

# Web Security Assignment



IT19130026

Samarasinghe M.L.S

<b>Content</b>	<b>Page</b>
<b>Introduction</b>	<b>03</b>
<b>Selecting a Domain</b>	<b>04</b>
<b>Getting Subdomains count</b>	<b>05</b>
<b>Frist Scan set</b>	<b>07</b>
<b>Results of First Scan set</b>	<b>11</b>
<b>Scan using Nikto Tool (port 80)</b>	<b>15</b>
<b>Scan using Nikto Tool (port 443)</b>	<b>36</b>
<b>Vulnerability Explanation</b>	<b>56</b>
<b>Scan using Lazyrecon</b>	<b>65</b>
<b>Inspect using Burp suite</b>	<b>66</b>
<b>References</b>	<b>67</b>

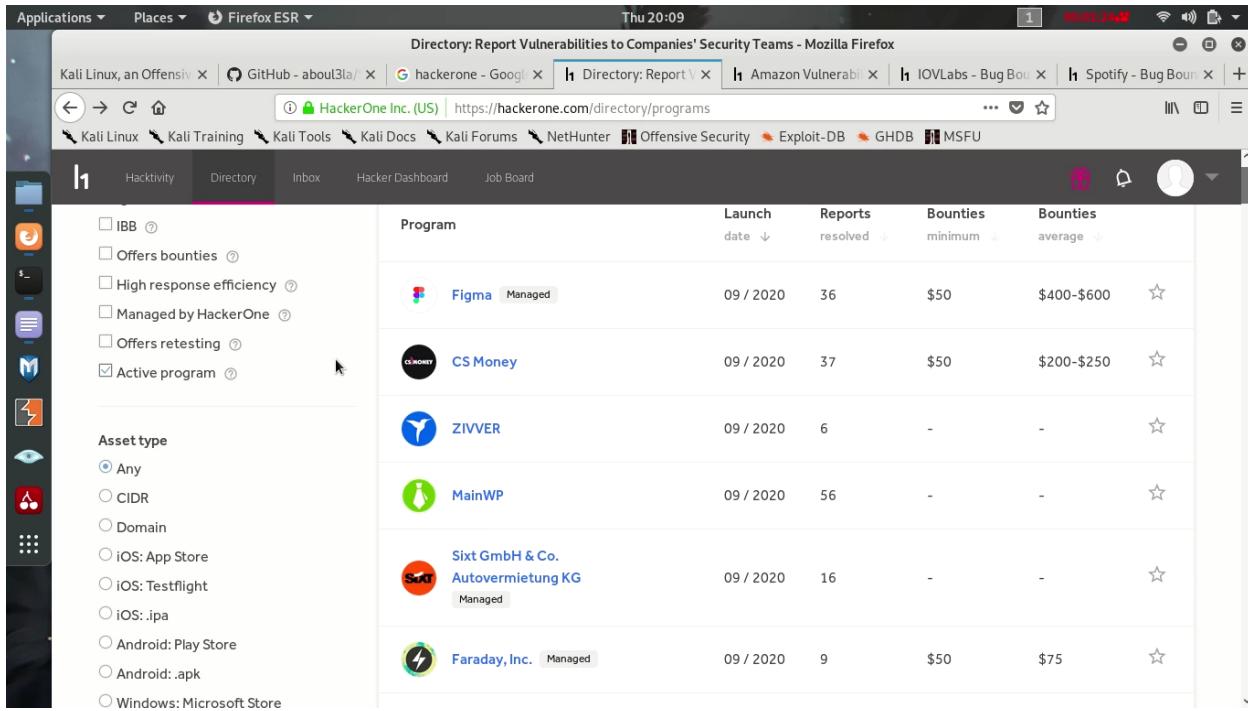
## Introduction

To complete this assignment, I used a few basic scans using few tools to check for the Top 10 Vulnerabilities listed by OWASP

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfigurations
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerability
- Insufficient logging and monitoring

I used **Sblist3r**, **Nikto**, **Netspaker pro**, **lazyrecon** for this scanning process.

## Selecting a Domain



The screenshot shows a Firefox ESR browser window with multiple tabs open. The active tab is 'Directory: Report Vulnerabilities to Companies' Security Teams - Mozilla Firefox' at <https://hackerone.com/directory/programs>. The page displays a list of active programs, each with a logo, name, status, launch date, report count, minimum bounty, average bounty, and a star icon for favoriting. The left sidebar includes filters for Hacktivity, Directory, Inbox, and Job Board, and dropdown menus for Asset type (Any selected) and other filtering options like IBB, Offers bounties, High response efficiency, Managed by HackerOne, Offers retesting, and Active program.

Program	Launch date	Reports resolved	Bounties minimum	Bounties average	Action
Figma Managed	09 / 2020	36	\$50	\$400-\$600	
CS Money	09 / 2020	37	\$50	\$200-\$250	
ZIVVER	09 / 2020	6	-	-	
MainWP	09 / 2020	56	-	-	
Sixt GmbH & Co. Autovermietung KG Managed	09 / 2020	16	-	-	
Faraday, Inc. Managed	09 / 2020	9	\$50	\$75	

To select a Subdomain, I logged in to the hackerone bug bounty program and I selected “[spotofy.com](#)” as my domain.

## Getting Subdomains count

I used this python tool called **Sublist3r** to scan my domain “**Spotify.com**” for its subdomain count.

You can use this link to watch the video hoe I selected a domain, how I installed this tool and scanned using this tool.

Link for the recorded Video #1:

<https://drive.google.com/file/d/1y4OAqTkz3TSrkJJY196rl3U74uexdqSP/view?usp=sharing>

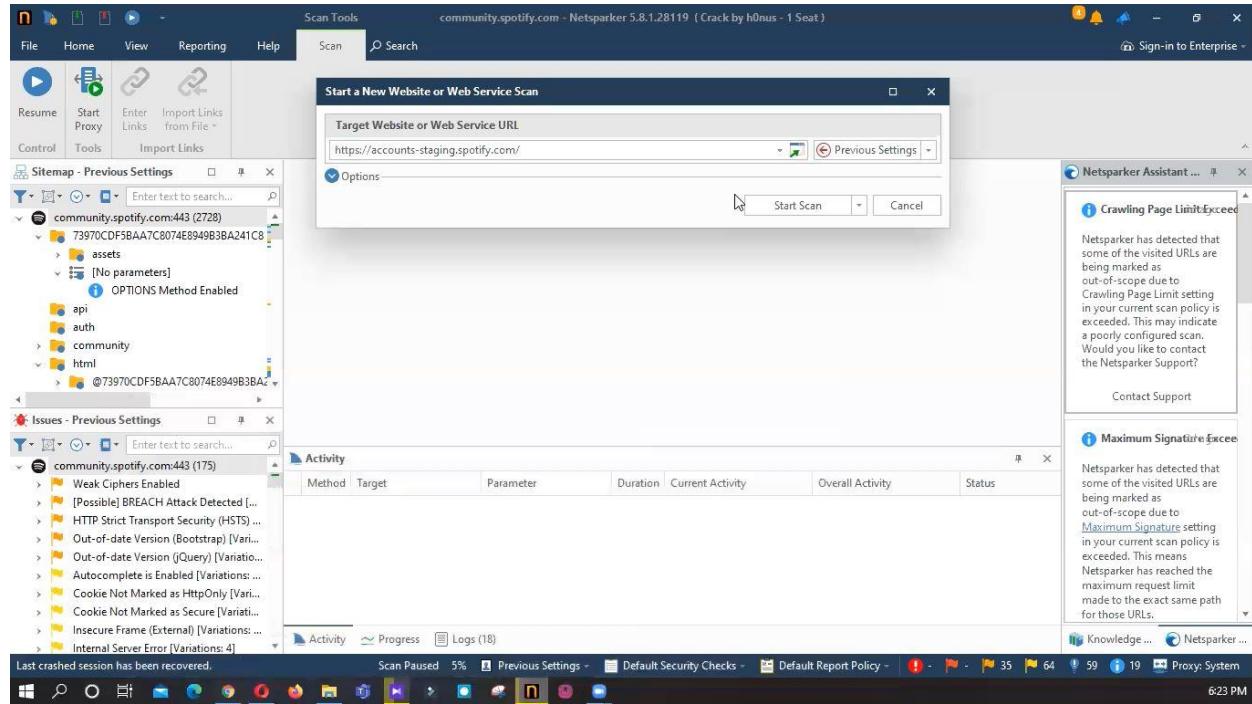
After that scan I got 158 subdomains as the results. Then I decided to use the subdomain list of 20 given in the hackerone platform's spotify page.

- accounts-staging.spotify.com
- accounts.spotify.com
- ads.spotify.com
- artists.spotify.com
- canvas.spotify.com
- certomato.spotify.com
- community.spotify.com
- csat-support-help-page-mobile.spotify.com
- developer.spotify.com
- homething.spotify.com
- hrblog.spotify.com
- newsroom.spotify.com
- podcasters.spotify.com
- promo.spotify.com
- purple.spotify.com
- spotify.com
- support.spotify.com
- surveys.spotify.com
- uplink.spotify.com
- works.spotify.com

## First Scan set

After I got subdomain list, I tried to scan few of them using that Netsparker Pro tool.

**Accounts-staging.spotify.com**



**Result:**

- Weak Ciphers Enabled
- HTTP Strict Transport Security (HSTS) ...
- Cookie Not Marked as HttpOnly [Variations: ...]
- Cookie Not Marked as Secure [Variations: ...]
- Insecure Frame (External) [Variations: ...]
- Insecure Transportation Security Protocols
- Missing X-Frame-Options Header [Variations: ...]
- Insecure Transportation Security Protocols
- Expect-CT Not Enabled
- Missing X-XSS-Protection Header [Variations: ...]

Here I get these two medium range vulnerabilities only. Other low range vulnerabilities wont effect to the domain.

## Account.spotify.com

The screenshot shows the Netsparker Web Security Scanner interface. The main window displays a 'Start a New Website or Web Service Scan' dialog with the URL 'https://accounts-staging.spotify.com/' entered. The 'Scan Tools' tab is selected. On the left, there's a tree view of the website's structure, including 'ott', 'recover', 'en', and 'login'. The 'Issues - Previous Settings' section lists 138 findings, with several items highlighted in yellow. The 'Response' tab shows raw request and response data. The 'Progress' tab displays a graph of scan speed and progress, currently at 25.84% completion. The status bar at the bottom indicates the scan started on 10/13/2020 at 6:24:31 PM.

## Results:

The screenshot shows the detailed results for the 'accounts.spotify.com:443 (147)' scan. A red box highlights two specific findings under the 'Issues' section: 'Weak Ciphers Enabled' and 'HTTP Strict Transport Security (HSTS) ...'. Both of these findings are marked with a yellow warning icon. The list also includes other findings such as 'Cookie Not Marked as HttpOnly [Vari...]', 'Cookie Not Marked as Secure [Variati...', 'Insecure Frame (External) [Variations: ...]', 'Insecure Transportation Security Prot...', 'Internal Server Error [Variations: 3]', '[Possible] Phishing by Navigating Bro...', 'Missing X-Frame-Options Header [Va...', and 'Insecure Transportation Security Prot...'. The entire list is preceded by a small Spotify logo icon.

## adstudio.spotify.com

The screenshot shows the Netsparker Web Security Scanner interface. A modal window titled "Start a New Website or Web Service Scan" is open, displaying the URL "https://adstudio.spotify.com/". Below the URL, there are two tabs: "CONFIRMED" (selected) and "MEDIUM". The main pane shows the URL "https://accounts.spotify.com/" and a 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), and TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xC013). The "Issues - Previous Settings" panel on the left lists 147 issues, including "Weak Ciphers Enabled" and "HTTP Strict Transport Security (HSTS) ...". The "Progress" panel shows a green bar for "Scan Speed" and a blue bar for "Scan Progress" at 100.00%. The bottom status bar indicates "Scan Finished". The "Knowledge Base (18)" panel on the right contains links to various findings.

## Results:

The screenshot shows the scan results for "adstudio.spotify.com:443 (79)". The results are listed in a tree view. Two specific items are highlighted with a red border: "Weak Ciphers Enabled" and "HTTP Strict Transport Security (HSTS) ...". Other visible items include "Cookie Not Marked as HttpOnly", "Cookie Not Marked as Secure", "Insecure Frame (External) [Variations: 1]", "Insecure Transportation Security Prot...", "Internal Server Error [Variations: 6]", "Missing X-Frame-Options Header [Va...]", "Insecure Transportation Security Prot...", and "Content Security Policy (CSP) Not Im...".

## spotify.com

The screenshot shows the Netsparker interface with a scan in progress for the website <https://spotify.com/>. The main window displays a list of issues found during the scan, including:

- Weak Ciphers Enabled
- HTTP Strict Transport Security (HSTS) Error
- Insecure Transportation Security Protocol
- Insecure Transportation Security Protocol
- Expect-CT Not Enabled

The 'Issues - Previous Settings' panel on the left lists various security-related findings. The 'External References' panel on the right provides links to OWASP guidelines and other resources. The 'Progress' section at the bottom shows the scan's progress, speed, and activity metrics.

## Results:

The results pane for [spotify.com:443](https://spotify.com:443) shows the following findings:

- Weak Ciphers Enabled
- HTTP Strict Transport Security (HSTS) Error
- Insecure Transportation Security Protocol
- Insecure Transportation Security Protocol
- Expect-CT Not Enabled

The first two items, 'Weak Ciphers Enabled' and 'HTTP Strict Transport Security (HSTS) Error', are highlighted with a red border.

Here you can see I got the same results after scanning these subdomains.

## Results of first Scan Set

### Weak Ciphers Enabled

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)

### CLASSIFICATION

- PCI DSS 3.26.5.4
- OWASP 2013A6
- OWASP 2017A3
- CWE327
- CAPEC217
- WASC4
- ISO27001A.14.1.3

### CVSS 3.0 SCORE

Base6.8 (Medium)

- Temporal6.8 (Medium)
- Environmental6.8 (Medium)
- CVSS Vector String
- CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

### CVSS 3.1 SCORE

- Base6.8 (Medium)
- Temporal6.8 (Medium)
- Environmental6.8 (Medium)
- CVSS Vector String
- CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

## **Vulnerability Details**

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.

## **Actions to Take**

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

SSLCipherSuite HIGH: MEDIUM: !MD5: !RC4

Lighttpd:

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

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

a. Click Start, click Run, type regedt32 or type regedit, and then click OK.

b. In Registry Editor, locate the following registry key:

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

c. Set "Enabled" DWORD to "0x0" for the following registry keys:

- SCHANNEL\Ciphers\DES 56/56
- SCHANNEL\Ciphers\RC4 64/128
- SCHANNEL\Ciphers\RC4 40/128
- SCHANNEL\Ciphers\RC2 56/128
- SCHANNEL\Ciphers\RC2 40/128
- SCHANNEL\Ciphers\NULL
- SCHANNEL\Hashes\MD5Remedy

Configure your web server to disallow using weak ciphers.

## **External References**

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)

- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd

### **HTTP strict Transport Security (HSTS) Errors and Warnings**

#### **CLASSIFICATION:**

- OWASP 2013A5
- OWASP 2017A6
- CWE16
- WASC15
- ISO27001A.14.1.2

#### **Error Resolution**

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

#### **Vulnerability Details**

Netspaker 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.

#### **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 include Subdomains 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)

#### External References

- HTTP Strict Transport Security (HSTS) HTTP Header
- Wikipedia - HTTP Strict Transport Security Implementation
- Check HSTS Preload status and eligibility

You can use this link to watch how I scanned those subdomains using Netsparker Pro tool.

Link for the recorded Video #2:

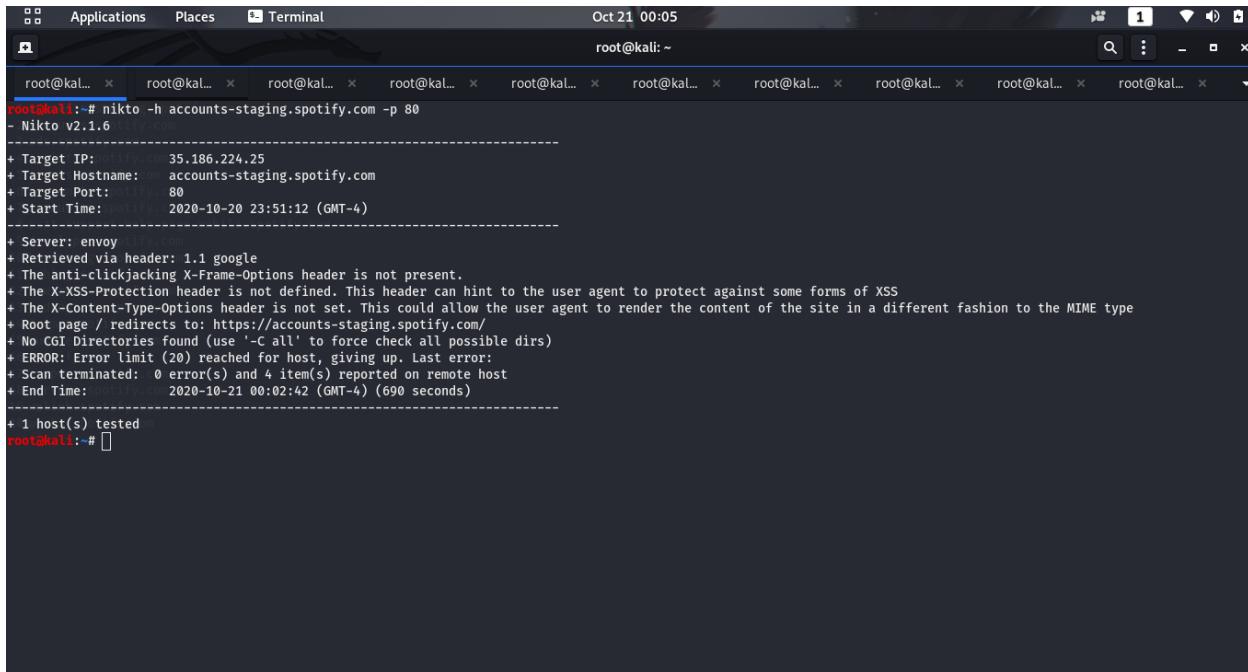
<https://drive.google.com/file/d/183Q2k5rshggQe78FGcbklpTkze48B0iW/view?usp=sharing>

## Scan using Nikto Tool (port 80)

After above scans, I realized Netspaker takes time. Then I decided to use Nikto tool before Netspaker because Nikto is speeder than Netspaker and after that scan few specific subdomains using Netspaker.

### First, I scanned all subdomains for port 80.

**accounts-staging.spotify.com**

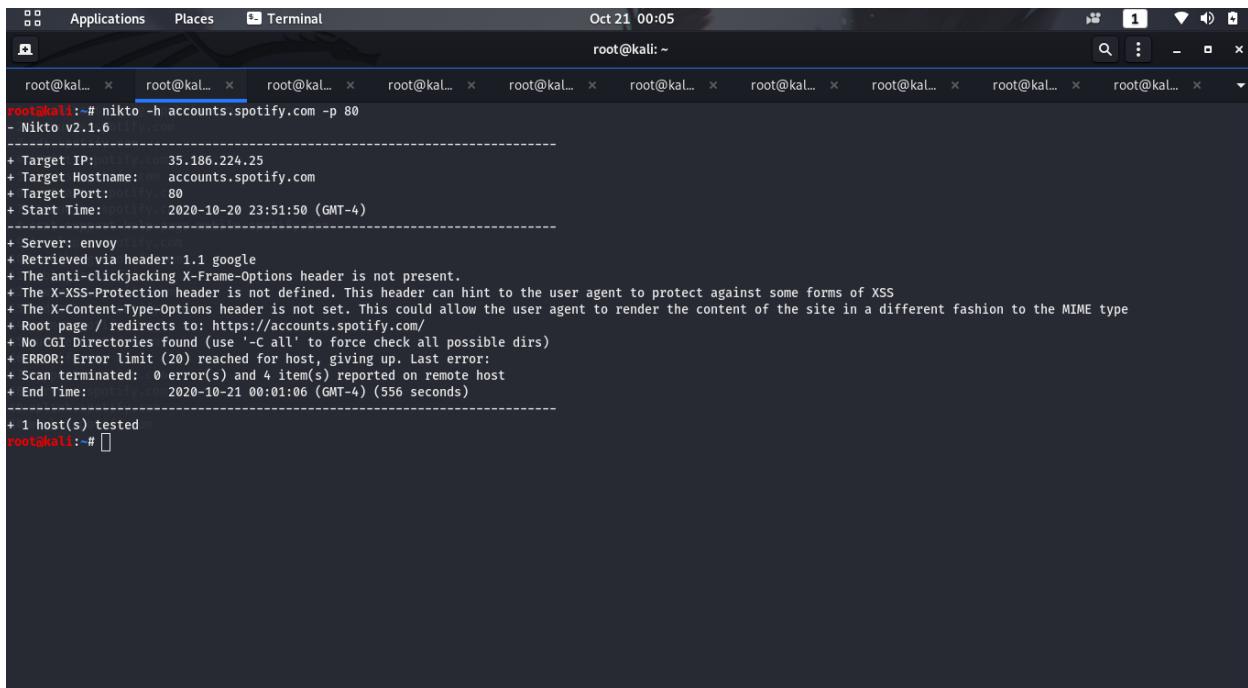


```
root@kali:~# nikto -h accounts-staging.spotify.com -p 80
- Nikto v2.1.6
[+] http://accounts-staging.spotify.com:80
[+] Target IP: 35.186.224.25
[+] Target Hostname: accounts-staging.spotify.com
[+] Target Port: 80
[+] Start Time: 2020-10-20 23:51:12 (GMT-4)
[+] Server: envoy
[+] Retrieved via header: 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://accounts-staging.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: 0 error(s) and 4 item(s) reported on remote host
[+] End Time: 2020-10-21 00:02:42 (GMT-4) (690 seconds)

+ 1 host(s) tested
root@kali:~#
```

