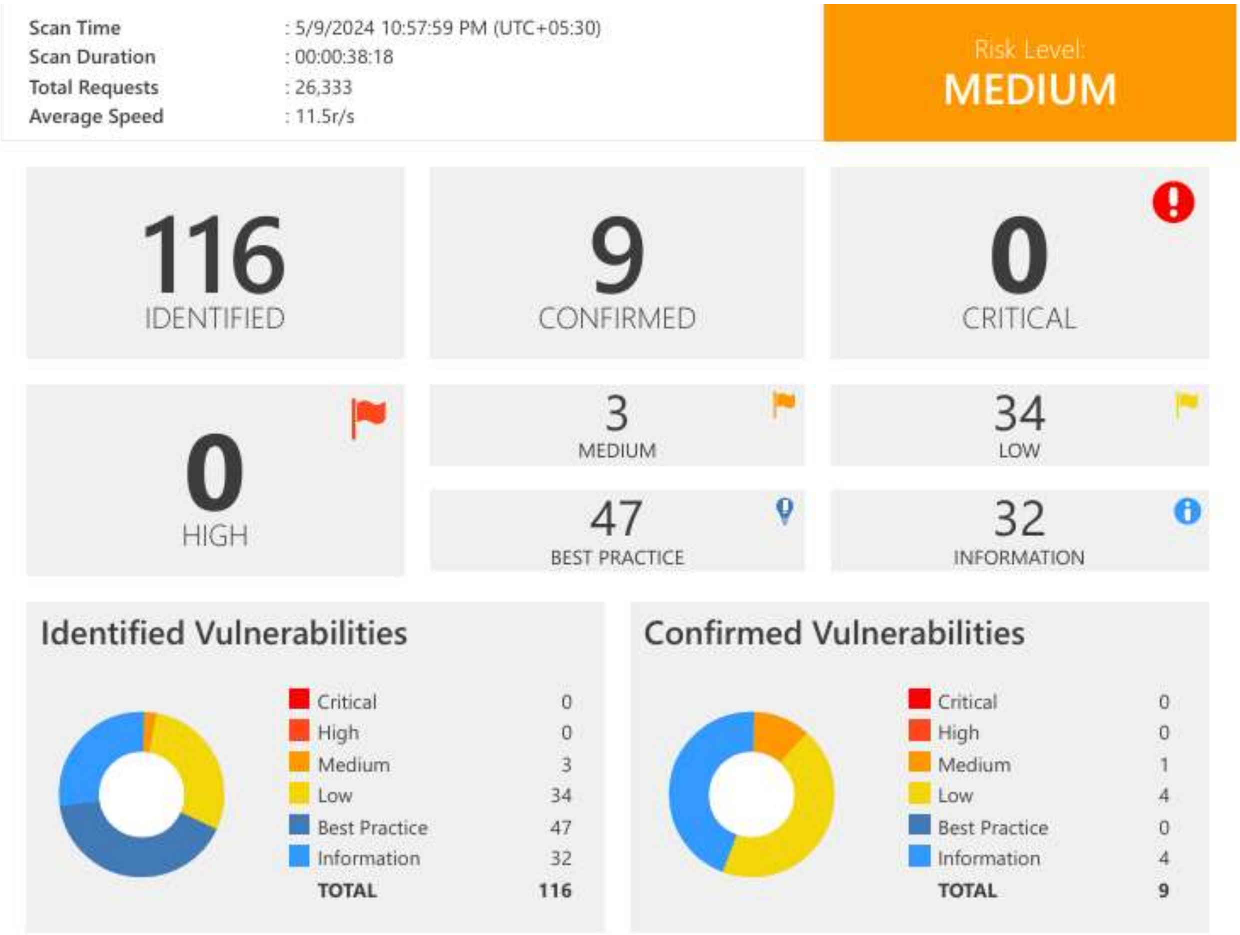


```
┌──(malith㉿kali)-[~]
└─$ wafw00f www.eero.com

                ______
               /      \
              (  W00f! )
               \  ____/
               ,,              404 Hack Not Found

                                                 405 Not Allowed

                                      403 Forbidden

                         502 Bad Gateway          500 Internal Error

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.eero.com
[+] The site https://www.eero.com is behind AWS Elastic Load Balancer (Amazon) WAF.
[~] Number of requests: 2
```



```
┌──(malith㉿kali)-[~]
└─$ subfinder -d www.eero.com

               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Loading provider config from the default location: /home/malith/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for www.eero.com
panic: runtime error: invalid memory address or nil pointer dereference
[signal SIGSEGV: segmentation violation code=0x1 addr=0x10 pc=0xd8fa75]

goroutine 97 [running]:
github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run.func1()
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:36 +0x255
created by github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run in goroutine 38
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:28 +0x10d
```

Vulnerabilities Found.



Scan Time	: 5/9/2024 10:57:59 PM (UTC+05:30)
Scan Duration	: 00:00:38:18
Total Requests	: 26,333
Average Speed	: 11.5r/s

Risk Level:
MEDIUM

116 IDENTIFIED

9 CONFIRMED

0 CRITICAL

0 HIGH

3 MEDIUM

34 LOW

47 BEST PRACTICE

32 INFORMATION

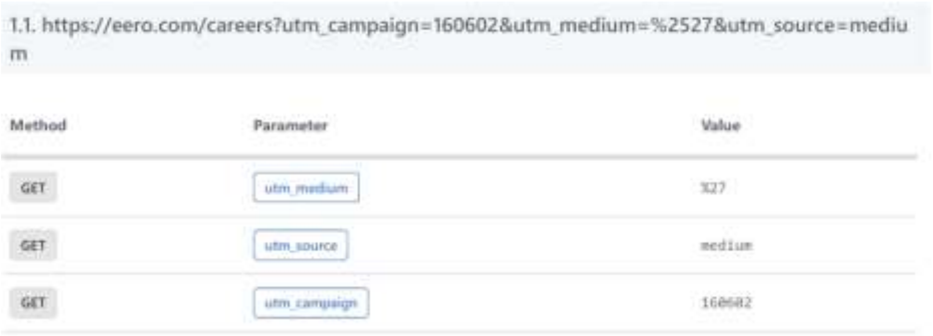
Identified Vulnerabilities

Critical	0
High	0
Medium	3
Low	34
Best Practice	47
Information	32
TOTAL	**116**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	4
Best Practice	0
Information	4
TOTAL	**9**

[Possible] BREACH Attack Detected



1.1. https://eero.com/careers?utm_campaign=160602&utm_medium=%2527&utm_source=medium

Method	Parameter	Value
GET	utm_medium	%27
GET	utm_source	medium
GET	utm_campaign	160602

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.eero.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

The vulnerability identified as [Possible] Breach Attack Detected indicates a potentially serious security risk. It usually means that illegal or suspicious activity has been found within a network or system by the intrusion detection system or security monitoring tools. The word "Possible" emphasizes the need of an instant inquiry and reaction, even though it suggests that the breach hasn't been conclusively established. These weaknesses may result in data theft, system compromise, or illegal access. In order to resolve this problem, a prompt and complete reaction is needed. This includes analyzing the detected activity in detail, determining the possible source of the breach, and putting security measures in place to stop future exploitation. The significance of proactive threat detection and incident response techniques in preserving sensitive data and network integrity is highlighted by this vulnerability.

• Impact Assessment

In relation to the OWASP category about a [Possible] Breach Attack Detected vulnerability on the website www.eero.com , several security risks and repercussions have been found. The following possible outcomes are among the significant effects of this vulnerability:

consequences:

1. **Data Compromise:** As this case indicates, a breach attack may result in unauthorized access to private information kept on the eero website. This could include private data such as payment information and customer information.

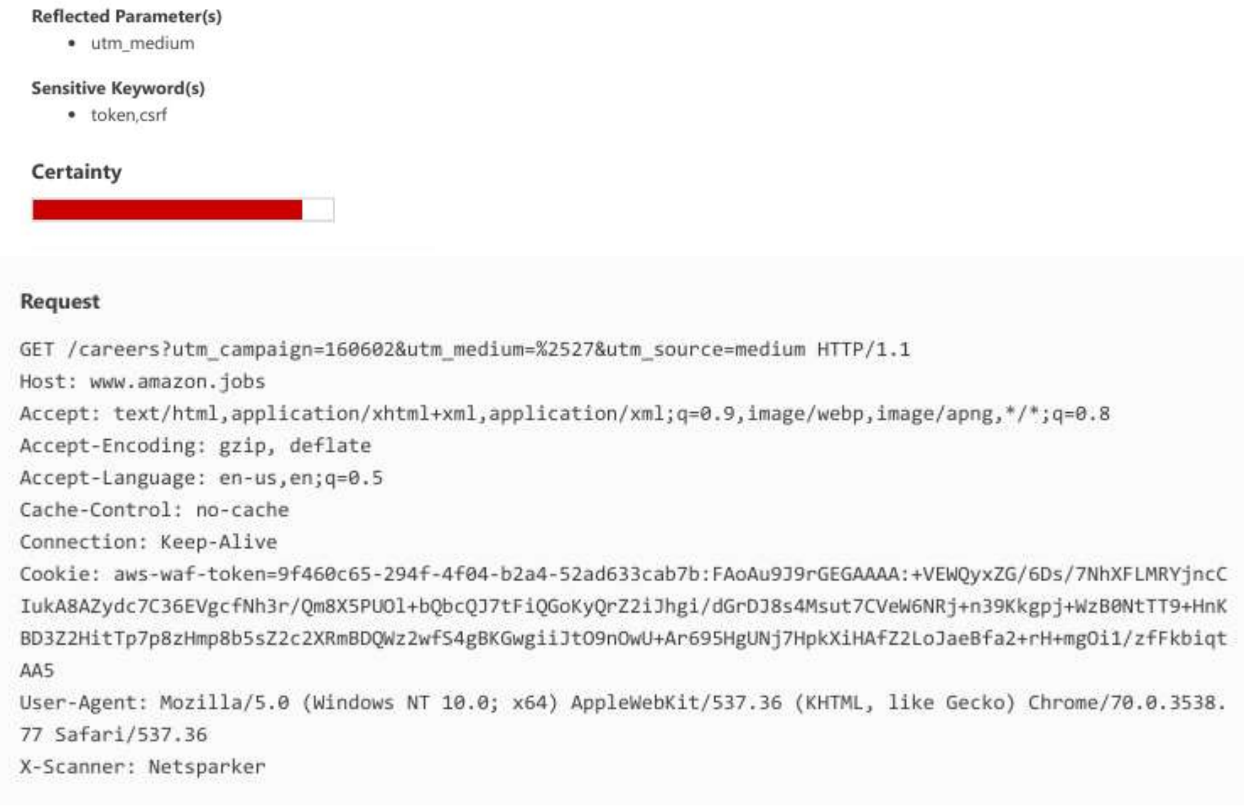
2. **Privacy Violation:** A breach attack might violate user privacy, which would be upsetting to the impacted customers and might put eero in legal hot water.

3. **Financial Consequences:** Financial repercussions from breach occurrences might include regulatory fines, legal costs, and the requirement to compensate impacted parties. The financial stability of eero may be impacted by these obligations.

4. **Operational Disruption:** eero's regular activities may be disrupted when responding to a breach attack, which calls for significant resources. It might take a lot of time and resources to respond to incidents, remediate them, and communicate with others.

Strengthening security measures, keeping an eye out for attempted breaches, and regularly evaluating and improving the website's security controls are essential for mitigating this vulnerability. Users are put in danger when this problem is ignored, and Boozt's standing, financial soundness, and general business ethics are all at stake. Depending on the behavior of hostile actors and the degree of security flaws on the website, the vulnerability's exact impact may vary.

- ## Request



Reflected Parameter(s)

- utm_medium

Sensitive Keyword(s)

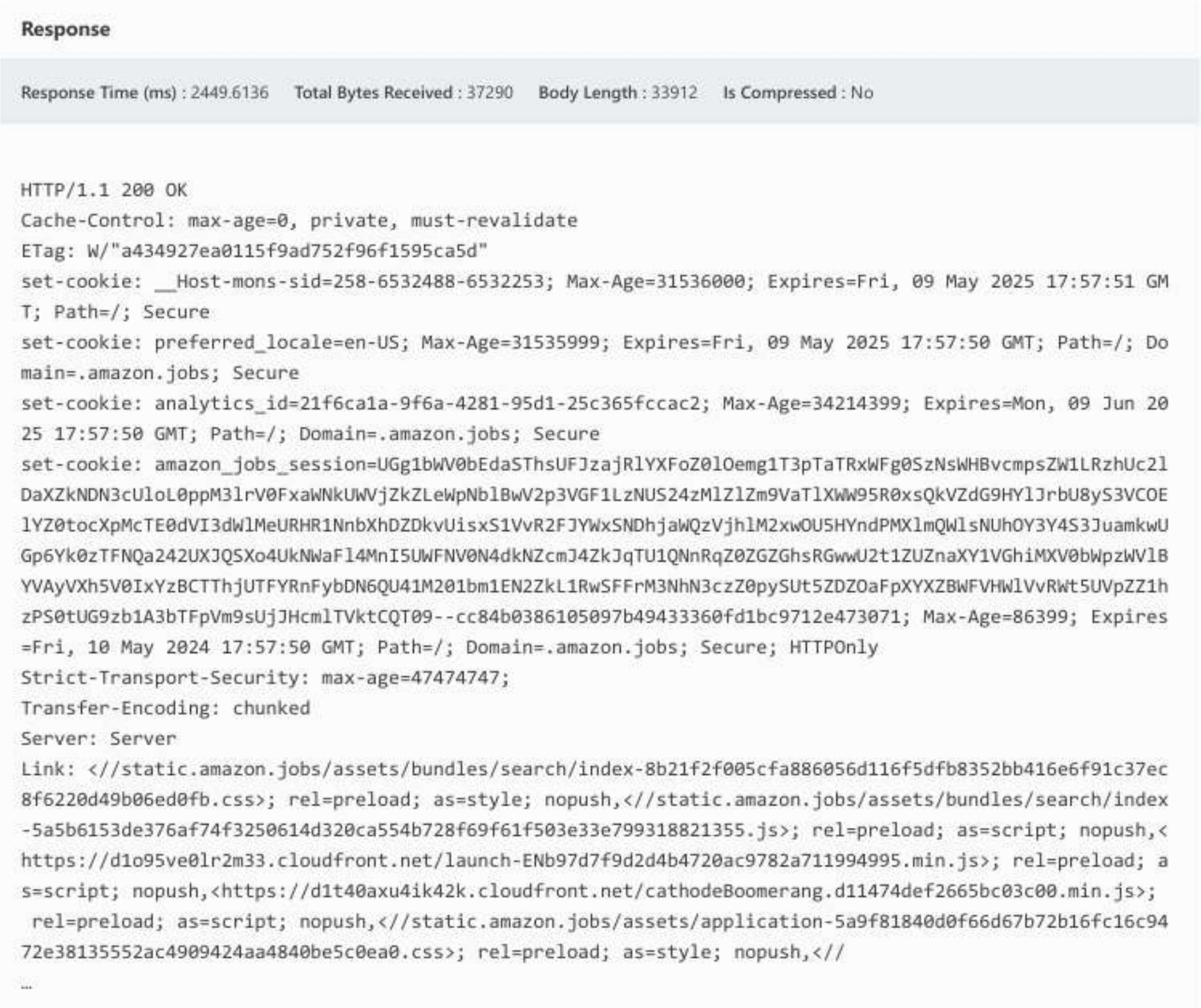
- token,csrf

Certainty

Request

```
GET /careers?utm_campaign=160602&utm_medium=%2527&utm_source=medium HTTP/1.1
Host: www.amazon.jobs
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
Connection: Keep-Alive
Cookie: aws-waf-token=9f460c65-294f-4f04-b2a4-52ad633cab7b:FAoAu9J9rGEGAAAA:+VEWQyxZG/6Ds/7NhXFLMRYjncC
IukA8AZydc7C36EVgcfNh3r/Qm8X5PUOl+bQbcQJ7tFiQGoKyQrZ2iJhgi/dGrDJ8s4Msut7CVeW6NRj+n39Kkgpj+WzB0NtTT9+HnK
BD3Z2HitTp7p8zHmp8b5sZ2c2XRmBDQWz2wfS4gBKGwgiiJtO9nOwU+Ar695HgUNj7HpkXiHAfZ2LoJaeBfa2+rH+mgOi1/zfFkbiqt
AA5
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**

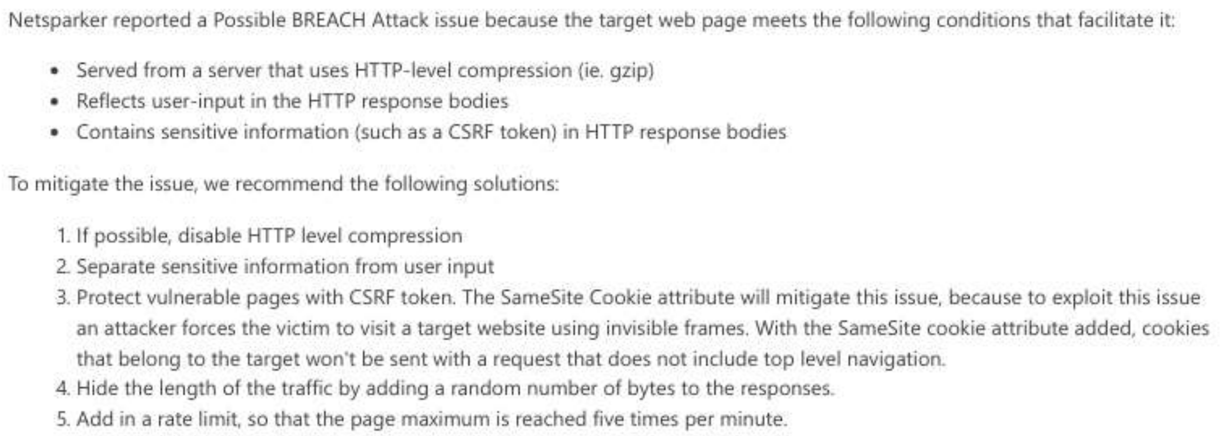


Response

Response Time (ms) : 2449.6136 Total Bytes Received : 37290 Body Length : 33912 Is Compressed : No

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
ETag: W/"a434927ea0115f9ad752f96f1595ca5d"
set-cookie: __Host-mons-sid=258-6532488-6532253; Max-Age=31536000; Expires=Fri, 09 May 2025 17:57:51 GM
T; Path=/; Secure
set-cookie: preferred_locale=en-US; Max-Age=31535999; Expires=Fri, 09 May 2025 17:57:50 GMT; Path=/; Do
main=.amazon.jobs; Secure
set-cookie: analytics_id=21f6ca1a-9f6a-4281-95d1-25c365fccac2; Max-Age=34214399; Expires=Mon, 09 Jun 20
25 17:57:50 GMT; Path=/; Domain=.amazon.jobs; Secure
set-cookie: amazon_jobs_session=UGg1bWV0bEdaSThsUFJzajRlYXFoZ0lOemg1T3pTaTRxWFg0SzNsWHBvcmpsZW1LRzhUc2l
DaXZkNDN3cUloL0ppM3lrV0FxaWNkUWVjZkZLeWpNblBwV2p3VGF1LzNUS24zMlZlZm9VaTlXWW95R0xsQkVZdG9HYlJrbU8yS3VCOE
lYZ0tocXpMcTE0dVI3dWlMeURHR1NnbXhDZDkvUisxS1VvR2FJYWxSNDhjaWQzVjhlM2xwOU5HYndPMXlmQWlsNUhOY3Y4S3JuamkwU
Gp6Yk0zTFNQa242UXJQSXo4UkNWaFl4MnI5UWFNV0N4dkNZcmJ4ZkJqTU1QNnRqZ0ZGZGhsRGwwU2t1ZUZnaXY1VGhiMXV0bWpzWVlB
YVAyVXh5V0IxYzBCTThjUTFYRnFybDN6QU41M201bm1EN2ZkL1RwSFFrM3NhN3czZ0pySUt5ZDZOaFpXYXZBWFVHWlVvRWt5UVpZZ1h
zPS0tUG9zb1A3bTFpVm9sUjJHcmlTVktCQT09--cc84b0386105097b49433360fd1bc9712e473071; Max-Age=86399; Expires
=Fri, 10 May 2024 17:57:50 GMT; Path=/; Domain=.amazon.jobs; Secure; HTTPOnly
Strict-Transport-Security: max-age=47474747;
Transfer-Encoding: chunked
Server: Server
Link: <//static.amazon.jobs/assets/bundles/search/index-8b21f2f005cfa886056d116f5dfb8352bb416e6f91c37ec
8f6220d49b06ed0fb.css>; rel=preload; as=style; nopush,<//static.amazon.jobs/assets/bundles/search/index
-5a5b6153de376af74f3250614d320ca554b728f69f61f503e33e799318821355.js>; rel=preload; as=script; nopush,<
https://d1o95ve0lr2m33.cloudfront.net/launch-ENb97d7f9d2d4b4720ac9782a711994995.min.js>; rel=preload; a
s=script; nopush,<https://d1t40axu4ik42k.cloudfront.net/cathodeBoomerang.d11474def2665bc03c00.min.js>;
 rel=preload; as=script; nopush,<//static.amazon.jobs/assets/application-5a9f81840d0f66d67b72b16fc16c94
72e38135552ac4909424aa4840be5c0ea0.css>; rel=preload; as=style; nopush,<//
…
```

- ## Remediation



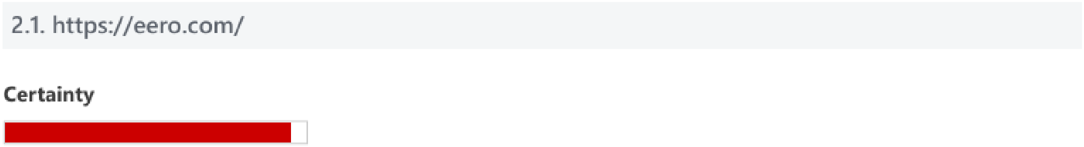
Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

- Served from a server that uses HTTP-level compression (ie. gzip)
- Reflects user-input in the HTTP response bodies
- Contains sensitive information (such as a CSRF token) in HTTP response bodies

To mitigate the issue, we recommend the following solutions:

1. If possible, disable HTTP level compression
2. Separate sensitive information from user input
3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
4. Hide the length of the traffic by adding a random number of bytes to the responses.
5. Add in a rate limit, so that the page maximum is reached five times per minute.

HTTP Strict Transport Security (HSTS) Policy Not Enabled



2.1. https://eero.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://www.eero.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.eero.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.

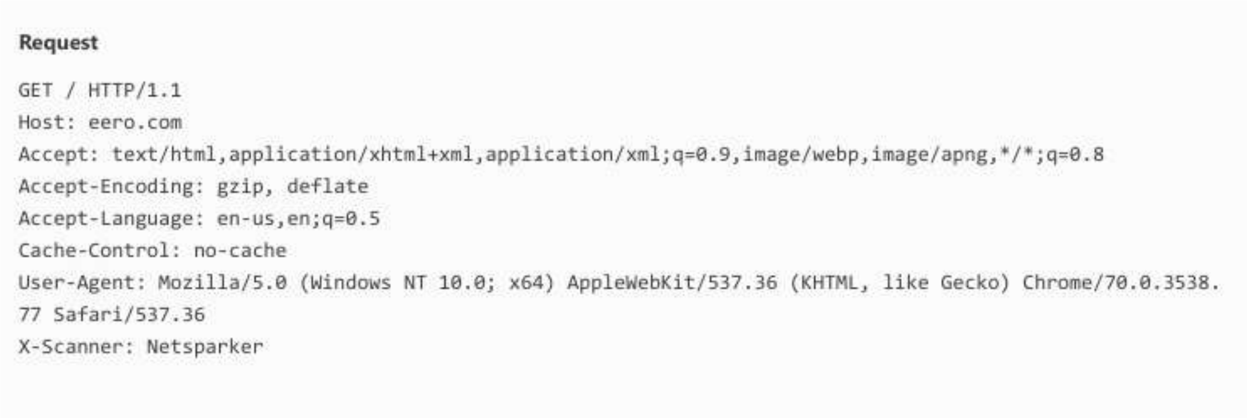
3. Phishing and Data Theft: By pretending to be www.trafficfactory.com, cybercriminals may leverage this vulnerability to conduct phishing attacks and fool victims into disclosing sensitive information such login passwords, personal information, or bank account information. Financial losses and data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

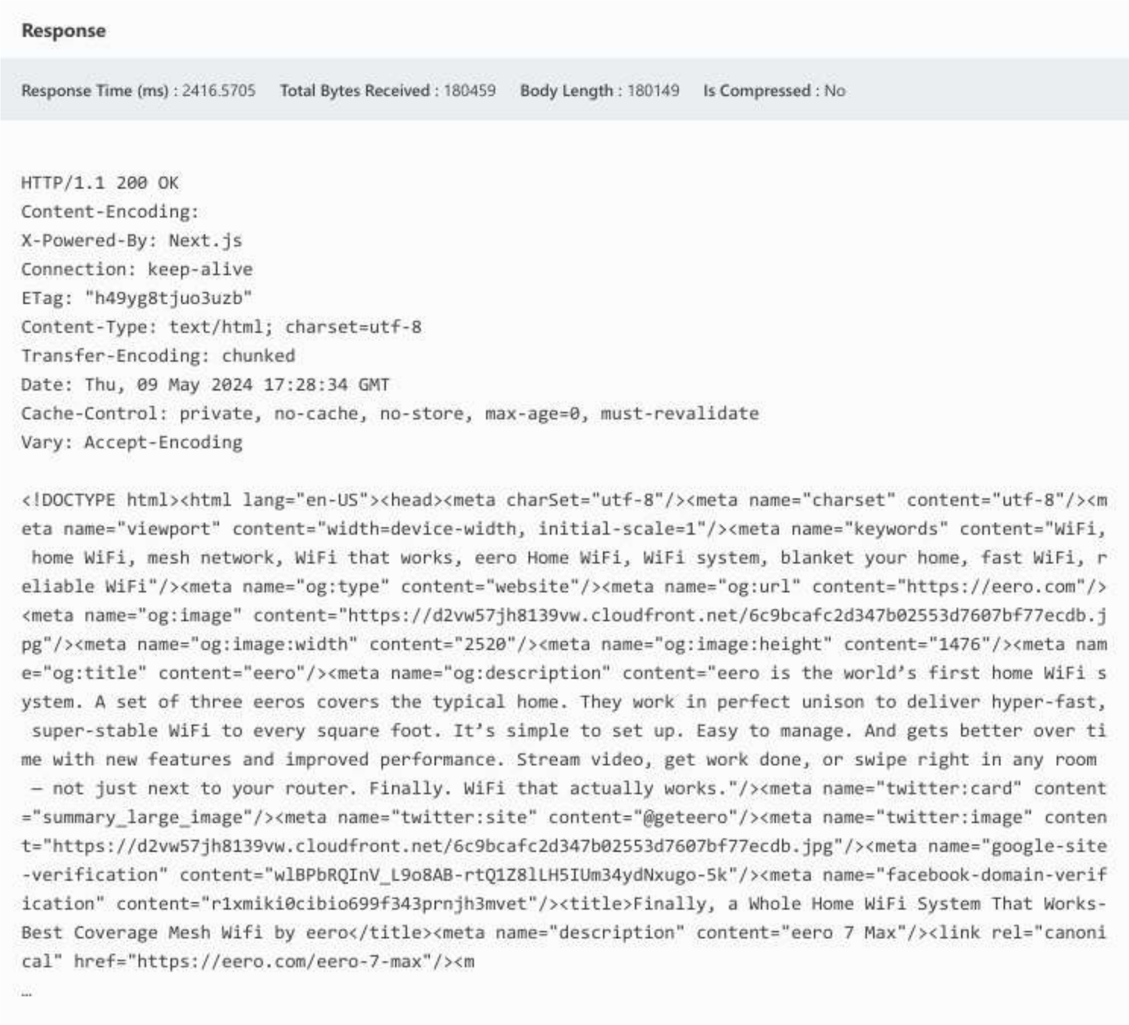
Turning on HSTS is essential to fixing this vulnerability. This security feature prevents downgrading attacks and improves overall security by guaranteeing that all communications with the website are encrypted and safe. Quick HSTS implementation can help the website comply with legal obligations, preserve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

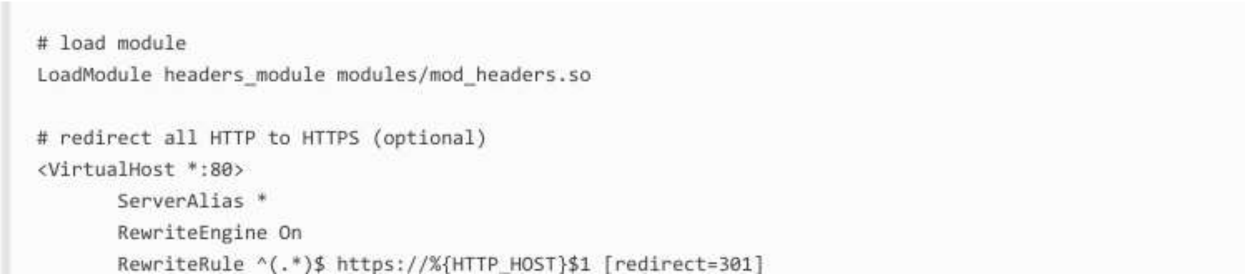
Response Time (ms) : 2416.5705 **Total Bytes Received** : 180459 **Body Length** : 180149 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Encoding:
X-Powered-By: Next.js
Connection: keep-alive
ETag: "h49yg8tjuo3uzb"
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Date: Thu, 09 May 2024 17:28:34 GMT
Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate
Vary: Accept-Encoding

