★ Practical 4 :- HTTP load testing using h2load

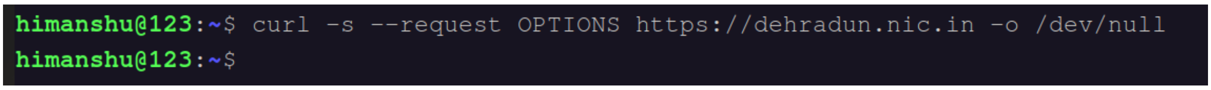
Analysing network requests and responses using developer tools in the browser is typically done through tools like Chrome Developer Tools or Firefox Developer Tools. Since you want to perform these tasks in a terminal on Ubuntu, you can use curl along with other command-line tools. Below is a step-by-step guide for each of your tasks:

- **The task I have here is through the command-line interface (CLI).**

➢ Task 1. List of non-GET requests and determine their request body:

This command sends an OPTIONS request to the specified URL. The response headers will contain information about the allowed methods, including POST or others. If POST is allowed, you can try making a POST request with data to get the request body.

a. **Command :- curl -s --request OPTIONS https://dehradun.nic.in -o /dev/null**



```
himanshu@123:~$ curl -s --request OPTIONS https://dehradun.nic.in -o /dev/null
himanshu@123:~$
```

- **curl:** The command-line tool for making HTTP requests.

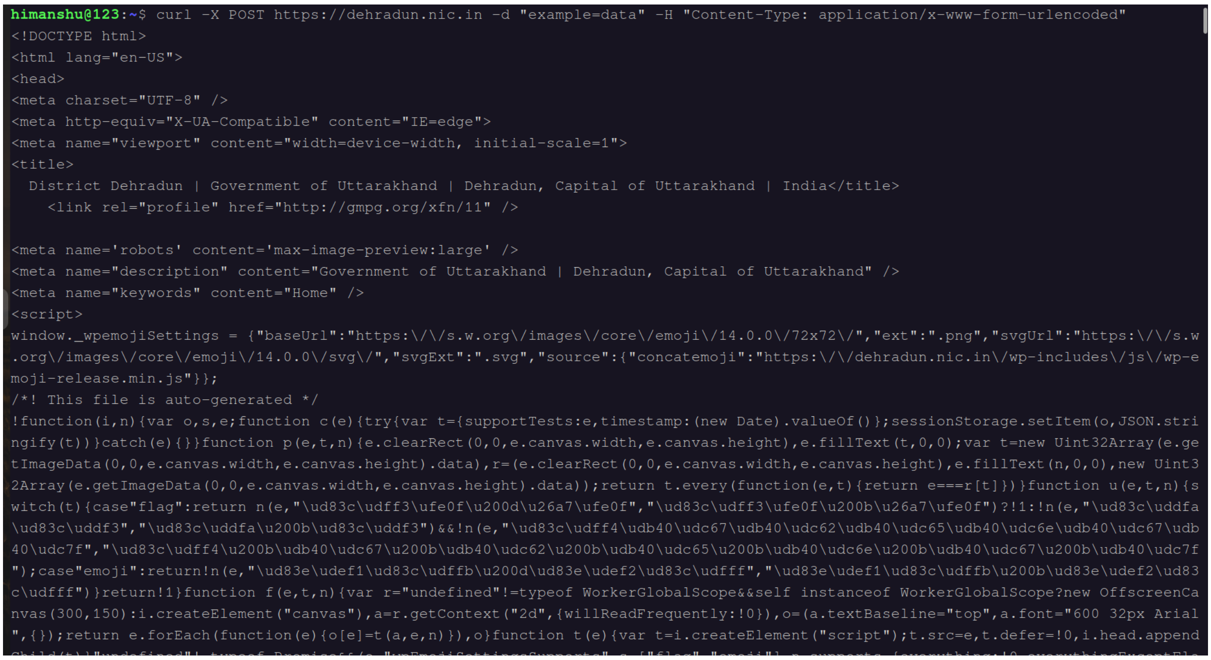
- **-s or --silent:** This option is used to make curl operate in silent mode, meaning it will not show progress or error messages. It's often used when you want to suppress unnecessary output.

- **--request OPTIONS:** This option specifies the HTTP method to be used for the request. In this case, it's set to OPTIONS. The OPTIONS method is used to describe the communication options for the target resource.