1. Clickjacking
2. X-XSS-Protection header is not defined
3. X-Content-Type-Options header is not set

## accounts.spotify.com

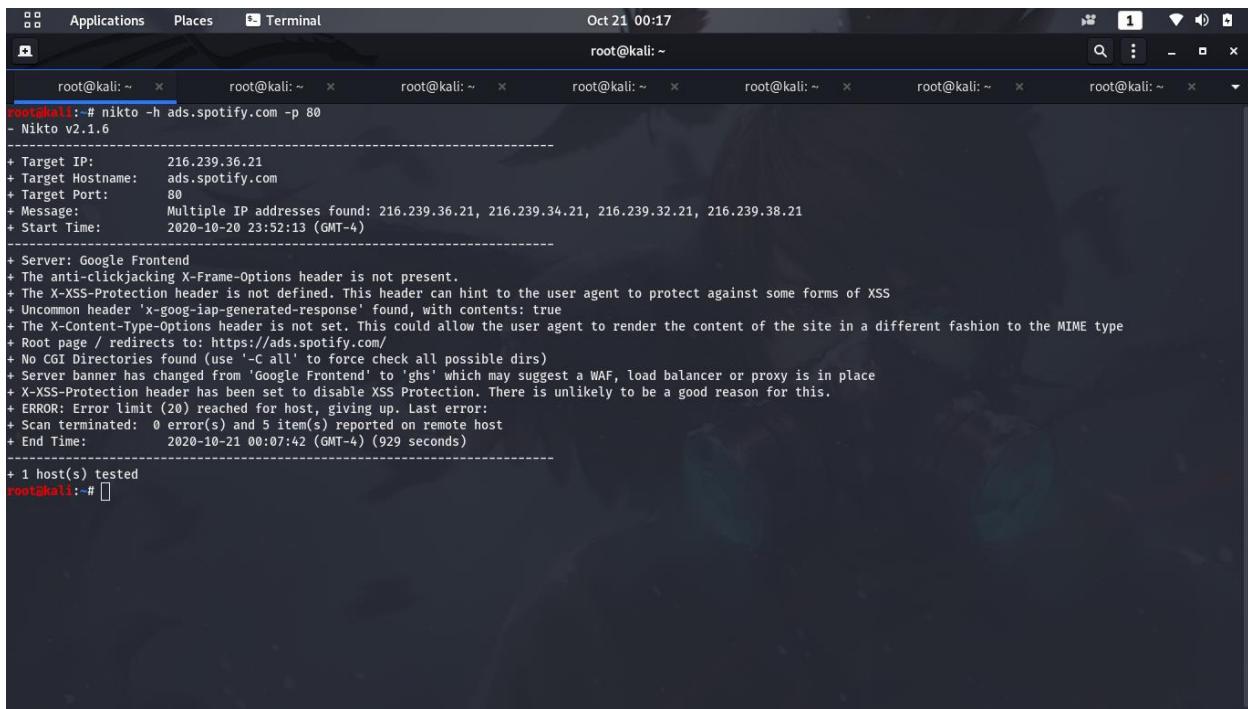


The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "Terminal". The date and time "Oct 21 00:05" are displayed at the top right. The command entered is "nikto -h accounts.spotify.com -p 80". The output of the scan is displayed below:

```
root@kali:~# nikto -h accounts.spotify.com -p 80
- Nikto v2.1.6
-----
+ Target IP: 35.186.224.25
+ Target Hostname: accounts.spotify.com
+ Target Port: 80
+ Start Time: 2020-10-20 23:51:50 (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://accounts.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: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2020-10-21 00:01:06 (GMT-4) (556 seconds)
-----
+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. X-Content-Type-Options header is not set**

## ads.spotify.com



The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "Terminal". The date and time "Oct 21 00:17" are displayed at the top right. There are multiple tabs open, all labeled "root@kali: ~". The current tab contains the output of a Nikto scan:

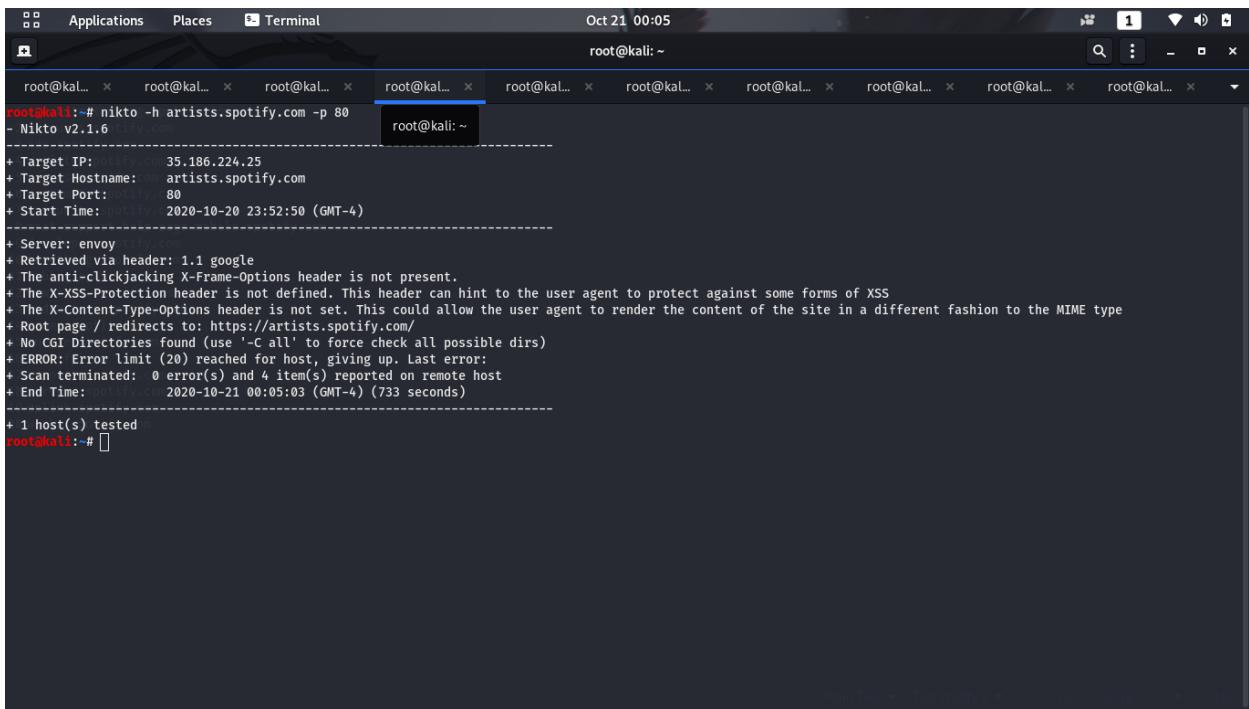
```
root@kali: ~ # nikto -h ads.spotify.com -p 80
- Nikto v2.1.6
-----
+ Target IP:      216.239.36.21
+ Target Hostname: ads.spotify.com
+ Target Port:    80
+ Message:        Multiple IP addresses found: 216.239.36.21, 216.239.34.21, 216.239.32.21, 216.239.38.21
+ Start Time:     2020-10-20 23:52:13 (GMT-4)

+ Server: Google Frontend
+ 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-goog-iap-generated-response' found, with contents: true
+ 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://ads.spotify.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'Google Frontend' to 'ghs' which may suggest a WAF, load balancer or proxy is in place
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 5 item(s) reported on remote host
+ End Time:       2020-10-21 00:07:42 (GMT-4) (929 seconds)

+ 1 host(s) tested
root@kali: ~ #
```

1. Clickjacking
2. X-XSS-Protection header is not defined
3. X-Content-Type-Options header is not set

## artists.spotify.com

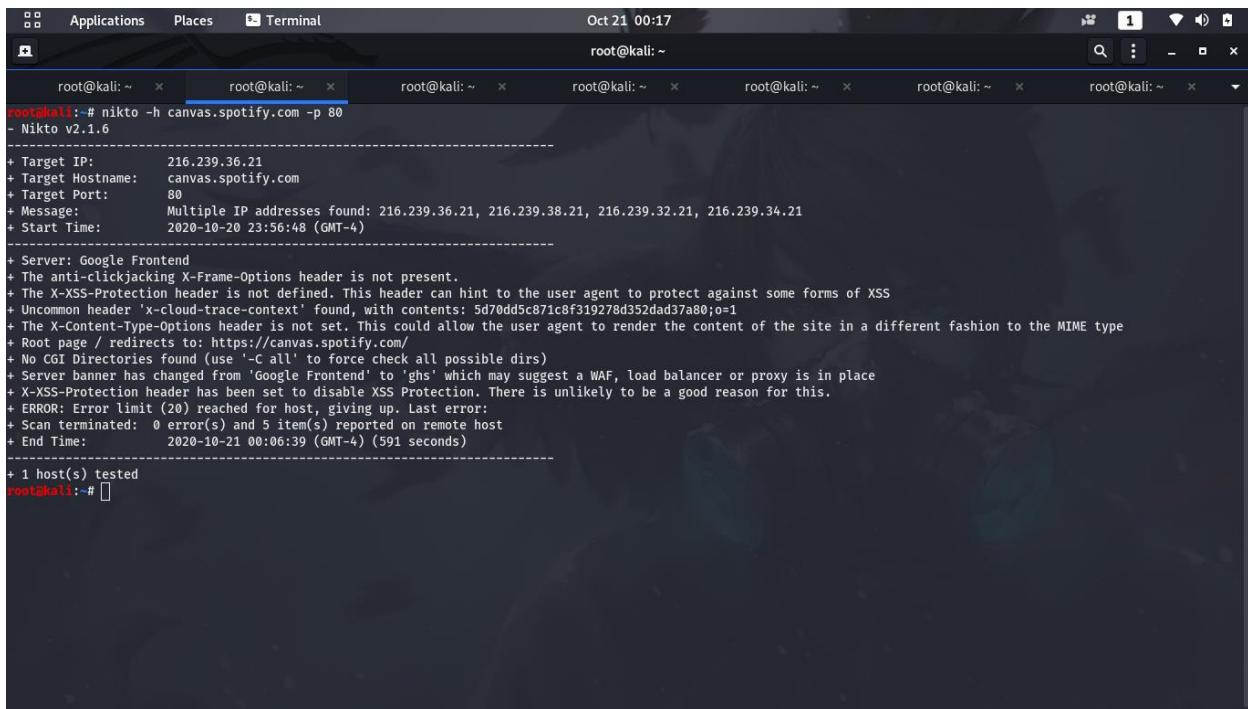


```
root@kali:~# nikto -h artists.spotify.com -p 80
- Nikto v2.1.6
[+] http://artists.spotify.com:80

-----[+]
+ Target IP: 35.186.224.25
+ Target Hostname: artists.spotify.com
+ Target Port: 80
+ Start Time: 2020-10-20 23:52:50 (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://artists.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: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2020-10-21 00:05:03 (GMT-4) (733 seconds)
-----[+]
+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. X-Content-Type-Options header is not set**

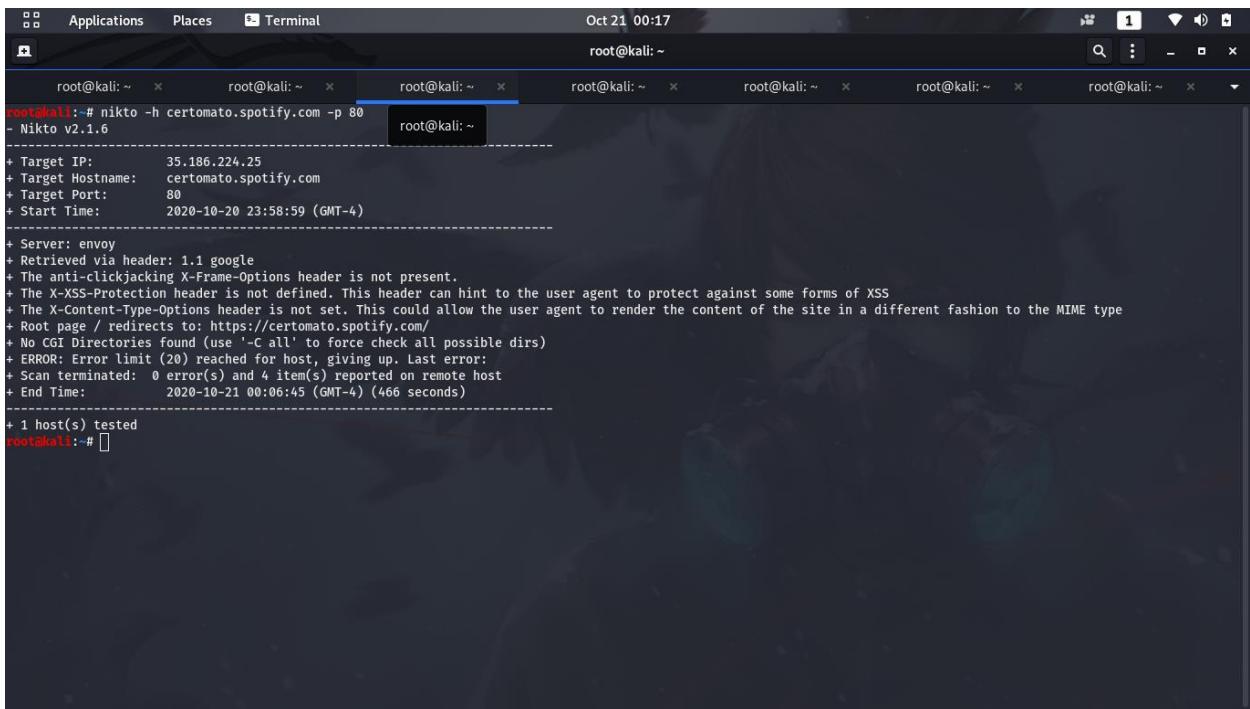
## canvas.spotify.com



```
root@kali: ~ x root@kali: ~ x
Oct 21 00:17
root@kali: ~
root@kali: # nikto -h canvas.spotify.com -p 80
- Nikto v2.1.6
-----
+ Target IP: 216.239.36.21
+ Target Hostname: canvas.spotify.com
+ Target Port: 80
+ Message: Multiple IP addresses found: 216.239.36.21, 216.239.38.21, 216.239.32.21, 216.239.34.21
+ Start Time: 2020-10-20 23:56:48 (GMT-4)
-----
+ Server: Google Frontend
+ 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-cloud-trace-context' found, with contents: 5d70ddd5c871c8f319278d352dad37a80;o=1
+ 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://canvas.spotify.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'Google Frontend' to 'ghs' which may suggest a WAF, load balancer or proxy is in place
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2020-10-21 00:06:39 (GMT-4) (591 seconds)
-----
+ 1 host(s) tested
root@kali: #
```

1. Clickjacking
2. X-XSS-Protection header is not defined
3. X-Content-Type-Options header is not set

## certomato.spotify.com



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title is 'Terminal' and the date and time are 'Oct 21 00:17'. There are multiple tabs in the terminal, all labeled 'root@kali: ~'. The active tab displays the output of the Nikto web scanner. The command run was 'nikto -h certomato.spotify.com -p 80'. The output shows the target IP is 35.186.224.25, the target hostname is certomato.spotify.com, and the target port is 80. The start time was 2020-10-20 23:58:59 (GMT-4) and the end time was 2020-10-21 00:06:45 (GMT-4). The scan took 466 seconds. The report highlights several issues:

- + 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://certomato.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: 0 error(s) and 4 item(s) reported on remote host
- + End Time: 2020-10-21 00:06:45 (GMT-4) (466 seconds)

+ 1 host(s) tested

root@kali: #

1. Clickjacking
2. X-XSS-Protection header is not defined
3. X-Content-Type-Options header is not set

## community.spotify.com

```

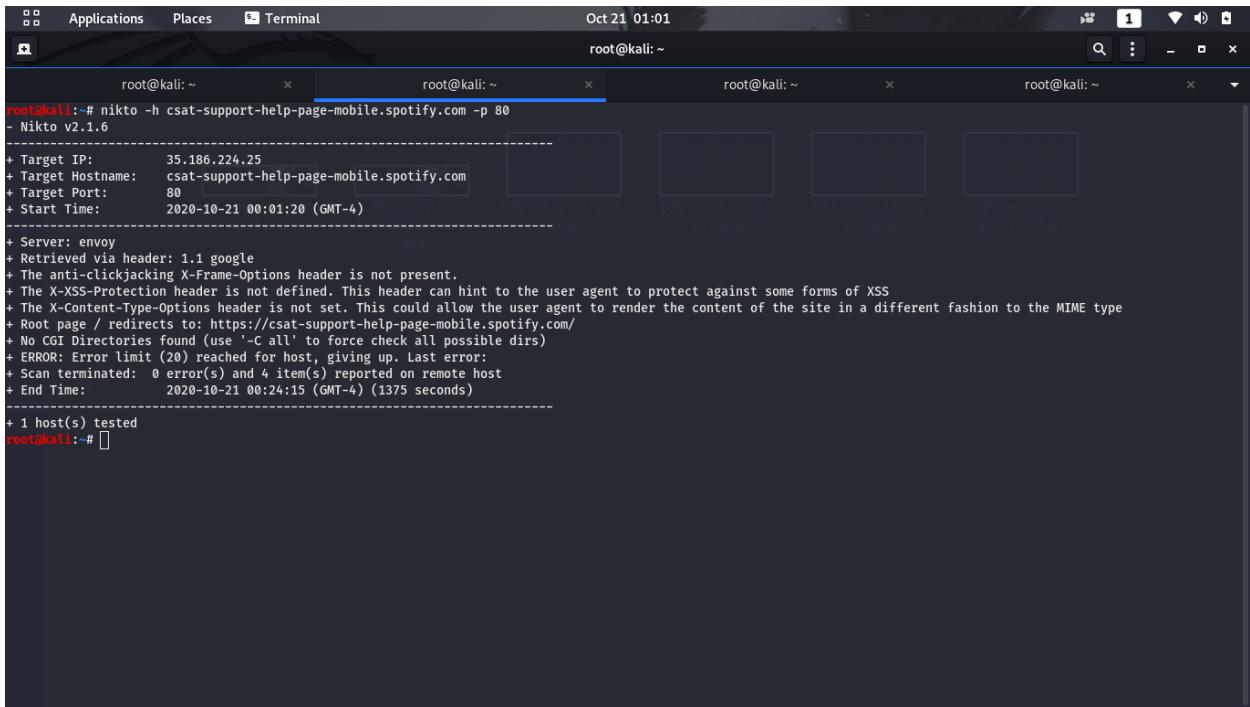
root@kali:~# Applications Places Terminal Oct 21 01:01
root@kali:~# nikto -h community.spotify.com -p 80
root@kali:~# Nikto v2.1.6
-----[REDACTED]-----[REDACTED]-----[REDACTED]-----[REDACTED]-----[REDACTED]
+ Target IP: 13.33.234.15
+ Target Hostname: community.spotify.com
+ Target Port: 80
+ Message: Multiple IP addresses found: 13.33.234.15, 13.33.234.59, 13.33.234.69, 13.33.234.91
+ Start Time: 2020-10-21 00:00:11 (GMT-4)
-----[REDACTED]-----[REDACTED]-----[REDACTED]-----[REDACTED]-----[REDACTED]
+ Server: Apache
+ Retrieved via header: 1.1 e43c7f33e20c02c01ba46ebadfa00ed4.cloudfront.net (CloudFront)
+ 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-amz-cf-id' found, with contents: swtjfjgskFq5HtG0Ae2Nc4zzFx-yCiwudQfervChG36_ixNoQTKg==
+ Uncommon header 'x-cache' found, with contents: Miss from cloudfront
+ Uncommon header 'x-amz-cf-pop' found, with contents: MAD51-C1
+ 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
+ Cookie AWSALBCORS created without the httponly flag
+ Cookie AWSALBCORS created without the httponly flag
+ Cookie LithiumUserInfo created without the httponly flag
+ Cookie LithiumUserSecure created without the httponly flag
+ Root page / redirects to: https://community.spotify.com/
+ Cookie LithiumCookiesAccepted created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/t5/forums/forumtopicprintpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/ideas/ideaprintpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/blogs/blogarticleprintpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/tkb/allarticlesprintpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/tkb/articleprintpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/media/gallerypage/*all/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/help/faapage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/usersonlinepage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/recentpostspage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/util/componentrenderpage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/tkb/articlehistorypage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/replypage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/postpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
-----[REDACTED]-----[REDACTED]-----[REDACTED]-----[REDACTED]-----[REDACTED]
root@kali:~# Applications Places Terminal Oct 21 01:01
root@kali:~# nikto -h community.spotify.com -p 80
root@kali:~# root@kali:~# root@kali:~# root@kali:~# root@kali:~#
-----[REDACTED]-----[REDACTED]-----[REDACTED]-----[REDACTED]-----[REDACTED]
+ Entry '/t5/notes/composepage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/notes/privatenotespage/tab/compose/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/notes/v1.1/privatenotespage/tab/compose/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/notifications/notifymoderatorpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/auth/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/plugins/common/feature/oauth/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/plugins/common/feature/oauth2sso/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/plugins/common/feature/saml/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/plugins/common/feature/openidconnectsso/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/plugins/common/feature/openidssso/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/t5/occasions/createoccasiionpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/occasions/editoccasionpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/forumtopicprintpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/blogs/blogarticleprintpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/help/faapage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/searchpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/tagdetailpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/tagleaderboardpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/user/viewprofilepage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/kudosleaderboardpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/tkb/articlehistorypage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/replypage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/usersonlinepage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/recentpostspage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Server banner has changed from 'Apache' to 'CloudFront' which may suggest a WAF, load balancer or proxy is in place
+ Entry '/spotify/attachments/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/searchpage/tab/tkb/*' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/util/componentrenderpage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/custom/page/page-id/Threepwood/*' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ "robots.txt" contains 62 entries which should be manually viewed.
+ 8056 requests: 1 error(s) and 55 item(s) reported on remote host
+ End Time: 2020-10-21 00:50:58 (GMT-4) (3047 seconds)
+ 1 host(s) tested
root@kali:~# 
```

Since this report is hard to understand, I used Netsparker Pro to scan this subdomain again.

The screenshot shows the Netsparker web security scanner interface. The main window displays the 'HTTP Request / Response' tab, showing a raw request for a file named 'sp-bootstrap.min.js'. The request includes headers such as 'GET / HTTP/1.1', 'Host: community.spotify.com', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8', and 'Accept-Encoding: gzip, deflate'. Below the request is a 'Response' section showing a single line of text: 'HTTP/1.1 200 OK Set-Cookie: AwSALB=GfUz5gSbqoA+ZIye48VJKL8u9WteXQDI8gL5u25XKLvPan0qoq02QGv2pofzhq0Kgmb/jLvCA6znoRCQSp0Szeqxnk...'. To the left of the main window, there is a tree view of the scanned URLs under 'community.spotify.com:443 (1166)' and a list of 'Issues - Previous Settings' which includes items like '[Possible] BREACH Attack Detected [Variations: 1]', '[HTTP Strict Transport Security (HSTS) Policy Not Enabled]', '[Out-of-date Version (jQuery) [Variations: 11]]', '[Autocomplete is Enabled [Variations: 11]]', '[Cookie Not Marked as HttpOnly [Variations: 11]]', '[Cookie Not Marked as Secure [Variations: 11]]', '[Insecure Frame (External) [Variations: 11]]', '[Internal Server Error]', '[Missing X-Frame-Options Header]', and '[Insecure Transportation Security Protocol]'. On the right side of the interface, there are two warning boxes: 'DOM Load Timeout Exceeded' and 'Crawling Page Limit Exceeded'. The 'DOM Load Timeout Exceeded' box states that 'Netsparker has detected that the configured DOM Load Timeout value is insufficient to load some of the URLs in your scan. Increase the value in the Scan Policy to keep the scan coverage at its best.' The 'Crawling Page Limit Exceeded' box states that 'Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Crawling Page Limit setting in your current scan policy is exceeded. This may indicate a poorly configured scan. Would you like to contact the Netsparker Support?'. At the bottom of the interface, there is a progress bar showing 'Scan Progress' at 100.00% and various activity metrics: Links: 7500, Failed Requests: 1105, 404 Responses: 91, Head Requests: 200, Total Requests: 2981, Elapsed: 01:08:28, Start: 10/22/2020 1:13:58 AM.