<!DOCTYPE html><html lang="en-US"><head><meta charSet="utf-8"/><meta name="charset" content="utf-8"/><m
eta name="viewport" content="width=device-width, initial-scale=1"/><meta name="keywords" content="WiFi,
 home WiFi, mesh network, WiFi that works, eero Home WiFi, WiFi system, blanket your home, fast WiFi, r
eliable WiFi"/><meta name="og:type" content="website"/><meta name="og:url" content="https://eero.com"/>
<meta name="og:image" content="https://d2vw57jh8139vw.cloudfront.net/6c9bcafc2d347b02553d7607bf77ecdb.j
pg"/><meta name="og:image:width" content="2520"/><meta name="og:image:height" content="1476"/><meta nam
e="og:title" content="eero"/><meta name="og:description" content="eero is the world’s first home WiFi s
ystem. A set of three eeros covers the typical home. They work in perfect unison to deliver hyper-fast,
 super-stable WiFi to every square foot. It’s simple to set up. Easy to manage. And gets better over ti
me with new features and improved performance. Stream video, get work done, or swipe right in any room
 — not just next to your router. Finally. WiFi that actually works."/><meta name="twitter:card" content
="summary_large_image"/><meta name="twitter:site" content="@geteero"/><meta name="twitter:image" conten
t="https://d2vw57jh8139vw.cloudfront.net/6c9bcafc2d347b02553d7607bf77ecdb.jpg"/><meta name="google-site
-verification" content="wlBPbRQInV_L9o8AB-rtQ1Z8lLH5IUm34ydNxugo-5k"/><meta name="facebook-domain-verif
ication" content="r1xmiki0cibio699f343prnjh3mvet"/><title>Finally, a Whole Home WiFi System That Works-
Best Coverage Mesh Wifi by eero</title><meta name="description" content="eero 7 Max"/><link rel="canoni
cal" href="https://eero.com/eero-7-max"/><m
…
```

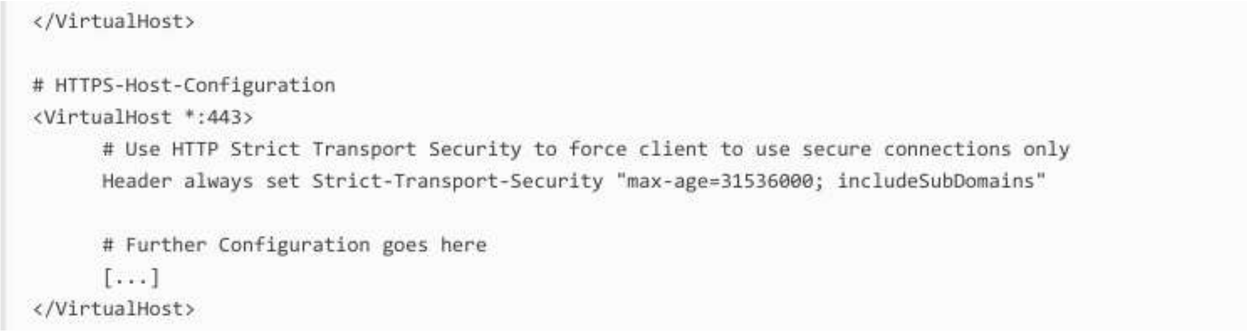
- ## Remediation

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.

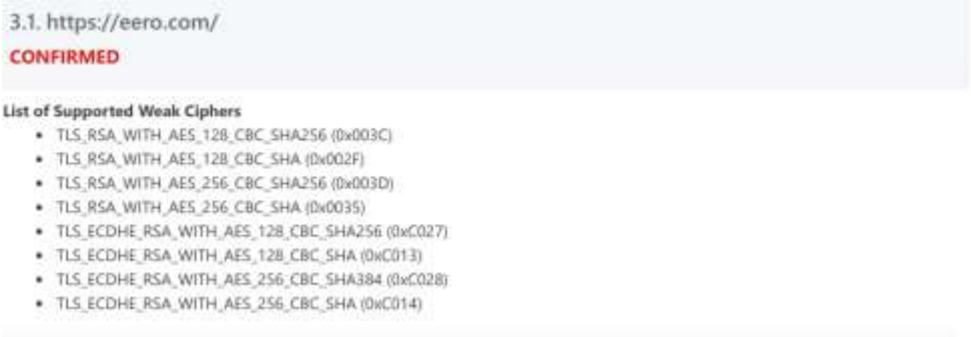


```
# load module
LoadModule headers_module modules/mod_headers.so

# 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>
```

Weak Ciphers Enabled



3.1. https://eero.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

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.eero.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.

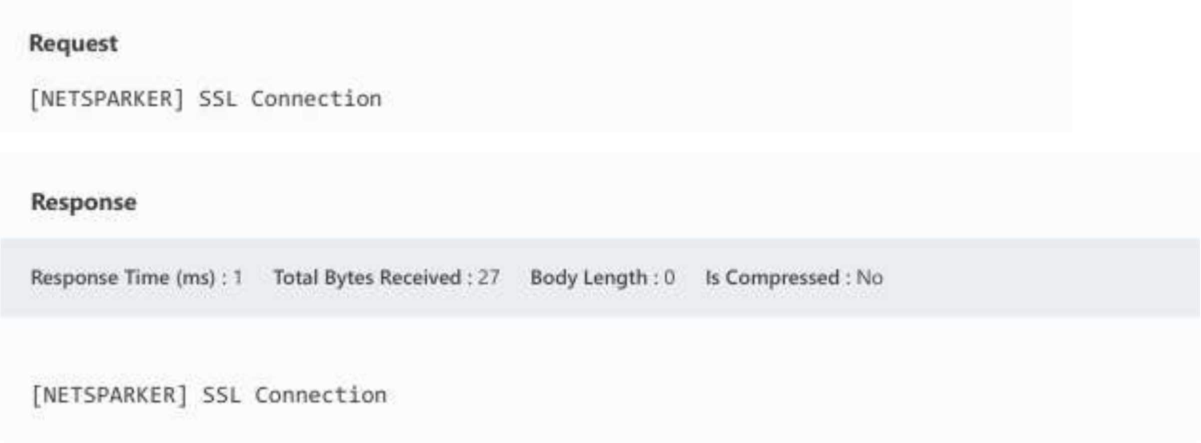
3. **Enhanced Attack Surface:** Cybercriminals can more easily exploit vulnerabilities and obtain illegal access to a website, its servers, and underlying systems when weak ciphers provide them a larger attack surface.

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

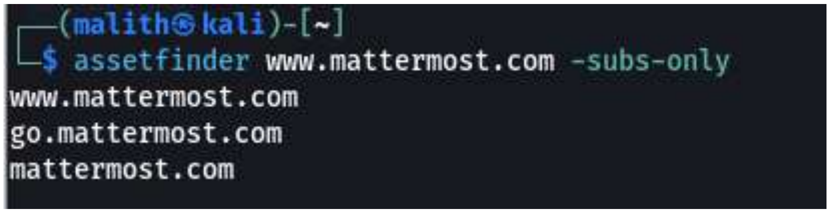
Response Time (ms) : 1 **Total Bytes Received :** 27 **Body Length :** 0 **Is Compressed :** No

```
[NETSPARKER] SSL Connection
```

Bug Bounty 3 (mattermost)

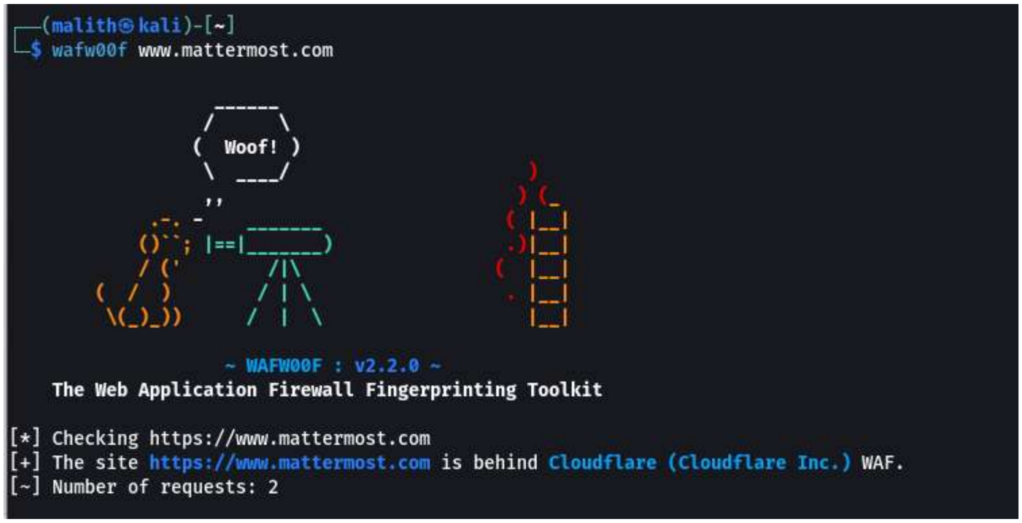
Reconnaissance

Firstly, I used the Assetfinder tool to find the subdomains of the mattermost website. Assetfinder tool is used to find the subdomains of a website.

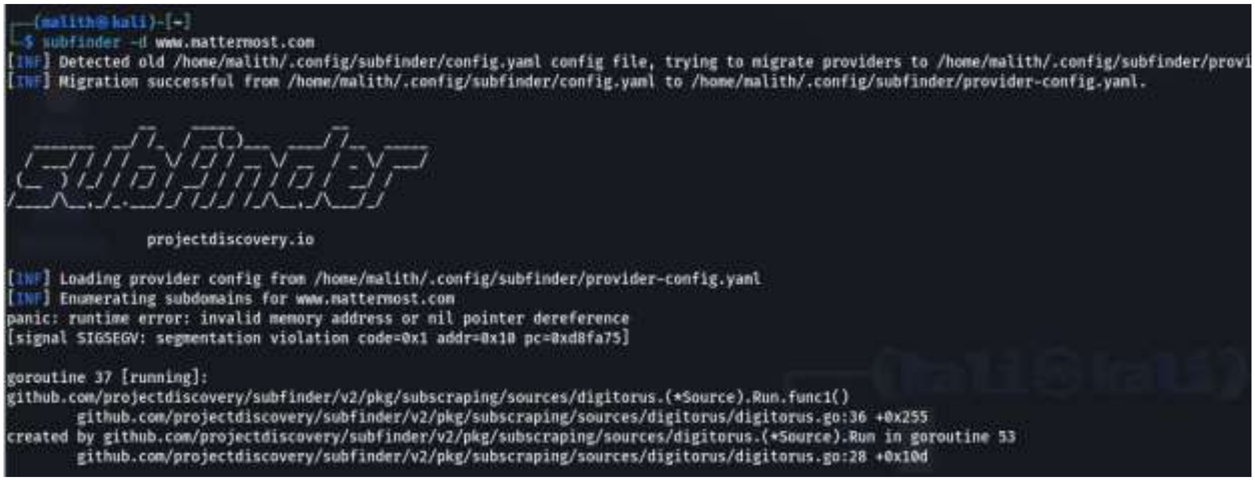


```
┌──(malith㉿kali)-[~]
└─$ assetfinder www.mattermost.com -subs-only
www.mattermost.com
go.mattermost.com
mattermost.com
```

Then, I got the subdomains list as.

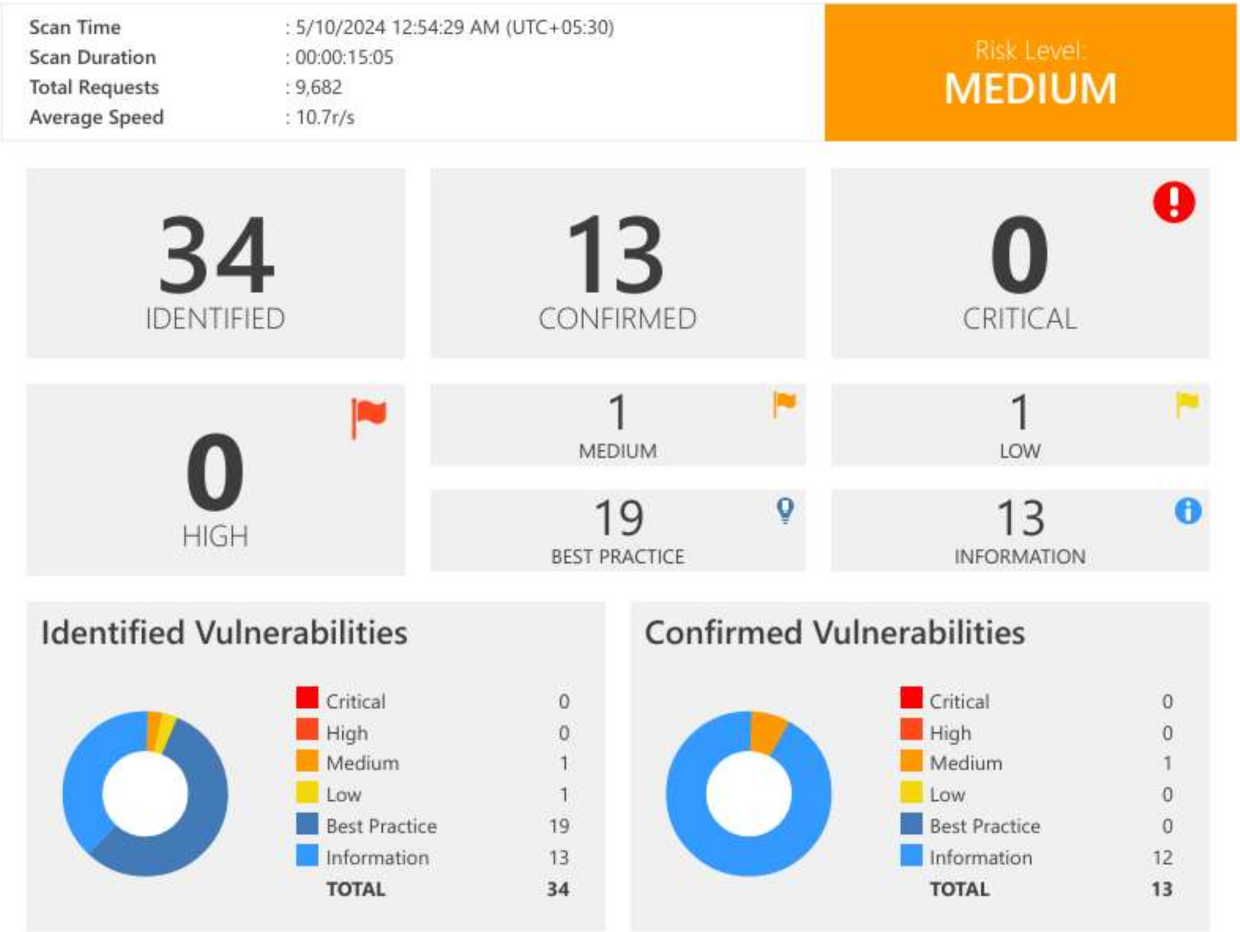


```
┌──(malith㉿kali)-[~]
└─$ wafw00f www.mattermost.com

                ______
               /      \
              (  Woof! )
               \  ____/                      )
               ,,                           ) (_
          .-. -    _______                 ( |__|
         ()``; |==|_______)               .)|__|
         / ('        /|\                  (  |__|
     (  /  )        / | \                  . |__|
      \(_)_))      /  |  \                   |__|

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.mattermost.com
[+] The site https://www.mattermost.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```



```
┌──(malith㉿kali)-[~]
└─$ subfinder -d www.mattermost.com
[INF] Detected old /home/malith/.config/subfinder/config.yaml config file, trying to migrate providers to /home/malith/.config/subfinder/provi
[INF] Migration successful from /home/malith/.config/subfinder/config.yaml to /home/malith/.config/subfinder/provider-config.yaml.

                projectdiscovery.io

[INF] Loading provider config from /home/malith/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for www.mattermost.com
panic: runtime error: invalid memory address or nil pointer dereference
[signal SIGSEGV: segmentation violation code=0x1 addr=0x10 pc=0xd8fa75]

goroutine 37 [running]:
github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run.func1()
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:36 +0x255
created by github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run in goroutine 53
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:28 +0x10d
```

Vulnerabilities Found.



Scan Time	: 5/10/2024 12:54:29 AM (UTC+05:30)
Scan Duration	: 00:00:15:05
Total Requests	: 9,682
Average Speed	: 10.7r/s

Risk Level:
MEDIUM

34	IDENTIFIED
13	CONFIRMED
0	CRITICAL
0	HIGH
1	MEDIUM
1	LOW
19	BEST PRACTICE
13	INFORMATION

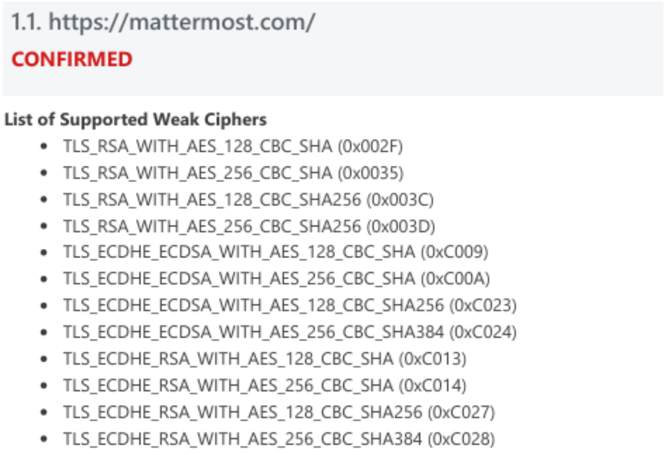
Identified Vulnerabilities

🟥 Critical	0
🟧 High	0
🟧 Medium	1
🟨 Low	1
🟦 Best Practice	19
🟦 Information	13
TOTAL	**34**

Confirmed Vulnerabilities

🟥 Critical	0
🟧 High	0
🟧 Medium	1
🟨 Low	0
🟦 Best Practice	0
🟦 Information	12
TOTAL	**13**

Weak Ciphers Enabled



1.1. https://mattermost.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_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
- 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://mattermost.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://mattermost.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.

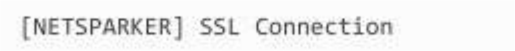
2. Regulatory Non-Compliance: Using weak ciphers may put Starbucks at variance with data protection rules and industry norms, potentially leading to legal and financial implications for non-compliance.

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.

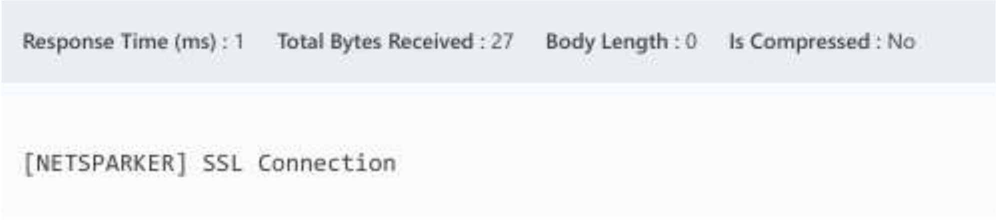
It is vital to fix this Weak Cipher Enabled issue swiftly by adopting strong encryption methods and ciphers. Failure to do so not only expose users to potential security concerns but also damages Starbucks' reputation, legal compliance, and general corporate integrity. The repercussions of the vulnerability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

- **Request**



```
[NETSPARKER] SSL Connection
```

- **Response**



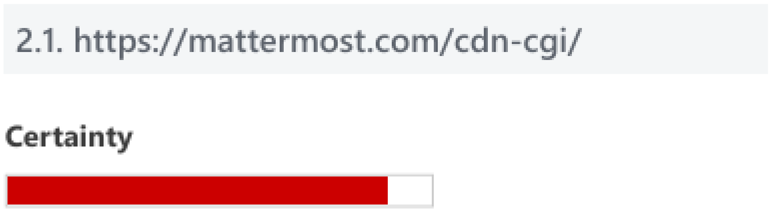
Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

- **Remediation**

Configure your web server to disallow using weak ciphers.

Missing Content-Type Header



2.1. https://mattermost.com/cdn-cgi/

Certainty

Date of Discovery: 20/04/2024

Date of Reporting: 21/04/2024

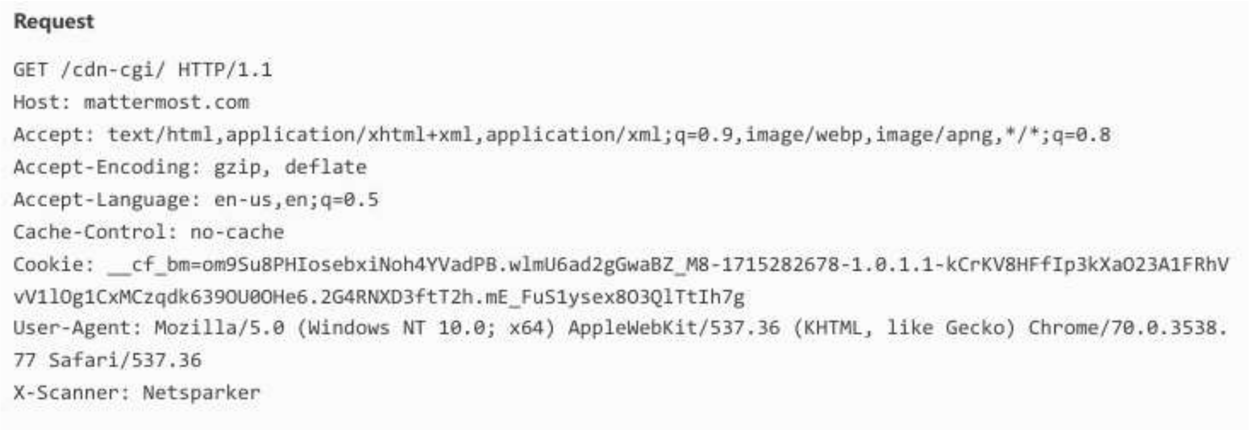
- ### Description

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.

This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.

The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image

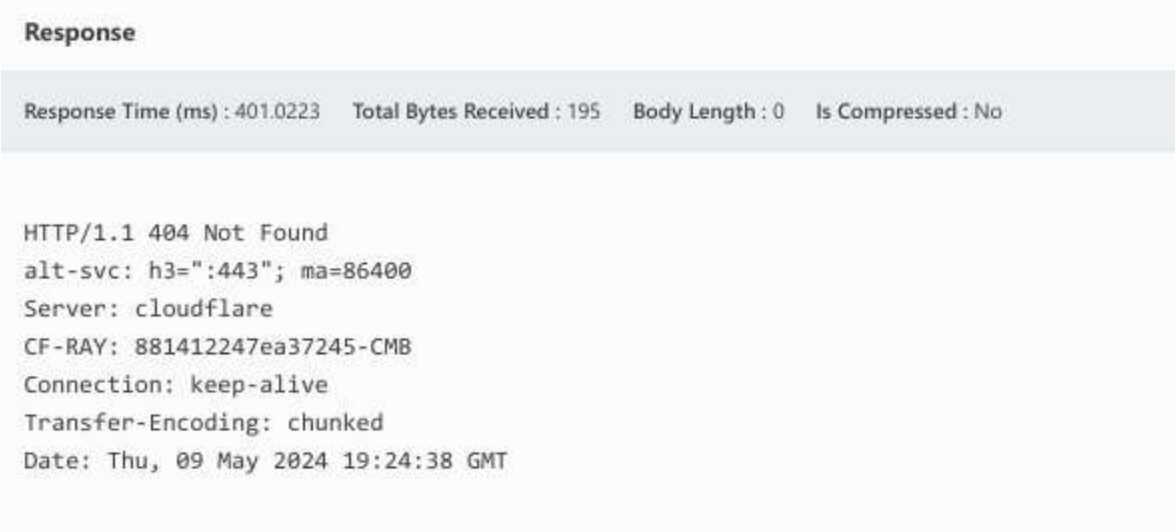
- **Request**



Request

```
GET /cdn-cgi/ HTTP/1.1
Host: mattermost.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
Cookie: __cf_bm=om9Su8PHIosebxiNoh4YVadPB.wlmU6ad2gGwaBZ_M8-1715282678-1.0.1.1-kCrKV8HFfIp3kXaO23A1FRhV
vV1lOg1CxMCzqdk639OU0OHe6.2G4RNXD3ftT2h.mE_FuS1ysex8O3QlTtIh7g
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

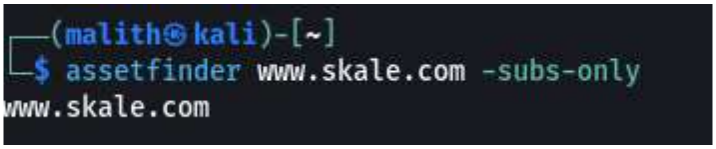
Response Time (ms) : 401.0223 **Total Bytes Received** : 195 **Body Length** : 0 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
alt-svc: h3=":443"; ma=86400
Server: cloudflare
CF-RAY: 881412247ea37245-CMB
Connection: keep-alive
Transfer-Encoding: chunked
Date: Thu, 09 May 2024 19:24:38 GMT
```

Bug Bounty 4 (skale)

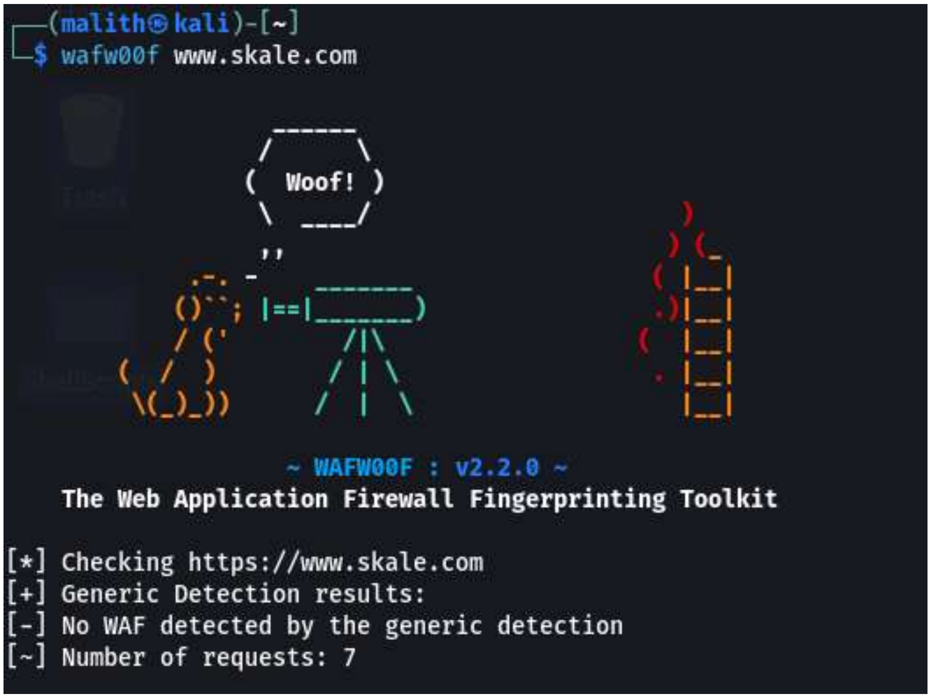
Reconnaissance

Firstly, I used the Assetfinder tool to find the subdomains of the skale website. Assetfinder tool is used to find the subdomains of a website.

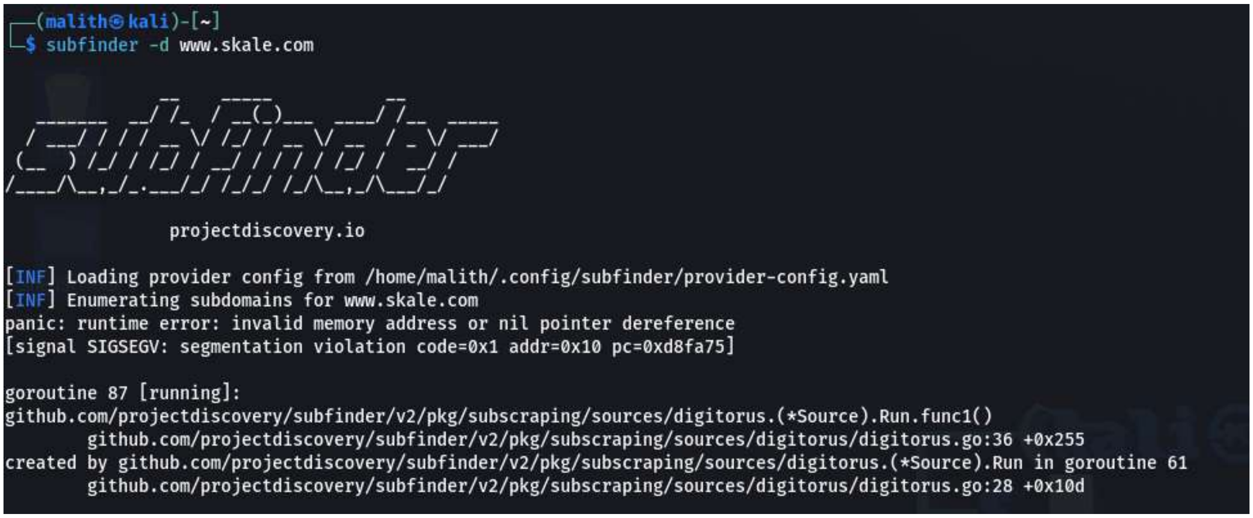


```
┌──(malith㉿kali)-[~]
└─$ assetfinder www.skale.com -subs-only
www.skale.com
```

Then, I got the subdomains list as below.

