Sri Lanka Institute of Information Technology

Web Audit

Individual Assignment

IE2062 – Web Security

Submitted by:

Student Registration Number	Student Name
IT21369506	Sumathipala LGHN

28/05/2023

Table of Contents

ACKNOWLEDGEMENT

Learning is not a simple task. People may say, learning is just only a task that gaining an understanding of the task with only the theoretical part of it. No it is not. Learning means theoretical part with the practice of that theory. To be a great person in a field like cyber security, the practice is a must for everyone in this field.

It was a new experience in this module as this gave us more practical knowledge than the theoretical knowledge with real world examples. In class we used real world software applications and examples in leaning this module. As it gave us a more interest in this subject module.

I would want to convey my heartfelt thanks to Dr. Lakmal Rupasinghe, the module's professor in charge, Ms. Chethana liyanapathirana, and the other additional assistant lecturers who assisted and advised in the completion of this project.

OBJECTIVE OF THIS AUDIT

The security audit on https://www.coca-colacompany.com/ is carried out in conjunction with this year's project provided for the second year second semester of the Web Security module. The goal of whole audit is to discover as many security flaws as achievable within the specified scope, label those based on the following exposure levels, as well as expose those by reporting them.

BREIF EXPLANTION TOP 10 OF OWASP

The Open Web Application Security Project which also known as OWAP is an important platform that creates widely accessible publications, techniques, reference, services, as well as technology in the subject of the security of web applications. Open and free assets will be provided by the OWASP. OWASP Foundation which is a profitless foundation manages this. OWASP includes over thirty-two thousand freely working individuals worldwide that do protection evaluations as well as for researching.

What is a Vulnerability? Vulnerabilities in software programs are common. There are unintended vulnerabilities or gaps in software systems that could be exploited in theory. For instance, there may be a flaw that allows a cybercriminal to access data that is otherwise safe.

These vulnerabilities are often sought by software programmers. When they find a vulnerability, they investigate it, develop a "fix" to address it, and then include the patch in a new version of the program. However, this is a time-consuming process. When a bug is discovered, hackers from all over the world will try to exploit it.

The OWASP Top - ten is indeed a generally acknowledged list which ranks those best ten cyber threats impacting online applications. Even if there are more than 10 security dangers in applications, the goal of the OWASP List of top is to ensure ethical hackers knowledgeable along with at minimum a more significant security threats as well as teach individuals importance of being able protect over threats. This list will be updated eventually year by year. By visiting this site https://owasp.org/www-project-top-ten/ we can observe the list updated frequently.

As this is an audit in 2021, the top ten list of OWASP can be shown as below:

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Login and Monitoring Failures
10. Server-Side Request Forgery

This is a comparison of year 2017 and 2021.

2017	2021
A01:2017-Injection	A01:2021-Broken Access Control
A02:2017-Broken Authentication	A02:2021-Cryptographic Failures
A03:2017-Sensitive data Exposure	A03:2021-Injection
A04:2017-XML External Entities(XXE)	A04:2021-Insecure Design
A05:2017-Broken Access Control	A05:2021-Security Misconfiguration
A06:2017-Security Misconfiguration	A06:2021-Vulnerable and Outdated Components
A07:2017-Cross-Site Scripting(XSS)	A07:2021-Identification and Authentication Failures
A08:2017-Insecure Deserialization	A08:2021-Software and Data Integrity Failures
A09:2017-Using Components with known Vulnerabilities	A09:2021-Security Login and Monitoring Failures
A10:2017-Insuffient Logging & Monitoring	A10:2021-Server-Side Request Forgery

Now let's discuss about each threat individually in year 2021.

1. **Broken Access Control**

   Access control maintains rules and regulation by preventing individuals from acting further than the scope of given authorized privileges. Modification or destruction and Information disclosure will happen due to failures in Authentication. Down below are some of the vulnerabilities

   - Accessibility can only be provided for certain skills, roles, or individuals, and yet is open to anybody, in breach of the concept of lowest privilege or refuse as definition.
   - Circumventing checks in access control via changing the URL's inner functionality or rather the HTML webpage, or by manipulating API calls with an exploit toolkit.
   - Allowing anybody else's profile to be viewed or edited by giving its personally identifiable information.
   - Get into API's which there are no access control. Such as DELETE, PUT and POST.
   - As an unauthorized person, push surfing to authorized sites or protected resources as just a regular User of the System.

2. **Cryptographic Failures**

   To discover the security requirements for data carriage and still data must be protected as the at the very beginning. As Examples, passwords, health details, credit card details, personal information of an individual, secrets in a business can be listed down.

   - Leak of confidential data is the main effect of this flaw.

3. **Injection**

   Whenever users enter data that is handled by the client, the software interprets it as actual instructions / variables, resulting in an injection vulnerability. The above kind of

assaults are rather prevalent. Such that, it's indeed completely reliant on the technology involved and how it evaluates input from the user.

These are some of the common injection attacks:

- Command Injection
- SQL Injection

4. Insecure Design

Insecure design is a broad phrase that refers to a wide range of faults and is described as "control design that is either lacking or insufficient." Even if a design is secure, implementing flaws might guide towards security flaws. Insecure design can be fixed perfectly because they are not designed with security controls which are need to protect again specific type of attacks. Another aspect that contributes to unsafe design is the absence of commercial level of risk implicit in the system or application could be created, and therefore the breakdown to decide what type of security architecture is necessary.

5. Security Misconfiguration

Whenever protection setups really aren't handled correctly, misconfigurations arise. Some of the misconfigurations are:

- Whenever there are unchanged passwords and usernames of the profile which I given as the defaults. such as Username as admin and password as admin123.
- Whenever pages, Services, privileges and accounts are enabled that are not required.
- Cloud platform permissions, for example S3 buckets, are inadequately set.
- When the unsecured headers are being used(HTTP)
- Glitches that are descriptive enough to enable a hacker to gather more knowledge of the target platform.

6. Vulnerable and Outdated Components

Unless the fundamental applications used on the website are old, there is a good possibility of discovering a well-known security flaws which may be exploited to obtain to break into the system. As a result, as a malicious actor, someone should perform extremely simple tasks. But now it has been come to the top of the list more than it was used to be.

7. Identification and Authentication Failures

In Modern Web applications, a great role of work is done by the User itself. If a security vulnerability in authentication process is found by the Malicious Actor, that individual has the authority to operate as a legitimate system user. To guard from user identification threats, it is essential to ascertain the identity of the user, authenticate this person, and maintain this process. Here are some of the examples for this:

- In a situation like if the malicious has a list of credentials of the users, then he/she can perform a credential stuffing which is an automated attack.
- The malicious actor can attack with a brute force.
- It is very easy to attack when users use the default password given by the system. For example, username as “admin” and password as “admin123.”
- When there are cryptographic failures like using weak algorithms and saves password as plain texts.
- When there is no multi-factor authentication process
- After a successful authentication, using again the session identifier.

8. Software and Data Integrity Failures

Breakdowns in data and software integrity can caused by executable as well as infrastructure which don't even defend from integrity breaches. Security breach, malicious programs, or compromise of the system can all occur as a result of an unsafe CI/CD pipelines. Insecure deserialization occurs when objects or content are encrypted or converted around an architecture which a malicious actor may view as well as alter.

9. Security Login and Monitoring Failures

The above aids in the detection, escalation, and response to ongoing intrusions. The breakdowns cannot be identified without this monitoring and logging. Whenever web technologies are created, the activities of the users must be recorded. So attackers recorded can be tracked because of this as a help. When there are no logging mechanisms in the system it is hard to detect the attackers when they logged into the system. This happens when:

- Logins, unsuccessful logins, and elevated transactions are not reported as verifiable events.
- Cautions as well as faults create no, insufficient, or ambiguous log records.
- App as well as API records aren't really checked regarding unusual behavior.
- During real-time or near real-time, this same program neither identify, escalate, and perhaps even notify for ongoing threats.
- When there are penetration tastings or dynamic scans the system do not alert.

10. Server-Side Request Forgery

That whenever a web service fetches a distant service without verifying the consumer URL, a SSRF vulnerability occurs. It enables an attacker to force a program to submit a constructed query to an undesired location, even if it is guarded either by firewall, a form of network access control list which we call in shorted form as ACL or VPN. Fetching a URL is now more regular as every web programs gives the individual features which are more comfortable with. Because of cloud services and architectural complexity, the intensity of SSRF is increasing. And also, the prevalence of SSRF is rising.

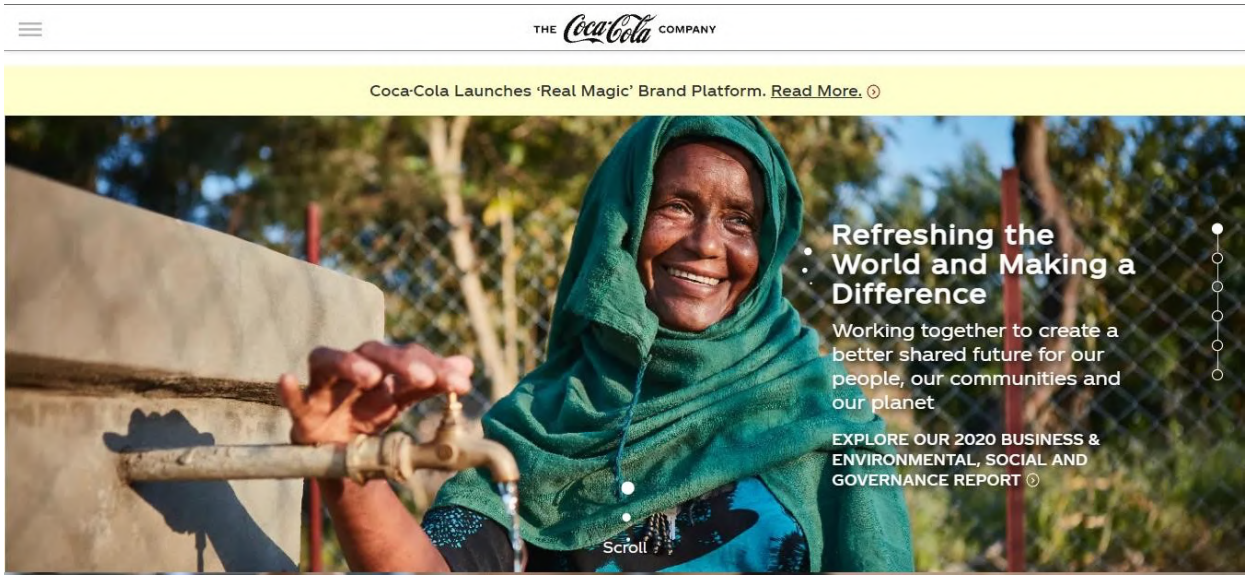
RISK SERVERITY RATING

To help you better determine which hazards need to be corrected, Netsparker classifies them using the risk points in its scans and reports. There are four levels of risk:

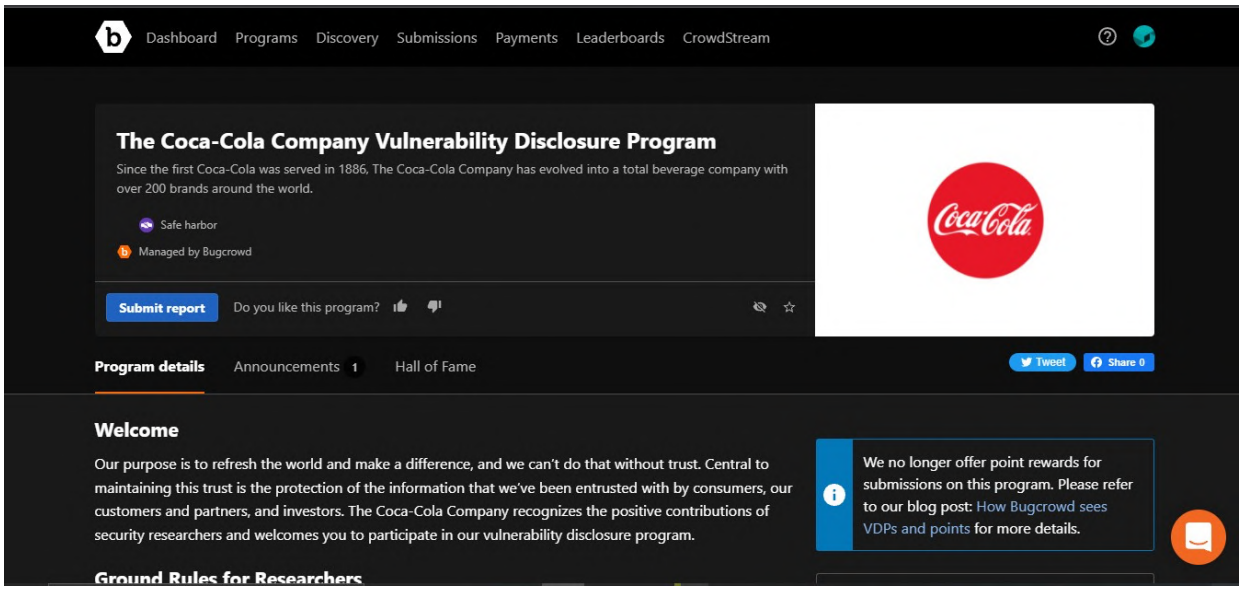
CRITICAL 	This represents the critical security level of the risk level. Critical Severity vulnerabilities may let hackers or the malicious actor to install and run mostly on web service or application server or gain confidential material.
HIGH 	This represents the high security level of the risk level. Cyber hackers may be able to get access to program data and resources if the problems are rated as High Severity. The distinction among Critical & High Severity vulnerabilities seems to be that a hostile hacker cannot execute code or an instruction on the program or server upon a High Severity flaw.
MEDIUM 	This represents the medium security level of the risk level. Medium Severity problems are typically caused by mistakes as well as inadequacies inside this process of recognition. Cyber hackers can get access to confidential information on the program or server by attempting to exploit various security flaws.
LOW 	This represents the low security level of the risk level. Leakage of information, setup problems, and an absence of certain safety precautions are among the Low Severity concerns. These could be coupled with additional concerns of a greater severity level, as well as this would be used in dealing with social manipulation (coercing individuals into doing certain activities or disclosing significant data) to have a more serious effect mostly on targeted..

ABOUT THE TARGET

The Coca-Cola Company (https://www.coca-colacompany.com/) is a worldwide beverages business based in Atlanta, Georgia that was founded under Delaware's General Corporation Law. The Coca-Cola Company is involved in the production, selling, and advertising several non - alcoholic beverage extracts and syrups, as well as alcoholic drinks.

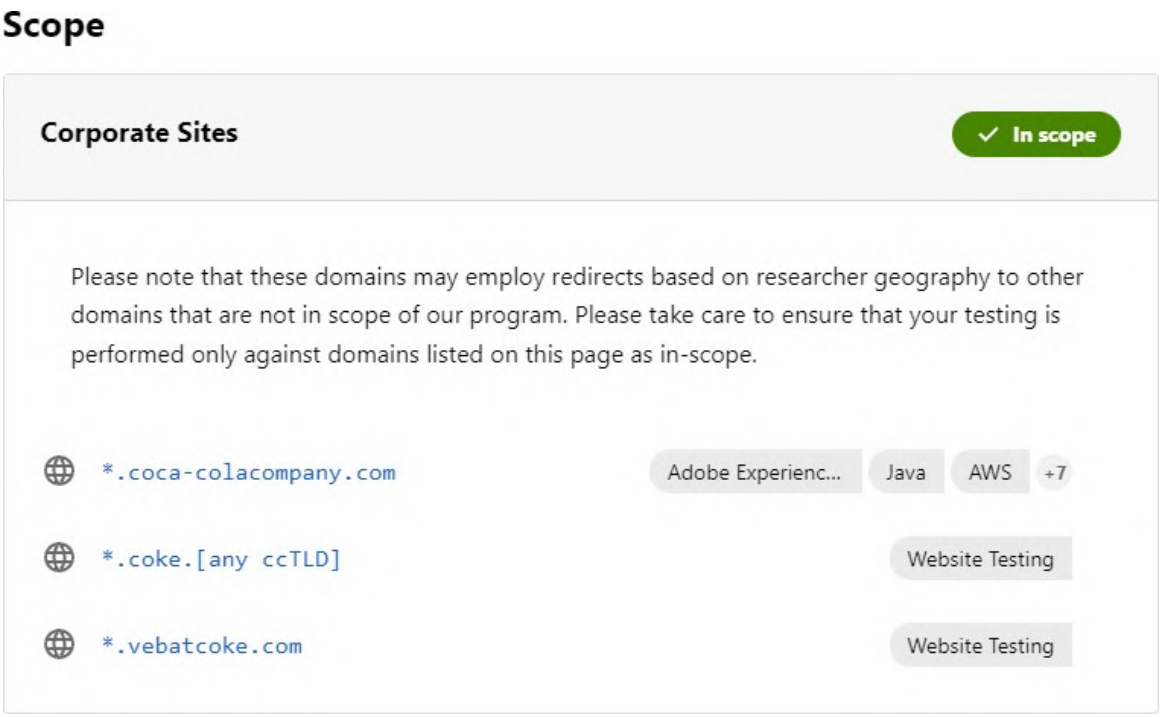


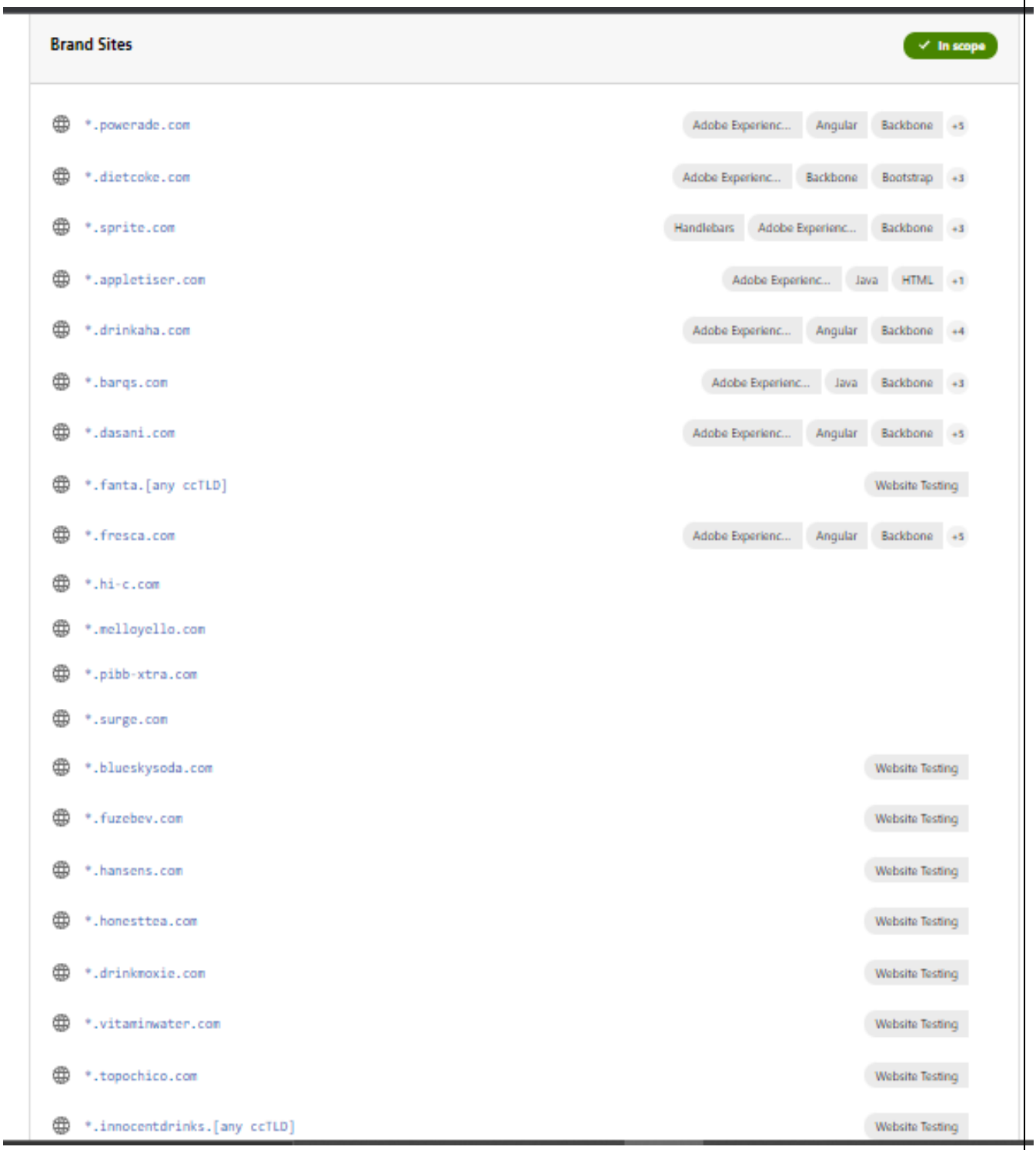
As the expectation of finding vulnerabilities of their system, they have launched a bug bounty program in the Bugcrowd Platform (https://bugcrowd.com/coca-cola).



SCOPES OF THIS ASSESMENT

The scopes of this are given as down below according to https://bugcrowd.com/coca-cola .




Brand Sites
In scope
*.powerade.com
Adobe Experienc...
Angular
Backbone
+5
*.dietcoke.com
Adobe Experienc...
Backbone
Bootstrap
+3
*.sprite.com
Handlebars
Adobe Experienc...
Backbone
+3
*.appletiser.com
Adobe Experienc...
Java
HTML
+1
*.drinkaha.com
Adobe Experienc...
Angular
Backbone
+4
*.barqs.com
Adobe Experienc...
Java
Backbone
+3
*.dasani.com
Adobe Experienc...
Angular
Backbone
+5
*.fanta.[any ccTLD]
Website Testing
*.fresca.com
Adobe Experienc...
Angular
Backbone
+5
*.hi-c.com
*.melloyello.com
*.pibb-xtra.com
*.surge.com
*.blueskysoda.com
Website Testing
*.fuzebev.com
Website Testing
*.hansens.com
Website Testing
*.honesttea.com
Website Testing
*.drinkmoxie.com
Website Testing
*.vitaminwater.com
Website Testing
*.topochico.com
Website Testing
*.innocentdrinks.[any ccTLD]
Website Testing

Supporting Sites

✓ In scope

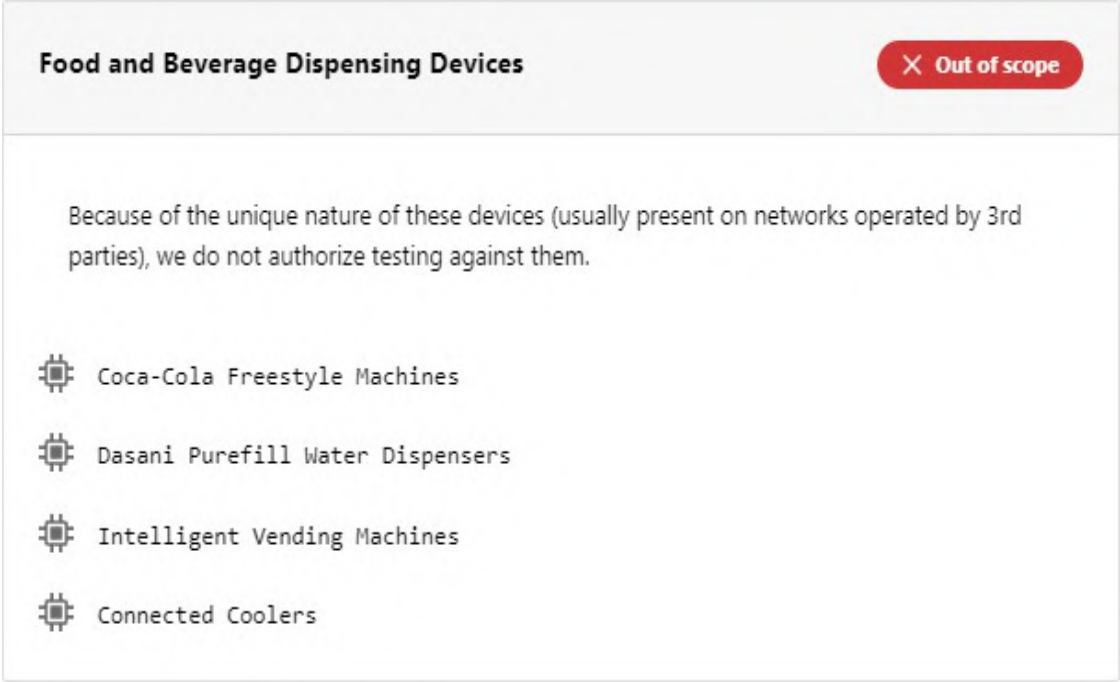
The websites in this target group serve intermediate functions that drive our larger environment such as performing redirection, hosting static assets, etc. If you spend time testing our other sites, you will likely encounter these domains.

Please note that these domains may employ redirects to other domains that are not in scope of our program, especially on *.cokeurl.com. Testing is only authorized for domains explicitly listed on this page. Additionally, where basic authentication is encountered, please do not attempt to brute force these prompts.

*.ko.com	
*.cokeurl.com	
*.tccc-aem.com	Website Testing
*.testko.com	

OUT OF SCOPE

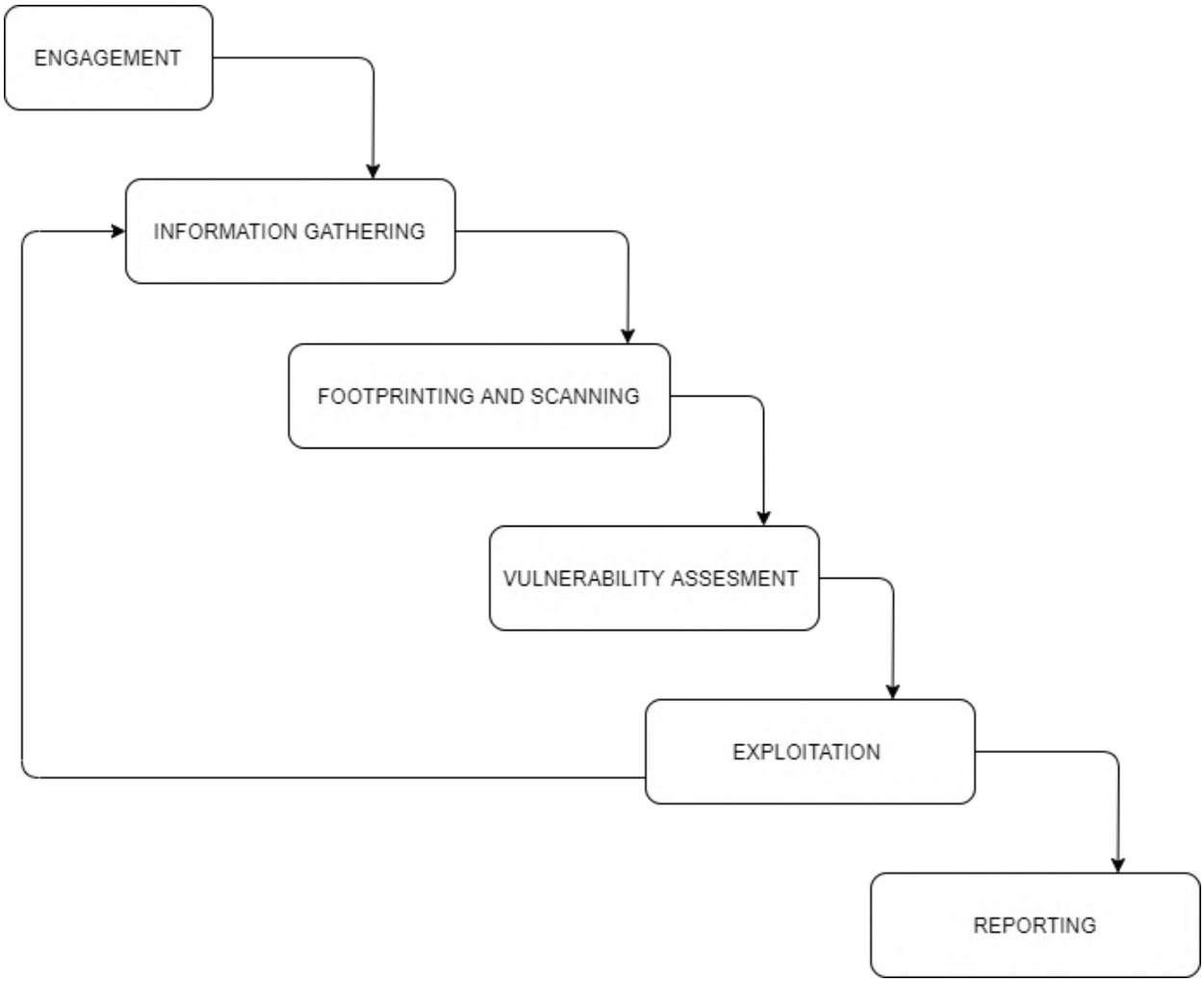
These are the OUT OF SCOPES given in https://bugcrowd.com/coca-cola.