- 1. BREACH Attack (Possible)**
- 2. HTTP Strict Transport Security (HSTS) Policy Not Enabled**
- 3. Out-of-date Version (jQuery)**
- 4. Autocomplete is Enabled**
- 5. Cookie Not Marked as Http Only**
- 6. Cookie Not Marked as Secure**
- 7. Insecure Frame (External)**
- 8. Missing X-Frame-Options Header**

## csat-support-help-page-mobile.spotify.com



The screenshot shows a Kali Linux desktop environment with four terminal windows open. The active terminal window displays the output of a Nikto scan against the target host. The output highlights several security issues:

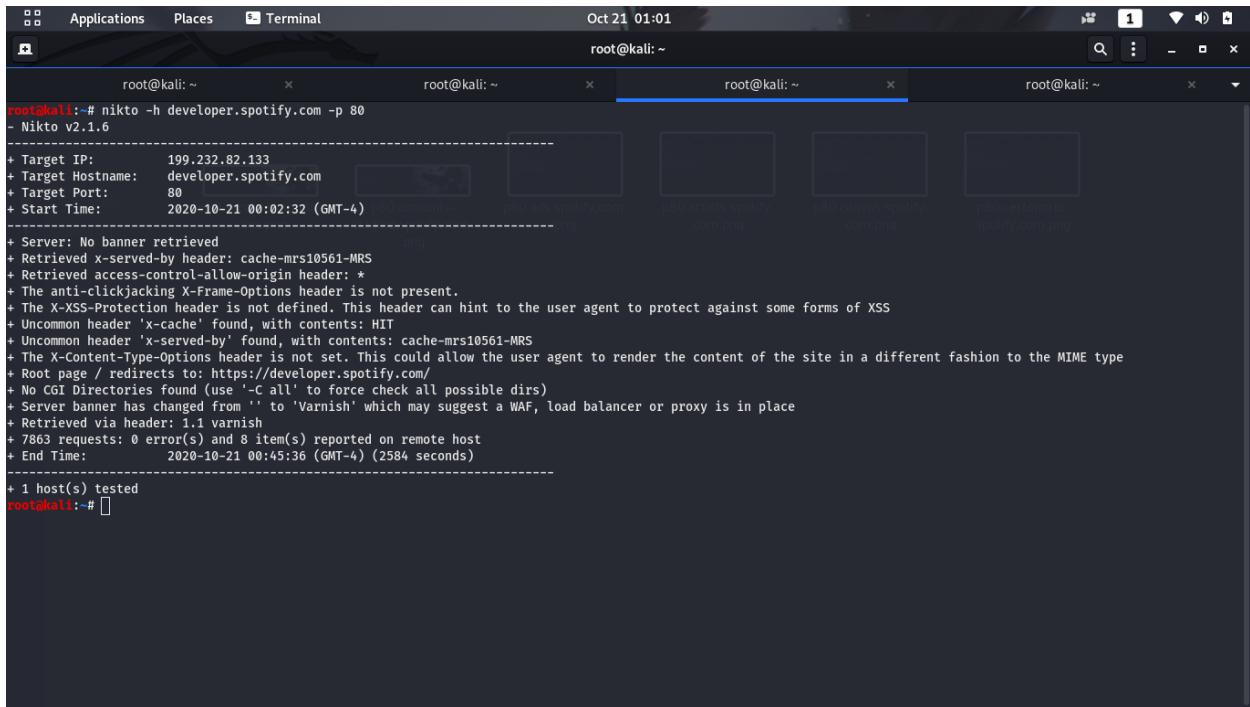
```
root@kali:~# nikto -h csat-support-help-page-mobile.spotify.com -p 80
- Nikto v2.1.6
[+] Target IP:      35.186.224.25
[+] Target Hostname: csat-support-help-page-mobile.spotify.com
[+] Target Port:    80
[+] Start Time:    2020-10-21 00:01:20 (GMT-4)
[+] End Time:      2020-10-21 00:24:15 (GMT-4) (1375 seconds)

[+] 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://csat-support-help-page-mobile.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: 0 error(s) and 4 item(s) reported on remote host
[+] End Time:      2020-10-21 00:24:15 (GMT-4) (1375 seconds)

[+] 1 host(s) tested
root@kali:~#
```

1. Clickjacking
2. X-XSS-Protection header is not defined
3. X-Content-Type-Options header is not set

## developer.spotify.com



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title bar says "Terminal". The date and time at the top right of the screen are "Oct 21 01:01". The terminal window has four tabs, all labeled "root@kali: ~". The active tab displays the output of a Nikto scan:

```
root@kali:~# nikto -h developer.spotify.com -p 80
- Nikto v2.1.6

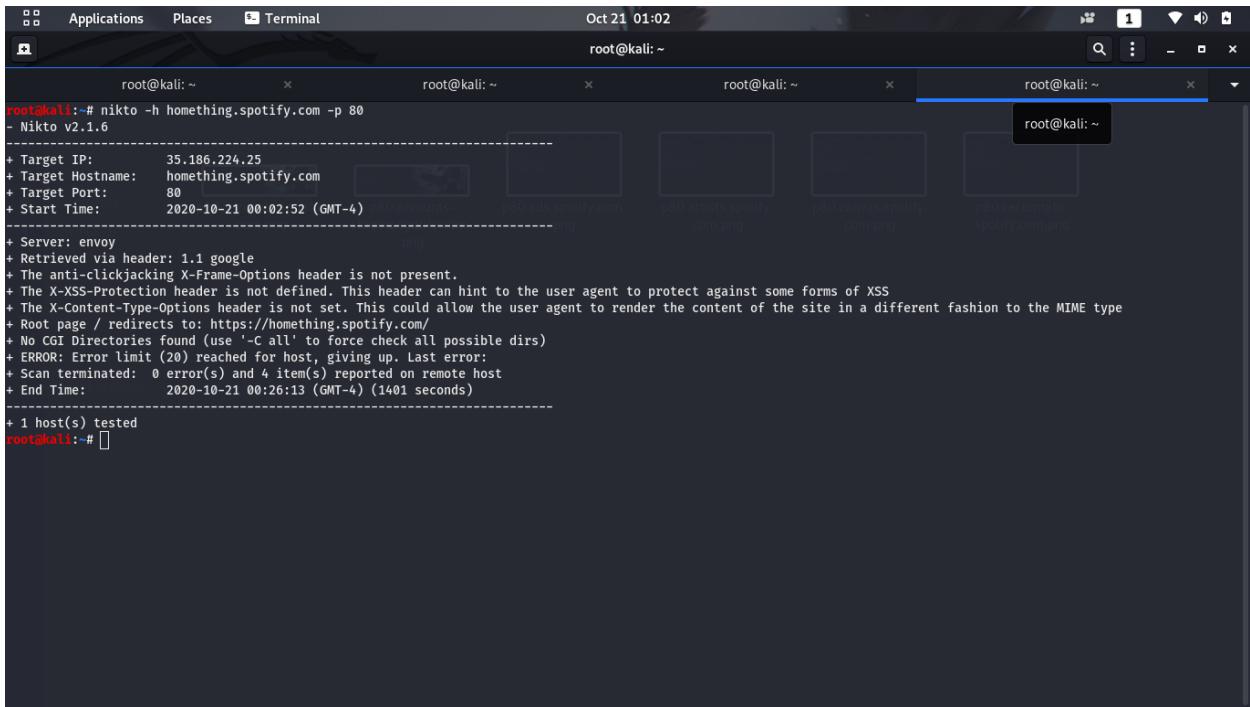
+ Target IP:      199.232.82.133
+ Target Hostname: developer.spotify.com
+ Target Port:    80
+ Start Time:    2020-10-21 00:02:32 (GMT-4)

+ Server: No banner retrieved
+ Retrieved x-served-by header: cache-mrs10561-MRS
+ Retrieved access-control-allow-origin header: *
+ 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-served-by' found, with contents: cache-mrs10561-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://developer.spotify.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from '' to 'Varnish' which may suggest a WAF, load balancer or proxy is in place
+ Retrieved via header: 1.1 varnish
+ 7863 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:       2020-10-21 00:45:36 (GMT-4) (2584 seconds)

+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. X-Content-Type-Options header is not set**

## homething.spotify.com



The screenshot shows a terminal window titled "Terminal" with four tabs open, all belonging to the root user at kali:~. The current tab displays the output of a Nikto scan against the host homething.spotify.com on port 80. The scan results highlight several security issues:

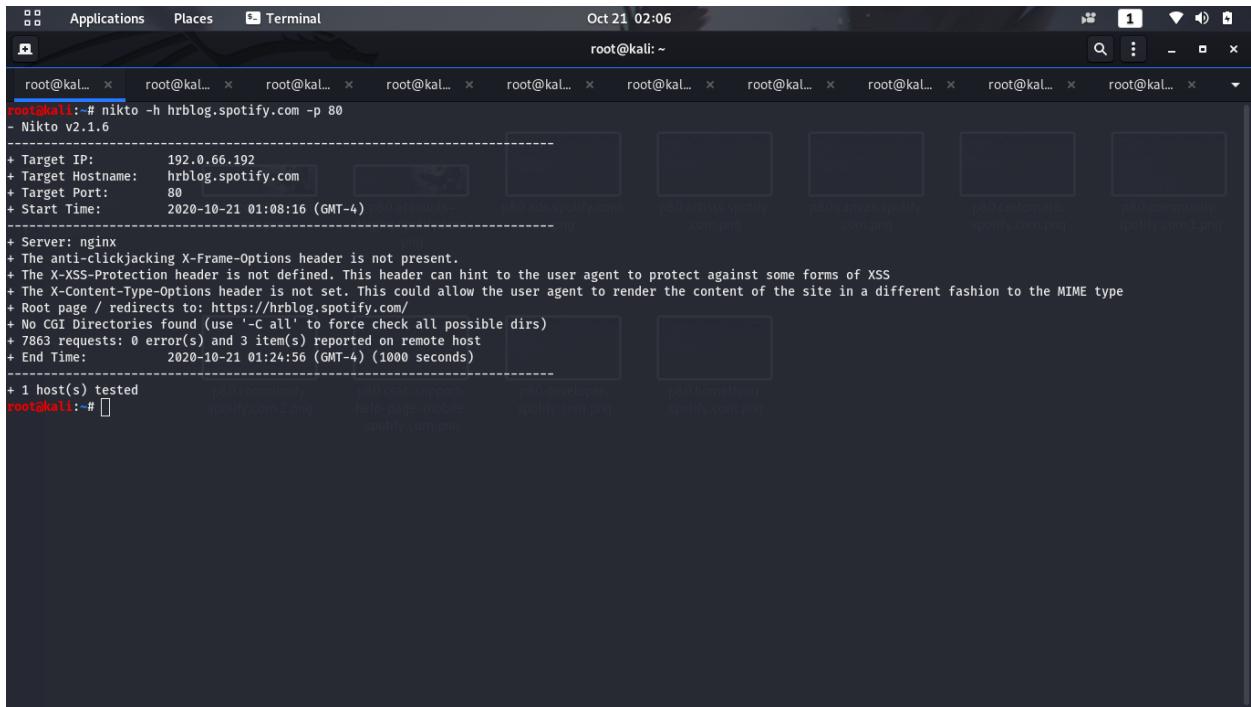
```
root@kali:~# nikto -h homething.spotify.com -p 80
- Nikto v2.1.6
[+] Target IP:      35.186.224.25
[+] Target Hostname: homething.spotify.com
[+] Target Port:    80
[+] Start Time:    2020-10-21 00:02:52 (GMT-4)
[+] End Time:      2020-10-21 00:26:13 (GMT-4) (1401 seconds)

[+] 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://homething.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: 0 error(s) and 4 item(s) reported on remote host
[+] End Time:      2020-10-21 00:26:13 (GMT-4) (1401 seconds)

[+] 1 host(s) tested
root@kali:~#
```

1. Clickjacking
2. X-XSS-Protection header is not defined
3. X-Content-Type-Options header is not set

## hrblog.spotify.com



The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "Terminal". The date and time "Oct 21 02:06" are displayed at the top right. The terminal window has multiple tabs, all showing the command "root@kali: ~". The current tab displays the output of the Nikto web scanner. The output shows the following details:

```
root@kali:~# nikto -h hrblog.spotify.com -p 80
- Nikto v2.1.6

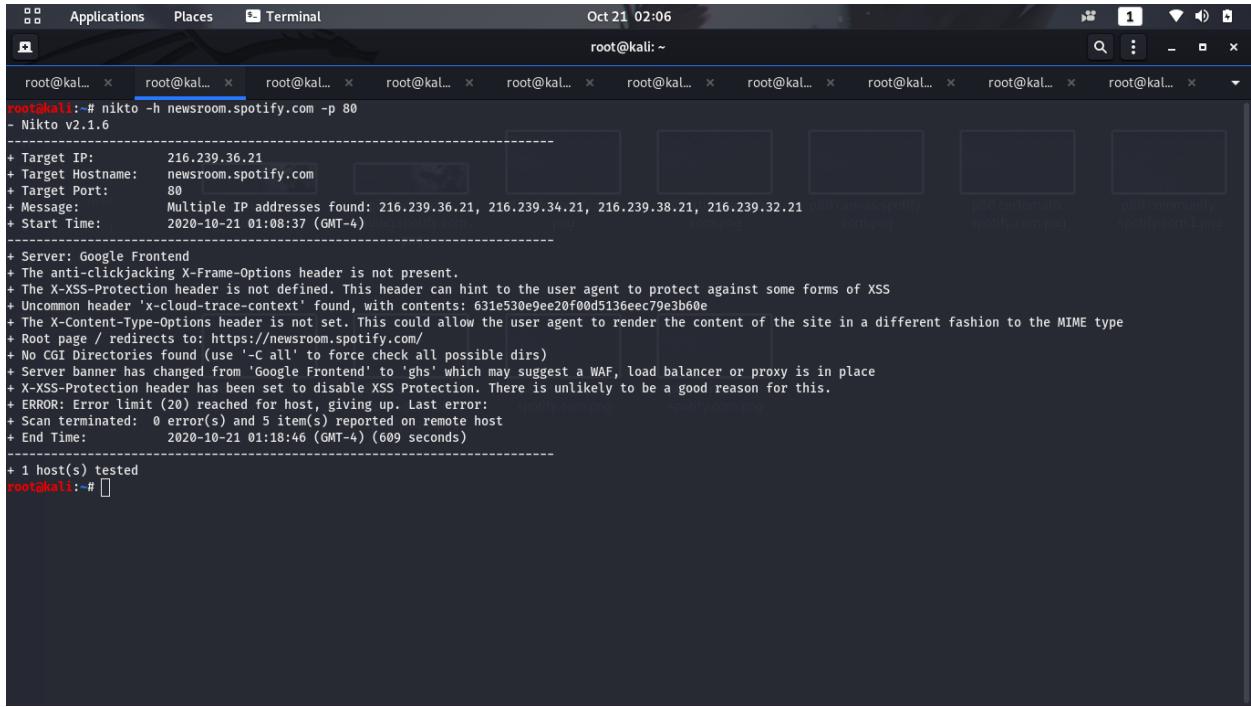
+ Target IP:      192.0.66.192
+ Target Hostname: hrblog.spotify.com
+ Target Port:    80
+ Start Time:    2020-10-21 01:08:16 (GMT-4)

+ Server: nginx
+ 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://hrblog.spotify.com/
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ 7863 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:       2020-10-21 01:24:56 (GMT-4) (1000 seconds)

+ 1 host(s) tested
root@kali:~#
```

1. Clickjacking
2. X-XSS-Protection header is not defined
3. X-Content-Type-Options header is not set

## newsroom.spotify.com

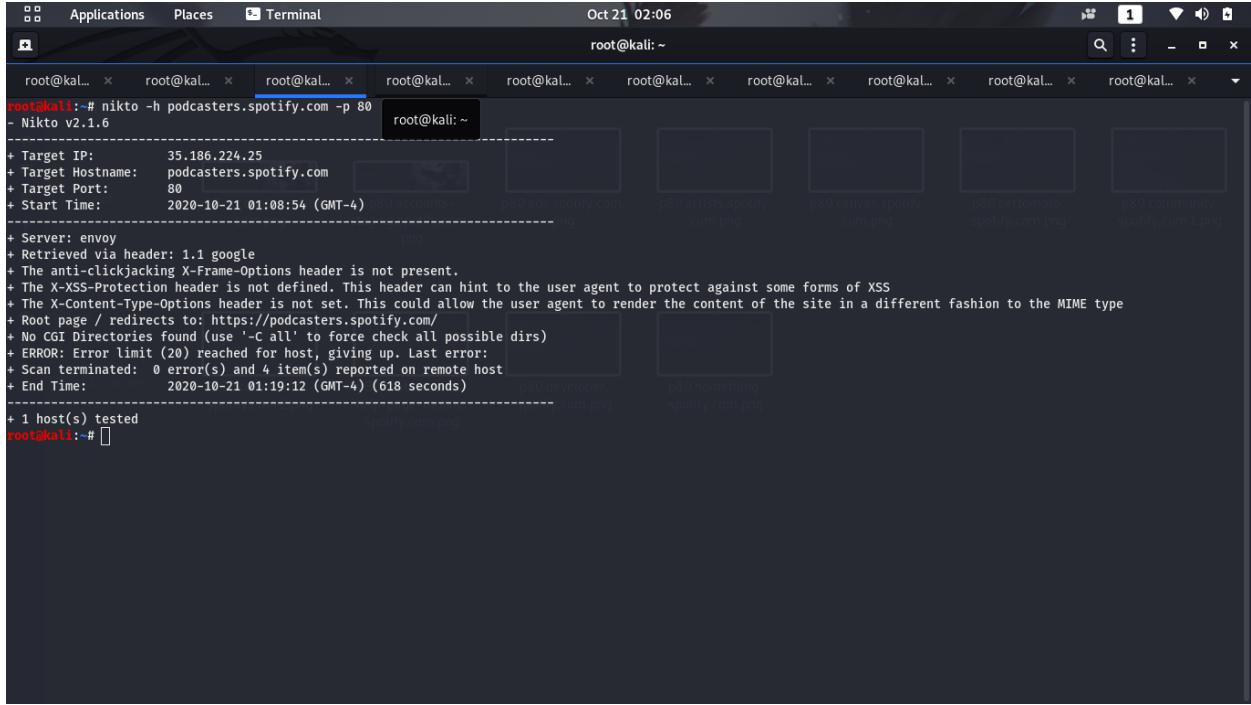


The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "Applications Places Terminal". The date and time at the top right are "Oct 21 02:06". The current directory is "root@kali: ~". The terminal window contains the output of a Nikto scan:

```
root@kali:~# nikto -h newsroom.spotify.com -p 80
- Nikto v2.1.6
-----
+ Target IP: 216.239.36.21
+ Target Hostname: newsroom.spotify.com
+ Target Port: 80
+ Message: Multiple IP addresses found: 216.239.36.21, 216.239.34.21, 216.239.38.21, 216.239.32.21
+ Start Time: 2020-10-21 01:08:37 (GMT-4)
-----  
+ Server: Google Frontend
+ 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-cloud-trace-context' found, with contents: 631e530e9ee20f00d5136eec79e3b60
+ 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://newsroom.spotify.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'Google Frontend' to 'ghs' which may suggest a WAF, load balancer or proxy is in place
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ ERROR: Error limit (20) reached for host, giving up. Last error: 2020-10-21 01:18:46 (GMT-4)
+ Scan terminated: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2020-10-21 01:18:46 (GMT-4) (609 seconds)
-----  
+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. X-Content-Type-Options header is not set**

## podcasters.spotify.com

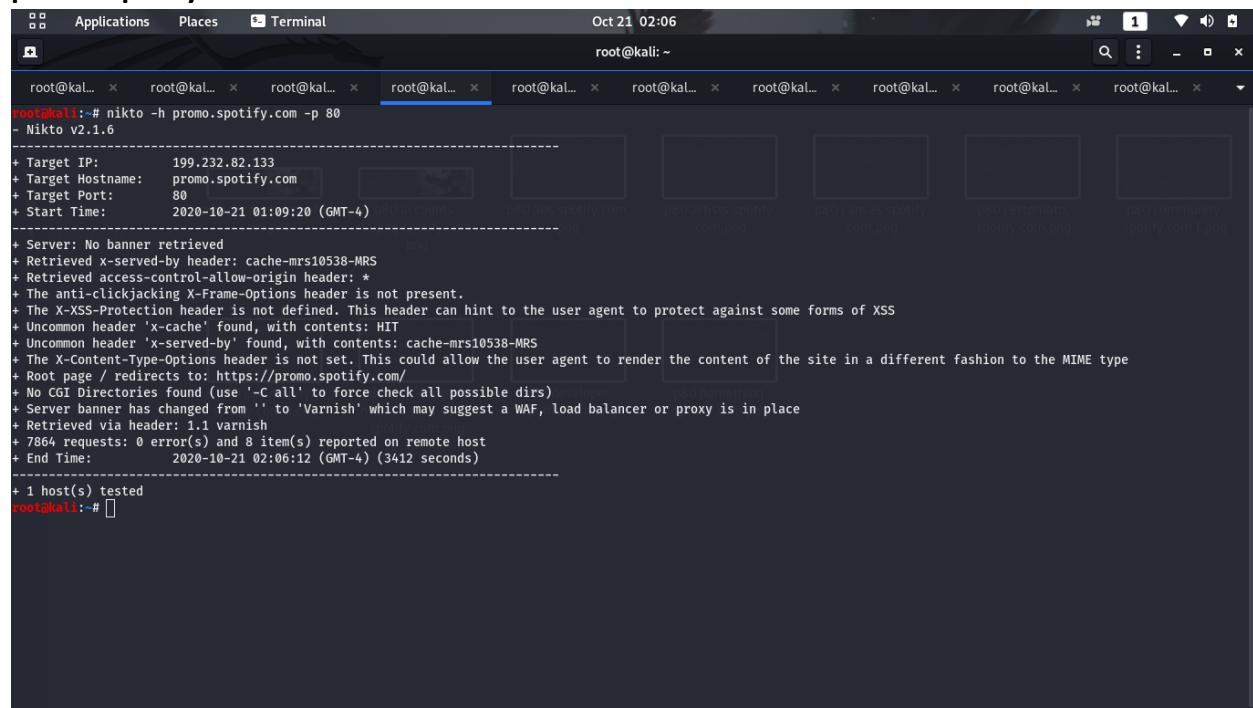


The screenshot shows a terminal window titled "Terminal" with multiple tabs open, all showing "root@kali: ~". The current tab displays the output of a Nikto scan against the host "podcasters.spotify.com" on port 80. The scan was performed on October 21, 2020, at 02:06. The output highlights several security issues:

```
root@kali:~# nikto -h podcasters.spotify.com -p 80
- Nikto v2.1.6
+ Target IP: 35.186.224.25
+ Target Hostname: podcasters.spotify.com
+ Target Port: 80
+ Start Time: 2020-10-21 01:08:54 (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://podcasters.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: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2020-10-21 01:19:12 (GMT-4) (618 seconds)
+ 1 host(s) tested
root@kali:~#
```