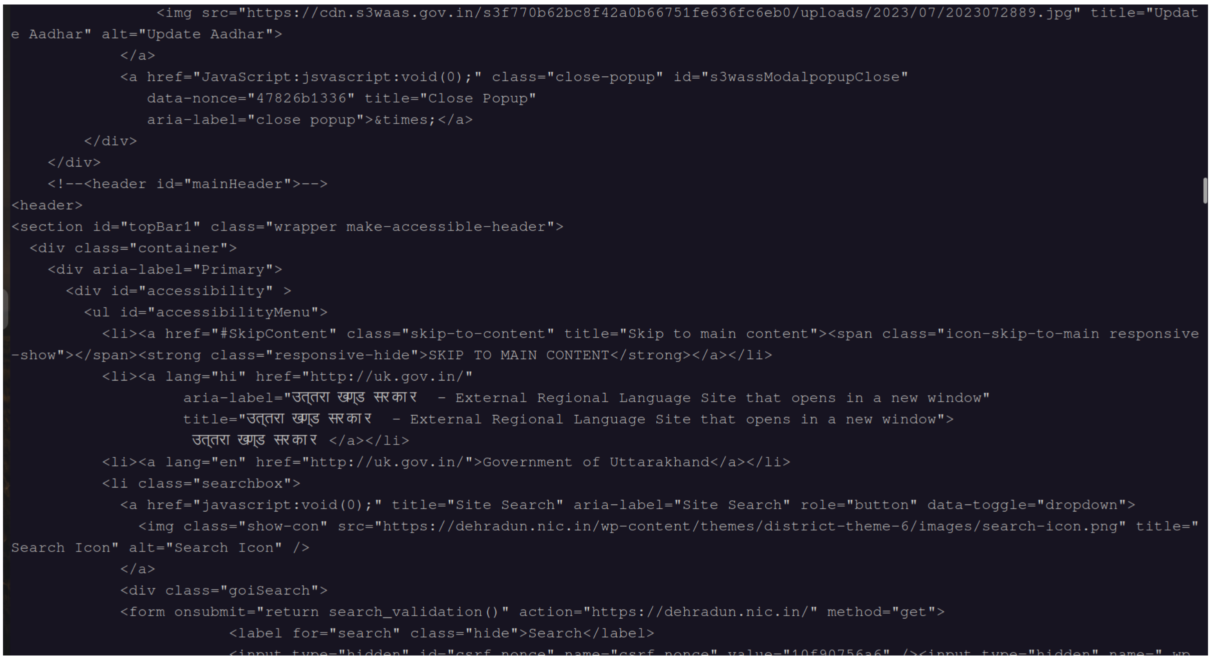
- **https://dehradun.nic.in :** This is the URL to which the HTTP request is being sent. It appears to be the website for Dehradun, an Indian city.

- **-o /dev/null:** This option is used to write the output of the curl command to a file. In this case, it's being written to /dev/null, which is a special file on Unix-like operating systems that discards all data written to it. Essentially, this part of the command is saying "send the output to nowhere" or "ignore the output."

