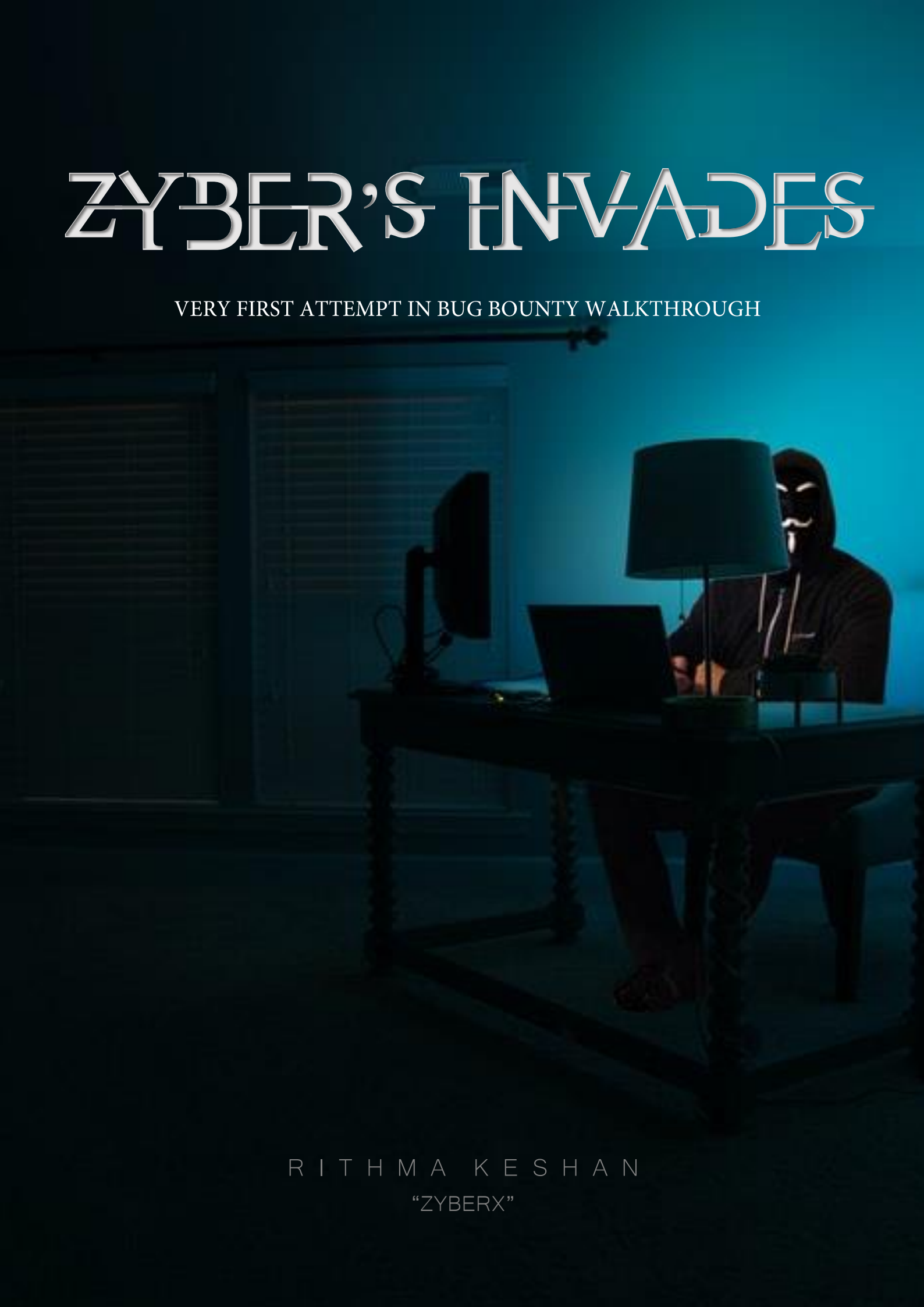
ZYBER'S INVADES

VERY FIRST ATTEMPT IN BUG BOUNTY WALKTHROUGH



RITHMA KESHAN

"ZYBERX"

Sri Lanka Institute of Information Technology

B.Sc. (Hons) Information Technology Specializing in Cyber Security

IE2062 – Web Security

Bug Bounty Assignment & Web Audit

February 2022

Submitted by:

Student Registration Number	Student Name
[redacted]	W.B.G.R.K. Maduthisara

Contents

1. Acknowledgement

I would like to express my special thank of gratitude to the lecture in charge of the 2nd year Web Security module of Sri Lanka Institute of Information Technology (SLIIT) Dr. Lakmal Rupasinghe and Ms. Chethana Liyanapathirana, who guided us through the process of completing this assignment.

In addition, I would like to express my gratitude to Ms. Chathu Udagedara and Ms. Menaka Moonamaldniya, who provided us the practical knowledge to complete this task.

And I'd like to express my gratitude to all my friends, who were supported to complete my assignment.

2. Assessment Objectives

The objective of this assessment is to measure the capabilities to understand web security fundamentals in a theoretical foundation and apply it to a real-world practical scenario. Hence, I have selected to audit https://www.spotify.com as my targeted website, using proper methodologies. I'm providing all the submission details including my experience in this report & explain all the correct and incorrect steps taken in my experiments.

3. Introduction

For this assignment we had to use a web system which is listed in a bug bounty program. So I decided to select www.spotify.com which was listed in HackerOne.

3.1 Overview of the Spotify

Spotify is a digital music, podcast and video service that gives access to millions of songs and other content from creators all over the world which is under the type of Music streaming service originated in Sweden. [1] And this is founded on 23 April 2006 by Daniel Ek and Martin Lorentzon. Spotify is one of the largest music streaming service providers, with over 422 million monthly active users, including 182 million paying subscribers, as of March 2022. Spotify is available across a range of devices including, [2]

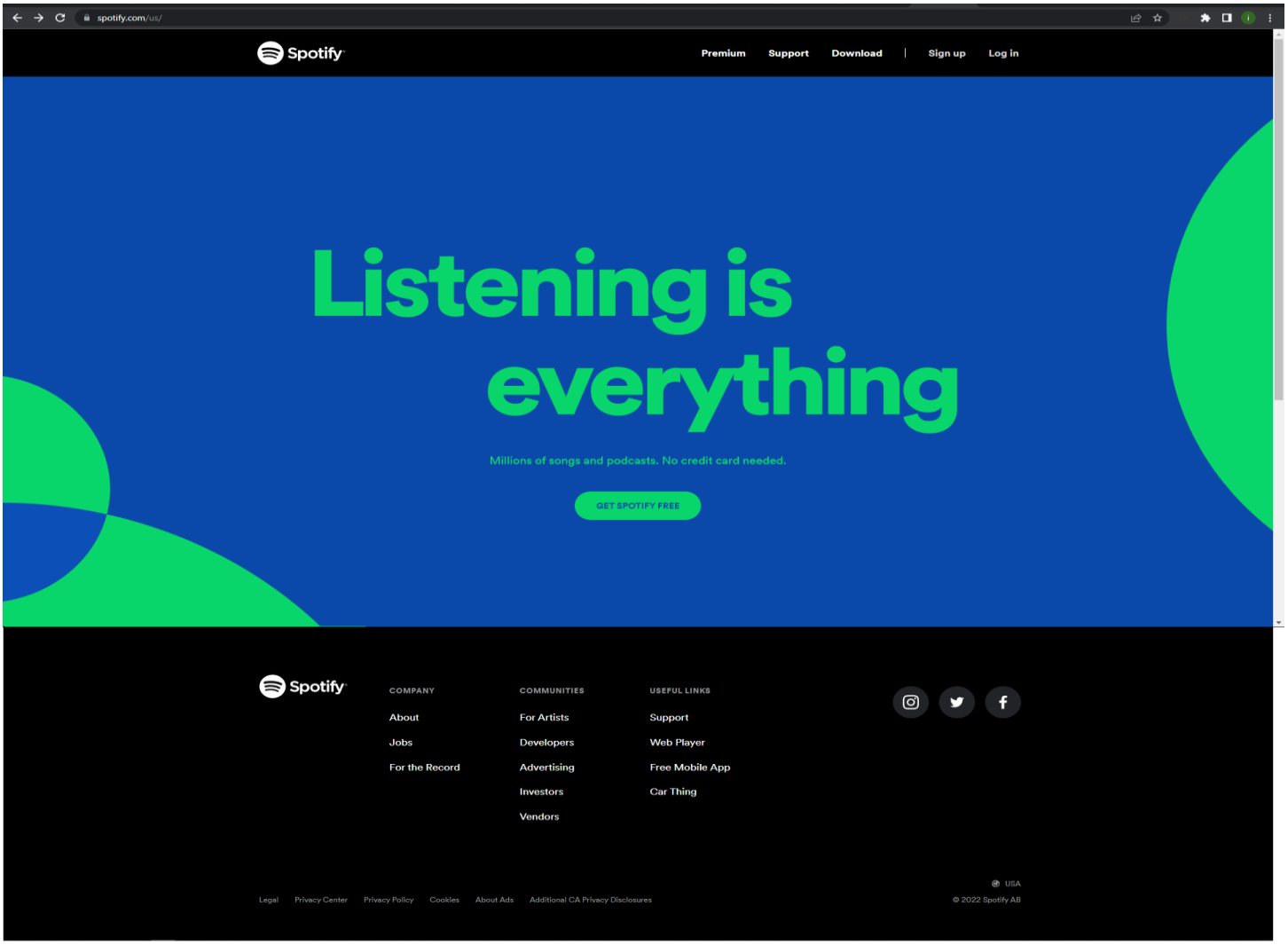
- Windows
- MacOS
- Linux computers
- iOS and
- Android smartphones and tablets
- Smart home devices such as the *Amazon Echo* and *Google Nest* lines of products
- Digital media players like *Roku.*

Basic functions such as playing music are totally free, but you can also choose to upgrade to Spotify Premium. Spotify Offers 3 subscription types to users. [2]

Type	Remove ads	Mobile listening	Sound quality	Listen offline	Spotify Connect
Spotify Free	No	Limited (shuffle-only mode)	Up to 160 kbit/s Vorbis or 128 kbit/s Advanced Audio Coding for the web player	No	Limited (Spotify Connect device using the new SDK)
Spotify Premium	Yes	Yes	Up to 320 kbit/s Vorbis or 256 kbit/s AAC for the web player	Yes	Yes
Spotify HiFi (planned)[129]	Yes	Yes	Compact Disc Digital Audio quality lossless	Yes	Yes

Figure 1 Accounts & Subscription Types

Spotify.com website overview (Windows)



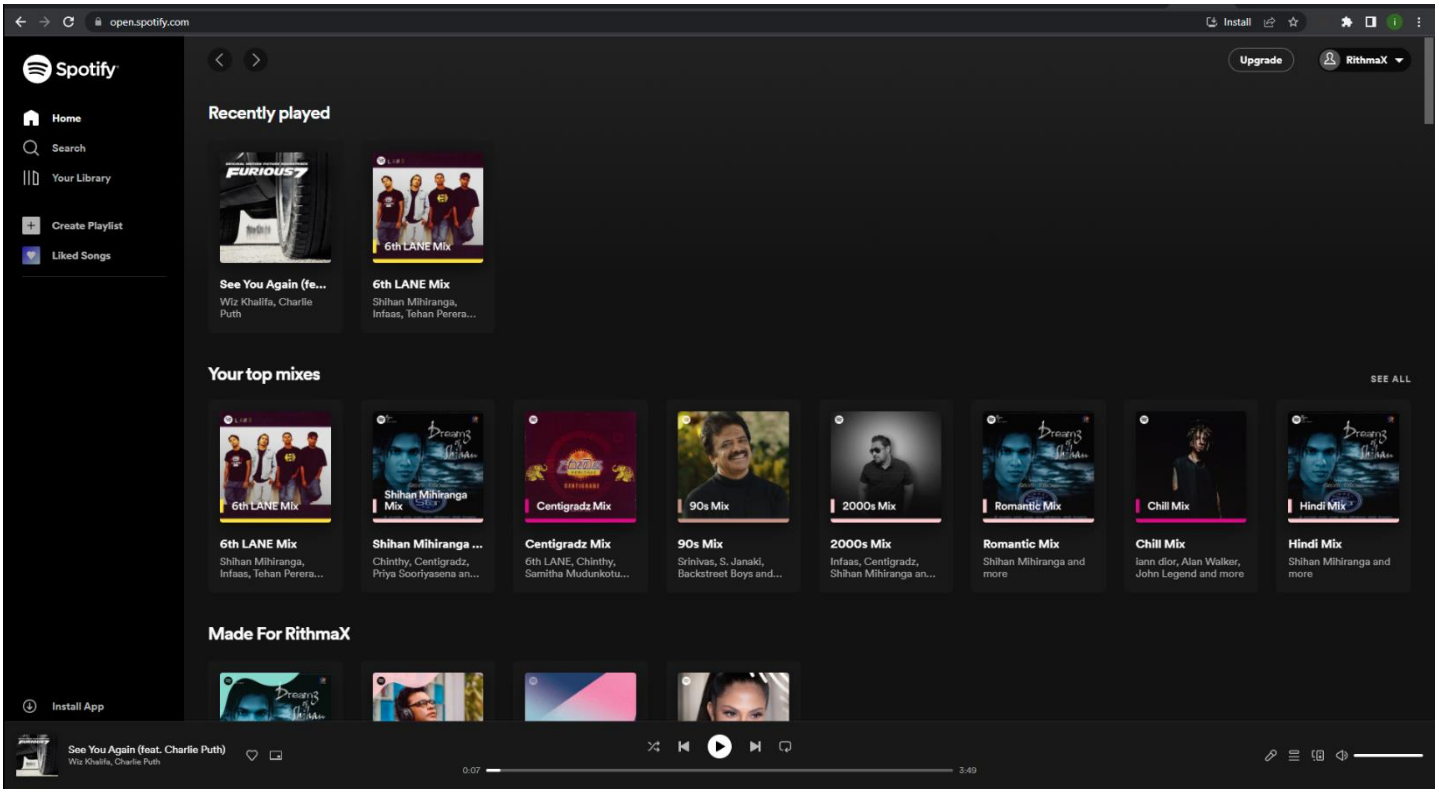


Figure 2 Spotify web player

Spotify Windows application overview

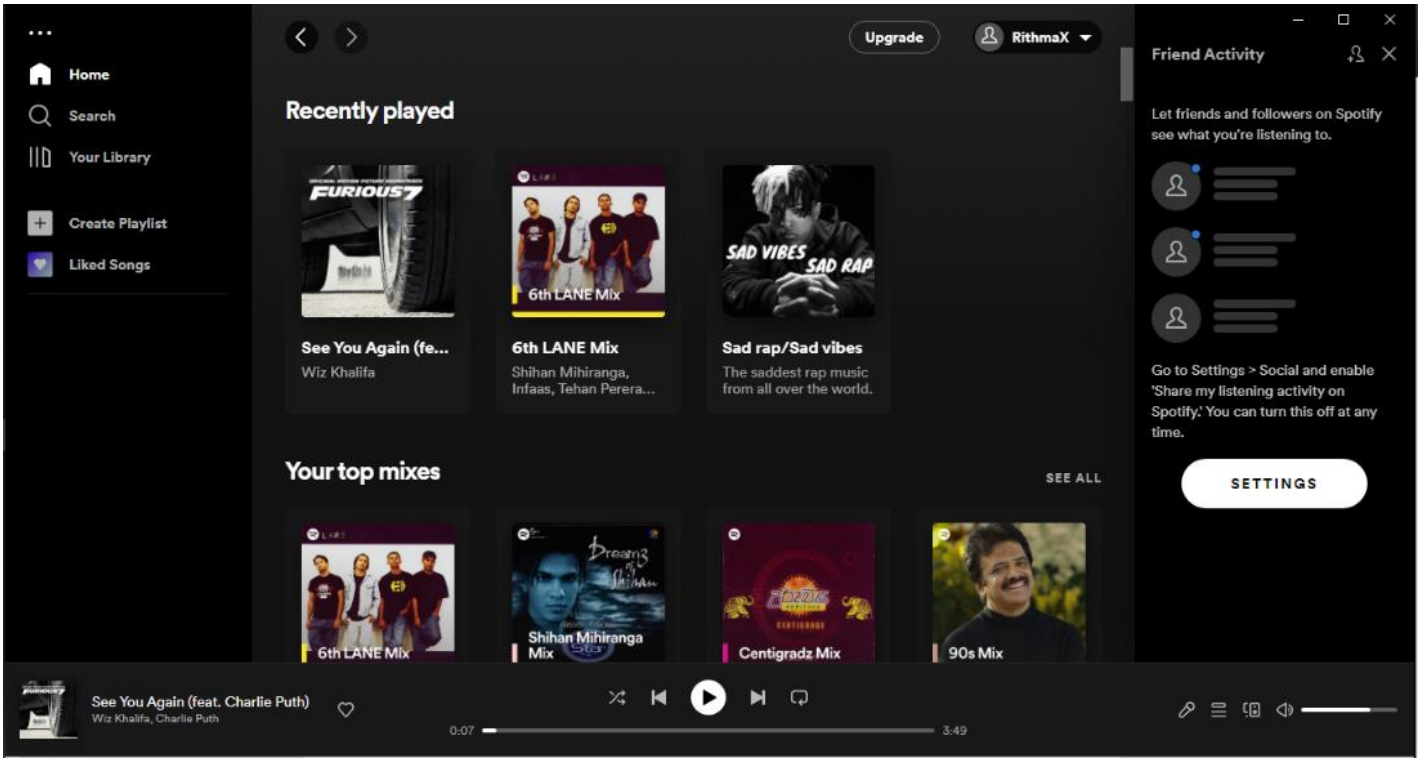


Figure 4 Spotify App (Windows)

Spotify iOS application overview

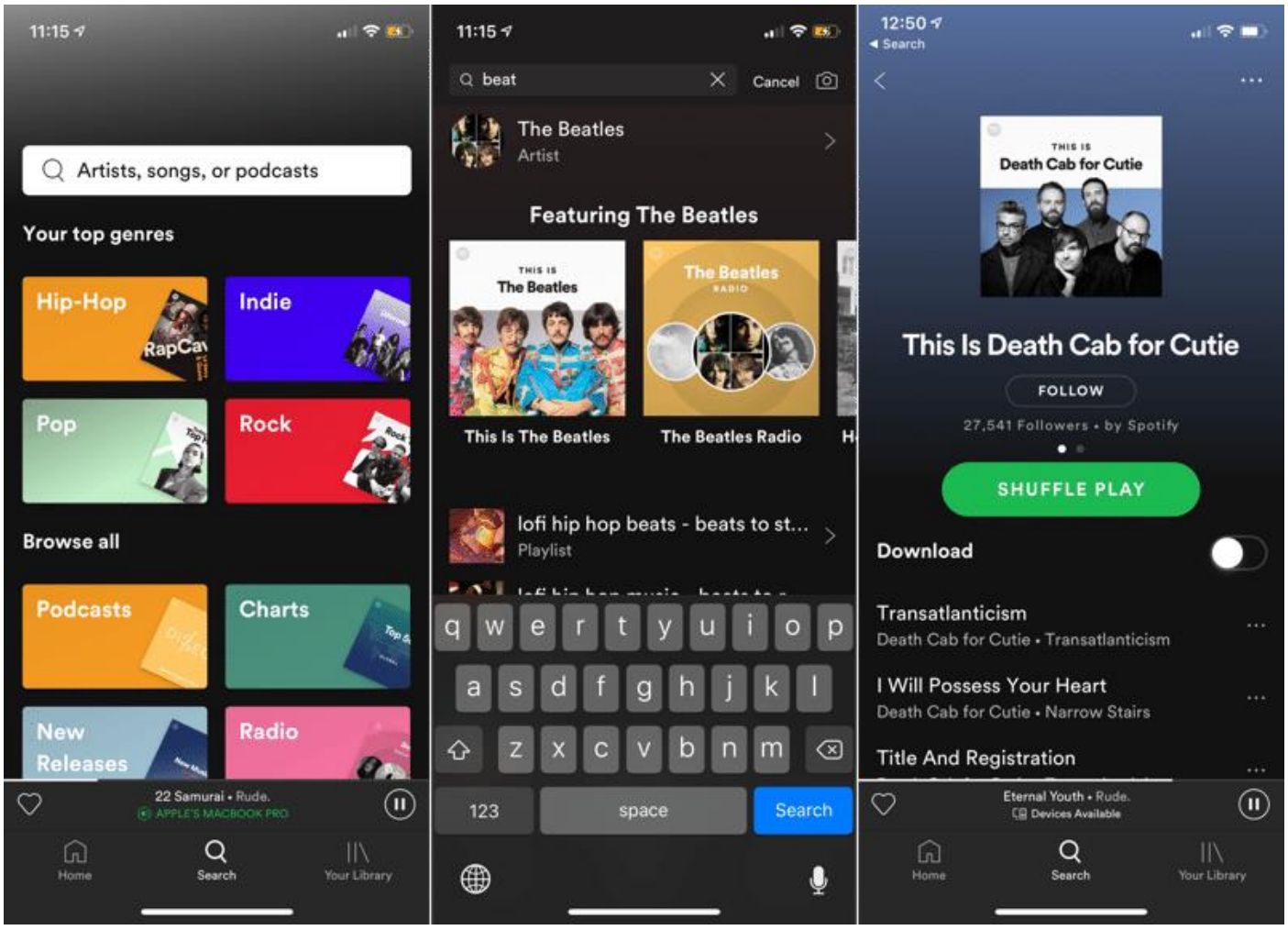


Figure 3 Spotify iOS app

Spotify Android application overview

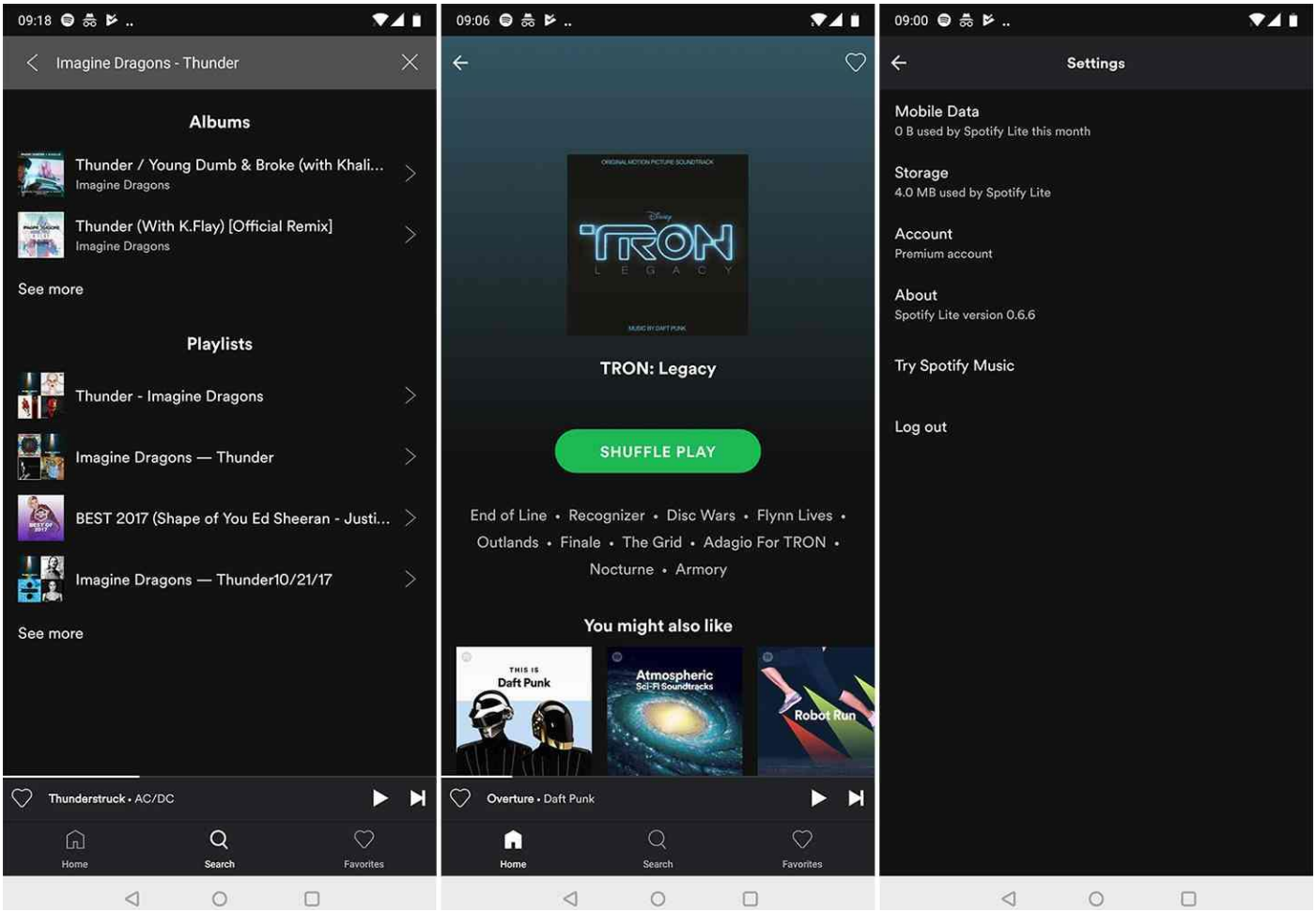


Figure 5 Spotify Android app

Spotify Roku Platform application overview

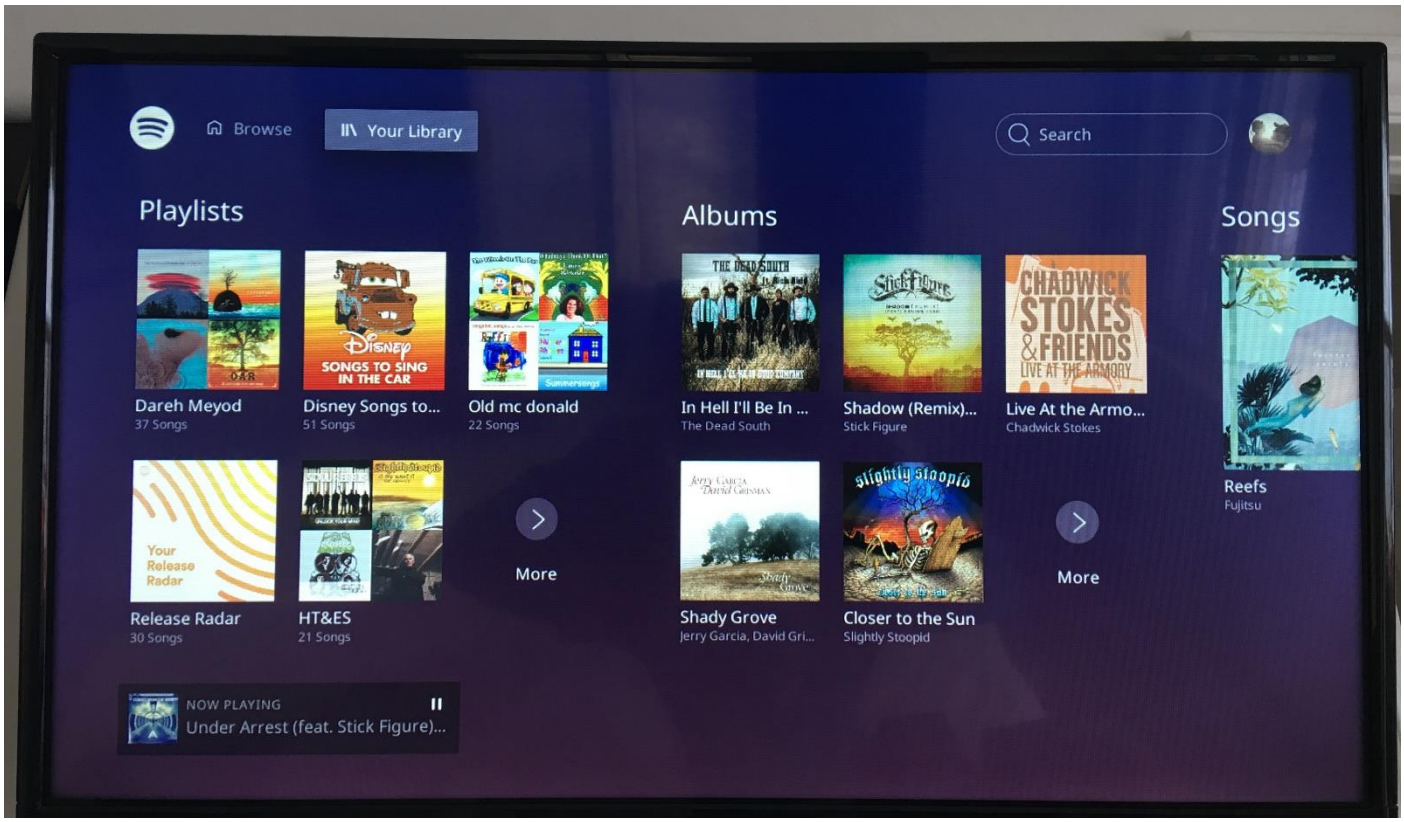


Figure 7 Spotify Roku app

In this assessment my goal is to find vulnerabilities in the Spotify platform and identify the relevant risks according to the levels. The scope of the auditing will be limited to following domains as they are published by Spotify in hackerone.