1. Clickjacking
2. X-XSS-Protection header is not defined
3. X-Content-Type-Options header is not set

## promo.spotify.com



The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "Applications Places Terminal". The window title is "root@kali...". The date and time at the top right are "Oct 21 02:06". The terminal content is a Nikto scan output for the host "promo.spotify.com" on port 80. The scan was started on "2020-10-21 01:09:20 (GMT-4)". The output highlights several security issues:

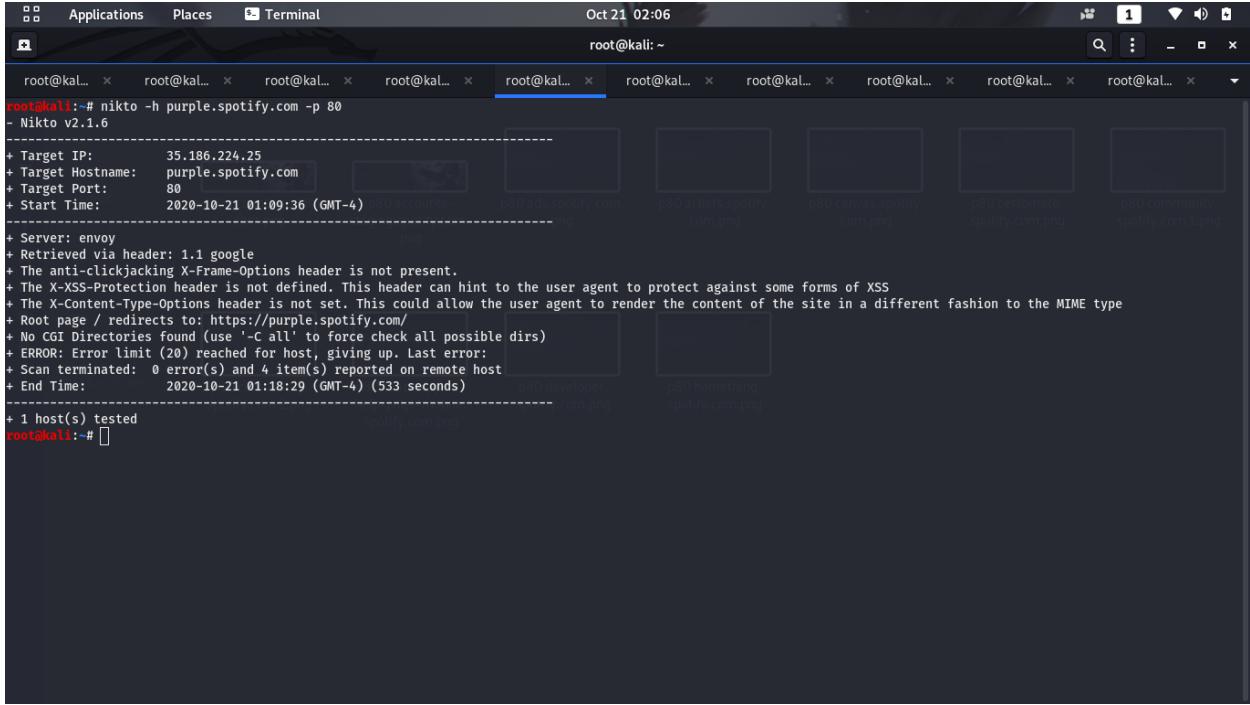
- + Target IP: 199.232.82.133
- + Target Hostname: promo.spotify.com
- + Target Port: 80
- + Start Time: 2020-10-21 01:09:20 (GMT-4)
- + Server: No banner retrieved
- + Retrieved x-served-by header: cache-mrs10538-MRS
- + Retrieved access-control-allow-origin header: \*
- + The anti-clickjacking X-Frame-Options 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-served-by' found, with contents: cache-mrs10538-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://promo.spotify.com/
- + No CGI Directories found (use '-C all' to force check all possible dirs)
- + Server banner has changed from '' to 'Varnish' which may suggest a WAF, load balancer or proxy is in place
- + Retrieved via header: 1.1 varnish
- + 7864 requests: 0 error(s) and 8 item(s) reported on remote host
- + End Time: 2020-10-21 02:06:12 (GMT-4) (3412 seconds)

+ 1 host(s) tested

root@kali:~#

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. X-Content-Type-Options header is not set**

## purple.spotify.com



The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "Terminal". The date and time "Oct 21 02:06" are at the top right. The terminal window has multiple tabs, all showing "root@kali: ~". The active tab displays the output of the Nikto web scanner. The command run was "nikto -h purple.spotify.com -p 80". The output highlights several security issues:

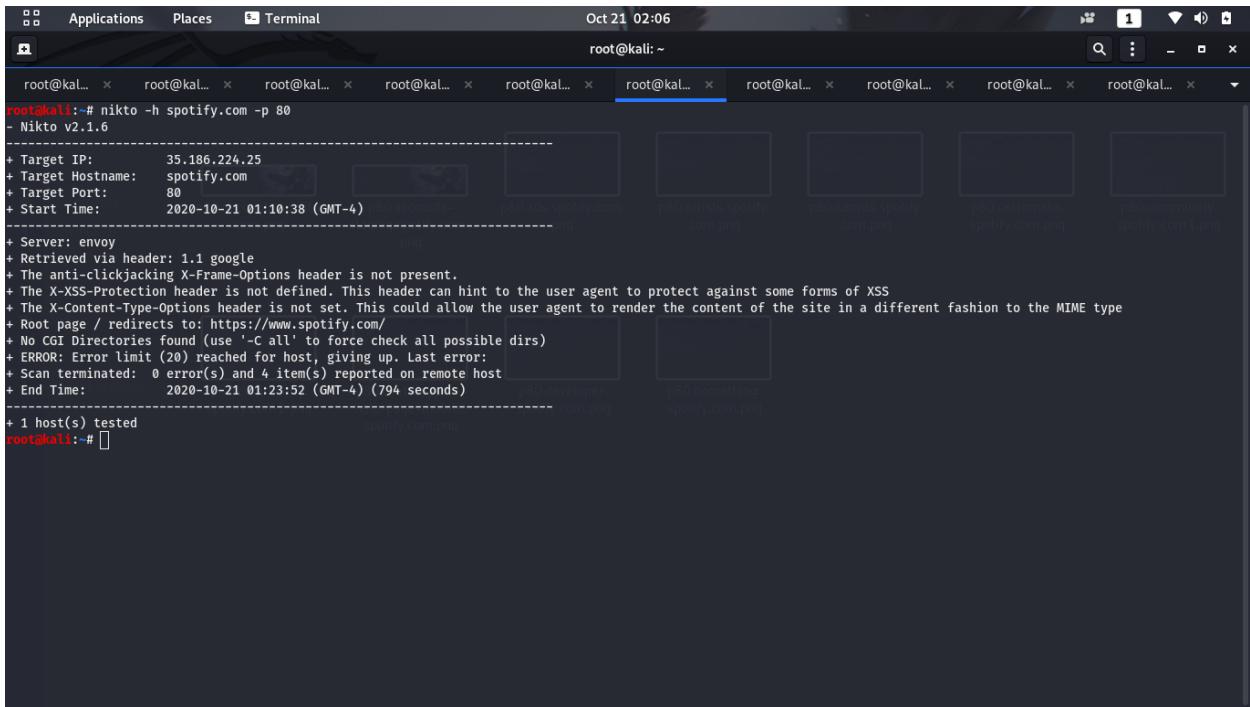
```
root@kali:~# nikto -h purple.spotify.com -p 80
- Nikto v2.1.6
[+] Target IP: 35.186.224.25
[+] Target Hostname: purple.spotify.com
[+] Target Port: 80
[+] Start Time: 2020-10-21 01:09:36 (GMT-4)
[+] End Time: 2020-10-21 01:18:29 (GMT-4) (533 seconds)

[+] 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://purple.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: 0 error(s) and 4 item(s) reported on remote host
[+] End Time: 2020-10-21 01:18:29 (GMT-4) (533 seconds)

[+] 1 host(s) tested
root@kali:~#
```

1. Clickjacking
2. X-XSS-Protection header is not defined
3. X-Content-Type-Options header is not set

## spotify.com



The screenshot shows a terminal window titled "Terminal" with the command "nikto -h spotify.com -p 80" run by root user. The output indicates several security issues:

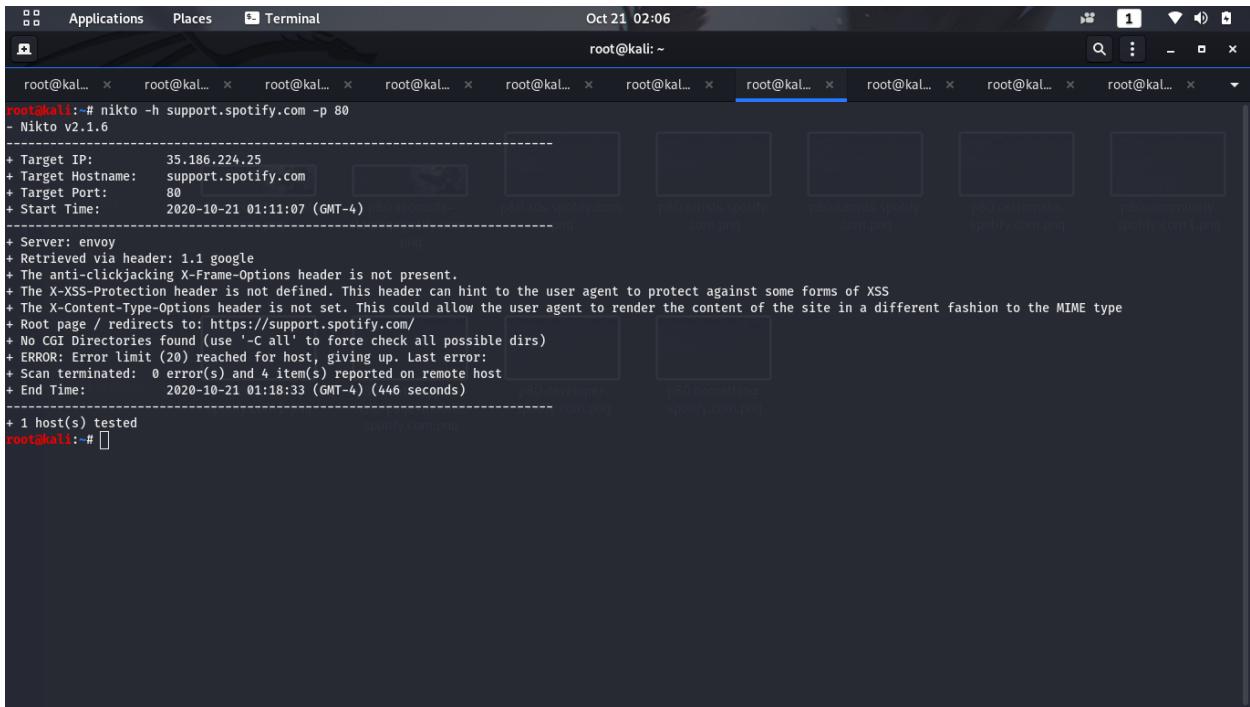
```
root@kali:~# nikto -h spotify.com -p 80
- Nikto v2.1.6
-----
+ Target IP:      35.186.224.25
+ Target Hostname: spotify.com
+ Target Port:    80
+ Start Time:    2020-10-21 01:10:38 (GMT-4)
+ Server: envoy
+ Retrieved via header: 1.1 google
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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: 0 error(s) and 4 item(s) reported on remote host
+ End Time:       2020-10-21 01:23:52 (GMT-4) (794 seconds)
-----
```

+ 1 host(s) tested

root@kali:~#

1. Clickjacking
2. X-XSS-Protection header is not defined
3. X-Content-Type-Options header is not set

## support.spotify.com



The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "Terminal". The date and time "Oct 21 02:06" are at the top right. The terminal window has multiple tabs, all showing "root@kali...". The current tab displays the output of a Nikto scan:

```
root@kali:~# nikto -h support.spotify.com -p 80
- Nikto v2.1.6

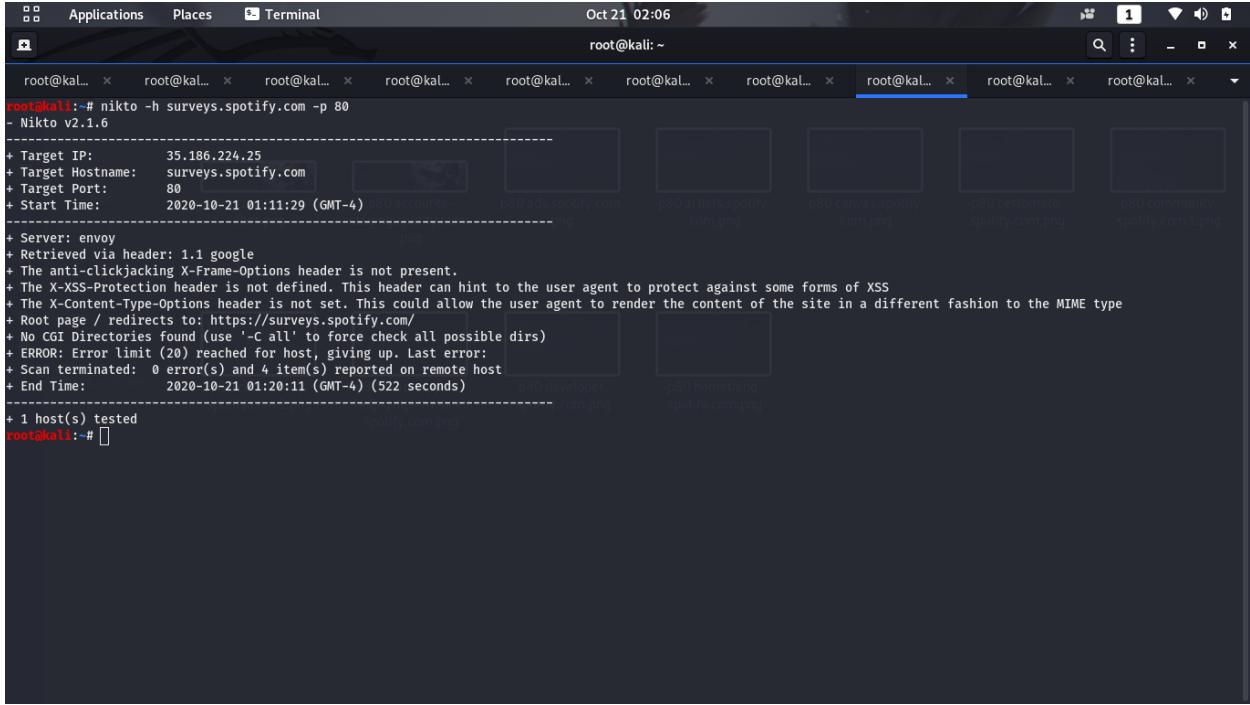
+ Target IP:      35.186.224.25
+ Target Hostname: support.spotify.com
+ Target Port:    80
+ Start Time:    2020-10-21 01:11:07 (GMT-4)

+ 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://support.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: 0 error(s) and 4 item(s) reported on remote host
+ End Time:        2020-10-21 01:18:33 (GMT-4) (446 seconds)

+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. X-Content-Type-Options header is not set**

## surveys.spotify.com



The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "Terminal". The date and time "Oct 21 02:06" are at the top right. The terminal window has multiple tabs, all labeled "root@kali...". The active tab shows the output of a Nikto scan:

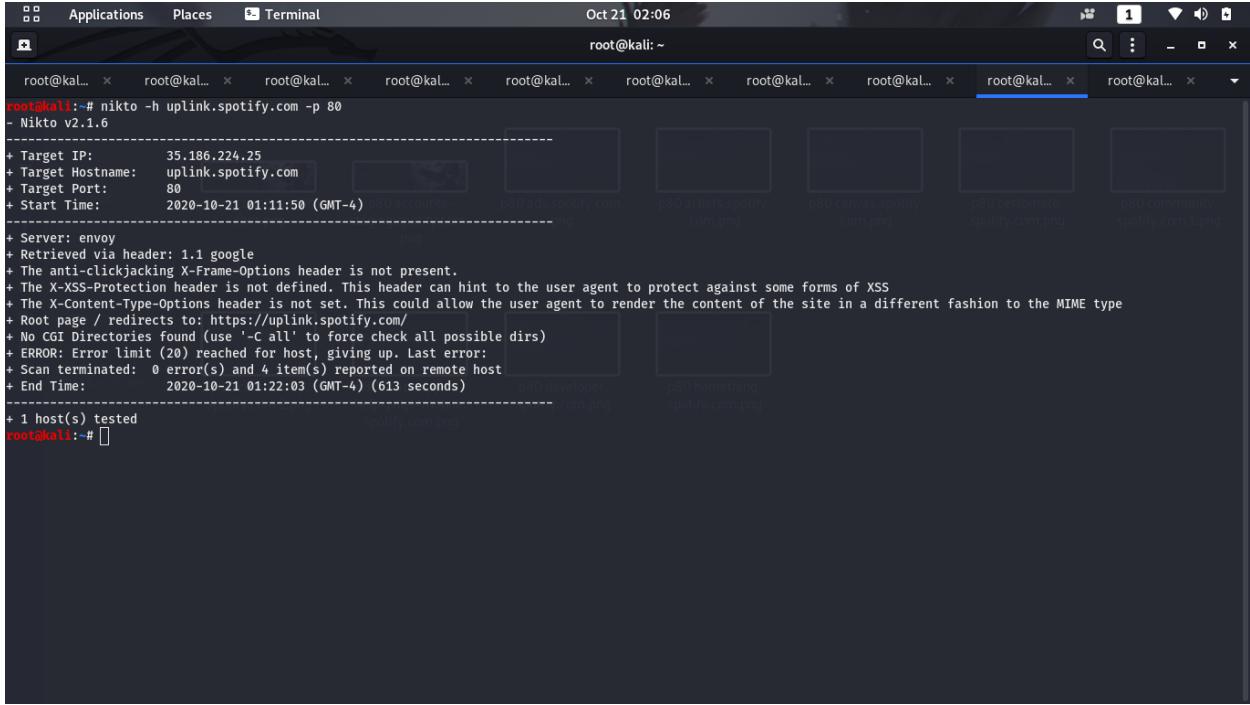
```
root@kali:~# nikto -h surveys.spotify.com -p 80
- Nikto v2.1.6
[+] Target IP: 35.186.224.25
[+] Target Hostname: surveys.spotify.com
[+] Target Port: 80
[+] Start Time: 2020-10-21 01:11:29 (GMT-4)
[+] End Time: 2020-10-21 01:20:11 (GMT-4) (522 seconds)

[+] 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://surveys.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: 0 error(s) and 4 item(s) reported on remote host
[+] End Time: 2020-10-21 01:20:11 (GMT-4) (522 seconds)

[+] 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. X-Content-Type-Options header is not set**

## uplink.spotify.com



The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "Terminal". The date and time "Oct 21 02:06" are at the top right. The terminal window has multiple tabs, all showing "root@kali...". The current tab displays the output of the Nikto web scanner. The command run was "nikto -h uplink.spotify.com -p 80". The output highlights several security issues:

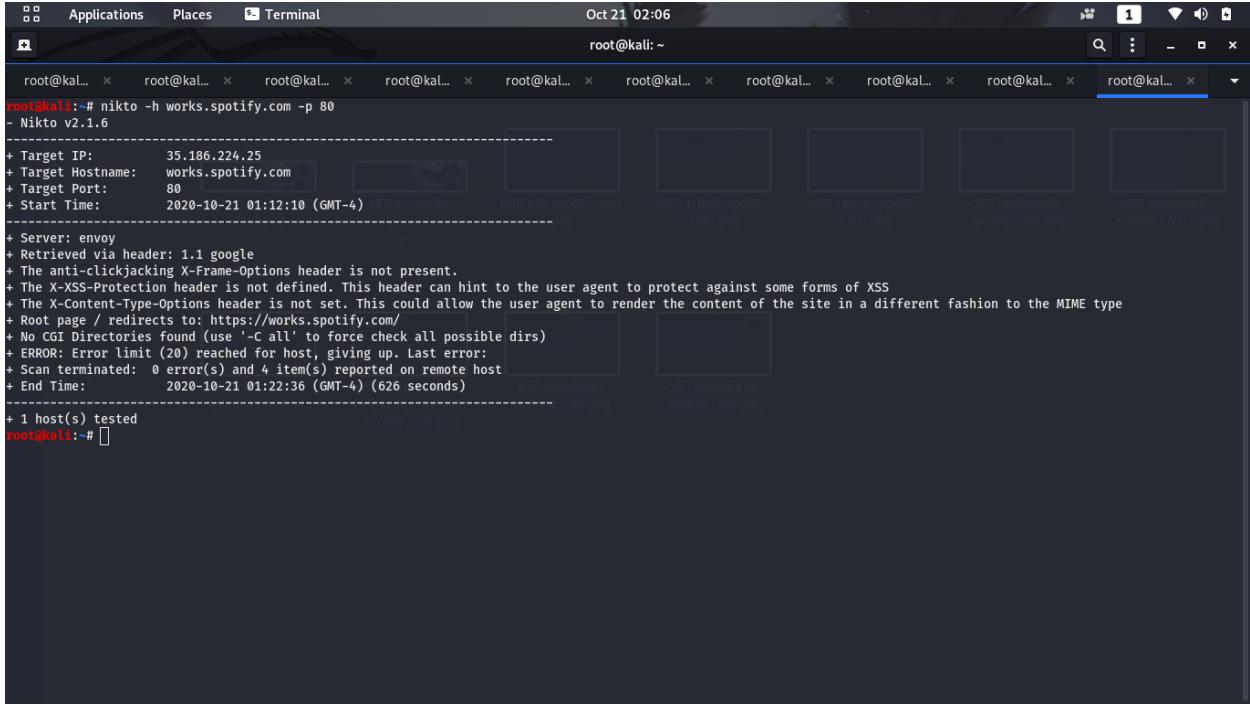
```
root@kali:~# nikto -h uplink.spotify.com -p 80
- Nikto v2.1.6
[+] Target IP: 35.186.224.25
[+] Target Hostname: uplink.spotify.com
[+] Target Port: 80
[+] Start Time: 2020-10-21 01:11:50 (GMT-4)
[+] End Time: 2020-10-21 01:22:03 (GMT-4) (613 seconds)

[+] 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://uplink.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: 0 error(s) and 4 item(s) reported on remote host
[+] End Time: 2020-10-21 01:22:03 (GMT-4) (613 seconds)

[+] 1 host(s) tested
root@kali:~# 
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. X-Content-Type-Options header is not set**

## works.spotify.com



The screenshot shows a terminal window titled "Terminal" with a dark theme. The command "nikto -h works.spotify.com -p 80" is run by root user at 02:06 on Oct 21. The output of the scan is displayed, highlighting several security issues:

```
root@kali:~# nikto -h works.spotify.com -p 80
- Nikto v2.1.6
-----
+ Target IP:      35.186.224.25
+ Target Hostname: works.spotify.com
+ Target Port:    80
+ Start Time:    2020-10-21 01:12:10 (GMT-4)
-----
```

Issues found:

- + 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://works.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: 0 error(s) and 4 item(s) reported on remote host
- + End Time: 2020-10-21 01:22:36 (GMT-4) (626 seconds)

+ 1 host(s) tested

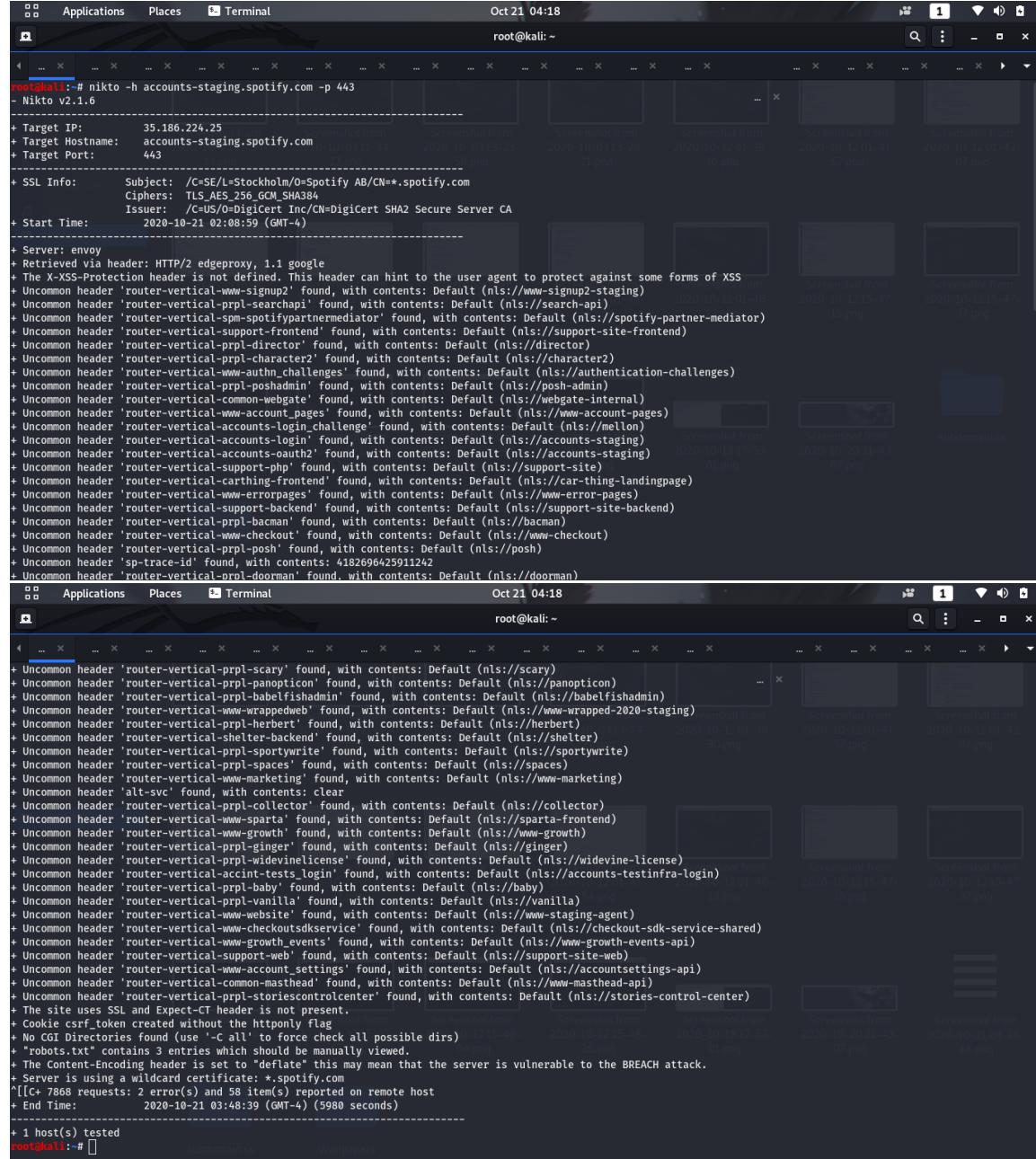
```
root@kali:~# 
```

1. Clickjacking
2. X-XSS-Protection header is not defined
3. X-Content-Type-Options header is not set

## Scan using Nikto Tool (port 443)

After scanning all subdomains for port 80, I Scanned all of them again for port 443 for further more.

**accounts-staging.spotify.com**



```

root@kali:~# nikto -h accounts-staging.spotify.com -p 443
Niko v2.1.6

+ Target IP: 35.186.224.25
+ Target Hostname: accounts-staging.spotify.com
+ Target Port: 443

+ SSL Info: Subject: /C=SE/L=Stockholm/O=Spotify AB/CN=*.spotify.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA

+ Start Time: 2020-10-21 02:08:59 (GMT-4)

+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 1.1 google
+ 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 'router-vertical-www-signin2' found, with contents: Default (nls://www-signin2-staging)
+ Uncommon header 'router-vertical-prpl-searchapi' found, with contents: Default (nls://search-api)
+ Uncommon header 'router-vertical-spmp-spotifypartnermediator' found, with contents: Default (nls://spotify-partner-mediator)
+ Uncommon header 'router-vertical-support-frontend' found, with contents: Default (nls://support-site-frontend)
+ Uncommon header 'router-vertical-prpl-director' found, with contents: Default (nls://director)
+ Uncommon header 'router-vertical-prpl-character2' found, with contents: Default (nls://character2)
+ Uncommon header 'router-vertical-www-auth-challenges' found, with contents: Default (nls://authentication-challenges)
+ Uncommon header 'router-vertical-prpl-poshadmin' found, with contents: Default (nls://posh-admin)
+ Uncommon header 'router-vertical-common-webgate' found, with contents: Default (nls://webgate-internal)
+ Uncommon header 'router-vertical-www-account_pages' found, with contents: Default (nls://www-account-pages)
+ Uncommon header 'router-vertical-accounts-login_challenge' found, with contents: Default (nls://mellon)
+ Uncommon header 'router-vertical-accounts-login' found, with contents: Default (nls://accounts-staging)
+ Uncommon header 'router-vertical-accounts-oauth2' found, with contents: Default (nls://accounts-staging)
+ Uncommon header 'router-vertical-support-php' found, with contents: Default (nls://support-site)
+ Uncommon header 'router-vertical-carthring-frontend' found, with contents: Default (nls://car-thing-landingpage)
+ Uncommon header 'router-vertical-www-errorpages' found, with contents: Default (nls://www-error-pages)
+ Uncommon header 'router-vertical-support-backend' found, with contents: Default (nls://support-site-backend)
+ Uncommon header 'router-vertical-prpl-bacman' found, with contents: Default (nls://bacman)
+ Uncommon header 'router-vertical-www-checkout' found, with contents: Default (nls://www-checkout)
+ Uncommon header 'router-vertical-prpl-posh' found, with contents: Default (nls://posh)
+ Uncommon header 'sp-trace-id' found, with contents: 4182696425911242
+ Uncommon header 'router-vertical-prpl-doorman' found, with contents: Default (nls://doorman)

root@kali:~# nikto -h accounts-staging.spotify.com -p 443
Niko v2.1.6

+ Uncommon header 'router-vertical-prpl-scarfy' found, with contents: Default (nls://scary)
+ Uncommon header 'router-vertical-prpl-panopticon' found, with contents: Default (nls://panopticon)
+ Uncommon header 'router-vertical-prpl-babelfishadmin' found, with contents: Default (nls://babelfishadmin)
+ Uncommon header 'router-vertical-www-wrappedweb' found, with contents: Default (nls://www-wrapped-2020-staging)
+ Uncommon header 'router-vertical-prpl-herbert' found, with contents: Default (nls://herbert)
+ Uncommon header 'router-vertical-shelter-backend' found, with contents: Default (nls://shelter)
+ Uncommon header 'router-vertical-prpl-sportywrite' found, with contents: Default (nls://sportywrite)
+ Uncommon header 'router-vertical-prpl-spaces' found, with contents: Default (nls://spaces)
+ Uncommon header 'router-vertical-www-marketing' found, with contents: Default (nls://www-marketing)
+ Uncommon header 'alt-svc' found, with contents: clear
+ Uncommon header 'router-vertical-prpl-collector' found, with contents: Default (nls://collector)
+ Uncommon header 'router-vertical-www-sparta' found, with contents: Default (nls://sparta-frontend)
+ Uncommon header 'router-vertical-www-growth' found, with contents: Default (nls://www-growth)
+ Uncommon header 'router-vertical-prpl-ginger' found, with contents: Default (nls://ginger)
+ Uncommon header 'router-vertical-prpl-widevinelicense' found, with contents: Default (nls://widevine-license)
+ Uncommon header 'router-vertical-acc-tests_login' found, with contents: Default (nls://accounts-testinfra-login)
+ Uncommon header 'router-vertical-prpl-baby' found, with contents: Default (nls://baby)
+ Uncommon header 'router-vertical-prpl-vanilla' found, with contents: Default (nls://vanilla)
+ Uncommon header 'router-vertical-www-website' found, with contents: Default (nls://www-staging-agent)
+ Uncommon header 'router-vertical-www-checkoutsdkservice' found, with contents: Default (nls://checkout-sdk-service-shared)
+ Uncommon header 'router-vertical-www-growth_events' found, with contents: Default (nls://www-growth-events-api)
+ Uncommon header 'router-vertical-support-web' found, with contents: Default (nls://support-site-web)
+ Uncommon header 'router-vertical-www-account_settings' found, with contents: Default (nls://accountsettings-api)
+ Uncommon header 'router-vertical-common-masthead' found, with contents: Default (nls://www-masthead-api)
+ Uncommon header 'router-vertical-prpl-storiescontrolcenter' found, with contents: Default (nls://stories-control-center)
+ The site uses SSL and Expect-CT header is not present.
+ Cookie csrf_token created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 3 entries which should be manually viewed.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server is using a wildcard certificate: *.spotify.com
'[C+ 7868 requests: 2 error(s) and 58 item(s) reported on remote host
+ End Time: 2020-10-21 03:48:39 (GMT-4) (5980 seconds)

+ 1 host(s) tested
root@kali:~#

```

1. X-XSS-Protection header is not defined
2. Server is using Wildcard Certification

**accounts.spotify.com**

```
root@kali:~# nikto -h accounts.spotify.com -p 443
- Nikto V2.1.6

+ Target IP:      35.186.224.25
+ Target Hostname: accounts.spotify.com
+ Target Port:    443

+ SSL Info:       Subject: /C=SE/L=Stockholm/O=Spotify AB/CN=*.spotify.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time:    2020-10-21 02:09:38 (GMT-4)

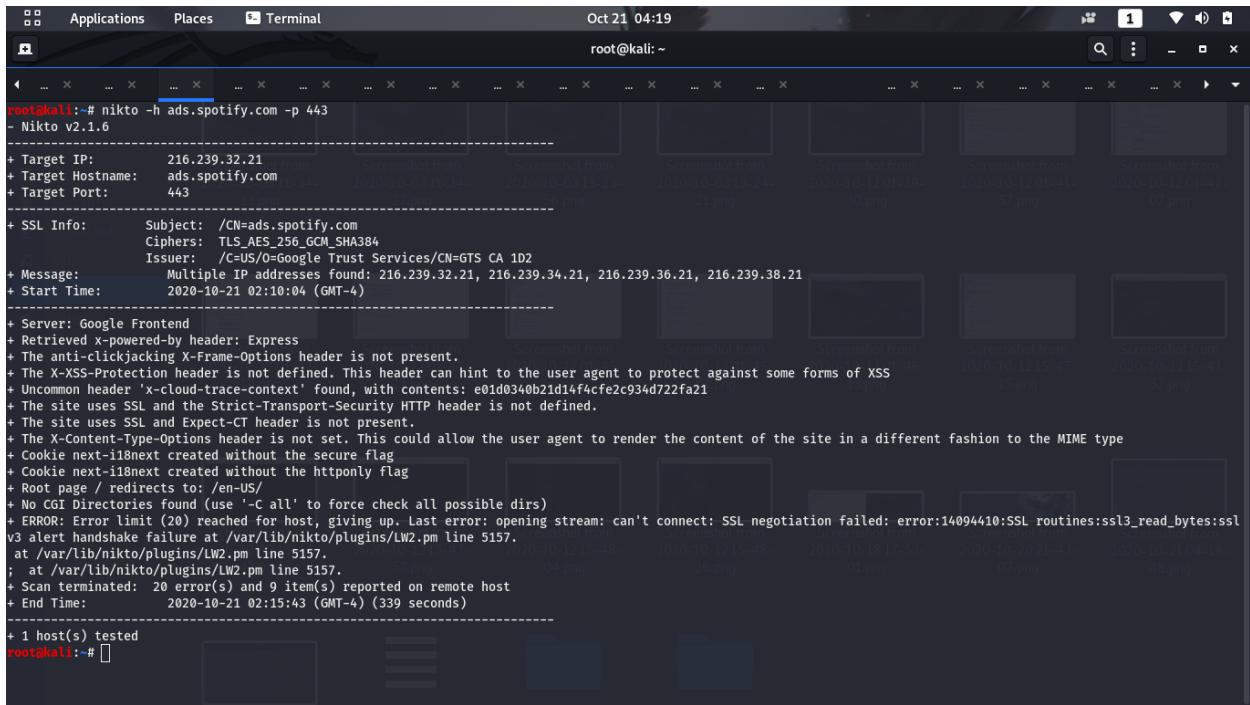
+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 1.1 google
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'alt-svc' found, with contents: clear
+ Uncommon header 'sp-trace-id' found, with contents: 853e7a9eac101751
+ The site uses SSL and Expect-CT header is not present.
+ Cookie csrf_token created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 3 entries which should be manually viewed.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server is using a wildcard certificate: *.spotify.com
+ 7868 requests: 2 error(s) and 9 item(s) reported on remote host
+ End Time:      2020-10-21 03:43:58 (GMT-4) (5660 seconds)

+ 1 host(s) tested
root@kali:~#
```

**1. X-XSS-Protection header is not defined**

**2. Server is using Wildcard Certification**

## ads.spotify.com



The screenshot shows a terminal window titled "Terminal" with the command "nikto -h ads.spotify.com -p 443" run by root user at 04:19 on Oct 21. The output of the scan is displayed, highlighting several security issues:

```
root@kali:~# nikto -h ads.spotify.com -p 443
- Nikto v2.1.6

+ Target IP: 216.239.32.21
+ Target Hostname: ads.spotify.com
+ Target Port: 443
+ SSL Info: Subject: /CN=ads.spotify.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=US/O=Google Trust Services/CN=GTS CA 1D2
+ Message: Multiple IP addresses found: 216.239.32.21, 216.239.34.21, 216.239.36.21, 216.239.38.21
+ Start Time: 2020-10-21 02:10:04 (GMT-4)

+ Server: Google Frontend
+ Retrieved x-powered-by header: Express
+ 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-cloud-trace-context' found, with contents: e01d0340b21d14fcfe2c934d722fa21
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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
+ Cookie next-i18next created without the secure flag
+ Cookie next-i18next created without the httponly flag
+ Root page / redirects to: /en-US/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:ssl
v3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated: 20 error(s) and 9 item(s) reported on remote host
+ End Time: 2020-10-21 02:15:43 (GMT-4) (339 seconds)

+ 1 host(s) tested
root@kali:~#
```

1. **Clickjacking**
2. **X-XSS-Protection header is not defined**
3. **X-Content-Type-Options header is not set**

## artists.spotify.com

```
root@kali:~# nikto -h artists.spotify.com -p 443
- Nikto v2.1.6

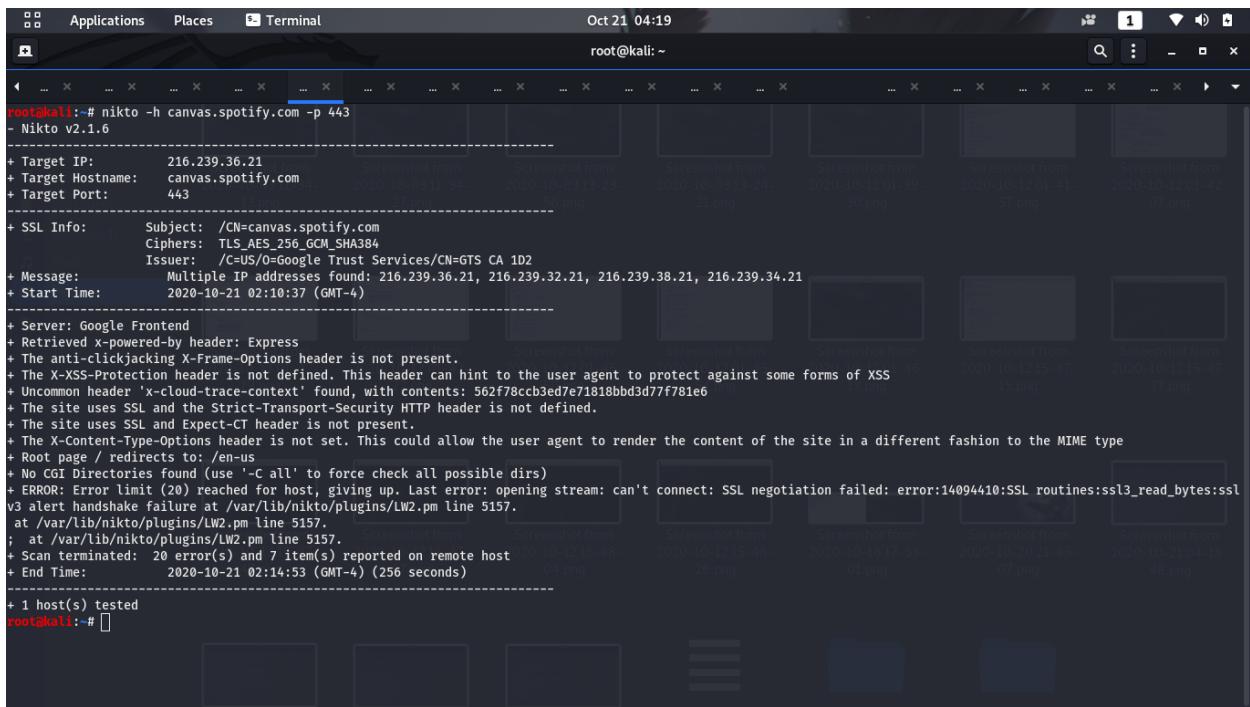
+ Target IP:      35.186.224.25
+ Target Hostname: artists.spotify.com
+ Target Port:    443
+ SSL Info:       Subject: /C=SE/L=Stockholm/O=Spotify AB/CN=*.spotify.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time:     2020-10-21 02:10:22 (GMT-4)

+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 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
+ Uncommon header 'alt-svc' found, with contents: clear
+ The site uses SSL and Expect-CT header is not present.
+ Uncommon header 'refresh' found, with contents: 0;url=/TEAAWL72
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ Entry '/c/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server is using a wildcard certificate: *.spotify.com
+ 7864 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:       2020-10-21 03:32:00 (GMT-4) (4898 seconds)

+ 1 host(s) tested
root@kali:~#
```

1. **Clickjacking**
2. **X-XSS-Protection header is not defined**
3. **Server is using Wildcard Certification**

## canvas.spotify.com



```
root@kali:~# nikto -h canvas.spotify.com -p 443
- Nikto v2.1.6

+ Target IP: 216.239.36.21
+ Target Hostname: canvas.spotify.com
+ Target Port: 443
+ SSL Info: Subject: /CN=canvas.spotify.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=Google Trust Services/CN=GTS CA 1D2
+ Message: Multiple IP addresses found: 216.239.36.21, 216.239.32.21, 216.239.38.21, 216.239.34.21
+ Start Time: 2020-10-21 02:10:37 (GMT-4)

+ Server: Google Frontend
+ Retrieved x-powered-by header: Express
+ 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-cloud-trace-context' found, with contents: 562f78ccbb3ed7e71818bbd3d77f781e6
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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: /en-us
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:ssl
v3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5157.
: at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated: 20 error(s) and 7 item(s) reported on remote host
+ End Time: 2020-10-21 02:14:53 (GMT-4) (256 seconds)

+ 1 host(s) tested
root@kali:~#
```

1. **Clickjacking**
2. **X-XSS-Protection header is not defined**
3. **X-Content-Type-Options header is not set**

## certomato.spotify.com

```
root@kali:~# nikto -h certomato.spotify.com -p 443
- Nikto v2.1.6

+ Target IP: 35.186.224.25
+ Target Hostname: certomato.spotify.com
+ Target Port: 443
+ SSL Info: Subject: /C=SE/L=Stockholm/O=Spotify AB/CN=*.spotify.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time: 2020-10-21 02:10:55 (GMT-4)