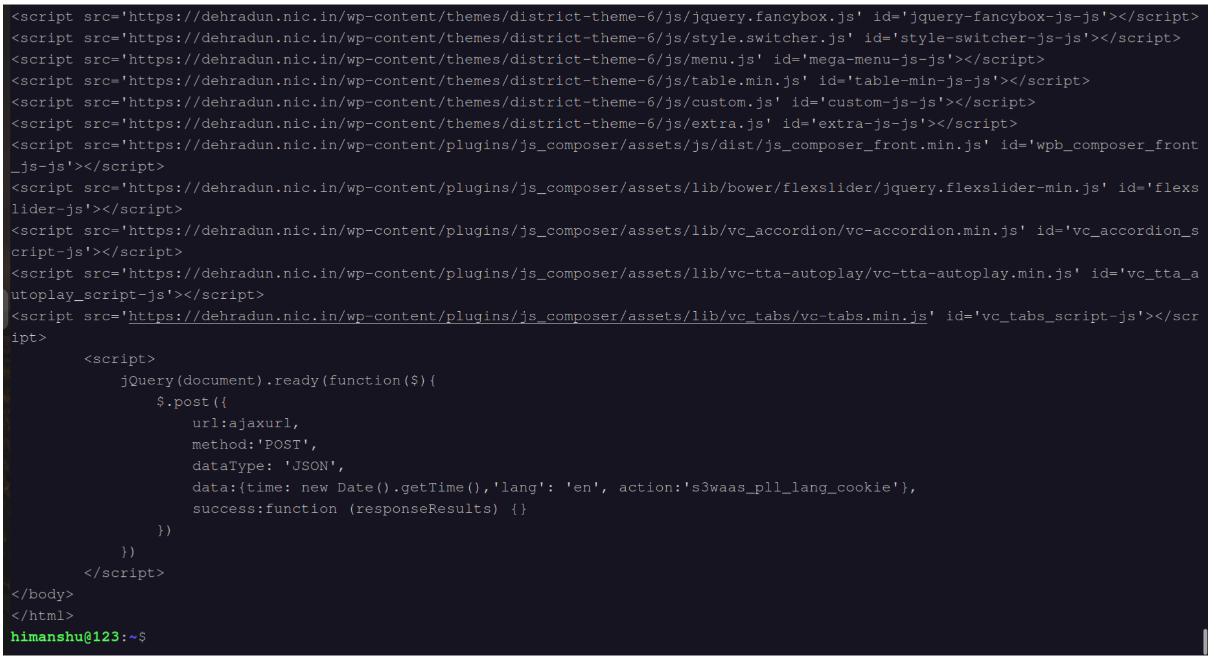
b. **command :- curl -X POST https://dehradun.nic.in -d "example=data" -H "Content-Type: application/x-www-form-urlencoded"**



```
himanshu@123:~$ curl -X POST https://dehradun.nic.in -d "example=data" -H "Content-Type: application/x-www-form-urlencoded"
<!DOCTYPE html>
<html lang="en-US">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>
  District Dehradun | Government of Uttarakhand | Dehradun, Capital of Uttarakhand | India</title>
    <link rel="profile" href="http://gmpg.org/xfn/11" />

<meta name='robots' content='max-image-preview:large' />
<meta name="description" content="Government of Uttarakhand | Dehradun, Capital of Uttarakhand" />
<meta name="keywords" content="Home" />
<script>
window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/14.0.0\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w
.org\/images\/core\/emoji\/14.0.0\/svg\/","svgExt":".svg","source":{"concatemoji":"https:\/\/dehradun.nic.in\/wp-includes\/js\/wp-e
moji-release.min.js"}};
/*! This file is auto-generated */
!function(i,n){var o,s,e;function c(e){try{var t={supportTests:e,timestamp:(new Date).valueOf()};sessionStorage.setItem(o,JSON.stri
ngify(t))}catch(e){}}function p(e,t,n){e.clearRect(0,0,e.canvas.width,e.canvas.height),e.fillText(t,0,0);var t=new Uint32Array(e.ge
tImageData(0,0,e.canvas.width,e.canvas.height).data),r=(e.clearRect(0,0,e.canvas.width,e.canvas.height),e.fillText(n,0,0),new Uint3
2Array(e.getImageData(0,0,e.canvas.width,e.canvas.height).data));return t.every(function(e,t){return e===r[t]})}function u(e,t,n){s
witch(t){case"flag":return n(e,"\ud83c\udff3\ufe0f\u200d\u26a7\ufe0f","\ud83c\udff3\ufe0f\u200b\u26a7\ufe0f")?!1:!n(e,"\ud83c\uddfa
\ud83c\uddf3","\ud83c\uddfa\u200b\ud83c\uddf3")&&!n(e,"\ud83c\udff4\udb40\udc67\udb40\udc62\udb40\udc65\udb40\udc6e\udb40\udc67\udb
40\udc7f","\ud83c\udff4\u200b\udb40\udc67\u200b\udb40\udc62\u200b\udb40\udc65\u200b\udb40\udc6e\u200b\udb40\udc67\u200b\udb40\udc7f
");case"emoji":return!n(e,"\ud83e\udef1\ud83c\udffb\u200d\ud83e\udef2\ud83c\udfff","\ud83e\udef1\ud83c\udffb\u200b\ud83e\udef2\ud83
c\udfff")}return!1}function f(e,t,n){var r="undefined"!=typeof WorkerGlobalScope&&self instanceof WorkerGlobalScope?new OffscreenCa
nvas(300,150):i.createElement("canvas"),a=r.getContext("2d",{willReadFrequently:!0}),o=(a.textBaseline="top",a.font="600 32px Arial
",{});return e.forEach(function(e){o[e]=t(a,e,n)}),o}function t(e){var t=i.createElement("script");t.src=e,t.defer=!0,i.head.append
```



```
                <img src="https://cdn.s3waas.gov.in/s3f770b62bc8f42a0b66751fe636fc6eb0/uploads/2023/07/2023072889.jpg" title="Updat
e Aadhar" alt="Update Aadhar">
            </a>
            <a href="JavaScript:jsvascript:void(0);" class="close-popup" id="s3wassModalpopupClose"
               data-nonce="47826b1336" title="Close Popup"
               aria-label="close popup">&times;</a>
        </div>
    </div>
    <!--<header id="mainHeader">-->
<header>
<section id="topBar1" class="wrapper make-accessible-header">
  <div class="container">