3.2 In Scope domains:

1) spotify.com
2) assets.spotify.com
3) api.spotify.com
4) spotify.net
5) spotifyforbrands.com
6) backstage.io

3.3 Out Scope domains:

- 99music.theringer.com
- 99music.theringer.com
- besttv.theringer.com
- fantasyfootball.theringer.com
- fastfood.theringer.com
- heists.theringer.com
- inflight.theringer.com
- nbadraft.theringer.com
- nfldraft.theringer.com
- superheroes.theringer.com
- theringer.com
- thrones.theringer.com
- tradevalue.theringer.com

Domain	spotify.com	Critical	Eligible
Domain	assets.spotify.com	Critical	Eligible
Domain	api.spotify.com	Critical	Eligible
Domain	spotify.net	Critical	Eligible
Domain	spotifyforbrands.com	Critical	Eligible
Domain	backstage.io	Critical	Eligible

3.4 Out Of Scope Vulnerabilities

3.4.1 Things explicitly ask you not to do:

- When experimenting, please only attack accounts belonging to you. Do not use leaked or compromised accounts belonging to other users. Vulnerabilities that were discovered using leaked or compromised accounts will be disqualified.
- Do not run automated scans without checking with us first. They are often very noisy.
- Do not test the physical security of Spotify offices, employees, equipment, et.c.
- Do not test using social engineering techniques (phishing, vishing, et.c.)
- Do not perform DoS or DDoS attacks.
- In any way attack our end users or engage in trade of stolen user credentials.

3.4.2 Finding types specifically excluded from the bounty:

- Reports of compromised accounts, accounts exposed in data breaches, or publicly accessible password dumps are not in scope for the bug bounty program but can be reported through our support site or support@spotify.com.
- Open redirect vulnerabilities which use a Spotify subdomain and the /mellon/logout URL to implement a redirect
- Other redirect vulnerabilities that *don't* rely on Mellon should still be reported.
- Descriptive error messages (e.g. Stack Traces, application or server errors).
- HTTP 404 codes/pages or other HTTP non-200 codes/pages.
- Fingerprinting / banner disclosure on common/public services.
- Disclosure of known public files or directories, (e.g. robots.txt).
- Clickjacking and issues only exploitable through clickjacking.
- CSRF on forms that are available to anonymous users (e.g. the contact form).
- Logout Cross-Site Request Forgery (logout CSRF).
- Presence of application or web browser 'autocomplete' or 'save password' functionality.
- Lack of Secure/HTTP Only flags on non-sensitive Cookies.
- Lack of Security Speedbump when leaving the site.
- Weak Captcha / Captcha Bypass
- Absence of brute force countermeasures (e.g. rate limiting, account lockout), unless a successful attack can be demonstrated.
- OPTIONS HTTP method enabled
- Username / email enumeration
- via Login Page error message
- via Forgot Password error message
- Missing HTTP security headers, specifically (https://www.owasp.org/index.php/List_of_useful_HTTP_headers), e.g.
- Strict-Transport-Security
- X-Frame-Options
- X-XSS-Protection
- X-Content-Type-Options [3]

- Content-Security-Policy, X-Content-Security-Policy, X-WebKit-CSP
- Content-Security-Policy-Report-Only
- SSL Issues, e.g.
- SSL Attacks such as BEAST, BREACH, Renegotiation attack
- SSL Forward secrecy not enabled
- SSL weak / insecure cipher suites
- Content spoofing / text injection without HTML/CSS
- Weak password policies
- Mail configuration issues including SPF, DKIM, DMARC settings
- Host header injection without exploitation
- DNSSEC configuration
- Assets we don't own such as expired domains even if they are listed in scope. [3]

3.4.3 Out of Scope bugs for Android apps

- Shared links leaked through the system clipboard.
- Any URIs leaked because a malicious app has permission to view URIs opened
- Absence of certificate pinning
- Sensitive data in URLs/request bodies when protected by TLS
- User data stored unencrypted on external storage
- Lack of obfuscation is out of scope
- oauth "app secret" hard-coded/recoverable in apk
- Crashes due to malformed Intents sent to exported Activity/Service/BroadcastReceive (exploiting these for sensitive data leakage is commonly in scope)
- Any kind of sensitive data stored in app private directory
- Lack of binary protection control in android app [3]

3.4.4 Out of Scope bugs for iOS apps

- Lack of Exploit mitigations ie PIE, ARC, or Stack Canaries
- Absence of certificate pinning
- Path disclosure in the binary
- User data stored unencrypted on the file system
- Lack of obfuscation is out of scope
- Lack of jailbreak detection is out of scope
- oauth "app secret" hard-coded/recoverable
- Crashes due to malformed URL Schemes
- Lack of binary protection (anti-debugging) controls
- Snapshot/Pasteboard leakage
- Runtime hacking exploits (exploits only possible in a jailbroken environment) [3]

4. Information Gathering (Reconnaissance Phase)

Information Gathering means gathering different kinds of information about the target website or the company and it also known as reconnaissance phase. This can be express as the beginning stage of Ethical hacking, where penetration testers or both black hat & white hat hackers try to gather all the information about their target. To perform a successful attack, we must gather more information about our target. And this method used to determine the needs of customers and users by analysts. These information are very important to perform attacks like brute force attacks. Recon phase can be done by many ways like,

- Footprinting
- Scanning
- Enumeration
- Reconnaissance

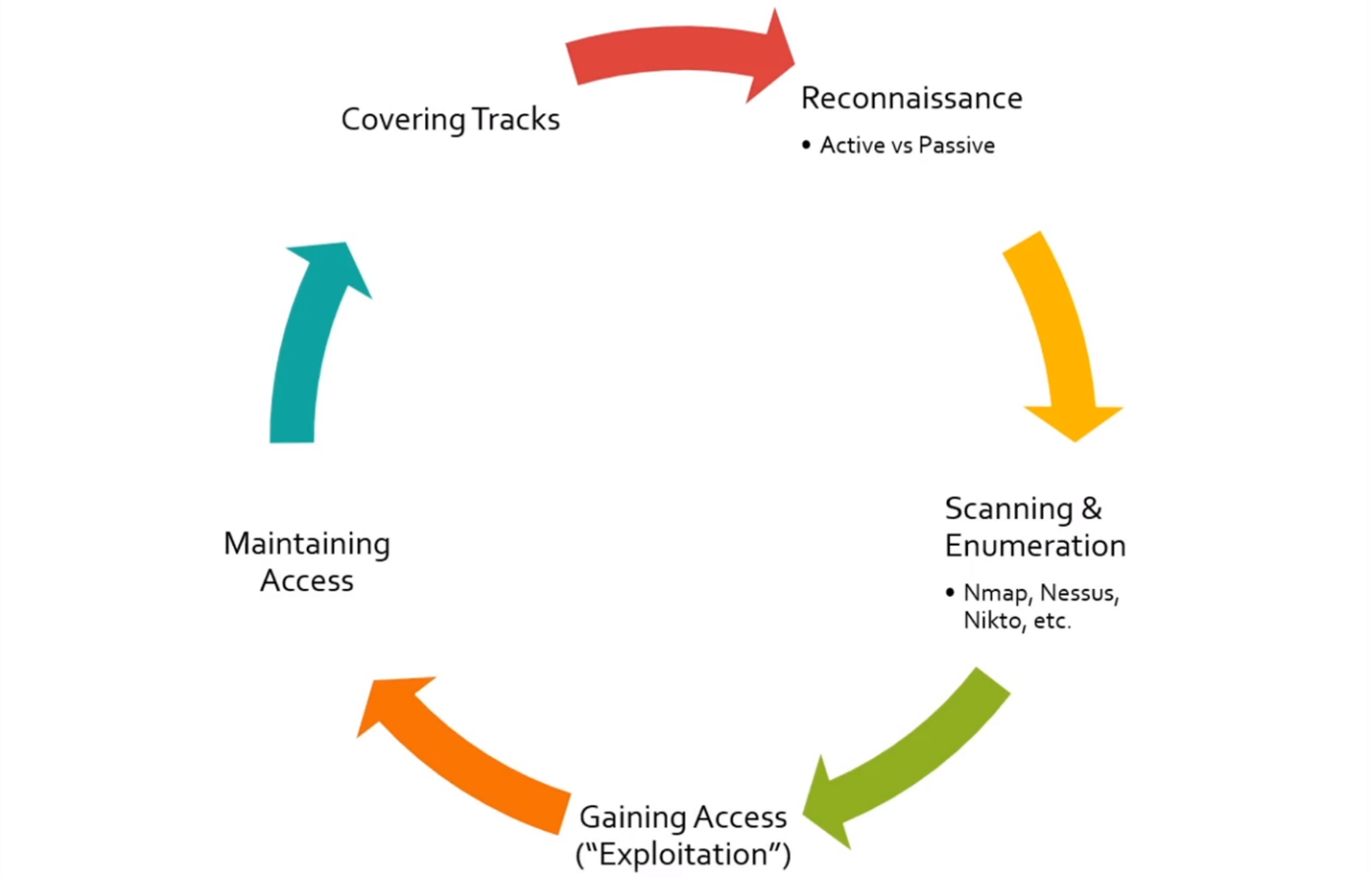


Figure 8 Information gathering

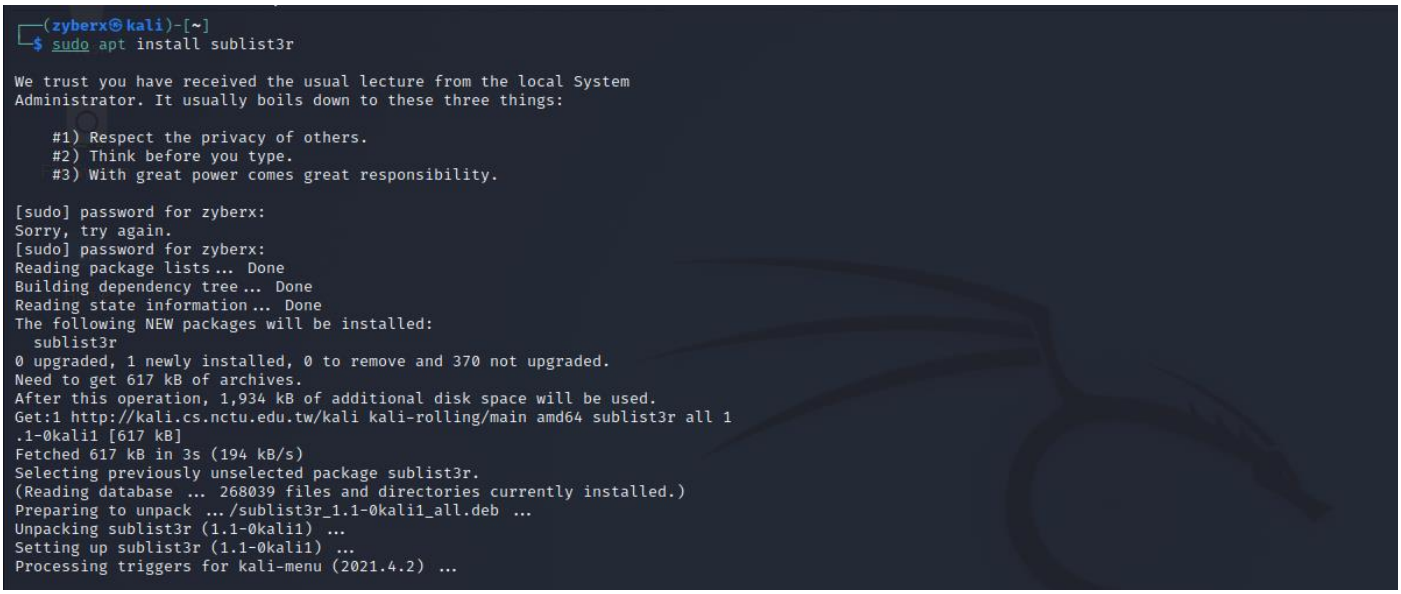
4.1 Sub Domain Enumeration

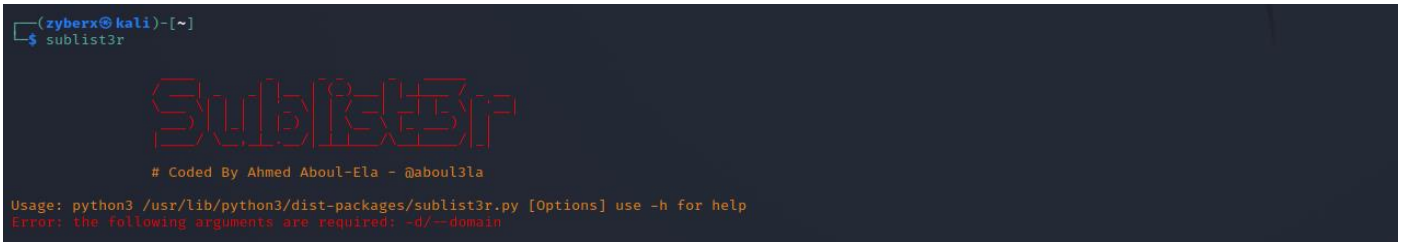
In this phase we can find valid & resolvable subdomains of the targeted domains. Following tools are used on this assignment.

- Sublist3r
- Amas
- SubBrute

Sublist3r

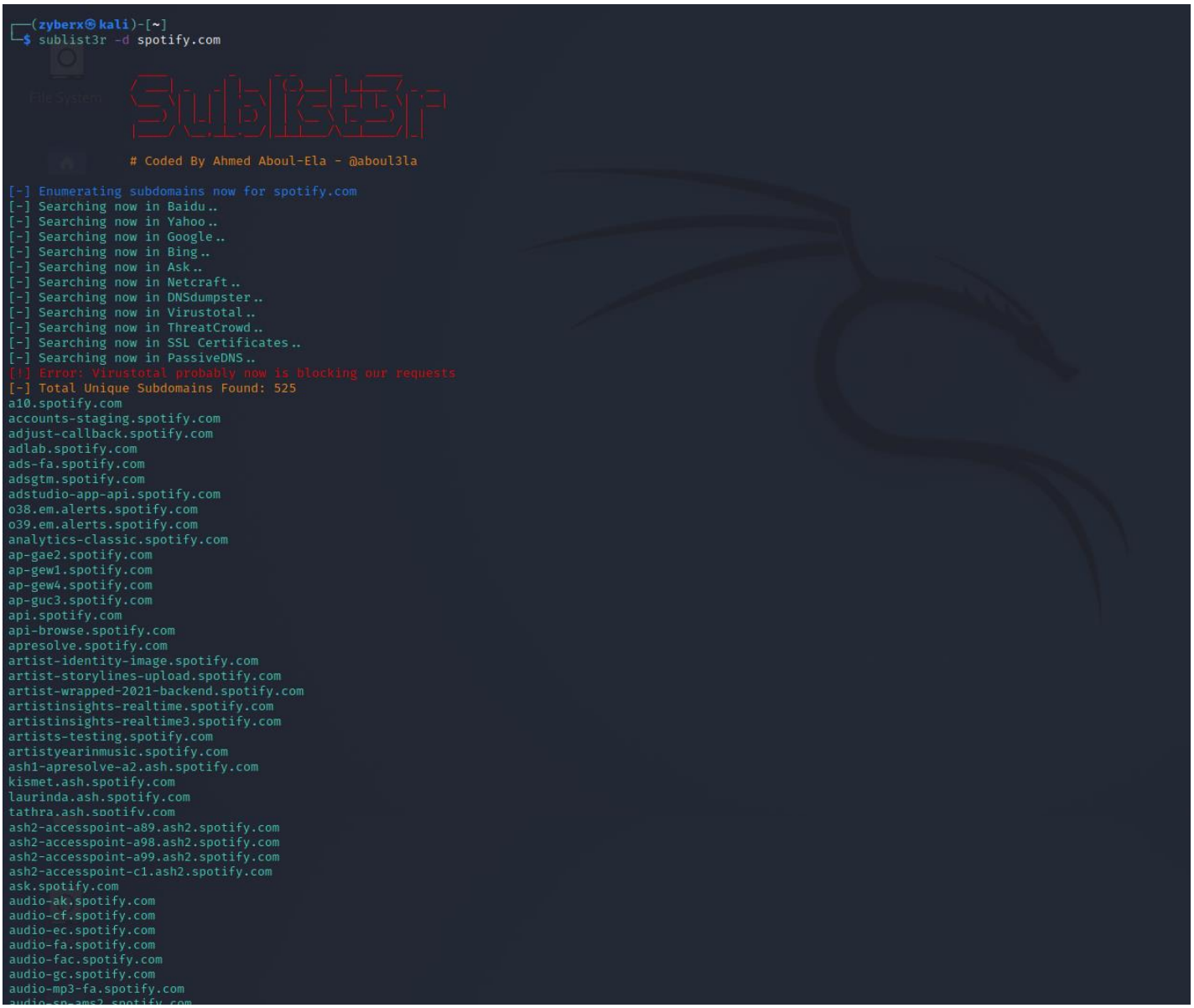
Installation





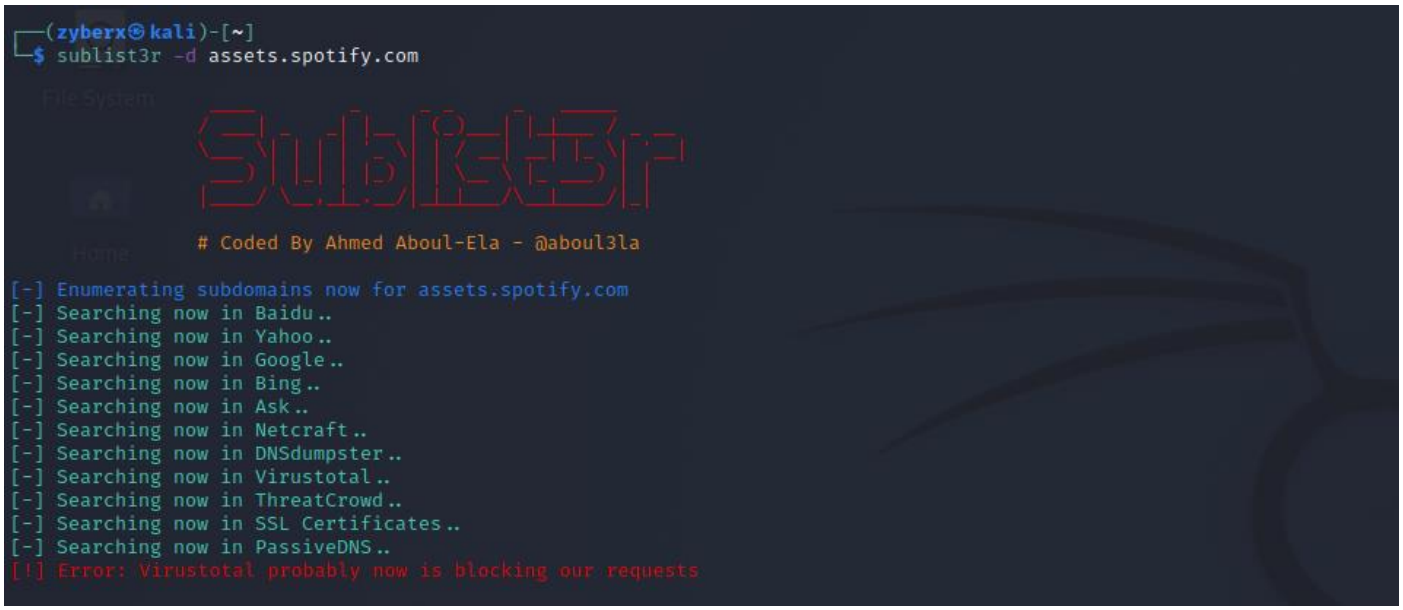
Finding Subdomains of selected domains

Spotify.com



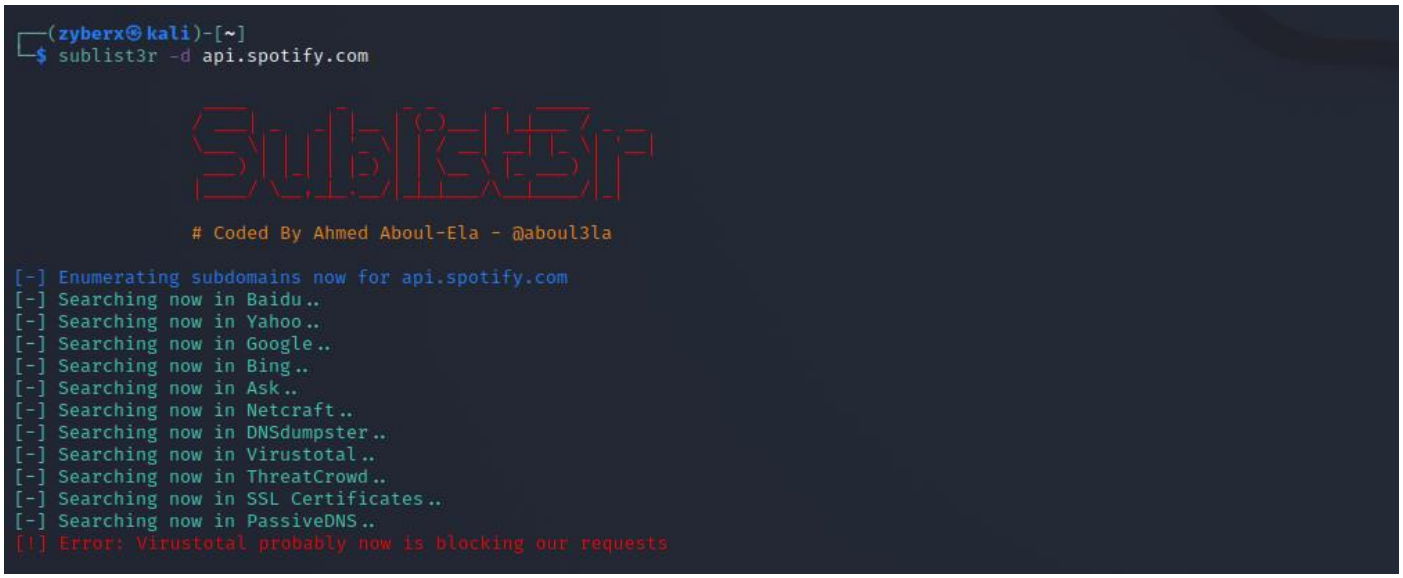
Using Sublist3r tool found 525 total unique subdomains for Spotify.com