- Coca-Cola Freestyle Machines
- iotDasani Purefill Water Dispensers
- iotIntelligent Vending Machines
- iotConnected Coolers

ASSESMENT METHOLOGY

There are proper steps to follow when conducting a risk assessment or penetration test to get the maximum benefit. Otherwise, the examiner will end up with confusing results and return critical flaws. This assessment is based on the standard procedure of a professional penetration test.

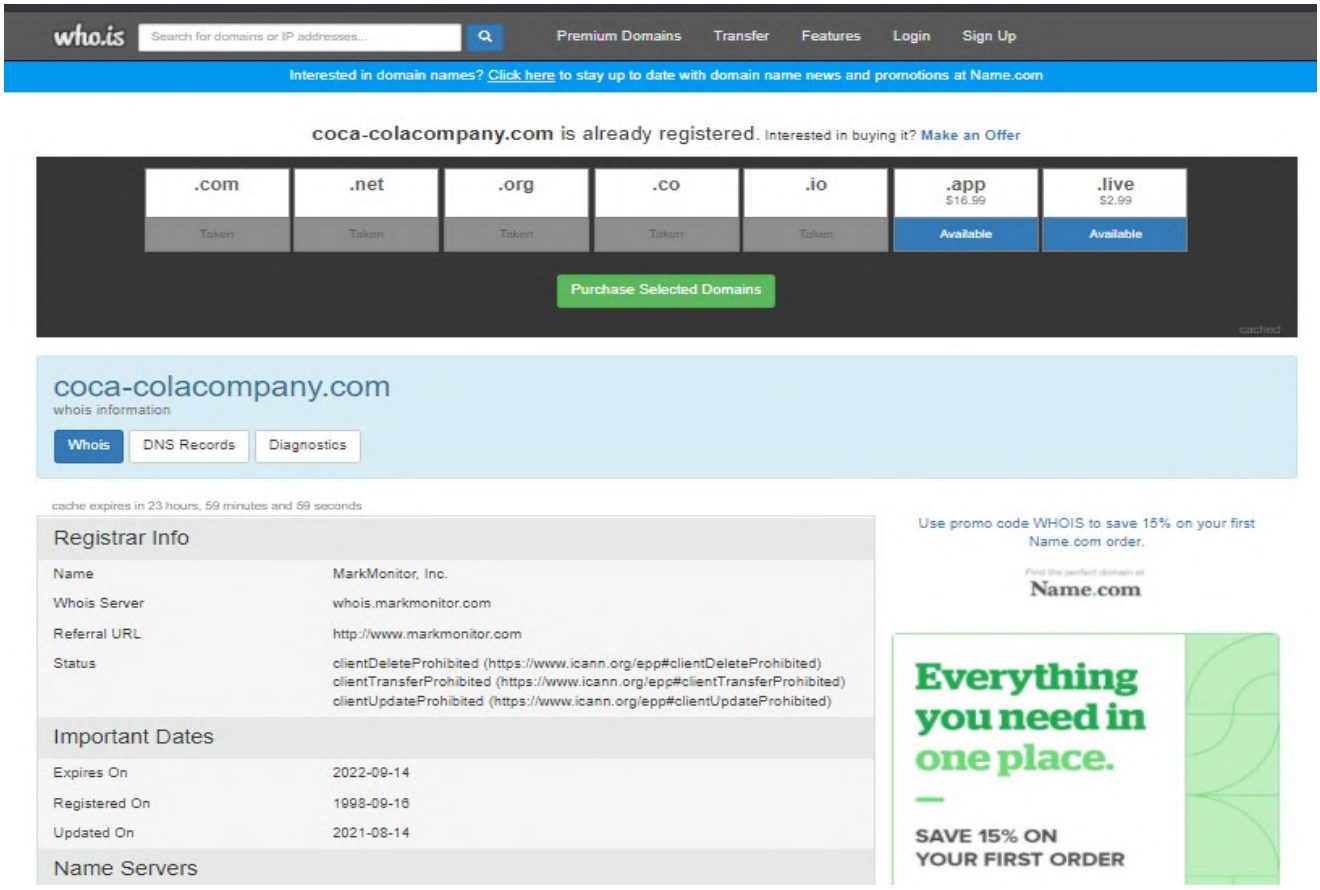


INFORMATION GATHERING

The process of acquiring various types of facts towards the intended victim or system is known as information gathering. That would be an essential and influential step to be done by security researchers or malicious actors (either white hat or black hat) as the first procedure or maybe even the initial stage of Ethical Hacking. The further details you know regarding the actual objective, the further likely individuals are to receive outcomes that are appropriate. Collection of information is more than just a step inside the secure inspection process. To acquire a deeper understanding of penetration testing, each researcher (pen tester) and attacker must learn this technique. The above phase is required though you might require whatever details during attacking whatever victim.

Target Validation

Methods for ongoing data security checking that confirm the presence of flaws. remote access testing, social engineering, penetration testing, physical security testing and Password cracking, are some of the techniques used. In here I have used Whois (https://who.is/) for this.



Subdomain Hunting

Calculating subdomains is an important element of a website risk assessment. The procedure of discovering sub-domains for one single or multiple domains is known as sub-domain hunting. Sub-domain hunting can disclose a large number of domains/sub-domains which are in coverage of an audit program, increasing the likelihood of detecting errors. Discovering apps operating on buried, abandoned sub-domains might help in the identification of serious flaws. Having similar flaws are frequently found in multiple domains/applications of a certain business.

1. Sublist3r

Sublist3r is indeed a Python program that uses OSINT to start listing website subdomains. This assists ethical hackers and fault researchers in collecting as well as gathering subdomains for the domain being targeted. Sublist3r searches for subdomains on Google, Yahoo, Bing, Baidu, and Ask. Virustotal, DNSdumpster, Netcraft, ReverseDNS and ThreatCrowd, are also used by Sublist3r to identify subdomains. As this is not a preinstalled tool, we have to install this tool manually. According to this website https://github.com/aboul3la/Sublist3r we need a python version of 2.7 or 3. Subbrute was merged using Sublist3r to boost overall chances of brute forcing additional subdomains with a better set of words.

We can use the given command to install the tool via terminal.

git clone https://github.com/aboul3la/Sublist3r.git.

First of all, we need to go the Sublist3r directory

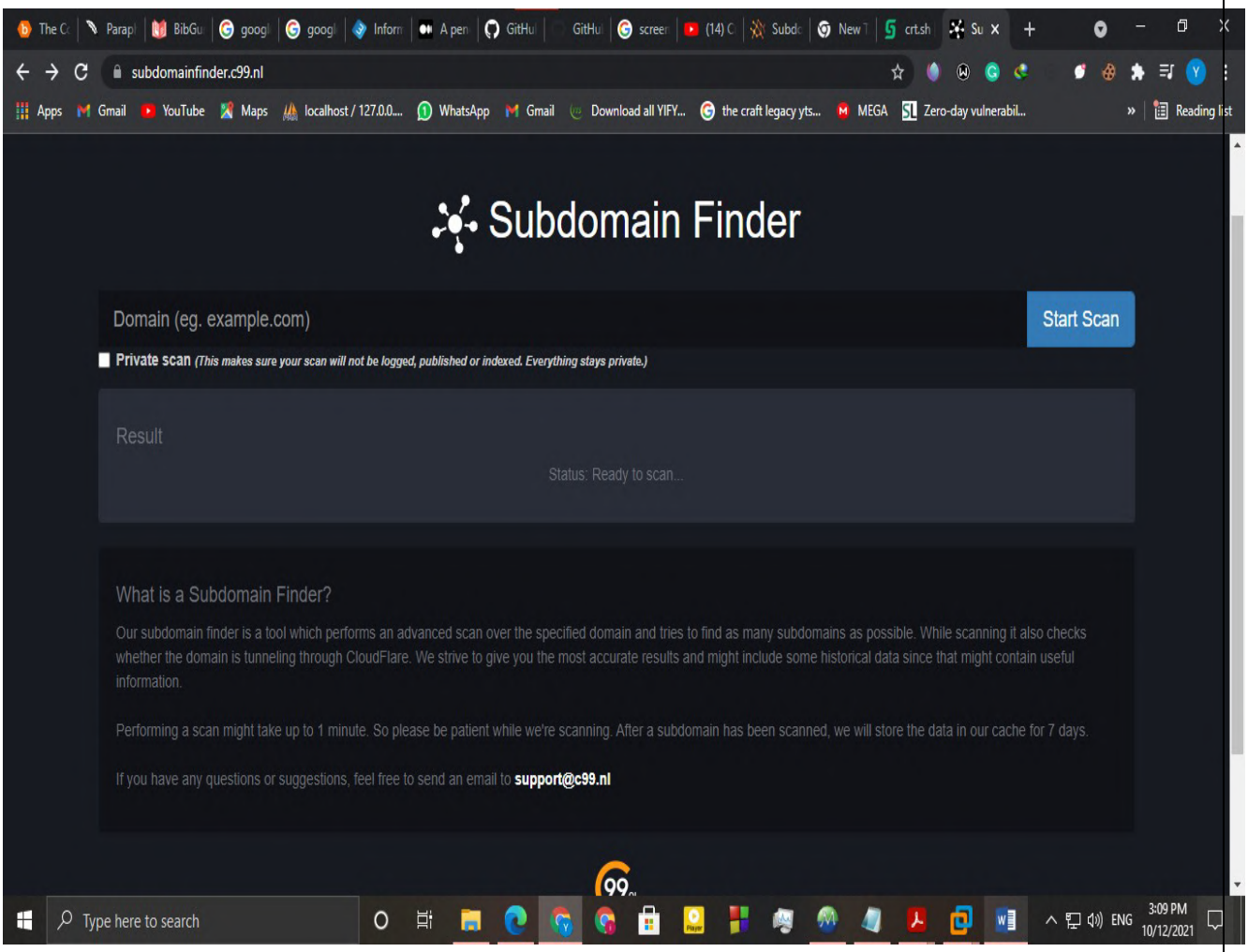
```
┌──(yasitha㉿kali)-[~]
└─$ cd Sublist3r

┌──(yasitha㉿kali)-[~/Sublist3r]
└─$ python3 sublist3r.py -d coca-colacompany.com

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for coca-colacompany.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 25
```

Sublist3r found only 25 unique subdomains from https://www.coca-colacompany.com/. They are given down below.

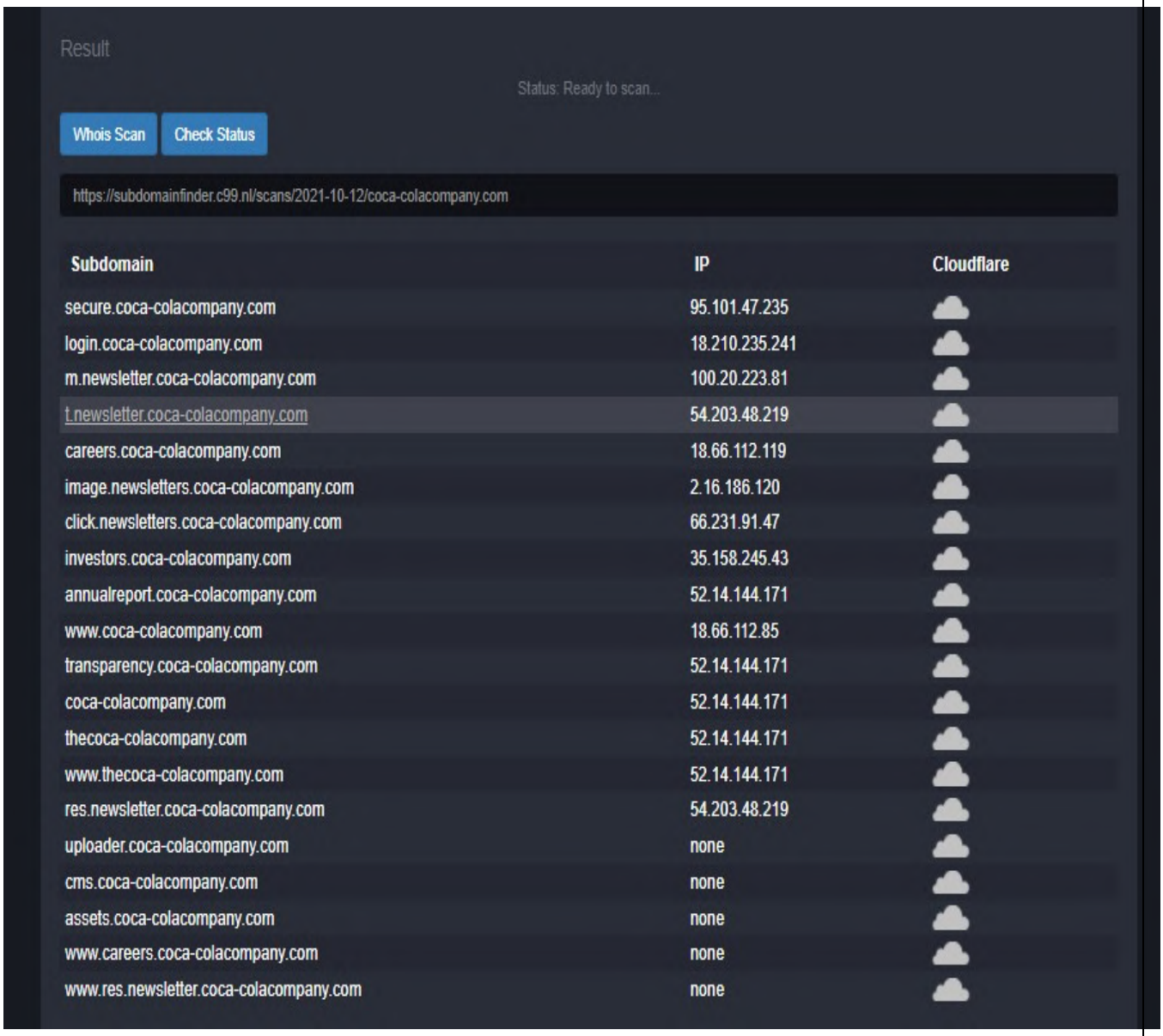
```
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 25
www.coca-colacompany.com
annualreport.coca-colacompany.com
assets.coca-colacompany.com
careers.coca-colacompany.com
www.careers.coca-colacompany.com
cms.coca-colacompany.com
investors.coca-colacompany.com
login.coca-colacompany.com
newsletter.coca-colacompany.com
m.newsletter.coca-colacompany.com
r171.newsletter.coca-colacompany.com
r172.newsletter.coca-colacompany.com
r173.newsletter.coca-colacompany.com
r174.newsletter.coca-colacompany.com
res.newsletter.coca-colacompany.com
www.res.newsletter.coca-colacompany.com
t.newsletter.coca-colacompany.com
click.newsletters.coca-colacompany.com
image.newsletters.coca-colacompany.com
mta.newsletters.coca-colacompany.com
secure.coca-colacompany.com
transparency.coca-colacompany.com
uploader.coca-colacompany.com
thecoca-colacompany.com
www.thecoca-colacompany.com
```

2. Online Subdomain Finder

The C99.nl subdomain finder (https://subdomainfinder.c99.nl/) is an utility that does an extensive scanning of a given domain in the hopes of discovering as much of it subdomains as achievable. During the scan, it looks to see if the domain is using Cloudflare to tunnel traffic. This aims to have a more consistent readings possible, and it may incorporate past data if it has useful insights.



These are the results found through the scan.

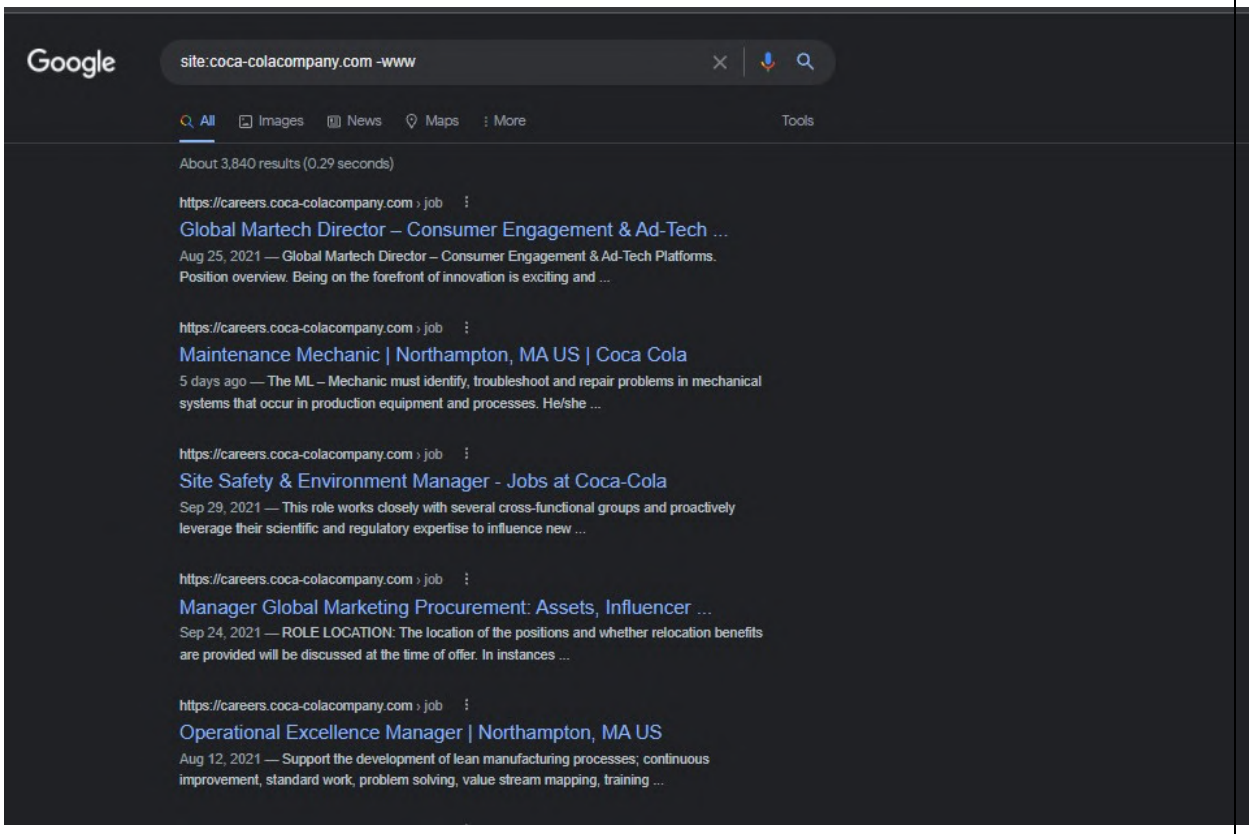


Subdomain	IP	Cloudflare
secure.coca-colacompany.com	95.101.47.235	
login.coca-colacompany.com	18.210.235.241	
m.newsletter.coca-colacompany.com	100.20.223.81	
t.newsletter.coca-colacompany.com	54.203.48.219	
careers.coca-colacompany.com	18.66.112.119	
image.newsletters.coca-colacompany.com	2.16.186.120	
click.newsletters.coca-colacompany.com	66.231.91.47	
investors.coca-colacompany.com	35.158.245.43	
annualreport.coca-colacompany.com	52.14.144.171	
www.coca-colacompany.com	18.66.112.85	
transparency.coca-colacompany.com	52.14.144.171	
coca-colacompany.com	52.14.144.171	
thecoca-colacompany.com	52.14.144.171	
www.thecoca-colacompany.com	52.14.144.171	
res.newsletter.coca-colacompany.com	54.203.48.219	
uploader.coca-colacompany.com	none	
cms.coca-colacompany.com	none	
assets.coca-colacompany.com	none	
www.careers.coca-colacompany.com	none	
www.res.newsletter.coca-colacompany.com	none	

3. Google Searching Method(Google-Fu)

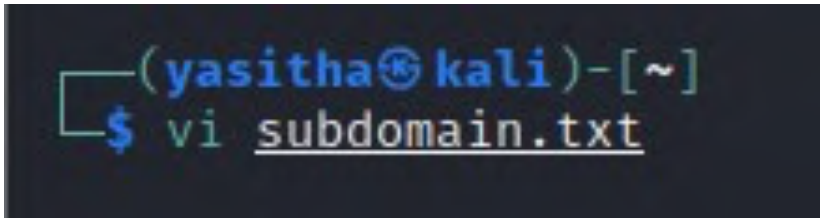
Google-Fu refers to the ability to use the Google search engine. It may be used to discover a great deal of knowledge about a particular domain.

site:coca-colacompany.com -www



Alive Subdomain finding

Here we have to sore all the subdomains found during the scan in a text file



Now we have to filter the alive subdomains from the domains in the text file. To do that we have to install httprobe tool through https://github.com/tomnomnom/httprobe . I am going to use the code given below to do it using httprobe tool.

```
┌──(yasitha㉿kali)-[~]
└─$ cat subdomain.txt | httprobe >> alivedomain.txt
```

After the scan finishes we have to check in the alivedoamin.txt file

```
File  Actions  Edit  View  Help

┌──(yasitha㉿kali)-[~]
└─$ cat alivedomain.txt
https://www.coca-colacompany.com
https://investors.coca-colacompany.com
http://www.coca-colacompany.com
https://login.coca-colacompany.com
https://annualreport.coca-colacompany.com
https://m.newsletter.coca-colacompany.com
http://investors.coca-colacompany.com
https://careers.coca-colacompany.com
http://careers.coca-colacompany.com
http://login.coca-colacompany.com
http://annualreport.coca-colacompany.com
http://m.newsletter.coca-colacompany.com
https://res.newsletter.coca-colacompany.com
https://t.newsletter.coca-colacompany.com
https://transparency.coca-colacompany.com
https://image.newsletters.coca-colacompany.com
http://res.newsletter.coca-colacompany.com
https://thecoca-colacompany.com
http://t.newsletter.coca-colacompany.com
http://transparency.coca-colacompany.com
https://secure.coca-colacompany.com
https://www.thecoca-colacompany.com
http://thecoca-colacompany.com
http://image.newsletters.coca-colacompany.com
http://www.thecoca-colacompany.com
http://secure.coca-colacompany.com
http://click.newsletters.coca-colacompany.com

┌──(yasitha㉿kali)-[~]
└─$
```

Harvesting Emails

We'll have been using stolen databases on the internet to look for usernames, passwords as well as probable emails in this phase. Users can employ brute-force assaults whether we can discover e-mail as well as username similarities.