    <div aria-label="Primary">
      <div id="accessibility" >
        <ul id="accessibilityMenu">
          <li><a href="#SkipContent" class="skip-to-content" title="Skip to main content"><span class="icon-skip-to-main responsive
-show"></span><strong class="responsive-hide">SKIP TO MAIN CONTENT</strong></a></li>
          <li><a lang="hi" href="http://uk.gov.in/"
                   aria-label="उत्तरा खण्ड सरकार  - External Regional Language Site that opens in a new window"
                   title="उत्तरा खण्ड सरकार  - External Regional Language Site that opens in a new window">
                    उत्तरा खण्ड सरकार </a></li>
          <li><a lang="en" href="http://uk.gov.in/">Government of Uttarakhand</a></li>
          <li class="searchbox">
            <a href="javascript:void(0);" title="Site Search" aria-label="Site Search" role="button" data-toggle="dropdown">
              <img class="show-con" src="https://dehradun.nic.in/wp-content/themes/district-theme-6/images/search-icon.png" title="
Search Icon" alt="Search Icon" />
            </a>
            <div class="goiSearch">
            <form onsubmit="return search_validation()" action="https://dehradun.nic.in/" method="get">
                        <label for="search" class="hide">Search</label>
```



```
<script src='https://dehradun.nic.in/wp-content/themes/district-theme-6/js/jquery.fancybox.js' id='jquery-fancybox-js-js'></script>
<script src='https://dehradun.nic.in/wp-content/themes/district-theme-6/js/style.switcher.js' id='style-switcher-js-js'></script>
<script src='https://dehradun.nic.in/wp-content/themes/district-theme-6/js/menu.js' id='mega-menu-js-js'></script>
<script src='https://dehradun.nic.in/wp-content/themes/district-theme-6/js/table.min.js' id='table-min-js-js'></script>
<script src='https://dehradun.nic.in/wp-content/themes/district-theme-6/js/custom.js' id='custom-js-js'></script>
<script src='https://dehradun.nic.in/wp-content/themes/district-theme-6/js/extra.js' id='extra-js-js'></script>
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/js/dist/js_composer_front.min.js' id='wpb_composer_front
_js-js'></script>
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/bower/flexslider/jquery.flexslider-min.js' id='flexs
lider-js'></script>
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/vc_accordion/vc-accordion.min.js' id='vc_accordion_s
cript-js'></script>
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/vc-tta-autoplay/vc-tta-autoplay.min.js' id='vc_tta_a
utoplay_script-js'></script>
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/vc_tabs/vc-tabs.min.js' id='vc_tabs_script-js'></scr
ipt>
        <script>
            jQuery(document).ready(function($){
                $.post({
                    url:ajaxurl,
                    method:'POST',
                    dataType: 'JSON',
                    data:{time: new Date().getTime(),'lang': 'en', action:'s3waas_pll_lang_cookie'},
                    success:function (responseResults) {}
                })
            })
        </script>
</body>
</html>
himanshu@123:~$
```