assets.spotify.com



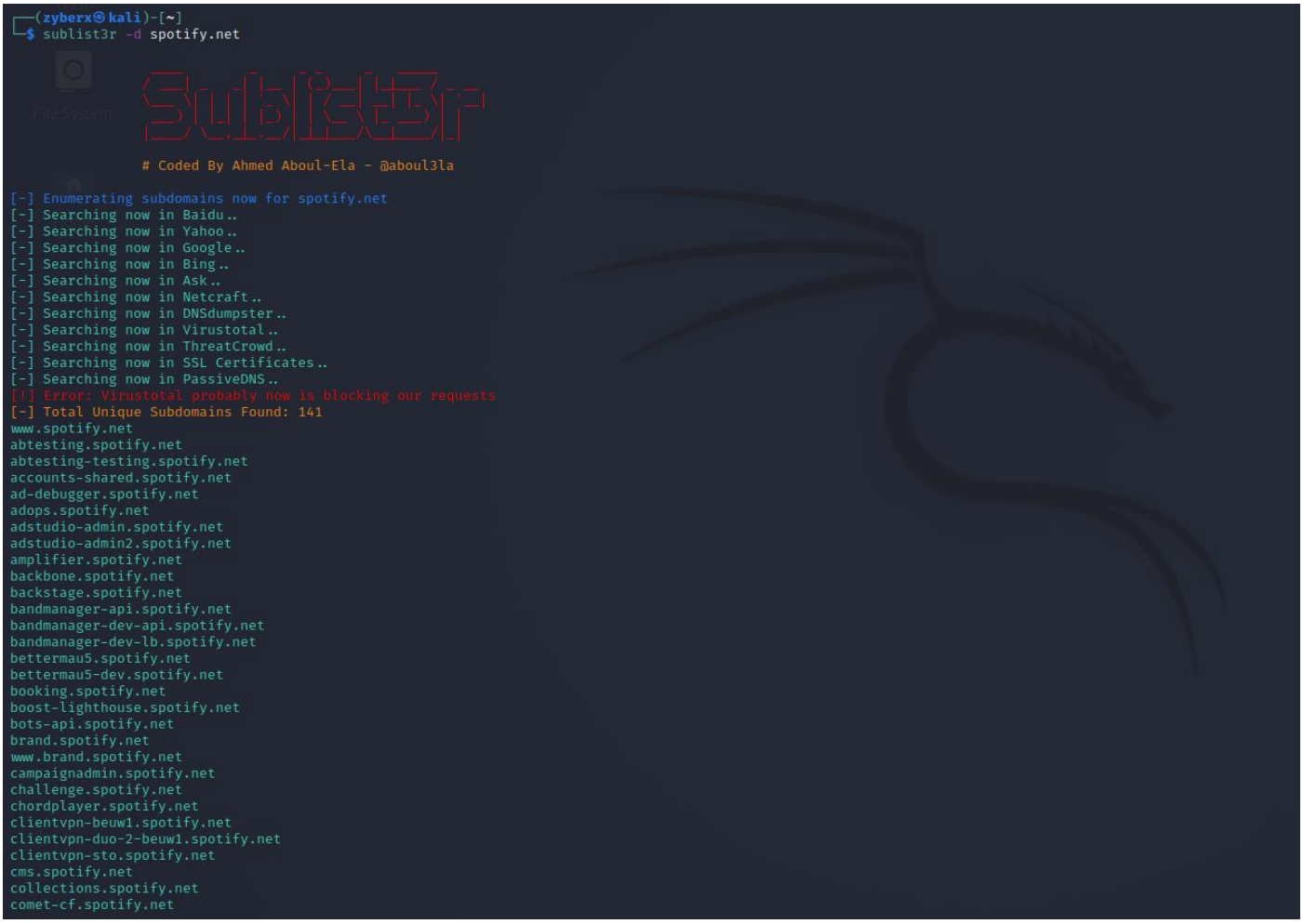
Using Sublist3r tool Not found any unique subdomains for assets.spotify.com

api.spotify.com



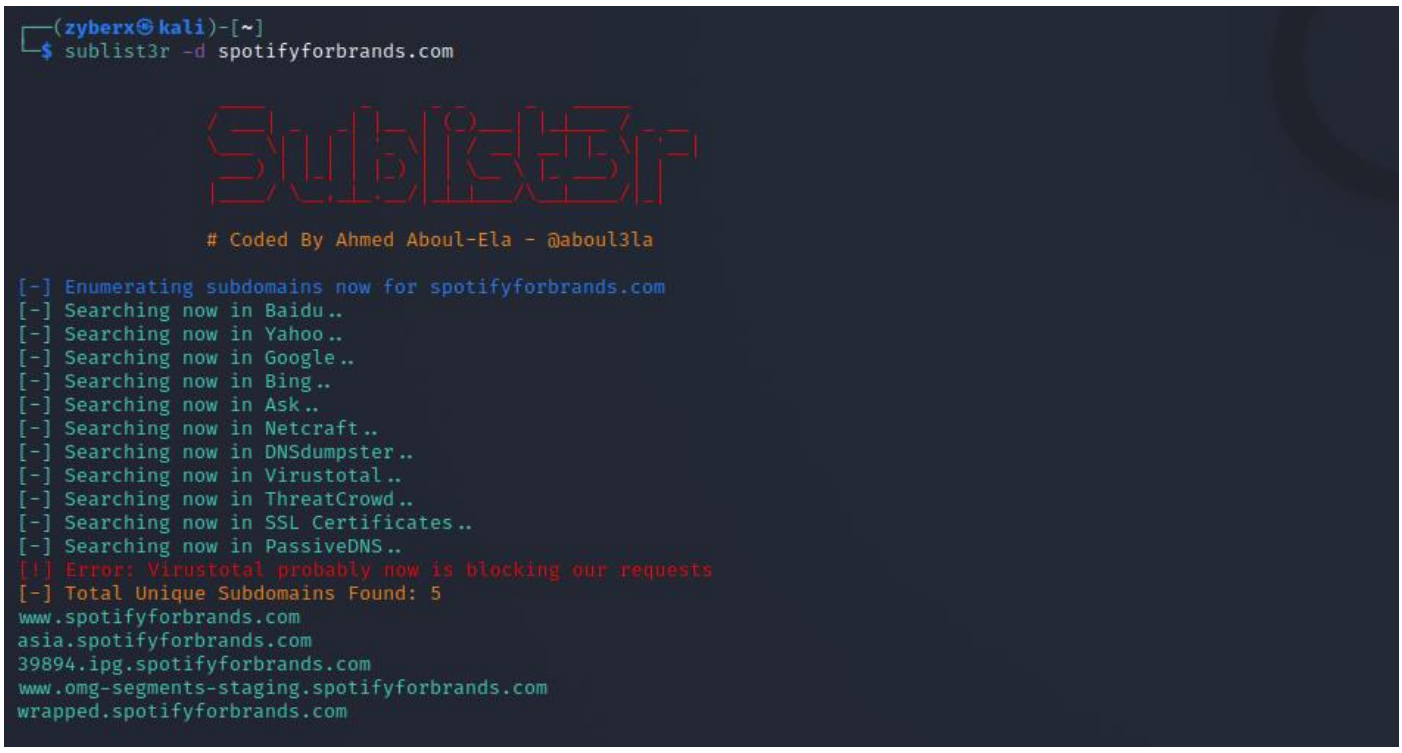
Using Sublist3r tool Not found any unique subdomains for api.spotify.com

spotify.net

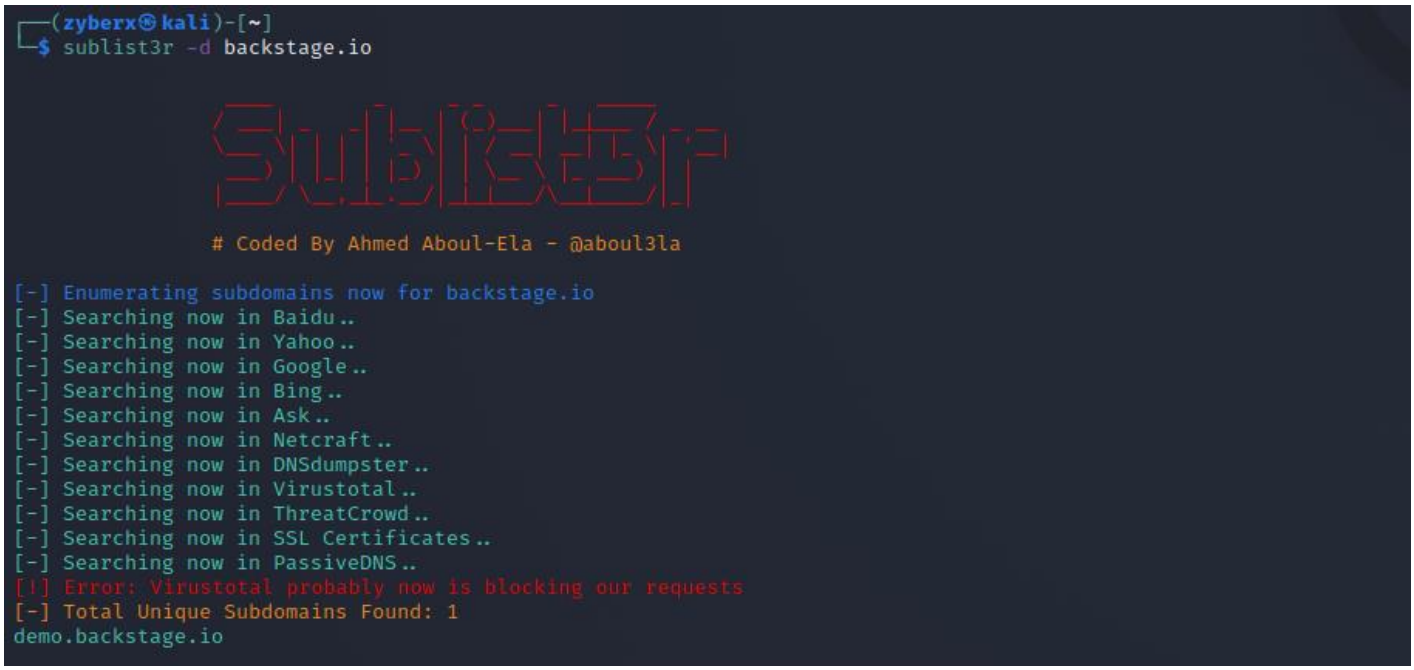


Using Sublist3r tool found 141 total unique subdomains for Spotify.net

spotifyforbrands.com



Using Sublist3r tool found 5 total unique subdomains for Spotifyforbrands.com



Using Sublist3r tool found only 1 total unique subdomains for backstage.io

OWASP Amass

The OWA SP Amass tool can be used to obtain subdomain names by scraping data sources, reverse DNS sweeping, recursive brute forcing. [3] In my case its pre-installed with KALI Linux which I'm using in my virtual machine.

Spotify.com

```
┌──(zyberx㉿kali)-[~]
└─$ amass enum -d spotify.com
spotify.com
ns3.spotify.com
ap-gae2.spotify.com
pci-testing.spotify.com
ns2.spotify.com
guc3-dealer-ssl.spotify.com
lexikon-slack-app.spotify.com
tableau-slack-app.spotify.com
guc3-dealer.spotify.com
gew1-dealer-ssl.spotify.com
hrblog.spotify.com
pci.spotify.com
canvas.spotify.com
newsroom.spotify.com
tags.spotify.com
ap-gew1.spotify.com
ns9.spotify.com
motionbrand.spotify.com
ns5.spotify.com
apresolve.spotify.com
dealer.spotify.com
noteable.spotify.com
edge-web-split-geo.dual-gslb.spotify.com
mobile-ap.spotify.com
ap-guc3.spotify.com
ap.single-gslb.spotify.com
edge-web-russia.dual-gslb.spotify.com
content-delivery.spotify.com
webapi-wg.dual-gslb.spotify.com
gew1-dnsauthslave-public-2lsn.gew1.spotify.com
esdk-ffl.spotify.com
mydata.spotify.com
canary-certificate-for-noop.spotify.com
guc3-dnsauthslave-pubns-72vd.guc3.spotify.com
ns4.spotify.com
wg.spotify.com
gew1-dealer.spotify.com
ap.spotify.com
podstart.spotify.com
carthing.spotify.com
live.spotify.com
stations.spotify.com
origin-play.spotify.com
backstage.spotify.com
adstudio-help.spotify.com
lite-images-i.spotify.com
partner-provisioning.spotify.com
todaystopfans.spotify.com
partners.spotify.com
timecapsule.spotify.com
pixel-static.spotify.com
login5.spotify.com
newsroom-old.spotify.com

OWASP Amass v3.15.0                                https://github.com/OWASP/Amass
347 names discovered - scrape: 118, alt: 24, dns: 8, api: 163, cert: 34
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
        162.159.128.0/22        1    Subdomain Name(s)
ASN: 0 - Reserved Network Address Blocks
        10.0.0.0/8              1    Subdomain Name(s)
ASN: 14340 - SALESFORCE - Salesforce.com, Inc.
        101.53.160.0/19         1    Subdomain Name(s)
        160.8.0.0/16            3    Subdomain Name(s)
ASN: 15169 - GOOGLE - Google LLC
        35.190.0.0/16           2    Subdomain Name(s)
        104.155.64.0/19         1    Subdomain Name(s)
        34.158.0.0/16           1    Subdomain Name(s)
        35.186.192.0/18         215  Subdomain Name(s)
        146.148.0.0/17          2    Subdomain Name(s)
        35.187.128.0/19         1    Subdomain Name(s)
        2a00:1450:400e::/48     1    Subdomain Name(s)
        34.133.0.0/16           1    Subdomain Name(s)
        2607:f8b0:4004::/48     5    Subdomain Name(s)
        35.244.0.0/14           1    Subdomain Name(s)
        34.96.0.0/17            1    Subdomain Name(s)
        104.199.64.0/19         5    Subdomain Name(s)
        2607:f8b0:400e::/48     6    Subdomain Name(s)
        2001:4860::/32          20   Subdomain Name(s)
        35.224.0.0/14           9    Subdomain Name(s)
        104.154.96.0/19         3    Subdomain Name(s)
        35.204.0.0/15           2    Subdomain Name(s)
        35.200.0.0/15           4    Subdomain Name(s)
        142.250.160.0/19        1    Subdomain Name(s)
        34.135.0.0/16           1    Subdomain Name(s)
        104.197.224.0/19        2    Subdomain Name(s)
        34.98.64.0/18           1    Subdomain Name(s)
        35.240.0.0/14           6    Subdomain Name(s)
        104.199.224.0/19        1    Subdomain Name(s)
        130.211.0.0/17          2    Subdomain Name(s)
        104.198.16.0/20         1    Subdomain Name(s)
        64.233.160.0/19         5    Subdomain Name(s)
        216.239.32.0/20         28   Subdomain Name(s)
        172.217.194.0/24        6    Subdomain Name(s)
        2600:1900::/31          219  Subdomain Name(s)
        34.68.0.0/14            2    Subdomain Name(s)
```

Using Amass tool, found 347 subdomains of Spotify.com

Assets.spotify.com

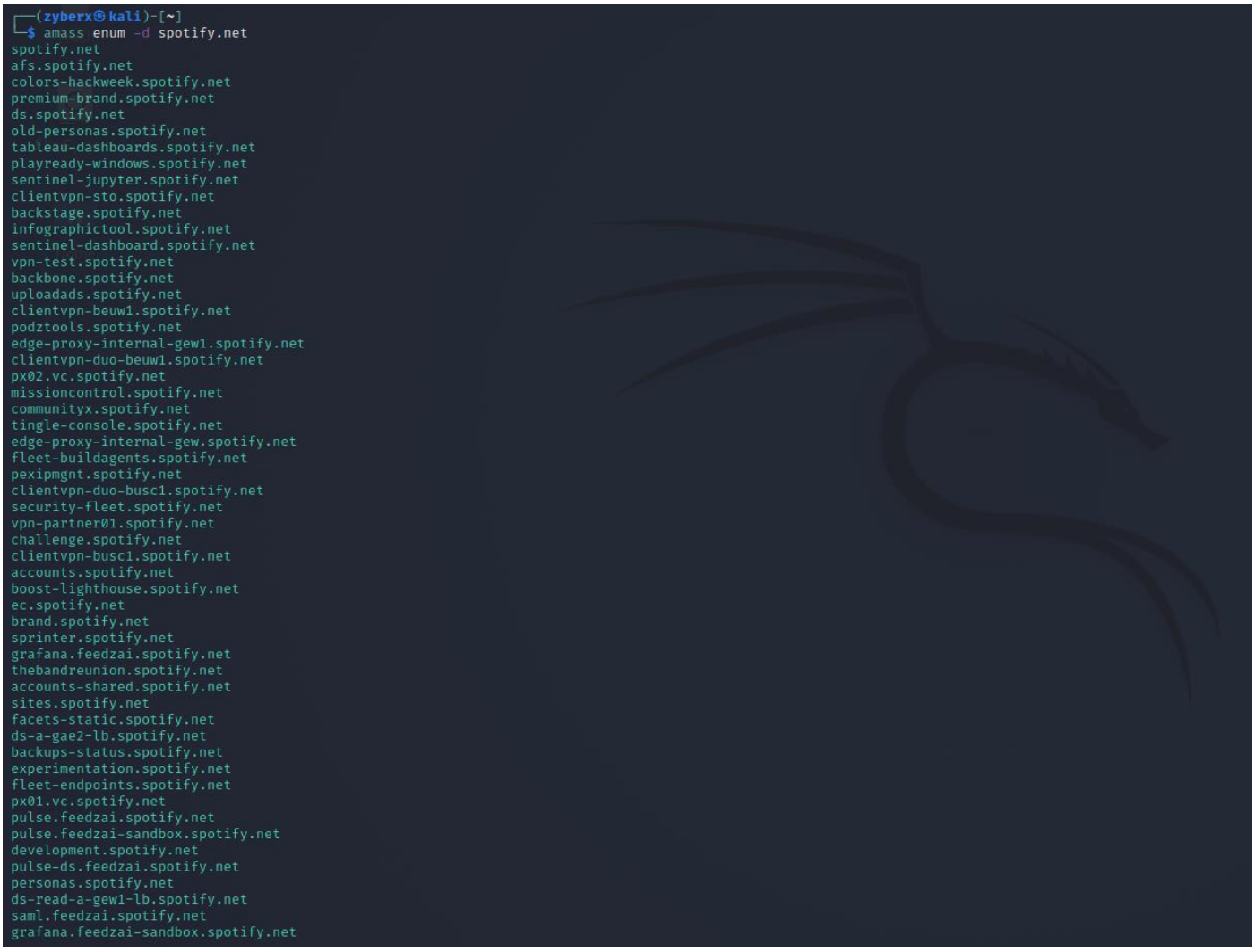
```
┌──(zyberx㉿kali)-[~]
└─$ amass enum -d assets.spotify.com
assets.spotify.com

OWASP Amass v3.15.0                                 https://github.com/OWASP/Amass
--------------------------------------------------------------------------------
1 names discovered - dns: 1
--------------------------------------------------------------------------------
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        13.227.165.0/24         4    Subdomain Name(s)
        2600:9000:21c4::/48     8    Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
```

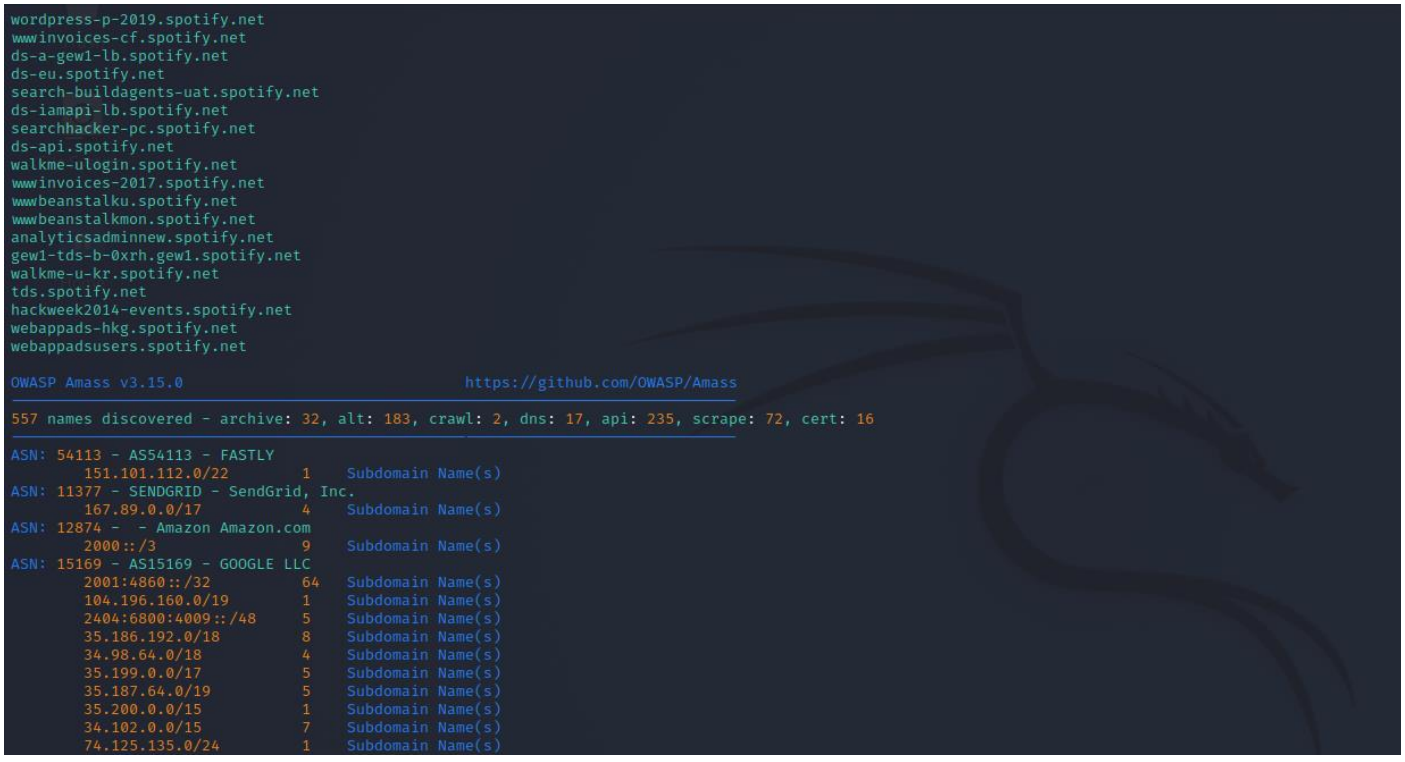
Using Amass tool, found only 1 subdomain of assets.spotify.com

api.spotify.com

```
┌──(zyberx㉿kali)-[~]
└─$ amass enum -d api.spotify.com
api.spotify.com

OWASP Amass v3.15.0                                 https://github.com/OWASP/Amass
--------------------------------------------------------------------------------
1 names discovered - dns: 1
--------------------------------------------------------------------------------
ASN: 15169 - GOOGLE - Google LLC
        35.186.192.0/18         1    Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
```

Using Amass tool, found only 1 subdomain of api.spotify.com





Using Amass tool, found 557 subdomains of spotify.net

Spotifyforbrands.com

```
┌──(zyberx㉿kali)-[~]
└─$ amass enum -d spotifyforbrands.com
spotifyforbrands.com
playlist.spotifyforbrands.com
wpp.spotifyforbrands.com
ipg-partner.spotifyforbrands.com
api1.spotifyforbrands.com
sales.spotifyforbrands.com
sales-staging.spotifyforbrands.com
deckbuilder.spotifyforbrands.com
creativeportfolio.spotifyforbrands.com
creativeportal.spotifyforbrands.com
www.creativeportfolio.spotifyforbrands.com
www.creativeportal.spotifyforbrands.com
api1-staging.spotifyforbrands.com
omnicom-partner-staging.spotifyforbrands.com
partner.spotifyforbrands.com
havas-segments-staging.spotifyforbrands.com
bose-segments.spotifyforbrands.com
sea.spotifyforbrands.com
havas-segments.spotifyforbrands.com
segments-staging.spotifyforbrands.com
havas-partner-staging.spotifyforbrands.com
ipg-partner-staging.spotifyforbrands.com
partner-staging.spotifyforbrands.com
dentsu-partner-staging.spotifyforbrands.com
customsegment-staging.spotifyforbrands.com
ipg-segments-staging.spotifyforbrands.com
segments.spotifyforbrands.com
creativeportfolio-staging.spotifyforbrands.com
wpp-partner-staging.spotifyforbrands.com
ipg-segments.spotifyforbrands.com
www.deckbuilder.spotifyforbrands.com
omg-segments-staging.spotifyforbrands.com
discovery.spotifyforbrands.com
wpp-partner.spotifyforbrands.com
bose-segments-staging.spotifyforbrands.com
publicis-segments-staging.spotifyforbrands.com
omnicom-partner.spotifyforbrands.com
omg-segments.spotifyforbrands.com
demobuilder-staging.spotifyforbrands.com
discovery-staging.spotifyforbrands.com
ru.spotifyforbrands.com
dentsu-partner.spotifyforbrands.com
demobuilder.spotifyforbrands.com
www.bose-segments-staging.spotifyforbrands.com
www-profiles.creativeportal.spotifyforbrands.com
wwwpass.omg-segments.spotifyforbrands.com
wwwvi.havas-segments-staging.spotifyforbrands.com
www.omnicom-partner.spotifyforbrands.com
salesportal.spotifyforbrands.com
www.dentsu-partner-staging.spotifyforbrands.com
wwwgermany.api1.spotifyforbrands.com
api2.spotifyforbrands.com
www2012.sea.spotifyforbrands.com
www.wpp-partner.spotifyforbrands.com
www-container.omnicom-partner-staging.spotifyforbrands.com
www.partner.spotifyforbrands.com
www-admin1.omg-segments-staging.spotifyforbrands.com
www.bose-segments.spotifyforbrands.com
www-april.havas-segments.spotifyforbrands.com
b2b.spotifyforbrands.com
www.ipg-segments-staging.spotifyforbrands.com
wwwy.ipg-partner.spotifyforbrands.com
www.api1.spotifyforbrands.com
api.spotifyforbrands.com
www.discovery.spotifyforbrands.com
www-stg.ipg-segments.spotifyforbrands.com
www-8.omnicom-partner.spotifyforbrands.com
wwwprofile.omg-segments-staging.spotifyforbrands.com

OWASP Amass v3.15.0                                https://github.com/OWASP/Amass
-------------------------------------------------------------------------------
162 names discovered - dns: 1, api: 29, cert: 60, alt: 51, archive: 18, crawl: 3
-------------------------------------------------------------------------------
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        52.24.0.0/13            5    Subdomain Name(s)
ASN: 1257 - AS1257 - TELE2 SVERIGE AB
        193.12.0.0/14           6    Subdomain Name(s)
ASN: 14618 - AMAZON-AES - Amazon.com, Inc.
        3.208.0.0/13            1    Subdomain Name(s)
        52.54.0.0/15            1    Subdomain Name(s)
        3.80.0.0/12             1    Subdomain Name(s)
        54.144.0.0/14           51   Subdomain Name(s)
        34.224.0.0/12           1    Subdomain Name(s)
ASN: 15169 - GOOGLE - Google LLC
        64.233.165.0/24         1    Subdomain Name(s)
        2a00:1450:4010::/48     2    Subdomain Name(s)
        64.233.161.0/24         1    Subdomain Name(s)
        142.251.32.0/19         2    Subdomain Name(s)
        216.239.32.0/20         140  Subdomain Name(s)
        2001:4860::/32          120  Subdomain Name(s)
        172.253.62.0/24         59   Subdomain Name(s)
        2a00:1450:400e::/48     59   Subdomain Name(s)
        2607:f8b0:4004::/48     2    Subdomain Name(s)
        173.194.222.0/24        1    Subdomain Name(s)
        2a00:1450:4006::/48     1    Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
```