1. By using via theHarvester

Another Python-based program, theHarvester, is similar to sublist3r. Ethical hackers are using this program to collect data regarding subdomains, emails, banners, hosts, open ports, as well as employee names from publicly available sources such as search engines, SHODAN computer database and the PGP key servers.


```
optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Company name or domain to search.
  -l LIMIT, --limit LIMIT
                        Limit the number of search results, default=500.
  -S START, --start START
                        Start with result number X, default=0.
  -g, --google-dork     Use Google Dorks for Google search.
  -p, --proxies         Use proxies for requests, enter proxies in proxies.yaml.
  -s, --shodan          Use Shodan to query discovered hosts.
  --screenshot SCREENSHOT
                        Take screenshots of resolved domains specify output directory: --screenshot output_directory
  -v, --virtual-host    Verify host name via DNS resolution and search for virtual hosts.
  -e DNS_SERVER, --dns-server DNS_SERVER
                        DNS server to use for lookup.
  -t DNS_TLD, --dns-tld DNS_TLD
                        Perform a DNS TLD expansion discovery, default False.
  -r, --take-over       Check for takeovers.
  -n, --dns-lookup      Enable DNS server lookup, default False.
  -c, --dns-brute       Perform a DNS brute force on the domain.
  -f FILENAME, --filename FILENAME
                        Save the results to an HTML and/or XML file.
  -b SOURCE, --source SOURCE
                        baidu, bing, bingapi, bufferoverun, certspotter, crtsh, dnsdumpster, duckduckgo, exalead, github-code, google, hackertarget, hunter, intelx,
                        linkedin, linkedin_links, netcraft, otx, pentesttools, projectdiscovery, qwant, rapiddns, securityTrails, spyse, sublist3r, threatcrowd,
                        threatminer, trello, twitter, urlscan, virustotal, yahoo
```

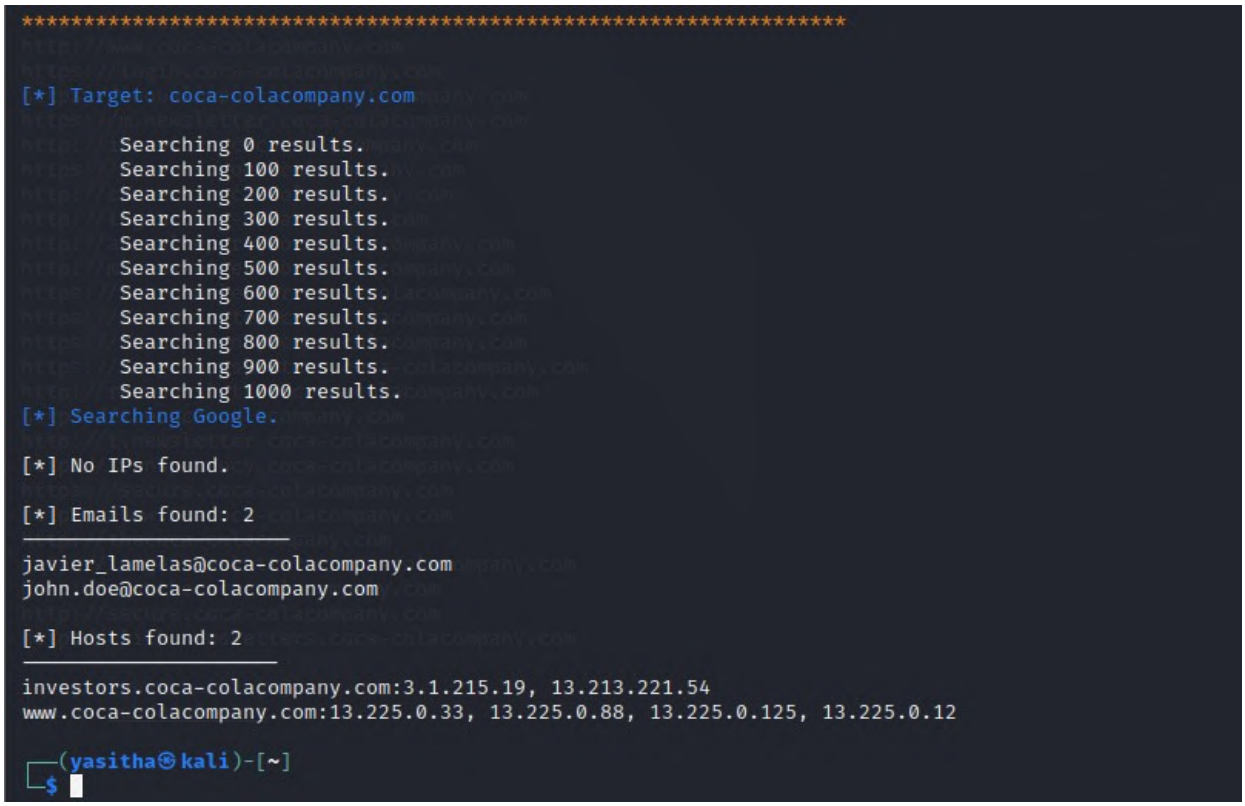
After the scan we can find emails on coca-colacompany.com. these are the emails found through the scan

[*] Emails found: 2

---

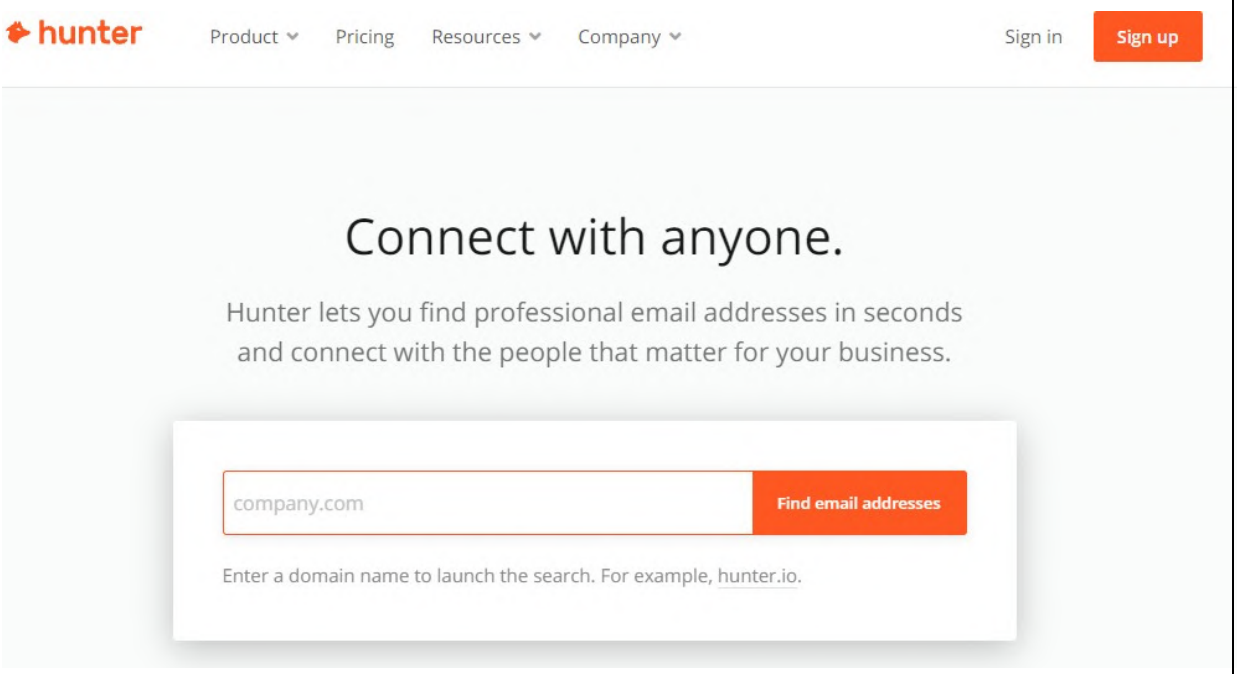
javier_lamelas@coca-colacompany.com

john.doe@coca-colacompany.com

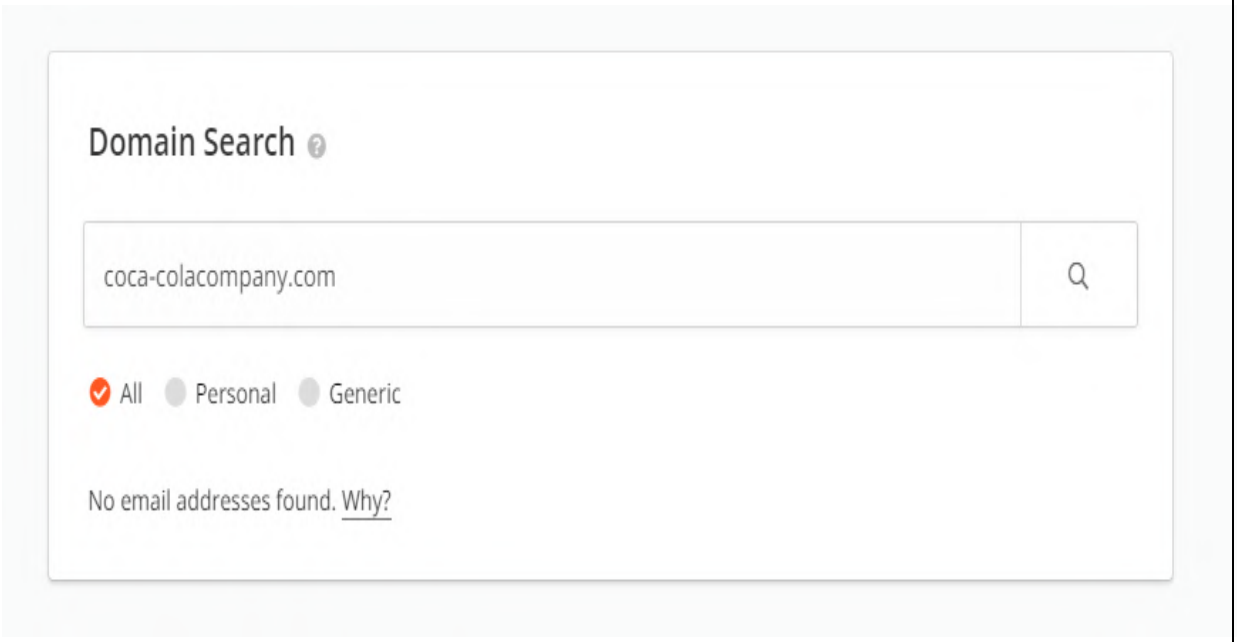


2. Using hunter.io

This is also a platform that we can use to find emails.



But I couldn't find any results on this platform.



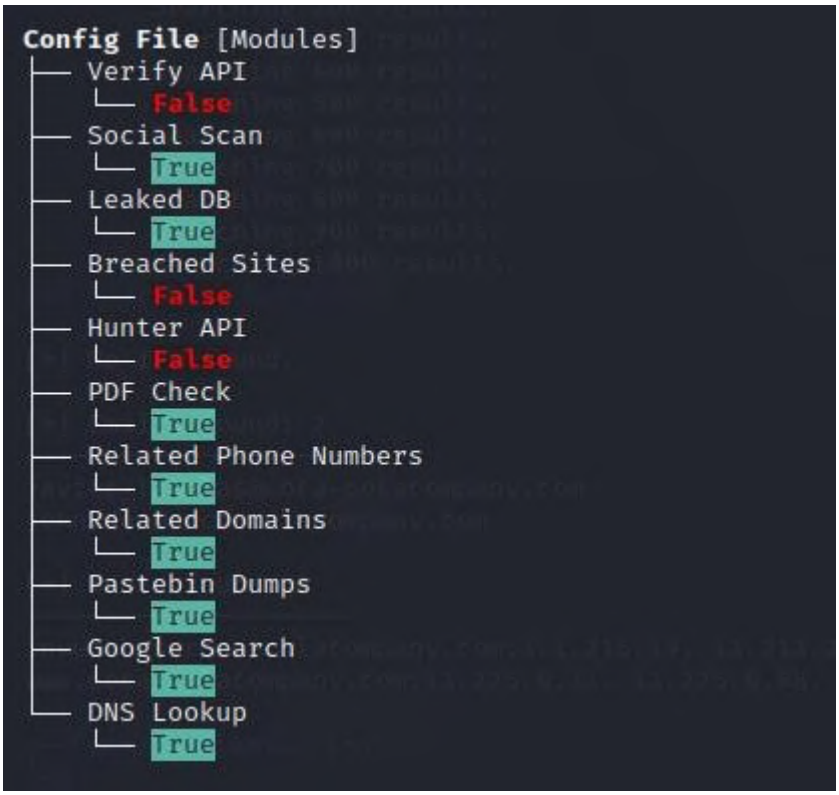
Email OSINT

Using open-source intelligence technologies, users might learn so much about these e-mails.

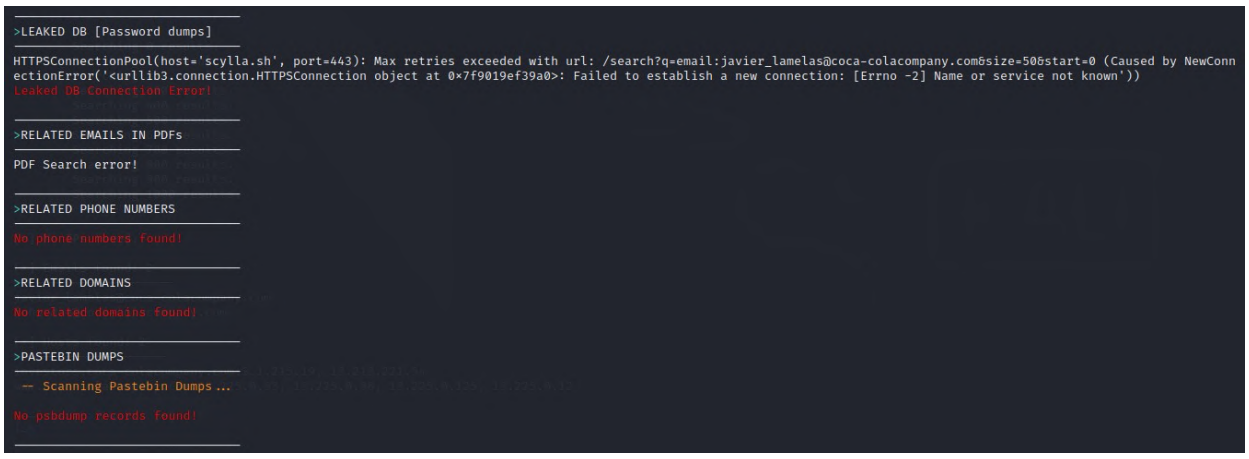
- **MOSINT**

  MOSINT is an email-focused OSINT tool. This tool assists us in gathering information about the intended recipient of the email. Such as;

  - Checks whether the email exits.
  - Get a list of numbers that are linked.
  - Google Search
  - Look for breaches of data.
  - Use Social scan to examine social profiles.
  - Look for related domains.
  - Pastebin Dump Scanning
  - Look for emails that are relevant for PDFs and API.



This show us the Social media accounts which are connected with the relevant email.



```
>GOOGLING
 -- Google Searching ... [Pastebin & Throwbin]
!Google Search may not work properly.

Google Search error!
```

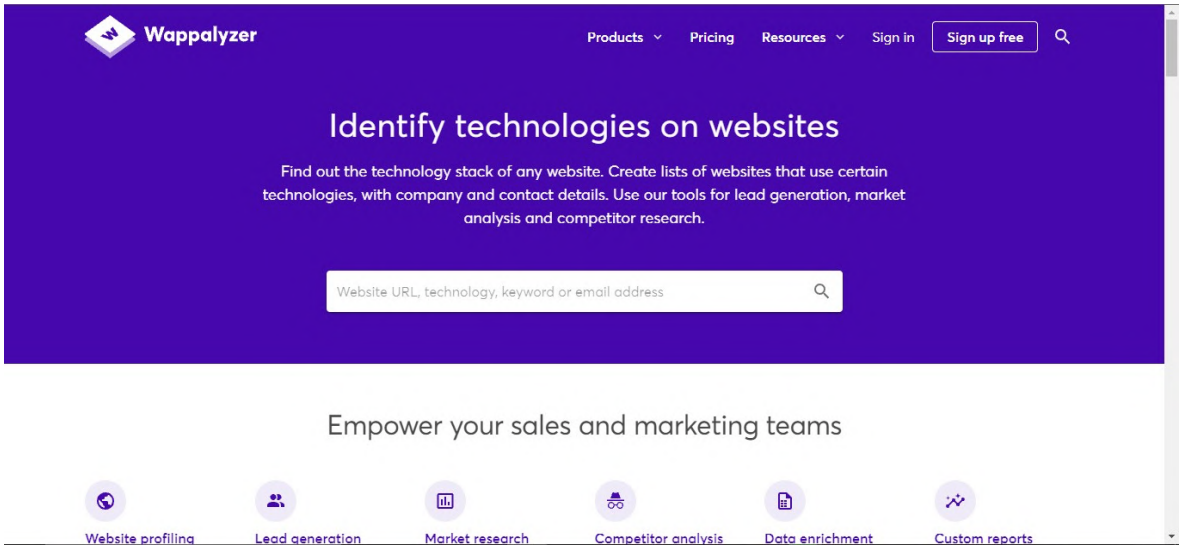
The following DNS entries were connected with the e-mail:

```
>DNS LOOKUP
 -- DNS Records [ Cloudflare ]
+-------------+-----------------------------------------------------------------------------------------------------+
| Record Type |                                                Answer                                               |
+-------------+-----------------------------------------------------------------------------------------------------+
|          NS |                                          ns1-09.azure-dns.com.                                      |
|          NS |                                          ns2-09.azure-dns.net.                                      |
|          NS |                                          ns3-09.azure-dns.org.                                      |
|          NS |                                          ns4-09.azure-dns.info.                                     |
|           A |                                              52.14.144.171                                          |
|         TXT |                    "facebook-domain-verification=0rpf1rbxv22prbrmwmd7igijjolwta"                    |
|         TXT |  "v=DMARC1; p=none; fo=1; rua=mailto:dmarcreports@coca-cola.com; ruf=mailto:dmarcreports@coca-cola.com" |
|         TXT |                                              "v=spf1 -all"                                          |
|          MX |                                              10 ns1.ko.com.                                         |
+-------------+-----------------------------------------------------------------------------------------------------+

┌──(yasitha㉿kali)-[~/mosint]
└─$
```

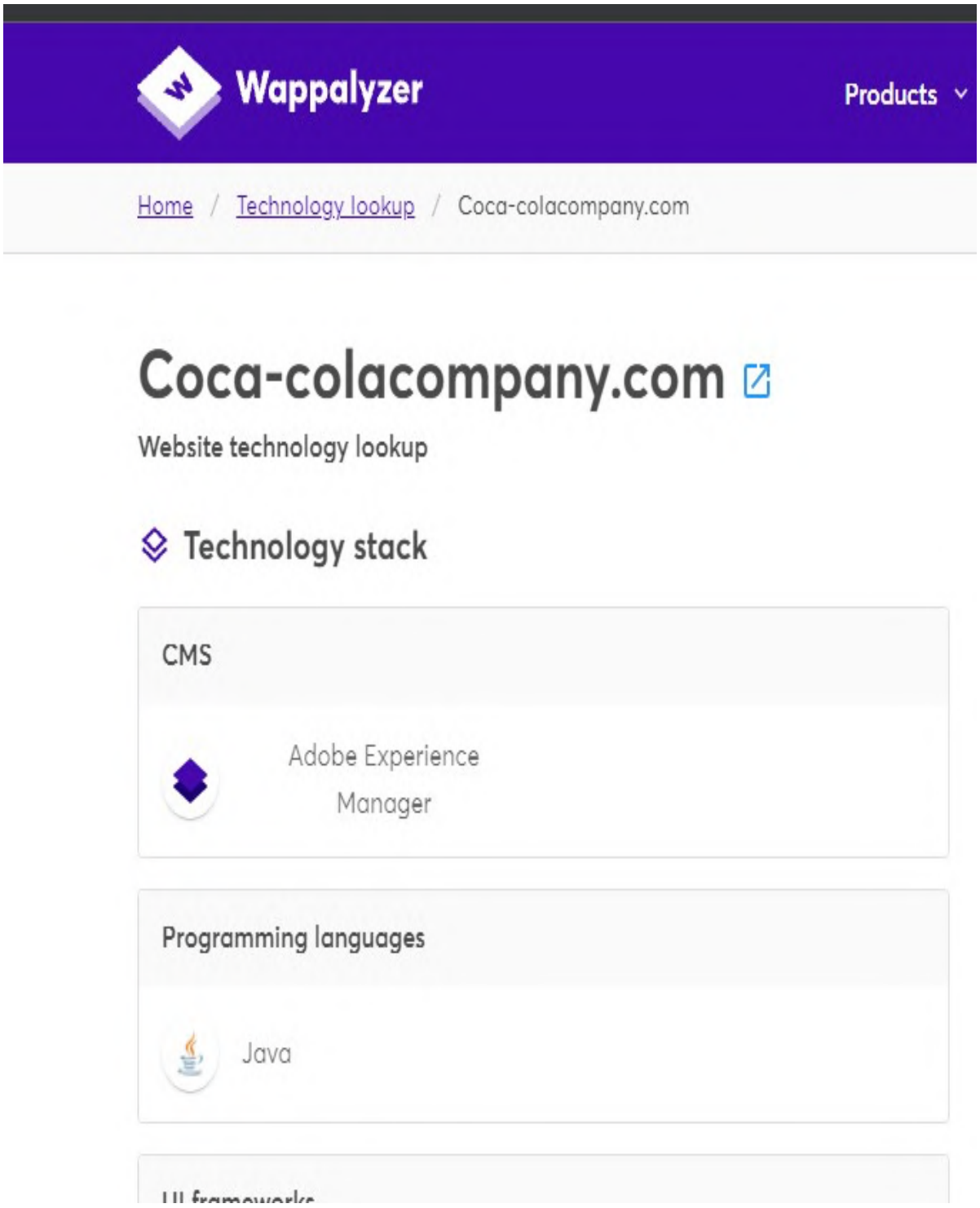
Finding Out Web Technologies

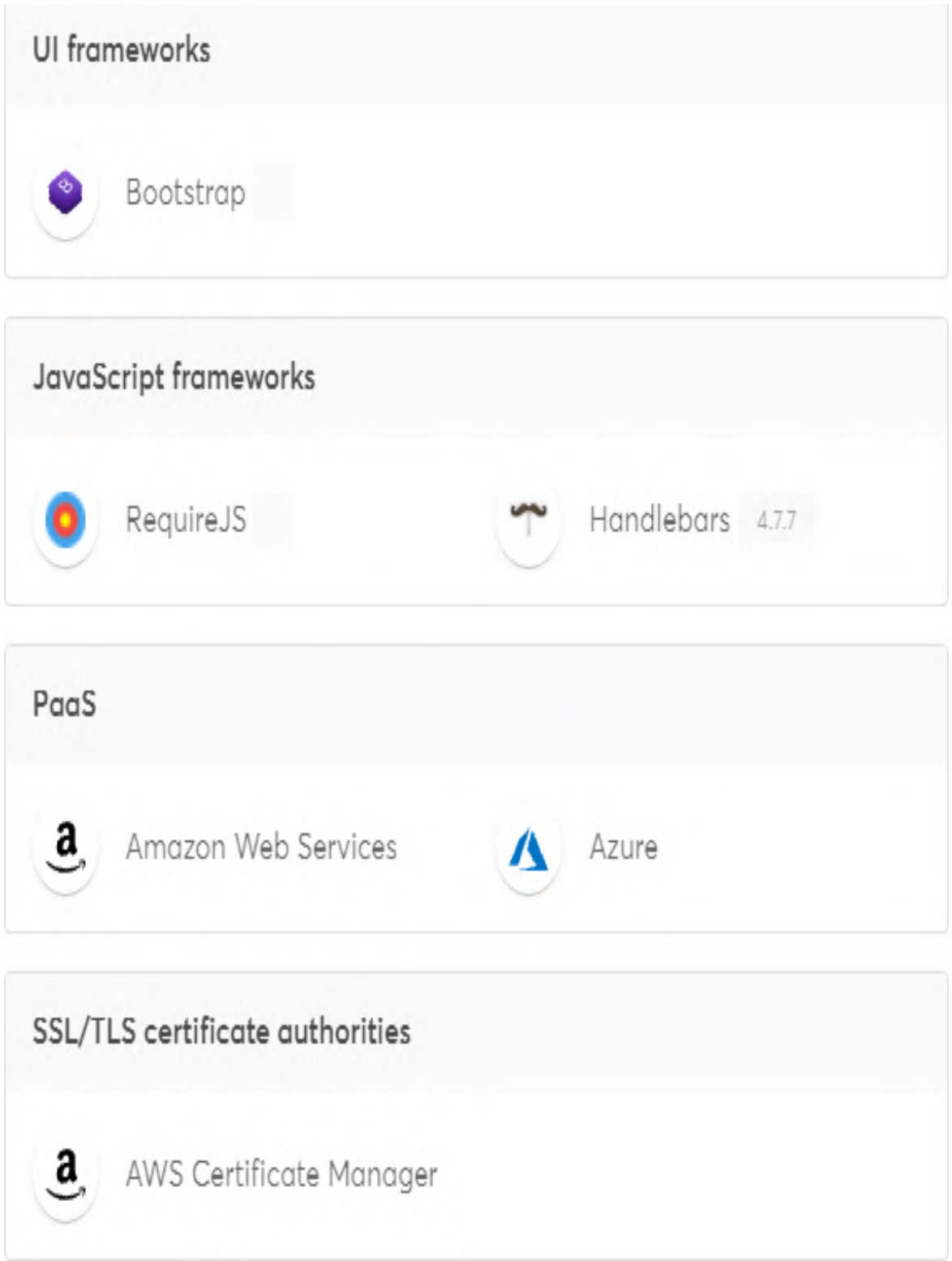
Web technology refers to the techniques by which devices connect with each other using markup languages as well as multimedia packages. Those same technologies might well have flaws that we may look at during the penetration assessment process.

1. Via Wappalyzer.com



This website can be used to identify the technologies of a particular website. Down below are the search results of it.