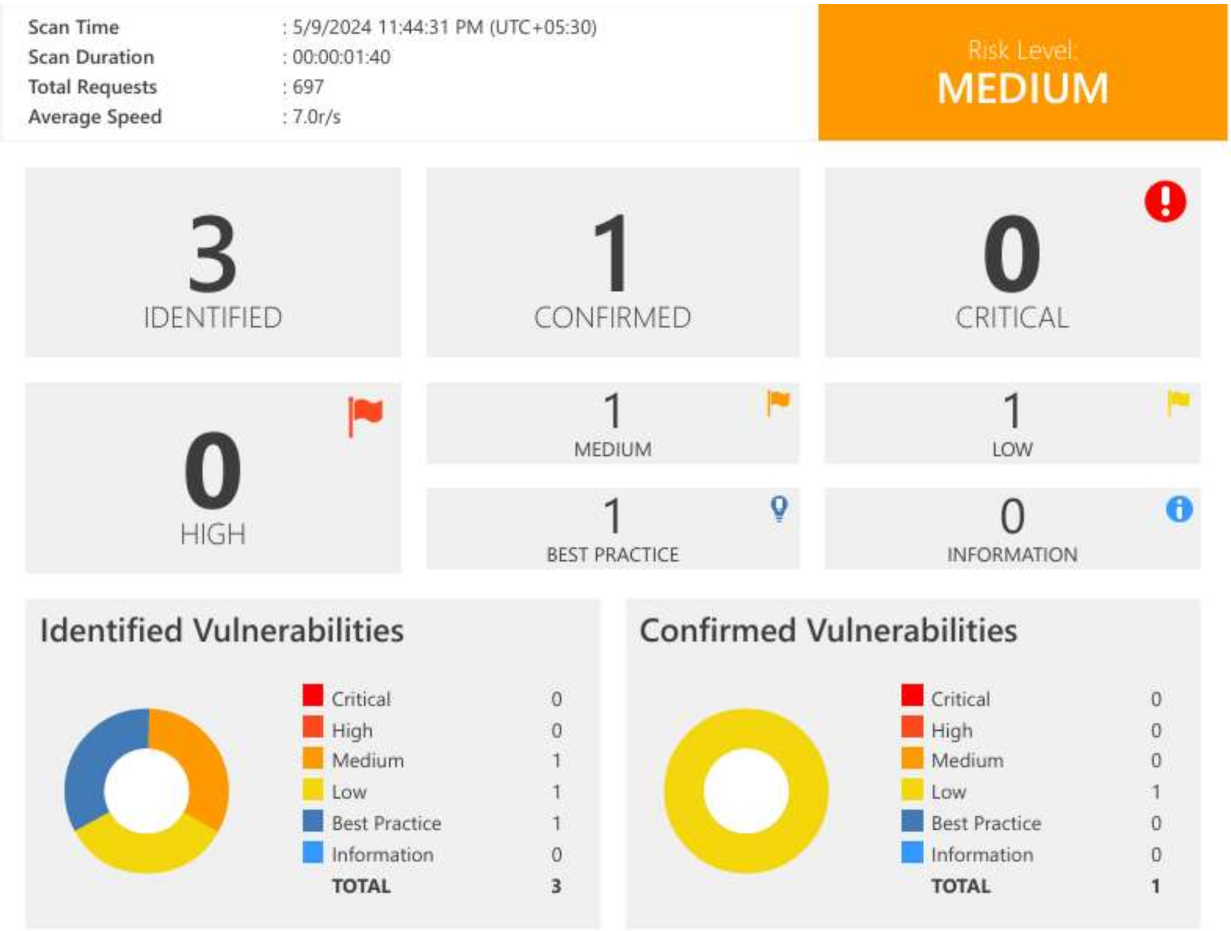


```
┌──(malith㉿kali)-[~]
└─$ wafw00f www.skale.com

                ______
               /      \
              (  Woof! )
               \  ____/                      )
               ,,                          ) (_
           .-. -    _______              ( |__|
          ()``; |==|_______)             .)|__|
          / ('        /|\                ( |__|
      (  /  )        / | \               . |__|
       \(_)_))      /  |  \                |__|

                  ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.skale.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```



```
┌──(malith㉿kali)-[~]
└─$ subfinder -d www.skale.com

               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Loading provider config from /home/malith/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for www.skale.com
panic: runtime error: invalid memory address or nil pointer dereference
[signal SIGSEGV: segmentation violation code=0x1 addr=0x10 pc=0xd8fa75]

goroutine 87 [running]:
github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run.func1()
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:36 +0x255
created by github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run in goroutine 61
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:28 +0x10d
```

Vulnerabilities Found.



Scan Time	: 5/9/2024 11:44:31 PM (UTC+05:30)
Scan Duration	: 00:00:01:40
Total Requests	: 697
Average Speed	: 7.0r/s

Risk Level:
MEDIUM

3 IDENTIFIED

1 CONFIRMED

0 CRITICAL

0 HIGH

1 MEDIUM

1 LOW

1 BEST PRACTICE

0 INFORMATION

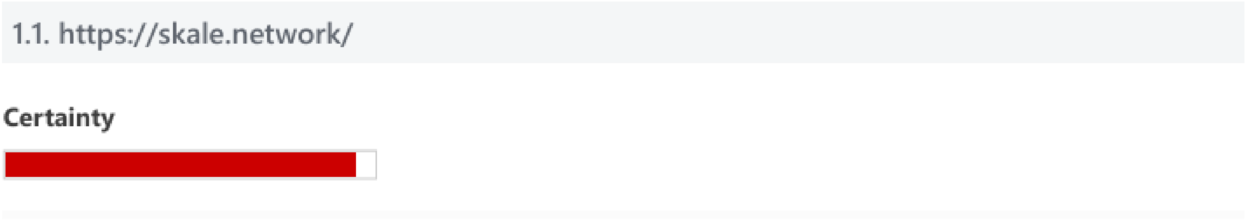
Identified Vulnerabilities

🟥 Critical	0
🟥 High	0
🟧 Medium	1
🟨 Low	1
🟦 Best Practice	1
🟦 Information	0
TOTAL	**3**

Confirmed Vulnerabilities

🟥 Critical	0
🟥 High	0
🟧 Medium	0
🟨 Low	1
🟦 Best Practice	0
🟦 Information	0
TOTAL	**1**

HTTP Strict Transport Security (HSTS) Policy Not Enabled



1.1. https://skale.network/

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://skale.network/ . 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.

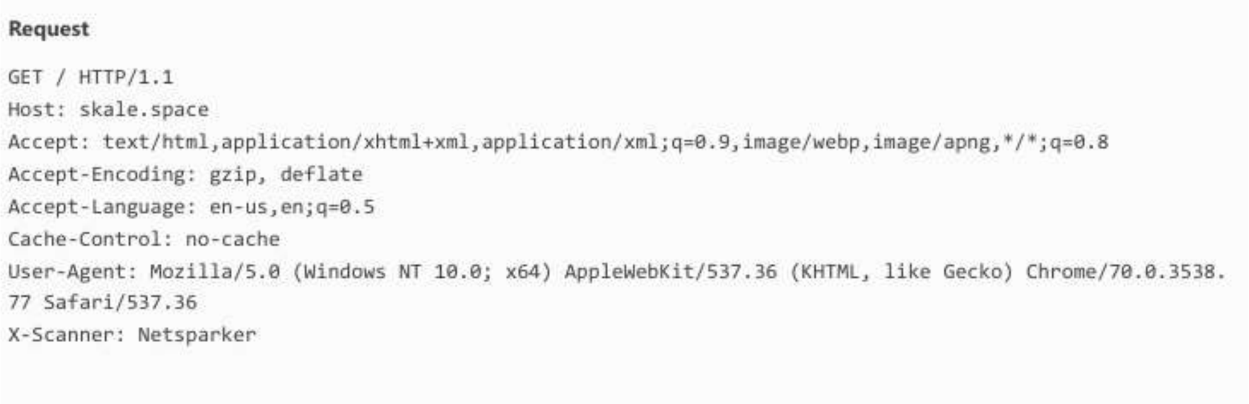
3. Phishing and Data Theft: By pretending to be www.echobox.com, cybercriminals may leverage this vulnerability to conduct phishing attacks and fool victims into disclosing sensitive information such login passwords, personal information, or bank account information. Financial losses and data theft may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

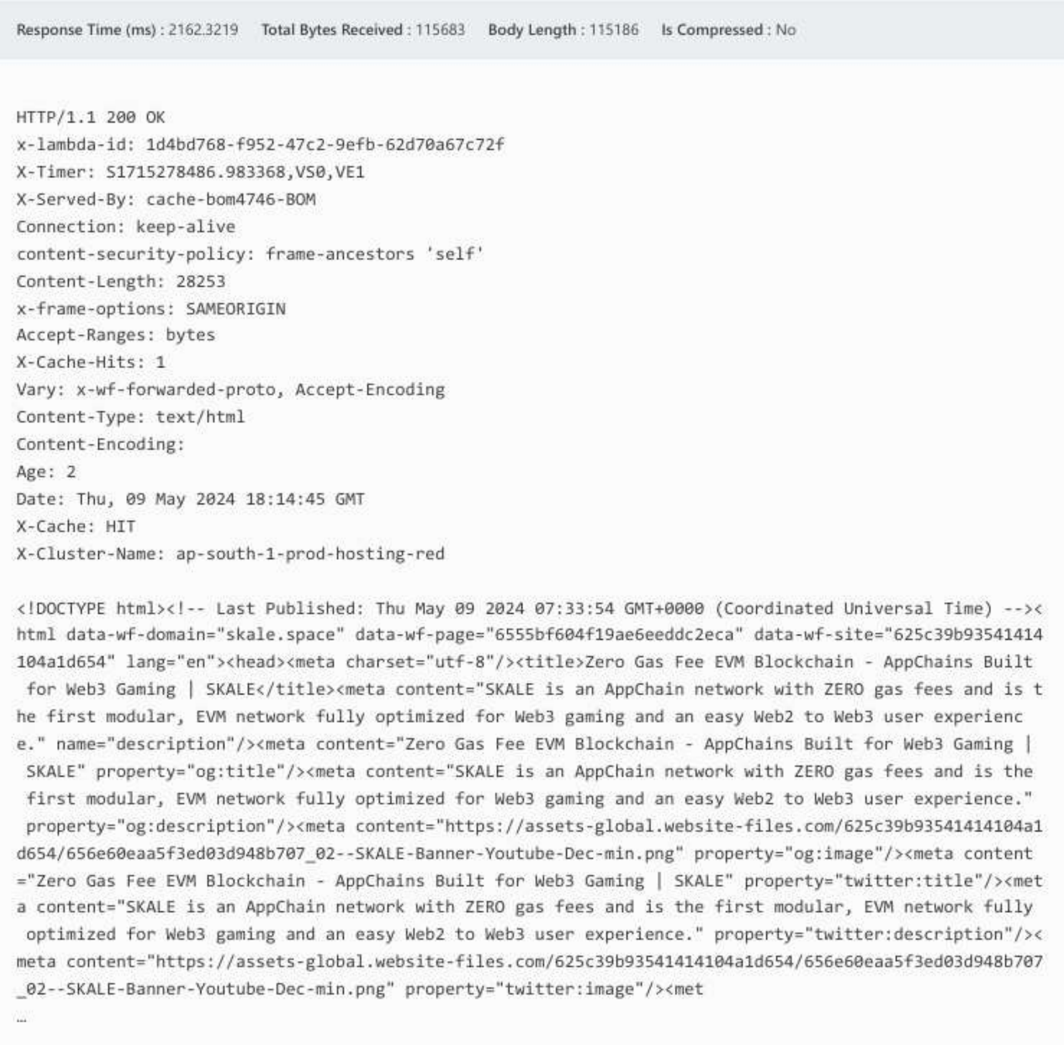
- **Request**



Request

```
GET / HTTP/1.1
Host: skale.space
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
```

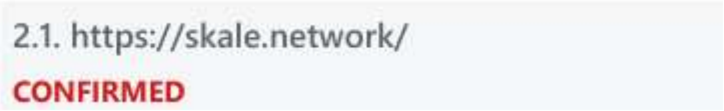
- **Response**



Response Time (ms) : 2162.3219 Total Bytes Received : 115683 Body Length : 115186 Is Compressed : No

```
HTTP/1.1 200 OK
x-lambda-id: 1d4bd768-f952-47c2-9efb-62d70a67c72f
X-Timer: S1715278486.983368,VS0,VE1
X-Served-By: cache-bom4746-BOM
Connection: keep-alive
content-security-policy: frame-ancestors 'self'
Content-Length: 28253
x-frame-options: SAMEORIGIN
Accept-Ranges: bytes
X-Cache-Hits: 1
Vary: x-wf-forwarded-proto, Accept-Encoding
Content-Type: text/html
Content-Encoding:
Age: 2
Date: Thu, 09 May 2024 18:14:45 GMT
X-Cache: HIT
X-Cluster-Name: ap-south-1-prod-hosting-red

<!DOCTYPE html><!-- Last Published: Thu May 09 2024 07:33:54 GMT+0000 (Coordinated Universal Time) --><
html data-wf-domain="skale.space" data-wf-page="6555bf604f19ae6eeddc2eca" data-wf-site="625c39b93541414
104a1d654" lang="en"><head><meta charset="utf-8"/><title>Zero Gas Fee EVM Blockchain - AppChains Built
 for Web3 Gaming | SKALE</title><meta content="SKALE is an AppChain network with ZERO gas fees and is t
he first modular, EVM network fully optimized for Web3 gaming and an easy Web2 to Web3 user experienc
e." name="description"/><meta content="Zero Gas Fee EVM Blockchain - AppChains Built for Web3 Gaming |
 SKALE" property="og:title"/><meta content="SKALE is an AppChain network with ZERO gas fees and is the
 first modular, EVM network fully optimized for Web3 gaming and an easy Web2 to Web3 user experience."
 property="og:description"/><meta content="https://assets-global.website-files.com/625c39b93541414104a1
d654/656e60eaa5f3ed03d948b707_02--SKALE-Banner-Youtube-Dec-min.png" property="og:image"/><meta content
="Zero Gas Fee EVM Blockchain - AppChains Built for Web3 Gaming | SKALE" property="twitter:title"/><met
a content="SKALE is an AppChain network with ZERO gas fees and is the first modular, EVM network fully
 optimized for Web3 gaming and an easy Web2 to Web3 user experience." property="twitter:description"/><
meta content="https://assets-global.website-files.com/625c39b93541414104a1d654/656e60eaa5f3ed03d948b707
_02--SKALE-Banner-Youtube-Dec-min.png" property="twitter:image"/><met
…
```

Internal Server Error



2.1. https://skale.network/

CONFIRMED

Date of Discovery: 20/04/2024

Date of Reporting: 21/04/2024

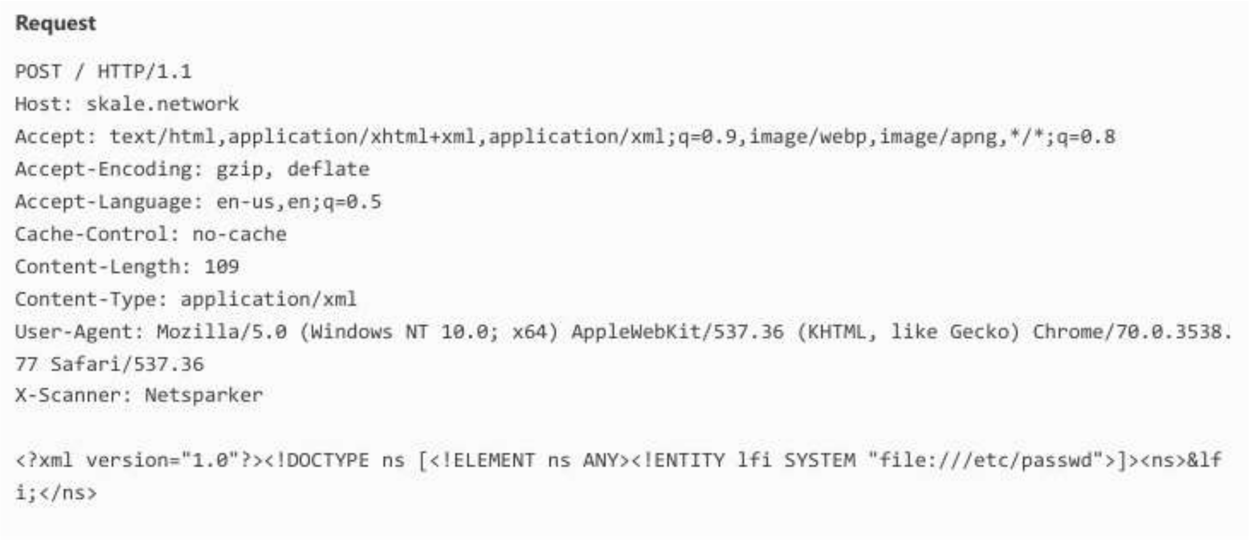
- ## Description

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

- ## Impact

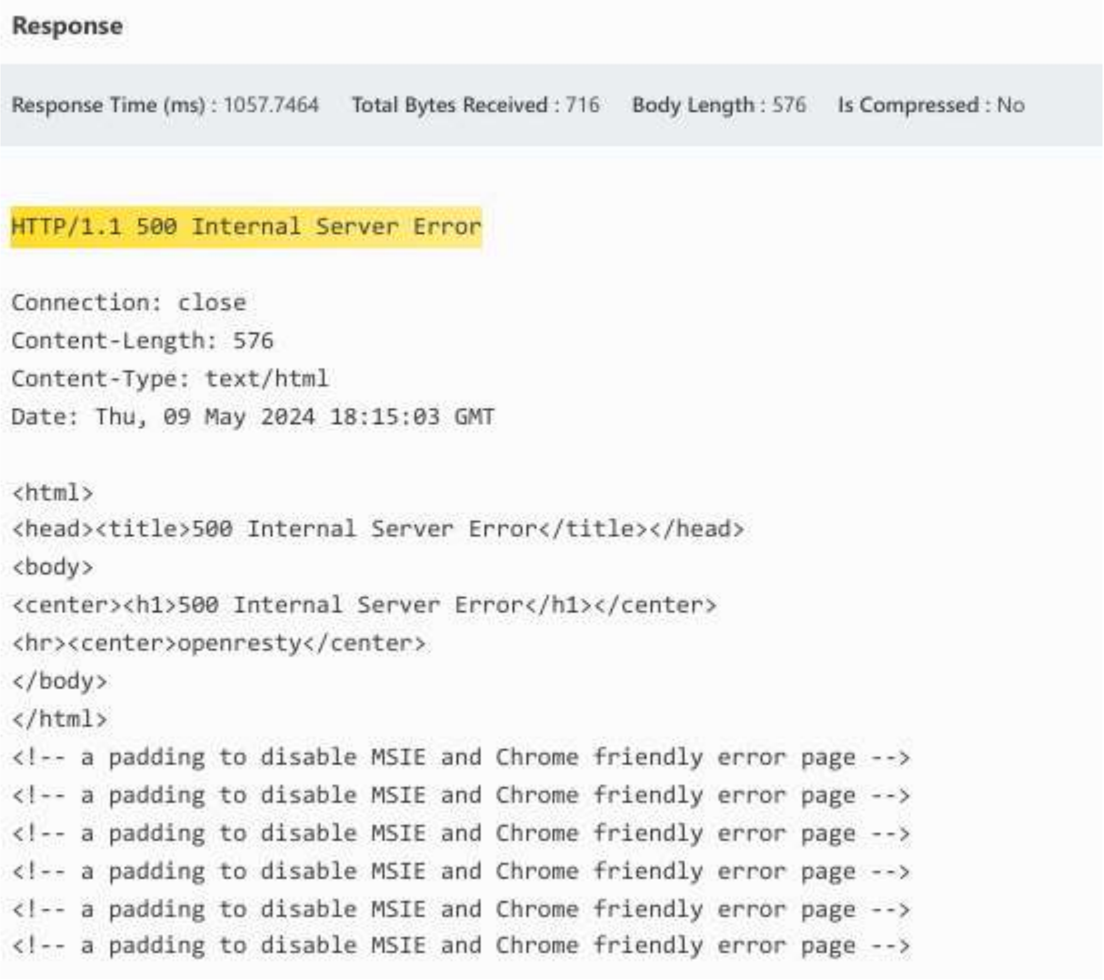
The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

- ## Proof of Concept



Request

```
POST / HTTP/1.1
Host: skale.network
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
Content-Length: 109
Content-Type: application/xml
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

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "file:///etc/passwd">]><ns>&lf
i;</ns>
```



Response

Response Time (ms) : 1057.7464 **Total Bytes Received** : 716 **Body Length** : 576 **Is Compressed** : No

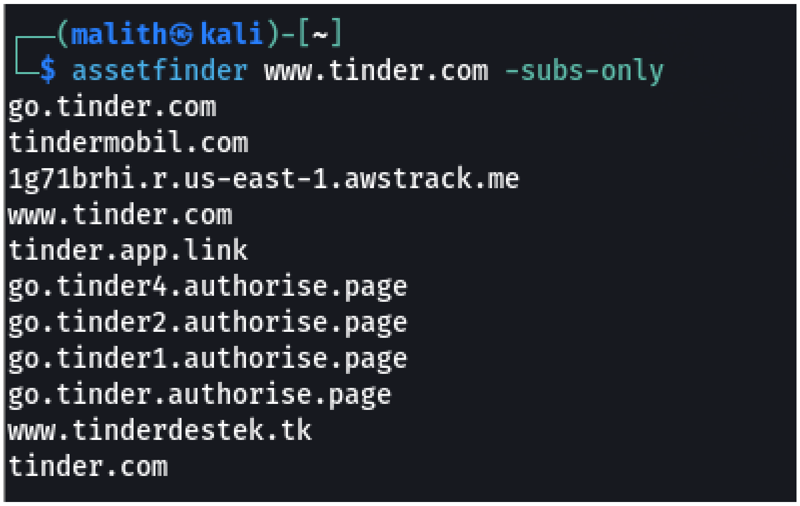
```
HTTP/1.1 500 Internal Server Error

Connection: close
Content-Length: 576
Content-Type: text/html
Date: Thu, 09 May 2024 18:15:03 GMT

<html>
<head><title>500 Internal Server Error</title></head>
<body>
<center><h1>500 Internal Server Error</h1></center>
<hr><center>openresty</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

Bug Bounty 5 (tinder)

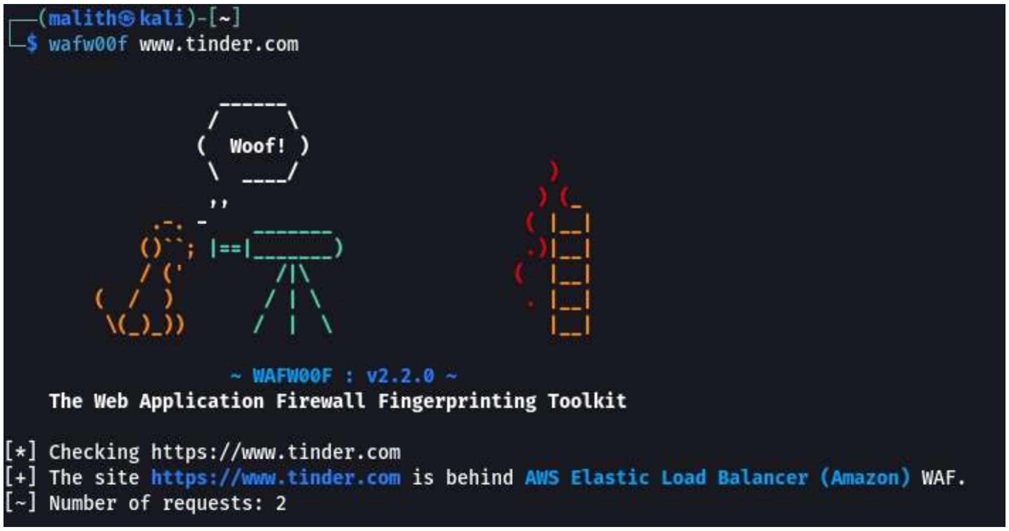
Reconnaissance

Firstly, I used the Assetfinder tool to find the subdomains of the tinder website. Assetfinder tool is used to find the subdomains of a website.

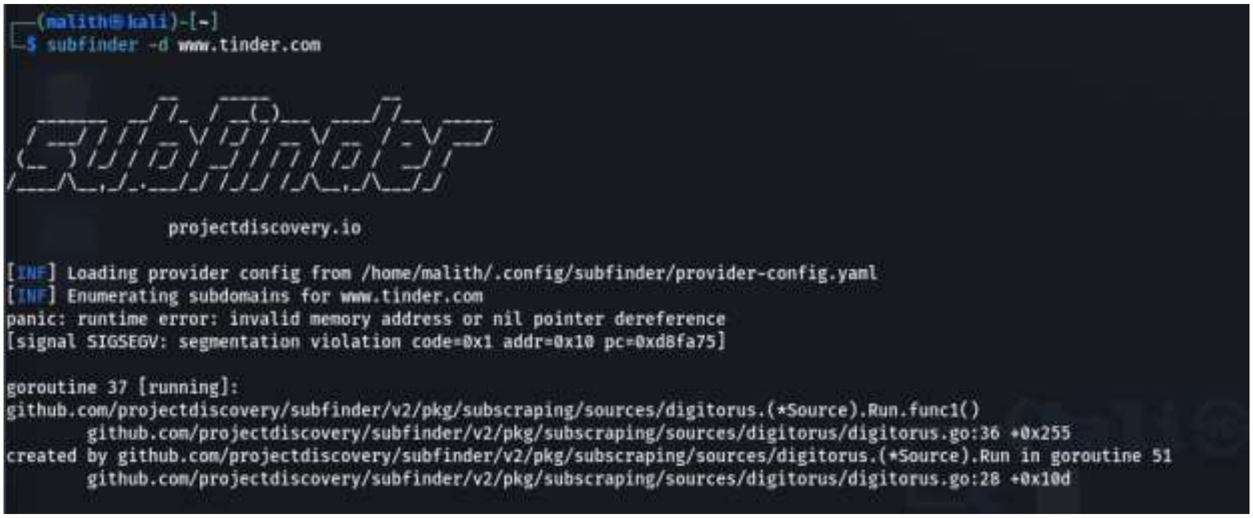
Then, I got the subdomains list as below.



```
┌──(malith㉿kali)-[~]
└─$ assetfinder www.tinder.com -subs-only
go.tinder.com
tindermobil.com
1g71brhi.r.us-east-1.awstrack.me
www.tinder.com
tinder.app.link
go.tinder4.authorise.page
go.tinder2.authorise.page
go.tinder1.authorise.page
go.tinder.authorise.page
www.tinderdestek.tk
tinder.com
```

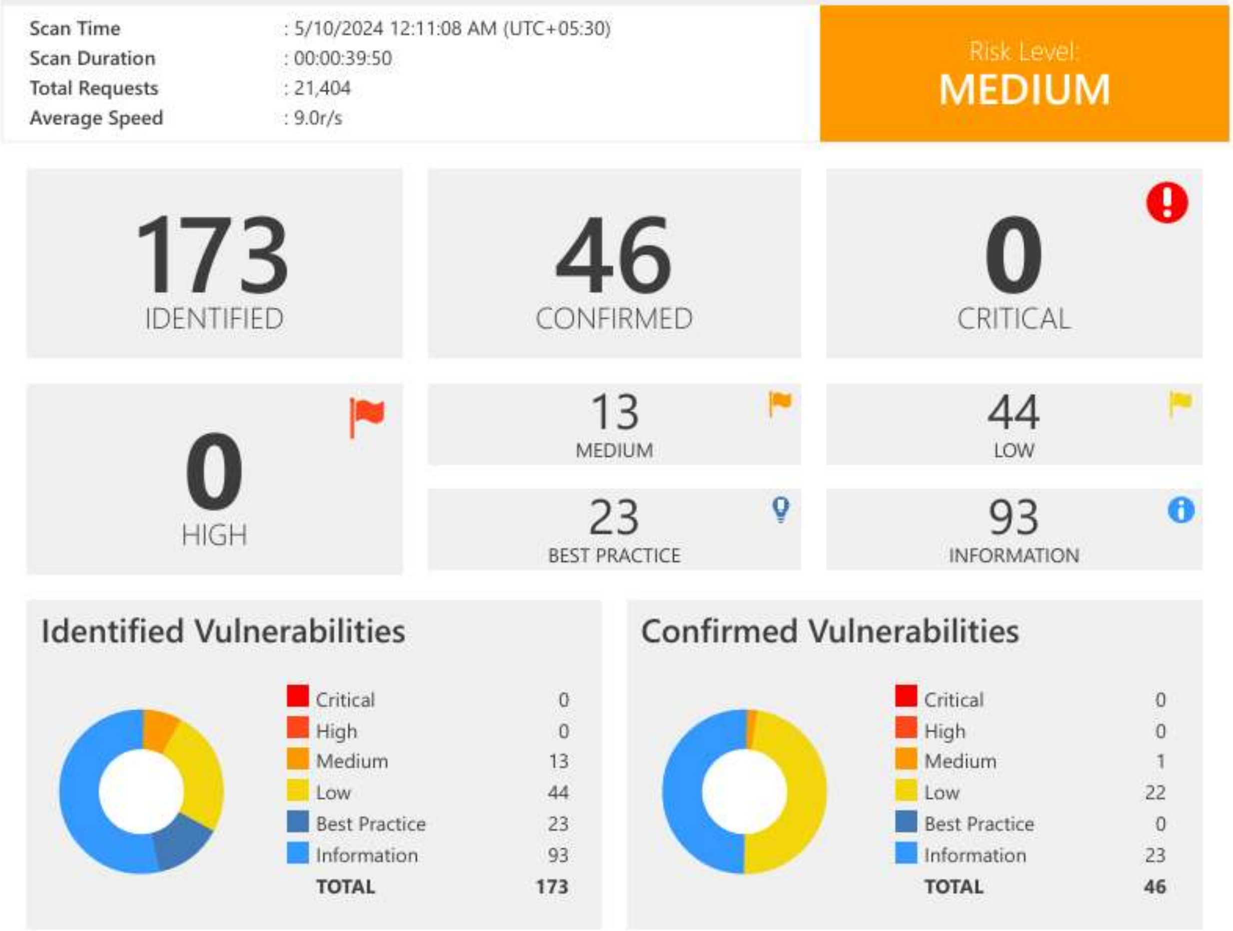


```
┌──(malith㉿kali)-[~]
└─$ wafw00f www.tinder.com

                ______
               /      \
              (  Woof! )
               \  ____/                      )
               ,,                           ) (_
          .-. -    _______                 ( |__|
         ()``; |==|_______)                .)|__|
         / ('        /|\                  (  |__|
     (  /  )        / | \                  . |__|
      \(_)_))      /  |  \                   |__|

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.tinder.com
[+] The site https://www.tinder.com is behind AWS Elastic Load Balancer (Amazon) WAF.
[~] Number of requests: 2
```



```
┌──(malith㉿kali)-[~]
└─$ subfinder -d www.tinder.com

               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Loading provider config from /home/malith/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for www.tinder.com
panic: runtime error: invalid memory address or nil pointer dereference
[signal SIGSEGV: segmentation violation code=0x1 addr=0x10 pc=0xd8fa75]

goroutine 37 [running]:
github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run.func1()
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:36 +0x255
created by github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run in goroutine 51
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:28 +0x10d
```

Vulnerabilities Found.