Using Amass tool, found 167 subdomains of spotifyforbrands.com

Backstage.io

Using Amass tool, found 5 subdomains of backstage.io

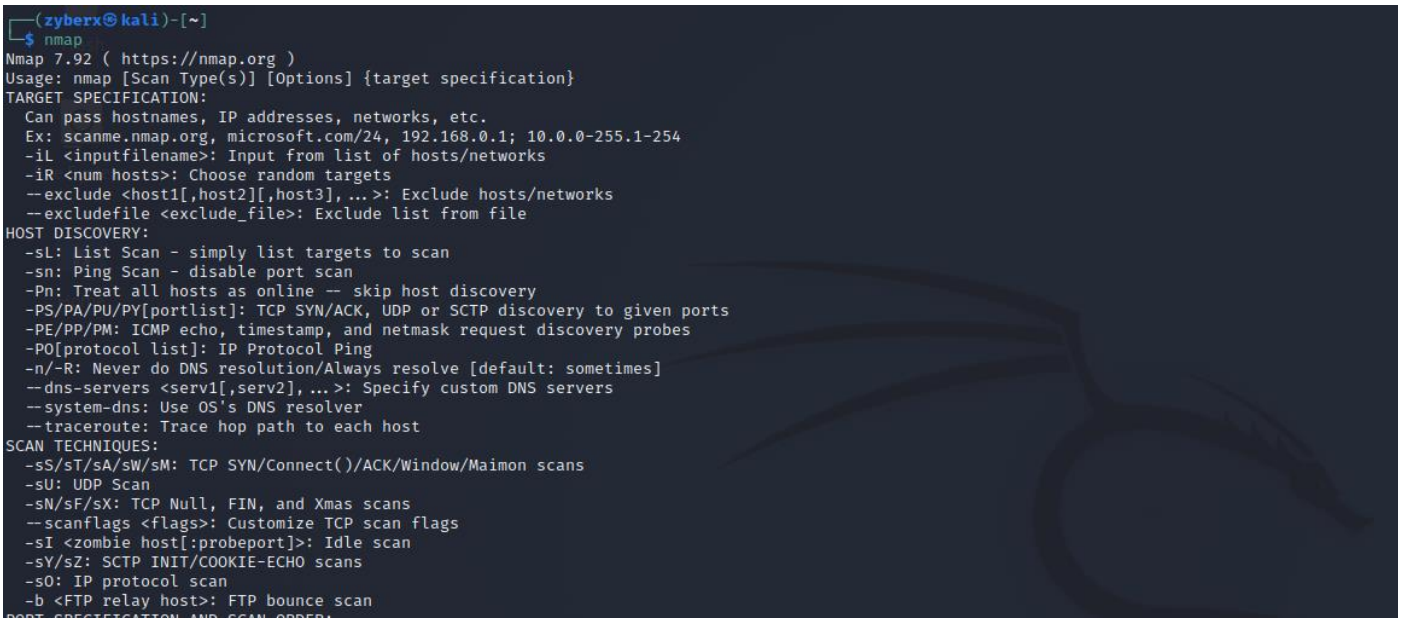
4.2 Find Open Ports and Running Devices on The Network

Nmap

Nmap or network mapper is a type of network scanner which was created by Gordon Lyon. By using this tool, we can discover hosts and services on a computer network by sending packets and analyzing the responses and can be used for security auditing. [6] Some features of the nmap,

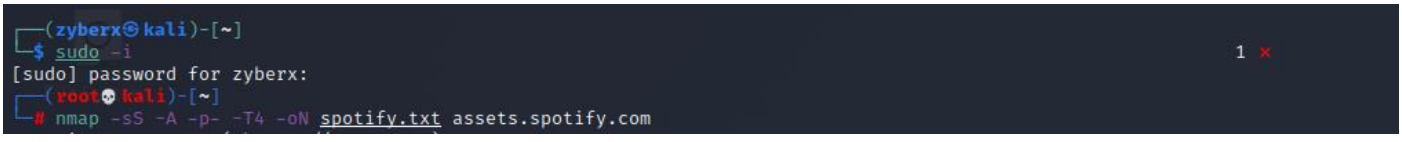
- Find Security issues
- Identify open ports
- Detect vulnerabilities
- Host discovery
- OS version detection
- Provide crucial information

However, if you are using Kali Linux or parrot OS, it comes pre-installed.



To use the nmap tool requires root privileges. Use following command to acquire root permission.

Sudo i & Enter user password



To find open ports and running devices on the targeted domain use following command.

nmap -sS -A -p- -T4 -oN *DOMAIN NAME*

Finding open ports and running devices on spotify.com

```
┌──(root💀kali)-[~]
└─# nmap -sS -A -p- -T4 -oN spotify.txt spotify.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 11:58 EDT
Nmap scan report for spotify.com (35.186.224.25)
Host is up (0.0066s latency).
Other addresses for spotify.com (not scanned): 2600:1901:1:c36::
rDNS record for 35.186.224.25: 25.224.186.35.bc.googleusercontent.com
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
25/tcp  open  smtp?
| fingerprint-strings:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, LDAPSearchReq, RTSPRequest:
|     452 syntax error (connecting)
|     many errors
|   Hello, Help, Kerberos, LPDString, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     452 syntax error (connecting)
|   LANDesk-RC, NotesRPC, SIPOptions, WMSRequest, giop, ms-sql-s, oracle-tns:
|_    421 4.2.1 please try again later
|_smtp-commands: SMTP EHLO spotify.com: failed to receive data: connection closed
80/tcp  open  http      envoy
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP:
|     HTTP/1.0 400 Bad Request
|     Content-Length: 54
|     Content-Type: text/html; charset=UTF-8
|     Date: Fri, 03 Jun 2022 16:07:27 GMT
|     <html><title>Error 400 (Bad Request)!!1</title></html>
|   FourOhFourRequest:
|     HTTP/1.0 301 Moved Permanently
|     location: https://35.186.224.25/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     date: Fri, 03 Jun 2022 16:07:16 GMT
|     server: envoy
|     content-length: 0
|     Via: 1.1 google
|   GetRequest, HTTPOptions:
|     HTTP/1.0 301 Moved Permanently
|     location: https://35.186.224.25/
|     date: Fri, 03 Jun 2022 16:07:10 GMT
|     server: envoy
|     content-length: 0
|     Via: 1.1 google
|   Help:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/html; charset=UTF-8
|     Referrer-Policy: no-referrer
|     Content-Length: 273
|     Date: Fri, 03 Jun 2022 16:07:27 GMT
|     <html><head>
|     <meta http-equiv="content-type" content="text/html;charset=utf-8">
|     <title>400 Bad Request</title>
|     </head>
|     <body text=#000000 bgcolor=#ffffff>
|     <h1>Error: Bad Request</h1>
|     <h2>Your client has issued a malformed or illegal request.</h2>
|     <h2></h2>
|     </body></html>
|   RTSPRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/html; charset=UTF-8
|     Referrer-Policy: no-referrer
|     Content-Length: 273
|     Date: Fri, 03 Jun 2022 16:07:11 GMT
|     <html><head>
|     <meta http-equiv="content-type" content="text/html;charset=utf-8">
|     <title>400 Bad Request</title>
|     </head>
|     <body text=#000000 bgcolor=#ffffff>
|     <h1>Error: Bad Request</h1>
|     <h2>Your client has issued a malformed or illegal request.</h2>
|     <h2></h2>
|_    </body></html>
|_http-title: Did not follow redirect to https://www.spotify.com/
|_http-server-header: envoy
443/tcp open  ssl/https envoy
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     HTTP/1.0 400 Bad Request
|     Content-Length: 54
|     Content-Type: text/html; charset=UTF-8
|     Date: Fri, 03 Jun 2022 16:07:28 GMT
|     <html><title>Error 400 (Bad Request)!!1</title></html>
```

```
FourOhFourRequest, HTTPOptions:
  HTTP/1.0 404 Not Found
  vary: Accept-Encoding
  date: Fri, 03 Jun 2022 16:07:17 GMT
  server: envoy
  Content-Length: 0
  Via: HTTP/2 edgeproxy, 1.1 google
  Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
GetRequest:
  HTTP/1.0 404 Not Found
  vary: Accept-Encoding
  date: Fri, 03 Jun 2022 16:07:16 GMT
  server: envoy
  Content-Length: 0
  Via: HTTP/2 edgeproxy, 1.1 google
  Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
RTSPRequest:
  HTTP/1.0 400 Bad Request
  Content-Type: text/html; charset=UTF-8
  Referrer-Policy: no-referrer
  Content-Length: 273
  Date: Fri, 03 Jun 2022 16:07:23 GMT
  <html><head>
  <meta http-equiv="content-type" content="text/html;charset=utf-8">
  <title>400 Bad Request</title>
  </head>
  <body text=#000000 bgcolor=#ffffff>
  <h1>Error: Bad Request</h1>
  <h2>Your client has issued a malformed or illegal request.</h2>
  <h2></h2>
  </body></html>
tor-versions:
  HTTP/1.0 400 Bad Request
```

```
SF:\r\n\r\n\n<html><head>\n<meta\x20http-equiv=\"content-type\"\x20content
SF:=\"text/html;charset=utf-8\">\n<title>400\x20Bad\x20Request</title>\n</
SF:head>\n<body\x20text=#000000\x20bgcolor=#ffffff>\n<h1>Error:\x20Bad\x20
SF:Request</h1>\n<h2>Your\x20client\x20has\x20issued\x20a\x20malformed\x20
SF:or\x20illegal\x20request\.</h2>\n<h2></h2>\n</body></html>\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.92%T=SSL%I=7%D=6/3%Time=629A31B5%P=x86_64-pc-linux-gnu%
SF:r(GetRequest,D4,"HTTP/1\.0\x20404\x20Not\x20Found\r\nvary:\x20Accept-En
SF:coding\r\ndate:\x20Fri,\x2003\x20Jun\x202022\x2016:07:16\x20GMT\r\nserv
SF:er:\x20envoy\r\nContent-Length:\x200\r\nVia:\x20HTTP/2\x20edgeproxy,\x2
SF:01\.1\x20google\r\nAlt-Svc:\x20h3=\":443\";\x20ma=2592000,h3-29=\":443\
SF:";\x20ma=2592000\r\n\r\n")%r(HTTPOptions,D4,"HTTP/1\.0\x20404\x20Not\x2
SF:0Found\r\nvary:\x20Accept-Encoding\r\ndate:\x20Fri,\x2003\x20Jun\x20202
SF:2\x2016:07:17\x20GMT\r\nserver:\x20envoy\r\nContent-Length:\x200\r\nVia
SF::\x20HTTP/2\x20edgeproxy,\x201\.1\x20google\r\nAlt-Svc:\x20h3=\":443\";
SF:\x20ma=2592000,h3-29=\":443\";\x20ma=2592000\r\n\r\n")%r(FourOhFourRequ
SF:est,D4,"HTTP/1\.0\x20404\x20Not\x20Found\r\nvary:\x20Accept-Encoding\r\
SF:ndate:\x20Fri,\x2003\x20Jun\x202022\x2016:07:17\x20GMT\r\nserver:\x20en
SF:voy\r\nContent-Length:\x200\r\nVia:\x20HTTP/2\x20edgeproxy,\x201\.1\x20
SF:google\r\nAlt-Svc:\x20h3=\":443\";\x20ma=2592000,h3-29=\":443\";\x20ma=
SF:2592000\r\n\r\n")%r(tor-versions,B3,"HTTP/1\.0\x20400\x20Bad\x20Request
SF:\r\nContent-Length:\x2054\r\nContent-Type:\x20text/html;\x20charset=UTF
SF:-8\r\nDate:\x20Fri,\x2003\x20Jun\x202022\x2016:07:18\x20GMT\r\n\r\n<htm
SF:l><title>Error\x20400\x20\(Bad\x20Request\)!!1</title></html>")%r(RTSPR
SF:equest,1AD,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text
SF:/html;\x20charset=UTF-8\r\nReferrer-Policy:\x20no-referrer\r\nContent-L
SF:ength:\x20273\r\nDate:\x20Fri,\x2003\x20Jun\x202022\x2016:07:23\x20GMT\
SF:r\n\r\n\n<html><head>\n<meta\x20http-equiv=\"content-type\"\x20content=
SF:\"text/html;charset=utf-8\">\n<title>400\x20Bad\x20Request</title>\n</h
SF:ead>\n<body\x20text=#000000\x20bgcolor=#ffffff>\n<h1>Error:\x20Bad\x20R
SF:equest</h1>\n<h2>Your\x20client\x20has\x20issued\x20a\x20malformed\x20o
SF:r\x20illegal\x20request\.</h2>\n<h2></h2>\n</body></html>\n")%r(DNSVers
SF:ionBindReqTCP,B3,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Length:
SF:\x2054\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nDate:\x20Fri,
SF:\x2003\x20Jun\x202022\x2016:07:28\x20GMT\r\n\r\n<html><title>Error\x204
SF:00\x20\(Bad\x20Request\)!!1</title></html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 3.X, Microsoft Windows XP|7|2012
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:wind
ows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Actiontec MI424WR-GEN3I WAP, Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7
or Windows Server 2012
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.15 ms 192.168.109.2
2   0.08 ms 25.224.186.35.bc.googleusercontent.com (35.186.224.25)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 603.38 seconds
```

Finding open ports and running devices assests.spotify.com

```
┌──(zyberx㉿kali)-[~]
└─$ sudo -i                                                                    1 ×
[sudo] password for zyberx:
┌──(root💀kali)-[~]
└─# nmap -sS -A -p- -T4 -oN spotify.txt assets.spotify.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 12:23 EDT
Nmap scan report for assets.spotify.com (13.224.250.78)
Host is up (0.0029s latency).
Other addresses for assets.spotify.com (not scanned): 13.224.250.10 13.224.250.109 13.224.250.52 2600:9000:21b4:aa0
0:3:5f0f:dbc0:93a1 2600:9000:21b4:b600:3:5f0f:dbc0:93a1 2600:9000:21b4:3000:3:5f0f:dbc0:93a1 2600:9000:21b4:8a00:3:
5f0f:dbc0:93a1 2600:9000:21b4:ca00:3:5f0f:dbc0:93a1 2600:9000:21b4:ce00:3:5f0f:dbc0:93a1 2600:9000:21b4:7400:3:5f0f
:dbc0:93a1 2600:9000:21b4:a400:3:5f0f:dbc0:93a1
rDNS record for 13.224.250.78: server-13-224-250-78.sin52.r.cloudfront.net
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
25/tcp  open  tcpwrapped
|_smtp-commands: SMTP EHLO assets.spotify.com: failed to receive data: connection closed
80/tcp  open  tcpwrapped
|_http-title: Did not follow redirect to https://assets.spotify.com/
|_http-server-header: CloudFront
443/tcp open  tcpwrapped
|_http-title: ERROR: The request could not be satisfied
|_http-server-header: CloudFront
| ssl-cert: Subject: commonName=assets.spotify.com/organizationName=Spotify AB/countryName=SE
| Subject Alternative Name: DNS:assets.spotify.com
| Not valid before: 2020-01-27T00:00:00
|_Not valid after:  2022-04-27T12:00:00
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP
SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual NAT device
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.15 ms 192.168.109.2
2   0.07 ms server-13-224-250-78.sin52.r.cloudfront.net (13.224.250.78)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 152.15 seconds
```

Finding open ports and running devices api.spotify.com

```
┌──(root💀kali)-[~]
└─# nmap -sS -A -p- -T4 -oN spotify.txt api.spotify.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 12:32 EDT
Nmap scan report for api.spotify.com (35.186.224.25)
Host is up (0.0028s latency).
Other addresses for api.spotify.com (not scanned): 2600:1901:1:c36::
rDNS record for 35.186.224.25: 25.224.186.35.bc.googleusercontent.com
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE        VERSION
25/tcp  open  tcpwrapped
|_smtp-commands: SMTP EHLO api.spotify.com: failed to receive data: connection closed
80/tcp  open  tcpwrapped
|_http-title: Did not follow redirect to https://api.spotify.com/
|_http-server-header: envoy
443/tcp open  ssl/tcpwrapped
| http-robots.txt: 1 disallowed entry
|_/
| http-title: Home | Spotify for Developers
|_Requested resource was https://developer.spotify.com/
| ssl-cert: Subject: commonName=*.spotify.com/organizationName=Spotify AB/countryName=SE
| Subject Alternative Name: DNS:*.spotify.com, DNS:spotify.com
| Not valid before: 2022-04-06T00:00:00
|_Not valid after:  2023-04-06T23:59:59
|_ssl-date: TLS randomness does not represent time
|_http-server-header: envoy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Brother MFC-7820N printer (94%), Digi Connect ME serial-to-Ethernet bridge (94%), Netgear SC101 Storage Central NAS device (91%), Aastra 480i I
one or Apple AirPort Express WAP (91%), GoPro HERO3 camera (91%), Konica Minolta bizhub 250 printer (91%), OUYA game console (91%), Crestron MPC-M5 AV controller or W
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.14 ms 192.168.109.2
2   0.06 ms 25.224.186.35.bc.googleusercontent.com (35.186.224.25)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 165.79 seconds
```

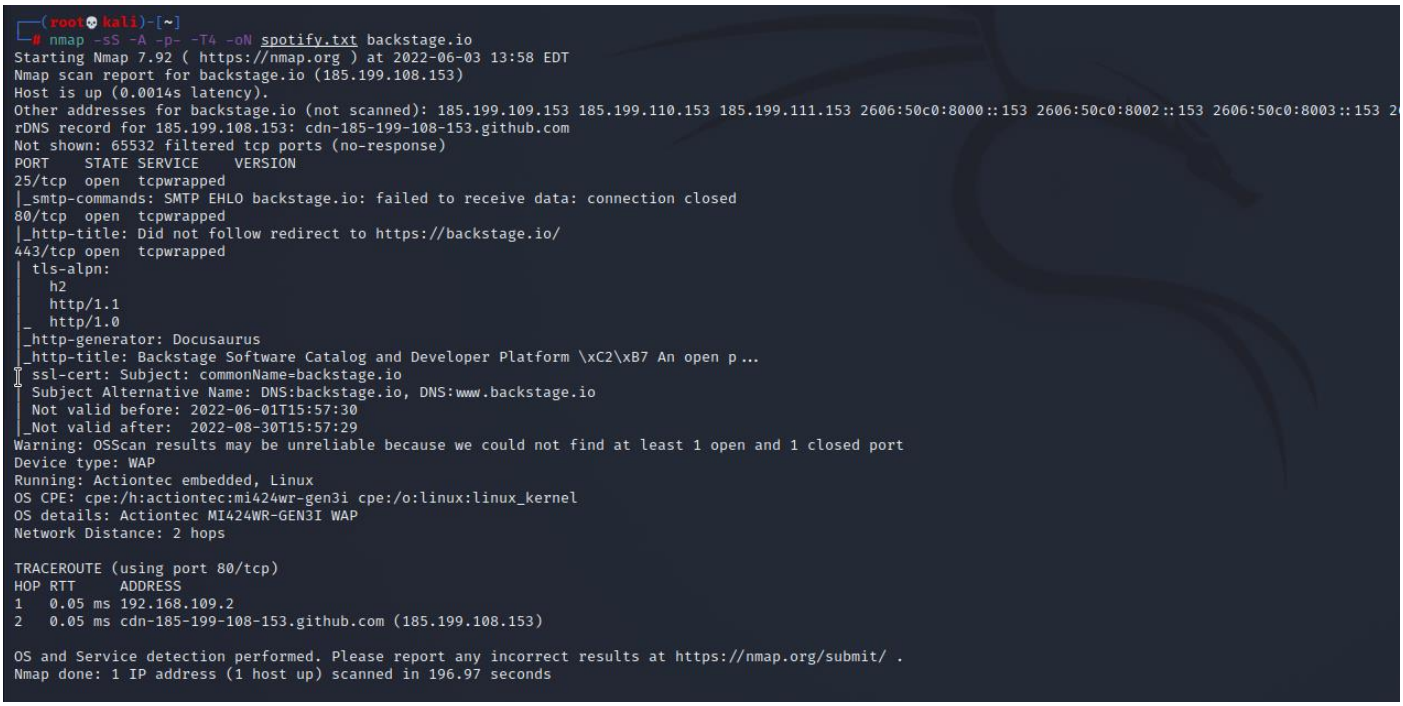
Finding open ports and running devices spotify.net

```
┌──(root💀kali)-[~]
└─# nmap -sS -A -p- -T4 -oN spotify.txt spotify.net
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 12:36 EDT
Nmap scan report for spotify.net (35.227.201.204)
Host is up (0.0051s latency).
rDNS record for 35.227.201.204: 204.201.227.35.bc.googleusercontent.com
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
25/tcp  open  smtp?
| fingerprint-strings:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, LDAPSearchReq, RTSPRequest:
|     452 syntax error (connecting)
|     many errors
|   Hello, Help, Kerberos, LPDString, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     452 syntax error (connecting)
|   NCP, NotesRPC, SIPOptions, TerminalServer, WMSRequest, giop, ms-sql-s, oracle-tns:
|_    421 4.2.1 please try again later
|_smtp-commands: SMTP EHLO spotify.net: failed to receive data: connection closed
80/tcp  open  http     Apache httpd
|_http-title: Did not follow redirect to https://spotify.net/mellon/login?ReturnTo=https%3A%2F%2Fspotify.net%2F&IdP=http%3A%2F%2Fwww.okta.com%2Fexk6vfwgijPqP7VZg1t7
443/tcp open  ssl/http Apache httpd
| tls-alpn:
|   grpc-exp
|   h2
|_  http/1.1
| ssl-cert: Subject: commonName=*.spotify.net/organizationName=Spotify AB/countryName=SE
| Subject Alternative Name: DNS:*.spotify.net, DNS:spotify.net
| Not valid before: 2022-01-20T00:00:00
|_Not valid after:  2023-01-20T23:59:59
| tls-nextprotoneg:
|   grpc-exp
|   h2
|_  http/1.1
|_http-title: Did not follow redirect to https://spotify.okta.com/app/spotifyprod_spotifynet_1/exk6vfwgijPqP7VZg1t7/sso/saml?SAMLRequest=hZLdTgIxEIVfZdN76C5%2FxQZIkIWERA0B9cI
GogpOe4MWtTMFoKZMb6aXF7rTjnUZPPnM5%2BKL5G%2BFQYRA1jsRLdOx2PbPh2qozuaJmneT4SBeqF46V0maqFnaSxZTEd1CQJ4fC5azCLGCpUMyjrgUdzqteNCKu9fJQHfPdF%2FdiShlBusMNaoHohK1lFh6srvXtn8i0858IU1
5DOqhD4bdmizG1mSUQLHzJoEh%2BLnckRaq4VR2OP8FmZfiRVL6sKCBsIR5vBzfriJxW7lgXkuXey9Ehr4AZvF5NRbVg3qYXJb6qR%2FDoxOl3DFcMs05Vnv6%2B128L8w1pX7H1r14xqCsahZWamYE%2FPswCGmIxCBUJOTiu%2F3
p%3A%2F%2Fwww.w3.org%2F2001%2F04%2Fxmldsig-more%23rsa-sha256&Signature=TiolqvD2M%2Bev%2BlcTwVWIbfMSE2JbqUPzCG8Su9tTwaQz6P2srECgyOXduW0kX0nKeU8SnDHwHaCGBuhCzF9NpfXVpyO1WvLz1ve
3jRUqrjIyaMHca78s%2B1wYGntnA93PFXXuysf3%2Fw9eSFEpEK8dkhBJ3OiXDf1auFC7ODIcyhYVlQUR94uyckK6mfuT%2BzgDMryy5Kr9it6hGwK6cOD0eGdr2zNAnBvljW1MFZusc7pcmSHi0SIKsmI8QnwCYqvIv0IFajClW7J
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.92%I=7%D=6/3%Time=629A391B%P=x86_64-pc-linux-gnu%r(Hello
SF:,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Help,1F,"452\x20s
SF:yntax\x20error\x20\(connecting\)\r\n")%r(GenericLines,34,"452\x20syntax
SF:\x20error\x20\(connecting\)\r\n421\x20too\x20many\x20errors\r\n")%r(Get
SF:Request,34,"452\x20syntax\x20error\x20\(connecting\)\r\n421\x20too\x20m
SF:any\x20errors\r\n")%r(HTTPOptions,34,"452\x20syntax\x20error\x20\(conne
SF:cting\)\r\n421\x20too\x20many\x20errors\r\n")%r(RTSPRequest,34,"452\x20
SF:syntax\x20error\x20\(connecting\)\r\n421\x20too\x20many\x20errors\r\n")
SF:%r(SSLSessionReq,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(T
SF:erminalServerCookie,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%
SF:r(TLSSessionReq,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Ke
SF:rberos,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(FourOhFourR
SF:equest,34,"452\x20syntax\x20error\x20\(connecting\)\r\n421\x20too\x20ma
SF:ny\x20errors\r\n")%r(LPDString,1F,"452\x20syntax\x20error\x20\(connecti
SF:ng\)\r\n")%r(LDAPSearchReq,34,"452\x20syntax\x20error\x20\(connecting\)
SF:\r\n421\x20too\x20many\x20errors\r\n")%r(SIPOptions,22,"421\x204\.2\.1\
SF:x20please\x20try\x20again\x20later\r\n")%r(TerminalServer,22,"421\x204\
SF-Port25-TCP:V=7.92%I=7%D=6/3%Time=629A391B%P=x86_64-pc-linux-gnu%r(Hello
SF:,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Help,1F,"452\x20s
SF:yntax\x20error\x20\(connecting\)\r\n")%r(GenericLines,34,"452\x20syntax
SF:\x20error\x20\(connecting\)\r\n421\x20too\x20many\x20errors\r\n")%r(Get
SF:Request,34,"452\x20syntax\x20error\x20\(connecting\)\r\n421\x20too\x20m
SF:any\x20errors\r\n")%r(HTTPOptions,34,"452\x20syntax\x20error\x20\(conne
SF:cting\)\r\n421\x20too\x20many\x20errors\r\n")%r(RTSPRequest,34,"452\x20
SF:syntax\x20error\x20\(connecting\)\r\n421\x20too\x20many\x20errors\r\n")
SF:%r(SSLSessionReq,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(T
SF:erminalServerCookie,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%
SF:r(TLSSessionReq,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Ke
SF:rberos,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(FourOhFourR
SF:equest,34,"452\x20syntax\x20error\x20\(connecting\)\r\n421\x20too\x20ma
SF:ny\x20errors\r\n")%r(LPDString,1F,"452\x20syntax\x20error\x20\(connecti
SF:ng\)\r\n")%r(LDAPSearchReq,34,"452\x20syntax\x20error\x20\(connecting\)
SF:\r\n421\x20too\x20many\x20errors\r\n")%r(SIPOptions,22,"421\x204\.2\.1\
SF:x20please\x20try\x20again\x20later\r\n")%r(TerminalServer,22,"421\x204\
SF:.2\.1\x20please\x20try\x20again\x20later\r\n")%r(NCP,22,"421\x204\.2\.1
SF:\x20please\x20try\x20again\x20later\r\n")%r(NotesRPC,22,"421\x204\.2\.1
SF:\x20please\x20try\x20again\x20later\r\n")%r(WMSRequest,22,"421\x204\.2\
SF:.1\x20please\x20try\x20again\x20later\r\n")%r(oracle-tns,22,"421\x204\.
SF:2\.1\x20please\x20try\x20again\x20later\r\n")%r(ms-sql-s,22,"421\x204\.
SF:2\.1\x20please\x20try\x20again\x20later\r\n")%r(giop,22,"421\x204\.2\.1
SF:\x20please\x20try\x20again\x20later\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X, Microsoft Windows XP|7|2012
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windo
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.09 ms 192.168.109.2
2   0.14 ms 204.201.227.35.bc.googleusercontent.com (35.227.201.204)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 229.09 seconds
```