UI frameworks
Bootstrap
JavaScript frameworks
RequireJS
Handlebars 4.7.7
PaaS
Amazon Web Services
Azure
SSL/TLS certificate authorities
AWS Certificate Manager

Appointment scheduling

Periodic

Widgets

Facebook

Twitter

Advertising

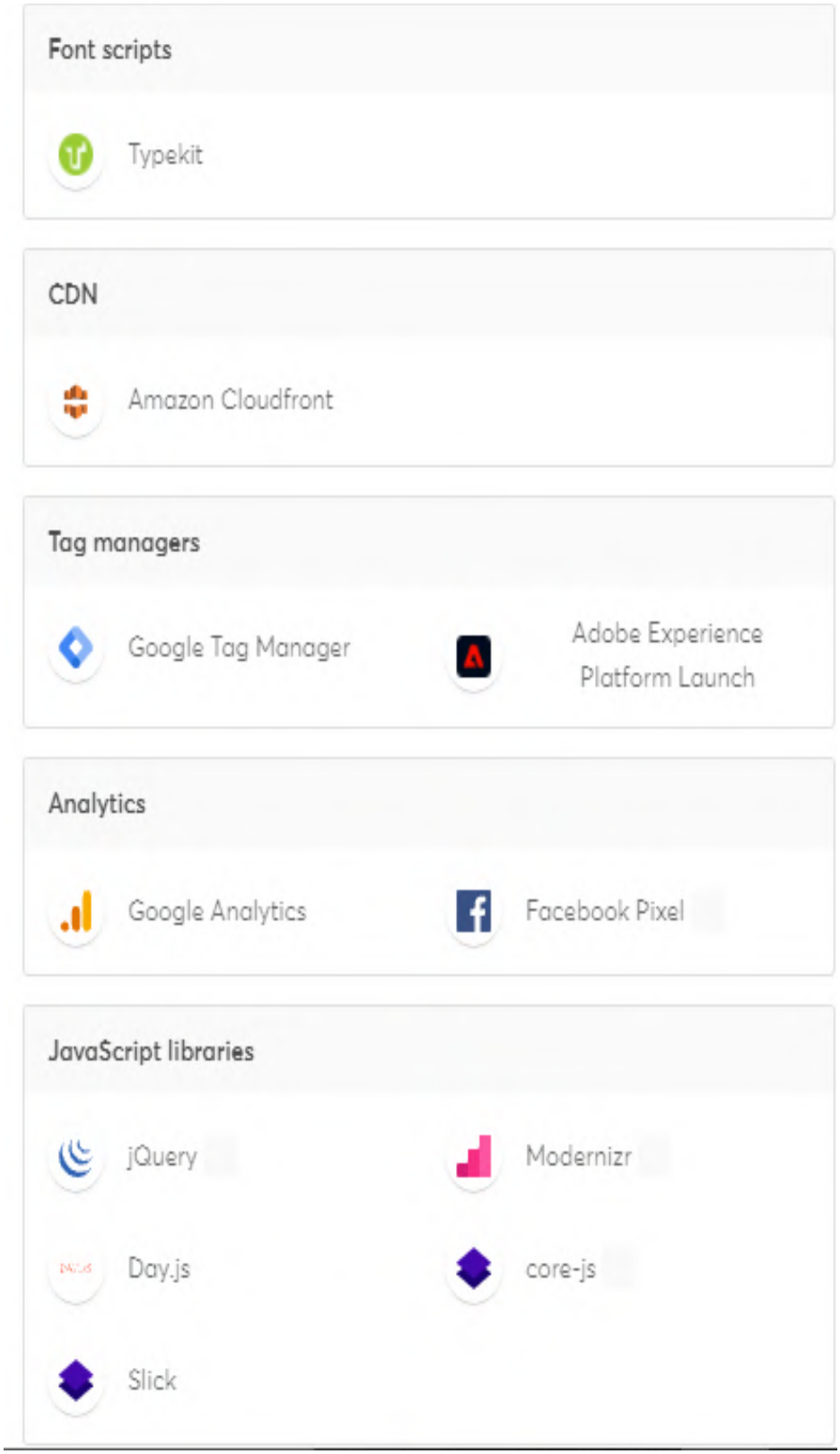
Twitter Ads

Miscellaneous

Amazon S3

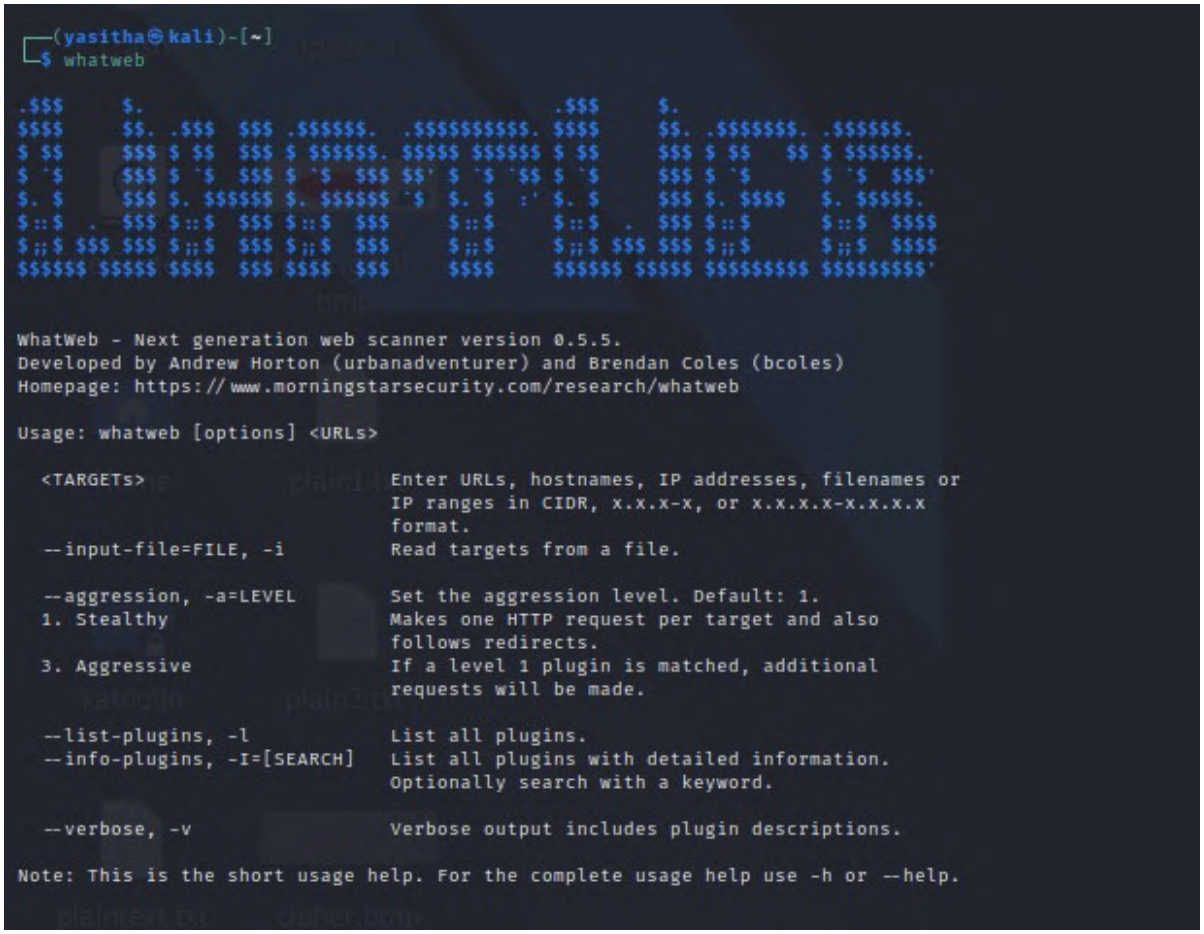
Cookie compliance

OneTrust

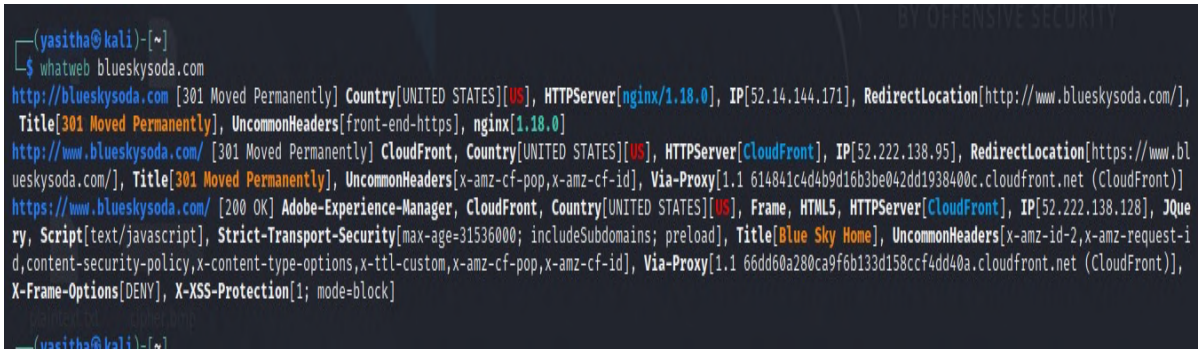

Font scripts
Typekit
CDN
Amazon Cloudfront
Tag managers
Google Tag Manager
Adobe Experience Platform Launch
Analytics
Google Analytics
Facebook Pixel
JavaScript libraries
jQuery
Modernizr
Day.js
core-js
Slick

2. Via WhatWeb

WhatWeb is a website identifier. It supports online technologies such as blog sites, web servers, content management systems (CMS), connected system, statistical/analytics packages, and JavaScript library.



In here in have used "**whatweb blueskysoda.com** "

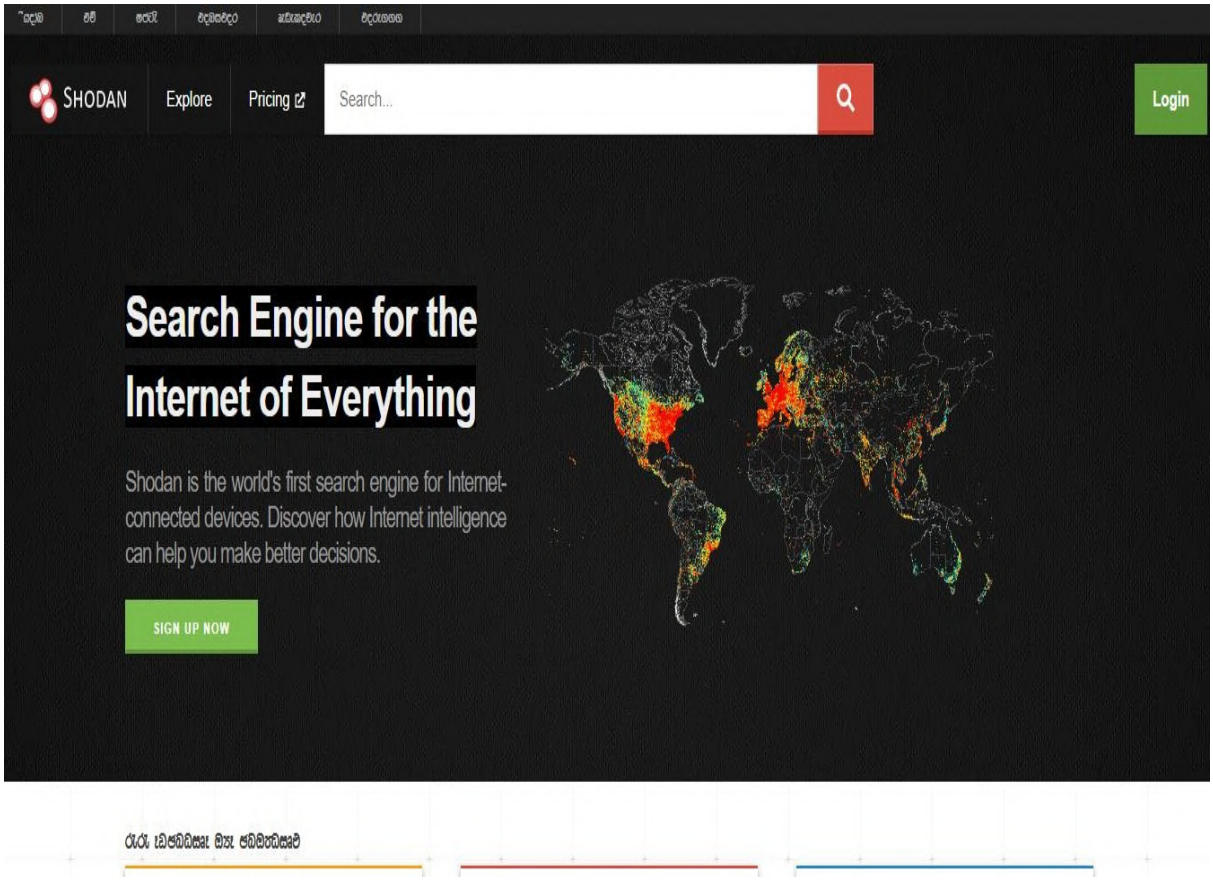


Internet Connected devices hunting

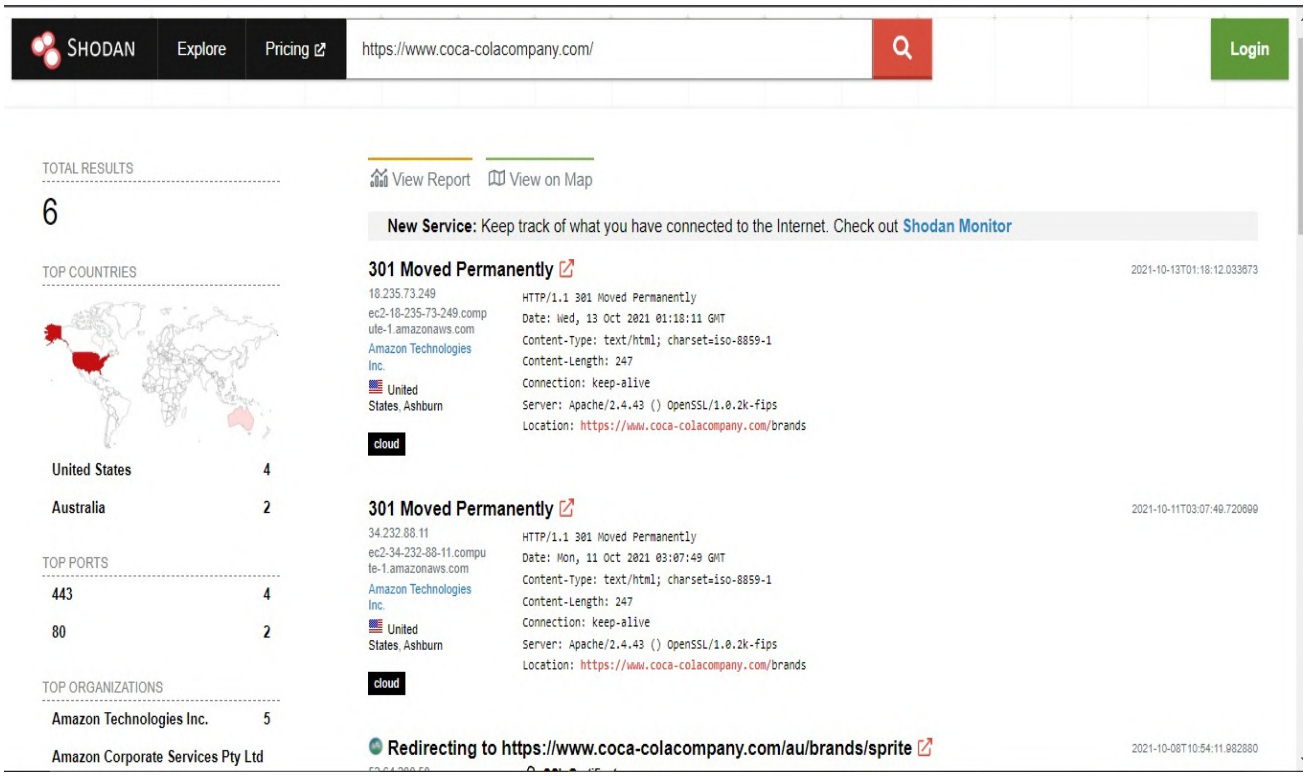
A system in figure is unquestionably linked to the internet through a multitude of devices. For example, laptops, smartphones, pcs, severs and many more. Throughout this phase, we scout out any internet-connected equipment, including IP addresses, web server information, and so on.

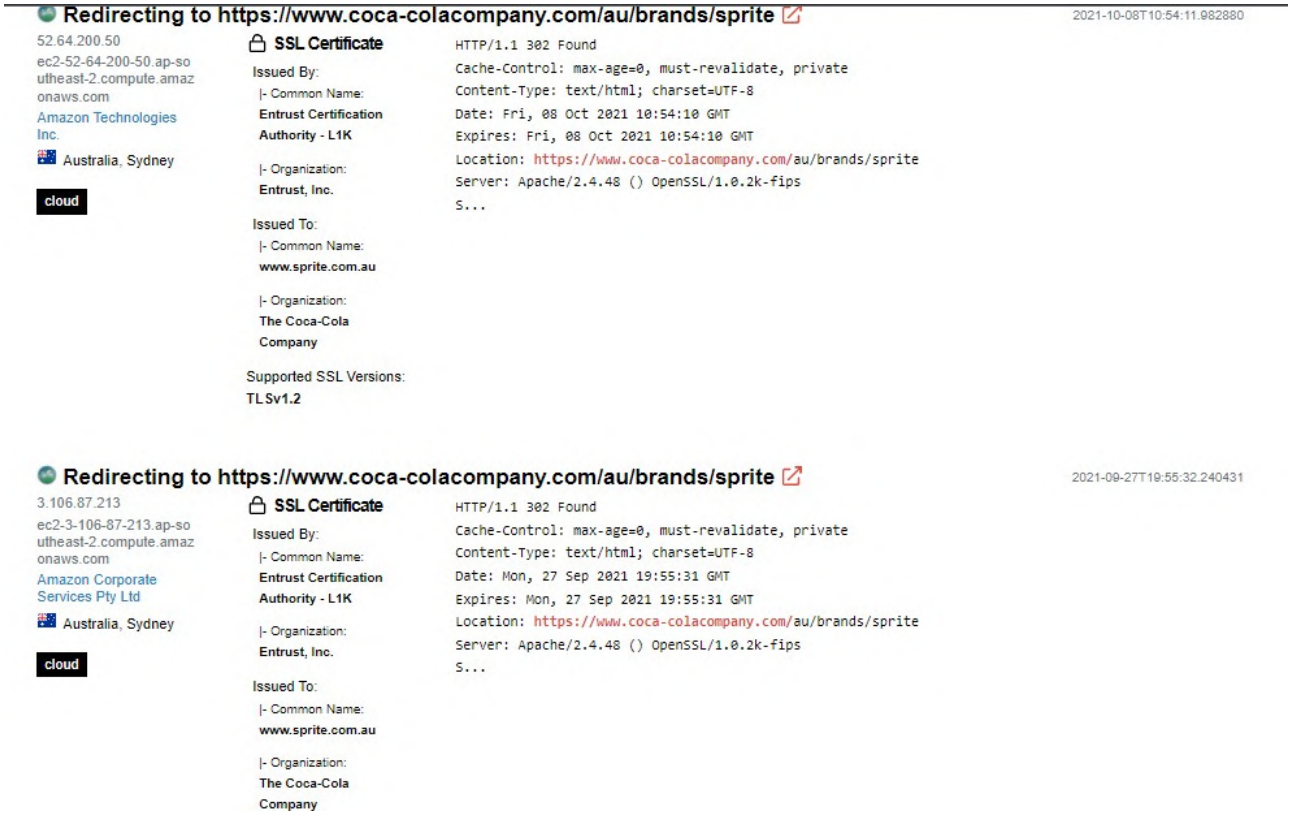
Via SHODAN

Shodan is a search engine targeting gadgets that are linked to the Web. Shodan collects data across all gadgets that are directly linked toward the Net. When an equipment is straightforwardly connected to the Internet, Shodan searches everything for publicly available data.

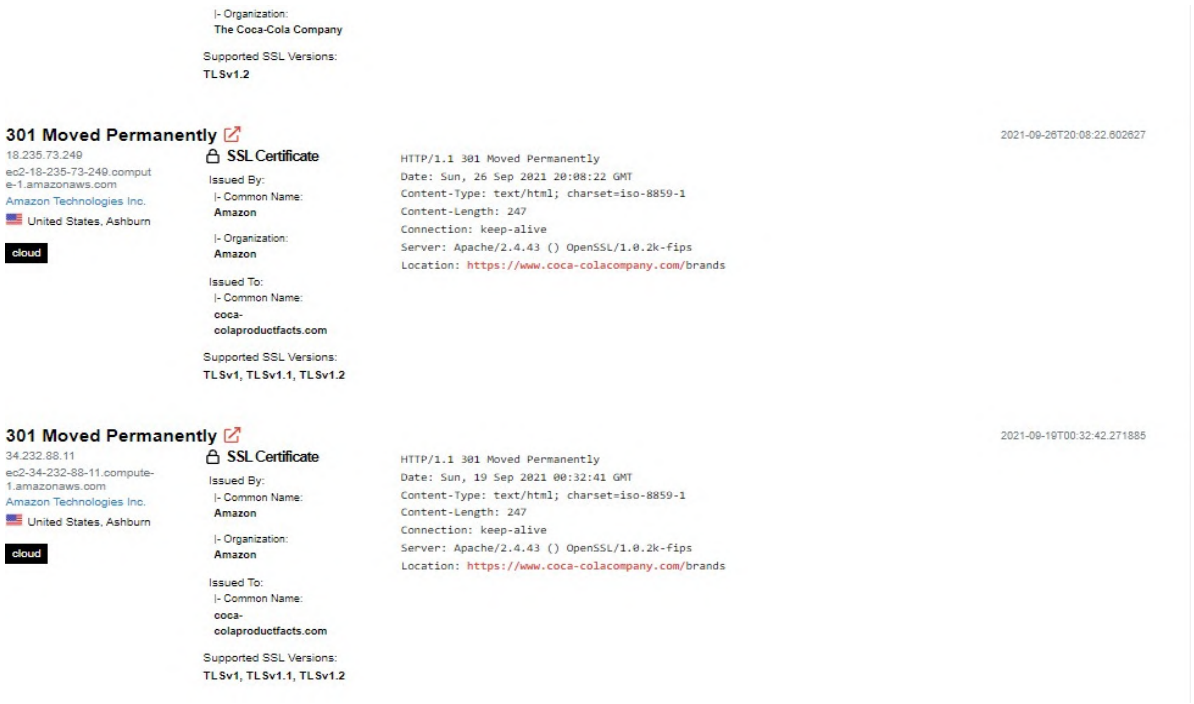


These are the results found in shodan.io


SHODAN
Explore
Pricing
https://www.coca-colacompany.com/
Login
TOTAL RESULTS
6
TOP COUNTRIES
United States 4
Australia 2
TOP PORTS
443 4
80 2
TOP ORGANIZATIONS
Amazon Technologies Inc. 5
Amazon Corporate Services Pty Ltd
View Report
View on Map
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
301 Moved Permanently
2021-10-13T01:18:12.033673
18.235.73.249
ec2-18-235-73-249.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn
cloud
HTTP/1.1 301 Moved Permanently
Date: Wed, 13 Oct 2021 01:18:11 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 247
Connection: keep-alive
Server: Apache/2.4.43 () OpenSSL/1.0.2k-fips
Location: https://www.coca-colacompany.com/brands
301 Moved Permanently
2021-10-11T03:07:49.720699
34.232.88.11
ec2-34-232-88-11.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn
cloud
HTTP/1.1 301 Moved Permanently
Date: Mon, 11 Oct 2021 03:07:49 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 247
Connection: keep-alive
Server: Apache/2.4.43 () OpenSSL/1.0.2k-fips
Location: https://www.coca-colacompany.com/brands
Redirecting to https://www.coca-colacompany.com/au/brands/sprite
2021-10-08T10:54:11.982880


Redirecting to https://www.coca-colacompany.com/au/brands/sprite
2021-10-08T10:54:11.982880
52.64.200.50
ec2-52-64-200-50.ap-southeast-2.compute.amazonaws.com
Amazon Technologies Inc.
Australia, Sydney
cloud
SSL Certificate
Issued By:
|- Common Name:
Entrust Certification Authority - L1K
|- Organization:
Entrust, Inc.
Issued To:
|- Common Name:
www.sprite.com.au
|- Organization:
The Coca-Cola Company
Supported SSL Versions:
TLSv1.2
HTTP/1.1 302 Found
Cache-Control: max-age=0, must-revalidate, private
Content-Type: text/html; charset=UTF-8
Date: Fri, 08 Oct 2021 10:54:10 GMT
Expires: Fri, 08 Oct 2021 10:54:10 GMT
Location: https://www.coca-colacompany.com/au/brands/sprite
Server: Apache/2.4.48 () OpenSSL/1.0.2k-fips
S...

Redirecting to https://www.coca-colacompany.com/au/brands/sprite
2021-09-27T19:55:32.240431
3.106.87.213
ec2-3-106-87-213.ap-southeast-2.compute.amazonaws.com
Amazon Corporate Services Pty Ltd
Australia, Sydney
cloud
SSL Certificate
Issued By:
|- Common Name:
Entrust Certification Authority - L1K
|- Organization:
Entrust, Inc.
Issued To:
|- Common Name:
www.sprite.com.au
|- Organization:
The Coca-Cola Company
HTTP/1.1 302 Found
Cache-Control: max-age=0, must-revalidate, private
Content-Type: text/html; charset=UTF-8
Date: Mon, 27 Sep 2021 19:55:31 GMT
Expires: Mon, 27 Sep 2021 19:55:31 GMT
Location: https://www.coca-colacompany.com/au/brands/sprite
Server: Apache/2.4.48 () OpenSSL/1.0.2k-fips
S...



The http requests, ip addresses, certification information and many more useful information are here.

DNS Reconnaissance

Tools such as DNSRecon, Nmap, and DNSenum, which are included in penetration testing packages, can be used to acquire details about domain name systems. Those utilities can conduct zone transfer, reverse lookup, zone wandering, standard record enumeration, Google lookup, domain brute-forcing and cache snooping.

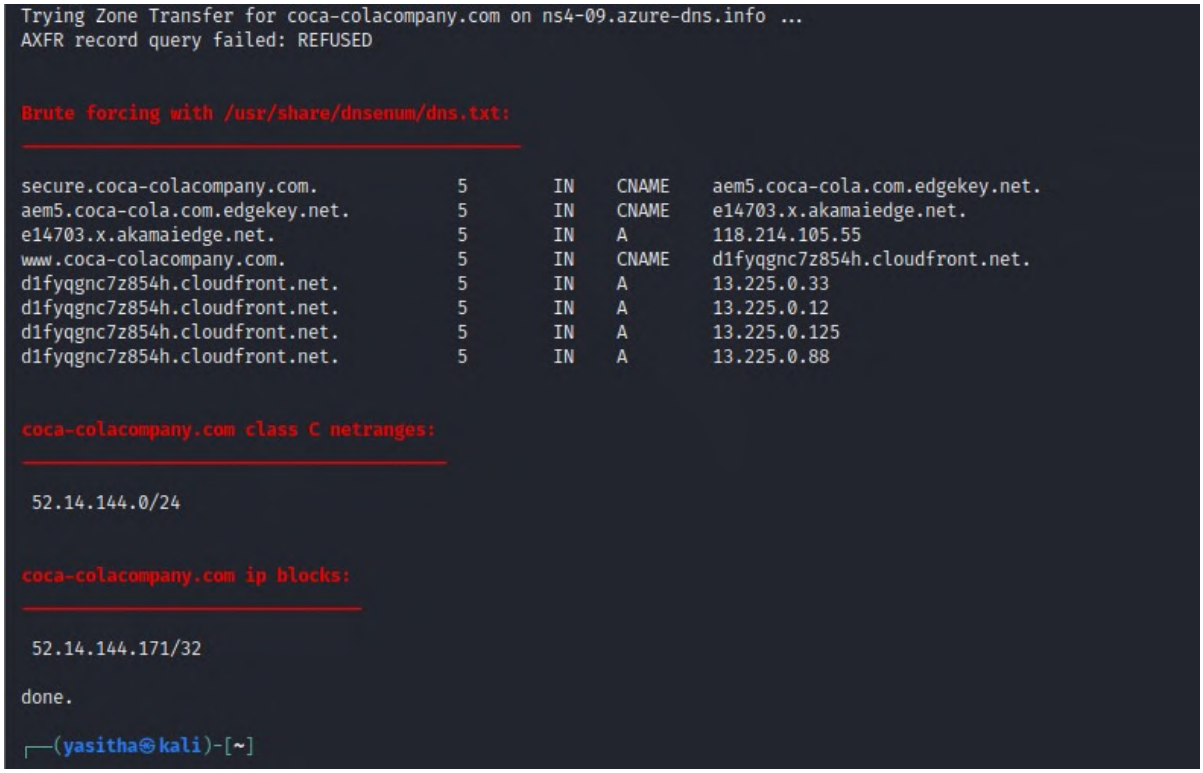
Via DNSenum

This is a simple tool to use. It is used without reverse lookup and get a .xml file as output.

```
┌──(yasitha㉿kali)-[~]
└─$ dnsenum --noreverse   -o file.xml coca-colacompany.com
dnsenum VERSION:1.2.6

-----   coca-colacompany.com   -----
```

These are some useful information.

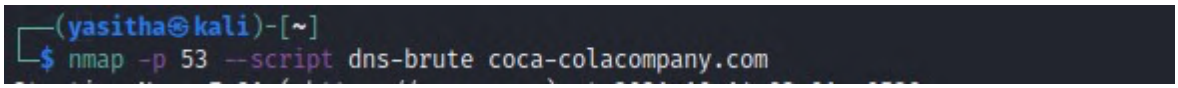
```
Host's addresses:
__________________

coca-colacompany.com.                    5        IN    A        52.14.144.171


Name Servers:
_____________

ns1-09.azure-dns.com.                    5        IN    A         40.90.4.9
ns2-09.azure-dns.net.                    5        IN    A         64.4.48.9
ns3-09.azure-dns.org.                    5        IN    A        13.107.24.9
ns4-09.azure-dns.info.                   5        IN    A        13.107.160.9


Mail (MX) Servers:
__________________


Trying Zone Transfers and getting Bind Versions:
________________________________________________


Trying Zone Transfer for coca-colacompany.com on ns1-09.azure-dns.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for coca-colacompany.com on ns4-09.azure-dns.info ...
AXFR record query failed: REFUSED

Trying Zone Transfer for coca-colacompany.com on ns3-09.azure-dns.org ...
AXFR record query failed: REFUSED
```



Via nmap

nmap is a tool that may be used to help obtain DNS information. Nmap features a concurrent reverse DNS resolution engine which is typically utilized element of a nmap scanning but could also be used separately about the scanning functionality to perform DNS enumeration.

supplying a script name of "dns-brute". And the target name as **coca-colacompany.com.**



Port as 53

And here are some useful information down below.