Scan Time	: 5/10/2024 12:11:08 AM (UTC+05:30)
Scan Duration	: 00:00:39:50
Total Requests	: 21,404
Average Speed	: 9.0r/s

Risk Level:
MEDIUM

173 IDENTIFIED

46 CONFIRMED

0 CRITICAL

0 HIGH

13 MEDIUM

44 LOW

23 BEST PRACTICE

93 INFORMATION

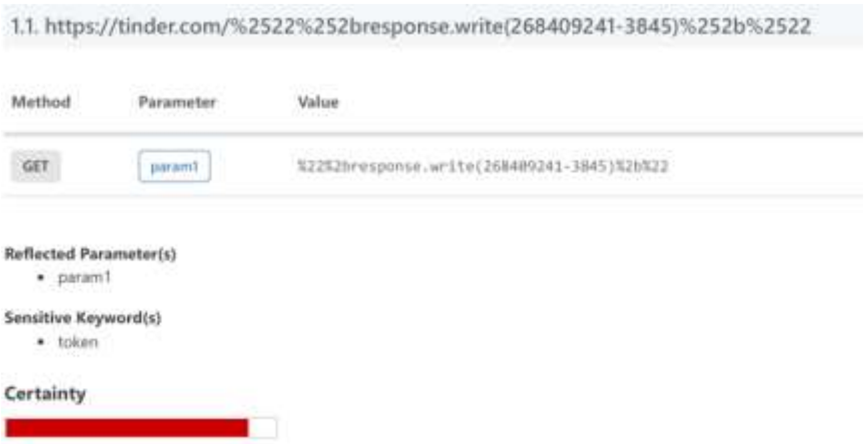
Identified Vulnerabilities

🟥 Critical	0
🟥 High	0
🟧 Medium	13
🟨 Low	44
🟦 Best Practice	23
🟦 Information	93
TOTAL	**173**

Confirmed Vulnerabilities

🟥 Critical	0
🟥 High	0
🟧 Medium	1
🟨 Low	22
🟦 Best Practice	0
🟦 Information	23
TOTAL	**46**

[Possible] BREACH Attack Detected



1.1. https://tinder.com/%2522%252bresponse.write(268409241-3845)%252b%2522

Method	Parameter	Value
GET	param1	%22%2bresponse.write(268409241-3845)%2b%22

Reflected Parameter(s)

- param1

Sensitive Keyword(s)

- token

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://tinder.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

The vulnerability identified as [Possible] Breach Attack Detected indicates a potentially serious security risk. It usually means that illegal or suspicious activity has been found within a network or system by the intrusion detection system or security monitoring tools. The word "Possible" emphasizes the need of an instant inquiry and reaction, even though it suggests that the breach hasn't been conclusively established. These weaknesses may result in data theft, system compromise, or illegal access. In order to resolve this problem, a prompt and complete reaction is needed. This includes analyzing the detected activity in detail, determining the possible source of the breach, and putting security measures in place to stop future exploitation. The significance of proactive threat detection and incident response techniques in preserving sensitive data and network integrity is highlighted by this vulnerability.

• Impact Assessment

In relation to the OWASP category about a [Possible] Breach Attack Detected vulnerability on the website www.tinder.com, several security risks and repercussions have been found. The following possible outcomes are among the significant effects of this vulnerability:

1. Data Compromise: As this case indicates, a breach attack may result in unauthorized access to private information kept on the tinder website. This could include private data such as payment information and customer information.

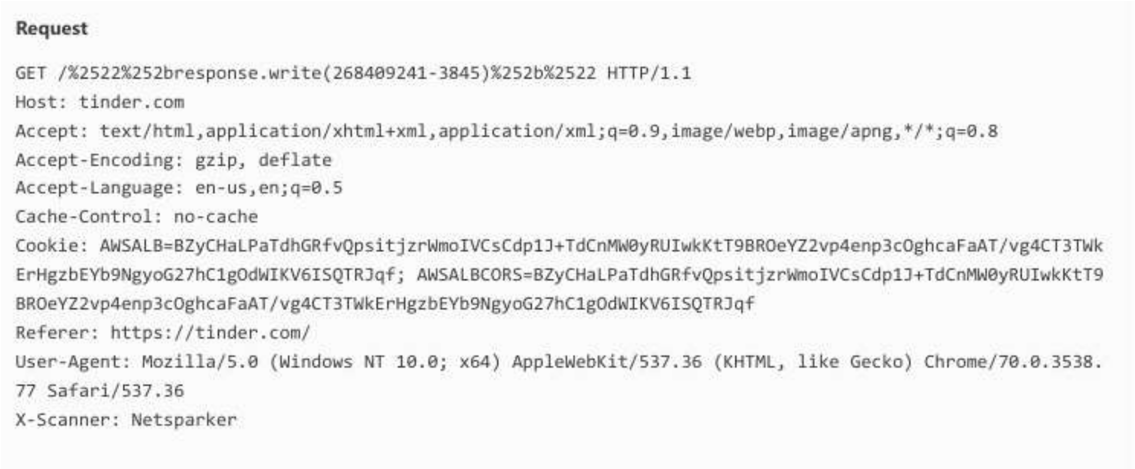
2. Privacy Violation: A breach attack might violate user privacy, which would be upsetting to the impacted customers and might put tinder in legal hot water.

3. Financial Consequences: Financial repercussions from breach occurrences might include regulatory fines, legal costs, and the requirement to compensate impacted parties. The financial stability of tinder may be impacted by these obligations.

4. Operational Disruption: tinder's regular activities may be disrupted when responding to a breach attack, which calls for significant resources. It might take a lot of time and resources to respond to incidents, remediate them, and communicate with others.

Strengthening security measures, keeping an eye out for attempted breaches, and regularly evaluating and improving the website's security controls are essential for mitigating this vulnerability. Users are put in danger when this problem is ignored, and tindert's standing, financial soundness, and general business ethics are all at stake. Depending on the behavior of hostile actors and the degree of security flaws on the website, the vulnerability's exact impact may vary.

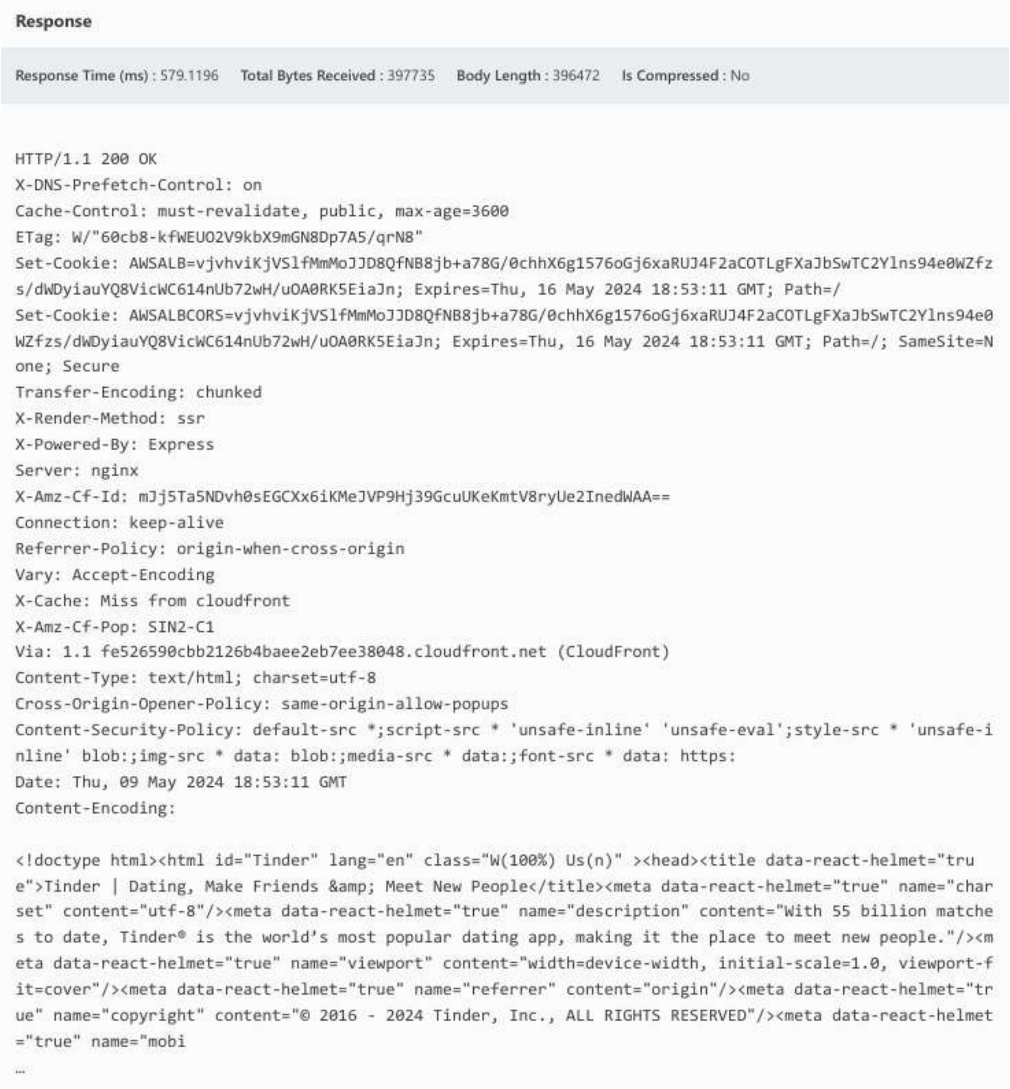
- Request



Request

```
GET /%2522%252bresponse.write(268409241-3845)%252b%2522 HTTP/1.1
Host: tinder.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
Cookie: AWSALB=BZyCHaLPaTdhGRfvQpsitjzrWmoIVCsCdp1J+TdCnMW0yRUIwkKtT9BROeYZ2vp4enp3cOghcaFaAT/vg4CT3TWk
ErHgzbEYb9NgyoG27hC1gOdWIKV6ISQTRJqf; AWSALBCORS=BZyCHaLPaTdhGRfvQpsitjzrWmoIVCsCdp1J+TdCnMW0yRUIwkKtT9
BROeYZ2vp4enp3cOghcaFaAT/vg4CT3TWkErHgzbEYb9NgyoG27hC1gOdWIKV6ISQTRJqf
Referer: https://tinder.com/
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

Response Time (ms) : 579.1196   Total Bytes Received : 397735   Body Length : 396472   Is Compressed : No

```
HTTP/1.1 200 OK
X-DNS-Prefetch-Control: on
Cache-Control: must-revalidate, public, max-age=3600
ETag: W/"60cb8-kfWEUO2V9kbX9mGN8Dp7A5/qrN8"
Set-Cookie: AWSALB=vjvhviKjVSlfMmMoJJD8QfNB8jb+a78G/0chhX6g1576oGj6xaRUJ4F2aCOTLgFXaJbSwTC2Ylns94e0WZfz
s/dWDyiauYQ8VicWC614nUb72wH/uOA0RK5EiaJn; Expires=Thu, 16 May 2024 18:53:11 GMT; Path=/
Set-Cookie: AWSALBCORS=vjvhviKjVSlfMmMoJJD8QfNB8jb+a78G/0chhX6g1576oGj6xaRUJ4F2aCOTLgFXaJbSwTC2Ylns94e0
WZfzs/dWDyiauYQ8VicWC614nUb72wH/uOA0RK5EiaJn; Expires=Thu, 16 May 2024 18:53:11 GMT; Path=/; SameSite=N
one; Secure
Transfer-Encoding: chunked
X-Render-Method: ssr
X-Powered-By: Express
Server: nginx
X-Amz-Cf-Id: mJj5Ta5NDvh0sEGCXx6iKMeJVP9Hj39GcuUKeKmtV8ryUe2InedWAA==
Connection: keep-alive
Referrer-Policy: origin-when-cross-origin
Vary: Accept-Encoding
X-Cache: Miss from cloudfront
X-Amz-Cf-Pop: SIN2-C1
Via: 1.1 fe526590cbb2126b4baee2eb7ee38048.cloudfront.net (CloudFront)
Content-Type: text/html; charset=utf-8
Cross-Origin-Opener-Policy: same-origin-allow-popups
Content-Security-Policy: default-src *;script-src * 'unsafe-inline' 'unsafe-eval';style-src * 'unsafe-i
nline' blob:;img-src * data: blob:;media-src * data:;font-src * data: https:
Date: Thu, 09 May 2024 18:53:11 GMT
Content-Encoding:

<!doctype html><html id="Tinder" lang="en" class="W(100%) Us(n)" ><head><title data-react-helmet="tru
e">Tinder | Dating, Make Friends &amp; Meet New People</title><meta data-react-helmet="true" name="char
set" content="utf-8"/><meta data-react-helmet="true" name="description" content="With 55 billion matche
s to date, Tinder® is the world’s most popular dating app, making it the place to meet new people."/><m
eta data-react-helmet="true" name="viewport" content="width=device-width, initial-scale=1.0, viewport-f
it=cover"/><meta data-react-helmet="true" name="referrer" content="origin"/><meta data-react-helmet="tr
ue" name="copyright" content="© 2016 - 2024 Tinder, Inc., ALL RIGHTS RESERVED"/><meta data-react-helmet
="true" name="mobi
…
```

To mitigate the issue, we recommend the following solutions:

1. If possible, disable HTTP level compression

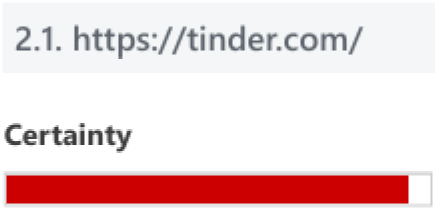
2. Separate sensitive information from user input

3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.

4. Hide the length of the traffic by adding a random number of bytes to the responses.

5. Add in a rate limit, so that the page maximum is reached five times per minute.

HTTP Strict Transport Security (HSTS) Policy Not Enabled



2.1. https://tinder.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://tinder.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.

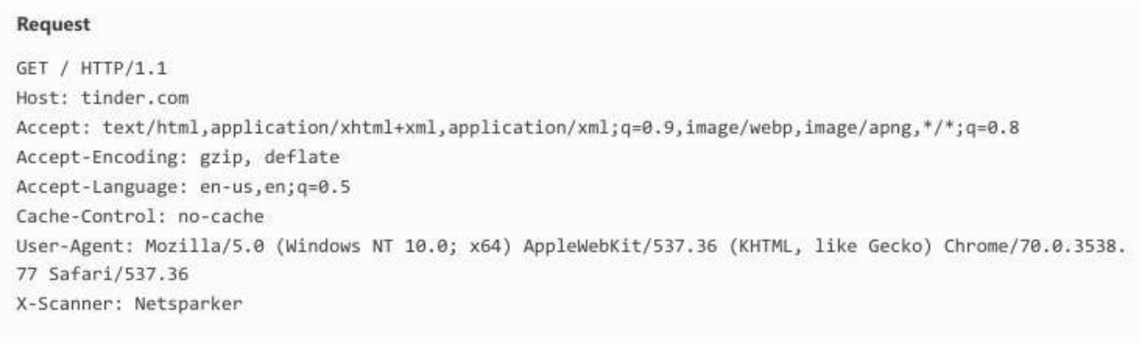
3. Phishing and Data Theft: By pretending to be www.echobox.com, cybercriminals may leverage this vulnerability to conduct phishing attacks and fool victims into disclosing sensitive information such login passwords, personal information, or bank account information. Financial losses and data theft may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

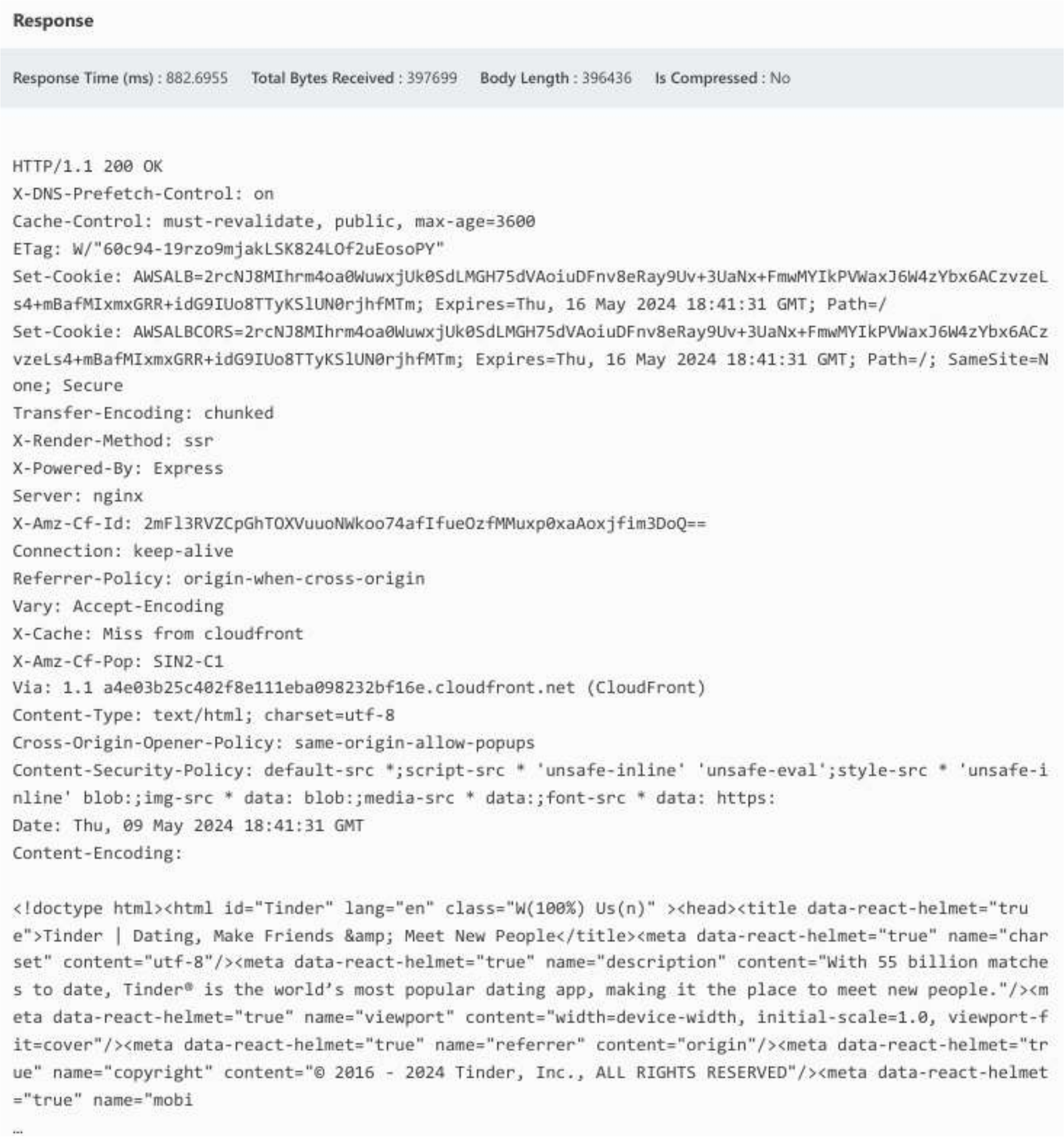
Turning on HSTS is essential to fixing this vulnerability. This security feature prevents downgrading attacks and improves overall security by guaranteeing that all communications with the website are encrypted and safe. Quick HSTS implementation can help the website comply with legal obligations, preserve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

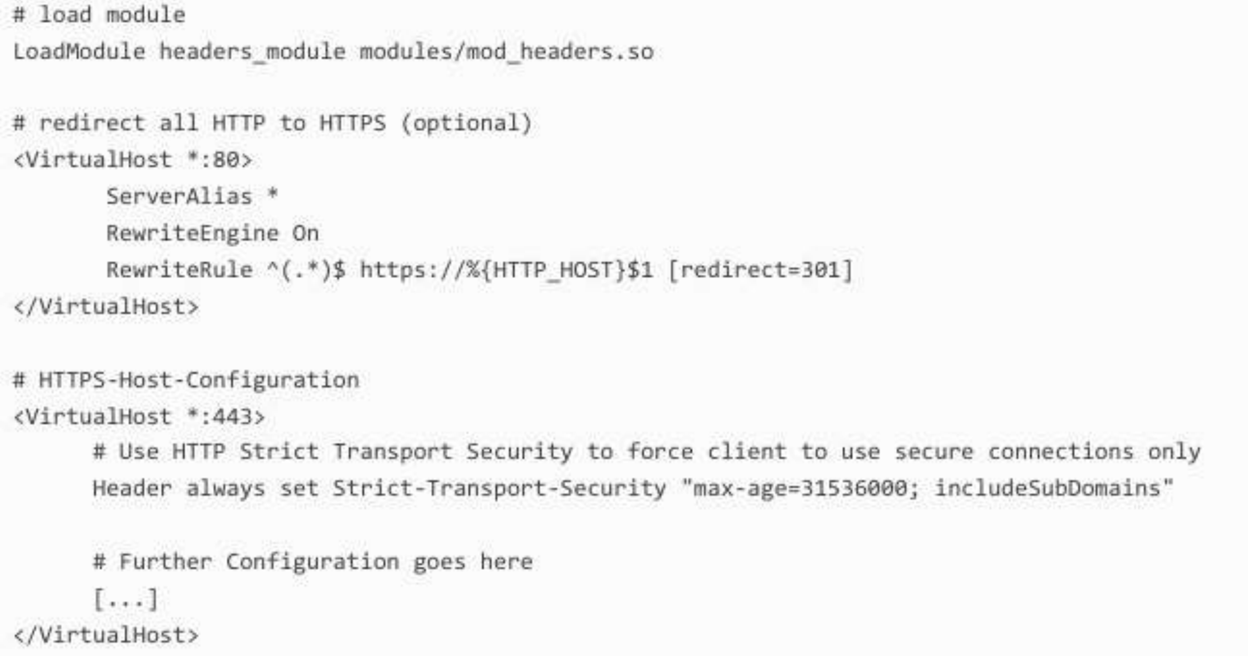
```
GET / HTTP/1.1
Host: tinder.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```



Response

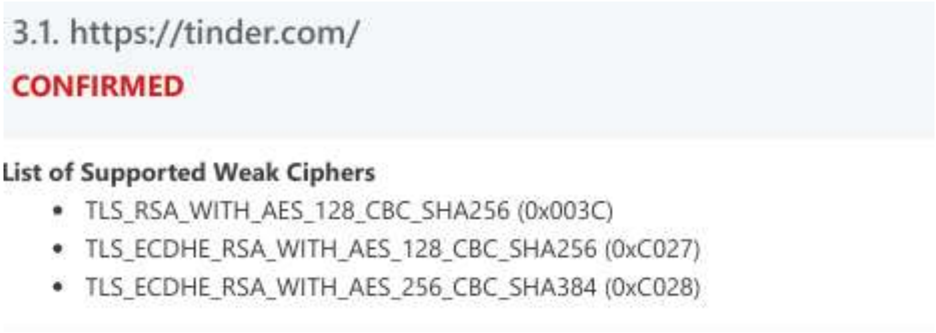
Response Time (ms) : 882.6955 Total Bytes Received : 397699 Body Length : 396436 Is Compressed : No

```
HTTP/1.1 200 OK
X-DNS-Prefetch-Control: on
Cache-Control: must-revalidate, public, max-age=3600
ETag: W/"60c94-19rzo9mjakLSK824LOf2uEosoPY"
Set-Cookie: AWSALB=2rcNJ8MIhrm4oa0WuwxjUk0SdLMGH75dVAoiuDFnv8eRay9Uv+3UaNx+FmwMYIkPVWaxJ6W4zYbx6ACzvzeL
s4+mBafMIxmxGRR+idG9IUo8TTyKSlUN0rjhfMTm; Expires=Thu, 16 May 2024 18:41:31 GMT; Path=/
Set-Cookie: AWSALBCORS=2rcNJ8MIhrm4oa0WuwxjUk0SdLMGH75dVAoiuDFnv8eRay9Uv+3UaNx+FmwMYIkPVWaxJ6W4zYbx6ACz
vzeLs4+mBafMIxmxGRR+idG9IUo8TTyKSlUN0rjhfMTm; Expires=Thu, 16 May 2024 18:41:31 GMT; Path=/; SameSite=N
one; Secure
Transfer-Encoding: chunked
X-Render-Method: ssr
X-Powered-By: Express
Server: nginx
X-Amz-Cf-Id: 2mFl3RVZCpGhTOXVuuoNWkoo74afIfueOzfMMuxp0xaAoxjfim3DoQ==
Connection: keep-alive
Referrer-Policy: origin-when-cross-origin
Vary: Accept-Encoding
X-Cache: Miss from cloudfront
X-Amz-Cf-Pop: SIN2-C1
Via: 1.1 a4e03b25c402f8e111eba098232bf16e.cloudfront.net (CloudFront)
Content-Type: text/html; charset=utf-8
Cross-Origin-Opener-Policy: same-origin-allow-popups
Content-Security-Policy: default-src *;script-src * 'unsafe-inline' 'unsafe-eval';style-src * 'unsafe-i
nline' blob:;img-src * data: blob:;media-src * data:;font-src * data: https:
Date: Thu, 09 May 2024 18:41:31 GMT
Content-Encoding:

<!doctype html><html id="Tinder" lang="en" class="W(100%) Us(n)" ><head><title data-react-helmet="tru
e">Tinder | Dating, Make Friends &amp; Meet New People</title><meta data-react-helmet="true" name="char
set" content="utf-8"/><meta data-react-helmet="true" name="description" content="With 55 billion matche
s to date, Tinder® is the world’s most popular dating app, making it the place to meet new people."/><m
eta data-react-helmet="true" name="viewport" content="width=device-width, initial-scale=1.0, viewport-f
it=cover"/><meta data-react-helmet="true" name="referrer" content="origin"/><meta data-react-helmet="tr
ue" name="copyright" content="© 2016 - 2024 Tinder, Inc., ALL RIGHTS RESERVED"/><meta data-react-helmet
="true" name="mobi
…
```



```
# 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>
```

1) Weak Ciphers Enabled



3.1. https://tinder.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- 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, https://www.tinder.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.

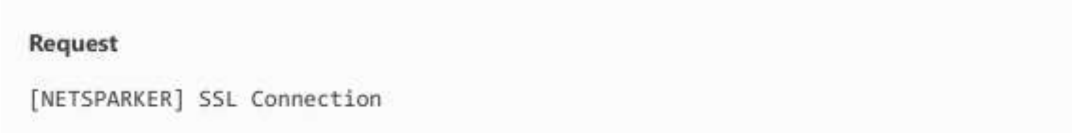
3. **Enhanced Attack Surface:** Cybercriminals can more easily exploit vulnerabilities and obtain illegal access to a website, its servers, and underlying systems when weak ciphers provide them a larger attack surface.

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.

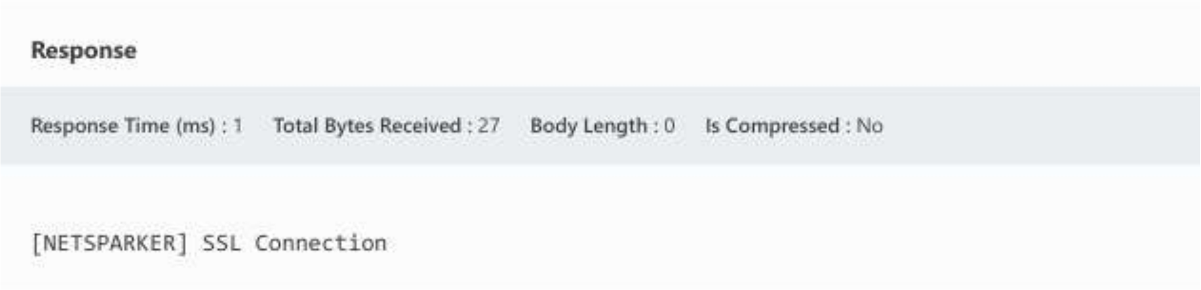
It is critical to use strong encryption techniques and ciphers to quickly resolve this Weak Cipher Enabled issue. Failing to do so puts Traffic Factory’s brand, legal compliance, and general company integrity in jeopardy in addition to exposing users to potential security risks. The actions of hostile 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
```

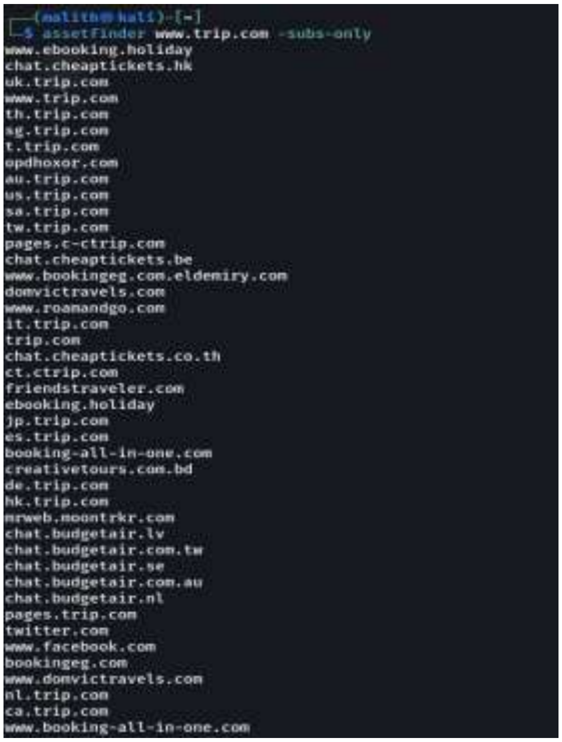
- **Remediation**

Configure your web server to disallow using weak ciphers.

Bug Bounty 6 (Trip)

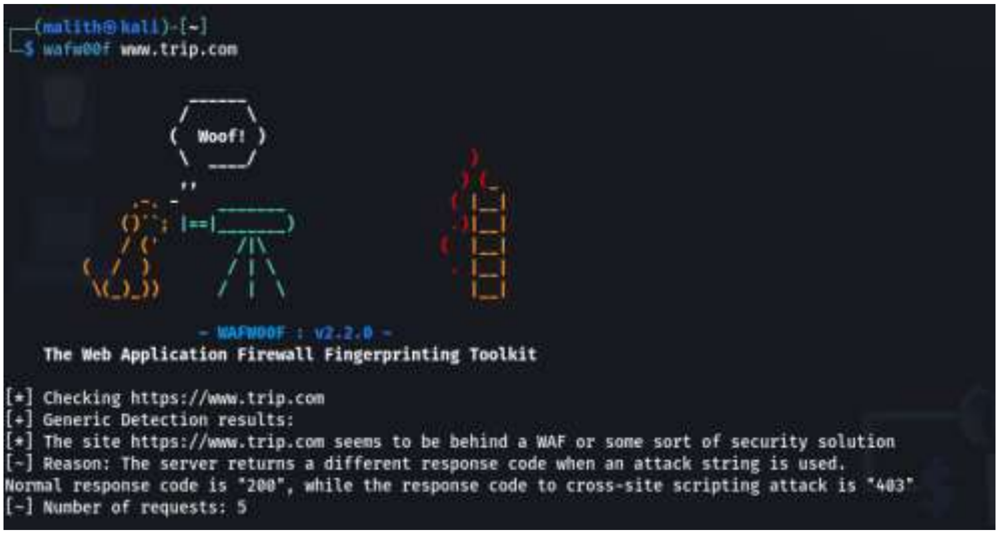
Reconnaissance

Firstly, I used the Assetfinder tool to find the subdomains of the trip website. Assetfinder tool is used to find the subdomains of a website.

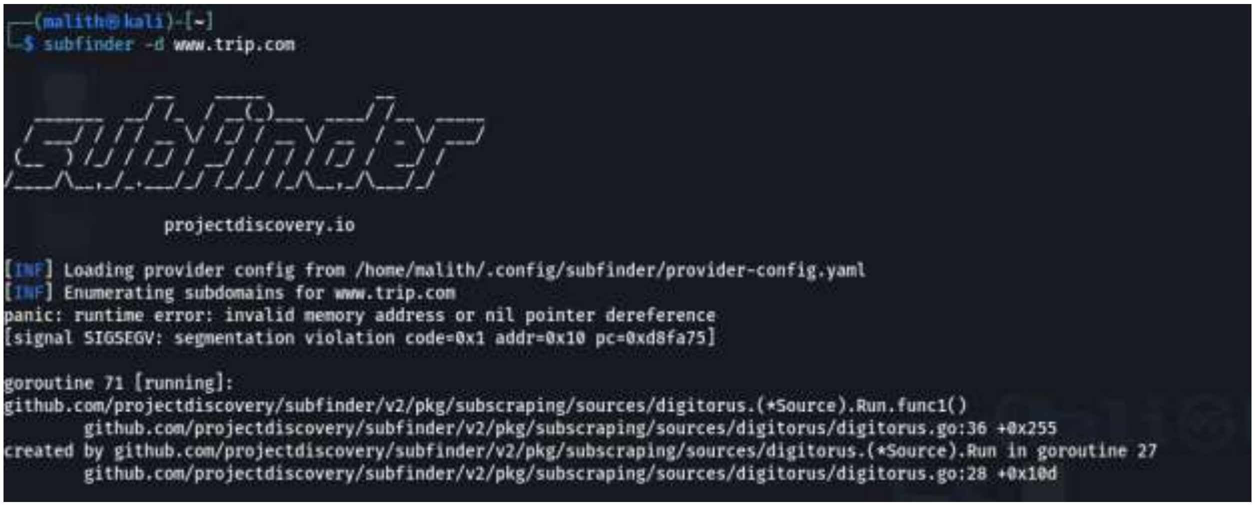