Finding open ports and running devices spotifyforbrands.com

```
┌──(root💀kali)-[~]
└─# nmap -sS -A -p- -T4 -oN spotify.txt spotifyforbrands.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 13:37 EDT
Nmap scan report for spotifyforbrands.com (216.239.36.21)
Host is up (0.0058s latency).
Other addresses for spotifyforbrands.com (not scanned): 216.239.38.21 216.239.34.21 216.239.32.21 2001:4860:4802:34::15 2001:4860:4802:36::15 2001:4860:4802:38
rDNS record for 216.239.36.21: any-in-2415.1e100.net
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
25/tcp  open  smtp?
| fingerprint-strings:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, LDAPSearchReq, RTSPRequest:
|     452 syntax error (connecting)
|     many errors
|   Hello, Help, Kerberos, LPDString, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     452 syntax error (connecting)
|   NCP, NotesRPC, SIPOptions, TerminalServer, WMSRequest, giop, ms-sql-s, oracle-tns:
|_    421 4.2.1 please try again later
|_smtp-commands: SMTP EHLO spotifyforbrands.com: failed to receive data: connection closed
80/tcp  open  http       Google httpd
|_http-title: Error 404 (Not Found)!!1
|_http-server-header: ghs
443/tcp open  ssl/https?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
SF-Port25-TCP:V=7.92%I=7%D=6/3%Time=629A4B3A%P=x86_64-pc-linux-gnu%r(Hello
SF:,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Help,1F,"452\x20s
SF:yntax\x20error\x20\(connecting\)\r\n")%r(GenericLines,34,"452\x20syntax
SF:\x20error\x20\(connecting\)\r\n421\x20too\x20many\x20errors\r\n")%r(Get
SF:Request,34,"452\x20syntax\x20error\x20\(connecting\)\r\n421\x20too\x20m
SF:any\x20errors\r\n")%r(HTTPOptions,34,"452\x20syntax\x20error\x20\(conne
SF:cting\)\r\n421\x20too\x20many\x20errors\r\n")%r(RTSPRequest,34,"452\x20
SF:syntax\x20error\x20\(connecting\)\r\n421\x20too\x20many\x20errors\r\n")
SF:%r(SSLSessionReq,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(T
SF:erminalServerCookie,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%
SF:r(TLSSessionReq,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Ke
SF:rberos,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(FourOhFourR
SF:equest,34,"452\x20syntax\x20error\x20\(connecting\)\r\n421\x20too\x20ma
SF:ny\x20errors\r\n")%r(LPDString,1F,"452\x20syntax\x20error\x20\(connecti
SF:ng\)\r\n")%r(LDAPSearchReq,34,"452\x20syntax\x20error\x20\(connecting\)
SF:\r\n421\x20too\x20many\x20errors\r\n")%r(SIPOptions,22,"421\x204\.2\.1\
SF:x20please\x20try\x20again\x20later\r\n")%r(TerminalServer,22,"421\x204\
SF:.2\.1\x20please\x20try\x20again\x20later\r\n")%r(NCP,22,"421\x204\.2\.1
SF:\x20please\x20try\x20again\x20later\r\n")%r(NotesRPC,22,"421\x204\.2\.1
SF:\x20please\x20try\x20again\x20later\r\n")%r(WMSRequest,22,"421\x204\.2\
SF:.1\x20please\x20try\x20again\x20later\r\n")%r(oracle-tns,22,"421\x204\.
SF:2\.1\x20please\x20try\x20again\x20later\r\n")%r(ms-sql-s,22,"421\x204\.
SF:2\.1\x20please\x20try\x20again\x20later\r\n")%r(giop,22,"421\x204\.2\.1
SF:\x20please\x20try\x20again\x20later\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X, Microsoft Windows XP|7|2012
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp::sp
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows S
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
```

Finding open ports and running devices backstage.io



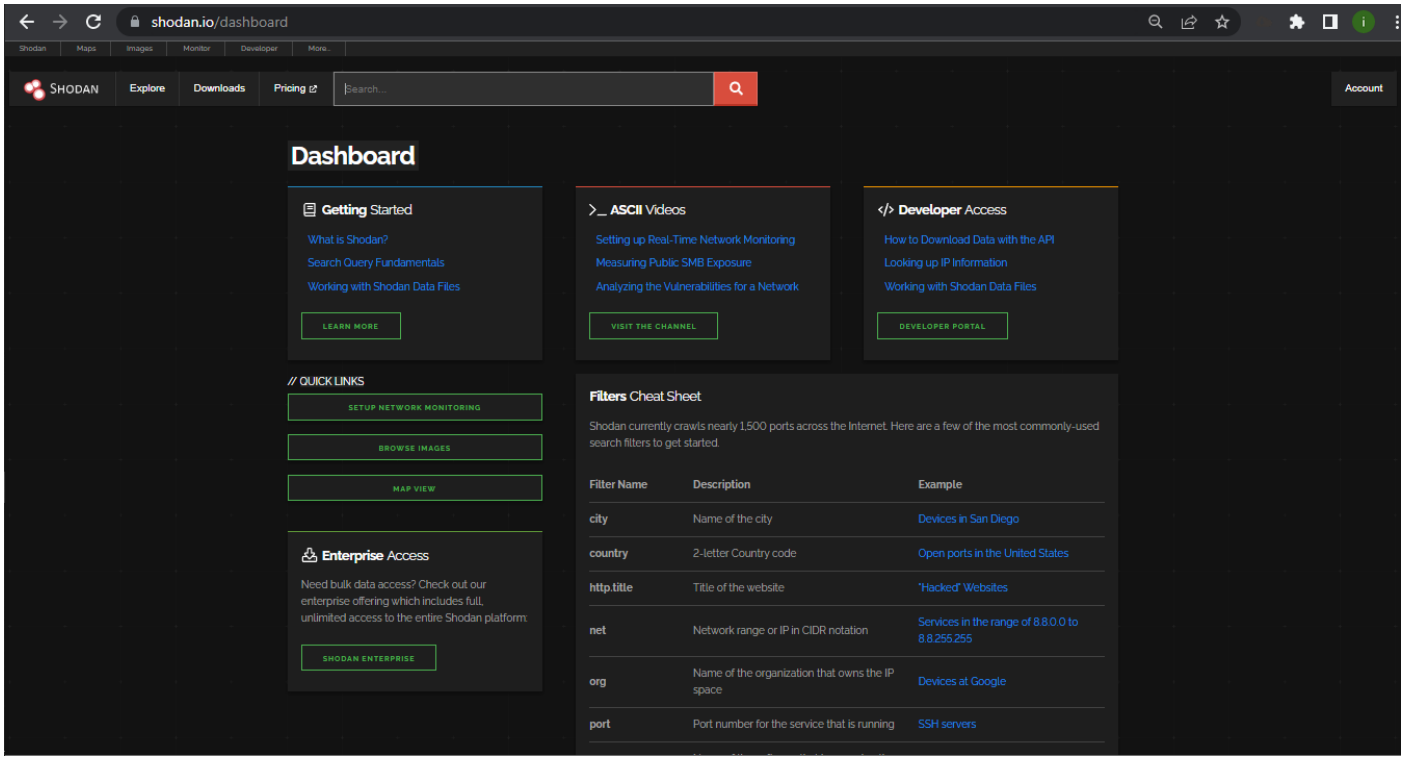
4.3 Public Device Enumeration

Shodan.io

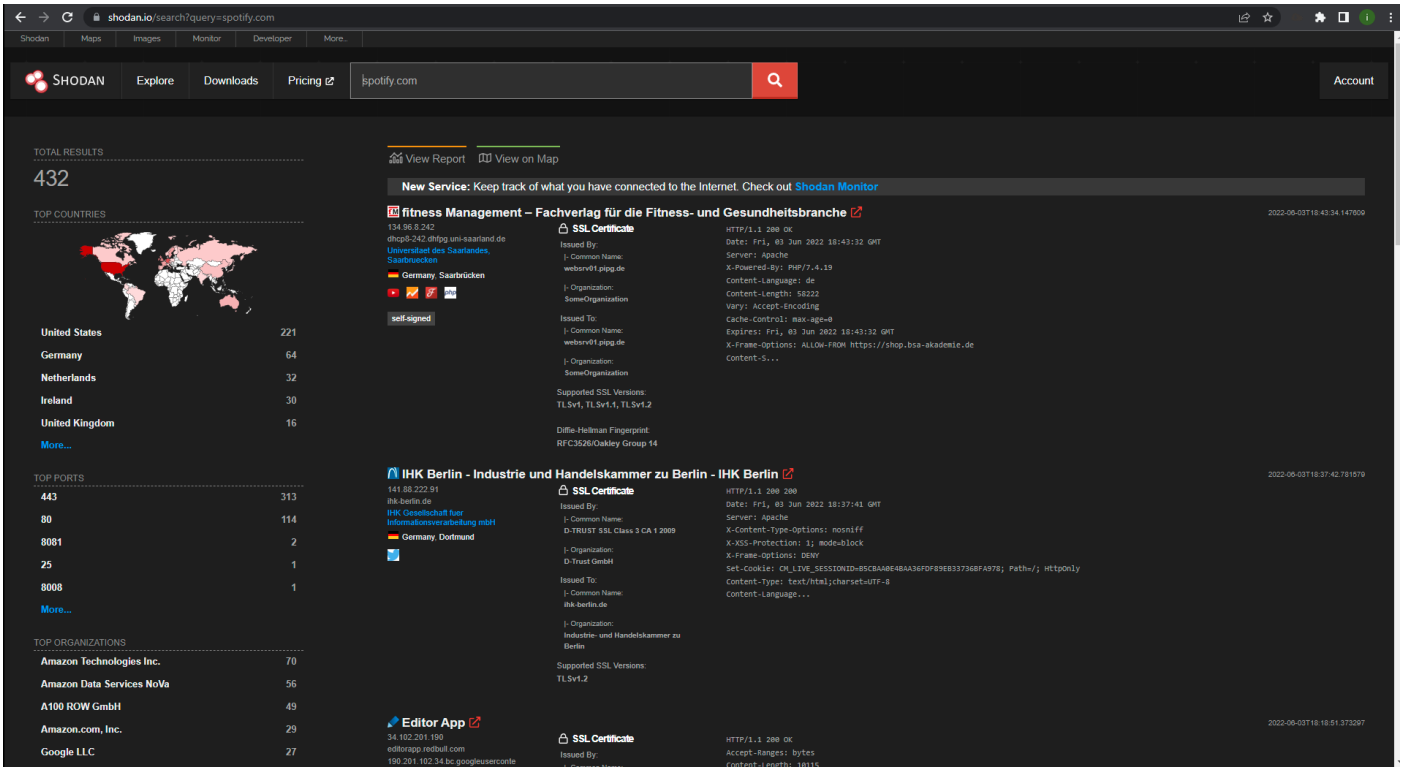
Shodan is a search engine that allows users to search for various types of internet-connected servers (webcams, routers, servers, and so on) using a number of filters. Some have referred to it as a search engine for service banners, which are metadata that the server sends back to the client. This metadata can include information about the server software, what options the service supports, a welcome message, or anything else the client can learn before interacting with the server.

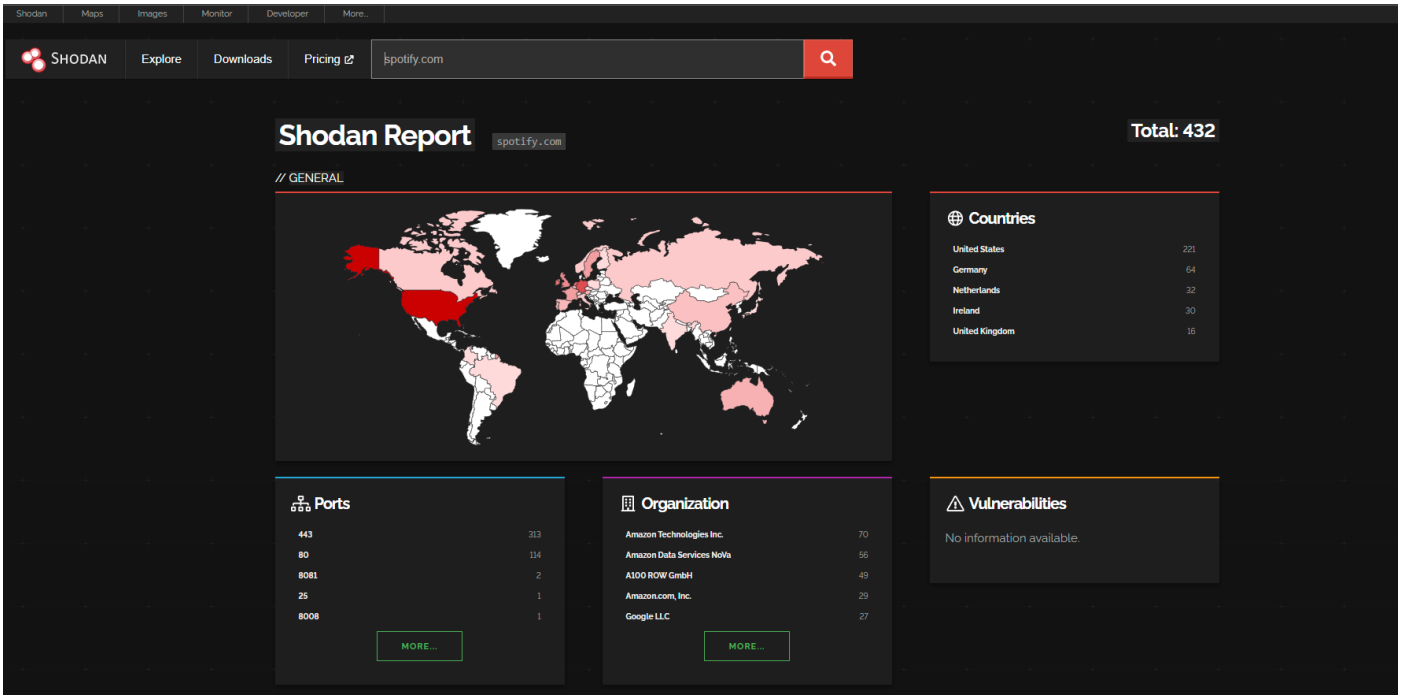
Shodan primarily collects data from web servers (HTTP/HTTPS - ports 80, 8080, 443, 8443), as well as FTP (port 21), SSH (port 22), Telnet (port 23), SNMP (port 161), IMAP (ports 143 or (encrypted) 993), SMTP (port 25), SIP (port 5060), and Real Time Streaming Protocol (port 5060), [2]

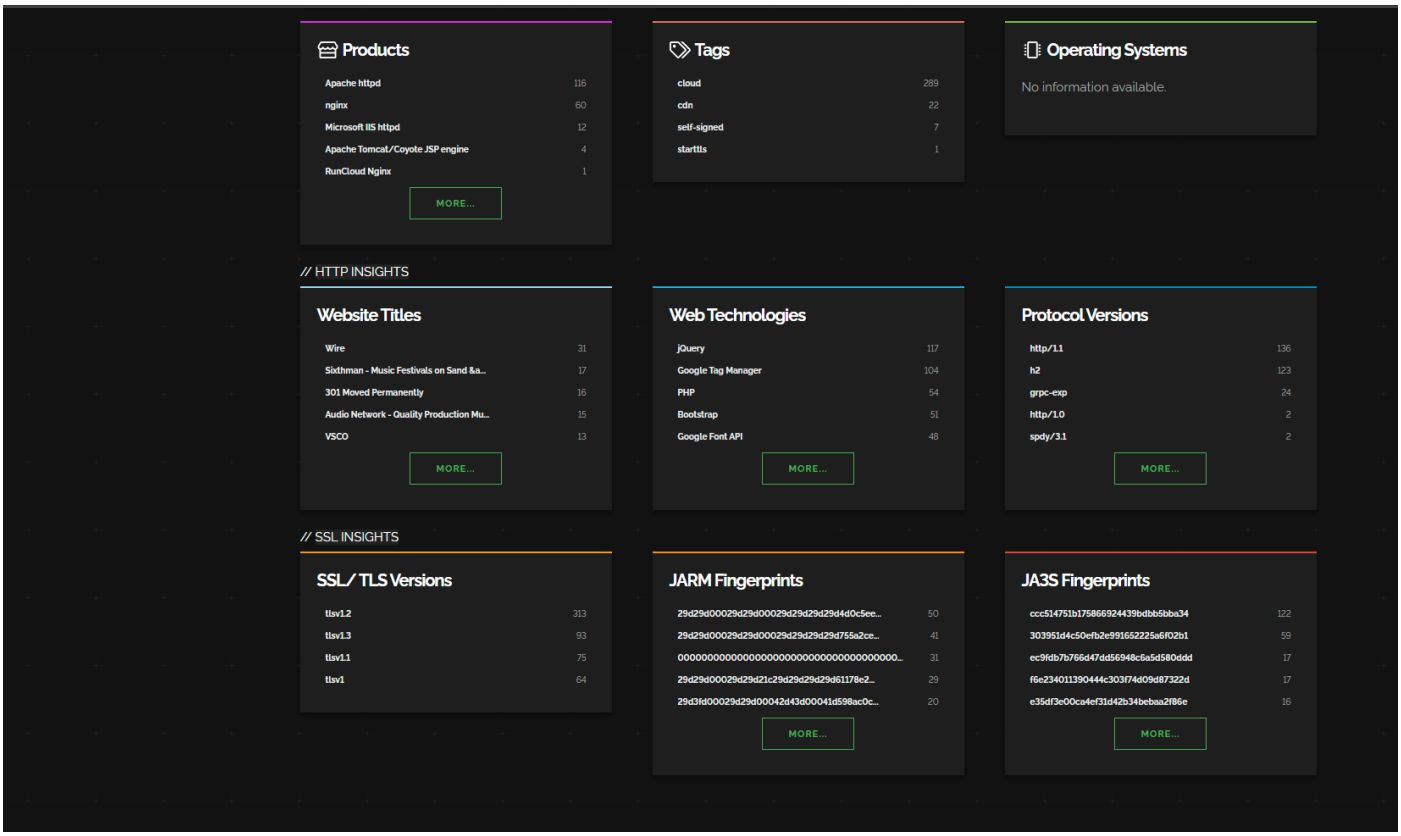
https://www.shodan.io/dashboard Click here to visit the website.



Shordan io search results for Spotify.com

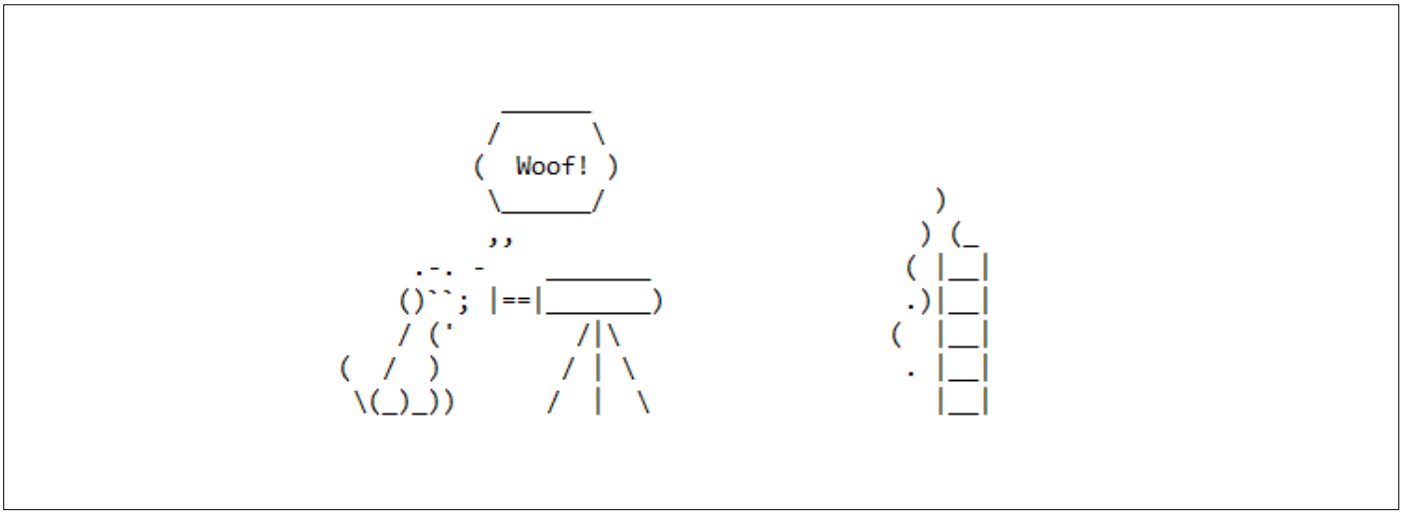





Products
Apache httpd 116
nginx 60
Microsoft IIS httpd 12
Apache Tomcat/Coyote JSP engine 4
RunCloud Nginx 1
MORE...
Tags
cloud 289
cdn 22
self-signed 7
starttls 1
Operating Systems
No information available.
// HTTP INSIGHTS
Website Titles
Wire 31
Sixthman - Music Festivals on Sand &a... 17
301 Moved Permanently 16
Audio Network - Quality Production Mu... 15
VSCO 13
MORE...
Web Technologies
jQuery 117
Google Tag Manager 104
PHP 54
Bootstrap 51
Google Font API 48
MORE...
Protocol Versions
http/1.1 136
h2 123
grpc-exp 24
http/1.0 2
spdy/3.1 2
MORE...
// SSL INSIGHTS
SSL/TLS Versions
tlsv1.2 313
tlsv1.3 93
tlsv1.1 75
tlsv1 64
JARM Fingerprints
29d29d00029d29d00029d29d29d29d4d0c5ee... 50
29d29d00029d29d00029d29d29d29d755a2ce... 41
00000000000000000000000000000000000000... 31
29d29d00029d29d21c29d29d29d29d61178e2... 29
29d3fd00029d29d00042d43d00041d598ac0c... 20
MORE...
JA3S Fingerprints
ccc514751b1758669244 39bdbb5bba34 122
303951d4c50efb2e991652225a6f02b1 59
ec9fdb7b766d47dd56948c6a5d580ddd 17
f6e234011390444c303f74d09d87322d 17
e35df3e00ca4ef31d42b34bebaa2f86e 16
MORE...

4.4 Check the Status of Firewall Protection in Target Domains

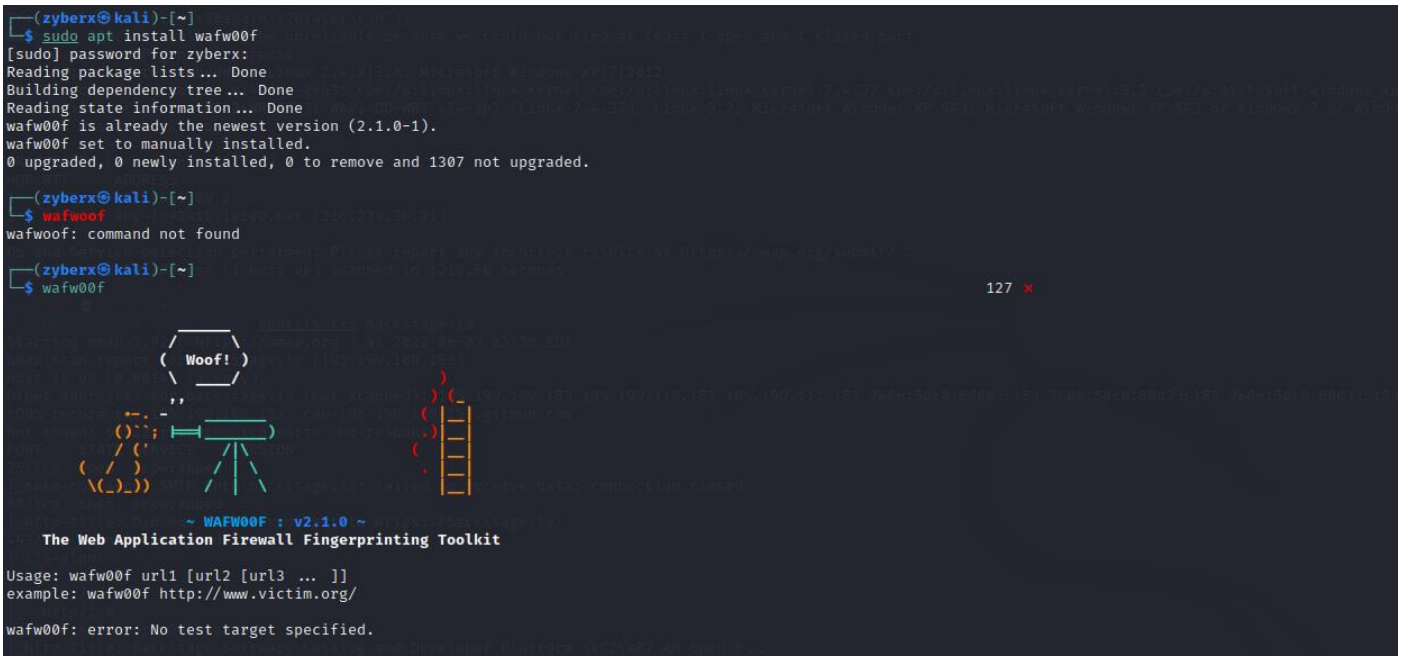
Wafw00f (The Web Application Firewall Fingerprinting Tool.)