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-14 02:01 +0530
Nmap scan report for coca-colacompany.com (52.14.144.171)
Host is up (0.091s latency).
rDNS record for 52.14.144.171: ec2-52-14-144-171.us-east-2.compute.amazonaws.com

PORT   STATE SERVICE
53/tcp open  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     secure.coca-colacompany.com - 118.214.105.55
|     www.coca-colacompany.com - 13.225.0.12
|     www.coca-colacompany.com - 13.225.0.125
|     www.coca-colacompany.com - 13.225.0.33
|     www.coca-colacompany.com - 13.225.0.88
|     www.coca-colacompany.com - 2600:9000:21b4:1600:9:1172:bc40:93a1
|     www.coca-colacompany.com - 2600:9000:21b4:2200:9:1172:bc40:93a1
|     www.coca-colacompany.com - 2600:9000:21b4:3600:9:1172:bc40:93a1
|     www.coca-colacompany.com - 2600:9000:21b4:7e00:9:1172:bc40:93a1
|     www.coca-colacompany.com - 2600:9000:21b4:ce00:9:1172:bc40:93a1
|     www.coca-colacompany.com - 2600:9000:21b4:d000:9:1172:bc40:93a1
|     www.coca-colacompany.com - 2600:9000:21b4:d600:9:1172:bc40:93a1
|_    www.coca-colacompany.com - 2600:9000:21b4:f200:9:1172:bc40:93a1

Nmap done: 1 IP address (1 host up) scanned in 79.50 seconds
```

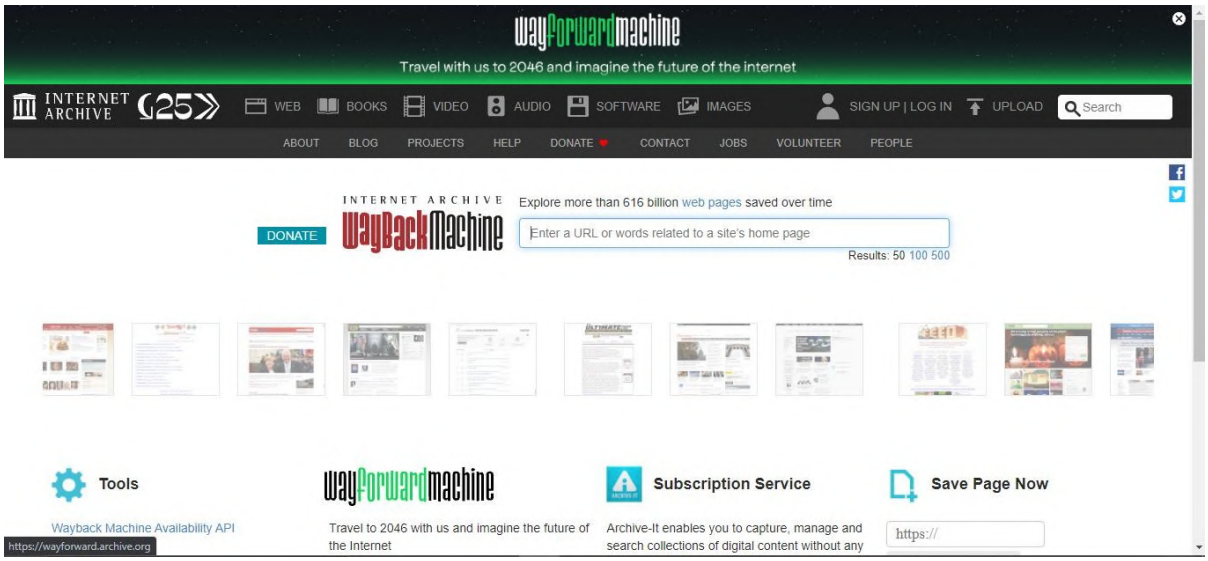
Hunting Archived Information

There might be some useful knowledge upon this webpages, including such pictures, neglected endpoints, and data backup that were previously used. These are known as archived material, and that we need to discover them such that one could also get a sense of how the webpage has evolved, and some valuable tips that we can utilize to the benefit.

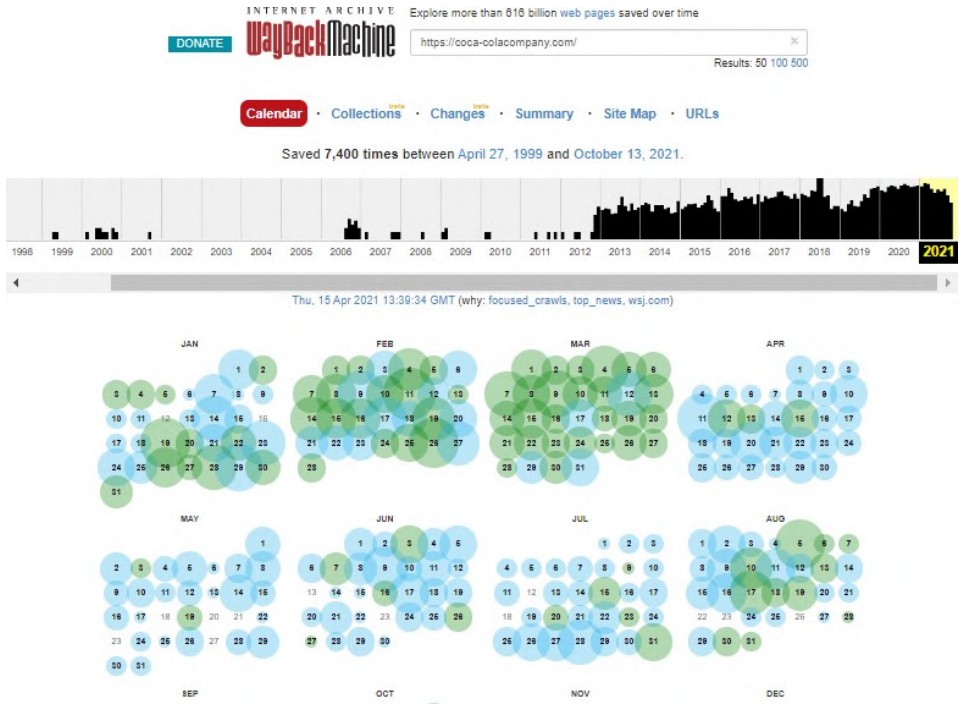
Via way back machine

The Wayback Machine is a web archive. This is a feature which lets users to access archived editions for webpages. Users towards the Wayback Machine may enter inside a URL, choose a date period, and also browse an archived version of the Website. Consider browsing during 1999 and seeing all the Y2K hoopla, or going back to a previous edition of their favorite Web site.

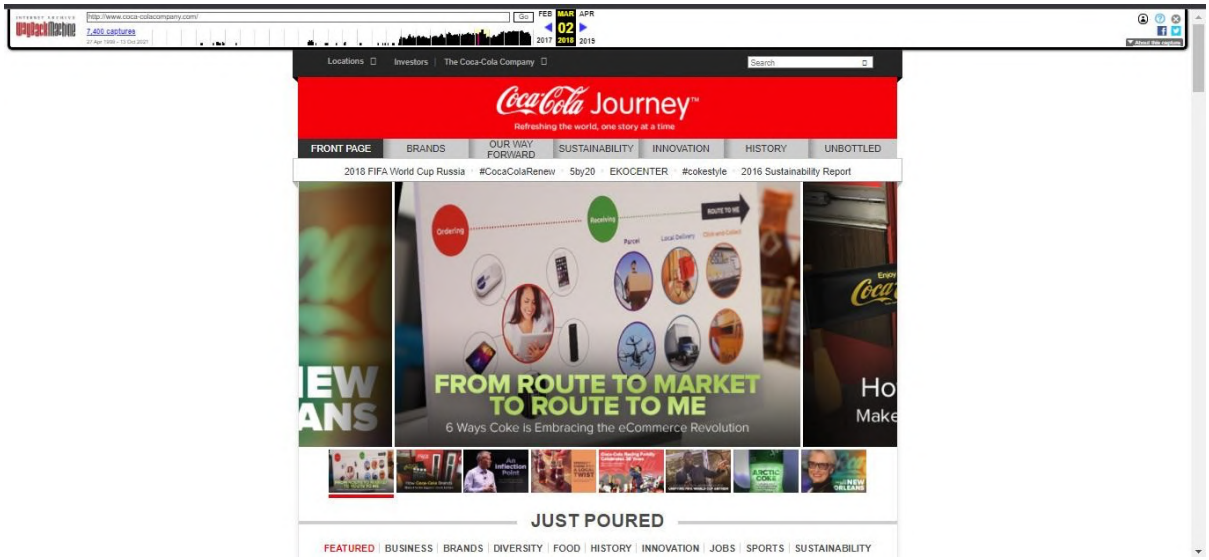
You can use this tool after visiting the following website http://web.archive.org/ .



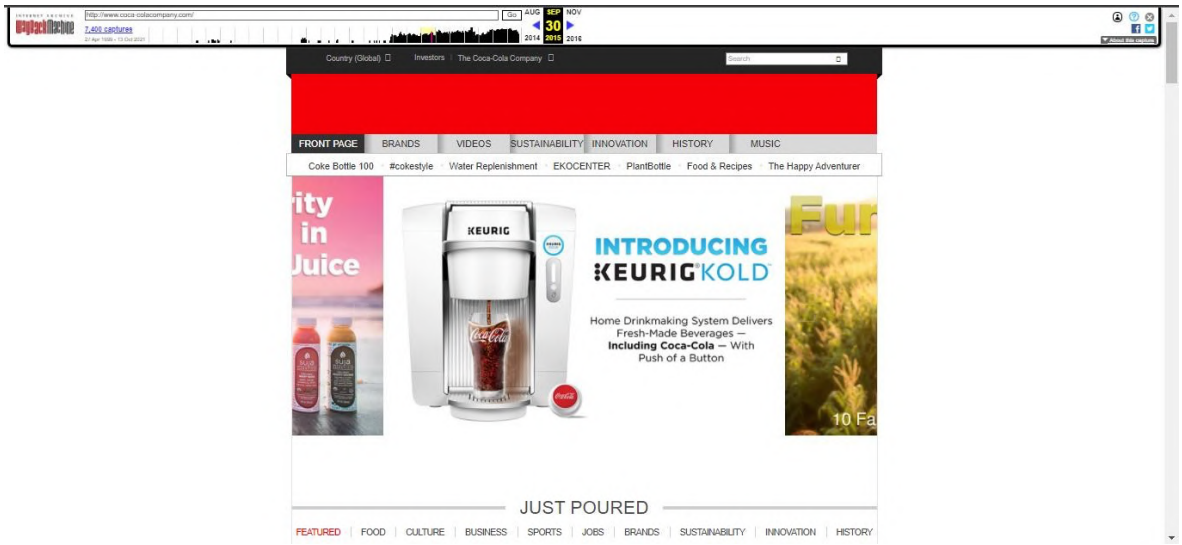
Now we can select the date from here.



Here is screenshot of 2nd of march 2018.



Here is screenshot of 30th of September 2015.



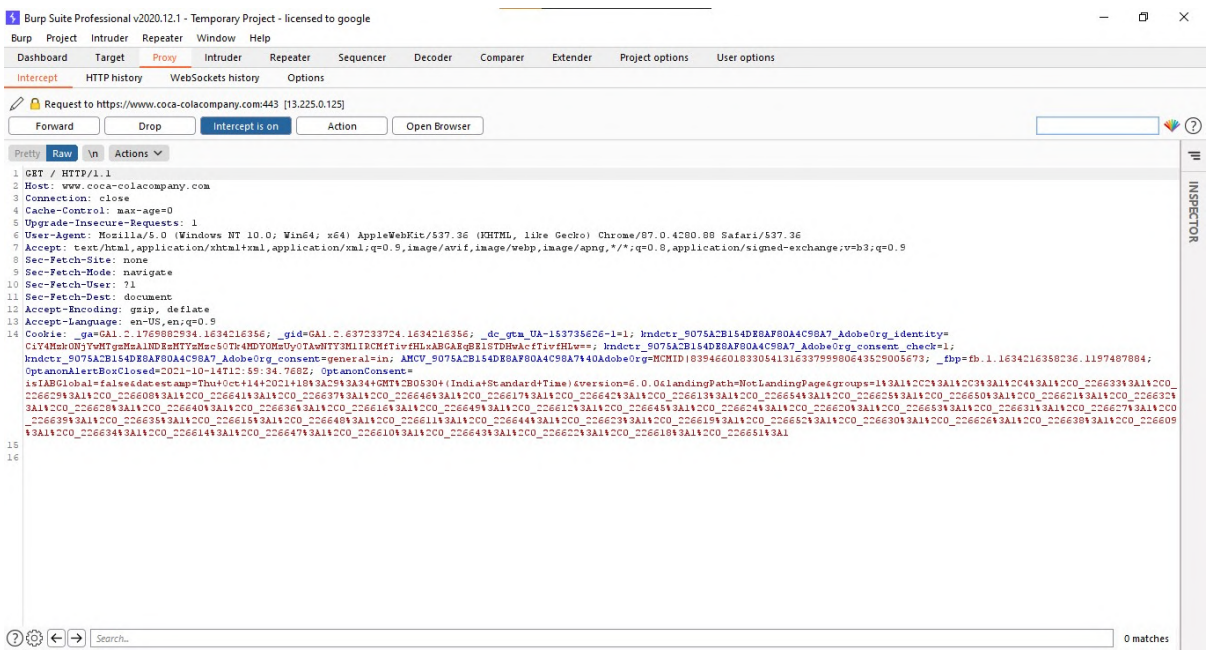
Scanning and Footprinting

The person who tests, takes an active role well with objective in providing a more comprehensive understanding of the victim's services, firewalls, open ports, in-scope servers, as well as other related details. This is indeed the point during which researchers aggressively gain knowledge concerning the objective. This provides us with critical data regarding the actual targeted system immediately.

Scanning with BurpSuit

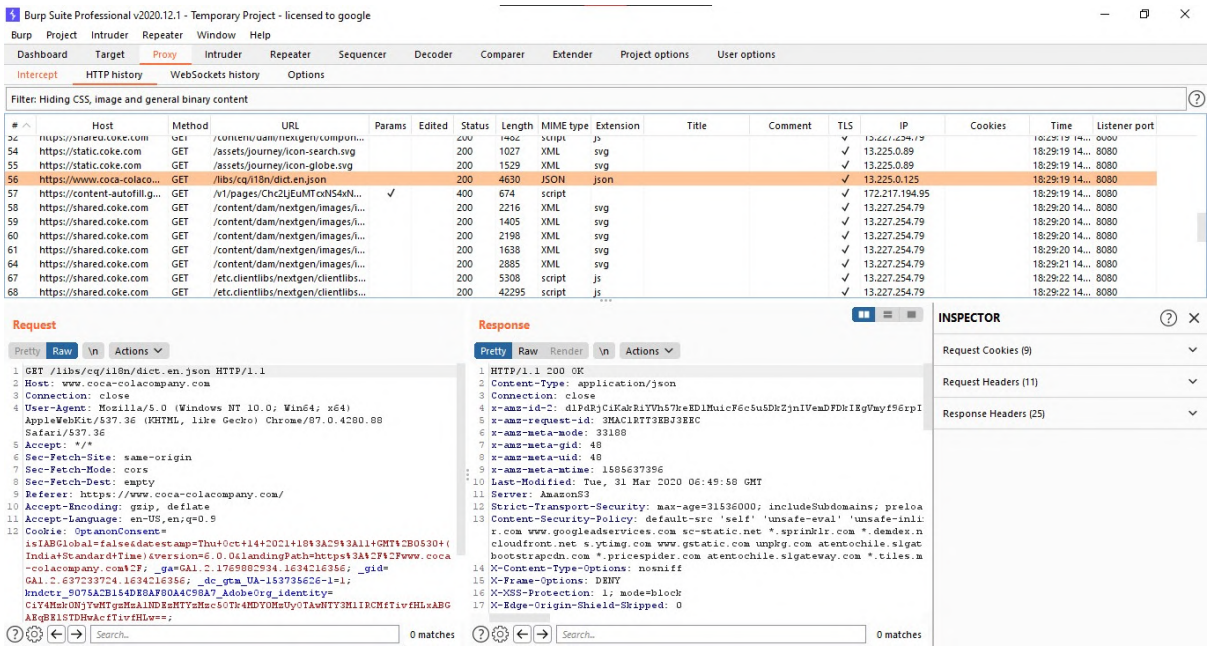
Burp, often known as the Burp Suite, is a collection of tools used to identify online application security. This application allows us to accomplish numerous activities which we would be unable to execute manual process, like as manipulating headers or cookies, modifying requests made or brute force attacks towards the server.

In here I intercepted https://www.coca-colacompany.com/ the website and captured.

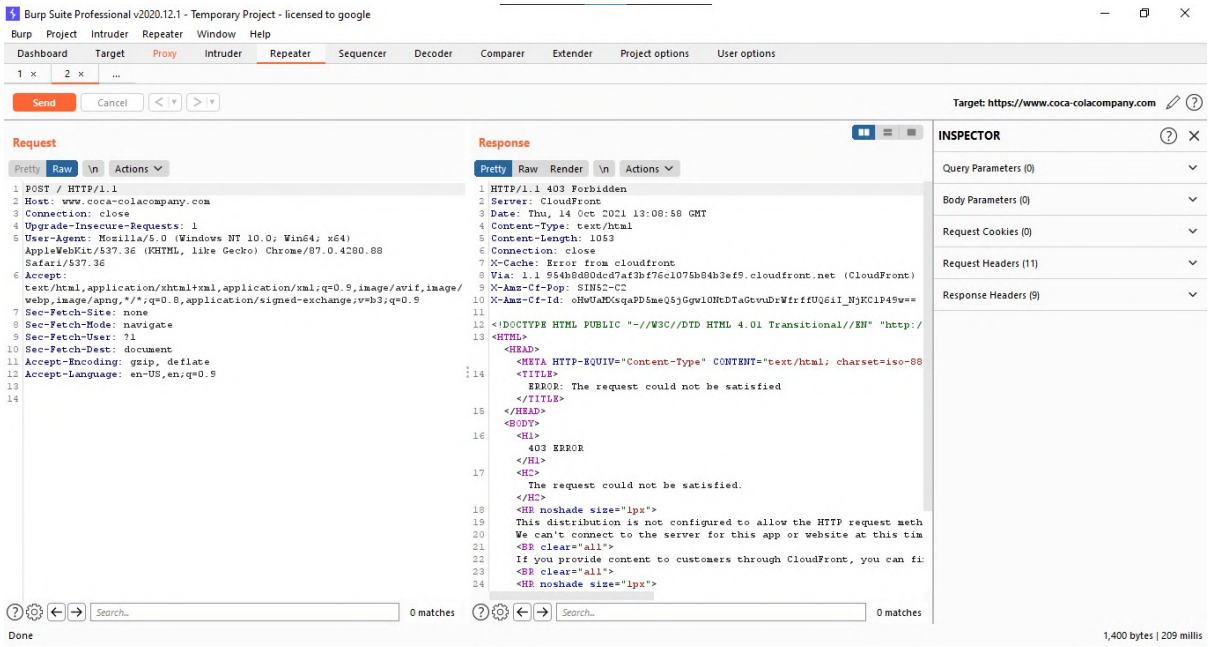


In here it is GET method used. So I now try to change the method into POST

By right clicking on the link we get a drop down to send to repeater.



Now in the repeater window change the response method to POST.

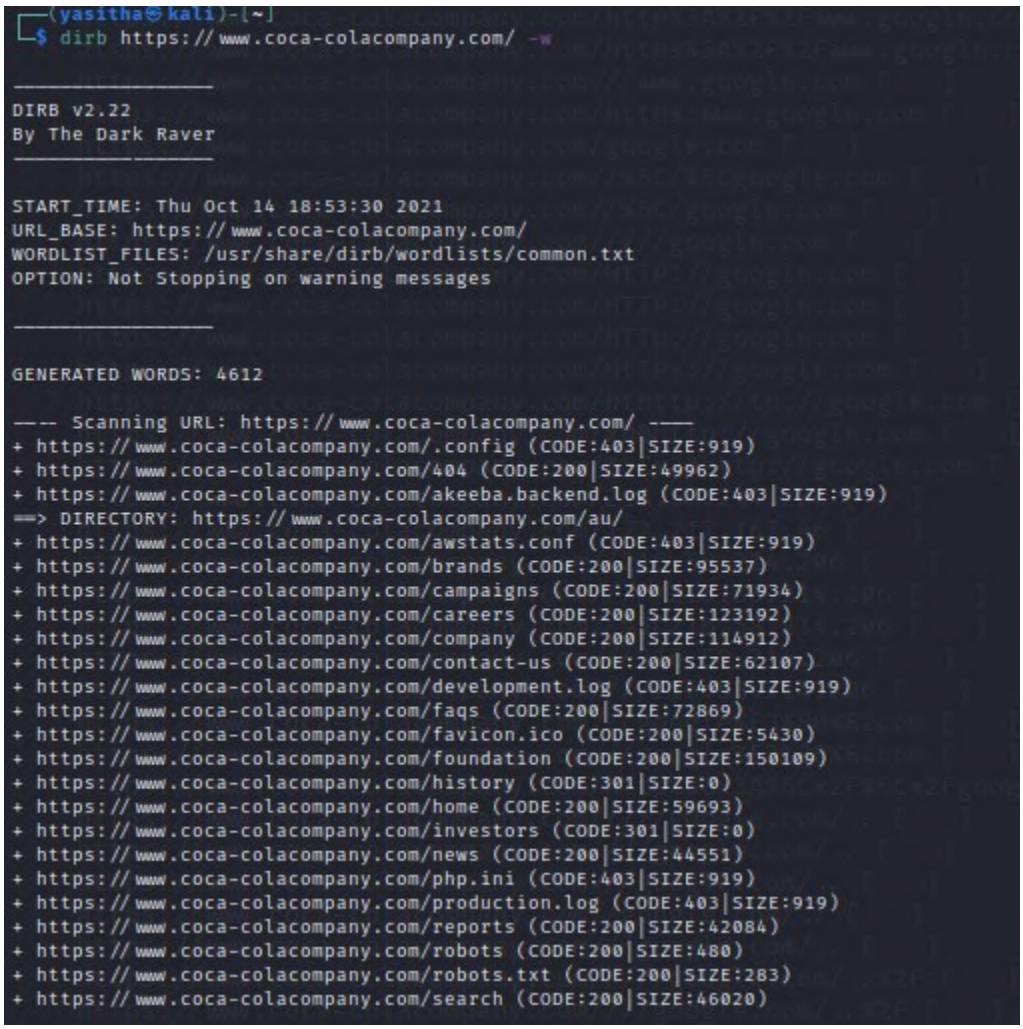


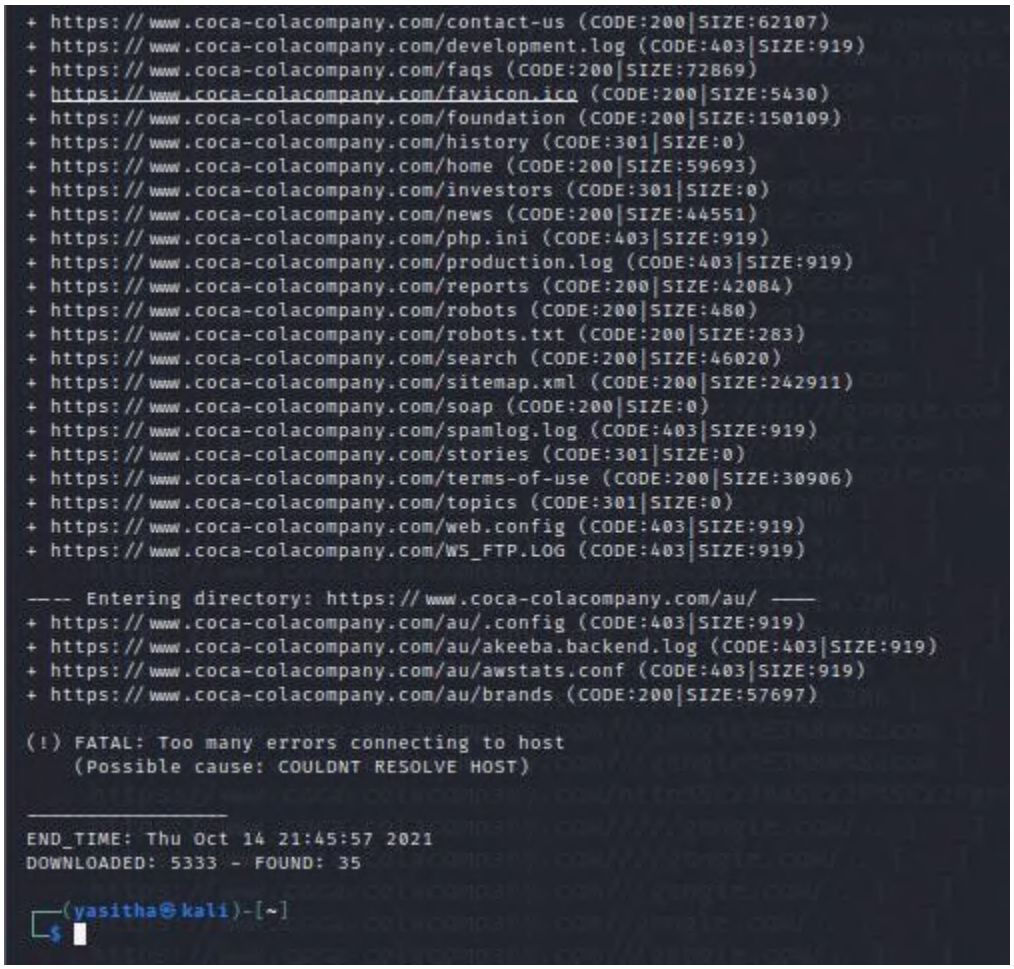
But I could get any useful information about the allowed methods.

Brute-forcing Directories

This assaults also been used to uncover hidden web content within a web - based application.

Via dirb





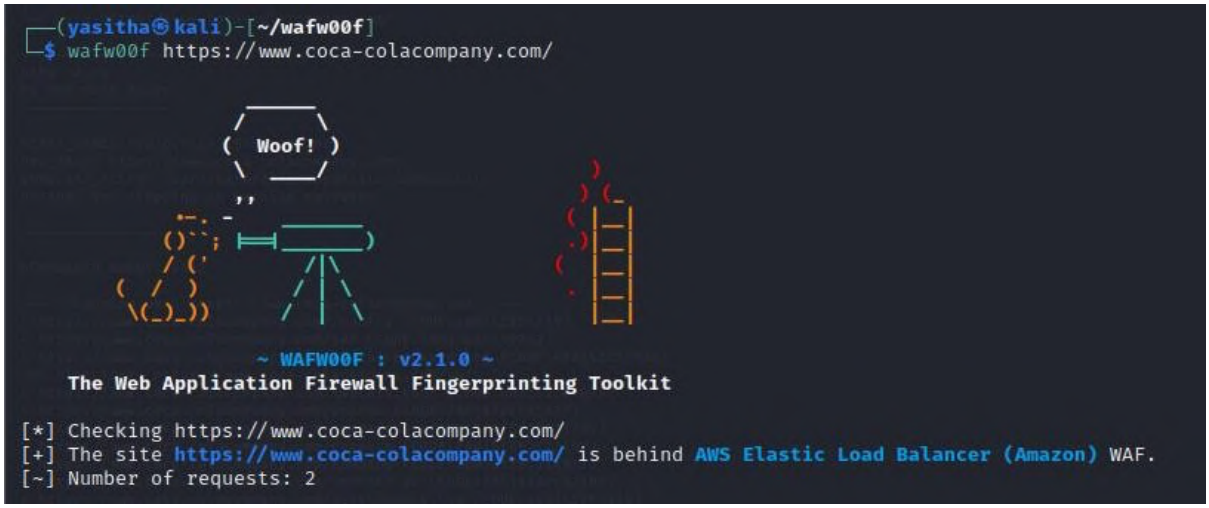
These are the directives found.

Fingerprinting web application firewalls

A web application firewall becomes another sort of firewall. A web application firewall monitors, filters, and blocks HTTP traffic as needed. Researchers have to learn regarding the actual firewall utilized in the objective since there are still bypassing flaws connected with this little particular web application firewall.

with WAFW00F

this tool can find in which firewall the site is behind.



In here the site is behind AWS Elastic Load Balancer (Amazon) firewall

Port scanning

Port scanning is a technique for identifying whether network ports are open and potentially getting or transmitting data. It is another method of delivering packets to specified ports on the server as well as evaluating the replies to exploitable weaknesses.

Via nmap

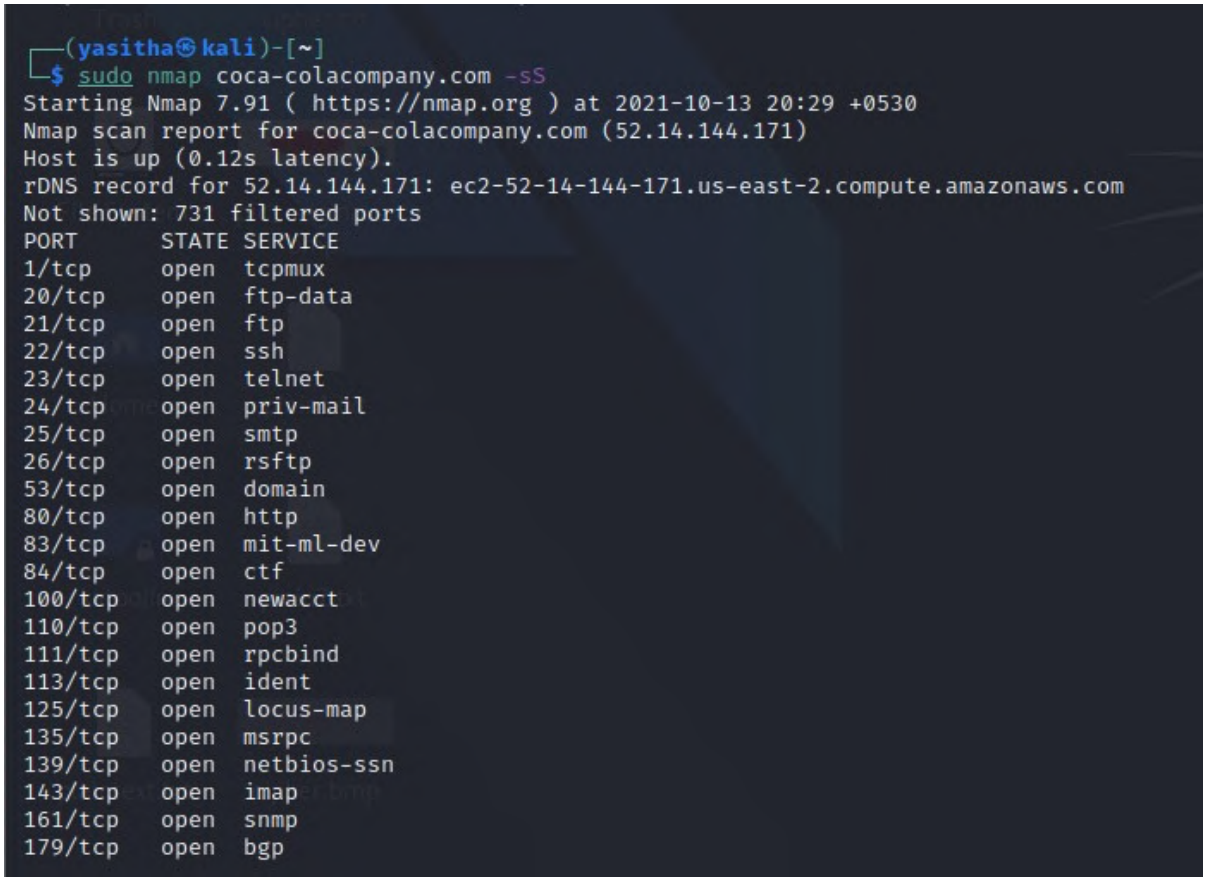
Nmap is the globe's most used network scanner for port security. This Nmap hosted vulnerability scanner can assist you in determining overall effectiveness of your basic security setup.