+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 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
+ Uncommon header 'alt-svc' found, with contents: clear
+ The site uses SSL and Expect-CT header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /certomatospotify.pem: Potentially interesting archive/cert file found.
+ /certomatospotify.com.tar.bz2: Potentially interesting archive/cert file found.
+ /certomato.spotify.com.tar: Potentially interesting archive/cert file found.
+ /site.alz: Potentially interesting archive/cert file found.
+ /certomato.cer: Potentially interesting archive/cert file found.
+ /backup.tar.lzma: Potentially interesting archive/cert file found.
+ /certomato.spotify.tar: Potentially interesting archive/cert file found.
+ /backup.jks: Potentially interesting archive/cert file found.
+ /certomato.tar: Potentially interesting archive/cert file found.
+ /com.tgz: Potentially interesting archive/cert file found.
+ /backup.war: Potentially interesting archive/cert file found.
+ /site.tar: Potentially interesting archive/cert file found.
+ /spotify.war: Potentially interesting archive/cert file found.
+ /certomatospotify.cer: Potentially interesting archive/cert file found.
+ /35.186.224.25.egg: Potentially interesting archive/cert file found.
+ /com.jks: Potentially interesting archive/cert file found.
+ /com.pem: Potentially interesting archive/cert file found.
+ /certomatospotifyvcom.iks: Potentially interesting archive/cert file found.

root@kali:~# nikto -h certomato.spotify.com -p 443
- Nikto v2.1.6

+ /certomatospotifycom.war: Potentially interesting archive/cert file found.
+ /35.186.224.25.tgz: Potentially interesting archive/cert file found.
+ /certomato.tgz: Potentially interesting archive/cert file found.
+ /certomato_spotify_com.tar.lzma: Potentially interesting archive/cert file found.
+ /spotify.tar.lzma: Potentially interesting archive/cert file found.
+ /certomato.spotify.com.tar: Potentially interesting archive/cert file found.
+ /35.186.224.25.jks: Potentially interesting archive/cert file found.
+ /35.186.224.25.alz: Potentially interesting archive/cert file found.
+ /com.alz: Potentially interesting archive/cert file found.
+ /certomato.spotify.com.cer: Potentially interesting archive/cert file found.
+ /com.cer: Potentially interesting archive/cert file found.
+ /site.war: Potentially interesting archive/cert file found.
+ /certomatospotify.war: Potentially interesting archive/cert file found.
+ /35.186.224.25.cer: Potentially interesting archive/cert file found.
+ /certomatospotify.tar: Potentially interesting archive/cert file found.
+ /certomato.pem: Potentially interesting archive/cert file found.
+ /spotify.pem: Potentially interesting archive/cert file found.
+ /35.186.224.25.tar.bz2: Potentially interesting archive/cert file found.
+ /certomato_spotify_com.egg: Potentially interesting archive/cert file found.
+ /certomatospotifycom.tar: Potentially interesting archive/cert file found.
+ /certomato_spotify_com.tar: Potentially interesting archive/cert file found.
+ /site.pem: Potentially interesting archive/cert file found.
+ /certomato.spotify.com.tar.lzma: Potentially interesting archive/cert file found.
+ /certomato_spotify_com.alz: Potentially interesting archive/cert file found.
+ /spotify.alz: Potentially interesting archive/cert file found.
+ /certomato.spotify.tar.bz2: Potentially interesting archive/cert file found.
+ /certomato.war: Potentially interesting archive/cert file found.
+ /certomato.jks: Potentially interesting archive/cert file found.
+ /site.cer: Potentially interesting archive/cert file found.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server is using a wildcard certificate: *.spotify.com
+ 7868 requests: 0 error(s) and 117 item(s) reported on remote host
+ End Time: 2020-10-21 03:29:33 (GMT-4) (4718 seconds)

+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. Server is using Wildcard Certification**

## community.spotify.com

```
root@kali:~# nikto -h community.spotify.com -p 443
- Nikto v2.1.6

+ Target IP: 13.225.255.114
+ Target Hostname: community.spotify.com
+ Target Port: 443
+ SSL Info: Subject: /C=US/ST=California/L=San Francisco/O=Khoros, LLC/CN=secure02.lithium.com
  Ciphers: TLS_AES_128_GCM_SHA256
  Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=digiCert SHA2 High Assurance Server CA
+ Message: Multiple IP addresses found: 13.225.255.114, 13.225.255.35, 13.225.255.101, 13.225.255.51
+ Start Time: 2020-10-21 02:12:32 (GMT-4)

+ Server: Apache
+ Retrieved via header: 1.1 9db58be50dbaa99adeb6f9e43f285e7.cloudfront.net (CloudFront)
+ 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-amz-cf-pop' found, with contents: TLV50-C1
+ Uncommon header 'x-amz-cf-id' found, with contents: 01hrQCeWU1vzEfcB6w_82Lz43AcNsWsb3COMdNIxODJwpCzVkjQ==
+ Uncommon header 'x-cache' found, with contents: Miss from cloudfront
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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
+ Cookie AWSALB created without the secure flag
+ Cookie AWSALB created without the httponly flag
+ Cookie AWSALBCORS created without the httponly flag
+ Cookie LithiumUserInfo created without the secure flag
+ Cookie LithiumUserInfo created without the httponly flag
+ Cookie LithiumUserSecure created without the httponly flag
+ Cookie LithiumVisitor created without the secure flag
+ Cookie LithiumCookiesAccepted created without the secure flag
+ Cookie LithiumCookiesAccepted created without the httponly flag
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ Entry '/t5/media/gallerypage/*all/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/help/faapage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/forums/useronlinepage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/forums/recentpostspage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/util/componentrenderpage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
Oct 21 04:19
root@kali:~# nikto -h community.spotify.com -p 443
- Nikto v2.1.6

+ Cookie LithiumCookiesAccepted created without the httponly flag
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ Entry '/t5/media/gallerypage/*all/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/help/faapage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/forums/useronlinepage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/forums/recentpostspage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/util/componentrenderpage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/forums/postpage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/notes/composepage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/notes/privateotespage/tabc/compose/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/t5/notes/v1_1/privateotespage/tabc/compose/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/auth/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/plugins/common/feature/oauth/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/plugins/common/feature/oauth2sso/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/plugins/common/feature/saml/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/plugins/common/feature/openidconnectsso/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/plugins/common/feature/openidss/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/t5/help/faapage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/forums/searchpage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/forums/tagleaderboardpage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/forums/kudosleaderboardpage/' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/t5/forums/useronlinepage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/forums/recentpostspage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/forums/searchpage/tabc/tkb#/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/util/componentrenderpage/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/t5/custom/page/page-id/Threeplwood#/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ "robots.txt" contains 62 entries which should be manually viewed.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:1408F10B:SSL routines:ssl3_get_record:wrong version number at /var/lib/nikto/plugins/LW2.pm line 5157.
at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated: 20 error(s) and 42 item(s) reported on remote host
+ End Time: 2020-10-21 02:24:04 (GMT-4) (692 seconds)

+ 1 host(s) tested
root@kali:~#
```

1. X-XSS-Protection header is not defined
2. X-Content-Type-Options header is not set

## csat-support-help-page-mobile.spotify.com

```
root@kali:~# nikto -h csat-support-help-page-mobile.spotify.com -p 443
- Nikto v2.1.6

+ Target IP:      35.186.224.25
+ Target Hostname: csat-support-help-page-mobile.spotify.com
+ Target Port:    443
+ SSL Info:       Subject: /C=SE/I=Stockholm/O=Spotify AB/CN=*.spotify.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time:     2020-10-21 02:13:11 (GMT-4)

+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 1.1 google
+ Retrieved x-powered-by header: Next.js
+ 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 'alt-svc' found, with contents: clear
+ The site uses SSL and Expect-CT header is not present.
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server is using a wildcard certificate: *.spotify.com
+ 7863 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:       2020-10-21 03:32:01 (GMT-4) (4730 seconds)

+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. Server is using Wildcard Certification**

## developer.spotify.com

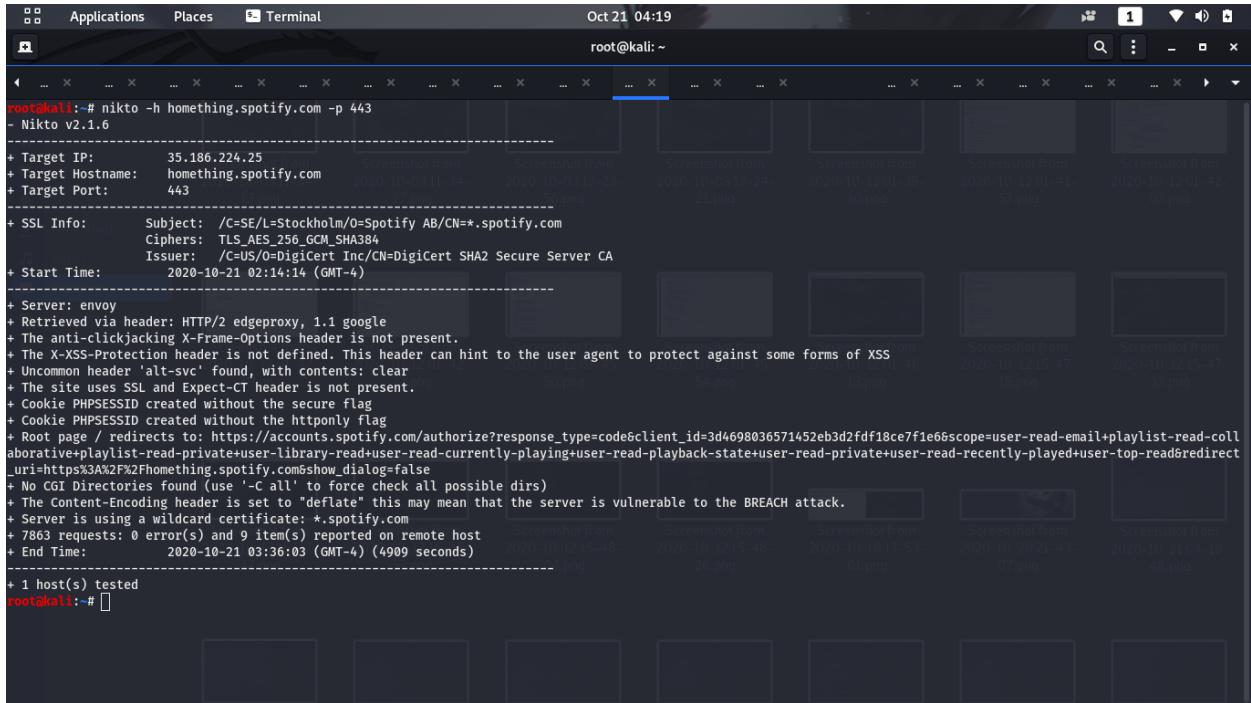
```
root@kali:~# nikto -h developer.spotify.com -p 443
- Nikto v2.1.6

+ Target IP:      151.101.2.133
+ Target Hostname: developer.spotify.com
+ Target Port:    443
+ SSL Info:       Subject: /C=SE/L=Stockholm/O=Spotify AB/CN=developer.spotify.com
                  Ciphers: ECDHE-RSA-AES128-GCM-SHA256
                  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Message:        Multiple IP addresses found: 151.101.2.133, 151.101.66.133, 151.101.130.133, 151.101.194.133
+ Start Time:     2020-10-21 02:13:58 (GMT-4)

+ Server: No banner retrieved
+ Retrieved x-served-by header: cache-ord1727-ORD, cache-mrs10533-MRS
+ Retrieved access-control-allow-origin header: *
+ 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, HIT
+ Uncommon header 'x-amz-meta-goog-reserved-file-mtime' found, with contents: 1597742701
+ Uncommon header 'x-served-by' found, with contents: cache-ord1727-ORD, cache-mrs10533-MRS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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)
+ Entry '/assets/branding-guidelines/color-rules-32x2x-1.png' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/assets/branding-guidelines/color-rules-48x2x-1.png' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 3 entries which should be manually viewed.
+ Server banner has changed from '' to 'Varnish' which may suggest a WAF, load balancer or proxy is in place
+ Retrieved via header: 1.1 varnish
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ OSVDB-3092: /support/: This might be interesting...
+ /console/: Application console found
```

1. Clickjacking
2. X-XSS-Protection header is not defined

## homething.spotify.com



```
root@kali:~# nikto -h homething.spotify.com -p 443
- Nikto v2.1.6

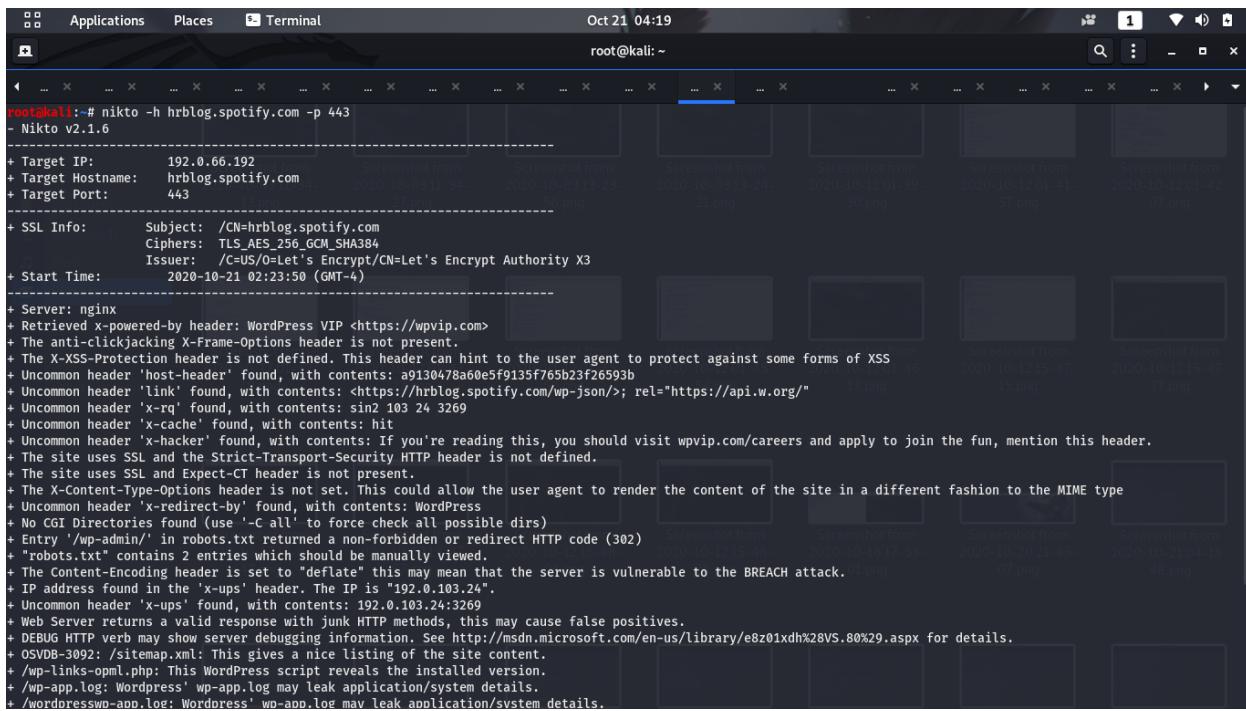
+ Target IP:      35.186.224.25
+ Target Hostname: homething.spotify.com
+ Target Port:    443
+ SSL Info:       Subject: /C=SE/I=Stockholm/O=Spotify AB/CN=*.spotify.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time:    2020-10-21 02:14:14 (GMT-4)

+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 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
+ Uncommon header 'alt-svc' found, with contents: clear
+ The site uses SSL and Expect-CT header is not present.
+ Cookie PHPSESSID created without the httponly flag
+ Cookie PHPSESSID created without the httponly flag
+ Root page / redirects to: https://accounts.spotify.com/authorize?response_type=code&client_id=3d4698036571452eb3dfdf18ce7f1e6&scope=user-read-email+playlist-read-collaborative+playlist-read-private+user-library-read+user-read-currently-playing+user-read-playback-state+user-read-private+user-read-recently-played+user-top-read&redirect_uri=https%3A%2F%2Fhomething.spotify.com&show_dialog=false
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server is using a wildcard certificate: *.spotify.com
+ 7863 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:      2020-10-21 03:36:03 (GMT-4) (4909 seconds)

+ 1 host(s) tested
root@kali:~#
```

1. **Clickjacking**
2. **X-XSS-Protection header is not defined**
3. **Server is using Wildcard Certification**
4. **cookie PHPSESSID created without the httponly flag**

## hrblog.spotify.com



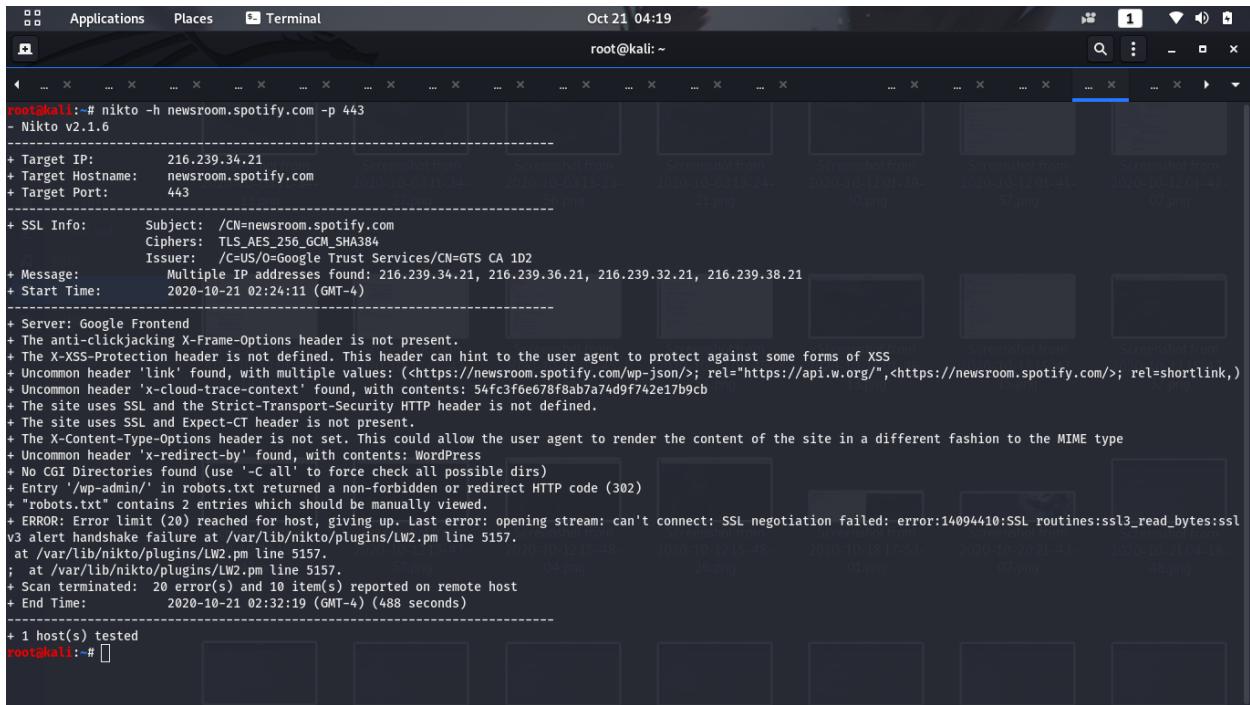
```
root@kali:~# nikto -h hrblog.spotify.com -p 443
- Nikto v2.1.6

+ Target IP:      192.0.66.192
+ Target Hostname: hrblog.spotify.com
+ Target Port:    443
+ SSL Info:       Subject: /CN=hrblog.spotify.com
                  Ciphers:  TLS_AES_256_GCM_SHA384
                  Issuer:  /C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
+ Start Time:    2020-10-21 02:23:50 (GMT-4)

+ Server: nginx
+ Retrieved x-powered-by header: WordPress VIP <https://wpvip.com>
+ 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 'host-header' found, with contents: a9130478a60e5f9135f765b23f26593b
+ Uncommon header 'link' found, with contents: <https://hrblog.spotify.com/wp-json/>; rel="https://api.w.org/"
+ Uncommon header 'x-rq' found, with contents: sin2 103 24 3269
+ Uncommon header 'x-cache' found, with contents: hit
+ Uncommon header 'x-hacker' found, with contents: If you're reading this, you should visit wpvip.com/careers and apply to join the fun, mention this header.
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ Entry '/wp-admin/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack. (1.png)
+ IP address found in the 'x-ups' header. The IP is "192.0.103.24".
+ Uncommon header 'x-ups' found, with contents: 192.0.103.24:3269
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-3092: /sitemap.xml: This gives a nice listing of the site content.
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /wp-app.log: Wordpress' wp-app.log may leak application/system details.
+ /wordpresswp-app.log: Wordpress' wp-app.log may leak application/system details.
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. X-Content-Type-Options header is not set**

## newsroom.spotify.com



The screenshot shows a terminal window titled "Terminal" running on a Kali Linux system. The command "nikto -h newsroom.spotify.com -p 443" is being executed. The output of the scan is displayed, highlighting several security issues:

```
root@kali:~# nikto -h newsroom.spotify.com -p 443
- Nikto v2.1.6

+ Target IP: 216.239.34.21
+ Target Hostname: newsroom.spotify.com
+ Target Port: 443
+ SSL Info: Subject: /CN=newsroom.spotify.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=US/O=Google Trust Services/CN=GTS CA 1D2
+ Message: Multiple IP addresses found: 216.239.34.21, 216.239.36.21, 216.239.32.21, 216.239.38.21
+ Start Time: 2020-10-21 02:24:11 (GMT-4)

+ Server: Google Frontend
+ 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 'link' found, with multiple values: (<https://newsroom.spotify.com/wp-json/>; rel="https://api.w.org/",<https://newsroom.spotify.com/>; rel=shortlink,) 
+ Uncommon header 'x-cloud-trace-context' found, with contents: 54fc3f6e678f8ab7a74d9f742e17b9cb
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and the Expect-CT header is not present.
+ 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
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ Entry '/wp-admin/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ "robots.txt" contains 2 entries which should be manually viewed.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:ssl
v3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5157.
at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated: 20 error(s) and 10 item(s) reported on remote host
+ End Time: 2020-10-21 02:32:19 (GMT-4) (488 seconds)

+ 1 host(s) tested
root@kali:~#
```