Like IPS and IDS, a firewall is a security device that analyzes incoming and outgoing traffic. A firewall can be made of hardware or software. The firewall is a security mechanism that monitors and filters incoming traffic while also preventing unwanted access to your company's or organization's internal systems. The firewall not only stops unlawful incoming traffic, but it also aids in the prevention of malicious software and files from infecting the system. It can act like an antivirus at times. However, it is not an antivirus. The WAF program defends against all types of attacks, including SQLi and XSS. This is a free and open-source program that can determine whether or not a website has a firewall. Even this tool will give you all the information about which firewall is present on the website. The WAFW00F can filter out requests just like a normal firewall.

Instalation

Sudo apt install wafw00f



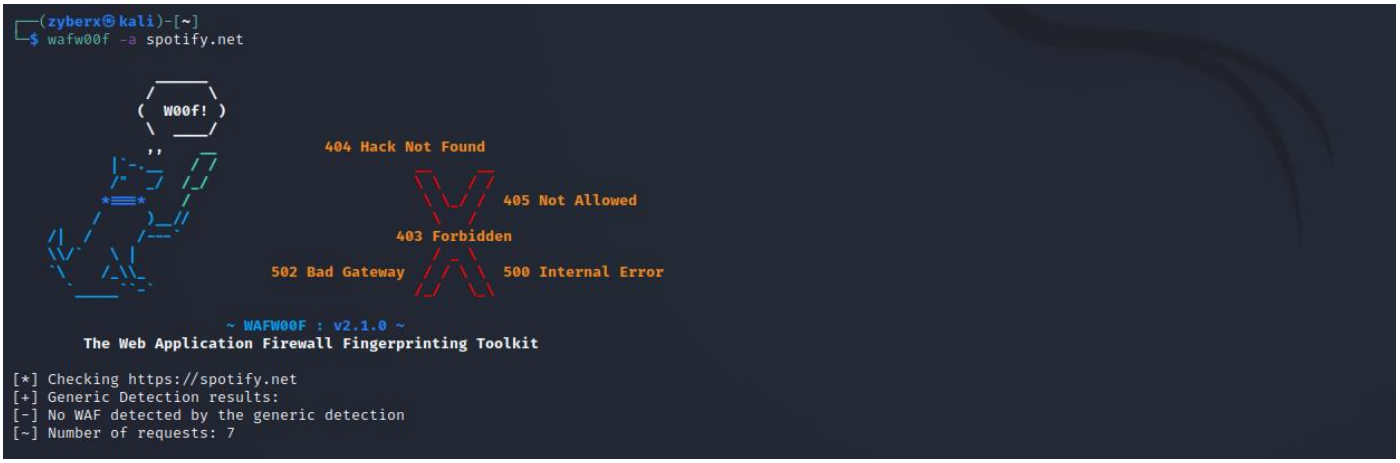
Search results of woow00f

Spotify.com

Assets.spotify.com

Api.spotify.com

Spotify.net



Spotifyforbrands.com

Error occurring when scanning this domain using the tool.

Backstage.io

5. Vulnerability Scanning

Vulnerability scanning is an examination of a computer's or network's potential points of exploit in order to find security weaknesses A vulnerability scan identifies and analyzes system flaws in computers, networks, and communications equipment, as well as predicting how successful countermeasures will be.

Authenticated and unauthenticated scans are the two types of vulnerability scanning. In the unauthenticated technique, the tester scans the network like an intruder would, without having trusted network access. Without logging into the network, such a scan reveals weaknesses that can be exploited. In an authorized scan, the tester enters in as a network user, revealing vulnerabilities that a trusted user, or an intruder who has acquired access as a trusted user, can exploit.

5.1. Nikto

Nikto is a free command-line vulnerability scanner that looks for harmful files/CGIs, obsolete server software, and other issues on webservers. It checks for both general and server-specific issues. Any cookies that are received are likewise captured and printed. The Nikto code is free software in and of itself, but the data files it takes to run it are not. Version 1.00 was released December 27, 2001. [2]

Nikto is a pluggable web server and CGI scanner written in Perl, using rfp's LibWhisker to perform fast security or informational checks. [7]

Features:

- Easily updatable CSV-format checks database
- Output reports in plain text or HTML
- Available HTTP versions automatic switching
- Generic as well as specific server software checks
- SSL support (through libnet-ssleay-perl)
- Proxy support (with authentication)
- Cookies support [7]

To check the in-scope domains I have used following command

nikto –h <domain>

Nikto search results

Spotify.com

```
┌──(zyberx㉿kali)-[~]
└─$ nikto -h spotify.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          35.186.224.25
+ Target Hostname:    spotify.com
+ Target Port:        80
+ Start Time:         2022-06-03 16:34:37 (GMT-4)
---------------------------------------------------------------------------
+ Server: envoy
+ Retrieved via header: 1.1 google
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.spotify.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  15 error(s) and 4 item(s) reported on remote host
+ End Time:           2022-06-03 16:44:48 (GMT-4) (611 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Assets.spotify.com

Api.spotify.com

Spotify.net

Spotifyforbrands.com

```
┌──(zyberx㉿kali)-[~]
└─$ nikto -h spotifyforbrands.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          216.239.38.21
+ Target Hostname:    spotifyforbrands.com
+ Target Port:        80
+ Message:           Multiple IP addresses found: 216.239.38.21, 216.239.34.21, 216.239.36.21, 216.239.32.21
+ Start Time:        2022-06-03 18:05:23 (GMT-4)
---------------------------------------------------------------------------
+ Server: ghs
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  5 error(s) and 2 item(s) reported on remote host
+ End Time:          2022-06-03 18:23:42 (GMT-4) (1099 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Backstage.io

```
┌──(zyberx㉿kali)-[~]
└─$ nikto -h backstage.io
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          185.199.108.153
+ Target Hostname:    backstage.io
+ Target Port:        80
+ Message:           Multiple IP addresses found: 185.199.108.153, 185.199.109.153, 185.199.111.153, 185.199.110.153
+ Start Time:        2022-06-03 17:29:41 (GMT-4)
---------------------------------------------------------------------------
+ Server: GitHub.com
+ Retrieved via header: 1.1 varnish
+ Retrieved x-served-by header: cache-mrs10563-MRS
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-cache' found, with contents: HIT
+ Uncommon header 'x-fastly-request-id' found, with contents: bb818ab447eeb90f8998462ceb8fdbf830ad7a73
+ Uncommon header 'x-github-request-id' found, with contents: 8204:663F:7BFEB5:D33340:629A7D44
+ Uncommon header 'x-timer' found, with contents: S1654291781.496116,VS0,VE0
+ Uncommon header 'x-served-by' found, with contents: cache-mrs10563-MRS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://backstage.io/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'x-origin-cache' found, with contents: HIT
+ Server banner has changed from 'GitHub.com' to 'Varnish' which may suggest a WAF, load balancer or proxy is in place
+ 7785 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:          2022-06-03 18:03:00 (GMT-4) (1999 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

5.2. Netsparker

Netsparker(Invicti) is an automated, yet fully configurable, web application security scanner that enables you to scan websites, web applications, and web services, and identify security flaws. Invicti can scan all types of web applications, regardless of the platform or the language with which they are built. [8]

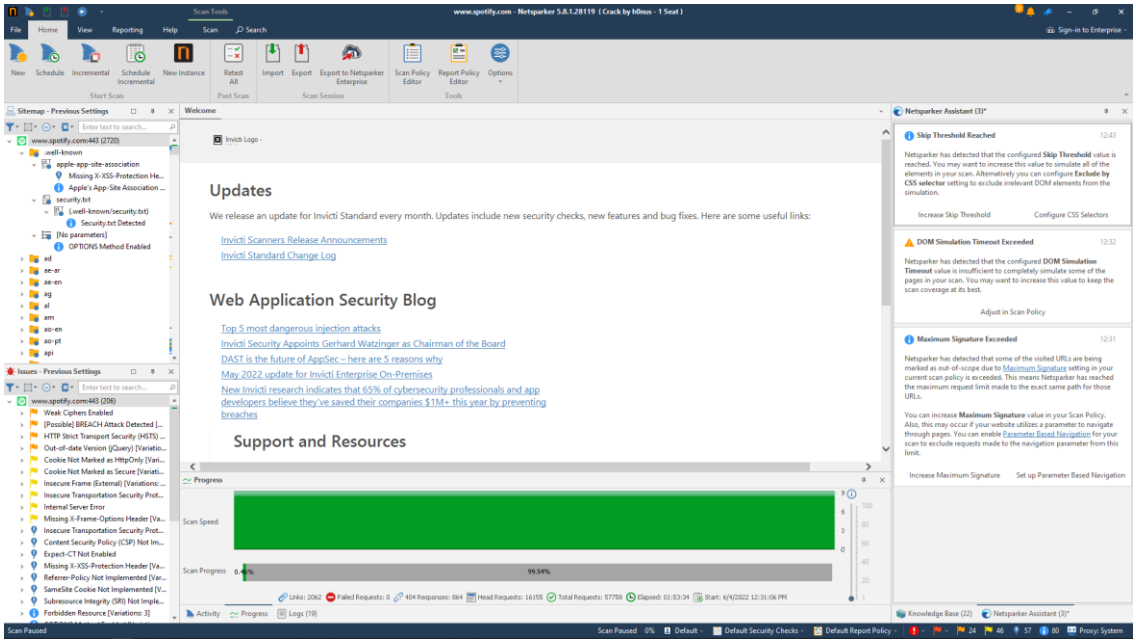
- Invicti is the only online web application security scanner that automatically exploits identified vulnerabilities in a read-only and safe way, in order to confirm identified issues.
- It also presents proof of the vulnerability so that you do not need to waste time manually verifying it. For example, in the case of a detected SQL injection vulnerability, it will show the database name as the proof of exploit.

This scanning technology is designed to help secure web applications easily without any fuss, so can focus on fixing the reported vulnerabilities. If Invicti cannot automatically confirm a vulnerability, it will inform about it by prefixing it with '[Possible]', and assigning a Certainty value, so we can know what should be fixed immediately. [8] For more details visit https://www.invicti.com/support/what-is-invicti/ .

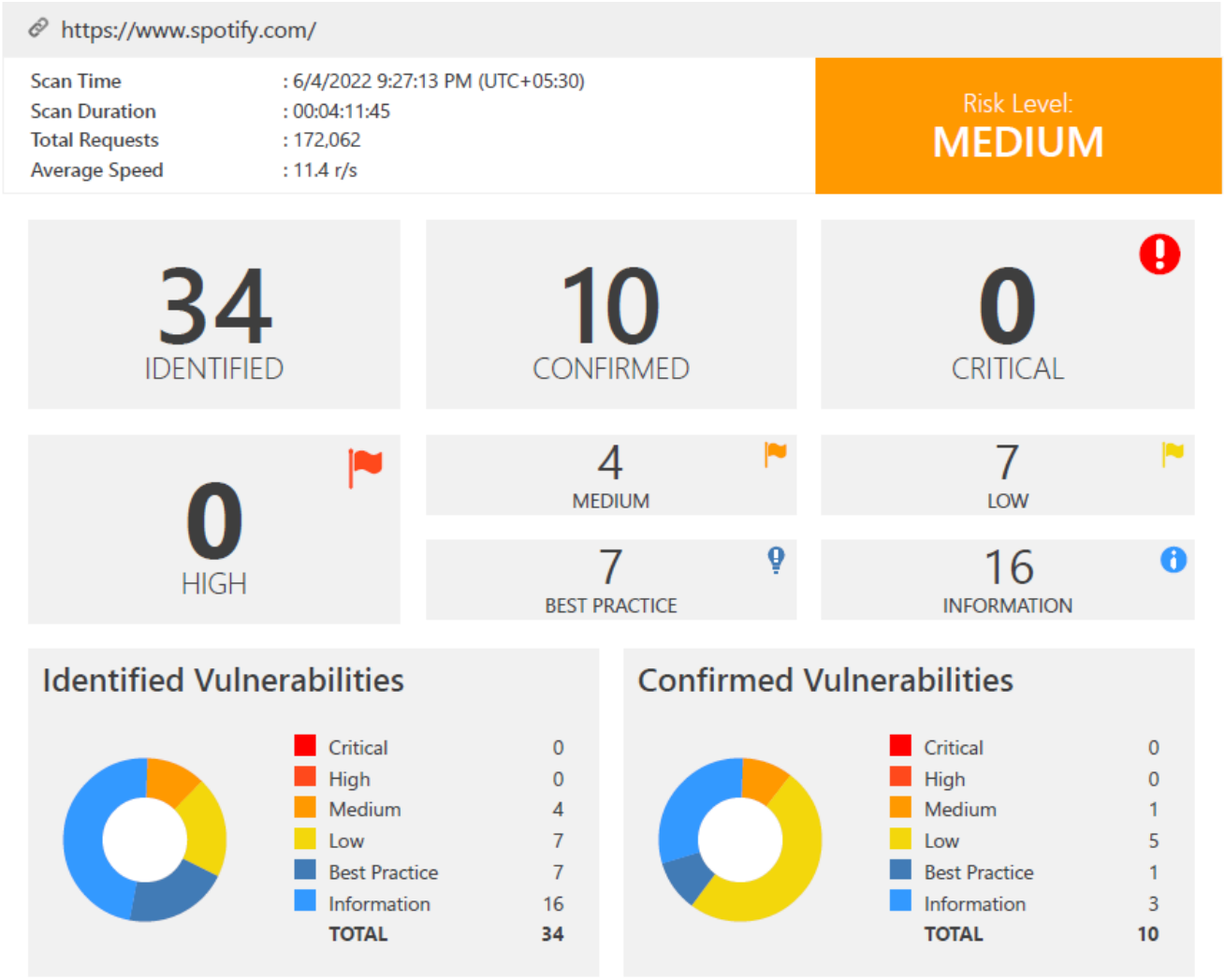
Invicti scanners can generate a proof when they identify the following vulnerability types:

- SQL Injection
- Boolean SQL Injection
- Blind SQL Injection
- Remote File Inclusion (RFI)
- Command Injection
- Blind Command Injection
- XML External Entity (XXE) Injection
- Remote Code Evaluation
- Local File Inclusion (LFI)
- Server-side Template Injection
- Remote Code Execution
- Injecton via Local File Inclusion

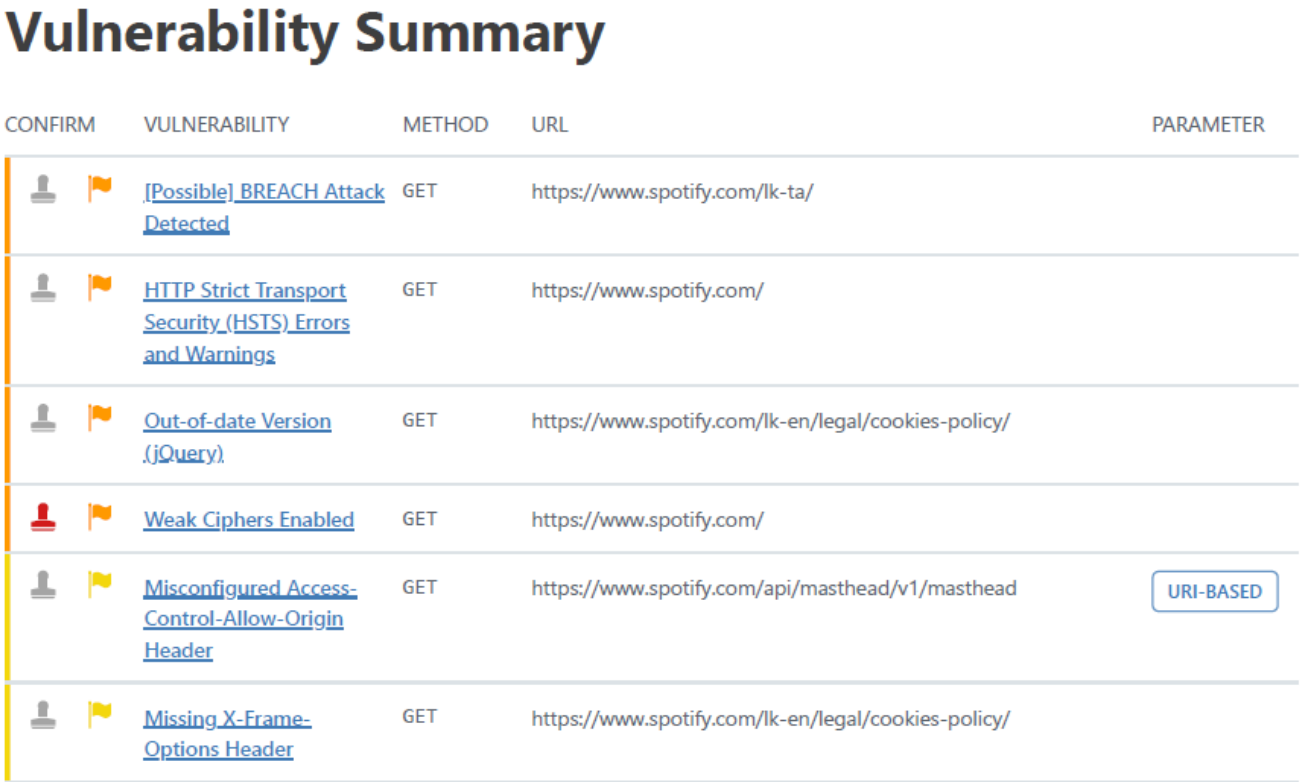
For my Audit I'm using Netsparker professional Edition(V to scan vulnerabilities of Spotify.com.



5.2.1. Spotify.com Netsparker vulnerability scanning



After Scanning the domain, I could find a 4 medium risk vulnerability & total of 34 vulnerabilities regarding the domain



Cookie Not Marked as HttpOnly	GET	https://www.spotify.com/sitemap_website.xml	
Cookie Not Marked as Secure	POST	https://www.spotify.com/api/growth-events/wwwanalyticsagnostic	
Insecure Frame (External)	GET	https://www.spotify.com/lk-en/	
Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://www.spotify.com/	
Internal Server Error	POST	https://www.spotify.com/	
Content Security Policy (CSP) Not Implemented	GET	https://www.spotify.com/lk-en/legal/privacy-policy/#s3	
Expect-CT Not Enabled	GET	https://www.spotify.com/	
Missing X-XSS-Protection Header	GET	https://www.spotify.com/.well-known/apple-app-site-association	
Referrer-Policy Not Implemented	GET	https://www.spotify.com/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	SameSite Cookie Not Implemented	GET	https://www.spotify.com/sitemap_website.xml	
	Subresource Integrity (SRI) Not Implemented	GET	https://www.spotify.com/lk-en/?nsextt=%0D%0Ans%3Anetsparker056650%3Dvuln	nsextt
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://www.spotify.com/	
	[Possible] Internal Path Disclosure (*nix)	GET	https://www.spotify.com/ad/download/linux/	
	[Possible] Internal Path Disclosure (Windows)	GET	https://www.spotify.com/lk-en/spotify/framework/analytics/track/c:/masthead.015794b097663086ccb6.js	
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://www.spotify.com/	
	Apple's App-Site Association (AASA) Detected	GET	https://www.spotify.com/.well-known/apple-app-site-association	

CDN Detected (Google Cloud CDN)	GET	http://www.spotify.com/sitemap.xml	
Email Address Disclosure	GET	https://www.spotify.com/.well-known/security.txt	URI-BASED
Generic Email Address Disclosure	GET	https://www.spotify.com/lk-en/legal/privacy-policy/#s3	
Nonce Usage Detected in Content Security Policy (CSP) Directive	GET	https://www.spotify.com/	
Scheme URI Detected in Content Security Policy (CSP) Directive	GET	https://www.spotify.com/	
Security.txt Detected	GET	https://www.spotify.com/.well-known/security.txt	URI-BASED
Sitemap Detected	GET	https://www.spotify.com/sitemap.xml	
Weak Nonce Detected in Content Security Policy (CSP) Declaration	GET	https://www.spotify.com/	

3 / 117

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://www.spotify.com/	
	Forbidden Resource	GET	https://www.spotify.com/.well-known/.htaccess	URI-BASED

1. [Possible] BREACH Attack Detected

MEDIUM 1

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website. Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

Impact

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests
- Measure the size of encrypted traffic

Vulnerabilities

1.1. https://www.spotify.com/lk-ta/

Method	Parameter	Value
GET	param1	lk-ta

Reflected Parameter(s)

- param1

Sensitive Keyword(s)

- nonce

Certainty

Request

```
GET /lk-ta/ HTTP/1.1
Host: www.spotify.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: sp_m=lk-en; sp_landing=https%3A%2F%2Fwww.spotify.com%2Flk-en%2F; sp_new=1; sp_t=3609ab3a-0dc5-4
a65-b6c5-39fdaa4028c1; sp_ab=%7B%222019_04_premium_menu%22%3A%22control%22%7D; spot=%7B%22t%22%3A165435
8242%2C%22m%22%3A%22lk-en%22%2C%22p%22%3Anull%7D; multiLanguage=1; ki_r=; ki_t=1654358249876%3B16543582
49876%3B1654358253375%3B1%3B2; sp_usid=181d8f51-335e-4ddf-b721-36c3b3a08391; spsess=YpqUqFdXzGPN6FdfGtp
W480lijHhQctCUtQEZOGt0fVS9fY5
Referer: https://www.spotify.com/lk-en/
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) : 795.8682 Total Bytes Received : 106032 Body Length : 104870 Is Compressed : No

```
HTTP/1.1 200 OK
cache-control: private, no-cache, no-store, max-age=0, must-revalidate
set-cookie: sp_m=lk-ta; Path=/; Domain=.spotify.com; Max-Age=115516800; Expires=Sat, 31 Jan 2026 15:57:
35 GMT; Secure; HttpOnly; SameSite=Lax
set-cookie: spot=%7B%22t%22%3A1654358242%2C%22m%22%3A%22lk-ta%22%2C%22p%22%3Anull%7D; Path=/; Domain=.s
potify.com; Max-Age=115516800; Expires=Sat, 31 Jan 2026 15:57:35 GMT; SameSite=Lax
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
x-join-the-band: https://www.spotify.com/jobs/
x-powered-by: Next.js
server: envoy
x-content-type-options: nosniff
x-frame-options: deny
vary: Accept-Encoding,Accept-Encoding
sp-trace-id: 7926cb35157b7f5c
Via: HTTP/2 edgeproxy, 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
content-type: text/html; charset=utf-8
content-security-policy: base-uri 'none'; connect-src https: wss:; form-action https:; frame-ancestors
 'self' https://*.spotify.com https://*.spotify.net; object-src 'none'; script-src 'nonce-83df5153f8ce4
7798652a17246fa6a4d' 'strict-dynamic' 'unsafe-inline' https:
date: Sat, 04 Jun 2022 15:57:36 GMT
content-encoding:
```

Remedy

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

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

To mitigate the issue, we recommend the following solutions:

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

2. HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM 1

Netsparker detected errors during parsing of Strict-Transport-Security header.