```
┌──(yasitha㉿kali)-[~]
└─$ nmap --help
Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
```

```
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

┌──(yasitha㉿kali)-[~]
```

In here I have used the command "**sudo nmap coca-colacompany.com -sS**"

-sS: TCP SYN/



VULNERABILITY ASSESMENT

A procedure of finding threats and hazards in networked computers, hardware, systems, applications, and other aspects of the IT environment is known as vulnerability assessment. Vulnerability assessments offer security staff as well as other users well with knowledge individuals have to identify and prioritize threats towards future repair inside the appropriate setting. Vulnerability assessments do an important part of the threat modeling and IT risk analysis life - cycles, since they serve protect safeguard network as well as information against illegal user access leaks. Vulnerability assessments typically leverage tools like vulnerability scanners to identify threats and flaws within an organization's IT infrastructure that represents possible weaknesses or hazards.

Why is this Vulnerability Assessments so necessary? Vulnerability assessments enable security staff to discover but also resolve security significant hazards in a consistent, thorough, as well as unambiguous manner. So this helps to:

- Quick but also reliable detection of IT cybersecurity incidents
- Corrective steps are being taken to fill any holes and secure critical information and systems.
- Safeguard yourself from privacy violations as well as other unwanted activities.

A vulnerability assessment investigates any broad variety of possible vulnerabilities throughout numerous networks, platforms, as well as other components of your on-premises but also clouds IT environment.

UTILIZED AUTOMATED TOOLS

Automation Testing Tools, also known as Test Automation Tools, are applications available that enable people in testing various pc, online, and mobile apps. These technologies offer automation options for automating the system testing. API testing, GUI testing, load testing, and are performance testing all capabilities among automated tools.

NETSPARKER PROFESSIONAL

Netsparker is an automatic, yet completely adjustable, online application vulnerability scanner which allows users to detect as well as discover security breaches in webpages, web apps, and online services. Netsparker helps to inspect various sorts of online applications, independent of technology or programming languages. Netsparker is the first online web application vulnerability analyzer which autonomously exposes detected flaws in a non-writable as well as secure manner to validate problems. It also provides evidence of the vulnerabilities; thus individuals don't have to spend energy manual process confirming it. Inside the instance of even a discovered SQL injection vulnerability, for instance, this will display the database file as evidence for exploitation.

These are the subdomains that I have been chosen.

- https://www.blueskysoda.com/
- https://www.fuzebev.com
- https://www.innocentdrinks.co.uk/
- https://www.vebatcoke.com/
- https://lk.coca-cola.com/en/home

1. Domain No01 : https://www.blueskysoda.com/

These are the vulnerabilities found throughout the scan

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Lodash)	GET	https://www.blueskysoda.com/tests	
	Out-of-date Version (Modernizr)	GET	https://www.blueskysoda.com/	
	Out-of-date Version (jQuery)	GET	https://www.blueskysoda.com/etc.clientlibs/clientlibs/granite/jquery.min.js	
	Weak Ciphers Enabled	GET	https://www.blueskysoda.com/	
	Cookie Not Marked as HttpOnly	GET	https://www.blueskysoda.com/	
	Cookie Not Marked as Secure	GET	https://www.blueskysoda.com/	
	Insecure Frame (External)	GET	https://www.blueskysoda.com/	
	Expect-CT Not Enabled	GET	https://www.blueskysoda.com/	
	Referrer-Policy Not Implemented	GET	https://www.blueskysoda.com/	
	Subresource Integrity (SRI) Not Implemented	GET	https://www.blueskysoda.com/	
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://www.blueskysoda.com/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://www.blueskysoda.com/	
	default-src Used in Content Security Policy (CSP)	GET	https://www.blueskysoda.com/	
	Forbidden Resource	POST	https://www.blueskysoda.com/	

a. Out-of-date Version (Lodash)

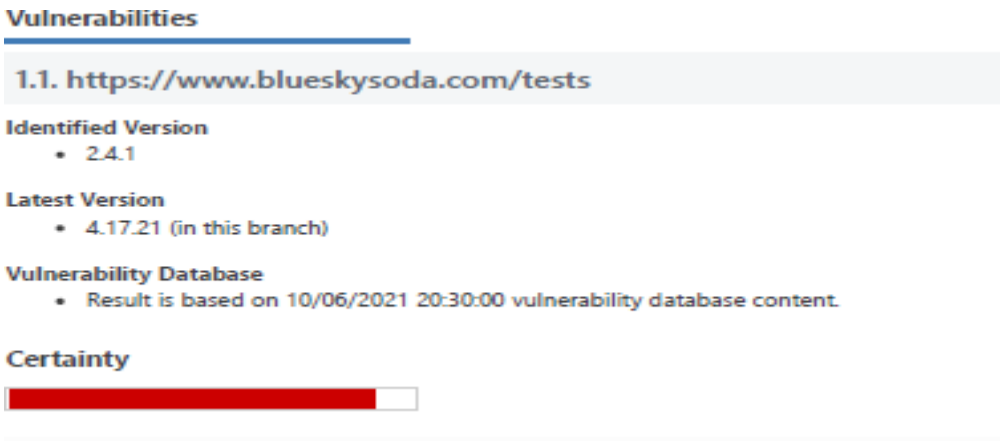
- **Risk : Critical**
- **Method : GET**
- **OWASP Top 10 Category : Top_10_2017-A9**

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

These are the vulnerabilities found regarding

- **Lodash Improper Neutralization of Special Elements used in a Command ('Command Injection') Vulnerability**
- **Lodash Other Vulnerability**
- **Lodash Prototype Pollution**
- **lodash Insufficient Information Vulnerability**
- **lodash Allocation of Resources Without Limits or Throttling Vulnerability**
- **lodash Insufficient Information Vulnerability**
- **lodash Allocation of Resources Without Limits or Throttling Vulnerability**
- **lodash Improper Input Validation Vulnerability**



Request

```
GET /tests HTTP/1.1
Host: www.blueskysoda.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: ps-location=6.9895%7C81.0557%7CLK%7C90000%7CBadulla%7CUva%20Province%7CBadulla%2C%20Uva%20Provi
nce%7C-1
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) : 455.7988 Total Bytes Received : 6489 Body Length : 5445 Is Compressed : No

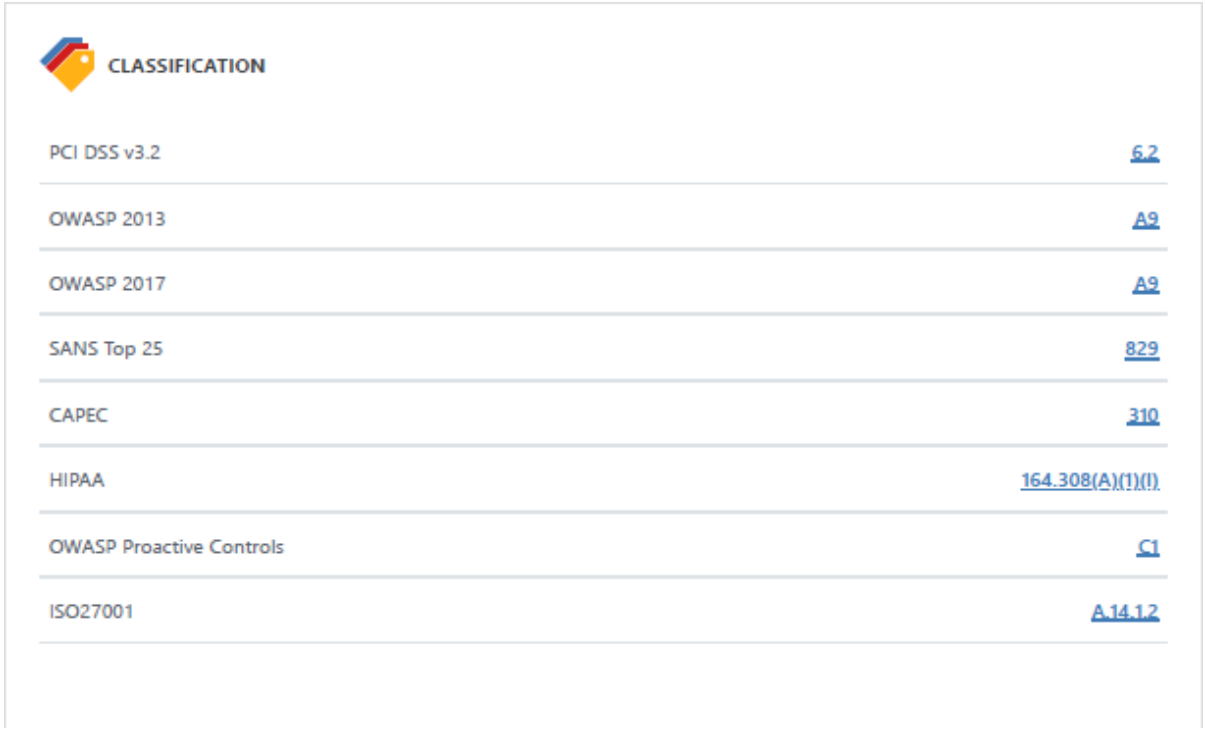
```
HTTP/1.1 200 OK
X-Cache: Miss from cloudfront
Cache-Control: max-age=86400
ETag: W/"226bb2258aa15d41f8eb28cb80b5f98a"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
x-amz-request-id: YGNWHAPN2GV38YA2
Server: CloudFront
X-Amz-Cf-Id: sDdIMvJ0kj1KpC4B7oeMT9dbvP8H8I0JtR_-zMrHhnUTlSgjCsEqaQ==
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Expires: Thu, 14 Oct 2021 06:11:50 GMT
X-Frame-Options: DENY
Vary: Accept-Encoding
Content-Encoding:
X-Amz-Cf-Pop: AMS50-C1
Via: 1.1 9463f100725b8b17da2d778617835761.cloudfront.net (CloudFront)
Last-Modified: Thu, 23 Apr 2020 15:31:38 GMT
Content-Type: text/html
x-amz-id-2: LXKCYi/B3RI5uB73xoJE8T0LkhmjDABx6c3uWpARWUpGuuCn+OReYaQRpu5M5/8iGTZwZCjTXXs=
x-ttl-custom: ttl=null
Content-Security-Policy: default-src https: data: blob: mediastream: 'unsafe-eval' 'unsafe-inline'; obj
ect-src 'none'; font-src https: data: 'self' 'unsafe-eval' 'unsafe-inline'
Date: Wed, 13 Oct 2021 06:11:51 GMT
Transfer-Encoding: chunked
```

```
<!DOCTYPE HTML>
<html lang="en">



<head>
    <meta charset="UTF-8"/>



    <link rel="canonical" href="https://tbd/tests"/>
```

```
     <meta property="og:url" content="https://tbd/tests"/>
     <meta property="content-path" content="/content/nagbrands/us/bluesky/en/tests"/>


     <meta name="template" content="content-page"/>
     <meta name="viewport" content="initial-scale=1, maximum-scale=1"/>



     <!-- OneTrust JS snippet -->



<!-- Google Tag Manager -->
<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-5SPB6DZ');</script>
<!-- End Google Tag Manager -->

—
```

Remedy

Upgrade your Lodash installation to the most recent stable version.



CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
SANS Top 25	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

b. Out-of-date Version (Modernizr)

- **Risk : High**
- **Method : GET**
- **OWASP Top 10 Category : Top_10_2017-A9**

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

These are the vulnerabilities found regarding

- Modernizr Sanitization bypass using HTML Entities

Vulnerabilities

2.1. https://www.blueskysoda.com/

Identified Version

- 2.8.3

Latest Version

- 3.11.8 (in this branch)

Vulnerability Database

- Result is based on 10/06/2021 20:30:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: www.blueskysoda.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) : 1406.2058 Total Bytes Received : 14377 Body Length : 13322 Is Compressed : No

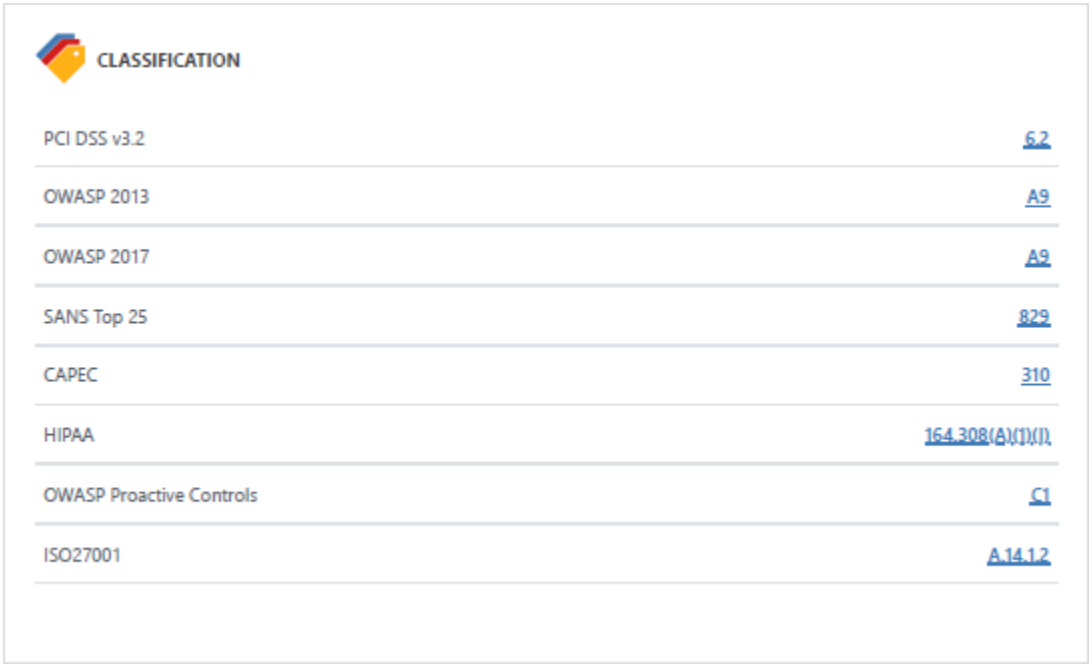
```
HTTP/1.1 200 OK
X-Cache: Hit from cloudfront
Age: 64339
Cache-Control: max-age=86400
ETag: W/"7471a375e962c13333e73136a9eb6944"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
x-amz-request-id: KM62JWGA32YJ2Y4V
Server: CloudFront
X-Amz-Cf-Id: JBylWBGTigfznWv-OrHRiCqr3Vsw1-oxRs61AQzRP8UVkBZXcFWttA==
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Expires: Wed, 13 Oct 2021 12:18:25 GMT
X-Frame-Options: DENY
Vary: Accept-Encoding
Content-Encoding:
X-Amz-Cf-Pop: AMS50-C1
Via: 1.1 559401aa49f4b835c1816ad004278e3e.cloudfront.net (CloudFront)
Last-Modified: Wed, 30 Jun 2021 15:39:38 GMT
Content-Type: text/html
x-amz-id-2: 18CeI0Bz1HM1phGLB20T4ADdFDmBydZgsvT8Dvupg4+Tf+rg8Z3sI1VLOhuSbCzeW0NDQv+g9Tg=
x-ttl-custom: ttl=null
Content-Security-Policy: default-src https: data: blob: mediastream: 'unsafe-eval' 'unsafe-inline'; obj
ect-src 'none'; font-src https: data: 'self' 'unsafe-eval' 'unsafe-inline'
Date: Tue, 12 Oct 2021 12:18:25 GMT
Transfer-Encoding: chunked
```

```
<!DOCTYPE HTML>
<html lang="en">




<head>

    <meta charset="UTF-8"/>



    <link rel="canonical" href="https://www.blueskysoda.com/home"/>
```

```
    <meta property="og:url" content="https://www.blueskysoda.com/home"/>
    <meta property="content-path" content="/content/nagbrands/us/bluesky/en/home"/>
        <meta name="ps-language" content="en"/>
<meta name="ps-country" content="US"/>
<meta name="ps-key" content="3983-5f7f7b3fff3815016a641064"/>


    <meta name="template" content="content-page"/>
    <meta name="viewport" content="initial-scale=1, maximum-scale=1"/>


        <link rel="preconnect" href="https://shared.coke.com"/>
        <link rel="preconnect" href="https://static.coke.com"/>
        <link rel="preconnect" href="https://use.typekit.net"/>


        <script>
            window.globalDataLayerObj = [{"tccc.attributes":{"tccc.dat
```

Remedy

Please update the Modernizr installation to the most recent stable version.



CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
SANS Top 25	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

c. Out-of-date Version (jQuery)

- **Risk : medium**
- **Method : GET**
- **OWASP Top 10 Category : Top_10_2017-A9**

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

These are the vulnerabilities found regarding

- jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
- JQuery Prototype Pollution Vulnerability

Vulnerabilities

3.1. https://www.blueskysoda.com/etc.clientlibs/clientlibs/granite/jquery.min.js

Identified Version
- 1.12.4

Latest Version
- 1.12.4 (in this branch)

Branch Status
- This branch has stopped receiving updates since 6/20/2016.

Vulnerability Database
- Result is based on 10/06/2021 20:30:00 vulnerability database content.

Certainty

Request

```
GET /etc.clientlibs/clientlibs/granite/jquery.min.js HTTP/1.1
Host: www.blueskysoda.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: ps-location=6.9895%7C81.0557%7CLK%7C90000%7CBadulla%7CUva%20Province%7CBadulla%2C%20Uva%20Provi
nce%7C-1
Referer: https://www.blueskysoda.com/tests
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) : 271.8311 Total Bytes Received : 114476 Body Length : 113314 Is Compressed : No

```
HTTP/1.1 200 OK
X-Cache: Hit from cloudfront
Age: 113
Cache-Control: max-age=7776000
ETag: W/"772fb04d4ce536dfb06c17e789ad4dbd"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
x-amz-request-id: YNMDYGPAMR7EFTA5
X-Amz-Cf-Pop: AMS50-C1
x-amz-meta-gid: 48
Server: CloudFront
X-Amz-Cf-Id: TrDYwdZHUaA1o_oC274zqjmVrrAgTYXV0X5KhPyd53JNMbM4KhsAxw==
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Expires: Tue, 11 Jan 2022 06:12:30 GMT
x-amz-id-2: 3GCbKI0u5BeIHUxdRQ2zZdcDULSPCZVzSVoyTiWuLuoA6TFjjyd766KL9i+F/7uip3zz2OCoswU=
x-ttl-custom: ttl=null
Content-Encoding:
Vary: Accept-Encoding
Via: 1.1 3c01812e357a7900959ea67a1c5782ad.cloudfront.net (CloudFront)
x-amz-meta-uid: 48
Last-Modified: Wed, 08 Apr 2020 19:45:10 GMT
Content-Type: application/javascript
x-amz-meta-mtime: 1586375107
x-amz-meta-mode: 33188
X-Frame-Options: DENY
Content-Security-Policy: default-src https: data: blob: mediastream: 'unsafe-eval' 'unsafe-inline'; obj
ect-src 'none'; font-src https: data: 'self' 'unsafe-eval' 'unsafe-inline'
Date: Wed, 13 Oct 2021 06:12:30 GMT
Transfer-En
…
lob: mediastream: 'unsafe-eval' 'unsafe-inline'; object-src 'none'; font-src https: data: 'self' 'unsaf
e-eval' 'unsafe-inline'
Date: Wed, 13 Oct 2021 06:12:30 GMT
Transfer-Encoding: chunked
```

```
/*!
 * jQuery JavaScript Library v1.12.4-aem
 * http://jquery.com/
 *
 * Includes Sizzle.js
 * http://sizzlejs.com/
 *
 * Copyright jQuery Foundation and other contributors
 * Released under the MIT license
 * http://jquery.org/license
 *
```

```
* Da
…
```

Remedy

Upgrade your jQuery installation to the most recent stable version.

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
SANS Top 25	829
CAPEC	310
HIPAA	164.308(A)(1)(I),
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

d. Weak Ciphers Enabled –Confirmed

- **Risk : Medium**
- **OWASP Top 10 Category : Top_10_2017-A3**

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

4.1. https://www.blueskysoda.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)

Request

```
[NETSPARKER] SSL Connection
```

Response

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

```
[NETSPARKER] SSL Connection
```

Actions to Take

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

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

2. Lighttpd:

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

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
   b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c. Set "Enabled" DWORD to "0x0" for the following registry keys:

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

Remedy

Simply ban the use of weaker ciphers on the web server.

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

e. Cookie Not Marked as HttpOnly – Confirmed

- **Risk : Low**
- **Method : GET**
- **OWASP Top 10 Category : Top_10_2017-A6**

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

5.1. https://www.blueskysoda.com/

CONFIRMED

Identified Cookie(s)

- ps-location
- ps-uid

Cookie Source

- JavaScript

Request

```
GET / HTTP/1.1
Host: www.blueskysoda.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) : 1406.2058 Total Bytes Received : 14377 Body Length : 13322 Is Compressed : No

```
HTTP/1.1 200 OK
X-Cache: Hit from cloudfront
Age: 64339
Cache-Control: max-age=86400
ETag: W/"7471a375e962c13333e73136a9eb6944"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
x-amz-request-id: KM62JWGA32YJ2Y4V
Server: CloudFront
X-Amz-Cf-Id: JBylWBGTigfznWv-OrHRiCqr3Vsw1-oxRs61AQzRP8UVkBZXcFWttA==
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Expires: Wed, 13 Oct 2021 12:18:25 GMT
X-Frame-Options: DENY
Vary: Accept-Encoding
Content-Encoding:
X-Amz-Cf-Pop: AMS50-C1
Via: 1.1 559401aa49f4b835c1816ad004278e3e.cloudfront.net (CloudFront)
Last-Modified: Wed, 30 Jun 2021 15:39:38 GMT
Content-Type: text/html
x-amz-id-2: 18CeI0Bz1HM1phGLB20T4ADdFDmBydZgsvT8Dvupg4+Tf+rg8Z3sI1VLOhuSbCzeW0NDQv+g9Tg=
x-ttl-custom: ttl=null
Content-Security-Policy: default-src https: data: blob: mediastream: 'unsafe-eval' 'unsafe-inline'; obj
ect-src 'none'; font-src https: data: 'self' 'unsafe-eval' 'unsafe-inline'
Date: Tue, 12 Oct 2021 12:18:25 GMT
Transfer-Encoding: chunked
```

```
<!DOCTYPE HTML>
<html lang="en">




<head>

    <meta charset="UTF-8"/>



    <link rel="canonical" href="https://www.blueskysoda.com/home"/>
```

```
    <meta property="og:url" content="https://www.blueskysoda.com/home"/>
    <meta property="content-path" content="/content/nagbrands/us/bluesky/en/home"/>
        <meta name="ps-language" content="en"/>
<meta name="ps-country" content="US"/>
<meta name="ps-key" content="3983-5f7f7b3fff3815016a641064"/>


    <meta name="template" content="content-page"/>
    <meta name="viewport" content="initial-scale=1, maximum-scale=1"/>


        <link rel="preconnect" href="https://shared.coke.com"/>
        <link rel="preconnect" href="https://static.coke.com"/>
        <link rel="preconnect" href="https://use.typekit.net"/>


        <script>
            window.globalDataLayerObj = [{"tccc.attributes":{"tccc.dat
…
```