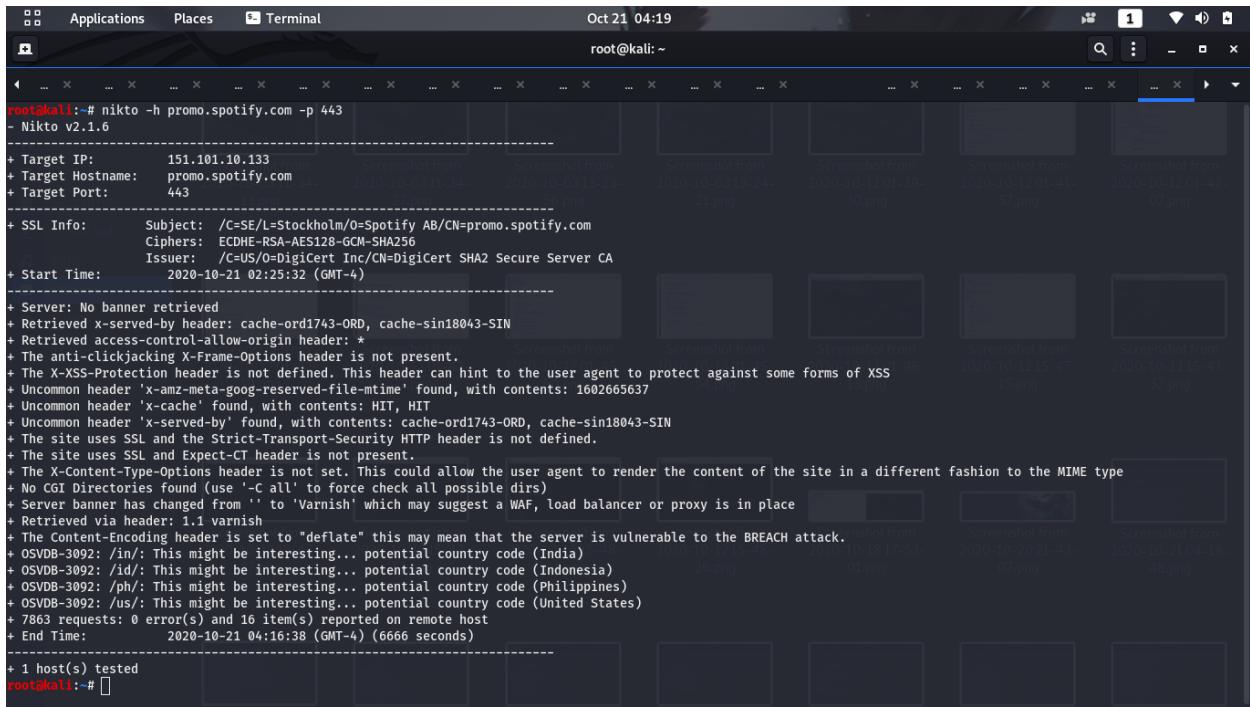
- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. X-Content-Type-Options header is not set**

## podcasters.spotify.com

```
Nikto v2.1.6
-----
+ Target IP:      35.186.224.25
+ Target Hostname: podcasters.spotify.com
+ Target Port:    443
-----[REDACTED]
+ SSL Info:      Subject: /C=SE/L=Stockholm/O=Spotify AB/CN=*.spotify.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time:    2020-10-21 02:25:14 (GMT-4)
-----[REDACTED]
+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 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
+ Uncommon header 'alt-svc' found, with contents: clear
+ The site uses SSL and Expect-CT header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /backup.tar.bz2: Potentially interesting archive/cert file found.
+ /com.tar.bz2: Potentially interesting archive/cert file found.
+ /podcasters.tar.bz2: Potentially interesting archive/cert file found.
+ /35.186.224.25.tar.bz2: Potentially interesting archive/cert file found.
+ /podcastersspotify.tar.bz2: Potentially interesting archive/cert file found.
+ /podcasters.spotify.tar.bz2: Potentially interesting archive/cert file found.
+ /podcasters.spotify.com.tar.bz2: Potentially interesting archive/cert file found.
+ /podcasters.spotify.com.tar.bz2: Potentially interesting archive/cert file found.
+ /podcasters.spotifycom.tar.bz2: Potentially interesting archive/cert file found.
+ /spotify.tar.bz2: Potentially interesting archive/cert file found.
+ /site.tar.bz2: Potentially interesting archive/cert file found.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server is using a wildcard certificate: *.spotify.com
[[c+ 7866 requests: 2 error(s) and 18 item(s) reported on remote host
+ End Time:      2020-10-21 03:59:01 (GMT-4) (5627 seconds)
-----[REDACTED]
+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. Server is using Wildcard Certification**

## promo.spotify.com



The screenshot shows a terminal window titled "Terminal" running on a Kali Linux system. The command entered is "nikto -h promo.spotify.com -p 443". The output of the scan is displayed, highlighting several security issues:

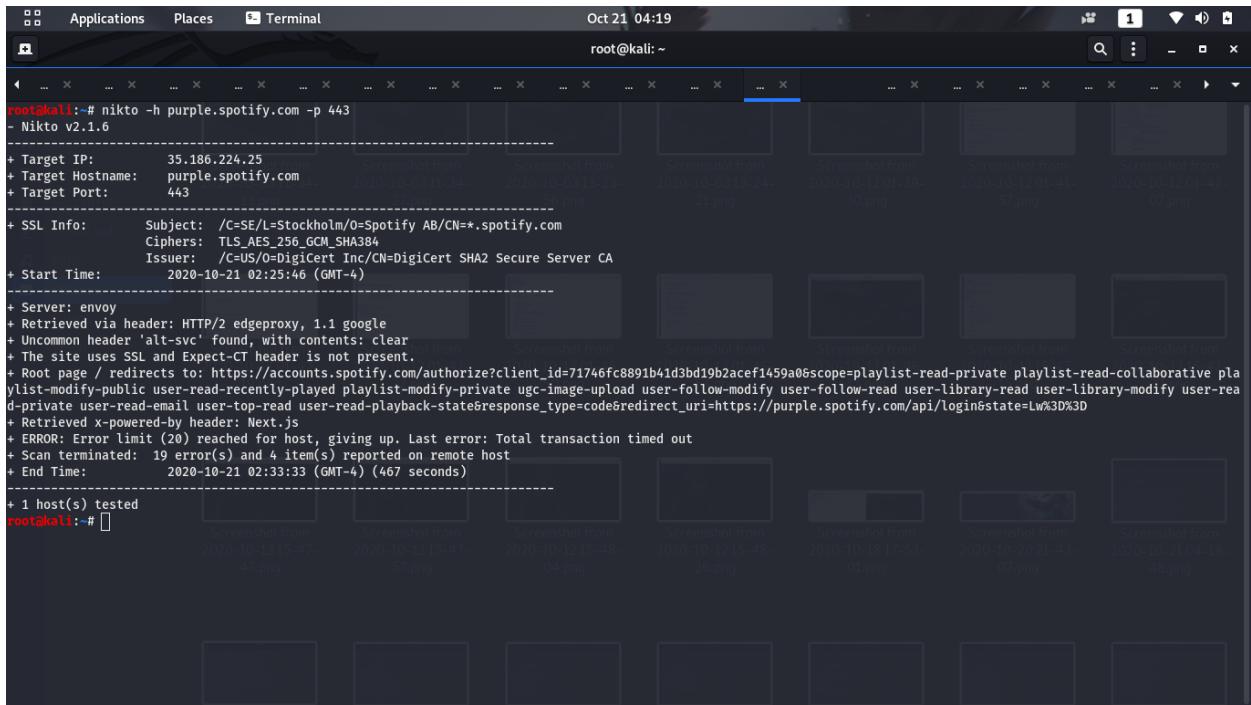
```
root@kali:~# nikto -h promo.spotify.com -p 443
- Nikto v2.1.6

+ Target IP:      151.101.10.133
+ Target Hostname: promo.spotify.com
+ Target Port:    443
+ SSL Info:       Subject: /C=SE/I=Stockholm/O=Spotify AB/CN=promo.spotify.com
                  Ciphers: ECDHE-RSA-AES128-GCM-SHA256
                  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time:    2020-10-21 02:25:32 (GMT-4)

+ Server: No banner retrieved
+ Retrieved x-served-by header: cache-ord1743-ORD, cache-sin18043-SIN
+ Retrieved access-control-allow-origin header: *
+ 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-amz-meta-goog-reserved-file-mtime' found, with contents: 1602665637
+ Uncommon header 'x-cache' found, with contents: HIT, HIT
+ Uncommon header 'x-served-by' found, with contents: cache-ord1743-ORD, cache-sin18043-SIN
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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)
+ Server banner has changed from '' to 'Varnish' which may suggest a WAF, load balancer or proxy is in place
+ Retrieved via header: 1.1 varnish
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ OSVDB-3092: /in/: This might be interesting... potential country code (India)
+ OSVDB-3092: /id/: This might be interesting... potential country code (Indonesia)
+ OSVDB-3092: /ph/: This might be interesting... potential country code (Philippines)
+ OSVDB-3092: /us/: This might be interesting... potential country code (United States)
+ 7863 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:    2020-10-21 04:16:38 (GMT-4) (6666 seconds)

+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. X-Content-Type-Options header is not set**

**purple.spotify.com**

The screenshot shows a terminal window titled "Terminal" running on Kali Linux. The command "nikto -h purple.spotify.com -p 443" is being executed. The output of the scan is displayed, detailing various findings about the target website.

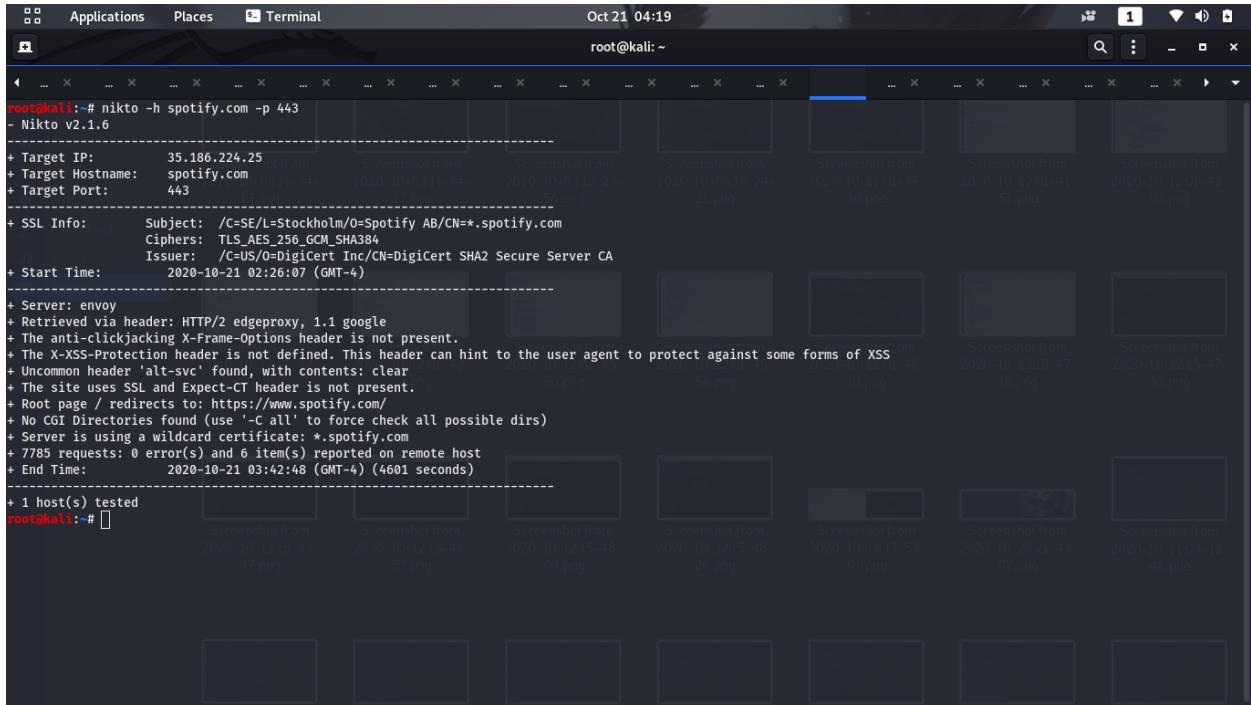
```
root@kali:~# nikto -h purple.spotify.com -p 443
- Nikto v2.1.6

+ Target IP:      35.186.224.25
+ Target Hostname: purple.spotify.com
+ Target Port:    443
+ SSL Info:      Subject: /C=SE/L=Stockholm/O=Spotify AB/CN=*.spotify.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time:    2020-10-21 02:25:46 (GMT-4)

+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 1.1 google
+ Uncommon header 'alt-svc' found, with contents: clear
+ The site uses SSL and Expect-CT header is not present.
+ Root page / redirects to: https://accounts.spotify.com/authorize?client_id=71746fc8891b41d3bd19b2acef1459a0&scope=playlist-read-private%20playlist-read-collaborative%20playlist-modify-public%20user-read-recently-played%20playlist-modify-private%20ugc-image-upload%20user-follow-modify%20user-follow-read%20user-library-read%20user-library-modify%20user-read-email%20user-top-read%20user-read-playback-state&response_type=code&redirect_uri=https://purple.spotify.com/api/login&state=Lw%3D%3D
+ Retrieved x-powered-by header: Next.js
+ ERROR: Error limit (20) reached for host, giving up. Last error: Total transaction timed out
+ Scan terminated: 19 error(s) and 4 item(s) reported on remote host
+ End Time:       2020-10-21 02:33:33 (GMT-4) (467 seconds)

+ 1 host(s) tested
root@kali:~#
```

## spotify.com



```
root@kali:~# nikto -h spotify.com -p 443
- Nikto v2.1.6

+ Target IP:      35.186.224.25
+ Target Hostname: spotify.com
+ Target Port:    443
+ SSL Info:       Subject: /C=SE/L=Stockholm/O=Spotify AB/CN=*.spotify.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time:     2020-10-21 02:26:07 (GMT-4)

+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 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
+ Uncommon header 'alt-svc' found, with contents: clear
+ The site uses SSL and Expect-CT header is not present.
+ Root page / redirects to: https://www.spotify.com/
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ Server is using a wildcard certificate: *.spotify.com
+ 7785 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:       2020-10-21 03:42:48 (GMT-4) (4601 seconds)

+ 1 host(s) tested
root@kali:~#
```

1. **Clickjacking**
2. **X-XSS-Protection header is not defined**
3. **Server is using Wildcard Certification**

## support.spotify.com

The terminal window shows a detailed security audit report for the host 35.186.224.25 (support.spotify.com) at port 443. The report includes SSL information, server headers, cookie analysis, and a summary of findings.

```
+ Target IP: 35.186.224.25
+ Target Hostname: support.spotify.com
+ Target Port: 443
+ SSL Info: Subject: /C=SE/L=Stockholm/O=Spotify AB/CN=*.spotify.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time: 2020-10-21 02:26:22 (GMT-4)

+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 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
+ Uncommon header 'alt-svc' found, with contents: clear
+ Uncommon header 'sp-trace-id' found, with contents: 53336671d5e9a91f
+ The site uses SSL and Expect-CT header is not present.
+ Root page / redirects to: https://support.spotify.com/int/
+ Retrieved x-powered-by header: Next.js
+ Uncommon header 'x-join-the-band' found, with contents: https://www.spotify.com/jobs/
+ Uncommon header 'report-to' found, with contents: { "group": "csp-endpoint", "max_age": 86400, "endpoints": [ { "url": "/api/concierge/csp/report-to" } ] }
+ Cookie sentry_sid created without the secure flag
+ Cookie sentry_sid created without the httponly flag
+ Cookie next-i18next created without the secure flag
+ Cookie next-i18next created without the httponly flag
+ Cookie sp__created created without the httponly flag
+ Cookie sp_new created without the httponly flag
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ "robots.txt" contains 5 entries which should be manually viewed.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server is using a wildcard certificate: *.spotify.com
+ Uncommon header 'refresh' found, with contents: 0;url=/servlet/custMsg?guestName=%3Cscript%3Ealert(%5C%22Vulnerable%5C%22)%3C%2Fscript%3E
+ 7868 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time: 2020-10-21 03:44:23 (GMT-4) (4681 seconds)

+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. Server is using Wildcard Certification**

## surveys.spotify.com

```
root@kali:~# nikto -h surveys.spotify.com -p 443
- Nikto v2.1.6

+ Target IP: 35.186.224.25
+ Target Hostname: surveys.spotify.com
+ Target Port: 443
+ SSL Info: Subject: /C=SE/L=Stockholm/O=Spotify AB/CN=*.spotify.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time: 2020-10-21 02:26:46 (GMT-4)

+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 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
+ Uncommon header 'alt-svc' found, with contents: clear
+ The site uses SSL and Expect-CT header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /surveys.egg: Potentially interesting archive/cert file found.
+ /35.186.224.25.tgz: Potentially interesting archive/cert file found.
+ /backup.tar.lzma: Potentially interesting archive/cert file found.
+ /surveys.spotify.tar.lzma: Potentially interesting archive/cert file found.
+ /35.186.224.25.tar: Potentially interesting archive/cert file found.
+ /backup.tar.bz2: Potentially interesting archive/cert file found.
+ /com.war: Potentially interesting archive/cert file found.
+ /surveys.spotify.war: Potentially interesting archive/cert file found.
+ /surveys.spotify.pem: Potentially interesting archive/cert file found.
+ /backup.pem: Potentially interesting archive/cert file found.
+ /spotify.cer: Potentially interesting archive/cert file found.
+ /surveys.spotify.com.tar: Potentially interesting archive/cert file found.
+ /spotify.egg: Potentially interesting archive/cert file found.
+ /surveys.spotify.cer: Potentially interesting archive/cert file found.
+ /surveys.spotify.com.pem: Potentially interesting archive/cert file found.
+ /surveys.spotify_com.tar.bz2: Potentially interesting archive/cert file found.
+ /surveys.spotify_com.cer: Potentially interesting archive/cert file found.
+ /backup.war: Potentially interesting archive/cert file found.

root@kali:~# nikto -h surveys.spotify.com -p 443
- Nikto v2.1.6

+ /surveys.spotifycom.tar.lzma: Potentially interesting archive/cert file found.
+ /site.pem: Potentially interesting archive/cert file found.
+ /surveys_spotify_com.egg: Potentially interesting archive/cert file found.
+ /surveys.spotify.tar: Potentially interesting archive/cert file found.
+ /surveys.spotify.war: Potentially interesting archive/cert file found.
+ /surveys.spotify.com.tgz: Potentially interesting archive/cert file found.
+ /surveys.spotifycom.tgz: Potentially interesting archive/cert file found.
+ /35.186.224.25.tar.bz2: Potentially interesting archive/cert file found.
+ /surveys.spotifycom.tar: Potentially interesting archive/cert file found.
+ /surveys.spotify_com.pem: Potentially interesting archive/cert file found.
+ /surveys.spotify_com.cer: Potentially interesting archive/cert file found.
+ /spotify.tar.bz2: Potentially interesting archive/cert file found.
+ /backup.tar: Potentially interesting archive/cert file found.
+ /com.tar.bz2: Potentially interesting archive/cert file found.
+ /surveys.war: Potentially interesting archive/cert file found.
+ /backup.alz: Potentially interesting archive/cert file found.
+ /backup.tgz: Potentially interesting archive/cert file found.
+ /surveys_spotify_com.tar: Potentially interesting archive/cert file found.
+ /35.186.224.25.cer: Potentially interesting archive/cert file found.
+ /com.pem: Potentially interesting archive/cert file found.
+ /surveys.spotify.pem: Potentially interesting archive/cert file found.
+ /surveys.spotify.com.tar.bz2: Potentially interesting archive/cert file found.
+ /surveys.spotifycom.egg: Potentially interesting archive/cert file found.
+ /surveys.tar.bz2: Potentially interesting archive/cert file found.
+ /site.egg: Potentially interesting archive/cert file found.
+ /spotify.war: Potentially interesting archive/cert file found.
+ /surveys.spotifycom.alz: Potentially interesting archive/cert file found.
+ /site.cer: Potentially interesting archive/cert file found.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server is using a wildcard certificate: *.spotify.com
+ OSVDB-23654: /profile.php?u=x2tRb9Efv: Powerboards is vulnerable to path disclosure.
+ 7871 requests: 0 error(s) and 118 item(s) reported on remote host
+ End Time: 2020-10-21 03:47:20 (GMT-4) (4834 seconds)

+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. Server is using Wildcard Certification**

## uplink.spotify.com

```
root@kali:~# nikto -h uplink.spotify.com -p 443
- Nikto v2.1.6

+ Target IP: 35.186.224.25
+ Target Hostname: uplink.spotify.com
+ Target Port: 443
+ SSL Info: Subject: /C=SE/L=Stockholm/O=Spotify AB/CN=*.spotify.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time: 2020-10-21 02:27:15 (GMT-4)

+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 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
+ Uncommon header 'alt-svc' found, with contents: clear
+ The site uses SSL and Expect-CT header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /backup.alz: Potentially interesting archive/cert file found.
+ /uplink.cer: Potentially interesting archive/cert file found.
+ /com.tar: Potentially interesting archive/cert file found.
+ /uplink.spotify.com.tgz: Potentially interesting archive/cert file found.
+ /35.186.224.25.war: Potentially interesting archive/cert file found.
+ /uplink.spotify.com.tar: Potentially interesting archive/cert file found.
+ /35.186.224.25.tar.lzma: Potentially interesting archive/cert file found.
+ /backup.tar.lzma: Potentially interesting archive/cert file found.
+ /backup.war: Potentially interesting archive/cert file found.
+ /uplink_spotify.com.tar.lzma: Potentially interesting archive/cert file found.
+ /uplinkspotify.egg: Potentially interesting archive/cert file found.
+ /35.186.224.25.cer: Potentially interesting archive/cert file found.
+ /com.cer: Potentially interesting archive/cert file found.
+ /spotify.tar.bz2: Potentially interesting archive/cert file found.
+ /uplink.egg: Potentially interesting archive/cert file found.
+ /uplink.spotify.tar.lzma: Potentially interesting archive/cert file found.
+ /uplink.spotify.com.pem: Potentially interesting archive/cert file found.
+ /site.alz: Potentially interesting archive/cert file found.

root@kali:~# nikto -h uplink.spotify.com -p 443
- Nikto v2.1.6

+ /com.alz: Potentially interesting archive/cert file found.
+ /uplink_spotify.com.tar: Potentially interesting archive/cert file found.
+ /uplinks.spotify.alz: Potentially interesting archive/cert file found.
+ /com.egg: Potentially interesting archive/cert file found.
+ /spotify.tar: Potentially interesting archive/cert file found.
+ /uplink.war: Potentially interesting archive/cert file found.
+ /uplinks.spotify.com.war: Potentially interesting archive/cert file found.
+ /uplinks.spotify.tar.bz2: Potentially interesting archive/cert file found.
+ /spotify.pem: Potentially interesting archive/cert file found.
+ /spotify.egg: Potentially interesting archive/cert file found.
+ /uplinks.spotify.tar: Potentially interesting archive/cert file found.
+ /com.jks: Potentially interesting archive/cert file found.
+ /uplink.tar.lzma: Potentially interesting archive/cert file found.
+ /uplink_spotify.com.war: Potentially interesting archive/cert file found.
+ /uplinks.spotify.com.tar.lzma: Potentially interesting archive/cert file found.
+ /35.186.224.25.tgz: Potentially interesting archive/cert file found.
+ /uplink.alz: Potentially interesting archive/cert file found.
+ /com.pem: Potentially interesting archive/cert file found.
+ /site.tar.bz2: Potentially interesting archive/cert file found.
+ /backup.cer: Potentially interesting archive/cert file found.
+ /site.tar: Potentially interesting archive/cert file found.
+ /uplinks.spotify.jks: Potentially interesting archive/cert file found.
+ /uplinks.spotify.com.egg: Potentially interesting archive/cert file found.
+ /uplink_spotify_com.cer: Potentially interesting archive/cert file found.
+ /spotify.war: Potentially interesting archive/cert file found.
+ /backup.egg: Potentially interesting archive/cert file found.
+ /uplink_spotify_com.egg: Potentially interesting archive/cert file found.
+ /uplink.spotify.tar: Potentially interesting archive/cert file found.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server is using a wildcard certificate: *.spotify.com
+ 7868 requests: 0 error(s) and 117 item(s) reported on remote host
+ End Time: 2020-10-21 03:45:01 (GMT-4) (4666 seconds)

+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. Server is using Wildcard Certification**

## works.spotify.com