Impact

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

Vulnerabilities

2.1. https://www.spotify.com/

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

Certainty

Request

```
GET / HTTP/1.1
Host: www.spotify.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) : 467.4591 Total Bytes Received : 75070 Body Length : 73667 Is Compressed : No

```
HTTP/1.1 200 OK
cache-control: private, no-cache, no-store, max-age=0, must-revalidate
set-cookie: sp_m=lk-en; Path=/; Domain=.spotify.com; Max-Age=115516800; Expires=Sat, 31 Jan 2026 15:57:
22 GMT; Secure; HttpOnly; SameSite=Lax
set-cookie: sp_t=2be84c99-5a0b-4778-81bd-8fd978d0c35e; Path=/; Domain=.spotify.com; Max-Age=31536000; E
xpires=Sun, 04 Jun 2023 15:57:22 GMT; Secure
set-cookie: sp_new=1; Path=/; Domain=.spotify.com; Max-Age=86400; Expires=Sun, 05 Jun 2022 15:57:22 GM
T; Secure
set-cookie: sp_landing=https%3A%2F%2Fwww.spotify.com%2Flk-en%2F; Path=/; Domain=.spotify.com; Max-Age=8
6400; Expires=Sun, 05 Jun 2022 15:57:22 GMT; Secure; HttpOnly
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
x-join-the-band: https://www.spotify.com/jobs/
x-powered-by: Next.js
server: envoy
x-content-type-options: nosniff
x-frame-options: deny
vary: Accept-Encoding,Accept-Encoding
sp-trace-id: f64c51dd23292194
Via: HTTP/2 edgeproxy, 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
content-type: text/html; charset=utf-8
content-security-policy: base-uri 'none'; connect-src https: wss:; form-action https:; frame-ancestors
 'self' https://*.spotify.com https://*.spotify.net; object-src 'none'; script-src 'nonce-db2ef240df7d4
2338cac6e59aad192a3' 'strict-dynamic' 'unsafe-inline' https:
date: Sat, 04 Jun 2022 15:57:22 GMT
content-encoding:

<!DOCTYPE html><html lang="en" dir="ltr"><head nonce="db2ef240df7d42338cac6e59aad192a3"><link rel="prel
oad" href="https://open.scdn.co/fonts/CircularSpUIv3T-Book.woff2" as="font" type="font/woff2" crossorig
in="true"/><link rel="preload" href="https://open.scdn.co/fonts/CircularSpUIv3T-Black.woff2" as="font"
 type="font/woff2" crossorigin="true"/><link rel="preload" href="https://open.scdn.co/fonts/CircularSpU
Iv3T-Bold.woff2" as="font" type="font/woff2" crossorigin="true"/><title>Listening is everything - Spoti
fy</title><meta charSet="utf-8"/><meta name="viewport" content="width=device-width,
…
```

Remedy

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

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
  - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
- The max-age must be at least 31536000 seconds (1 year)
- The includeSubDomains directive must be specified
- The preload directive must be specified
- If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

3. Out-of-date Version (jQuery)

MEDIUM 1

Netsparker identified the target web site is using jQuery and detected that it is out of date.

Impact

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

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the
dataType option, causing text/javascript responses to be executed.

Affected Versions
1.8.0 to 2.2.4

External References
- CVE-2015-9251

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

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions
1.9.0 to 3.4.1

External References
- CVE-2020-11023

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

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions
1.9.0 to 3.4.1

External References
- CVE-2020-11022

JQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Affected Versions
1.0 to 3.3.1

3.1. https://www.spotify.com/lk-en/legal/cookies-policy/

Identified Version

- 2.1.3

Latest Version

- 2.2.4 (in this branch)

Vulnerability Database

- Result is based on 06/03/2022 20:30:00 vulnerability database content.

Certainty

Request

```
GET /lk-en/legal/cookies-policy/ HTTP/1.1
Host: www.spotify.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: sp_m=lk-en; sp_landing=https%3A%2F%2Fwww.spotify.com%2Flk-en%2F; sp_new=1; sp_t=3609ab3a-0dc5-4
a65-b6c5-39fdaa4028c1; sp_ab=%7B%222019_04_premium_menu%22%3A%22control%22%7D; spot=%7B%22t%22%3A165435
8242%2C%22m%22%3A%22lk-en%22%2C%22p%22%3Anull%7D; multiLanguage=1; ki_r=; ki_t=1654358249876%3B16543582
49876%3B1654358253375%3B1%3B2; sp_usid=181d8f51-335e-4ddf-b721-36c3b3a08391; spsess=YpqUqFdXzGPN6FdfGtp
W480lijHhQctCUtQEZOGt0fVS9fY5
Referer: https://www.spotify.com/lk-en/
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) : 652.7314 Total Bytes Received : 51007 Body Length : 50107 Is Compressed : No

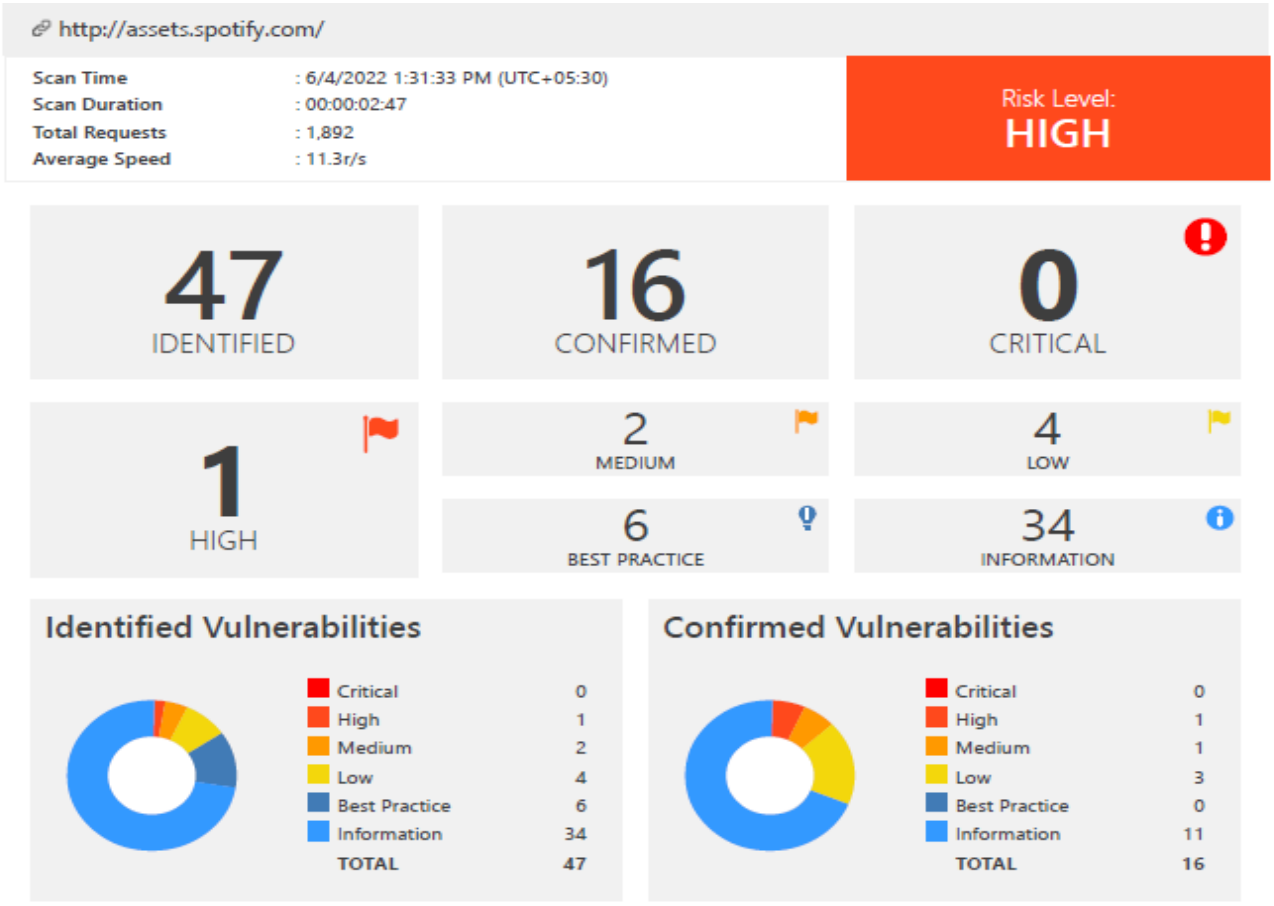
```
HTTP/1.1 200 OK
set-cookie: spsess=YpqUqFdXzGPN6FdfGtpW480lijHhQctCUtQEZOGt0fVS9fY5; path=/; secure; HttpOnly
set-cookie: sp_usid=181d8f51-335e-4ddf-b721-36c3b3a08391; expires=Sat, 04-Jun-2022 16:27:34 GMT; Max-Ag
e=1800; path=/; domain=.spotify.com; secure
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
server: envoy
x-content-type-options: nosniff
vary: Accept-Encoding
x-join-the-band: https://www.spotify.com/jobs/
sp-trace-id: d77765938b7e0a70
content-security-policy: base-uri 'none'; connect-src https: wss:; form-action https:; frame-ancestors
 'self' https://*.spotify.com https://*.spotify.net; object-src 'none'
Via: HTTP/2 edgeproxy, 1.1 google
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
content-type: text/html; charset=UTF-8
content-encoding:
date: Sat, 04 Jun 2022 15:57:34 GMT
cache-control: max-age
```

```
n" dir="ltr" xmlns:og="http://ogp.me/ns#" xmlns:fb="https://www.facebook.com/2008/fbml" class="">
  <head>

          <script nonce="5ded0b99e3774b21a7eacab6ee196fba" src="https://www.scdn.co/webpack/jquery-2.1.
3.min.259eea033d0896561456.js"></script>

            <script nonce="5ded0b99e3774b21a7eacab6ee196fba">
            var spweb = spweb || {};
spweb.config = {
  environment: {
    staticUrl: 'https://www.scdn.co'
  },
  sso: {
…
```

Remedy

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

5.2.2. Assets.spotify.com Netsparker vulnerability scanning



After Scanning the domain, I could find a 1 Highly risk vulnerability & total of 47 vulnerabilities regarding the domain.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Session Cookie Not Marked as Secure	GET	https://assets.spotify.com/default/redirectToken/2F34BE56-8D01-49E8-9C9FD3532962B6D7	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://assets.spotify.com/	
	Weak Ciphers Enabled	GET	https://assets.spotify.com/	
	Missing X-Frame-Options Header	GET	https://assets.spotify.com/.well-known/	
	Cookie Not Marked as HttpOnly	GET	https://assets.spotify.com/	
	Cookie Not Marked as HttpOnly	GET	https://assets.spotify.com/default/redirectToken/2F34BE56-8D01-49E8-9C9FD3532962B6D7	

Content Security Policy (CSP) Not Implemented	GET	https://assets.spotify.com/.well-known/	
Expect-CT Not Enabled	GET	https://assets.spotify.com/	
Missing X-XSS-Protection Header	GET	https://assets.spotify.com/.well-known/	
Referrer-Policy Not Implemented	GET	https://assets.spotify.com/.well-known/	
SameSite Cookie Not Implemented	GET	https://assets.spotify.com/	
SameSite Cookie Not Implemented	GET	https://assets.spotify.com/default/redirectToken/2F34BE56-8D01-49E8-9C9FD3532962B6D7	
Email Address Disclosure	GET	https://assets.spotify.com/login/	
Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/	
Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/097E76EF-FBE1-4FBA-A9952FF420679C76/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/0F5F40EE-24DF-4F2D-A90AAE295E3035CB/	
	Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/2928ECF5-4674-40E4-AE9DD8EDBCF23D8C/	
	Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/305F58DD-3109-412A-9EEEF6BA45C424A2/	
	Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/33917C29-95ED-4EFC-9BF99457C6DED36E/	
	Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/7A4608B4-E433-460B-BD8B97E72C442C6E/	
	Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/B5B87C21-4194-4FEC-9CCB2744F14C66BA/	
	Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/C518DB54-E616-44A5-A35E810E21188CC5/	
	Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/CCD6DEA3-09FD-4908-9961F5C1A15BBBDB/	
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/	
	Generic Email Address	GET	https://assets.spotify.com/login/redirectToken/	

Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/097E76EF-FBE1-4FBA-A9952FF420679C76/	
Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/0F5F40EE-24DF-4F2D-A90AAE295E3035CB/	
Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/2928ECF5-4674-40E4-AE9DD8EDBCF23D8C/	
Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/305F58DD-3109-412A-9EEEF6BA45C424A2/	
Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/33917C29-95ED-4EFC-9BF99457C6DED36E/	
Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/7A4608B4-E433-460B-BD8B97E72C442C6E/	

3 / 116

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/B5B87C21-4194-4FEC-9CCB2744F14C66BA/	
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/C518DB54-E616-44A5-A35E810E21188CC5/	
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/CCD6DEA3-09FD-4908-9961F5C1A15BBBDB/	
	Nginx Web Server Identified	GET	https://assets.spotify.com/	
	Forbidden Resource	GET	https://assets.spotify.com/.well-known/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0001BD)%3C/scRipt%3E	nsextt
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/097E76EF-FBE1-4FBA-A9952FF420679C76/	
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/0F5F40EE-24DF-4F2D-A90AAE295E3035CB/	
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/2928ECF5-4674-40E4-AE9DD8EDBCF23D8C/	
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/305F58DD-3109-412A-9EEEF6BA45C424A2/	
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/33917C29-95ED-4EFC-9BF99457C6DED36E/	
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/7A4608B4-E433-460B-BD8B97E72C442C6E/	

3 / 116

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/B5B87C21-4194-4FEC-9CCB2744F14C66BA/	
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/C518DB54-E616-44A5-A35E810E21188CC5/	
	Generic Email Address Disclosure	GET	https://assets.spotify.com/login/redirectToken/CCD6DEA3-09FD-4908-9961F5C1A15BBBDB/	
	Nginx Web Server Identified	GET	https://assets.spotify.com/	
	Forbidden Resource	GET	https://assets.spotify.com/.well-known/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0001BD)%3C/scRipt%3E	nsextt
	Forbidden Resource	GET	https://assets.spotify.com/.well-known/c%3a%5cboot.ini	
	Forbidden Resource	GET	https://assets.spotify.com/.well-known/c:/boot.ini	
	Forbidden Resource	GET	https://assets.spotify.com/.well-known/c:/windows/win.ini	
	Forbidden Resource	GET	https://assets.spotify.com/.well-known/etc/passwd	
	Forbidden Resource	GET	https://assets.spotify.com/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000187)%3C/scRipt%3E	nsextt
	Forbidden Resource	GET	https://assets.spotify.com/c%3a%5cboot.ini	
	Forbidden Resource	GET	https://assets.spotify.com/c:/boot.ini	
	Forbidden Resource	GET	https://assets.spotify.com/c:/windows/win.ini	
	Forbidden Resource	GET	https://assets.spotify.com/etc/passwd	
	Forbidden Resource	GET	https://assets.spotify.com/etc/passwd	

1. Session Cookie Not Marked as Secure

HIGH 1 CONFIRMED 1

Netsparker identified a session cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept the traffic, following a successful manin-

the-middle attack.

It is important to note that Netsparker inferred from the its name that the cookie in question is session related.

Impact

This cookie will be transmitted over a HTTP connection; therefore, 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 your website in order to steal the cookie

Vulnerabilities

1.1. https://assets.spotify.com/default/redirectToken/2F34BE56-8D01-49E8-9C9FD3532962B6D7

CONFIRMED

Identified Cookie(s)

- JSESSIONID

Cookie Source

- HTTP Header

Request

```
GET /default/redirectToken/2F34BE56-8D01-49E8-9C9FD3532962B6D7 HTTP/1.1
Host: assets.spotify.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: DEFAULTLOCALE=en_US; bynder=96A94F2D-EE6F-464A-A72F13F4E5B0A4D8; JSESSIONID=YCU9V4jhZkf50BmYNpq
sCNIO_a2mTqNNyNNzrj9-
Referer: http://assets.spotify.com/sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 546.9143 Total Bytes Received : 685 Body Length : 0 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: JSESSIONID=NNkyewvQlsIso7LrqGefv4AItdsI7dWdY8O53mWH; path=/

Via: 1.1 17d56a41c5d306f635a528df1fa752b8.cloudfront.net (CloudFront)
Server: nginx
Referrer-Policy: strict-origin-when-cross-origin
Connection: keep-alive
X-Amz-Cf-Pop: SIN52-C2
X-XSS-Protection: 1; mode=block
X-Amz-Cf-Id: siQnrpnsqpdeiOvTcMSdyXeVmNYeH_C-8ChLLGK3KexzIG9yC2haKg==
Content-Length: 0
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000
Content-Type: text/html;charset=UTF-8
X-Content-Type-Options: nosniff
Location: /login/redirectToken/2F34BE56-8D01-49E8-9C9FD3532962B6D7/
Date: Sat, 04 Jun 2022 08:03:55 GMT
X-Cache: Miss from cloudfront
```

Actions to Take

1. Mark all cookies used within the application as secure.

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.)*

2. HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM | 1

Netsparker detected errors during parsing of Strict-Transport-Security header.

Impact

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

Vulnerability

2.1. https://assets.spotify.com/

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

Certainty

Request

```
GET / HTTP/1.1
Host: login.getbynder.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) : 897.7757 Total Bytes Received : 61545 Body Length : 61002 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: bynder=A1A9BC5F-3EAE-4C34-83B901047C9C5B85;Path=/;Secure;HTTPOnly
Set-Cookie: DEFAULTLOCALE=en_US;Path=/
Server: nginx
Referrer-Policy: strict-origin-when-cross-origin
Connection: keep-alive
X-XSS-Protection: 1; mode=block
Content-Encoding:
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000
X-Content-Type-Options: nosniff
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 04 Jun 2022 08:01:48 GMT
Cache-Control: no-cache, no-store, must-revalidate
```

Remedy

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

Browser vendors declared:

Serve a valid certificate

- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
  - ❖ In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
  - ❖ The max-agemust be at least 31536000 seconds (1 year)
  - ❖ The includeSubDomainsdirective must be specified
  - ❖ The preloaddirective must be specified
  - ❖ If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the
  - ❖ page it redirects to)

3. HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM 1 CONFIRMED 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

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

3.1. https://assets.spotify.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)

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.

I. Click Start, click Run, type regedt32or type regedit, and then click OK.
II. In Registry Editor, locate the following registry key: HKLM\SYSTEM\Curre ntControlSet\Control\SecurityProviders
III. Set "Enabled" DWORD to "0x0" for the following registry keys:

SCHANNEL\Ciphers\DES 56/56

SCHANNEL\Ciphers\RC4 64/12 8

SCHANNEL\Ciphers\RC4 40/128

SCHANNEL\Ciphers\RC2 56/128

SCHANNEL\Ciphers\RC2 40/128

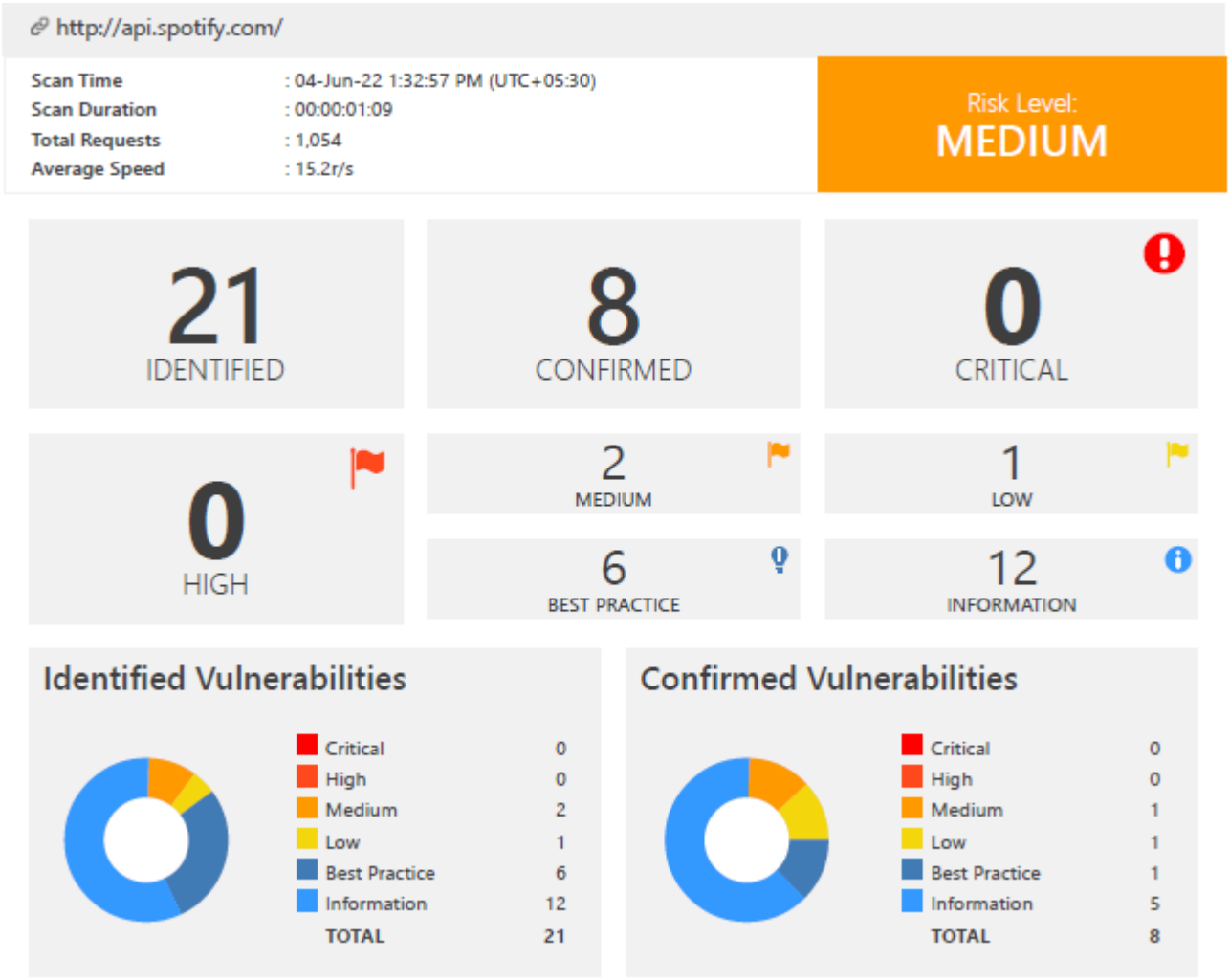
SCHANNEL\Ciphers\NULL

SCHANNEL\Hashes\MD5

Remedy

Configure your web server to disallow using weak ciphers.

5.2.3. Api.spotify.com Netsparker vulnerability scanning



After Scanning the domain, I could find 2 medium risk vulnerability & total of 21 vulnerabilities regarding the domain.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://api.spotify.com/	
	Weak Ciphers Enabled	GET	https://api.spotify.com/	
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://api.spotify.com/	
	Expect-CT Not Enabled	GET	https://api.spotify.com/	
	Missing X-XSS-Protection Header	GET	https://api.spotify.com/.well-known/	
	Missing X-XSS-Protection Header	GET	https://api.spotify.com/.well-known/apple-app-site-association	

	Missing X-XSS-Protection Header	GET	https://api.spotify.com/opensearch.xml	
	Missing X-XSS-Protection Header	GET	https://api.spotify.com/sitemap.xml	
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://api.spotify.com/	
	Authorization Required	GET	https://api.spotify.com/.well-known/	
	Authorization Required	GET	https://api.spotify.com/.well-known/apple-app-site-association	
	Authorization Required	GET	https://api.spotify.com/.well-known/c%3a%5cboot.ini	
	Authorization Required	GET	https://api.spotify.com/.well-known/c:/windows/win.ini	
	Authorization Required	GET	https://api.spotify.com/etc/passwd	
	Authorization Required	GET	https://api.spotify.com/opensearch.xml	
	CDN Detected (Google Cloud CDN)	GET	http://api.spotify.com/	
	Authorization Required	GET	https://api.spotify.com/.svn/wc.db	

2 / 47

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Authorization Required	GET	https://api.spotify.com/.well-known/c:/boot.ini	
	Authorization Required	GET	https://api.spotify.com/c:/boot.ini	
	Authorization Required	GET	https://api.spotify.com/c:/windows/win.ini	
	Authorization Required	GET	https://api.spotify.com/sitemap.xml	

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

MEDIUM | 1

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

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

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

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

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

Vulnerabilities

1.1. https://api.spotify.com/

Certainty

Request

```
GET / HTTP/1.1
Host: developer.spotify.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) : 349.8974 Total Bytes Received : 105677 Body Length : 105157 Is Compressed : No