```
┌──(malith㉿kali)-[~]
└─$ assetfinder www.trip.com -subs-only
www.ebooking.holiday
chat.cheaptickets.hk
uk.trip.com
www.trip.com
th.trip.com
sg.trip.com
t.trip.com
opdhoxor.com
au.trip.com
us.trip.com
sa.trip.com
tw.trip.com
pages.c-ctrip.com
chat.cheaptickets.be
www.bookingeg.com.eldemiry.com
domvictravels.com
www.roamandgo.com
it.trip.com
trip.com
chat.cheaptickets.co.th
ct.ctrip.com
friendstraveler.com
ebooking.holiday
jp.trip.com
es.trip.com
booking-all-in-one.com
creativetours.com.bd
de.trip.com
hk.trip.com
mrweb.moontrkr.com
chat.budgetair.lv
chat.budgetair.com.tw
chat.budgetair.se
chat.budgetair.com.au
chat.budgetair.nl
pages.trip.com
twitter.com
www.facebook.com
bookingeg.com
www.domvictravels.com
nl.trip.com
ca.trip.com
www.booking-all-in-one.com
```

Then, I got the subdomains list as below.

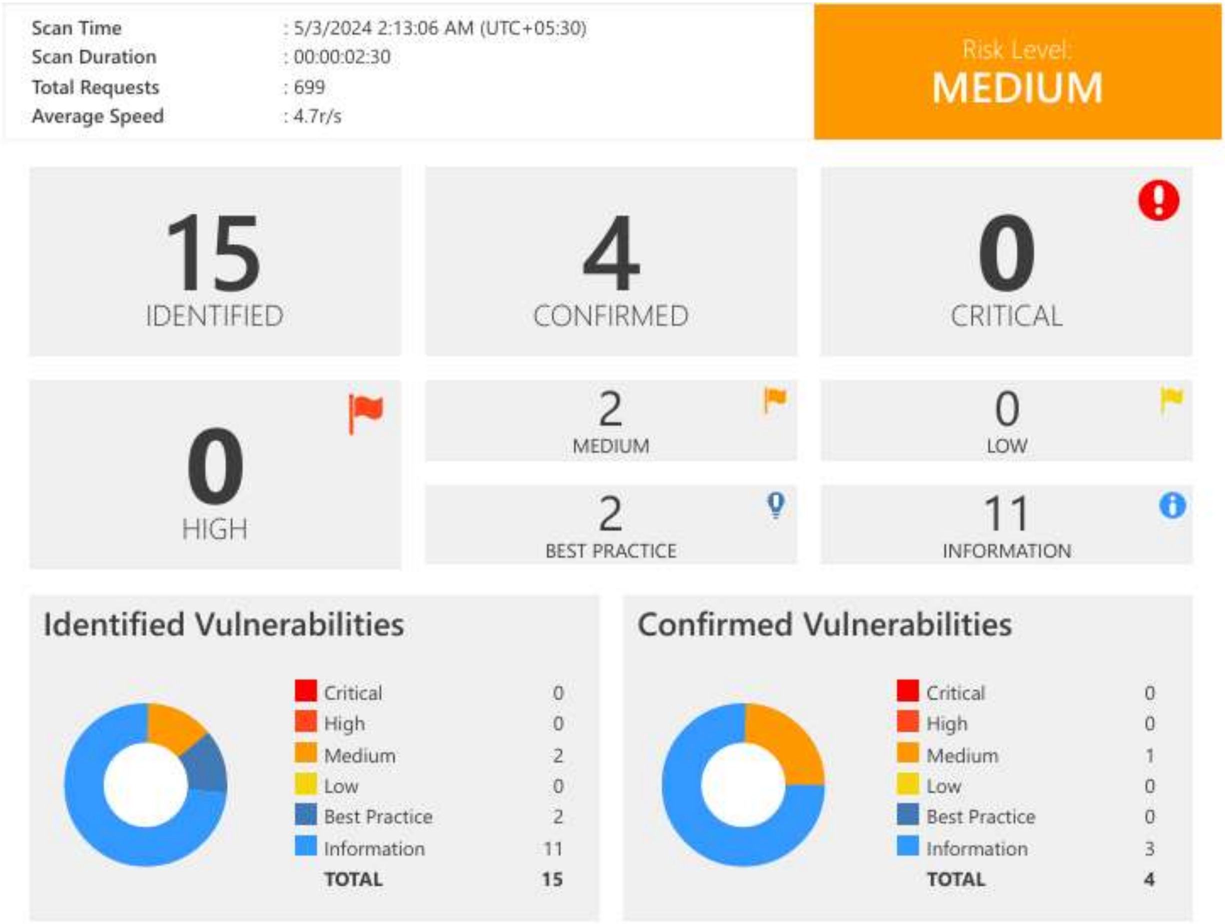


```
┌──(malith㉿kali)-[~]
└─$ wafw00f www.trip.com

                 (  Woof! )

                ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.trip.com
[+] Generic Detection results:
[*] The site https://www.trip.com seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "403"
[~] Number of requests: 5
```



```
┌──(malith㉿kali)-[~]
└─$ subfinder -d www.trip.com

                projectdiscovery.io

[INF] Loading provider config from /home/malith/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for www.trip.com
panic: runtime error: invalid memory address or nil pointer dereference
[signal SIGSEGV: segmentation violation code=0x1 addr=0x10 pc=0xd8fa75]

goroutine 71 [running]:
github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run.func1()
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:36 +0x255
created by github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run in goroutine 27
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:28 +0x10d
```

Vulnerabilities Found.



Scan Time : 5/3/2024 2:13:06 AM (UTC+05:30)
Scan Duration : 00:00:02:30
Total Requests : 699
Average Speed : 4.7r/s

Risk Level:
MEDIUM

15 IDENTIFIED

4 CONFIRMED

0 CRITICAL

0 HIGH

2 MEDIUM

0 LOW

2 BEST PRACTICE

11 INFORMATION

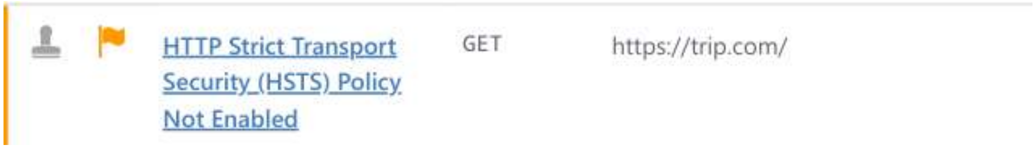
Identified Vulnerabilities

Critical	0
High	0
Medium	2
Low	0
Best Practice	2
Information	11
TOTAL	**15**

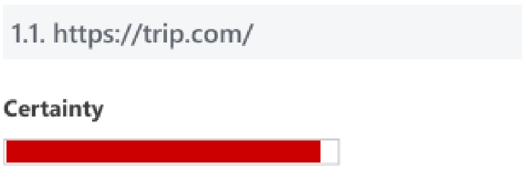
Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	0
Best Practice	0
Information	3
TOTAL	**4**

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



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



1.1. https://trip.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://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.

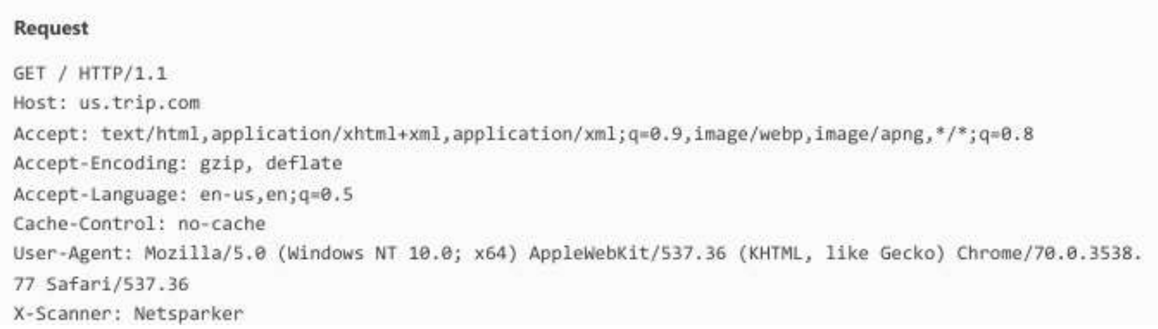
3. Phishing and Data Theft: By pretending to be www.echobox.com, cybercriminals may leverage this vulnerability to conduct phishing attacks and fool victims into disclosing sensitive information such login passwords, personal information, or bank account information. Financial losses and data theft may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

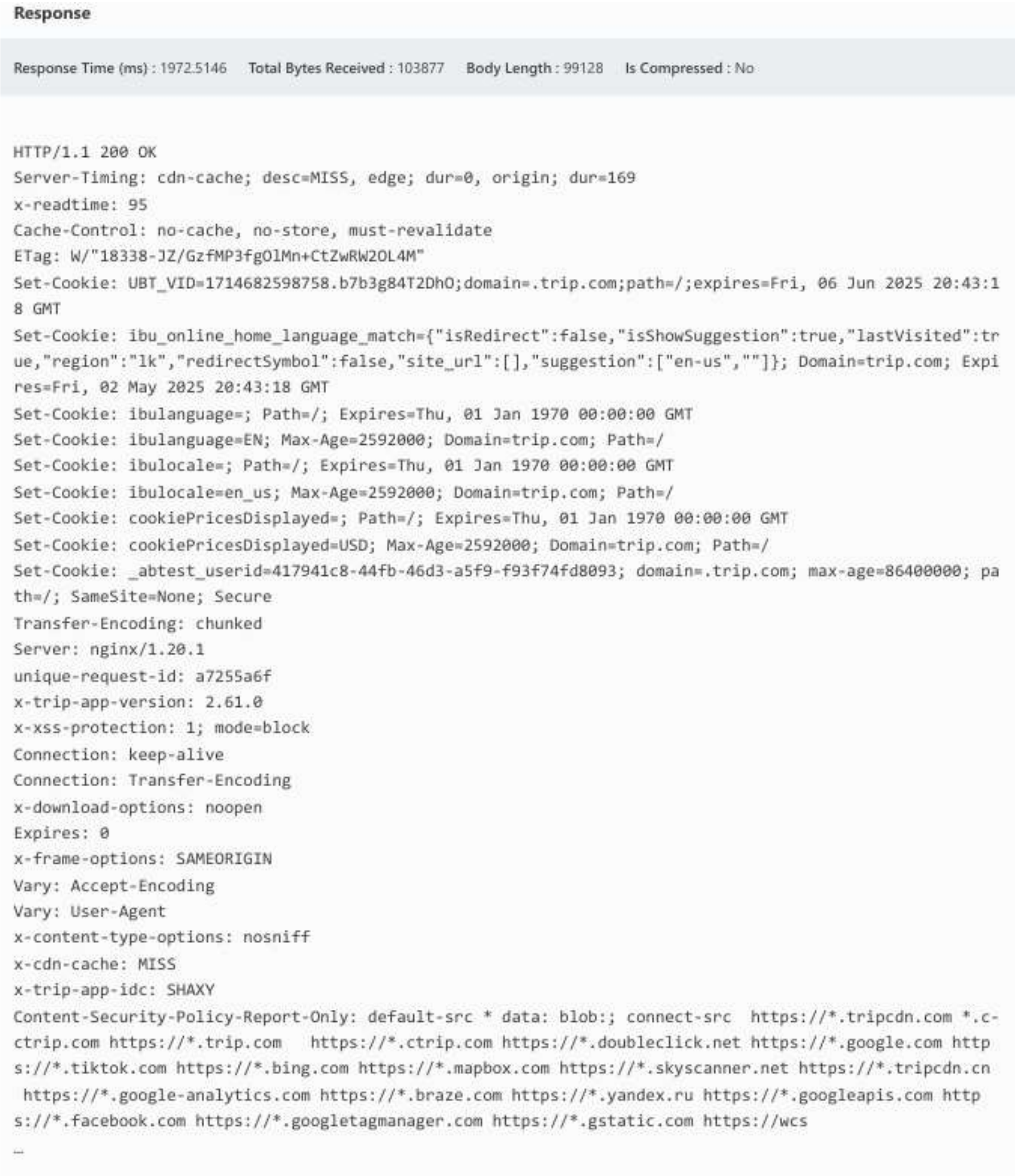
Turning on HSTS is essential to fixing this vulnerability. This security feature prevents downgrading attacks and improves overall security by guaranteeing that all communications with the website are encrypted and safe. Quick HSTS implementation can help the website comply with legal obligations, preserve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



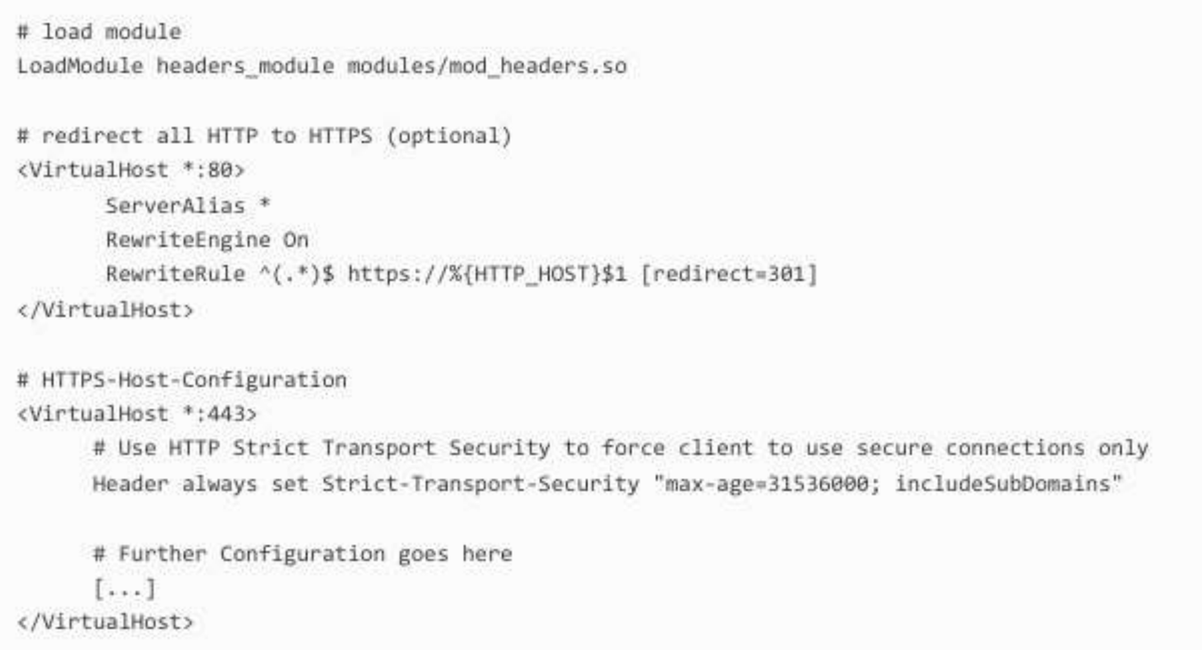
Request

```
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
```



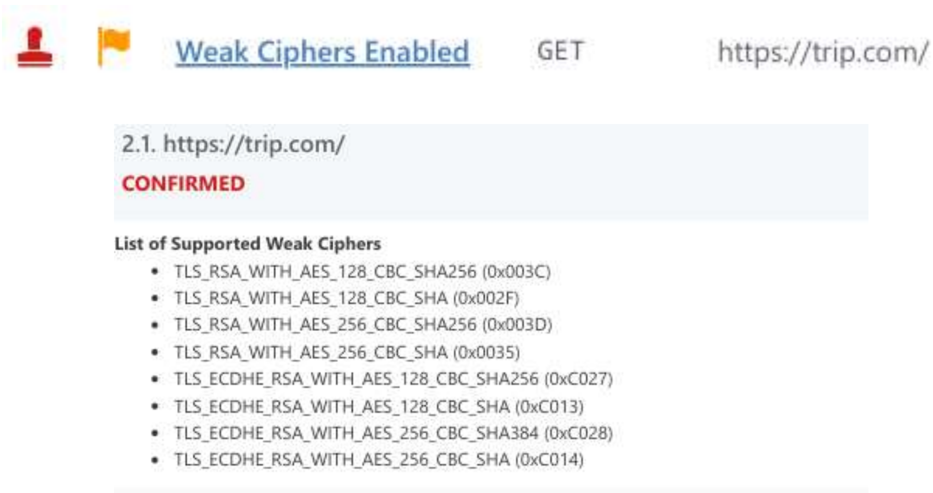
Response Time (ms) : 1972.5146   Total Bytes Received : 103877   Body Length : 99128   Is Compressed : No

```
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
…
```



```
# 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>
```

Weak Ciphers Enabled



Weak Ciphers Enabled GET https://trip.com/

2.1. https://trip.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

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.

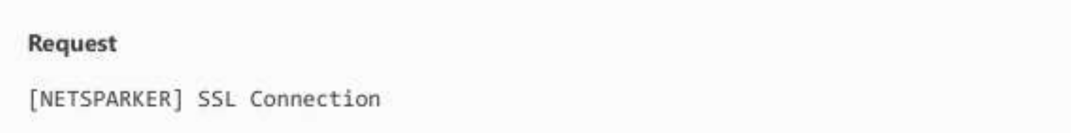
3. **Enhanced Attack Surface:** Cybercriminals can more easily exploit vulnerabilities and obtain illegal access to a website, its servers, and underlying systems when weak ciphers provide them a larger attack surface.

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.

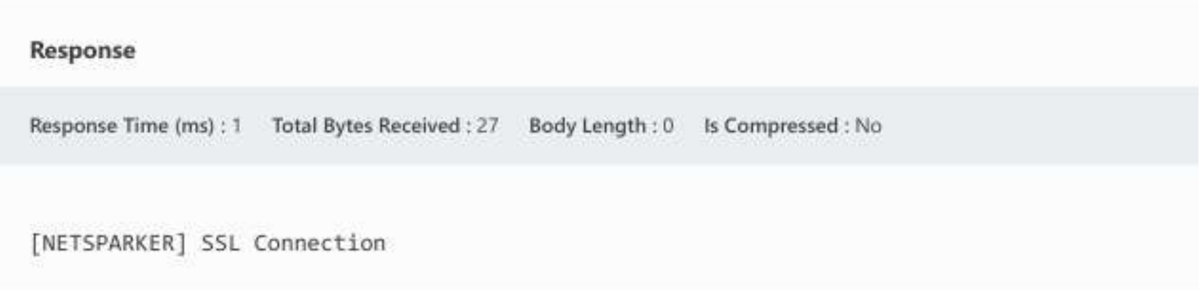
It is critical to use strong encryption techniques and ciphers to quickly resolve this Weak Cipher Enabled issue. Failing to do so puts Traffic Factory’s brand, legal compliance, and general company integrity in jeopardy in addition to exposing users to potential security risks. The actions of hostile 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
```

- **Remediation**

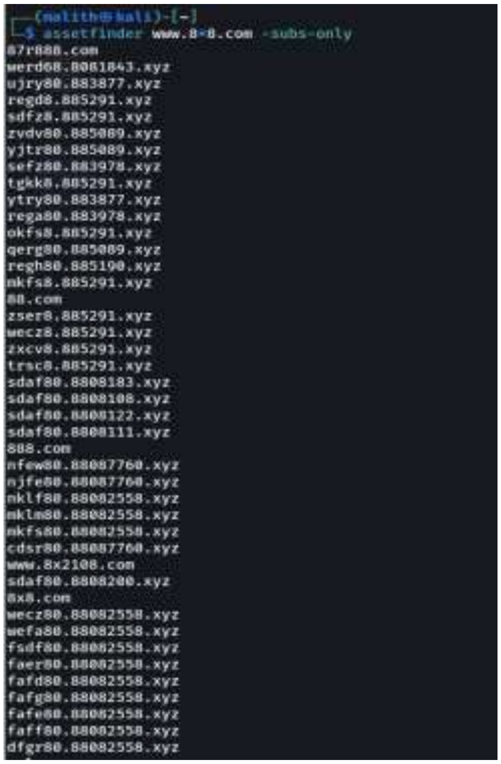
Configure your web server to disallow using weak ciphers.

Bug Bounty 7 (8x8)

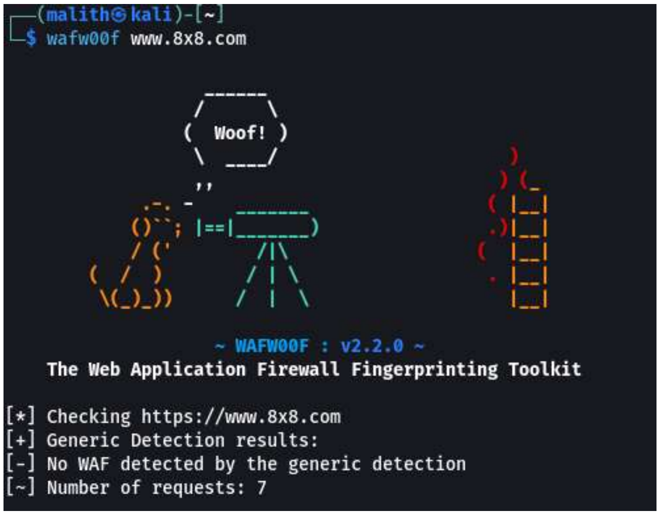
Reconnaissance

Firstly, I used the Assetfinder tool to find the subdomains of the 8x8 website. Assetfinder tool is used to find the subdomains of a website.

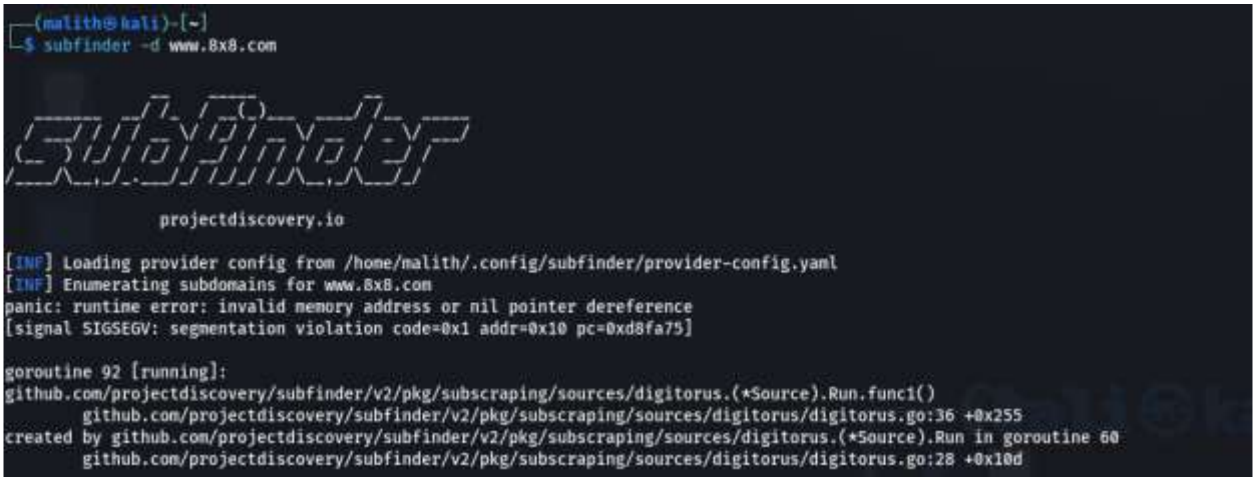
Then, I got the subdomains list as below.



```
┌──(malith㉿kali)-[~]
└─$ assetfinder www.8-8.com -subs-only
87r888.com
werd68.8081843.xyz
ujry80.883877.xyz
regd8.885291.xyz
sdfz8.885291.xyz
zvdv80.885089.xyz
yjtr80.885089.xyz
sefz80.883978.xyz
tgkk8.885291.xyz
ytry80.883877.xyz
rega80.883978.xyz
okfs8.885291.xyz
qerg80.885089.xyz
regh80.885190.xyz
mkfs8.885291.xyz
88.com
zser8.885291.xyz
wecz8.885291.xyz
zxcv8.885291.xyz
trsc8.885291.xyz
sdaf80.8808183.xyz
sdaf80.8808108.xyz
sdaf80.8808122.xyz
sdaf80.8808111.xyz
888.com
nfew80.88087760.xyz
njfe80.88087760.xyz
nklf80.88082558.xyz
mklm80.88082558.xyz
mkfs80.88082558.xyz
cdsr80.88087760.xyz
www.8x2108.com
sdaf80.8808200.xyz
8x8.com
wecz80.88082558.xyz
wefa80.88082558.xyz
fsdf80.88082558.xyz
faer80.88082558.xyz
fafd80.88082558.xyz
fafg80.88082558.xyz
fafe80.88082558.xyz
faff80.88082558.xyz
dfgr80.88082558.xyz
```

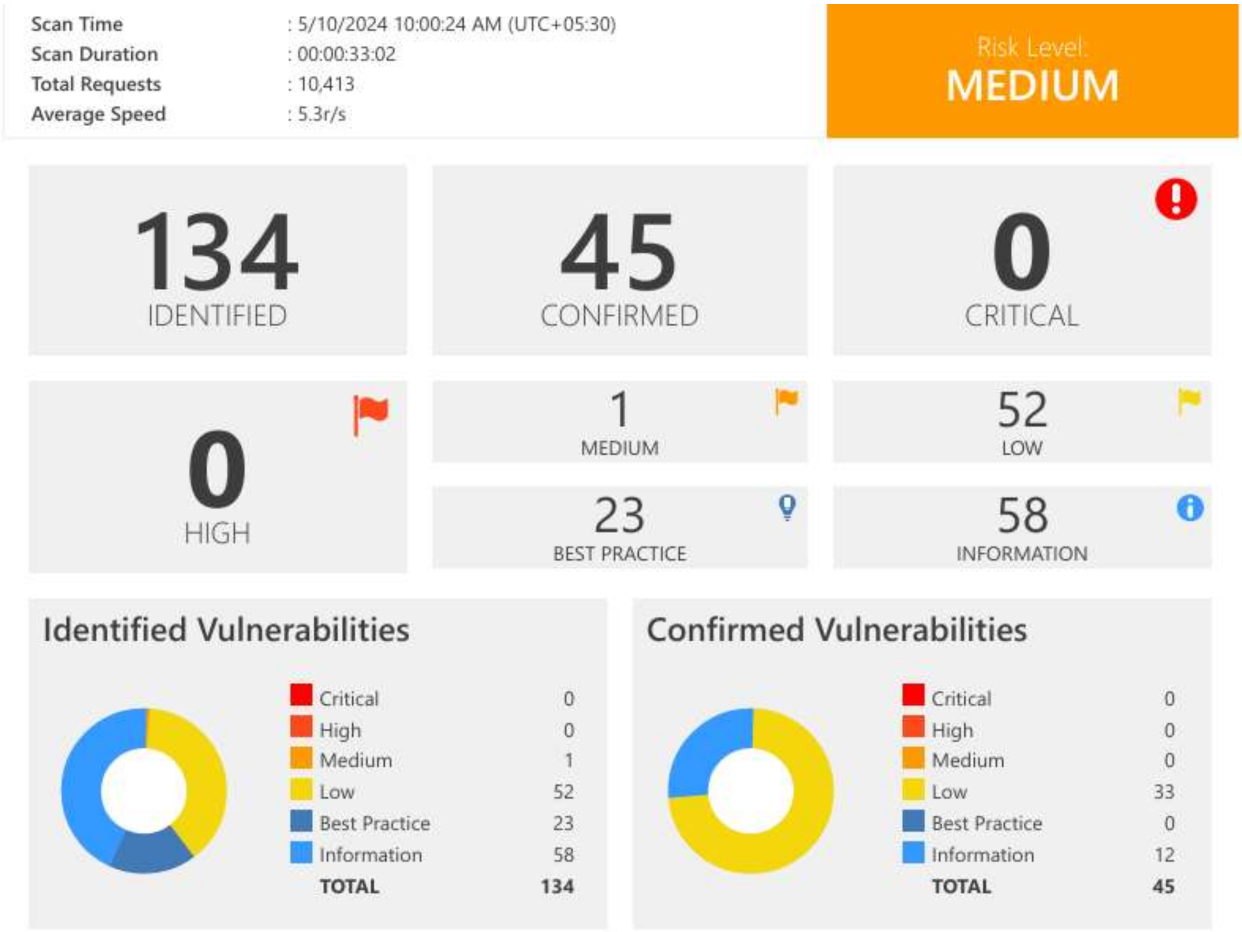


```
┌──(malith㉿kali)-[~]
└─$ wafw00f www.8x8.com

                ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.8x8.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```