- **curl:** The command-line tool for making HTTP requests.

- **-X POST:** Specifies the HTTP method as POST. This means you are sending data to the specified URL using the HTTP POST method.

- **https://dehradun.nic.in :** The URL to which the POST request is being made.

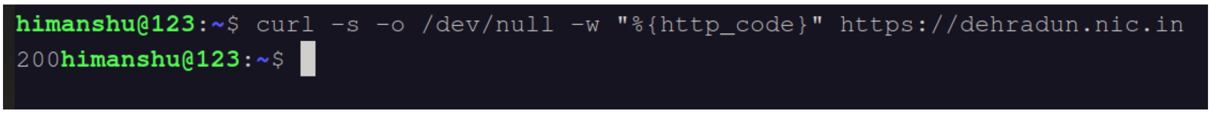
- **-d "example=data":** This option is used to send data in the request body. In this case, you are sending the data "example=data" as part of the POST request.

- **-H "Content-Type: application/x-www-form-urlencoded":** This option is used to set the HTTP header. In this case, you are setting the "Content-Type" header to "application/x-www-form-urlencoded," indicating that the data in the request body is formatted as URL-encoded form data.

➢ Task 2. List of non-200 responses:

This command will return the HTTP status code. If it's not 200, it means there is a non-200 response. You can then investigate further to see the actual response body:

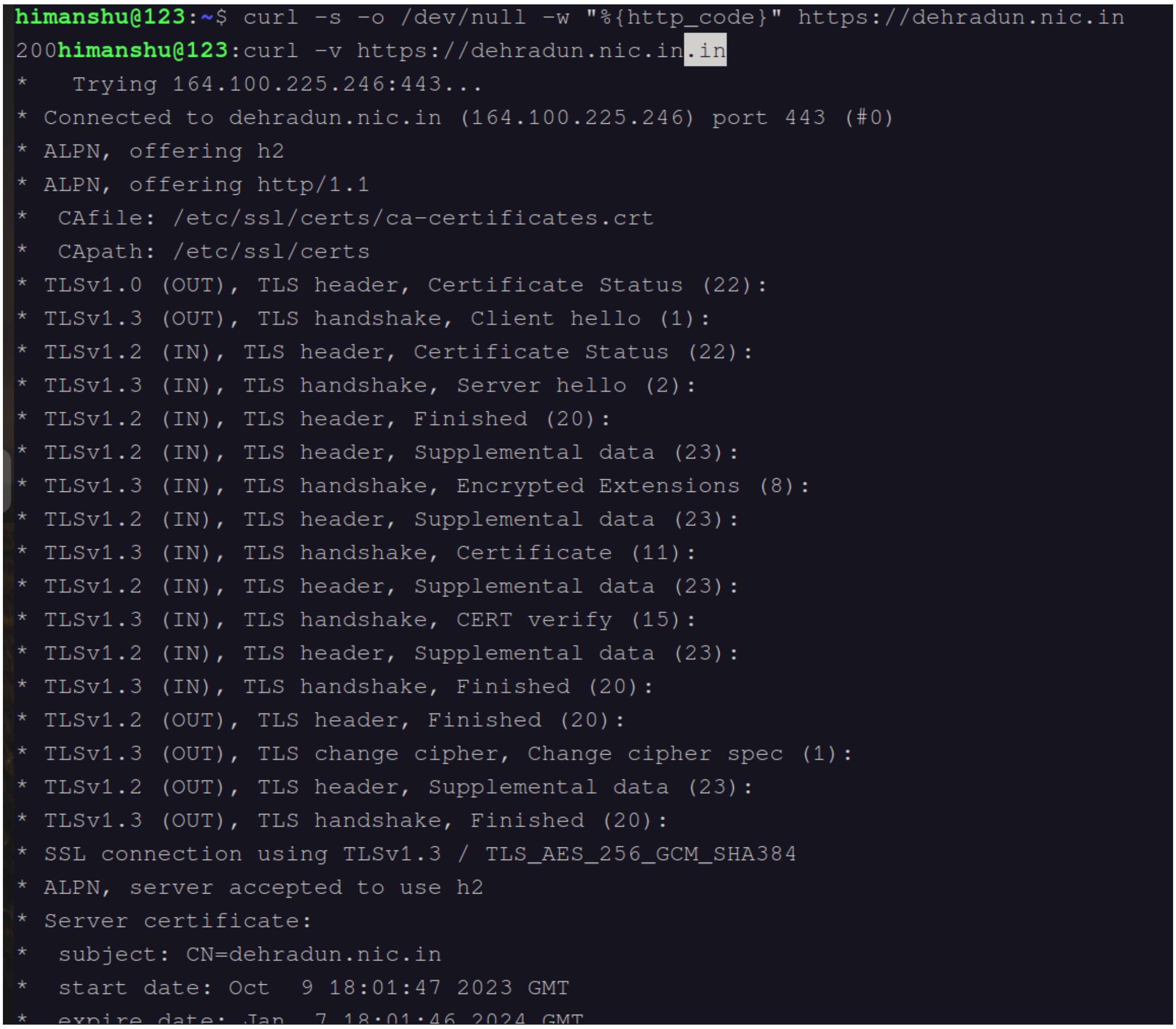
a. **Command :- curl -s -o /dev/null -w "%{http_code}" https://dehradun.nic.in**