```
HTTP/1.1 200 OK
x-amz-meta-goog-reserved-file-mtime: 1649809182
X-Cache: MISS, HIT, HIT
X-Served-By: cache-ord1727-ORD, cache-chi-kigq8000133-CHI, cache-mrs10541-MRS
Connection: keep-alive
Access-Control-Allow-Origin: *
Content-Length: 23149
Last-Modified: Wed, 13 Apr 2022 00:20:12 GMT
Accept-Ranges: bytes
X-Cache-Hits: 0, 2, 16222
Content-Type: text/html
Content-Encoding:
Age: 43262
Date: Sat, 04 Jun 2022 08:03:06 GMT
ETag: "f4eef12726a5e1b57c13daa94d44e23f"
Cache-Control: public, max-age=86400
```

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

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

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
       ServerAlias *
       RewriteEngine On
       RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

2. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

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://api.spotify.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

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 regedt32or 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 64/12 8

SCHANNEL\Ciphers\RC4 40/128

SCHANNEL\Ciphers\RC2 56/128

SCHANNEL\Ciphers\RC2 40/128

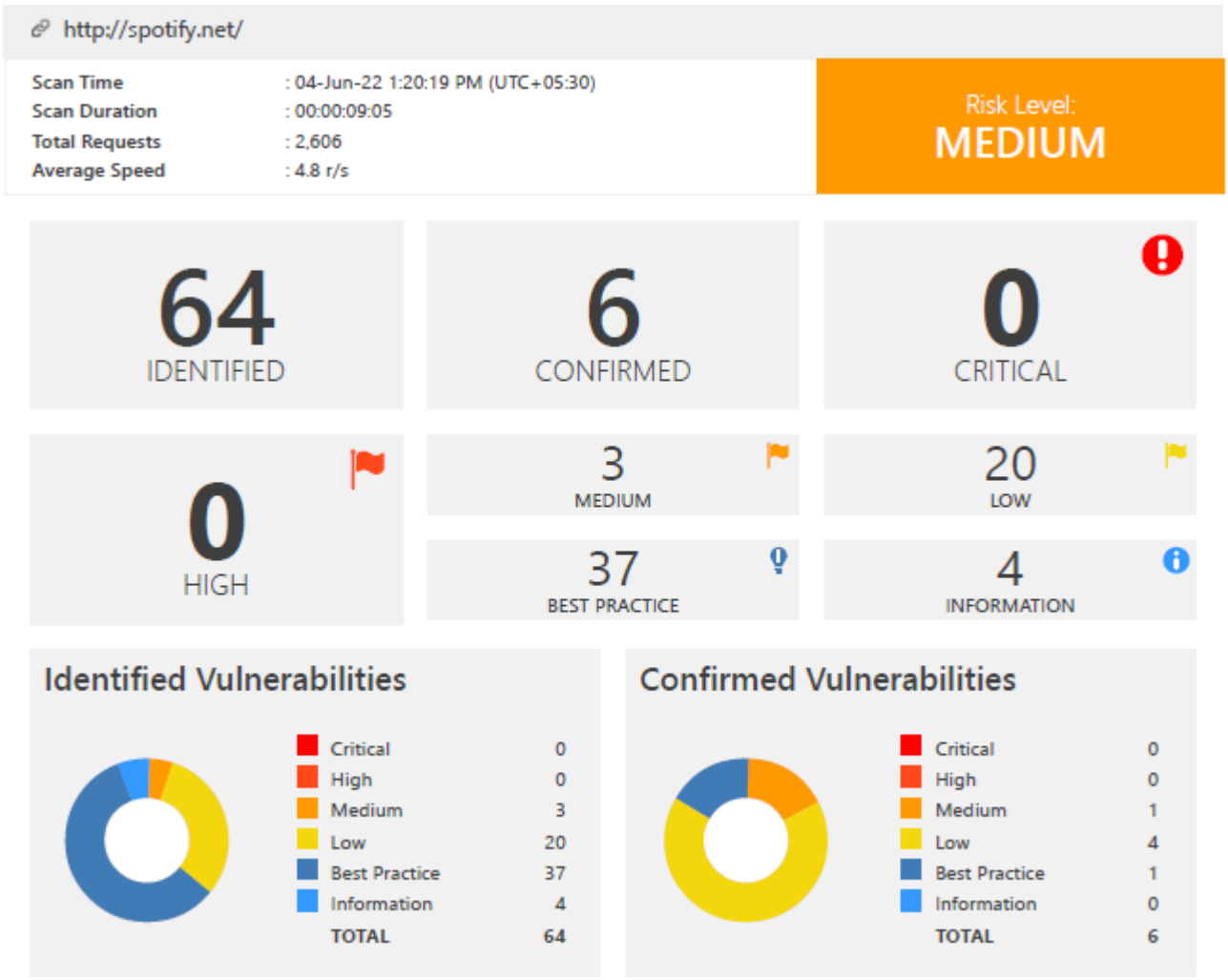
SCHANNEL\Ciphers\NULL

SCHANNEL\Hashes\MD5

Remedy

Configure your web server to disallow using weak ciphers

5.2.4. Spotify.net Netsparker vulnerability scanning



After Scanning the domain, I could find 3 medium risk vulnerability & total of 64 vulnerabilities regarding the domain.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] BREACH Attack Detected	GET	https://spotify.net/mellon/login?IdP=http%3A%2F%2Fwww.okta.com%2Fexk6vfwgijPqP7VZg1t7&ReturnTo=%2527	ReturnTo
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://spotify.net/	
	Weak Ciphers Enabled	GET	https://spotify.net/	
	Internal Server Error	POST	http://spotify.net/.well-known/apple-app-site-association	
	Internal Server Error	POST	http://spotify.net/opensearch.xml	
	Internal Server Error	POST	http://spotify.net/sitemap.xml	
	Internal Server Error	GET	https://spotify.net/mellon/login?IdP=%2fmellon%2flogin&ReturnTo=https%3A%2F%2Fspotify.net%2F	IdP

Internal Server Error	GET	https://spotify.net/mellon/login?IdP=login&ReturnTo=https%3A%2F%2Fspotify.net%2F	IdP
Missing X-Frame-Options Header	GET	http://spotify.net/	
Missing X-Frame-Options Header	GET	http://spotify.net/.well-known/	
Missing X-Frame-Options Header	GET	http://spotify.net/.well-known/apple-app-site-association	
Missing X-Frame-Options Header	HEAD	http://spotify.net/opensearch	
Missing X-Frame-Options Header	GET	http://spotify.net/open-search.gz	
Missing X-Frame-Options Header	GET	http://spotify.net/opensearch.xml	
Missing X-Frame-Options Header	GET	http://spotify.net/sitemap.xml	
Missing X-Frame-Options Header	GET	http://spotify.net/sitemap.xml.gz	

2 / 120

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Missing X-Frame-Options Header	GET	https://spotify.net/mellon/	
	Missing X-Frame-Options Header	GET	https://spotify.net/mellon/c:/boot.ini	URI-BASED
	Missing X-Frame-Options Header	GET	https://spotify.net/mellon/login?IdP=http%3A%2F%2Fwww.okta.com%2Fexk6vfwgijPqP7VZg1t7&ReturnTo=https%3A%2F%2Fspotify.net%2F	
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://spotify.net/	
	Internal Server Error	POST	http://spotify.net/	
	Internal Server Error	POST	http://spotify.net/.well-known/	

Internal Server Error	GET	https://spotify.net/mellon/login?IdP=%2527&ReturnTo=https%3A%2F%2Fspotify.net%2F	IdP
Content Security Policy (CSP) Not Implemented	GET	http://spotify.net/	
Content Security Policy (CSP) Not Implemented	GET	http://spotify.net/.well-known/	
Content Security Policy (CSP) Not Implemented	GET	http://spotify.net/.well-known/apple-app-site-association	
Content Security Policy (CSP) Not Implemented	GET	http://spotify.net/open-search.gz	
Content Security Policy (CSP) Not Implemented	GET	http://spotify.net/opensearch.xml	
Content Security Policy (CSP) Not Implemented	GET	http://spotify.net/sitemap.xml	
Content Security Policy (CSP) Not Implemented	GET	http://spotify.net/sitemap.xml.gz	
Content Security Policy (CSP) Not Implemented	GET	https://spotify.net/mellon/	
Content Security Policy (CSP) Not Implemented	GET	https://spotify.net/mellon/c%3a%5cboot.ini	URI-BASED
Content Security Policy (CSP) Not Implemented	GET	https://spotify.net/mellon/c:/boot.ini	URI-BASED
Content Security Policy (CSP) Not Implemented	GET	https://spotify.net/mellon/login?IdP=http%3A%2F%2Fwww.okta.com%2Fexk6vfwgijPqP7VZg1t7&ReturnTo=https%3A%2F%2Fspotify.net%2F	
Expect-CT Not Enabled	GET	https://spotify.net/	
Missing X-XSS-Protection Header	GET	http://spotify.net/	
Missing X-XSS-Protection Header	GET	http://spotify.net/.well-known/	
Missing X-XSS-Protection Header	GET	http://spotify.net/.well-known/apple-app-site-association	
Missing X-XSS-Protection Header	HEAD	http://spotify.net/opensearch	
Missing X-XSS-Protection Header	GET	http://spotify.net/open-search.gz	
Missing X-XSS-Protection Header	GET	http://spotify.net/opensearch.xml	
Missing X-XSS-Protection Header	GET	http://spotify.net/sitemap.xml	
Missing X-XSS-Protection Header	GET	http://spotify.net/sitemap.xml.gz	

Missing X-XSS-Protection Header	GET	https://spotify.net/mellon/c:/boot.ini	URI-BASED
Missing X-XSS-Protection Header	GET	https://spotify.net/mellon/login?ldP=http%3A%2F%2Fwww.okta.com%2Fexk6vfwgijPqP7VZg1t7&ReturnTo=https%3A%2F%2Fspotify.net%2F	
Referrer-Policy Not Implemented	GET	http://spotify.net/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Referrer-Policy Not Implemented	GET	http://spotify.net/.well-known/	
	Referrer-Policy Not Implemented	GET	http://spotify.net/.well-known/apple-app-site-association	
	Referrer-Policy Not Implemented	GET	http://spotify.net/open-search.gz	
	Referrer-Policy Not Implemented	GET	http://spotify.net/opensearch.xml	
	Referrer-Policy Not Implemented	GET	http://spotify.net/sitemap.xml	
	Referrer-Policy Not Implemented	GET	http://spotify.net/sitemap.xml.gz	
	Referrer-Policy Not Implemented	GET	https://spotify.net/mellon/	
	Referrer-Policy Not Implemented	GET	https://spotify.net/mellon/c%3a%5cboot.ini	URI-BASED
	Referrer-Policy Not Implemented	GET	https://spotify.net/mellon/c:/boot.ini	URI-BASED
	Referrer-Policy Not Implemented	GET	https://spotify.net/mellon/login?ldP=http%3A%2F%2Fwww.okta.com%2Fexk6vfwgijPqP7VZg1t7&ReturnTo=https%3A%2F%2Fspotify.net%2F	
	SameSite Cookie Not Implemented	GET	http://spotify.net/	
	Subresource Integrity (SRI) Not Implemented	GET	https://spotify.net/mellon/login?ldP=http%3A%2F%2Fwww.okta.com%2Fexk6vfwgijPqP7VZg1t7&ReturnTo=%2527	ReturnTo
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://spotify.net/	
	Apache Web Server Identified	GET	http://spotify.net/	

1. [Possible] BREACH Attack Detected

MEDIUM | 1

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

Impact

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests
- Measure the size of encrypted traffic

Vulnerabilities

1.1. https://spotify.net/mellon/login?IdP=http%3A%2F%2Fwww.okta.com%2Fexk6vfwgijPqP7VZg1t7&ReturnTo=%2527

Method	Parameter	Value
GET	IdP	http%3A%2F%2Fwww.okta.com%2Fexk6vfwgijPqP7VZg1t7
GET	ReturnTo	%27

Reflected Parameter(s)

- ReturnTo

Sensitive Keyword(s)

- token

Certainty

Request

```
GET /mellon/login?IdP=http%3A%2F%2Fwww.okta.com%2Fexk6vfwgijPqP7VZg1t7&ReturnTo=%2527 HTTP/1.1
Host: spotify.okta.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: GCLB=CLXDh8HdlNKzUQ; mellon-spotify.net=cookietest
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) : 1648.1145 Total Bytes Received : 21086 Body Length : 18627 Is Compressed : No

```
HTTP/1.1 200 OK
x-rate-limit-limit: 6000
cache-control: no-cache, no-store
Server: nginx
x-rate-limit-remaining: 5973
X-Robots-Tag: noindex,nofollow
set-cookie: sid=""; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
set-cookie: autolaunch_triggered=""; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
set-cookie: JSESSIONID=42C3F53CB9D622F2CFD63E031D019F99; Path=/; Secure; HttpOnly
set-cookie: t=spring; Path=/
set-cookie: DT=DI0aAzVbk0PRXCeoiol689tIA; Expires=Mon, 03-Jun-2024 07:51:02 GMT; Path=/; Secure
set-cookie: sid=""; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
x-okta-request-id: YpsO5pPyTBbiizg4L7WZswAACZk
Transfer-Encoding: chunked
p3p: CP="HONK"
pragma: no-cache
Public-Key-Pins-Report-Only: pin-sha256="r5EfzZxQVvQpKo3AgYRaT7X2bDO/kj3ACwmxfdT2zt8="; pin-sha256="Maq
lcUgk2mvY/RFSGeSwBRkI+rZ6/dxe/DuQfBT/vnQ="; pin-sha256="72G5IEvDEWn+EThf3qjR7/bQSWaS2ZSLqolhnO6iyJI=";
 pin-sha256="rrV6CLCCvqnk89gWibYT0JO6fNQ8cCit7GGoiVTjCOg="; max-age=60; report-uri="https://okta.report
-uri.com/r/default/hpkp/reportOnly"
x-content-type-options: nosniff
x-xss-protection: 0
expect-ct: report-uri="https://oktaexpectct.report-uri.com/r/t/ct/reportOnly", max-age=0
Connection: keep-alive
expires: 0
x-frame-options: SAMEORIGIN
Vary: Accept-Encoding
x-rate-limit-reset: 1654329106
content-language: en
Strict-Transport-Security: max-age=315360000; includeSubDomains
Content-Type: text/html;charset=utf-8
x-ua-compatible: IE=edge
content-security-policy: default-src 'self' spotify.okta.com *.oktacdn.com; connect-src 'self' spotify.
okta.com spotify-admin.okta.com *.oktacdn.com *.mixpanel.com *.mapbox.com app.pendo.io data.pendo.io pe
ndo-static-5634101834153984.storage.googleapis.com spotify.kerberos.okta.com spotify.mtls.okta.com http
s://oinmanager.okta.com data:; script-src 'unsafe-inline' 'unsafe-eval' 'self' spotify.okta.com *.oktac
dn.com; style-src 'unsafe-inline' 'self' spotify.okta.com *.oktacdn.com app.pendo.io cdn.pendo.io pendo
-static-5634101834153984.storag
```

Remedy

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

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

To mitigate the issue, we recommend the following solutions:

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

2. HTTP Strict Transport Security (HSTS) Errorsand Warnings

MEDIUM 1

Netsparker detected errors during parsing of Strict-Transport-Security header.

Impact

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

Vulnerabilities

2.1. https://spotify.net/

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

Certainty

Request

```
GET / HTTP/1.1
Host: spotify.okta.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) : 977.2993 Total Bytes Received : 21204 Body Length : 18745 Is Compressed : No

```
HTTP/1.1 200 OK
x-rate-limit-limit: 6000
cache-control: no-cache, no-store
Server: nginx
x-rate-limit-remaining: 5933
X-Robots-Tag: noindex,nofollow
set-cookie: sid=""; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
set-cookie: autolaunch_triggered=""; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
set-cookie: JSESSIONID=B20DF183555E780630F786D964E8A3C4; Path=/; Secure; HttpOnly
set-cookie: t=spring; Path=/
set-cookie: DT=DI0a3jkBEL2ThygH91kiu_h1A; Expires=Mon, 03-Jun-2024 07:50:30 GMT; Path=/; Secure
set-cookie: sid=""; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
x-okta-request-id: YpsOxmmmAQ5EiJcUKnxdZwAAB1Y
Transfer-Encoding: chunked
p3p: CP="HONK"
pragma: no-cache
Public-Key-Pins-Report-Only: pin-sha256="r5EfzZxQVvQpKo3AgYRaT7X2bDO/kj3ACwmxfdT2zt8="; pin-sha256="Maq
lcUgk2mvY/RFSGeSwBRkI+rZ6/dxe/DuQfBT/vnQ="; pin-sha256="72G5IEvDEWn+EThf3qjR7/bQSWaS2ZSLqolhnO6iyJI=";
 pin-sha256="rrV6CLCCvqnk89gWibYT0JO6fNQ8cCit7GGoiVTjCOg="; max-age=60; report-uri="https://okta.report
-uri.com/r/default/hpkp/reportOnly"
x-content-type-options: nosniff
x-xss-protection: 0
expect-ct: report-uri="https://oktaexpectct.report-uri.com/r/t/ct/reportOnly", max-age=0
Connection: keep-alive
expires: 0
x-frame-options: SAMEORIGIN
Vary: Accept-Encoding
x-rate-limit-reset: 1654329046
content-language: en
Strict-Transport-Security: max-age=315360000; includeSubDomains
Content-Type: text/html;charset=utf-8
x-ua-compatible: IE=edge
content-security-policy: default-src 'self' spotify.okta.com *.oktacdn.com; connect-src 'self' spotify.
okta.com spotify-admin.okta.com *.oktacdn.com *.mixpanel.com *.mapbox.com app.pendo.io data.pendo.io pe
ndo-static-5634101834153984.storage.googleapis.com spotify.kerberos.okta.com spotify.mtls.okta.com http
s://oinmanager.okta.com data:; script-src 'unsafe-inline' 'unsafe-eval' 'self' spotify.okta.com *.oktac
dn.com; style-src 'unsafe-inline' 'self' spotify.okta.com *.oktacdn.com app.pendo.io cdn.pendo.io pendo
-static-5634101834153984.storag
…
```

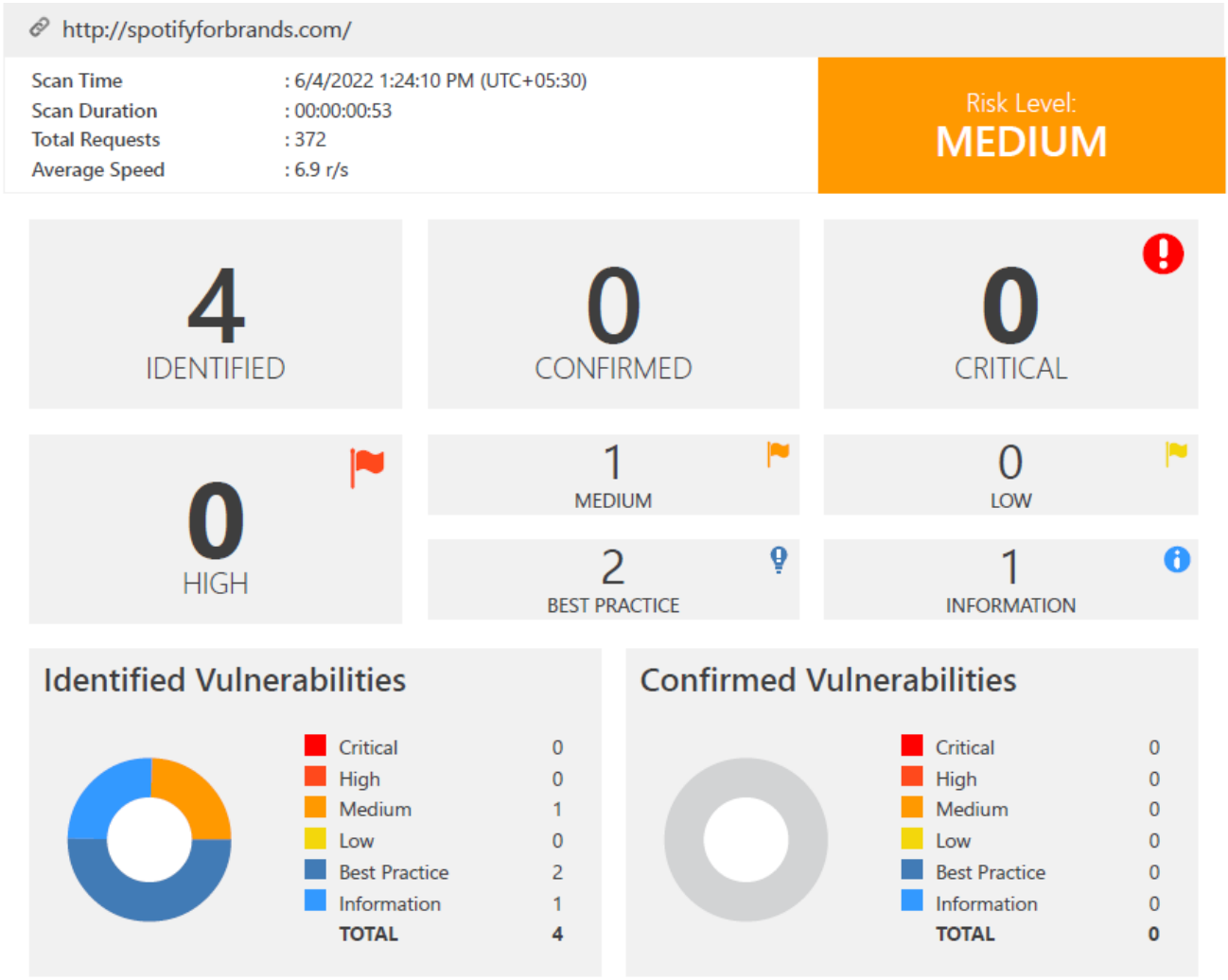
Remedy

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

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
    - ❖ In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
    - ❖ The max-age must be at least 31536000 seconds (1 year)
    - ❖ The includeSubDomains directive must be specified
    - ❖ The preload directive must be specified
    - ❖ If you are serving an additional redirect from your HTTPS site, that redirect must have HSTS header (rather than the page it redirects to)

5.2.5. Spotifyforbrands.com Netsparker vulnerability scanning



After Scanning the domain, I could find 1 medium risk vulnerability & total of 4 vulnerabilities regarding the domain.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	SSL/TLS Not Implemented	GET	https://spotifyforbrands.com/	
	Content Security Policy (CSP) Not Implemented	GET	http://spotifyforbrands.com/	
	Referrer-Policy Not Implemented	GET	http://spotifyforbrands.com/	
	Disabled X-XSS-Protection Header	GET	http://spotifyforbrands.com/	

Identified Vulnerabilities of Spotifyforbrands.com

1. SSL/TLS Not Implemented

MEDIUM | 1

Netsparker detected that SSL/TLS is not implemented.

Impact

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

Vulnerabilities

1.1. https://spotifyforbrands.com/

Certainty

Request

```
[NETSPARKER] SSL Connection
```

Response

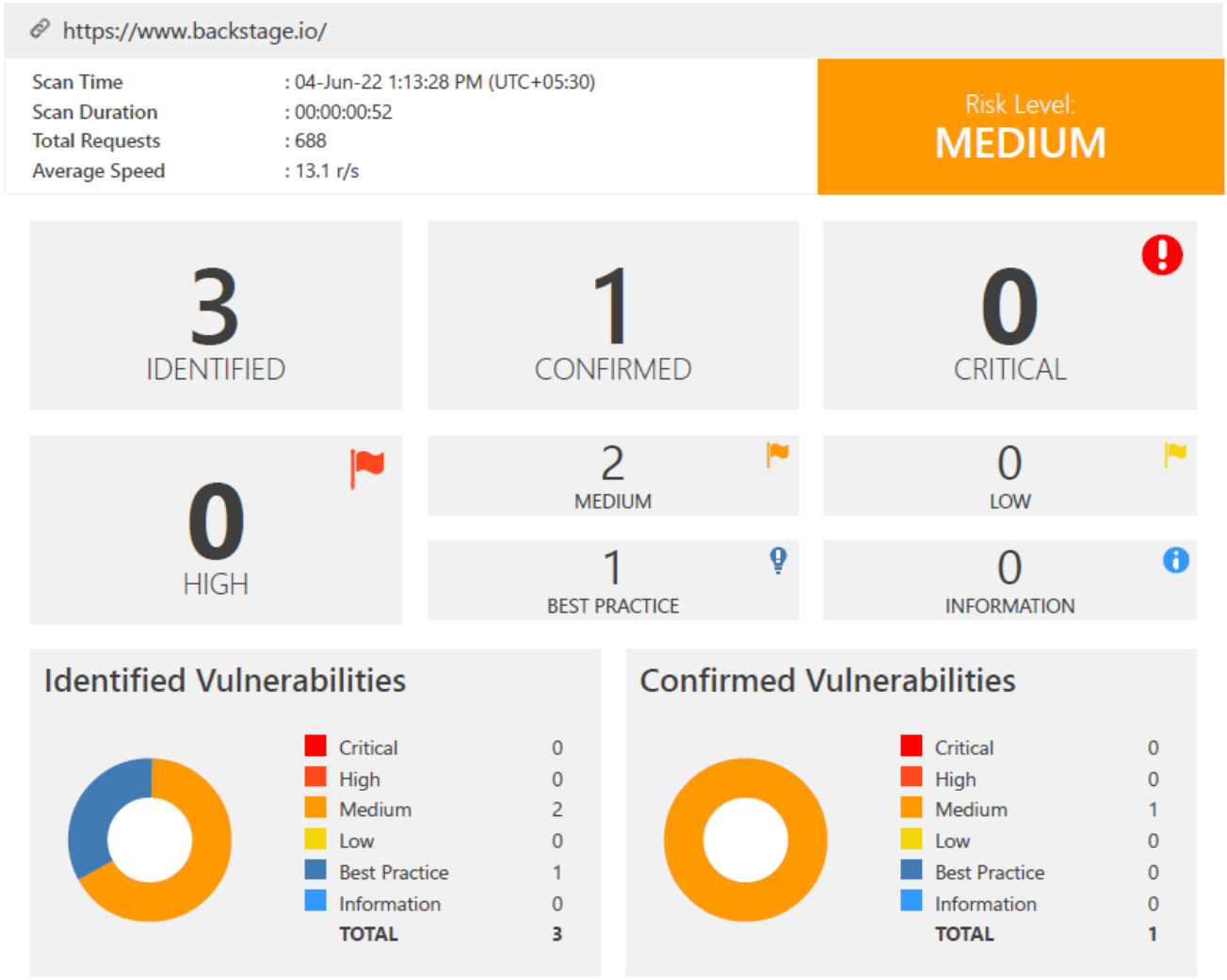
Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Remedy

We suggest that you implement SSL/TLS properly, for example by using the Certbot tool provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.

5.2.6. Backstage.io Netsparker vulnerability scanning



After Scanning the domain, I could find 2 medium risk vulnerability & total of 3 vulnerabilities regarding the domain.

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

MEDIUM 1

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

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

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

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

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

Vulnerabilities

1.1. https://www.backstage.io/

Certainty

Request

```
GET / HTTP/1.1
Host: backstage.io
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) : 304.3771 Total Bytes Received : 22749 Body Length : 22085 Is Compressed : No

```
HTTP/1.1 200 OK
X-Cache: HIT
X-Timer: S1654328616.361956,VS0,VE0
Age: 162
Cache-Control: max-age=600
ETag: W/"629a25d1-5645"
Access-Control-Allow-Origin: *
X-Fastly-Request-ID: d76c776ad1372f52f16fc65458cba46a14567db5
Server: GitHub.com
Connection: keep-alive
expires: Fri, 03 Jun 2022 21:04:42 GMT
Accept-Ranges: bytes
X-Cache-Hits: 8
Content-Length: 6055
X-GitHub-Request-Id: 1A98:24E7:C73CB:1404AA:629A7512
Vary: Accept-Encoding
Via: 1.1 varnish
X-Served-By: cache-qpg1266-QPG
Last-Modified: Fri, 03 Jun 2022 15:16:33 GMT
Content-Type: text/html; charset=utf-8
x-proxy-cache: MISS
Date: Sat, 04 Jun 2022 07:43:36 GMT
Content-Encoding:

<!DOCTYPE html><html lang=""><head><meta charSet="utf-8"/><meta http-equiv="X-UA-Compatible" content="I
E=edge"/><title>Backstage Software Catalog and Developer Platform · An open platform for building devel
oper portals</title><meta name="viewport" content="width=device-width, initial-scale=1.0"/><meta name
="generator" content="Docusaurus"/><meta name="description" content="An open platform for building deve
loper portals"/><meta property="og:title" content="Backstage Software Catalog and Developer Platform ·
 An open platform for building developer portals"/><meta property="og:type" content="website"/><meta pr
operty="og:url" content="https://backstage.io/"/><meta property="og:description" content="An open platf
orm for building developer portals"/><meta property="og:image" content="https://backstage.io/img/sharin
g-opengraph.png"/><meta name="twitter:card" content="summary"/><meta name="twitter:image" content="http
s://backstage.io/img/twitter-summary.png"/><link rel="shortcut icon" href="/img/favicon.ico"/><link rel
="stylesheet" href="https://cdn.jsdelivr.net/docsearch.js/1/docsearch.min.css"/><link rel="stylesheet"
 href="//cdnjs.cloudflare.com/ajax/libs/highlight.js/9.12.0/styles/monokai.min.css"/><link rel="alterna
te" type="application/atom+xml" href="https://backstage.io/blog/atom.xml" title="Backstage Software Cat
a
```

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

2. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

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.backstage.io/

CONFIRMED

List of Supported Weak Ciphers

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

Request

```
[NETSPARKER] SSL Connection
```

Response

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

```
[NETSPARKER] SSL Connection
```

5. Conclusion

In this report I have included all the information's & steps that I had taken to complete my audit on Spotify.com & it's some domains. And I made some recommendations to ensure the site security. All the vulnerabilities are classified according the risk levels & all the tools & mechanisms also included with explanations.

6. References

[1] "Spotify," Spotify, [Online]. Available: https://support.spotify.com/us/article/what-is-spotify/. [Accessed 02 06 2022].

[2] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Spotify. [Accessed 02 06 2022].

[3] Spotify, "Hackerone," [Online]. Available: https://hackerone.com/spotify?type=team&view_policy=true. [Accessed 03 06 2022].

[4] D. SON, "Penetration testing," [Online]. Available: https://securityonline.info/amass-subdomain-enumeration/#:~:text=The%20OWASP%20Amass%20tool%20suite,discover%20associated%20netblocks%20and%20ASNs.. [Accessed 03 06 2022].

[5] Mohdshariq, "Geeksforgeeks," [Online]. Available: https://www.geeksforgeeks.org/subbrute-tool-for-subdomain-brute-force/#:~:text=SubBrute%20is%20a%20free%20and,of%20anonymity%20for%20security%20researchers.. [Accessed 03 06 2022].

[6] N. org, "nmap," [Online]. Available: https://nmap.org/. [Accessed 03 06 2022].

[7] Nikto, "Kali org," [Online]. Available: https://www.kali.org/tools/nikto/. [Accessed 04 06 2022].

[8] Invicti, "Invicti," [Online]. Available: https://www.invicti.com/support/what-is-invicti/. [Accessed 04 06 2022].