```
┌──(malith㉿kali)-[~]
└─$ subfinder -d www.8x8.com

                projectdiscovery.io

[INF] Loading provider config from /home/malith/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for www.8x8.com
panic: runtime error: invalid memory address or nil pointer dereference
[signal SIGSEGV: segmentation violation code=0x1 addr=0x10 pc=0xd8fa75]

goroutine 92 [running]:
github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run.func1()
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:36 +0x255
created by github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run in goroutine 60
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:28 +0x10d
```

Vulnerabilities Found.



Scan Time : 5/10/2024 10:00:24 AM (UTC+05:30)
Scan Duration : 00:00:33:02
Total Requests : 10,413
Average Speed : 5.3r/s

Risk Level:
MEDIUM

134 IDENTIFIED

45 CONFIRMED

0 CRITICAL

0 HIGH

1 MEDIUM

52 LOW

23 BEST PRACTICE

58 INFORMATION

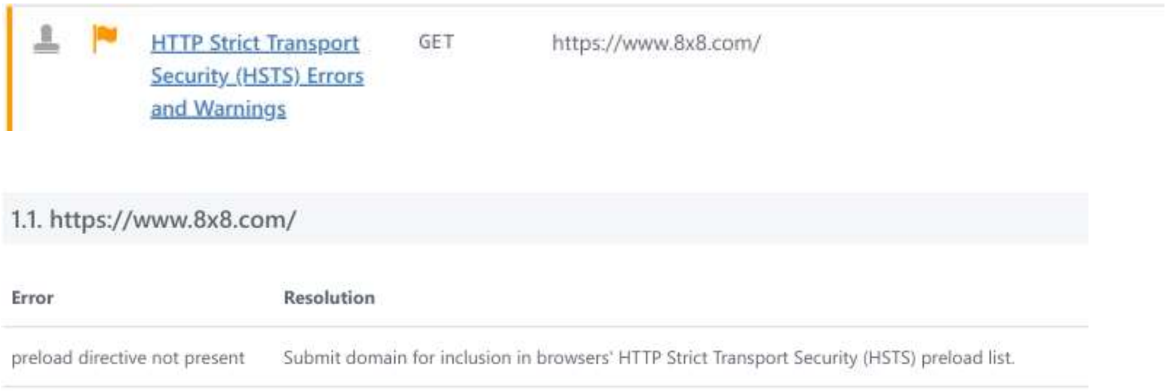
Identified Vulnerabilities

🟥 Critical	0
🟥 High	0
🟧 Medium	1
🟨 Low	52
🟦 Best Practice	23
🟦 Information	58
TOTAL	**134**

Confirmed Vulnerabilities

🟥 Critical	0
🟥 High	0
🟧 Medium	0
🟨 Low	33
🟦 Best Practice	0
🟦 Information	12
TOTAL	**45**

HTTP Strict Transport Security (HSTS) Errors and Warnings



HTTP Strict Transport Security (HSTS) Errors and Warnings GET https://www.8x8.com/

1.1. https://www.8x8.com/

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

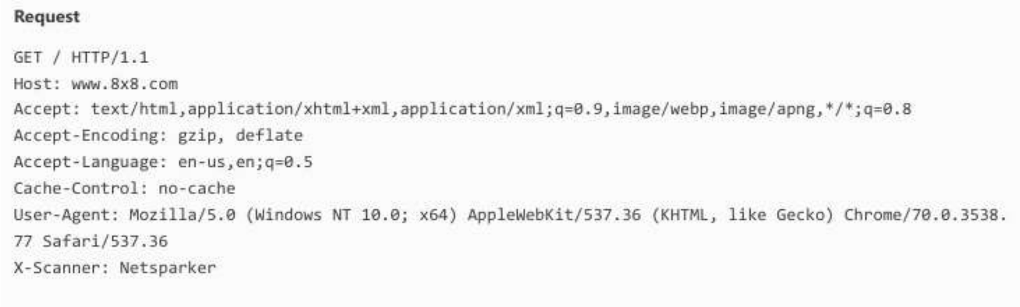
Date of Discovery: 20/04/2024

Date of Reporting: 21/04/2024

• Description

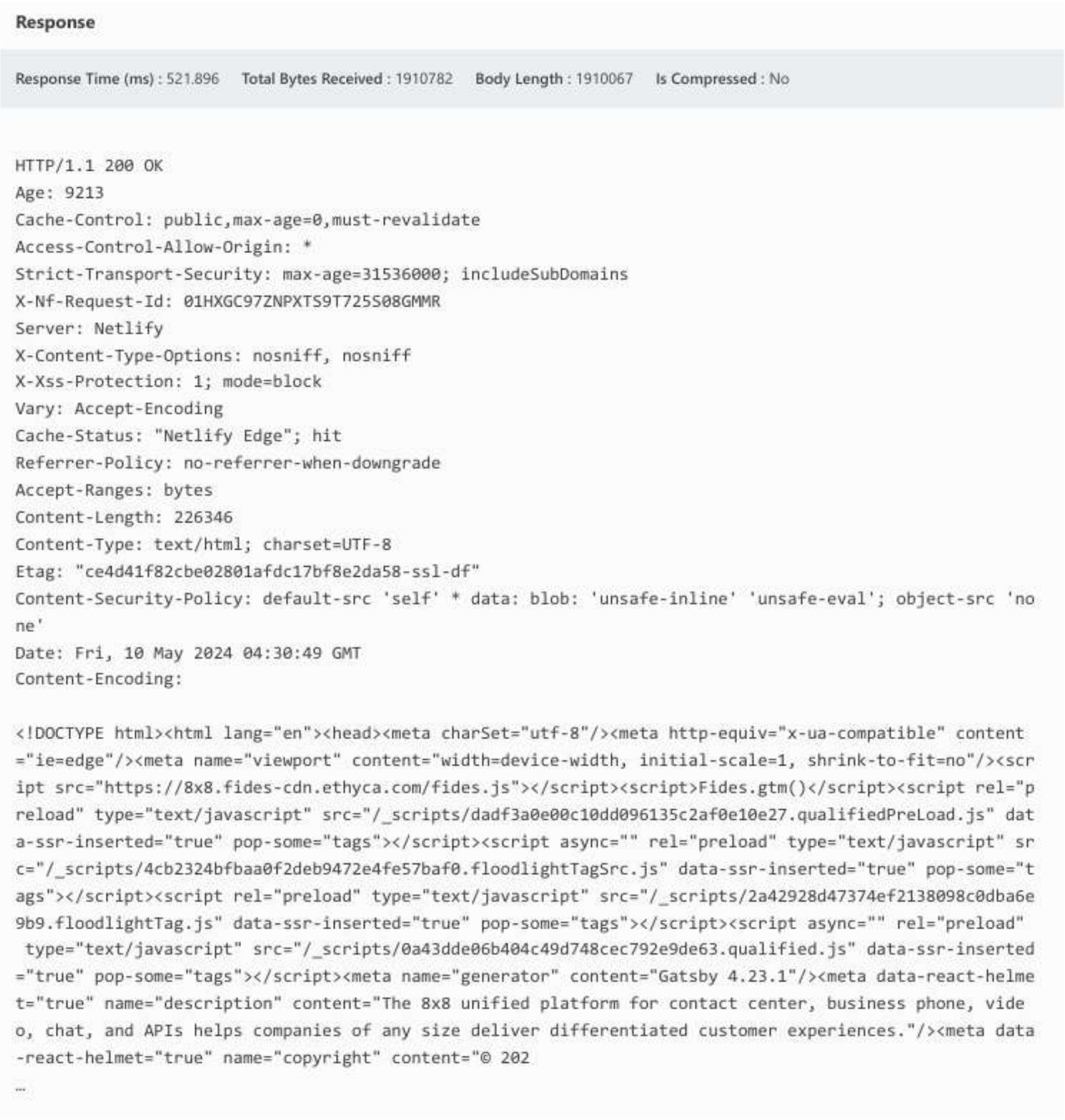
The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

• Proof of Concept



Request

```
GET / HTTP/1.1
Host: www.8x8.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

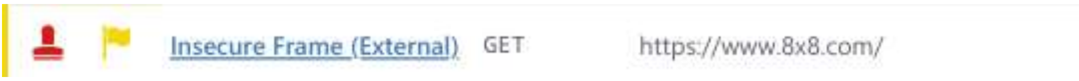
Response Time (ms) : 521.896 **Total Bytes Received :** 1910782 **Body Length :** 1910067 **Is Compressed :** No

```
HTTP/1.1 200 OK
Age: 9213
Cache-Control: public,max-age=0,must-revalidate
Access-Control-Allow-Origin: *
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Nf-Request-Id: 01HXGC97ZNPXTS9T725S08GMMR
Server: Netlify
X-Content-Type-Options: nosniff, nosniff
X-Xss-Protection: 1; mode=block
Vary: Accept-Encoding
Cache-Status: "Netlify Edge"; hit
Referrer-Policy: no-referrer-when-downgrade
Accept-Ranges: bytes
Content-Length: 226346
Content-Type: text/html; charset=UTF-8
Etag: "ce4d41f82cbe02801afdc17bf8e2da58-ssl-df"
Content-Security-Policy: default-src 'self' * data: blob: 'unsafe-inline' 'unsafe-eval'; object-src 'no
ne'
Date: Fri, 10 May 2024 04:30:49 GMT
Content-Encoding:

<!DOCTYPE html><html lang="en"><head><meta charSet="utf-8"/><meta http-equiv="x-ua-compatible" content
="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/><scr
ipt src="https://8x8.fides-cdn.ethyca.com/fides.js"></script><script>Fides.gtm()</script><script rel="p
reload" type="text/javascript" src="/_scripts/dadf3a0e00c10dd096135c2af0e10e27.qualifiedPreLoad.js" dat
a-ssr-inserted="true" pop-some="tags"></script><script async="" rel="preload" type="text/javascript" sr
c="/_scripts/4cb2324bfbaa0f2deb9472e4fe57baf0.floodlightTagSrc.js" data-ssr-inserted="true" pop-some="t
ags"></script><script rel="preload" type="text/javascript" src="/_scripts/2a42928d47374ef2138098c0dba6e
9b9.floodlightTag.js" data-ssr-inserted="true" pop-some="tags"></script><script async="" rel="preload"
 type="text/javascript" src="/_scripts/0a43dde06b404c49d748cec792e9de63.qualified.js" data-ssr-inserted
="true" pop-some="tags"></script><meta name="generator" content="Gatsby 4.23.1"/><meta data-react-helme
t="true" name="description" content="The 8x8 unified platform for contact center, business phone, vide
o, chat, and APIs helps companies of any size deliver differentiated customer experiences."/><meta data
-react-helmet="true" name="copyright" content="© 202
…
```

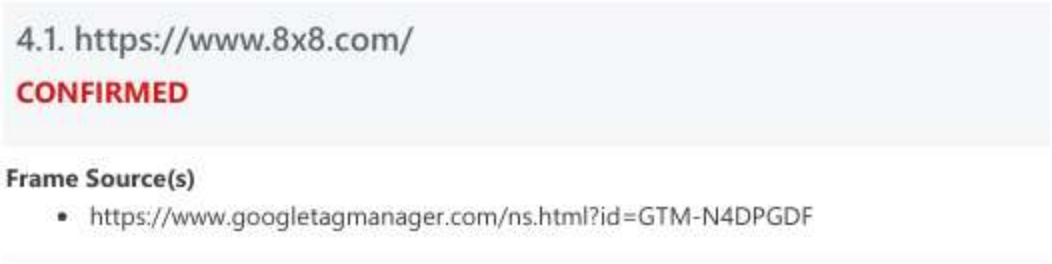
- ## Remediation

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Insecure Frame (External)



Insecure Frame (External) GET https://www.8x8.com/



4.1. https://www.8x8.com/

CONFIRMED

Frame Source(s)

- https://www.googletagmanager.com/ns.html?id=GTM-N4DPGDF

Date of Discovery: 20/04/2024

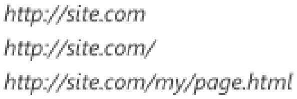
Date of Reporting: 21/04/2024

- ## Description & impact Assessment

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

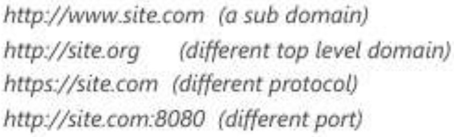
The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly

Here is an example, the URLs below all belong to the same origin as http://site.com:



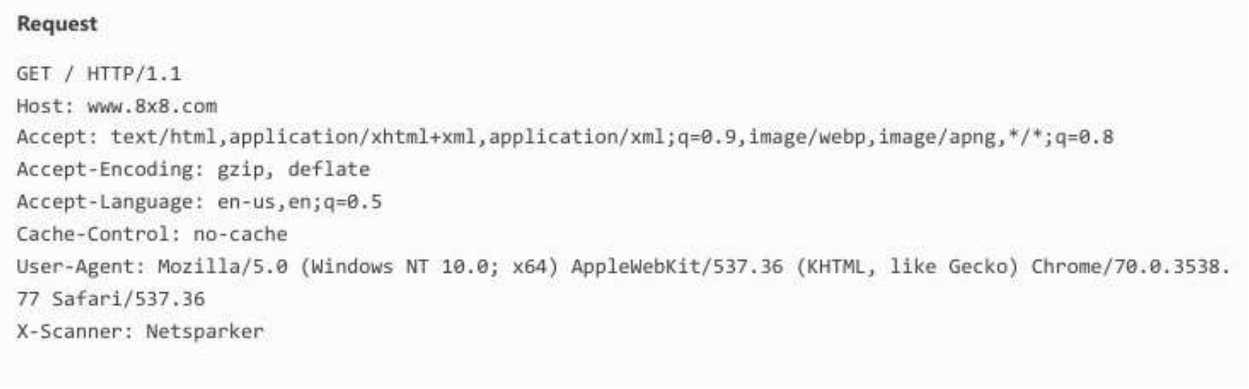
http://site.com
http://site.com/
http://site.com/my/page.html

Whereas the URLs mentioned below aren't from the same origin **as <u>http://site.com</u>**:



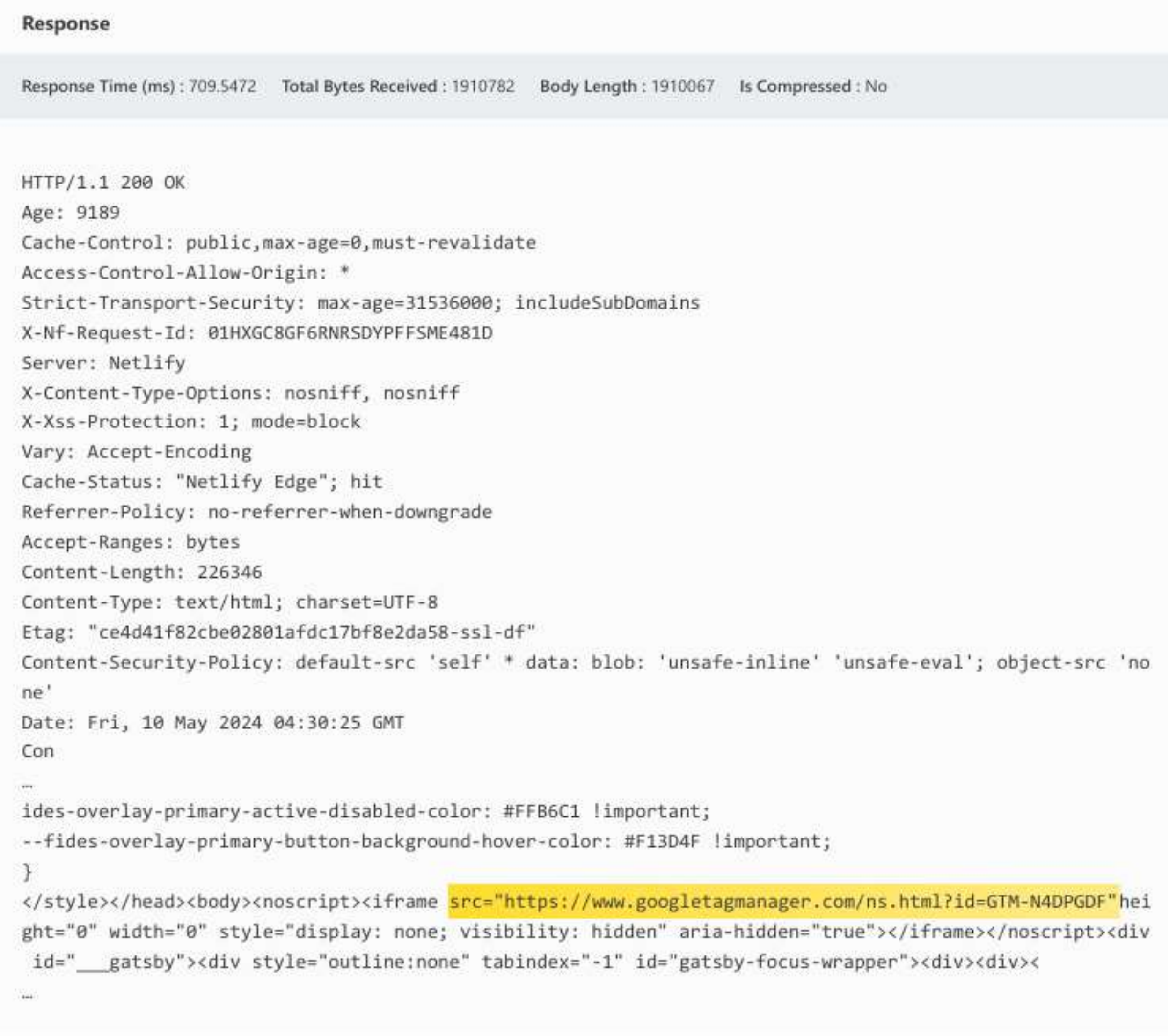
http://www.site.com (a sub domain)
http://site.org (different top level domain)
https://site.com (different protocol)
http://site.com:8080 (different port)

- Steps to Reproduce



Request

```
GET / HTTP/1.1
Host: www.8x8.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

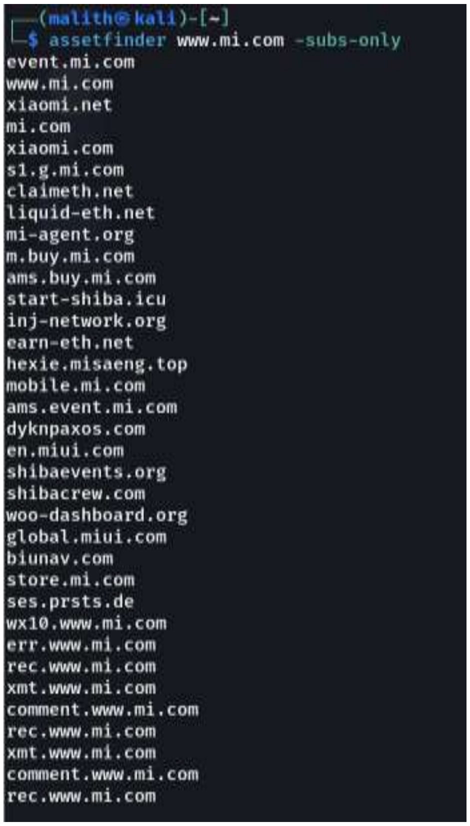
Response Time (ms) : 709.5472   Total Bytes Received : 1910782   Body Length : 1910067   Is Compressed : No

```
HTTP/1.1 200 OK
Age: 9189
Cache-Control: public,max-age=0,must-revalidate
Access-Control-Allow-Origin: *
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Nf-Request-Id: 01HXGC8GF6RNRSDYPFFSME481D
Server: Netlify
X-Content-Type-Options: nosniff, nosniff
X-Xss-Protection: 1; mode=block
Vary: Accept-Encoding
Cache-Status: "Netlify Edge"; hit
Referrer-Policy: no-referrer-when-downgrade
Accept-Ranges: bytes
Content-Length: 226346
Content-Type: text/html; charset=UTF-8
Etag: "ce4d41f82cbe02801afdc17bf8e2da58-ssl-df"
Content-Security-Policy: default-src 'self' * data: blob: 'unsafe-inline' 'unsafe-eval'; object-src 'no
ne'
Date: Fri, 10 May 2024 04:30:25 GMT
Con
…
ides-overlay-primary-active-disabled-color: #FFB6C1 !important;
--fides-overlay-primary-button-background-hover-color: #F13D4F !important;
}
</style></head><body><noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-N4DPGDF"hei
ght="0" width="0" style="display: none; visibility: hidden" aria-hidden="true"></iframe></noscript><div
 id="___gatsby"><div style="outline:none" tabindex="-1" id="gatsby-focus-wrapper"><div><div><
…
```

Bug Bounty 8 (mi)

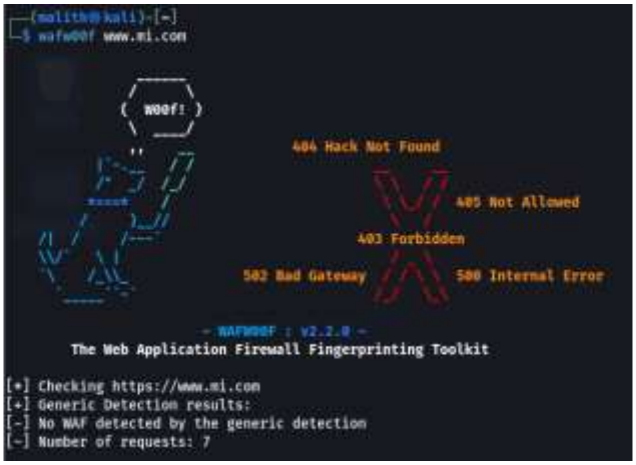
Reconnaissance

Firstly, I used the Assetfinder tool to find the subdomains of the mi website. Assetfinder tool is used to find the subdomains of a website.

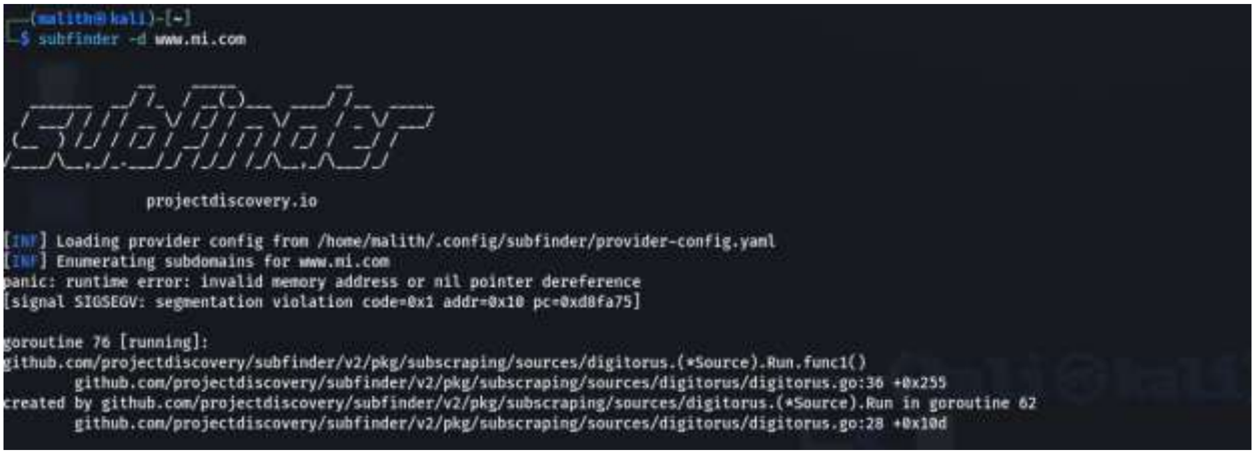


```
┌──(malith㉿kali)-[~]
└─$ assetfinder www.mi.com -subs-only
event.mi.com
www.mi.com
xiaomi.net
mi.com
xiaomi.com
s1.g.mi.com
claimeth.net
liquid-eth.net
mi-agent.org
m.buy.mi.com
ams.buy.mi.com
start-shiba.icu
inj-network.org
earn-eth.net
hexie.misaeng.top
mobile.mi.com
ams.event.mi.com
dyknpaxos.com
en.miui.com
shibaevents.org
shibacrew.com
woo-dashboard.org
global.miui.com
biunav.com
store.mi.com
ses.prsts.de
wx10.www.mi.com
err.www.mi.com
rec.www.mi.com
xmt.www.mi.com
comment.www.mi.com
rec.www.mi.com
xmt.www.mi.com
comment.www.mi.com
rec.www.mi.com
```

Then, I got the subdomains list as below.

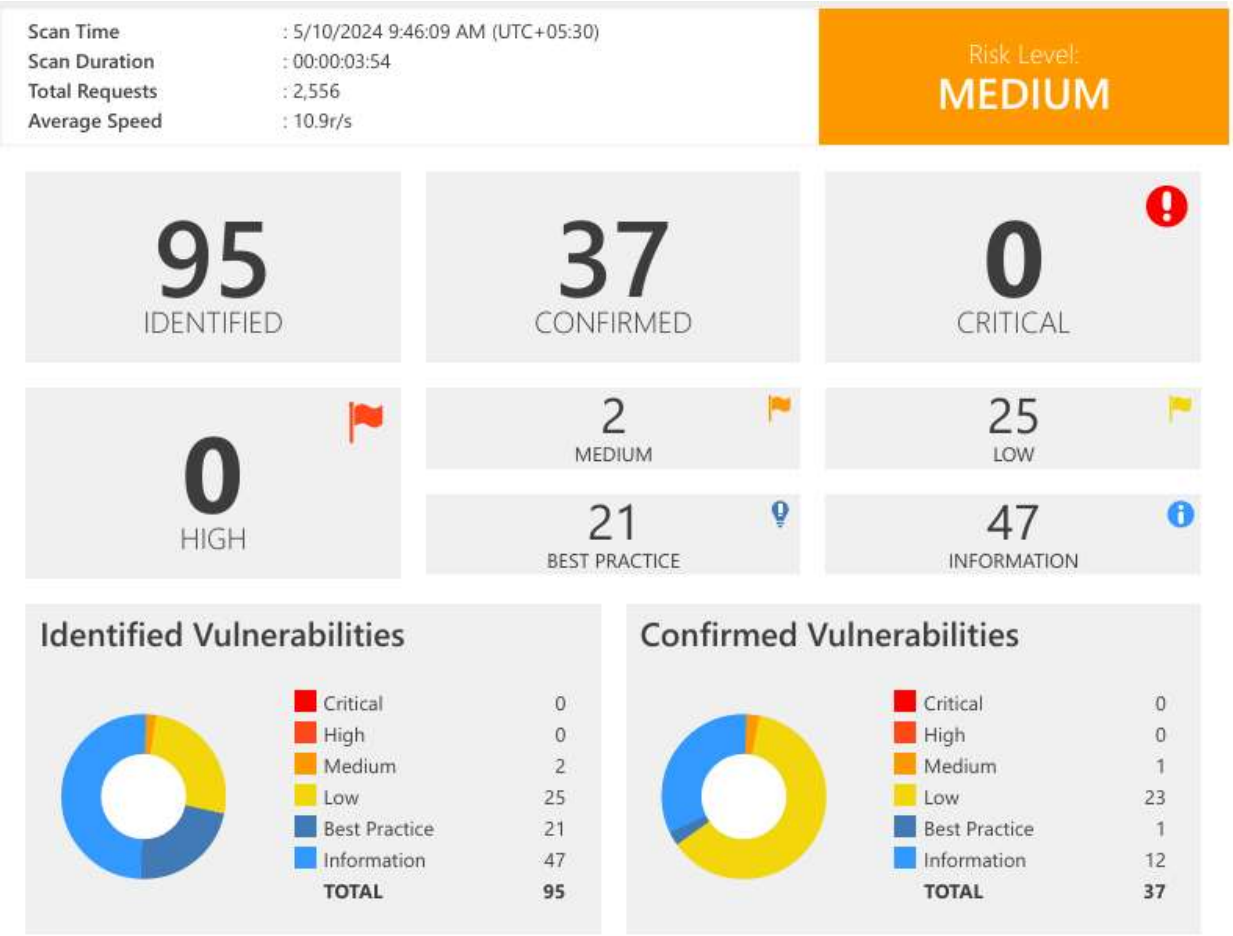


```
┌──(malith㉿kali)-[~]
└─$ wafw00f www.mi.com

                    ( W00f! )
                                  404 Hack Not Found
                                                        405 Not Allowed
                                            403 Forbidden
                           502 Bad Gateway              500 Internal Error

                        ~ WAFW00F : v2.2.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.mi.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
```



```
┌──(malith㉿kali)-[~]
└─$ subfinder -d www.mi.com

               projectdiscovery.io

[INF] Loading provider config from /home/malith/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for www.mi.com
panic: runtime error: invalid memory address or nil pointer dereference
[signal SIGSEGV: segmentation violation code=0x1 addr=0x10 pc=0xd8fa75]

goroutine 76 [running]:
github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run.func1()
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:36 +0x255
created by github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run in goroutine 62
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:28 +0x10d
```

Vulnerabilities Found.



Scan Time	: 5/10/2024 9:46:09 AM (UTC+05:30)
Scan Duration	: 00:00:03:54
Total Requests	: 2,556
Average Speed	: 10.9r/s

Risk Level:
MEDIUM

95 IDENTIFIED

37 CONFIRMED

0 CRITICAL

0 HIGH

2 MEDIUM

25 LOW

21 BEST PRACTICE

47 INFORMATION

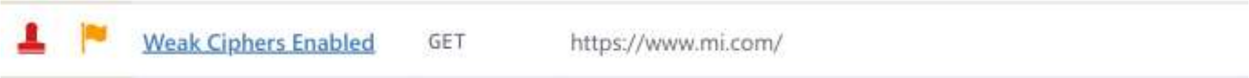
Identified Vulnerabilities

🟥	Critical	0
🟥	High	0
🟧	Medium	2
🟨	Low	25
🟦	Best Practice	21
🟦	Information	47
	TOTAL	**95**

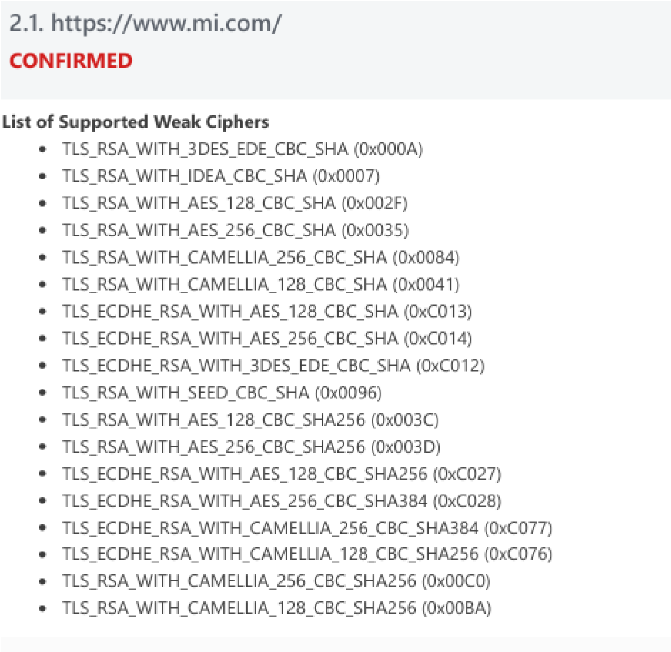
Confirmed Vulnerabilities

🟥	Critical	0
🟥	High	0
🟧	Medium	1
🟨	Low	23
🟦	Best Practice	1
🟦	Information	12
	TOTAL	**37**

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

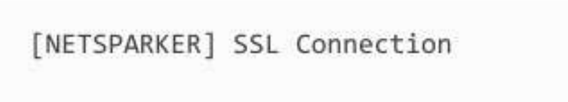
Under the OWASP category connected to poor Cipher Enabled vulnerabilities within the domain of **http://mi.com/**, various potential security threats have been found due to the usage of poor encryption protocols or ciphers. The impact of not addressing this vulnerability is considerable and includes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

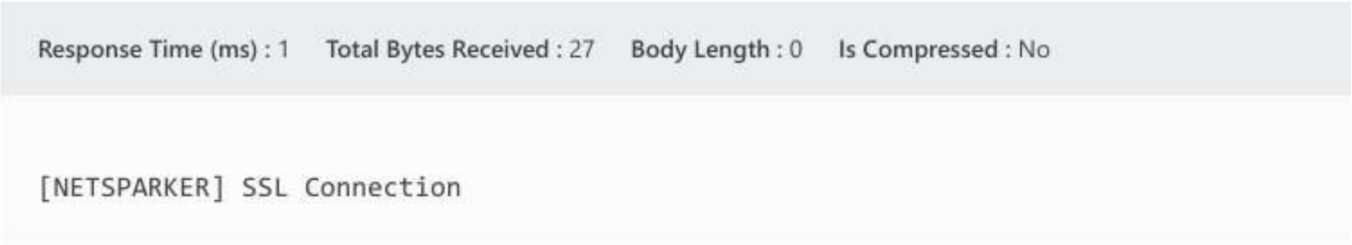
It is vital to fix this Weak Cipher Enabled issue swiftly by adopting strong encryption methods and ciphers. Failure to do so not only expose users to potential security concerns but also damages Starbucks' reputation, legal compliance, and general corporate integrity. The repercussions of the vulnerability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

- ## Request