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTPOnly protection.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
CAPEC	107
WASC	15
ISO27001	A.14.2.5

f. Cookie Not Marked as Secure – Confirmed

- **Risk : Low**
- **Method : GET**
- **OWASP Top 10 Category : Top_10_2017-A6**

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

Impact

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Vulnerabilities

6.1. https://www.blueskysoda.com/

CONFIRMED

Identified Cookie(s)

- ps-location
- ps-uid

Cookie Source

- JavaScript

Request

```
GET / HTTP/1.1
Host: www.blueskysoda.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) : 1406.2058 Total Bytes Received : 14377 Body Length : 13322 Is Compressed : No

```
HTTP/1.1 200 OK
X-Cache: Hit from cloudfront
Age: 64339
Cache-Control: max-age=86400
ETag: W/"7471a375e962c13333e73136a9eb6944"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
x-amz-request-id: KM62JWGA32YJ2Y4V
Server: CloudFront
X-Amz-Cf-Id: JBylWBGTigfznWv-OrHRiCqr3Vsw1-oxRs61AQzRP8UVkBZXcFWttA==
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Expires: Wed, 13 Oct 2021 12:18:25 GMT
X-Frame-Options: DENY
Vary: Accept-Encoding
Content-Encoding:
X-Amz-Cf-Pop: AMS50-C1
Via: 1.1 559401aa49f4b835c1816ad004278e3e.cloudfront.net (CloudFront)
Last-Modified: Wed, 30 Jun 2021 15:39:38 GMT
Content-Type: text/html
x-amz-id-2: 18CeI0Bz1HM1phGLB20T4ADdFDmBydZgsvT8Dvupg4+Tf+rg8Z3sI1VLOhuSbCzeW0NDQv+g9Tg=
x-ttl-custom: ttl=null
Content-Security-Policy: default-src https: data: blob: mediastream: 'unsafe-eval' 'unsafe-inline'; obj
ect-src 'none'; font-src https: data: 'self' 'unsafe-eval' 'unsafe-inline'
Date: Tue, 12 Oct 2021 12:18:25 GMT
Transfer-Encoding: chunked
```

```
<!DOCTYPE HTML>
<html lang="en">




<head>

    <meta charset="UTF-8"/>



    <link rel="canonical" href="https://www.blueskysoda.com/home"/>
```

```
    <meta property="og:url" content="https://www.blueskysoda.com/home"/>
    <meta property="content-path" content="/content/nagbrands/us/bluesky/en/home"/>
        <meta name="ps-language" content="en"/>
<meta name="ps-country" content="US"/>
<meta name="ps-key" content="3983-5f7f7b3fff3815016a641064"/>


    <meta name="template" content="content-page"/>
    <meta name="viewport" content="initial-scale=1, maximum-scale=1"/>


        <link rel="preconnect" href="https://shared.coke.com"/>
        <link rel="preconnect" href="https://static.coke.com"/>
        <link rel="preconnect" href="https://use.typekit.net"/>


        <script>
            window.globalDataLayerObj = [{"tccc.attributes":{"tccc.dat
…
```

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to be understand layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.

CLASSIFICATION

PCI DSS v3.2	6.5.10
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	614
CAPEC	102
WASC	15
ISO27001	A.14.1.2

CVSS 3.0 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String
CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE	
Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String
CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

g. Insecure Frame (External) – Confirmed

- **Risk : Low**
- **Method : GET**
- **OWASP Top 10 Category : Top_10_2017-A6**

Impact

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 *http://site.com* :

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)

When the `sandbox` attribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the `sandbox` attribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the iframe.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

`Sandbox` containing a value of :

- `allow-same-origin` will not treat it as a unique origin.
- `allow-top-navigation` will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.
- `allow-forms` will allow form submissions from inside the iframe.
- `allow-popups` will allow popups.
- `allow-scripts` will allow malicious script execution however it won't allow to create popups.

Vulnerabilities

7.1. https://www.blueskysoda.com/

CONFIRMED

Frame Source(s)

- https://www.googletagmanager.com/ns.html?id=GTM-5SPB6DZ

Request

```
GET / HTTP/1.1
Host: www.blueskysoda.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) : 1406.2058 Total Bytes Received : 14377 Body Length : 13322 Is Compressed : No

```
HTTP/1.1 200 OK
X-Cache: Hit from cloudfront
Age: 64339
Cache-Control: max-age=86400
ETag: W/"7471a375e962c13333e73136a9eb6944"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
x-amz-request-id: KM62JWGA32YJ2Y4V
Server: CloudFront
X-Amz-Cf-Id: JBylWBGTigfznWv-OrHRiCqr3Vsw1-oxRs61AQzRP8UVkBZXcFWttA==
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Expires: Wed, 13 Oct 2021 12:18:25 GMT
X-Frame-Options: DENY
Vary: Accept-Encoding
Content-Encoding:
X-Amz-Cf-Pop: AMS50-C1
Via: 1.1 559401aa49f4b835c1816ad004278e3e.cloudfront.net (CloudFront)
Last-Modified: Wed, 30 Jun 2021 15:39:38 GMT
Content-Type: text/html
x-amz-id-2: 18CeI0Bz1HM1phGLB20T4ADdFDmBydZgsvT8Dvupg4+Tf+rg8Z3sI1VLOhuSbCzeW0NDQv+g9Tg=
x-ttl-custom: ttl=null
Content-Security-Policy: default-src https: data: blob: mediastream: 'unsafe-eval' 'unsafe-inline'; obj
ect-src 'none'; font-src https: data: 'self' 'unsafe-eval' 'unsafe-inline'
Date: Tue, 12 Oct 2021 12:18:25 GMT
Transfer-En
…
nit="united-states" data-dataLayer-page-language="en-US" data-dataLayer-page-country="united-states-of-
america" data-genericLocale="sq_AL" data-experience="nagbrands">


        <noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-5SPB6DZ"
height="0" width="0" style="display:none;visibility:hidden"></iframe></noscript>
```

```
<a name="top_of_page"></a>
<div class="root responsivegrid">


<div clas
…
```

Remedy

- Apply sandboxing in inline frame

```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of `seamless` attribute and `allow-top-navigation`, `allow-popups` and `allow-scripts` in sandbox attribute.

CLASSIFICATION

OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

h. Forbidden Resource – Confirmed

- **Risk** : INFORMATION
- **Method** : **GET**

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

14.1. https://www.blueskysoda.com/

CONFIRMED

Request

```
POST / HTTP/1.1
Host: www.blueskysoda.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
Content-Length: 124
Content-Type: application/xml
Cookie: ps-location=6.9895%7C81.0557%7CLK%7C90000%7CBadulla%7CUva%20Province%7CBadulla%2C%20Uva%20Provi
nce%7C-1
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 "data:;base64,TlM3NzU0NTYxNDQ2N
Tc1">]><ns>&lfi;</ns>
```

Response

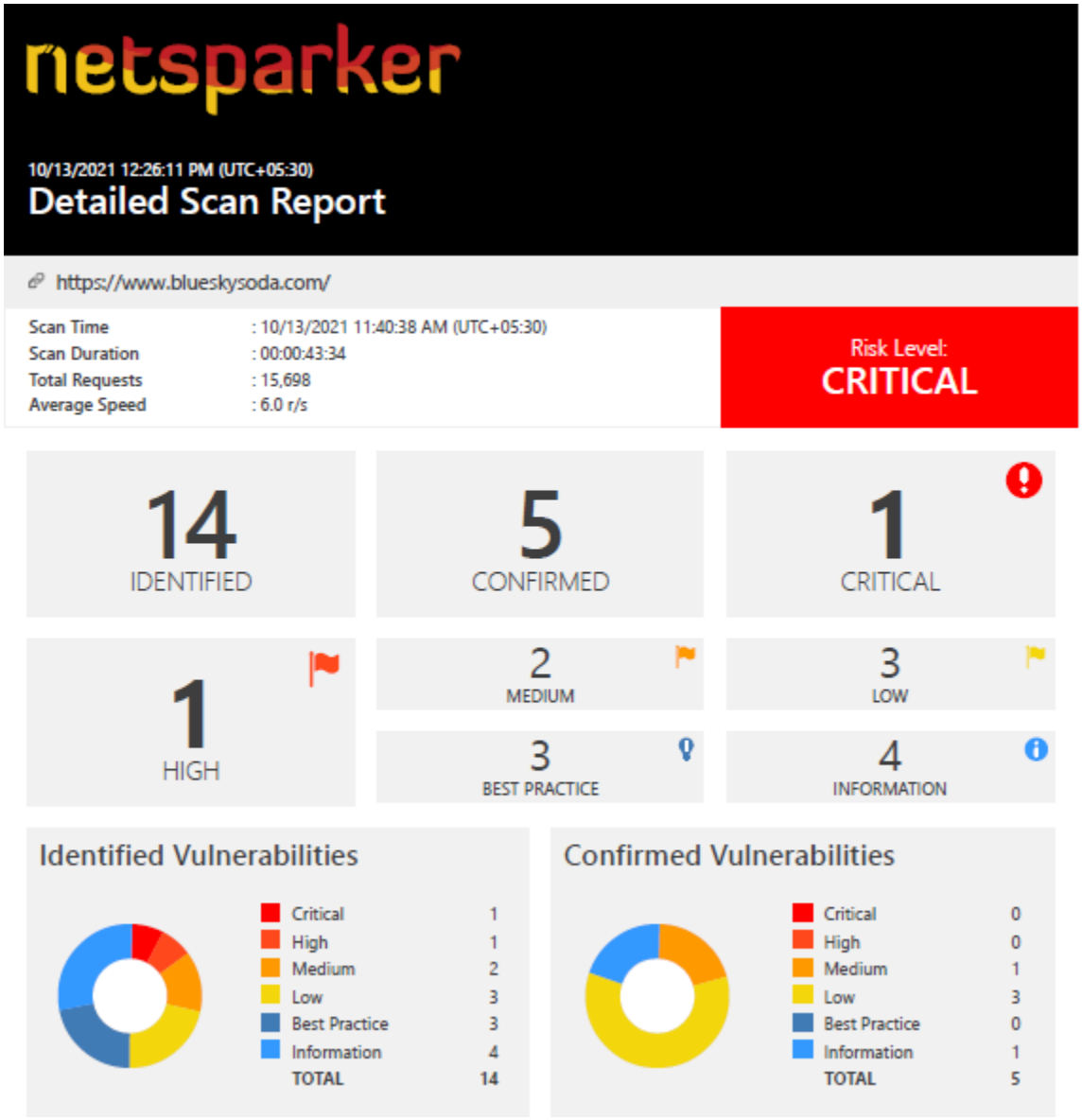
Response Time (ms) : 180.8935 Total Bytes Received : 1405 Body Length : 1053 Is Compressed : No

```
HTTP/1.1 403 Forbidden

Server: CloudFront
X-Amz-Cf-Id: OI8kZIAh9-GtMULOcWzE8X3nga6tsqcqG4BVZSKBQp_DWfpqs84-tA==
Connection: keep-alive
Via: 1.1 ac979e099d122e39d3a8fac95688a69a.cloudfront.net (CloudFront)
Content-Length: 1053
X-Cache: Error from cloudfront
Content-Type: text/html
X-Amz-Cf-Pop: AMS50-C1
Date: Wed, 13 Oct 2021 06:11:52 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<HTML><HEAD><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<TITLE>ERROR: The request could not be satisfied</TITLE>
</HEAD><BODY>
<H1>403 ERROR</H1>
<H2>The request could not be satisfied.</H2>
<HR noshade size="1px">
This distribution is not configured to allow the HTTP request method that was used for this request. Th
e distribution supports only cachable requests.
We can't connect to the server for this app or website at this time. There might be too much traffic or
 a configuration error. Try again later, or contact the app or website owner.
<BR clear="all">
If you provide content to customers through CloudFront, you can find steps to troubleshoot and help pre
vent this error by reviewing the CloudFront documentation.
<BR clear="all">
<HR noshade size="1px">
<PRE>
Generated by cloudfront (CloudFront)
Request ID: OI8kZIAh9-GtMULOcWzE8X3nga6tsqcqG4BVZSKBQp_DWfpqs84-tA==
</PRE>
<ADDRESS>
</ADDRESS>
</BODY></HTML>
```

CLASSIFICATION

OWASP Proactive Controls	C8
ISO27001	A.8.1.1

Summary of this Domain



2. Domain No02 : https://www.fuzebev.com

These are the vulnerabilities found

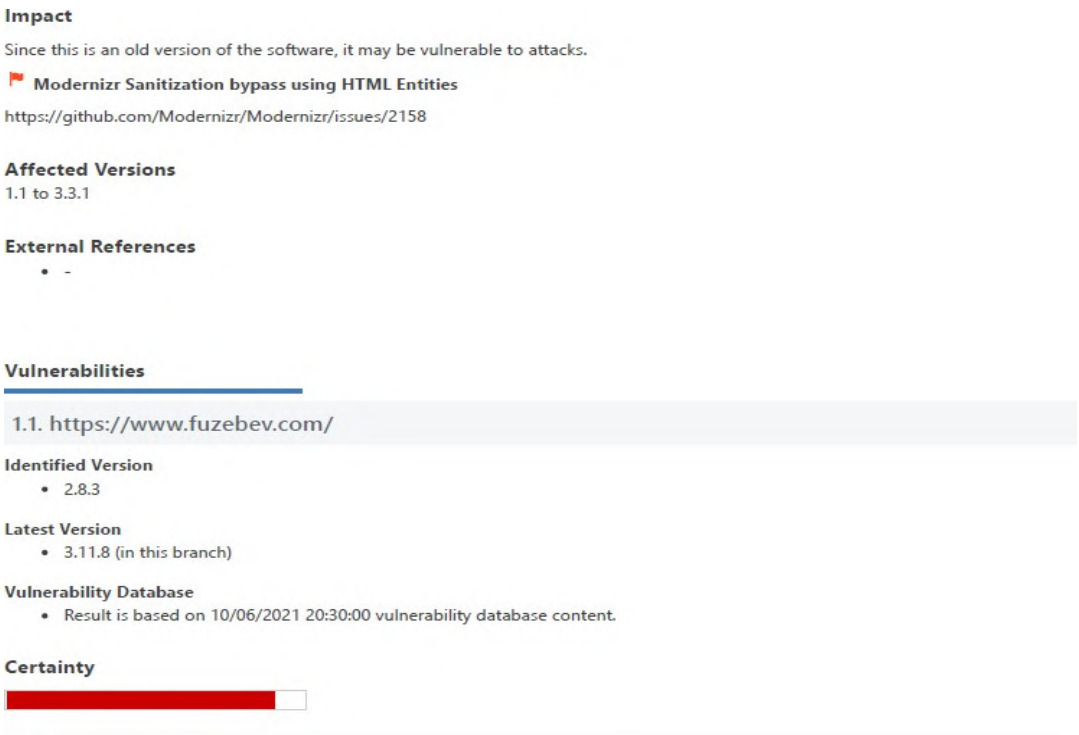
CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Modernizr)	GET	https://www.fuzebev.com/	
	Weak Ciphers Enabled	GET	https://www.fuzebev.com/	
	Cookie Not Marked as HttpOnly	GET	https://www.fuzebev.com/#mainContent	
	Cookie Not Marked as Secure	GET	https://www.fuzebev.com/#mainContent	
	Insecure Frame (External)	GET	https://www.fuzebev.com/	
	Expect-CT Not Enabled	GET	https://www.fuzebev.com/	
	Referrer-Policy Not Implemented	GET	https://www.fuzebev.com/	
	Subresource Integrity (SRI) Not Implemented	GET	https://www.fuzebev.com/	
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://www.fuzebev.com/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://www.fuzebev.com/	
	default-src Used in Content Security Policy (CSP)	GET	https://www.fuzebev.com/	
	Email Address Disclosure	GET	https://www.fuzebev.com/support	
	Out-of-date Version (jQuery)	GET	https://www.fuzebev.com/	
	Forbidden Resource	POST	https://www.fuzebev.com/	

a. Out-of-date Version (Modernizr)

Risk : **High**

Method : **GET**

OWASP Top 10 Category : **Top_10_2017-A9**



Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Modernizr Sanitization bypass using HTML Entities

https://github.com/Modernizr/Modernizr/issues/2158

Affected Versions

1.1 to 3.3.1

External References

- -

Vulnerabilities

1.1. https://www.fuzebev.com/

Identified Version

- 2.8.3

Latest Version

- 3.11.8 (in this branch)

Vulnerability Database

- Result is based on 10/06/2021 20:30:00 vulnerability database content.

Certainty

Remedy

Please upgrade your installation of Modernizr to the latest stable version.

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
SANS Top 25	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

b. Weak Ciphers Enabled – Confirmed

Risk : Medium

Method : GET

OWASP Top 10 Category : Top_10_2017-A3

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

2.1. https://www.fuzebev.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)

Request

```
[NETSPARKER] SSL Connection
```

Response

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

```
[NETSPARKER] SSL Connection
```

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

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
   b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c. Set "Enabled" DWORD to "0x0" for the following registry keys:

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

Remedy

Configure your web server to disallow using weak ciphers.

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

c. Cookie Not Marked as HttpOnly - Confirmed

- **Risk : Low**
- **Method : GET**
- **OWASP Top 10 Category : Top_10_2017-A6**

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

3.1. https://www.fuzebev.com/#mainContent

CONFIRMED

Identified Cookie(s)

- ps-location

Cookie Source

- JavaScript

Request

```
GET /#mainContent HTTP/1.1
Host: www.fuzebev.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: ps-location=6.9895%7C81.0557%7CLK%7C90000%7CBadulla%7CUva%20Province%7CBadulla%2C%20Uva%20Provi
nce%7C-1
Referer: https://www.fuzebev.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) : 240.2208 Total Bytes Received : 59804 Body Length : 58749 Is Compressed : No

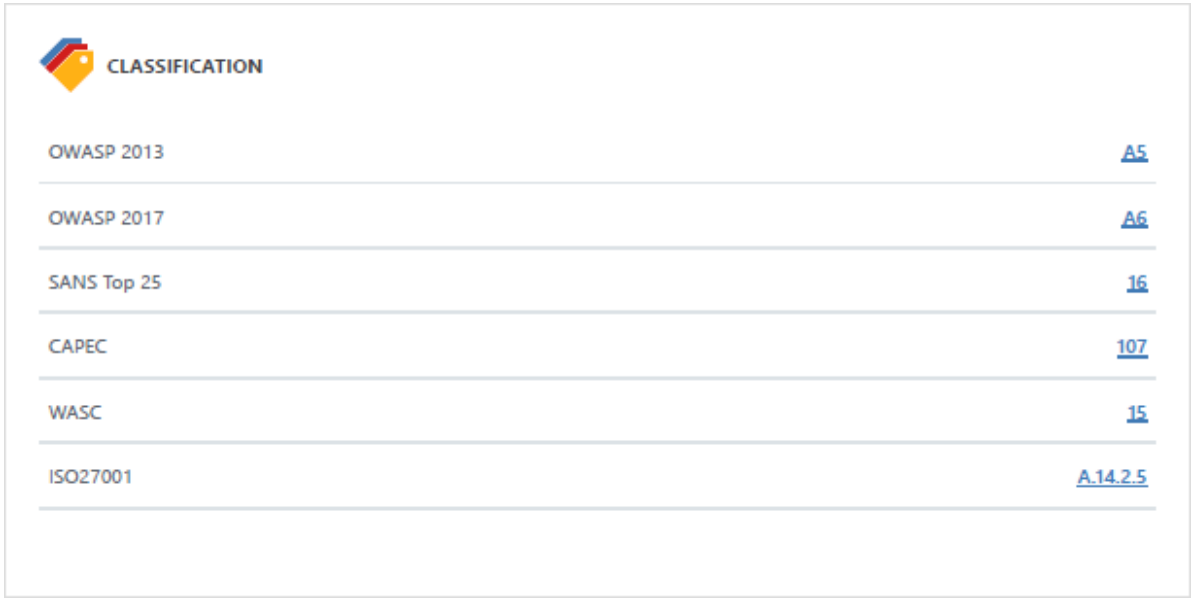
```
HTTP/1.1 200 OK
X-Cache: Hit from cloudfront
Age: 54801
Cache-Control: max-age=86400
ETag: W/"bc651274eedcb7b82ee5621733fa3bdb"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
x-amz-request-id: 74P4333KNT9MPRD1
X-Amz-Cf-Pop: ZRH50-C1
Server: CloudFront
X-Amz-Cf-Id: qICM2ZcdA4l7K4drOxsd2YSkJJFnpAkbge8KdZhZhUlrmIvayTUPsA==
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Expires: Wed, 13 Oct 2021 06:54:29 GMT
X-Frame-Options: DENY
Vary: Accept-Encoding
Transfer-Encoding: chunked
Via: 1.1 25d46f0dbca17b9a78cca036e17d8ad3.cloudfront.net (CloudFront)
Last-Modified: Thu, 10 Jun 2021 14:55:42 GMT
Content-Type: text/html
x-amz-id-2: M6M0nafbNOJWMChnix9MPnyqw8H4tgavjaPqn3A4jheQEamjcjo3MEIMSe3GYsc/curePC/UfXA=
x-ttl-custom: ttl=null
Content-Security-Policy: default-src https: data: blob: mediastream: 'unsafe-eval' 'unsafe-inline'; obj
ect-src 'none'; font-src https: data: 'self' 'unsafe-eval' 'unsafe-inline'
Date: Tue, 12 Oct 2021 06:54:30 GMT
Content-Encoding:
```

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTPOnly protection.



CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
CAPEC	107
WASC	15
ISO27001	A.14.2.5

d. Cookie Not Marked as Secure – Confirmed

- **Risk : Low**
- **Method : GET**
- **OWASP Top 10 Category : Top_10_2017-A3**

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

Impact

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Vulnerabilities

4.1. https://www.fuzebev.com/#mainContent

CONFIRMED

Identified Cookie(s)

- ps-location

Cookie Source

- JavaScript

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to be understand layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.

CLASSIFICATION

PCI DSS v3.2	6.5.10
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	614
CAPEC	102
WASC	15
ISO27001	A.14.1.2

CVSS 3.0 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String

CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String

CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

e. Insecure Frame (External) - Confirmed

- **Risk : Low**
- **Method : GET**
- **OWASP Top 10 Category : Top_10_2017-A6**

Impact

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.