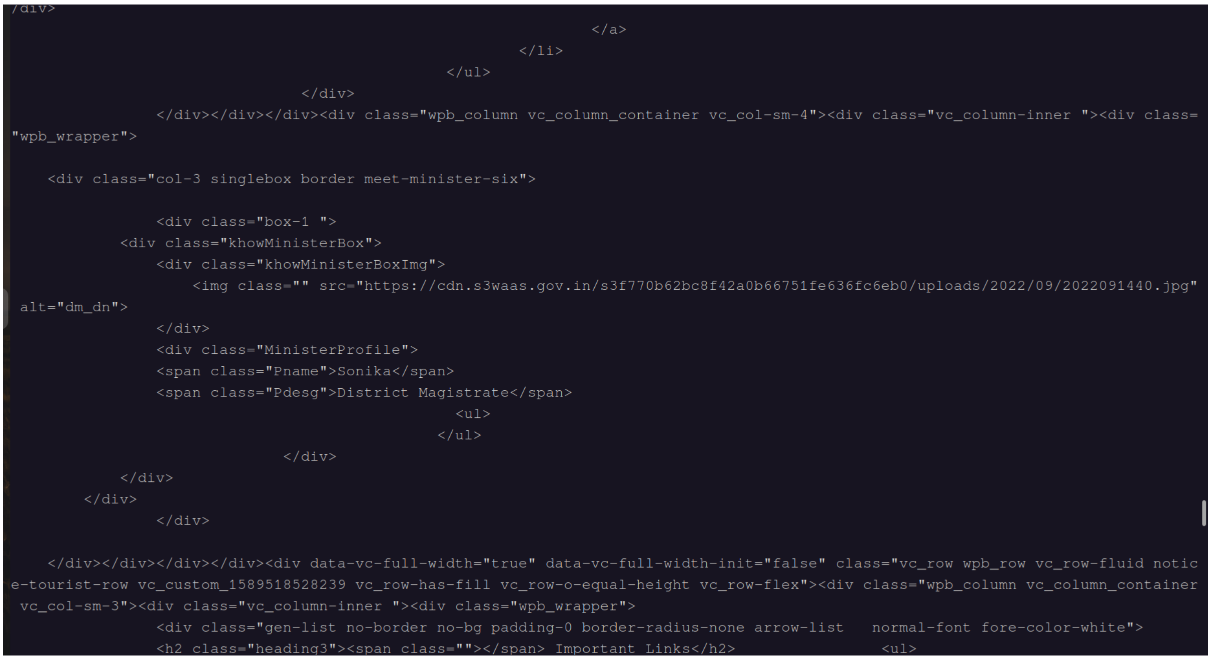
```
himanshu@123:~$ curl -s -o /dev/null -w "%{http_code}" https://dehradun.nic.in
200himanshu@123:~$
```

- **curl:** This is the command-line tool for making HTTP requests.
- **-s:** This option stands for "silent" or "quiet" mode. It prevents curl from showing progress information or error messages. It makes the command run in the background without displaying any output.
- **-o /dev/null:** This option redirects the output of the HTTP request to /dev/null, a special file on Unix-like operating systems that discards all data written to it. Essentially, this means that the response body will not be printed to the terminal.
- **-w "%{http_code}":** This option is used to specify a custom format for the output. In this case, it's using the %{http_code} format specifier, which will be replaced by the HTTP response code of the request.
- **https://dehradun.nic.in :** This is the URL of the website to which the HTTP request is being made.