```
[NETSPARKER] SSL Connection
```

- **Response**



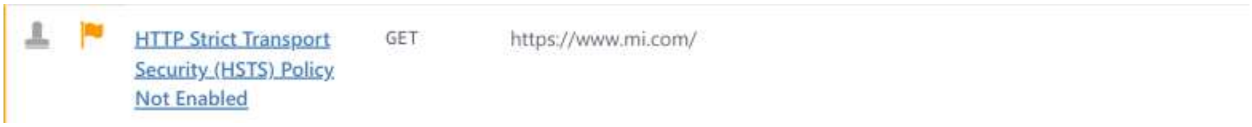
Response Time (ms) : 1   Total Bytes Received : 27   Body Length : 0   Is Compressed : No

```
[NETSPARKER] SSL Connection
```

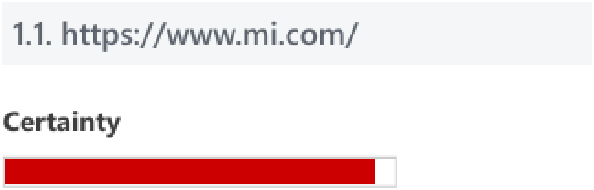
- **Remediation**

Configure your web server to disallow using weak ciphers.

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.

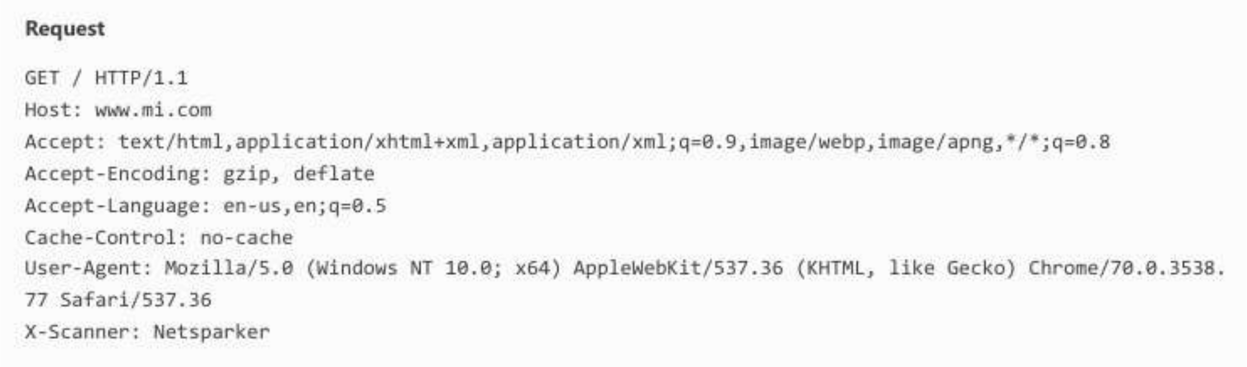
3. Phishing and Data Theft: By pretending to be www.echobox.com, cybercriminals may leverage this vulnerability to conduct phishing attacks and fool victims into disclosing sensitive information such login passwords, personal information, or bank account information. Financial losses and data theft may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

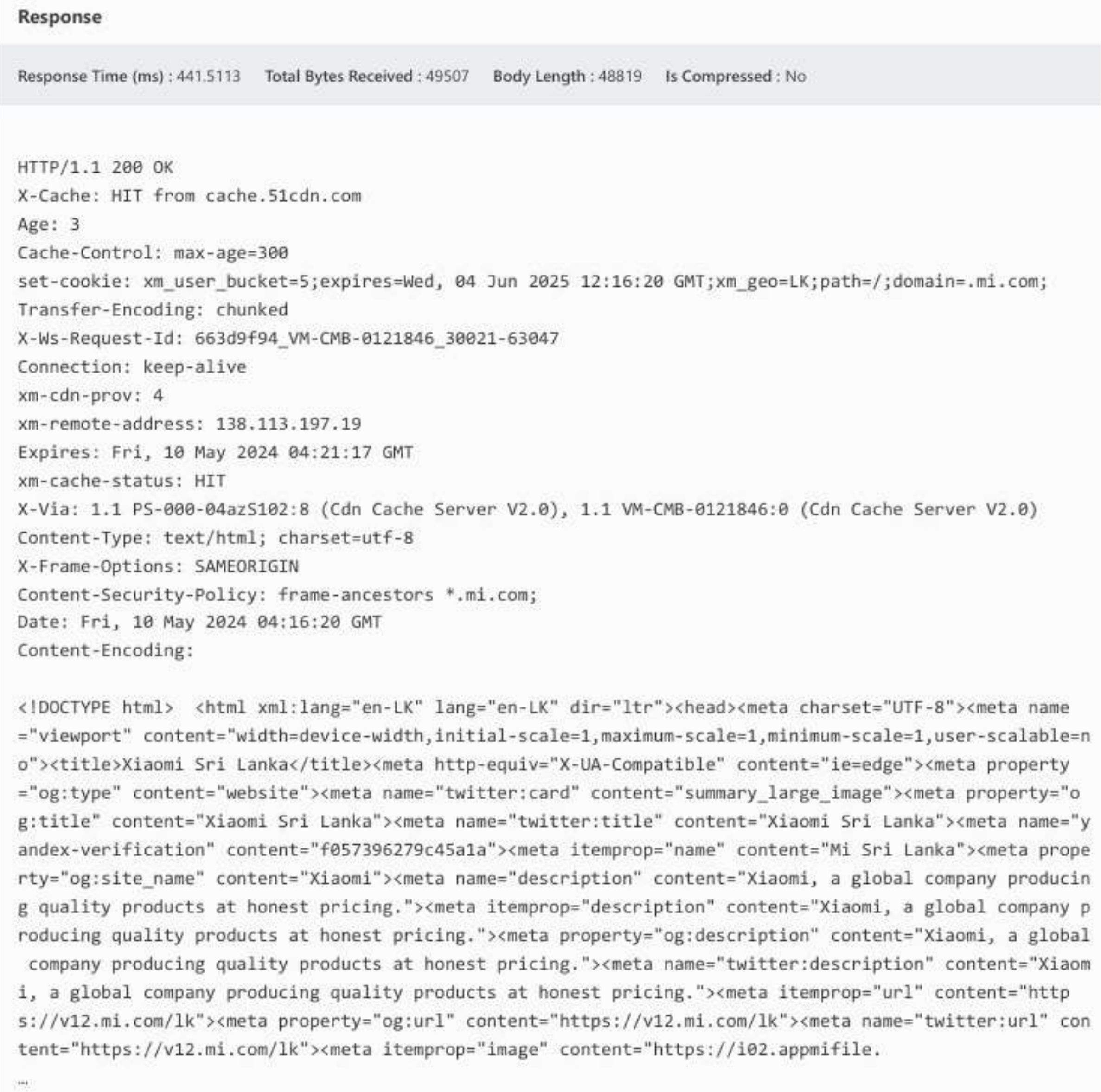
Turning on HSTS is essential to fixing this vulnerability. This security feature prevents downgrading attacks and improves overall security by guaranteeing that all communications with the website are encrypted and safe. Quick HSTS implementation can help the website comply with legal obligations, preserve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

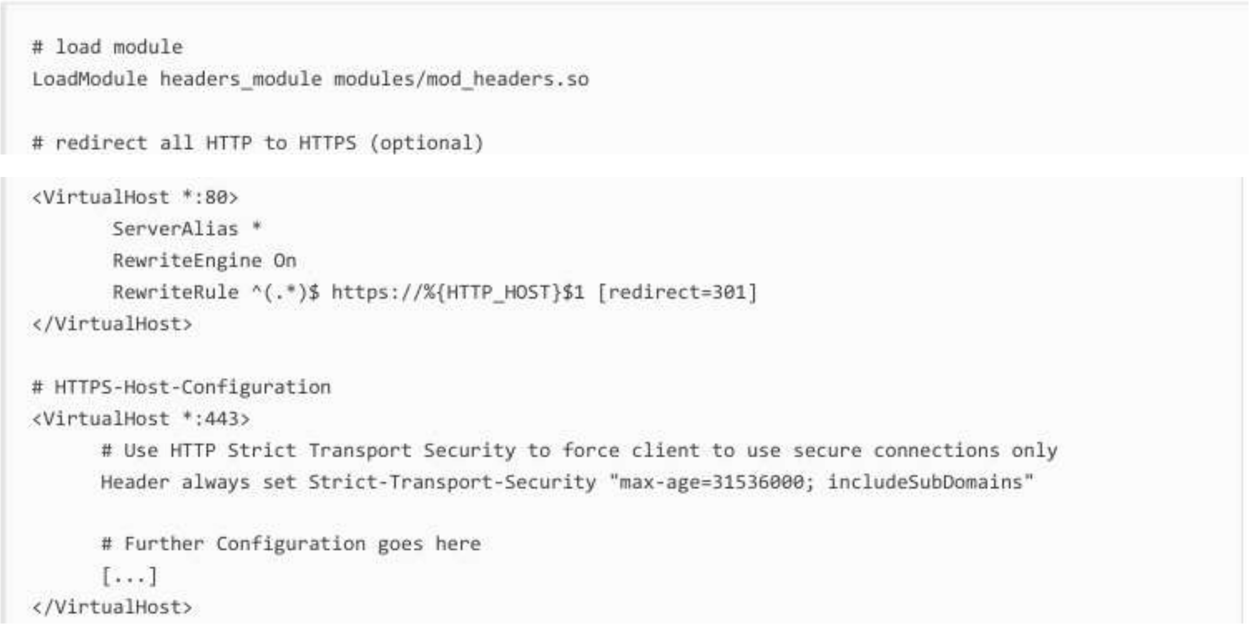


Response

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

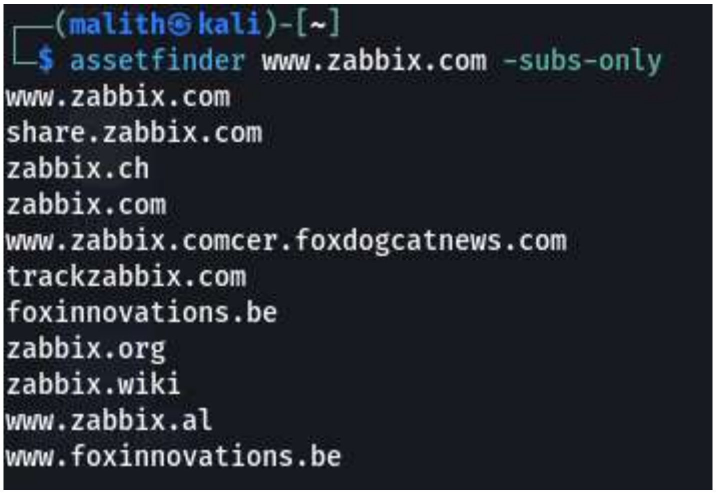


```
# load module
LoadModule headers_module modules/mod_headers.so

# 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>
```

Bug Bounty 9 (zabbix)

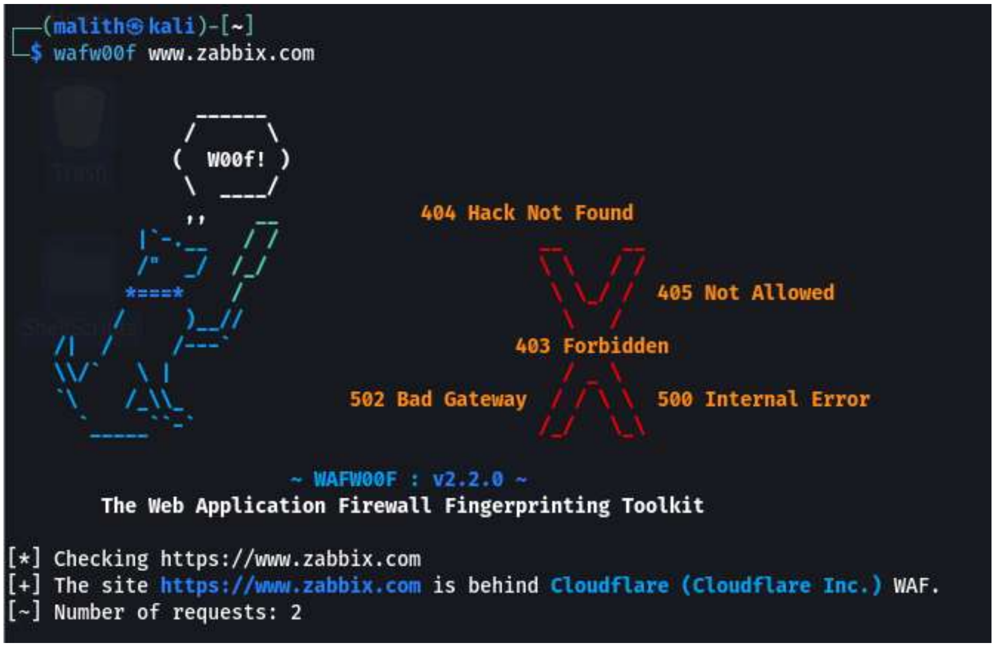
Reconnaissance

Firstly, I used the Assetfinder tool to find the subdomains of the zabbix website. Assetfinder tool is used to find the subdomains of a website.

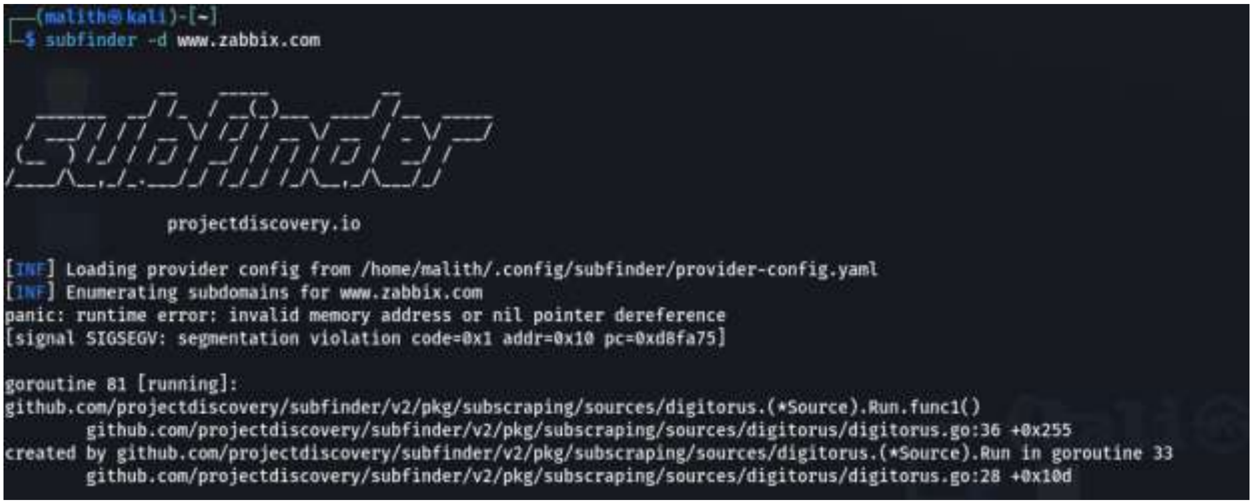


```
┌──(malith㉿kali)-[~]
└─$ assetfinder www.zabbix.com -subs-only
www.zabbix.com
share.zabbix.com
zabbix.ch
zabbix.com
www.zabbix.comcer.foxdogcatnews.com
trackzabbix.com
foxinnovations.be
zabbix.org
zabbix.wiki
www.zabbix.al
www.foxinnovations.be
```

Then, I got the subdomains list as below.

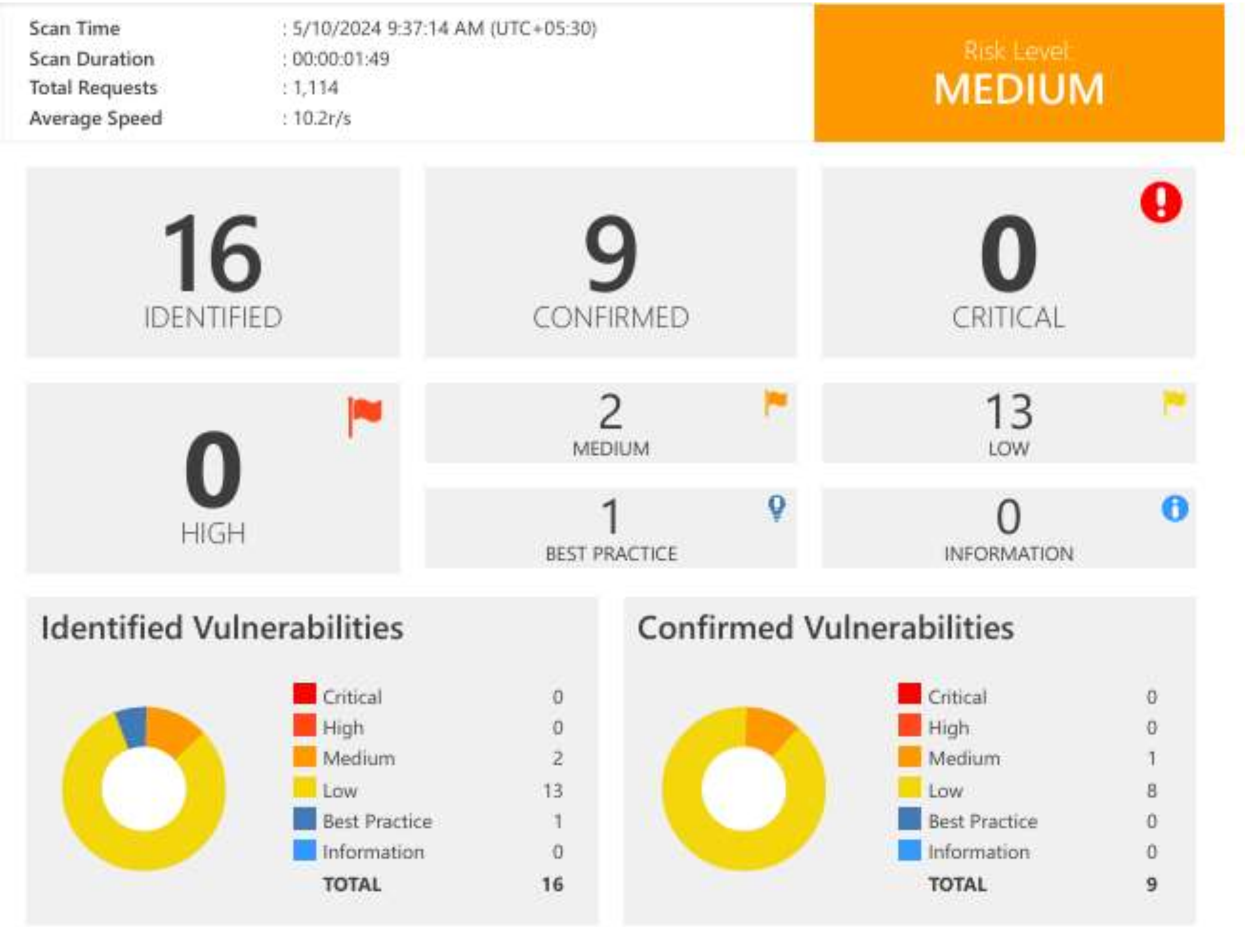


```
┌──(malith㉿kali)-[~]
└─$ wafw00f www.zabbix.com

                ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.zabbix.com
[+] The site https://www.zabbix.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```



```
┌──(malith㉿kali)-[~]
└─$ subfinder -d www.zabbix.com

                projectdiscovery.io

[INF] Loading provider config from /home/malith/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for www.zabbix.com
panic: runtime error: invalid memory address or nil pointer dereference
[signal SIGSEGV: segmentation violation code=0x1 addr=0x10 pc=0xd8fa75]

goroutine 81 [running]:
github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run.func1()
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:36 +0x255
created by github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run in goroutine 33
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:28 +0x10d
```

Vulnerabilities Found.



Scan Time	: 5/10/2024 9:37:14 AM (UTC+05:30)
Scan Duration	: 00:00:01:49
Total Requests	: 1,114
Average Speed	: 10.2r/s

Risk Level
MEDIUM

16 IDENTIFIED

9 CONFIRMED

0 CRITICAL

0 HIGH

2 MEDIUM

13 LOW

1 BEST PRACTICE

0 INFORMATION

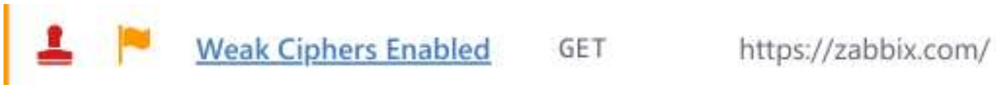
Identified Vulnerabilities

🟥	Critical	0
🟥	High	0
🟧	Medium	2
🟨	Low	13
🟦	Best Practice	1
🟦	Information	0
	TOTAL	16

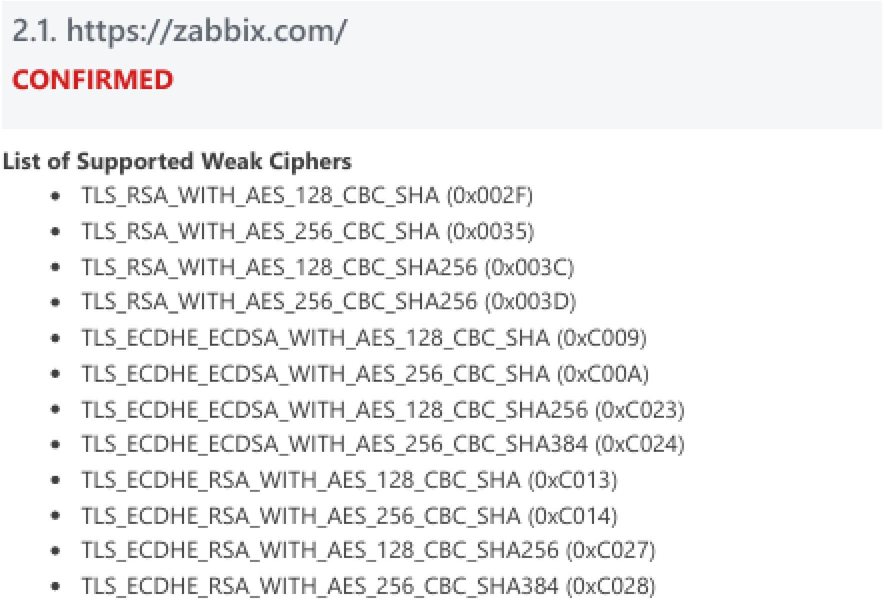
Confirmed Vulnerabilities

🟥	Critical	0
🟥	High	0
🟧	Medium	1
🟨	Low	8
🟦	Best Practice	0
🟦	Information	0
	TOTAL	9

Weak Ciphers Enabled



Weak Ciphers Enabled GET https://zabbix.com/



2.1. https://zabbix.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_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
- 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://zabbix.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

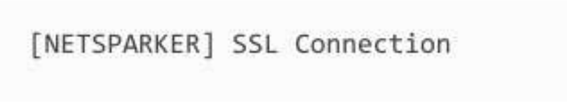
Under the OWASP category connected to poor Cipher Enabled vulnerabilities within the domain of **http://zabbix.com**/, various potential security threats have been found due to the usage of poor encryption protocols or ciphers. The impact of not addressing this vulnerability is considerable and includes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

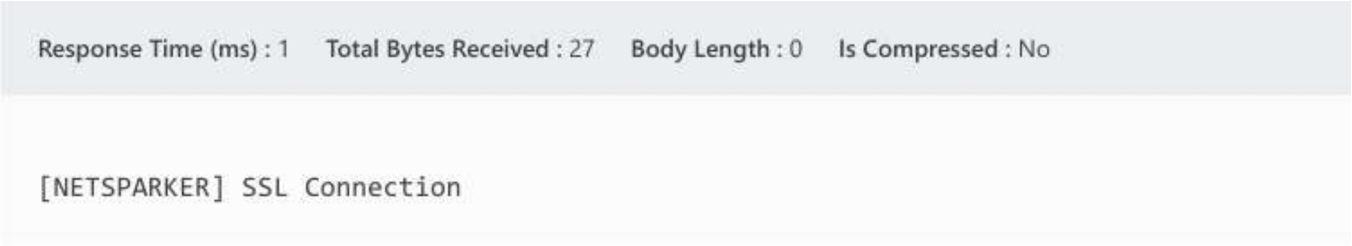
It is vital to fix this Weak Cipher Enabled issue swiftly by adopting strong encryption methods and ciphers. Failure to do so not only expose users to potential security concerns but also damages Starbucks' reputation, legal compliance, and general corporate integrity. The repercussions of the vulnerability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

- **Request**



```
[NETSPARKER] SSL Connection
```

- **Response**



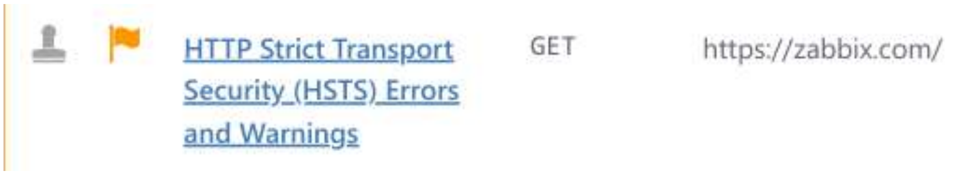
Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

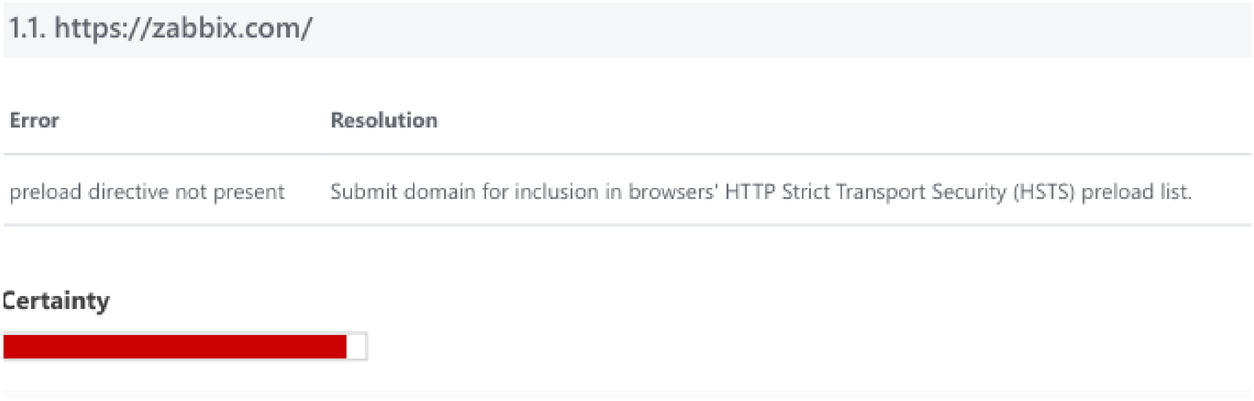
- **Remediation**

Configure your web server to disallow using weak ciphers.

HTTP Strict Transport Security (HSTS) Policy Not Enabled



HTTP Strict Transport Security (HSTS) Errors and Warnings | GET | https://zabbix.com/



1.1. https://zabbix.com/

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

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://zabbix.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.zabbix.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.