```
root@kali:~# nikto -h works.spotify.com -p 443
- Nikto v2.1.6

+ Target IP:      35.186.224.25
+ Target Hostname: works.spotify.com
+ Target Port:    443
+ SSL Info:       Subject: /C=SE/I=Stockholm/O=Spotify AB/CN=*.spotify.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time:    2020-10-21 02:27:32 (GMT-4)

+ Server: envoy
+ Retrieved via header: HTTP/2 edgeproxy, 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
+ Uncommon header 'alt-svc' found, with contents: clear
+ The site uses SSL and Expect-CT header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /worksspotifycom.alz: Potentially interesting archive/cert file found.
+ /35.186.224.25.alz: Potentially interesting archive/cert file found.
+ /com.tar.lzma: Potentially interesting archive/cert file found.
+ /works_spotify_com.tgz: Potentially interesting archive/cert file found.
+ /works.egg: Potentially interesting archive/cert file found.
+ /site.tar.lzma: Potentially interesting archive/cert file found.
+ /works.spotify.pem: Potentially interesting archive/cert file found.
+ /worksspotify.tar.lzma: Potentially interesting archive/cert file found.
+ /backup.pem: Potentially interesting archive/cert file found.
+ /site.jks: Potentially interesting archive/cert file found.
+ /worksspotify.pem: Potentially interesting archive/cert file found.
+ /35.186.224.25.tar: Potentially interesting archive/cert file found.
+ /works.pem: Potentially interesting archive/cert file found.
+ /spotify.cer: Potentially interesting archive/cert file found.
+ /works.spotify.tar.lzma: Potentially interesting archive/cert file found.
+ /site.tgz: Potentially interesting archive/cert file found.
+ /com.jks: Potentially interesting archive/cert file found.
+ /worksspotifyv.alz: Potentially interesting archive/cert file found.

root@kali:~# nikto -h works.spotify.com -p 443
- Nikto v2.1.6

+ /works.spotify.com.egg: Potentially interesting archive/cert file found.
+ /works.spotify.tgz: Potentially interesting archive/cert file found.
+ /site.cer: Potentially interesting archive/cert file found.
+ /works.spotify.com.war: Potentially interesting archive/cert file found.
+ /35.186.224.25.cer: Potentially interesting archive/cert file found.
+ /backup.tar.bz2: Potentially interesting archive/cert file found.
+ /worksspotifycom.tar.bz2: Potentially interesting archive/cert file found.
+ /works.tar.bz2: Potentially interesting archive/cert file found.
+ /35.186.224.25.tar.lzma: Potentially interesting archive/cert file found.
+ /spotify.jks: Potentially interesting archive/cert file found.
+ /works.spotify.war: Potentially interesting archive/cert file found.
+ /backup.tar.lzma: Potentially interesting archive/cert file found.
+ /worksspotify.tar.bz2: Potentially interesting archive/cert file found.
+ /site.tar: Potentially interesting archive/cert file found.
+ /35.186.224.25.pem: Potentially interesting archive/cert file found.
+ /com.tgz: Potentially interesting archive/cert file found.
+ /works.spotify.tar: Potentially interesting archive/cert file found.
+ /works.spotify.com.tar.lzma: Potentially interesting archive/cert file found.
+ /site.pem: Potentially interesting archive/cert file found.
+ /works.spotify.com.alz: Potentially interesting archive/cert file found.
+ /works.spotify.com.pem: Potentially interesting archive/cert file found.
+ /works_spotify_com.egg: Potentially interesting archive/cert file found.
+ /works.spotify.alz: Potentially interesting archive/cert file found.
+ /works.spotify.com.war: Potentially interesting archive/cert file found.
+ /worksspotify.cer: Potentially interesting archive/cert file found.
+ /com.pem: Potentially interesting archive/cert file found.
+ /com.tar.bz2: Potentially interesting archive/cert file found.
+ /spotify.tgz: Potentially interesting archive/cert file found.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server is using a wildcard certificate: *.spotify.com
+ 7869 requests: 0 error(s) and 117 item(s) reported on remote host
+ End Time:      2020-10-21 03:45:18 (GMT-4) (4666 seconds)

+ 1 host(s) tested
root@kali:~#
```

- 1. Clickjacking**
- 2. X-XSS-Protection header is not defined**
- 3. Server is using Wildcard Certification**

## Vulnerability Explanation

1. **Clickjacking** | LOW | CWE-693 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

### Description

Clickjacking (User Interface Redress Attack, UI Redress Attack, UI Redressing) is a malicious method of tricking a Web user to click on something other than what the user believes they are clicking on, thereby potentially exposing sensitive information or gaining control of their device while clicking on apparently harmless web pages.

The X-Frame-Options header was not returned by the server, which means this website may be at risk of a clickjacking attack. The HTTP response header for X-Frame-Options can be used to indicate if a browser should be allowed to make a page within a frame or iframe or not. To stop clickjacking attacks, sites may do this by ensuring that their content is not inserted into other sites.

### Remediating

Set your web server to include an X-Frame-Options header and a Frame-Ancestors Directive CSP header. For more detail about the potential values for this header, check the Web references.

2. **X-XSS-Protection header is not defined** | Best Practice | CWE-16, HIPAA-16, ISO27001-A.14.2.5, WASC-15

### Description

The response header for HTTP 'X-XSS-Protection' is a feature of modern browsers that allows their XSS auditors to be monitored by websites. The server is not configured to return a 'X-XSS-Protection' header, so any pages on this website may be at risk of an attack by Cross-Site Scripting (XSS).

### Remediation

Add the X-XSS-Protection header with the value of "1; mode = block"

- X-XSS-Protection: 1; mode=block

**3. X-Content-Type-Options header is not set** | LOW | CWE-16, ISO27001-A.14.1.2, WASC-15, OWASP 2013-A5, OWASP 2017-A6

### Description

The response header of the HTTP 'X-Content-Type-Options' prevents the MIME browser from sniffing a response away from the content-type declared.

The server did not return a proper 'X-Content-Type-Options' header, which means that a Cross-Site Scripting (XSS) attack may be at risk on this website.

### Impact

In browsers, MIME style sniffing is a standard function to find a suitable way to make data where the HTTP headers sent by the server are either inconclusive or absent. This allows older versions of Internet Explorer and Chrome to perform MIME sniffing on the response body, possibly allowing the response body to be interpreted and displayed as a type of content other than the intended content.

Once a website allows users to upload content which is then published on the web server, the issue arises. If an attacker is able to perform XSS (Cross-site Scripting) attacks by modifying the content to be accepted by the web application and made by the browser as HTML, it is possible to insert code into an image file, for example, and to have the victim execute it by viewing the image.

### Remediation

- 1) Make sure you send the content-type header while serving resources to correctly fit the type of resource being served. For e.g. if an HTML page is served, you can send an HTTP header
  - Content-Type: text/html
- 2) Add a "nosniff" X-Content-Type-Options header to tell the browser to trust what the site has sent is the acceptable content-type and not to try to "sniff" the actual content-type.
  - X-Content-Type-Options: nosniff

#### 4. BREACH Attack (Possible) | Medium | OWASP 2013-A9, OWASP 2017-A9, CWE310 | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

##### Description

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

##### Remediation

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:

- If possible, disable HTTP level compression
- Separate sensitive information from user input

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.

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

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

**5. HTTP Strict Transport Security (HSTS) Policy Not Enabled****6. Weak Ciphers Enabled**

(both of above are explained under first set of scans)

**7. Out-of-date Version (jQuery) | Medium | PCI DSS 3.2 -6.2, OWASP 2013 - A9, OWASP2017 - A9, CWE - 829, CAPEC – 310, HIPAA - 164.308(A)(1)(I), ISO27001 - A.14.1.2****Description**

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.

**Remediation**

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

**Known Vulnerabilities in this Version****jquery Cross-site Scripting (XSS) Vulnerability (CVE-2015-9251)**

- 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 - 1.2.1 to 1.12.4

**jquery Cross-site Scripting (XSS) Vulnerability (CVE-2019-11358)**

- 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 - 1.2.1 to 3.2.1

**8. Autocomplete is Enabled** | LOW | OWASP 2013 - A5, OWASP 2017 - A6, CWE – 16, WASC – 15, ISO27001 - A.14.1.2**Description**

Autocomplete is Enabled in one or more of the form fields which might contain sensitive information like "username", "credit card" or "CVV"

**Impact**

If the user wishes to save, the browser will store the information entered in these fields. This information may be stolen by an intruder who can access the victim's browser. This is particularly important if the program is widely used on shared devices, such as cyber cafes or airport terminals.

**Remediation**

Add the autocomplete="off" attribute to the form tag or individual "input" fields. Since early 2014, however, due to their integrated password management mechanism, major browsers have not complied with this instruction and give users to store passwords internally.

Find all input instances that store and disable autocomplete private data. Fields containing data such as data form "Credit Card" or "CCV" should not be cached. You may allow the application to cache usernames and remember passwords, but this is not recommended in most cases.

After fixing the identified problems, re-scan the application to ensure that all the fixes have been implemented correctly.

**9. Cookie Not Marked as Http Only** |LOW|OWASP 2013 - A5, OWASP 2017 - A6, CWE - 16, CAPEC - 107, WASC - 15, ISO27001 - A.14.2.5

**Description**

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

**Impact**

An attacker could easily access cookies and hijack the victim's session during a cross-site scripting attack.

**Remediation**

Label the HTTPOnly cookie. This is going to be an additional security layer against XSS. This is not a magic bullet, however, and will not safeguard the device from cross-site scripting attacks. An attacker can circumvent HTTPOnly security by using a method such as XSS Tunnel.

**10. Cookie Not Marked as Secure** |LOW|PCI DSS 3.26.5.10, OWASP 2013 - A6, OWASP 2017 - A3, CWE - 614, CAPEC -102, WASC – 15, ISO27001 - A.14.1.2

**Description**

An attacker who can effectively intercept and decode the traffic, or after a successful man-in-the-middle attack, may theoretically steal the cookie.

**Impact**

This cookie is transmitted over an HTTP link, so if this cookie is significant (such as a session cookie), it can be intercepted by an attacker and hijacked by the victim. If the intruder is able to execute a man-in-the-middle attack, the victim will be forced to make an HTTP request to steal the cookie.

**Remediation**

Mark all cookies used within the application as secure

**11. Insecure Frame (External)** | LOW | OWASP 2017A6, CWE -m 16, WASC – 15, ISO27001 - A.14.1.2**Description**

An attacker who can effectively intercept and decode the traffic, or after a successful man-in-the-middle attack, may theoretically steal the cookie.

**Impact**

This cookie is transmitted over an HTTP link, so if this cookie is significant (such as a session cookie), it can be intercepted by an attacker and hijacked by the victim. If the intruder is able to execute a man-in-the-middle attack, the victim will be forced to make an HTTP request to steal the cookie.

**Remediation**

Mark all cookies used within the application as secure

**12. Missing X-Frame-Options Header** | LOW | OWASP 2013A5, OWASP 2017 - A6, CWE – 693, CAPEC – 103, ISO27001A. - 14.2.5**Description**

The missing X-Frame-Options header means that a clickjacking attack may be at risk on this website.

The X-Frame-Options HTTP header field indicates a policy that determines if the transmitted resource should be made within a frame or an iframe by the browser. To avoid clickjacking attacks, servers should announce this policy in the header of their HTTP responses, which ensures that their content is not inserted into other pages or frames.

**Impact**

Clickjacking is when an attacker uses several transparent or opaque layers when they intend to click on the top-level page to trick a user into clicking on a button or connection on a framed page. The intruder then hijacks clicks intended for their page and routes them to another page, most likely owned by another program, domain, or both. Keystrokes may also be hijacked using a similar technique. A user can be led to believe that they are typing in the password to their email or bank account with a carefully designed mix of stylesheets, iframes, and text boxes, but are actually typing in an invisible frame operated by the attacker.

### Remediation

Sending correct X-Frame-Options to HTTP response headers that instruct the browser not to allow other domains to be framed.

- X-Frame-Options: DENY This absolutely denies frame / iframe loading.
- X-Frame-Options: SAMEORIGIN This option is only allowed if the site you want to load has the same origin.
- X-Frame-Options: ALLOW-FROM URL A particular URL is given to load itself into an iframe. Please notice that, however, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top-level window.

## 13. Server is using Wildcard Certification

### Description

There are additional security issues regarding the defense provided by SSL / TLS certificates when a wildcard certificate is reused across multiple subdomains hosted on multiple servers. The certificate will be compromised by adversaries in the case of a breach by one of the servers. There is a danger to the security and credibility of traffic to each site where the certificate is used. It would be possible for an intruder who gets the certificate to decrypt, read or alter, and re-encrypt traffic. This is likely to result in classified information being leaked and more targeted attacks being carried out.

In the event of a server breach, each server should have a unique certificate that is only valid for the subdomains and sites it is hosting, in order to limit the harm. There is almost no need to use wildcard certificates, with services such as Let's Encrypt providing free certificates and numerous solutions for automatic certificate renewal and deployment. In addition, wildcard certificates are ideal for the mishandling of private keys. If not safely stored or transferred, they can be compromised, requiring the revocation of a certificate.

#### 14. cookie PHPSESSID created without the httponly flag

##### Description

If the `HttpOnly` attribute is placed on a cookie, then the value of the cookie cannot be read or placed by JavaScript on the client side. This measure makes it marginally harder to exploit such client-side attacks, such as cross-site scripting, by preventing them from trivially capturing the cookie value via an embedded script.

##### Remediation

Usually, there is no valid reason for not setting the `HttpOnly` flag on all cookies. You can set the `HttpOnly` flag by adding this attribute within the applicable `Set-cookie` directive, unless you explicitly need valid client-side scripts within your application to read or set the value of a cookie.

We should be aware that in certain cases, the constraints placed by the `HttpOnly` flag can theoretically be circumvented, and that various other severe attacks, apart from basic cookie theft, can be delivered by client-side script injection.

## Scan using Lazyrecon

After that I try to scan using Lazyrecon tool. But I wasn't able to understand the report given after the scan.

**RECON REPORT FOR SPOTIFY.COM**

Generated by LazyRecon on Fri 16 Oct 2020 02:24:45 PM EDT

**TOTAL SCANNED SUBDOMAINS**

Subdomains	Scanned Urls
0	1

**POSSIBLE NS TAKEOVERS**

**WAYBACK DATA**

Params wordlist

**RECON REPORT FOR SPOTIFY.COM**

Generated by LazyRecon on Fri 16 Oct 2020 05:24:52 PM EDT

**TOTAL SCANNED SUBDOMAINS**

Subdomains	Scanned Urls
accounts.spotify.com	0 0
accounts-staging.spotify.com	41
adeventtracker.spotify.com	42
adlab.spotify.com	42
ads.developer.spotify.com	42
adsigtm.spotify.com	42
ads.spotify.com	43

**VIEW AQUATONE REPORT**

**DIG INFO**

```

; <>> DiG 9.11.5-P4-5.1+b1-Debian <>> spotify.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 41507
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;spotify.com.           IN      A
;
;; ANSWER SECTION:
spotify.com.        299     IN      A      35.186.224.25
;
;; Query time: 121 msec
;; SERVER: 2001:4860:4860::8888&5(2001:4860:4860:8888)
;; WHEN: Fri Oct 16 14:24:45 EDT 2020
;; MSG SIZE rcvd: 56

```

**HOST INFO**

```

spotify.com has address 35.186.224.25
spotify.com has IPv6 address 2600:1901:1:c36:
spotify.com mail is handled by 1 aspmx.l.google.com.
spotify.com mail is handled by 5 alt1.aspmx.l.google.com.
spotify.com mail is handled by 5 alt2.aspmx.l.google.com.
spotify.com mail is handled by 10 aspmx2.googlemail.com.
spotify.com mail is handled by 10 aspmx3.googlemail.com.
spotify.com mail is handled by 10 aspmx4.googlemail.com.
spotify.com mail is handled by 10 aspmx5.googlemail.com.

```

**NMAP RESULTS**

```

Not shown: 31 filtered ports
443/tcp open ssl/https envoy
5432/tcp open tcpwrapped
5900/tcp open tcpwrapped
8080/tcp open http-proxy

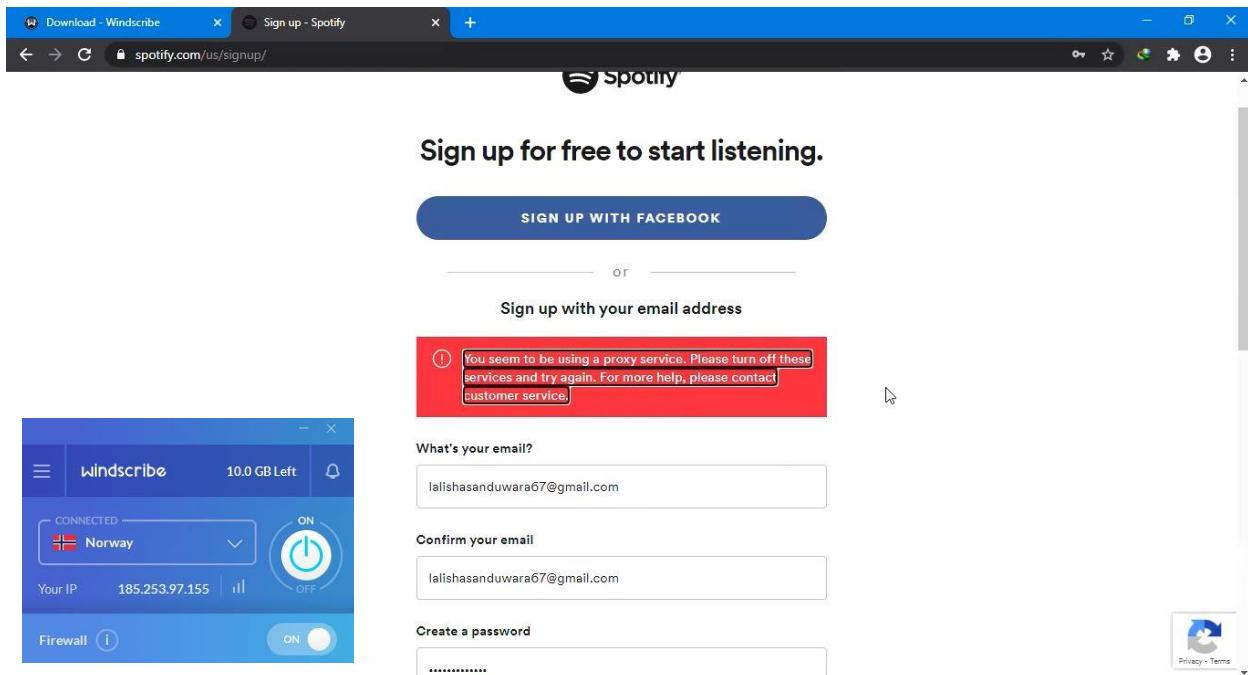
```

**VIEW AQUATONE REPORT**

I wasn't able to configure this out.

## Inspect using Burp suite

I also tried to inspect this Spotify.com using Burp suite. Before that I had to create a Spotify account. Since all of you know that Sri Lankans still have no access to create Spotify accounts. So that we have to use a VPN. So, I also installed a Windscribe VPN in my pc and tried to create a Spotify account. But results were as follow.



Because of this situation I was unable to inspect using the Burp suite.

## References

- Center, S., Definitions, I. and set, C., 2020. *Cookie Without Httponly Flag Set*. [online] Portswigger.net. Available at: <[https://portswigger.net/kb/issues/00500600\\_cookie-without-httponly-flag-set](https://portswigger.net/kb/issues/00500600_cookie-without-httponly-flag-set)> [Accessed 23 October 2020].
- Netsparker.com. 2020. *Missing X-Frame-Options Header / Netsparker*. [online] Available at: <<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-x-frame-options-header/>> [Accessed 23 October 2020].
- Owasp.org. 2020. *OWASP Foundation / Open Source Foundation For Application Security*. [online] Available at: <<https://owasp.org/>> [Accessed 23 October 2020].
- Academy, W. and scripting, C., 2020. *What Is Cross-Site Scripting (XSS) And How To Prevent It? / Web Security Academy*. [online] Portswigger.net. Available at: <<https://portswigger.net/web-security/cross-site-scripting>> [Accessed 23 October 2020].
- YouTube. 2020. *Web App Penetration Testing Tutorials*. [online] Available at: <<https://www.youtube.com/playlist?reload=9&list=PLBf0hzazHTGO3EpGAs718LvLsiMlv9dSC>> [Accessed 23 October 2020].
2020. [online] Available at: <<https://www.packetlabs.net/wildcard-certificates/#:~:text=Security%20Risks%20of%20Wildcard%20Certificates&text=An%20attacker%20who%20obtains%20the,information%20and%20further%20targeted%20attacks.>> [Accessed 23 October 2020].

### Final Video Link:

[https://drive.google.com/file/d/1uynBledb\\_zfqRF3sleA5zKDghw5PqMHW/view?usp=sharing](https://drive.google.com/file/d/1uynBledb_zfqRF3sleA5zKDghw5PqMHW/view?usp=sharing)