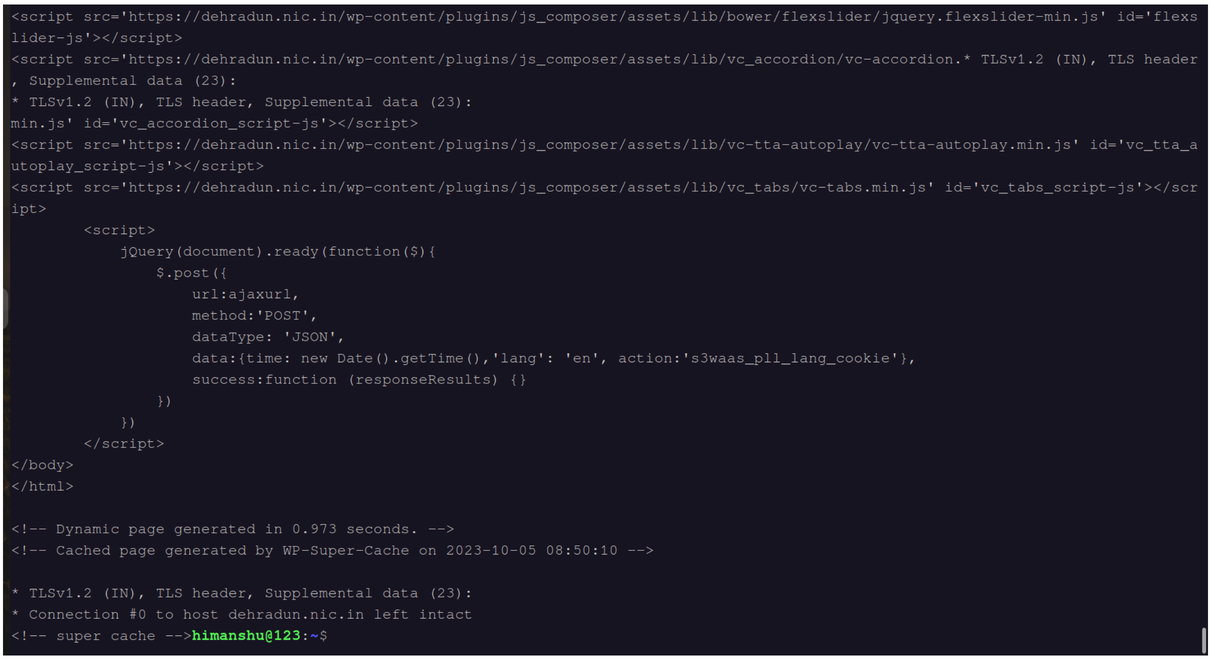
b. **Command :- curl -X POST https://dehradun.nic.in -d "example=data" -H "Content-Type: application/x-www-form-urlencoded"**



```
himanshu@123:~$ curl -s -o /dev/null -w "%{http_code}" https://dehradun.nic.in
200himanshu@123:curl -v https://dehradun.nic.in.in
*   Trying 164.100.225.246:443...
* Connected to dehradun.nic.in (164.100.225.246) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
*  CAfile: /etc/ssl/certs/ca-certificates.crt
*  CApath: /etc/ssl/certs
* TLSv1.0 (OUT), TLS header, Certificate Status (22):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS header, Finished (20):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.2 (OUT), TLS header, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server accepted to use h2
* Server certificate:
*  subject: CN=dehradun.nic.in
*  start date: Oct  9 18:01:47 2023 GMT
*  expire date: Jan  7 18:01:46 2024 GMT
```



```
/div>
                                                                </a>
                                                        </li>
                                                </ul>
                                </div>
                </div></div></div><div class="wpb_column vc_column_container vc_col-sm-4"><div class="vc_column-inner "><div class=
"wpb_wrapper">

    <div class="col-3 singlebox border meet-minister-six">

                <div class="box-1 ">
            <div class="khowMinisterBox">
                <div class="khowMinisterBoxImg">
                    <img class="" src="https://cdn.s3waas.gov.in/s3f770b62bc8f42a0b66751fe636fc6eb0/uploads/2022/09/2022091440.jpg"
 alt="dm_dn">
                </div>
                <div class="MinisterProfile">
                <span class="Pname">Sonika</span>
                <span class="Pdesg">District Magistrate</span>
                                                 <ul>
                                               </ul>
                              </div>
            </div>
        </div>
                </div>

    </div></div></div></div><div data-vc-full-width="true" data-vc-full-width-init="false" class="vc_row wpb_row vc_row-fluid notic
e-tourist-row vc_custom_1589518528239 vc_row-has-fill vc_row-o-equal-height vc_row-flex"><div class="wpb_column vc_column_container
 vc_col-sm-3"><div class="vc_column-inner "><div class="wpb_wrapper">
                <div class="gen-list no-border no-bg padding-0 border-radius-none arrow-list   normal-font fore-color-white">
                <h2 class="heading3"><span class=""></span> Important Links</h2>                <ul>
```