Vulnerabilities

5.1. https://www.fuzebev.com/

CONFIRMED

Frame Source(s)

- //www.googletagmanager.com/ns.html?id=GTM-MJBLR5M

Remedy

- Apply sandboxing in inline frame

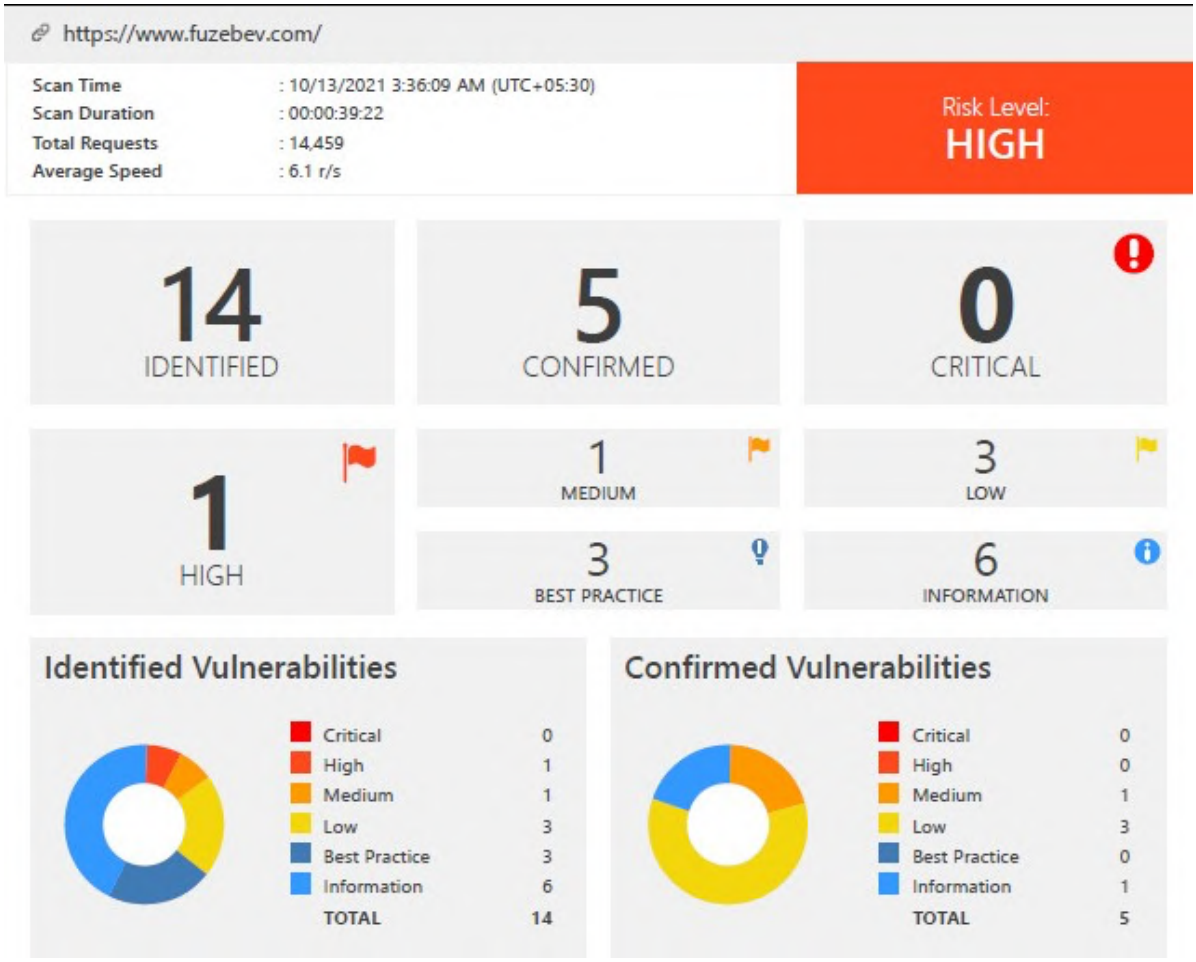
```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of `seamless` attribute and `allow-top-navigation`, `allow-popups` and `allow-scripts` in sandbox attribute.

CLASSIFICATION

OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

Summary of the Scan



3. Domain No03 : https://www.innocentdrinks.co.uk/

These are the vulnerabilities found from the scan.

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Modernizr)	GET	https://www.innocentdrinks.co.uk/	
	Weak Ciphers Enabled	GET	https://www.innocentdrinks.co.uk/	
	Cookie Not Marked as HttpOnly	GET	https://www.innocentdrinks.co.uk/	
	Cookie Not Marked as Secure	GET	https://www.innocentdrinks.co.uk/	
	Insecure Frame (External)	GET	https://www.innocentdrinks.co.uk/content/	
	Expect-CT Not Enabled	GET	https://www.innocentdrinks.co.uk/	
	Referrer-Policy Not Implemented	GET	https://www.innocentdrinks.co.uk/	
	Subresource Integrity (SRI) Not Implemented	GET	https://www.innocentdrinks.co.uk/	
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://www.innocentdrinks.co.uk/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://www.innocentdrinks.co.uk/	
	Email Address Disclosure	GET	https://www.innocentdrinks.co.uk/a-bit-about-us	
	Generic Email Address Disclosure	GET	https://www.innocentdrinks.co.uk/get-in-touch?nsextt=%2522%252bnetsparker(0x00F966)%252b%2522	nsextt
	Missing object-src in CSP Declaration	GET	https://www.innocentdrinks.co.uk/	
	Out-of-date Version (jQuery)	GET	https://www.innocentdrinks.co.uk/	
	Web Application Firewall Detected	GET	https://www.innocentdrinks.co.uk/%3Cscript%3Ealert(0)%3C/script%3E	URI-BASED

Same vulnerabilities were found even in this Subdomain

Summary of the scan

https://www.innocentdrinks.co.uk/

Scan Time	: 10/13/2021 12:58:45 PM (UTC+05:30)
Scan Duration	: 00:00:30:59
Total Requests	: 7,255
Average Speed	: 3.9 r/s

Risk Level: HIGH

17 IDENTIFIED	5 CONFIRMED	0 CRITICAL
1 HIGH	1 MEDIUM	3 LOW
	3 BEST PRACTICE	9 INFORMATION

Identified Vulnerabilities

Critical	0
High	1
Medium	1
Low	3
Best Practice	3
Information	9
TOTAL	17

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	3
Best Practice	0
Information	1
TOTAL	5

4. Domain no04 : https://www.vebatcoke.com/

These are the vulnerabilities found

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Modernizr)	GET	https://www.vebatcoke.com/	
	Weak Ciphers Enabled	GET	https://www.vebatcoke.com/	
	Insecure Frame (External)	GET	https://www.vebatcoke.com/	
	Expect-CT Not Enabled	GET	https://www.vebatcoke.com/	
	Referrer-Policy Not Implemented	GET	https://www.vebatcoke.com/	
	Subresource Integrity (SRI) Not Implemented	GET	https://www.vebatcoke.com/	
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://www.vebatcoke.com/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://www.vebatcoke.com/	
	default-src Used in Content Security Policy (CSP)	GET	https://www.vebatcoke.com/	
	Out-of-date Version (jQuery)	GET	https://www.vebatcoke.com/	
	Forbidden Resource	POST	https://www.vebatcoke.com/	
	Robots.txt Detected	GET	https://www.vebatcoke.com/robots.txt	

a. Robots.txt Detected

- **Risk** : INFORMATION
- **Method** : **GET**

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.

Vulnerabilities

12.1. https://www.vebatcoke.com/robots.txt

CONFIRMED

Interesting Robots.txt Entries

- Disallow:
- Sitemap: https://vebatcoke.com/sitemap.xml

Request

```
GET /robots.txt HTTP/1.1
Host: www.vebatcoke.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) : 217.0323 Total Bytes Received : 1067 Body Length : 68 Is Compressed : No

```
HTTP/1.1 200 OK
X-Cache: Hit from cloudfront
Age: 3
Cache-Control: max-age=86400
ETag: "cb09781c054df8f2233393ef36a864bd"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
x-amz-request-id: AZQZVT14P7ZM6ENP
Server: CloudFront
X-Amz-Cf-Id: zfbNGXFRdhGn_SH47-7mH64KN7xlSbTVIbMk1OnrEPUNvAzTFBGyqg==
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Expires: Thu, 14 Oct 2021 08:31:48 GMT
x-amz-id-2: 0cc/QnbX5C7mWzjEDdUOxPRpJd1LFgXkh7I2xa2/It4XFeomomrw5vGyxC8O3W3RA04BnnDssxc=
Content-Length: 68
X-Amz-Cf-Pop: AMS54-C1
Via: 1.1 eec12a22159207af63748eccf10799b3.cloudfront.net (CloudFront)
Last-Modified: Mon, 09 Aug 2021 14:35:14 GMT
Content-Type: text/plain
x-ttl-custom: ttl=null
X-Frame-Options: DENY
Content-Security-Policy: default-src https: data: blob: mediastream: 'unsafe-eval' 'unsafe-inline'; obj
ect-src 'none'; font-src https: data: 'self' 'unsafe-eval' 'unsafe-inline'
Date: Wed, 13 Oct 2021 08:31:49 GMT

User-agent: *
Disallow:

Sitemap: https://vebatcoke.com/sitemap.xml
```

Remedy

Ensure you have nothing sensitive exposed within this file, such as the path of an administration panel. If disallowed paths are sensitive and you want to keep it from unauthorized access, do not write them in the `Robots.txt`, and ensure they are correctly protected by means of authentication.
`Robots.txt` is only used to instruct search robots which resources should be indexed and which ones are not.

The following block can be used to tell the crawler to index files under /web/ and **ignore the rest**:

```
User-Agent: *
Allow: /web/
Disallow: /
```

Please note that when you use the instructions above, **search engines will not index your website** except for the specified directories.

If you want to hide certain section of the website from the search engines `X-Robots-Tag` can be set in the response header to tell crawlers whether the file should be indexed or not:

```
X-Robots-Tag: googlebot: nofollow
X-Robots-Tag: otherbot: noindex, nofollow
```

By using `X-Robots-Tag` you don't have to list the these files in your `Robots.txt`.

It is also not possible to prevent media files from being indexed by putting using Robots Meta Tags. `X-Robots-Tag` resolves this issue as well.

For Apache, the following snippet can be put into `httpd.conf` or an `.htaccess` file to restrict crawlers to index multimedia files without exposing them in `Robots.txt`

```
<Files ~ "\.pdf$">
 # Don't index PDF files.
 Header set X-Robots-Tag "noindex, nofollow"
</Files>
```

```
<Files ~ "\.(png|jpe?g|gif)$">
 #Don't index image files.
 Header set X-Robots-Tag "noindex"
</Files>
```

CLASSIFICATION

OWASP Proactive Controls	C7
ISO27001	A.18.1.3

Summary of the scan

https://www.vebatcoke.com/

Scan Time	: 10/13/2021 2:01:14 PM (UTC+05:30)
Scan Duration	: 00:00:15:20
Total Requests	: 6,941
Average Speed	: 7.5 r/s

Risk Level: HIGH

12 IDENTIFIED	4 CONFIRMED	0 CRITICAL
1 HIGH	1 MEDIUM	1 LOW
	3 BEST PRACTICE	6 INFORMATION

Identified Vulnerabilities

Critical	0
High	1
Medium	1
Low	1
Best Practice	3
Information	6
TOTAL	12

Confirmed Vulnerabilities

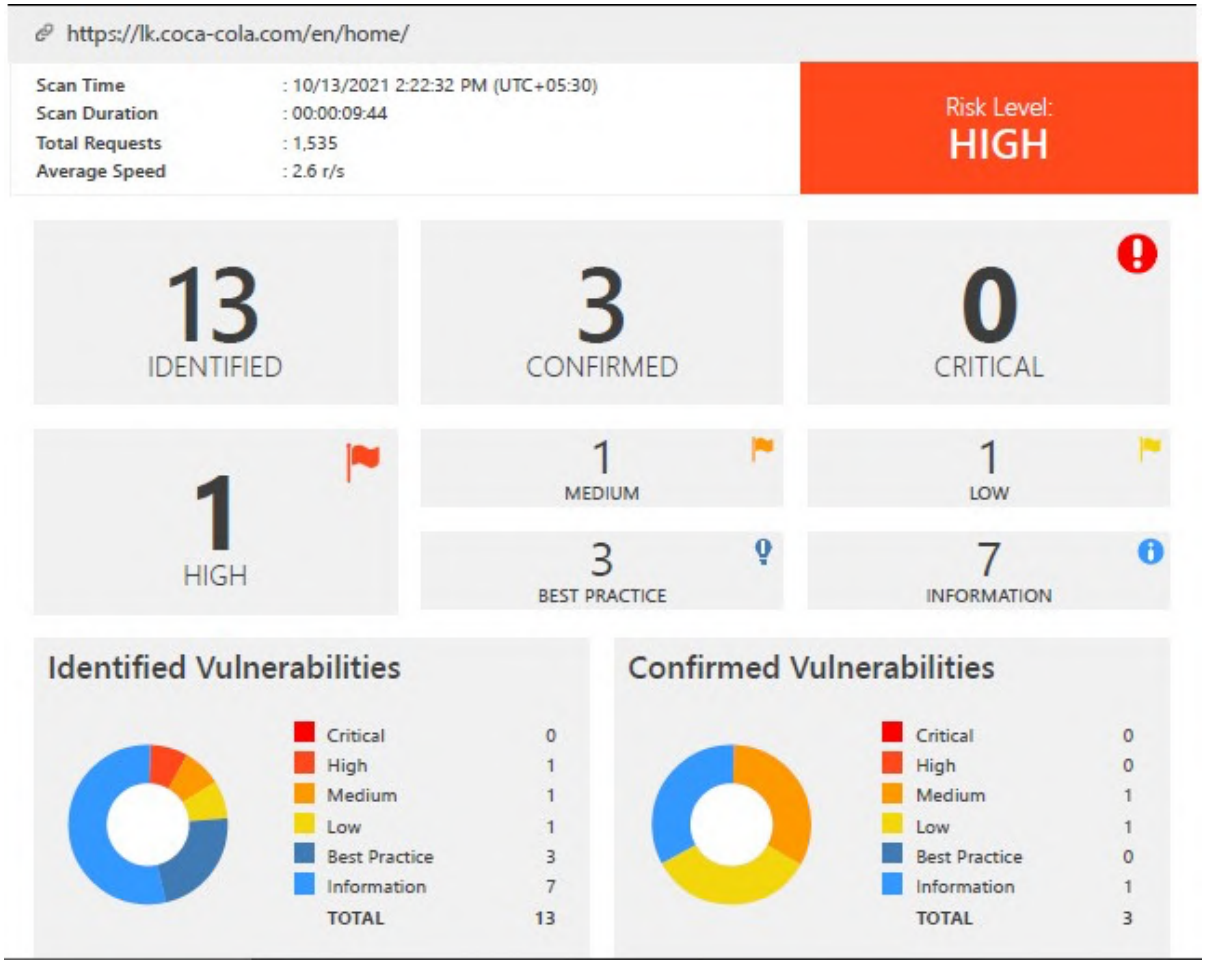
Critical	0
High	0
Medium	1
Low	1
Best Practice	0
Information	2
TOTAL	4

5. Domain 05 : https://lk.coca-cola.com/en/home

These are the vulnerabilities found

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Modernizr)	GET	https://lk.coca-cola.com/en/home/	
	Weak Ciphers Enabled	GET	https://lk.coca-cola.com/en/home/	
	Insecure Frame (External)	GET	https://lk.coca-cola.com/en/home/	
	Expect-CT Not Enabled	GET	https://lk.coca-cola.com/en/home/	
	Referrer-Policy Not Implemented	GET	https://lk.coca-cola.com/en/home/	
	Subresource Integrity (SRI) Not Implemented	GET	https://lk.coca-cola.com/en/home/	
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://lk.coca-cola.com/en/home/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://lk.coca-cola.com/en/home/	
	Missing object-src in CSP Declaration	GET	https://lk.coca-cola.com/en/home/	
	Out-of-date Version (jQuery)	GET	https://lk.coca-cola.com/en/home/	
	Web Application Firewall Detected	GET	https://lk.coca-cola.com/en/home/%3Cscript%3Ealert(0)%3C/script%3E	URI-BASED
	Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://lk.coca-cola.com/en/home/	
	Forbidden Resource	GET	https://lk.coca-cola.com/en/home/c:/boot.ini	URI-BASED

Summary of the scan

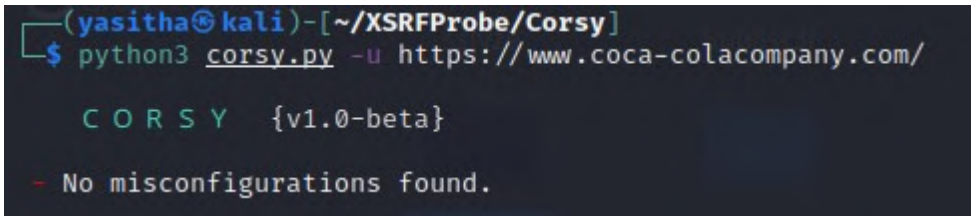


Manual Vulnerability Assessment

Testing CORS Misconfiguration

A CORS protocol which is called as "**Cross-Origin Resource Sharing**", uses several HTTP headers that indicate trustworthy web origins as well as related characteristics to make it available coming from different domain assets. Thrusted third parties and subdomains are examples for that. Through exposing CORS flaws, hackers could get access to classified information.

In here I have use a corsy as the CORS tool.



So in here no misconfigurations were found.

Analyzing Strength of the Cipher

A SSL certificate for HTTPS protocol provides high security contact between the server and the browser. Those certificates might have insecure ciphers attached to them. Individuals ought to figure out whether there are any existing vulnerable ciphers that individuals can utilize.

In here I use SSLyze tool. SSLyze which considers as a Python program that connects to a server and analyzes its SSL setup. It is intended to be quick and accurate, and that should aid companies as well as individuals through identifying misconfigurations in SSL server.

--regular Regular HTTPS scan; shortcut for --sslv2--sslv3--tlsv1

--tlsv1_1--tlsv1_2--tlsv1_3--reneg--resum--certinfo--

hide_rejected_ciphers--compression--heartbleed--

openssl_ccs--fallback--robot

```
┌──(yasitha㉿kali)-[~]
└─$ sslyze --regular coca-colacompany.com

CHECKING HOST(S) AVAILABILITY
-----------------------------

  coca-colacompany.com:443                      => 52.14.144.171



SCAN RESULTS FOR COCA-COLACOMPANY.COM:443 - 52.14.144.171
---------------------------------------------------------

* Downgrade Attacks:
      TLS_FALLBACK_SCSV:                    OK - Supported

* TLS 1.2 Cipher suites:
    Attempted to connect using 158 cipher suites.

    The server accepted the following 6 cipher suites:
      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384             256       ECDH: prime256v1 (256 bits)
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384             256       ECDH: prime256v1 (256 bits)
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                256       ECDH: prime256v1 (256 bits)
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256             128       ECDH: prime256v1 (256 bits)
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256             128       ECDH: prime256v1 (256 bits)
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                128       ECDH: prime256v1 (256 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                       OK - Supported
      Legacy RC4 Algorithm                  OK - Not Supported
```

```
    The server is configured to prefer the following cipher suite:
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256             128       ECDH: prime256v1 (256 bits)


* SSL 2.0 Cipher suites:
    Attempted to connect using 7 cipher suites; the server rejected all cipher suites.

* Certificates Information:
      Hostname sent for SNI:                coca-colacompany.com
      Number of certificates detected:      1


    Certificate #0 ( _RSAPublicKey )
      SHA1 Fingerprint:                     06c0f04058c9cc02a805698fdaea989814823a0a
      Common Name:                          redirect.coca-cola.com
      Issuer:                               Entrust Certification Authority - L1K
      Serial Number:                        1030343442077086232217552862148655889 86
      Not Before:                           2021-09-23
      Not After:                            2022-09-23
      Public Key Algorithm:                 _RSAPublicKey
      Signature Algorithm:                  sha256
      Key Size:                             2048
      Exponent:                             65537
      DNS Subject Alternative Names:        ['redirect.coca-cola.com', 'www.redirect.coca-cola.com', 'llamadodepapanoel.coca-cola.com.ar', 'llamadodelviejitopascuero.co
ca-cola.cl', 'llamadodepapanoel.coca-cola.com.py', 'llamadodepapanoel.coca-cola.com.uy', 'llamadodepapanoel.coca-cola.com.bo', 'careers.cokecanada.com', 'cocacola.com
.pl', 'coke.ie', 'coke2home.com', 'digitalworkplace.coke.com', 'fsi.fanta.de', 'parceiroretornavel.coca-cola.com.br', 'retornaveis.coca-cola.com.br', 'shortcut.coke.c
om', 'teams.coke.com', 'www.cocacola.com.pl', 'www.frestea.co.id', 'www.marky.coca-cola.ma', 'www.parceiroretornavel.coca-cola.com.br', 'www.parceiroretornavel.cocaco
la.com.br', 'www.retornaveis.coca-cola.com.br', 'www.retornaveis.cocacola.com.br', 'thecocacolacompany.com', 'www.thecocacolacompany.com', 'cocacolacompany.com', 'www
.cocacolacompany.com', 'thecoca-colacompany.com', 'www.thecoca-colacompany.com', 'practilonch.com', 'globalasb.coke.com', 'icoke.hk', 'fr.cocacolabelgium.be', 'nl.coc
acolabelgium.be', 'coca-cola-oesterreich.at', 'coke.co.za', 'www.coca-cola.com.ar', 'www.coca-cola.cl', 'gasdeverao.cocacola.com.br', 'fanta.lat', 'sprite.lat', 'spri
te.tw', 'www.sprite.tw', 'www.sprite.lat', 'www.fanta.lat', 'schweppes.gr', 'coca-cola.it', 'jatek.coke.hu', 'www.jatek.coke.hu', 'coke.net', 'cocacola.com.br', 'coca
-cola.com.br', 'andina.coke.net', 'andinarp.coke.net', 'bandeirantes.coke.net', 'cvi.coke.net', 'femsa.coke.net', 'simoes.coke.net', 'solar.coke.net', 'sorocaba.coke.
```

```
links.es', 'innocentdrinks.it', 'innocentdrinks.pt', 'fanta.no', 'www.fanta.no', 'tunisia.coca-cola.com']

    Certificate #0 - Trust
      Hostname Validation:              OK - Certificate matches server hostname
      Android CA Store (9.0.0_r9):      OK - Certificate is trusted
      Apple CA Store (iOS 13, iPadOS 13, macOS 10.15, watchOS 6, and tvOS 13):OK - Certificate is trusted
      Java CA Store (jdk-13.0.2):       OK - Certificate is trusted
      Mozilla CA Store (2020-06-21):    OK - Certificate is trusted
      Windows CA Store (2020-05-04):    OK - Certificate is trusted
      Symantec 2018 Deprecation:        OK - Not a Symantec-issued certificate
      Received Chain:                   redirect.coca-cola.com --> Entrust Certification Authority - L1K
      Verified Chain:                   redirect.coca-cola.com --> Entrust Certification Authority - L1K --> Entrust Root Certification Authority - G2
      Received Chain Contains Anchor:   OK - Anchor certificate not sent
      Received Chain Order:             OK - Order is valid
      Verified Chain contains SHA1:     OK - No SHA1-signed certificate in the verified certificate chain

    Certificate #0 - Extensions
      OCSP Must-Staple:                 NOT SUPPORTED - Extension not found
      Certificate Transparency:         OK - 3 SCTs included

    Certificate #0 - OCSP Stapling
                                        NOT SUPPORTED - Server did not send back an OCSP response

* Session Renegotiation:
      Client-initiated Renegotiation:   OK - Rejected
      Secure Renegotiation:             OK - Supported

* SSL 3.0 Cipher suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* TLS 1.1 Cipher suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.
```

```
* SSL 3.0 Cipher suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* TLS 1.1 Cipher suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* Deflate Compression:
                                     OK - Compression disabled

* TLS 1.0 Cipher suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* TLS 1.3 Cipher suites:
    Attempted to connect using 5 cipher suites; the server rejected all cipher suites.

* OpenSSL CCS Injection:
                                     OK - Not vulnerable to OpenSSL CCS injection

* ROBOT Attack:
                                     OK - Not vulnerable, RSA cipher suites not supported.

* OpenSSL Heartbleed:
                                     OK - Not vulnerable to Heartbleed

* TLS 1.2 Session Resumption Support:
     With Session IDs: PARTIALLY SUPPORTED (1 successful resumptions out of 5 attempts).
     With TLS Tickets: OK - Supported.


SCAN COMPLETED IN 63.87 S
```

Testing Cross Site Scripting

As there are many types of XSS attack, in here I am going to use XSStrike tool for this testing.

```
┌──(yasitha㉿kali)-[~/XSStrike]
└─$ python3 xsstrike.py -u https://www.coca-colacompany.com/search?q=coke&tags=
[1] 2090

┌──(yasitha㉿kali)-[~/XSStrike]
└─$
      XSStrike v3.1.4

[~] Checking for DOM vulnerabilities
[-] WAF detected: CloudFront (Amazon)
[!] Testing parameter: q
[-] No reflection found

[1]  + done       python3 xsstrike.py -u https://www.coca-colacompany.com/search?q=coke
┌──(yasitha㉿kali)-[~/XSStrike]
└─$
```

In here no this not vulnerable to XSS attacks.

Testing https request smuggling

As HTTP request smuggling is really a high severity flaw whereby a hacker smuggles an incorrect HTTP request to evade security measures. This gains illegal entry and engages in harmful operations.

So in here I have use smuggling tool to detect any https request smuggling.

```
┌──(yasitha㉿kali)-[~]
└─$ cd http-request-smuggling

┌──(yasitha㉿kali)-[~/http-request-smuggling]
└─$ python3 smuggle.py -u https://www.coca-colacompany.com/

                    SMUGGLING

            Author    :   Anshuman Pattnaik / @anspattnaik
            Blog      :   https://hackbotone.com/blog/http-request-smuggling-detection-tool
            Version   :   0.1
 ____________________________________________________________________________________

 [+]  Target URL  :  https://www.coca-colacompany.com/
 [+]  Method      :  POST
 [+]  Retry       :  2
 [+]  Timeout     :  10
 [+]  HRS Reports :  /home/yasitha/http-request-smuggling/reports/www.coca-colacompany.com

[spacejoin]      CL.TE      403      0.7s      OK
[spacejoin]      CL.TE      403      0.63s     OK
[spacejoin]      TE.CL      403      1.29s     OK
[spacejoin]      TE.CL      403      0.61s     OK
[default]        CL.TE      500      0.78s     OK
[default]        CL.TE      500      0.92s     OK
[default]        TE.CL      403      0.93s     OK
[default]        TE.CL      403      0.74s     OK
[underjoin]      CL.TE      403      2.1s      OK
```

```
[underjoin]      TE.CL      403      0.74s     OK
[underjoin]      TE.CL      403      0.75s     OK
[space1]         CL.TE      500      0.75s     OK
[space1]         CL.TE      500      1.01s     OK
[space1]         TE.CL      403      1.04s     OK
[space1]         TE.CL      403      0.79s     OK
[space2]         CL.TE      500      0.98s     OK
[space2]         CL.TE      500      0.89s     OK
[space2]         TE.CL      403      1.87s     OK
[space2]         TE.CL      403      0.95s     OK
[space3]         CL.TE      403      0.77s     OK
[space3]         CL.TE      403      2.13s     OK
[space3]         TE.CL      403      0.92s     OK
[space3]         TE.CL      403      1.09s     OK
[nameprefix1]    CL.TE      403      0.49s     OK
[nameprefix1]    CL.TE      403      0.78s     OK
[nameprefix1]    TE.CL      403      0.76s     OK
[nameprefix1]    TE.CL      403      0.86s     OK
[valueprefix1]   CL.TE      500      0.77s     OK
[valueprefix1]   CL.TE      500      0.93s     OK
[valueprefix1]   TE.CL      403      0.64s     OK
[valueprefix1]   TE.CL      403      0.91s     OK
[nospace1]       CL.TE      500      0.94s     OK
[nospace1]       CL.TE      500      0.94s     OK
[nospace1]       TE.CL      403      2.31s     OK
[nospace1]       TE.CL      403      0.78s     OK
[tabprefix1]     CL.TE      501      1.1s      OK
[tabprefix1]     CL.TE      501      0.89s     OK
[tabprefix1]     TE.CL      501      0.93s     OK
[tabprefix1]     TE.CL      501      1.11s     OK
[vertprefix1]    CL.TE      501      0.5s      OK
[vertprefix1]    CL.TE      501      0.73s     OK
```

In here all requests are ok. So, this not vulnerable to smuggling.

Testing Open redirection Vulnerability

Oralyzer is a simply Python tool that checks a website for Open Redirection vulnerabilities.

In here all ends with 404 and 403 code so there are no vulnerabilities

CONCLUSION

This assessment was about a vulnerability test on https://www.coca-colacompany.com/ . I have used manual and automated techniques for it. In here I have tested in scopes and subdomains as well. So any of restrictions were not violated during those scans. A proper mythology was followed.

Every concept is details as much I could. When analyzing domains, I found critical level vulnerability and some high level vulnerabilities through scans. The right technique was used throughout the evaluation, beginning with data collection and concluding with the vulnerability evaluation process. All of the methodology and tools used in the evaluation, as well as their results, are thoroughly addressed. Additionally, the impact of the revealed flaws, confirmation of the status of security flaws, and ways to mitigate the risk involved with the security flaws are all described in depth.

REFERENCES

[1] "OWASP Top ten web application security risks," *Owasp.org*. [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed: 08-Oct-2021].

[2] "Vulnerability Severity Levels," *Netsparker.com*, 26-Aug-2021. [Online]. Available: https://www.netsparker.com/support/vulnerability-severity-levels-netsparker/. [Accessed: 11-Oct-2021].

[3] S. Palmer, "Information Gathering Techniques," in *Web Application Vulnerabilities*, Elsevier, 2007, pp. 75–141.

[4] Bharath, "A penetration tester's guide to subdomain enumeration," *Appsecco*, 11-Oct-2017. [Online]. Available: https://blog.appsecco.com/a-penetration-testers-guide-to-sub-domain-enumeration-7d842d5570f6. [Accessed: 12-Oct-2021].

[5] A. Aboul-Ela, *Sublist3r: Fast subdomains enumeration tool for penetration testers*. .

[6] "What is Shodan? - Shodan Help Center," *Shodan.io*. [Online]. Available: https://help.shodan.io/the-basics/what-is-shodan. [Accessed: 13-Oct-2021].

[7] *Beyondtrust.com*. [Online]. Available: https://www.beyondtrust.com/resources/glossary/vulnerability-assessment. [Accessed: 13-Oct-2021].

[8] "whatweb," *Kali.org*. [Online]. Available: https://www.kali.org/tools/whatweb/. [Accessed: 13-Oct-2021].

[9] "What is Netsparker?," *Netsparker.com*, 04-Oct-2021. [Online]. Available: https://www.netsparker.com/support/what-is-netsparker/. [Accessed: 13-Oct-2021].