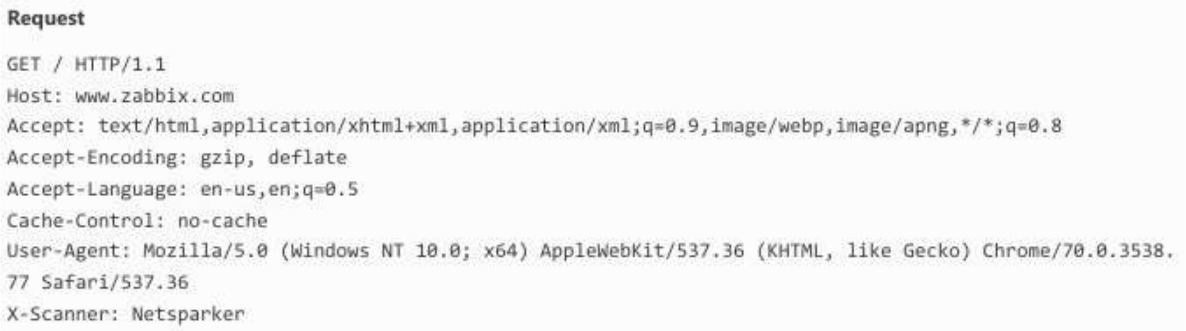
3. Phishing and Data Theft: By pretending to be www.echobox.com, cybercriminals may leverage this vulnerability to conduct phishing attacks and fool victims into disclosing sensitive information such login passwords, personal information, or bank account information. Financial losses and data theft may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

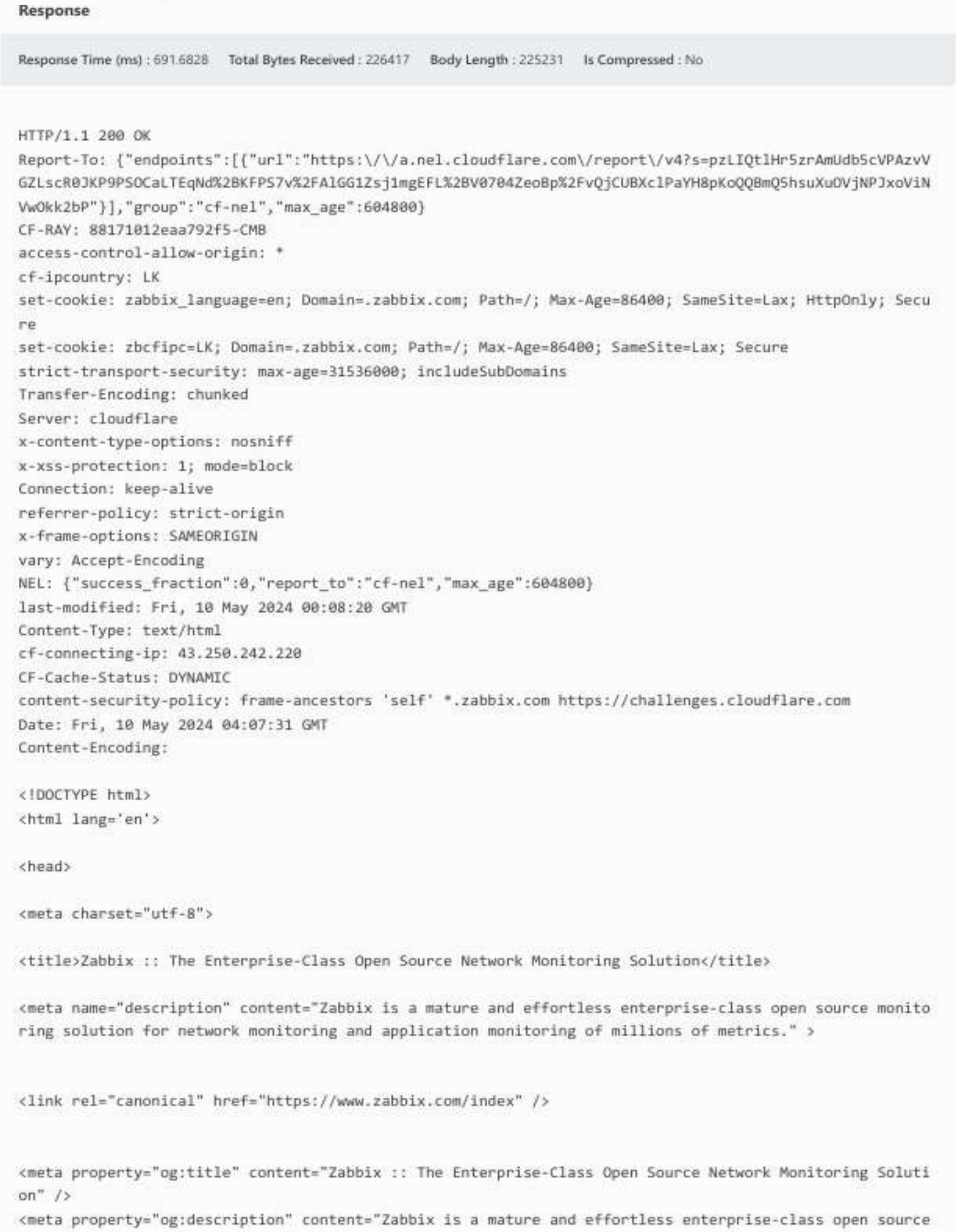
Turning on HSTS is essential to fixing this vulnerability. This security feature prevents downgrading attacks and improves overall security by guaranteeing that all communications with the website are encrypted and safe. Quick HSTS implementation can help the website comply with legal obligations, preserve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

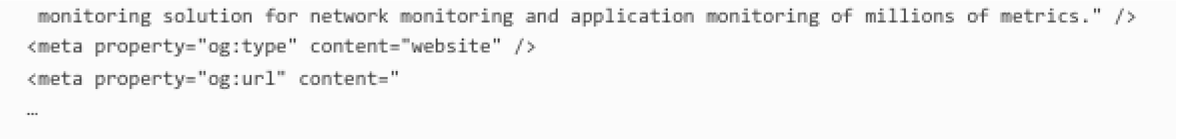
```
GET / HTTP/1.1
Host: www.zabbix.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```



Response

Response Time (ms) : 691.6828 Total Bytes Received : 226417 Body Length : 225231 Is Compressed : No

```
HTTP/1.1 200 OK
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=pzLIQtlHr5zrAmUdb5cVPAzvV
GZLscR0JKP9PSOCaLTEqNd%2BKFPS7v%2FAlGG1Zsj1mgEFL%2BV0704ZeoBp%2FvQjCUBXclPaYH8pKoQQBmQ5hsuXuOVjNPJxoViN
VwOkk2bP"}],"group":"cf-nel","max_age":604800}
CF-RAY: 88171012eaa792f5-CMB
access-control-allow-origin: *
cf-ipcountry: LK
set-cookie: zabbix_language=en; Domain=.zabbix.com; Path=/; Max-Age=86400; SameSite=Lax; HttpOnly; Secu
re
set-cookie: zbcfipc=LK; Domain=.zabbix.com; Path=/; Max-Age=86400; SameSite=Lax; Secure
strict-transport-security: max-age=31536000; includeSubDomains
Transfer-Encoding: chunked
Server: cloudflare
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
Connection: keep-alive
referrer-policy: strict-origin
x-frame-options: SAMEORIGIN
vary: Accept-Encoding
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
last-modified: Fri, 10 May 2024 00:08:20 GMT
Content-Type: text/html
cf-connecting-ip: 43.250.242.220
CF-Cache-Status: DYNAMIC
content-security-policy: frame-ancestors 'self' *.zabbix.com https://challenges.cloudflare.com
Date: Fri, 10 May 2024 04:07:31 GMT
Content-Encoding:

<!DOCTYPE html>
<html lang='en'>

<head>

<meta charset="utf-8">

<title>Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution</title>

<meta name="description" content="Zabbix is a mature and effortless enterprise-class open source monito
ring solution for network monitoring and application monitoring of millions of metrics." >


<link rel="canonical" href="https://www.zabbix.com/index" />


<meta property="og:title" content="Zabbix :: The Enterprise-Class Open Source Network Monitoring Soluti
on" />
<meta property="og:description" content="Zabbix is a mature and effortless enterprise-class open source
```

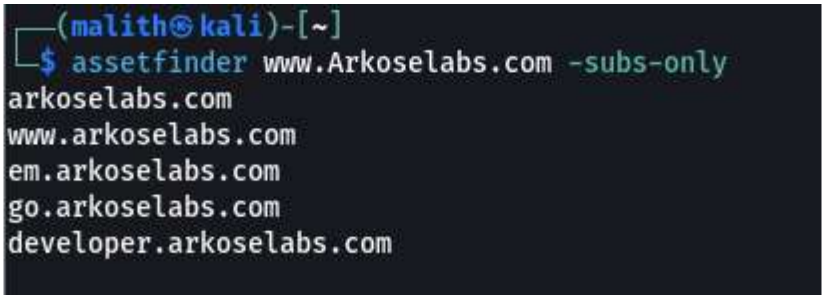


```
 monitoring solution for network monitoring and application monitoring of millions of metrics." />
<meta property="og:type" content="website" />
<meta property="og:url" content="
…
```

Bug Bounty 10 (Arkoselabs)

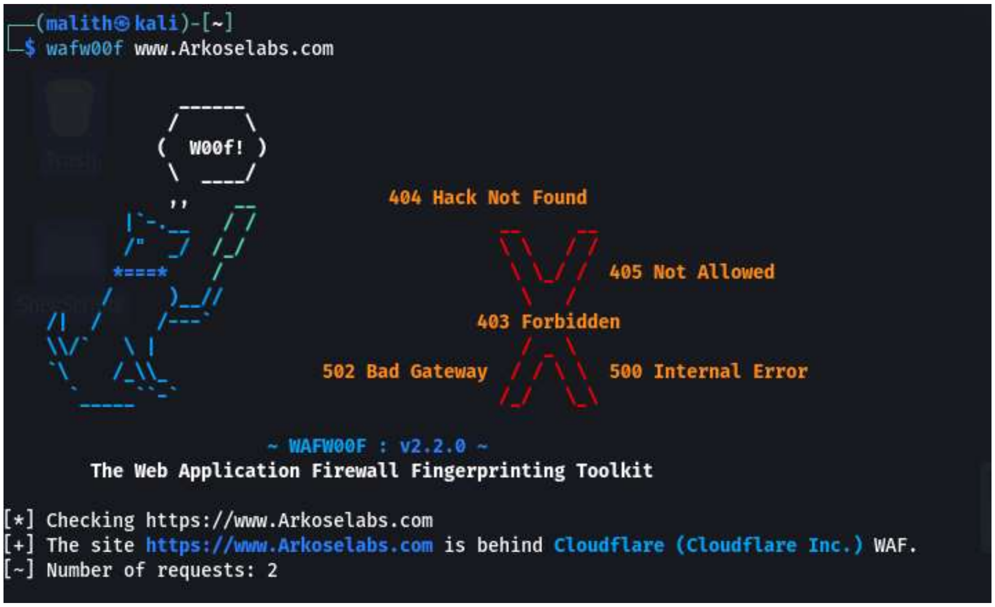
Reconnaissance

Firstly, I used the Assetfinder tool to find the subdomains of the Arkoselabs website. Assetfinder tool is used to find the subdomains of a website.

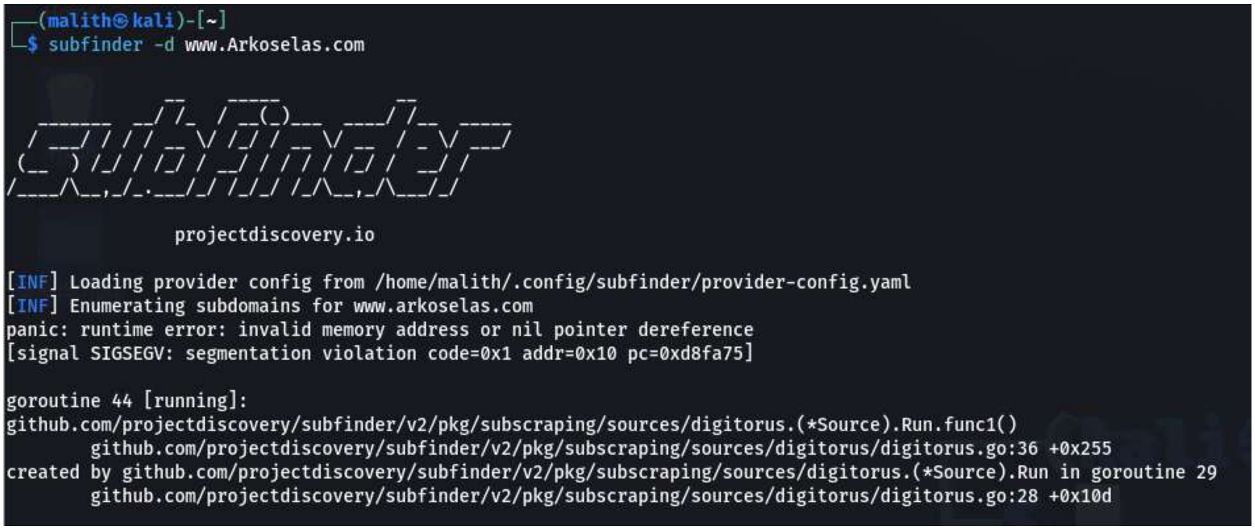


```
┌──(malith㉿kali)-[~]
└─$ assetfinder www.Arkoselabs.com -subs-only
arkoselabs.com
www.arkoselabs.com
em.arkoselabs.com
go.arkoselabs.com
developer.arkoselabs.com
```

Then, I got the subdomains list as below.

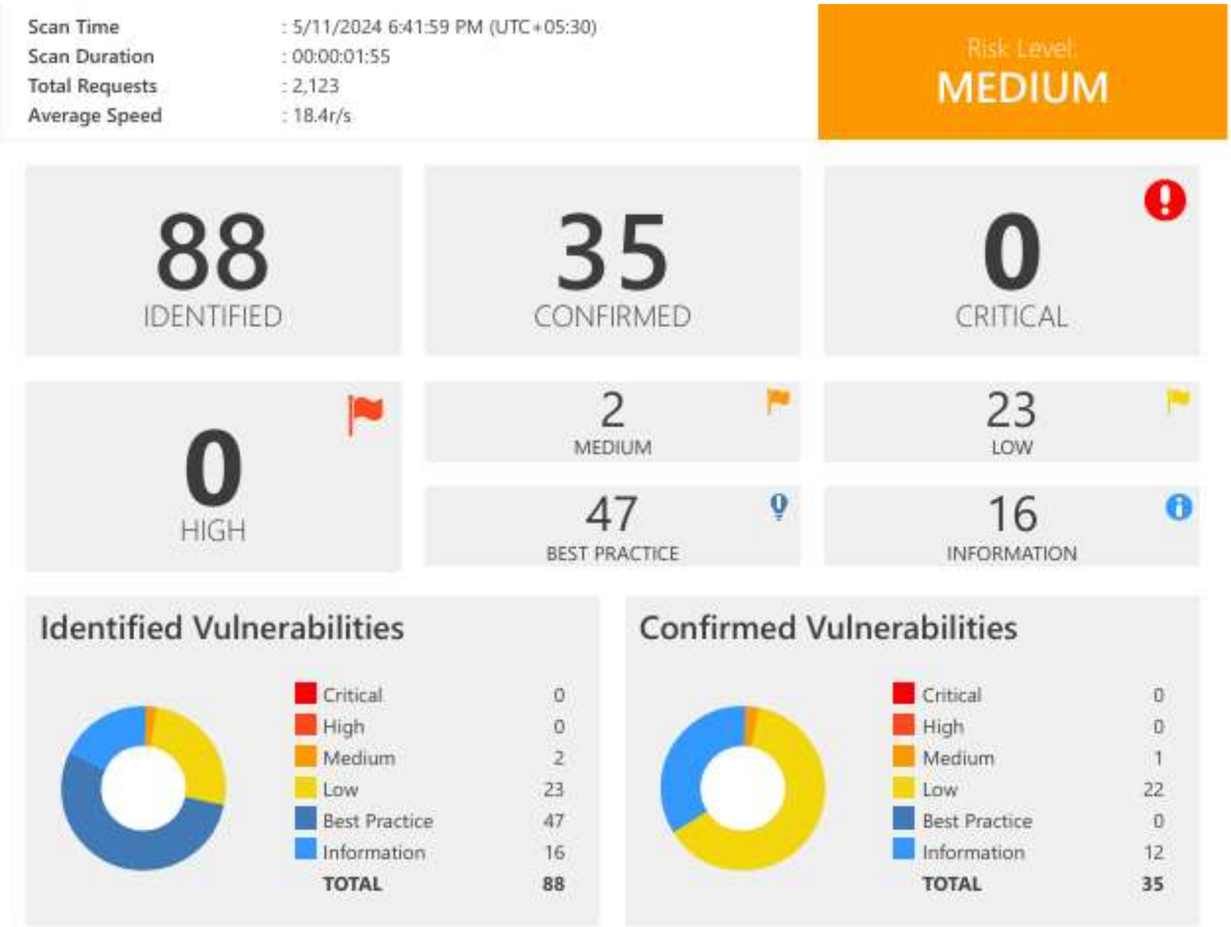


```
┌──(malith㉿kali)-[~]
└─$ wafw00f www.Arkoselabs.com

                ______
               /      \
              (  W00f! )
               \  ____/
               ,,    __            404 Hack Not Found
           |`-.__   / /                      __     __
           /"  _/  /_/                       \ \   / /         405 Not Allowed
          *===*    /                          \ \_/ /
         /        )__//                        \   /
    /|  /     /---`                        403 Forbidden
    \\/`    \ |                                / \
    `\    /_\\_                 502 Bad Gateway  / / \ \       500 Internal Error
      `_____``-`                              /_/   \_\

                        ~ WAFW00F : v2.2.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.Arkoselabs.com
[+] The site https://www.Arkoselabs.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```



```
┌──(malith㉿kali)-[~]
└─$ subfinder -d www.Arkoselas.com

               __    _____          __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Loading provider config from /home/malith/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for www.arkoselas.com
panic: runtime error: invalid memory address or nil pointer dereference
[signal SIGSEGV: segmentation violation code=0x1 addr=0x10 pc=0xd8fa75]

goroutine 44 [running]:
github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run.func1()
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:36 +0x255
created by github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus.(*Source).Run in goroutine 29
        github.com/projectdiscovery/subfinder/v2/pkg/subscraping/sources/digitorus/digitorus.go:28 +0x10d
```

Vulnerabilities Found.



Scan Time	: 5/11/2024 6:41:59 PM (UTC+05:30)
Scan Duration	: 00:00:01:55
Total Requests	: 2,123
Average Speed	: 18.4r/s

Risk Level: MEDIUM

88 IDENTIFIED	35 CONFIRMED	0 CRITICAL

0 HIGH	2 MEDIUM	23 LOW
	47 BEST PRACTICE	16 INFORMATION

Identified Vulnerabilities

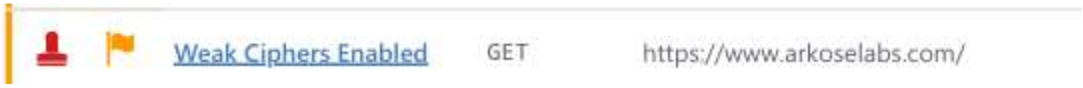
🟥 Critical	0
🟥 High	0
🟧 Medium	2
🟨 Low	23
🟦 Best Practice	47
🟦 Information	16
TOTAL	88

Confirmed Vulnerabilities

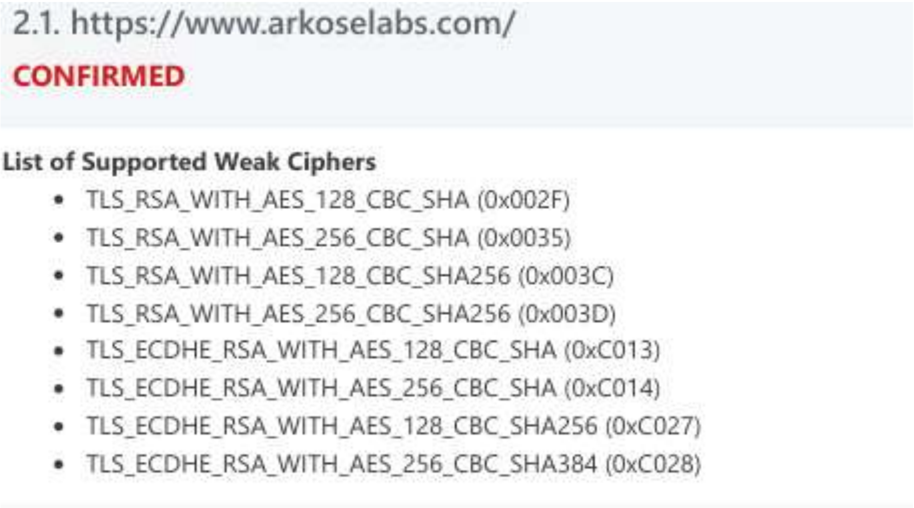
🟥 Critical	0
🟥 High	0
🟧 Medium	1
🟨 Low	22
🟦 Best Practice	0
🟦 Information	12
TOTAL	35

Vulnerability

Weak Ciphers Enabled



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



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

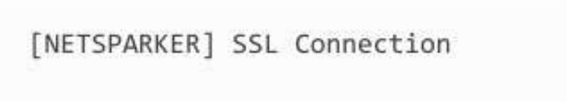
Under the OWASP category connected to poor Cipher Enabled vulnerabilities within the domain of **http://arkoselabs.com**/, various potential security threats have been found due to the usage of poor encryption protocols or ciphers. The impact of not addressing this vulnerability is considerable and includes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

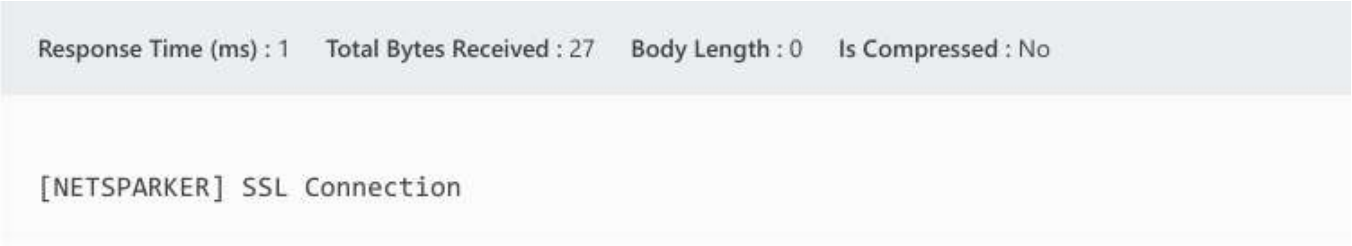
It is vital to fix this Weak Cipher Enabled issue swiftly by adopting strong encryption methods and ciphers. Failure to do so not only expose users to potential security concerns but also damages Starbucks' reputation, legal compliance, and general corporate integrity. The repercussions of the vulnerability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

- **Request**



```
[NETSPARKER] SSL Connection
```

- **Response**



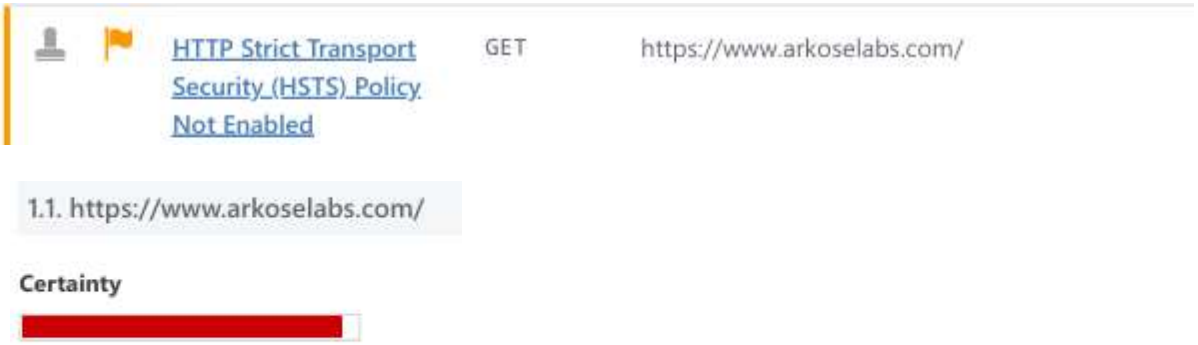
Response Time (ms) : 1   Total Bytes Received : 27   Body Length : 0   Is Compressed : No

```
[NETSPARKER] SSL Connection
```

- **Remediation**

Configure your web server to disallow using weak ciphers.

HTTP Strict Transport Security (HSTS) Policy Not Enabled


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

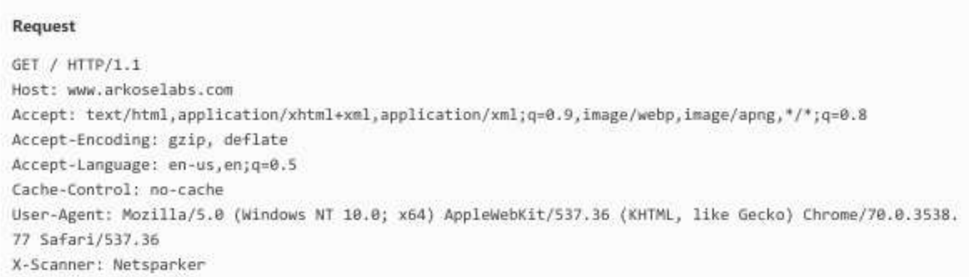
3. Phishing and Data Theft: By pretending to be www.echobox.com, cybercriminals may leverage this vulnerability to conduct phishing attacks and fool victims into disclosing sensitive information such login passwords, personal information, or bank account information. Financial losses and data theft may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

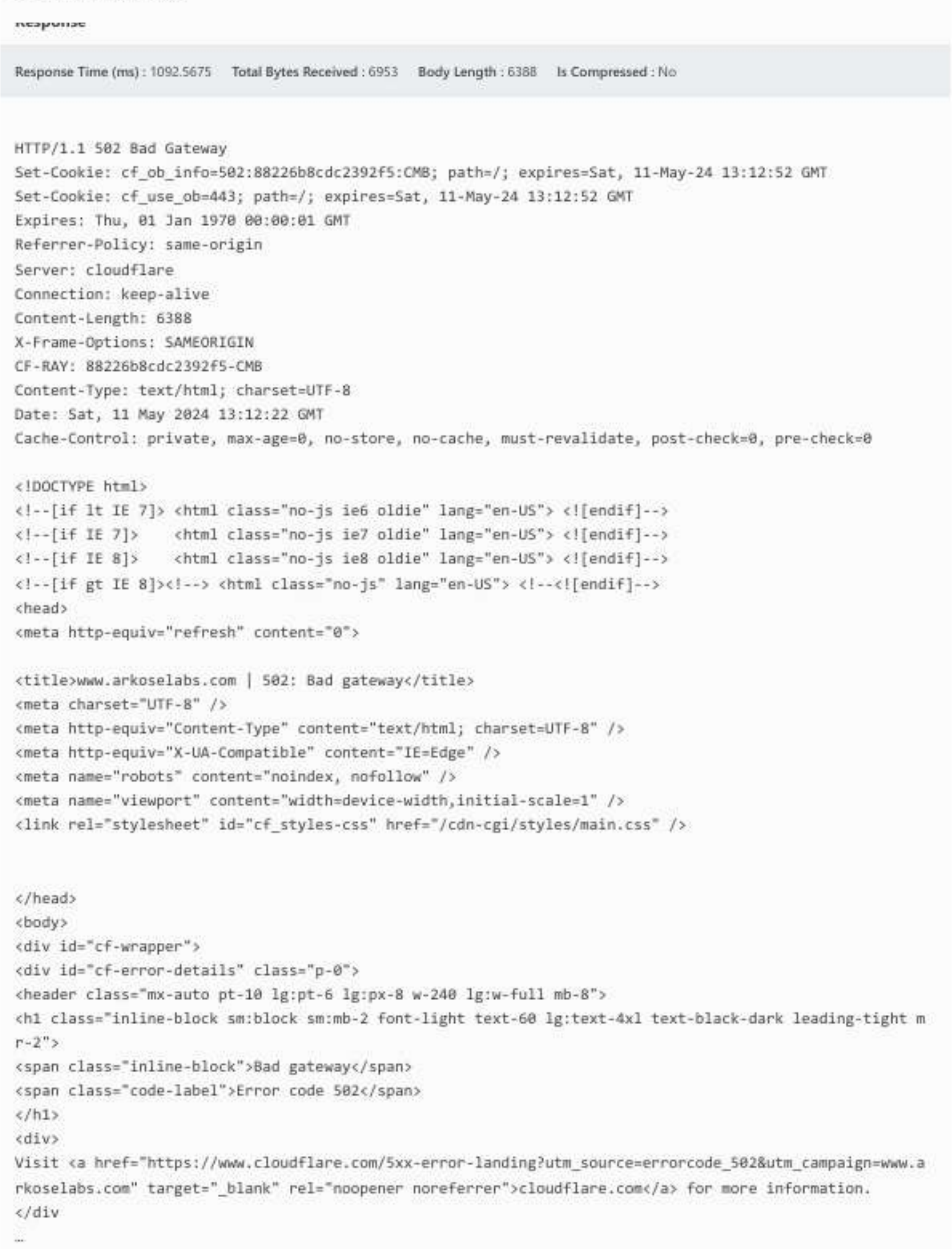
Turning on HSTS is essential to fixing this vulnerability. This security feature prevents downgrading attacks and improves overall security by guaranteeing that all communications with the website are encrypted and safe. Quick HSTS implementation can help the website comply with legal obligations, preserve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

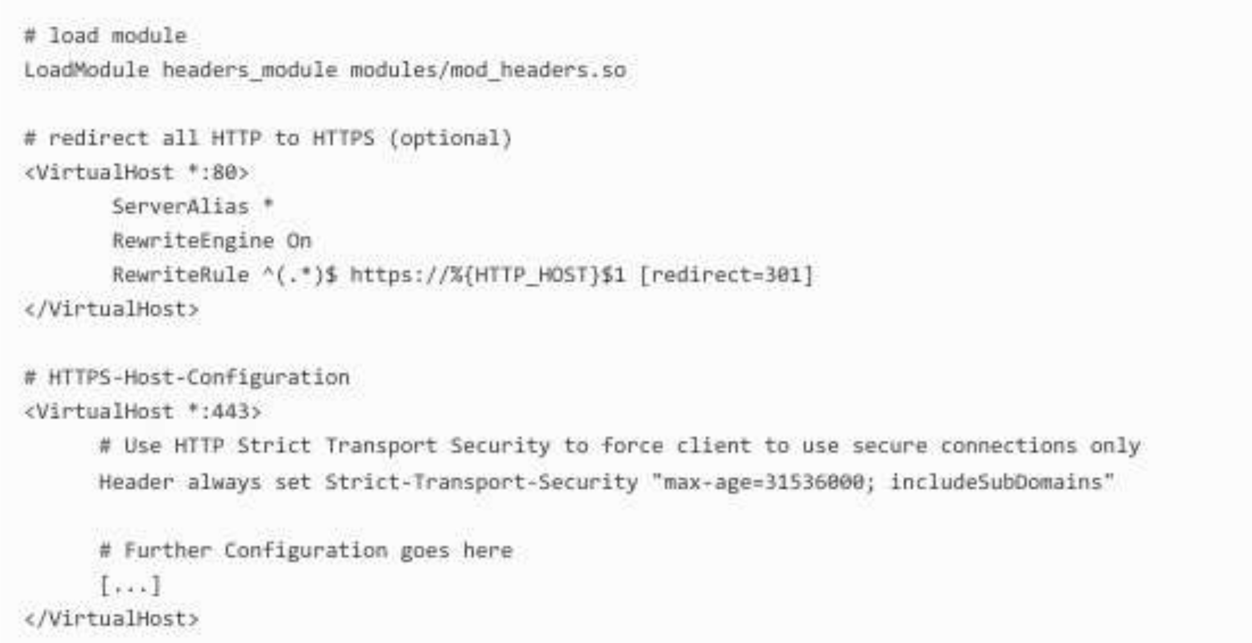


Response

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**



```
# 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>
```