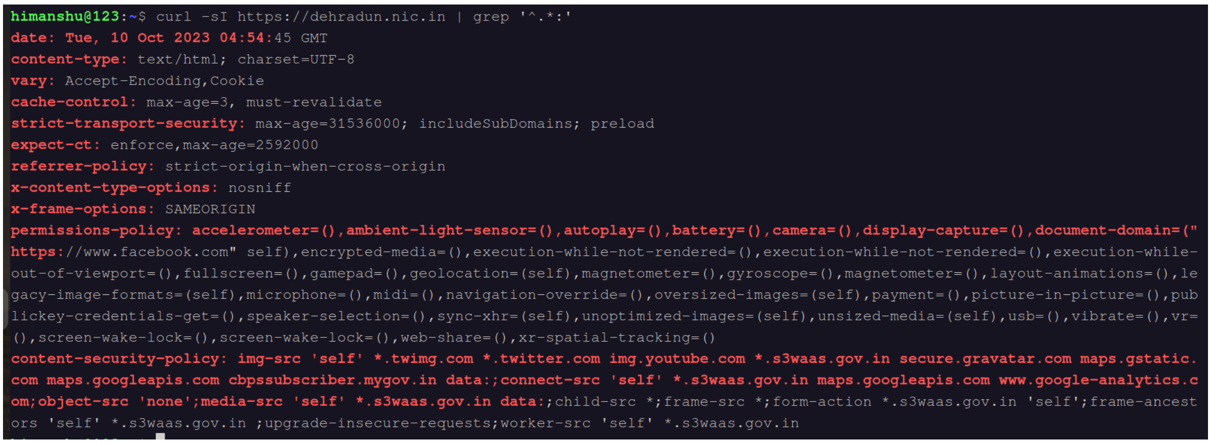


```
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/bower/flexslider/jquery.flexslider-min.js' id='flexs
lider-js'></script>
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/vc_accordion/vc-accordion.* TLSv1.2 (IN), TLS header
, Supplemental data (23):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
min.js' id='vc_accordion_script-js'></script>
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/vc-tta-autoplay/vc-tta-autoplay.min.js' id='vc_tta_a
utoplay_script-js'></script>
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/vc_tabs/vc-tabs.min.js' id='vc_tabs_script-js'></scr
ipt>
        <script>
            jQuery(document).ready(function($){
                $.post({
                    url:ajaxurl,
                    method:'POST',
                    dataType: 'JSON',
                    data:{time: new Date().getTime(),'lang': 'en', action:'s3waas_pll_lang_cookie'},
                    success:function (responseResults) {}
                })
            })
        </script>
</body>
</html>

<!-- Dynamic page generated in 0.973 seconds. -->
<!-- Cached page generated by WP-Super-Cache on 2023-10-05 08:50:10 -->

* TLSv1.2 (IN), TLS header, Supplemental data (23):
* Connection #0 to host dehradun.nic.in left intact
<!-- super cache -->himanshu@123:~$
```

➢ Task 3 . Find common headers:

This command retrieves the headers of the URL and filters out only the header lines.

a. **Command :- curl -sI https://dehradun.nic.in | grep '^.*:'**



```
himanshu@123:~$ curl -sI https://dehradun.nic.in | grep '^.*:'
date: Tue, 10 Oct 2023 04:54:45 GMT
content-type: text/html; charset=UTF-8
vary: Accept-Encoding,Cookie
cache-control: max-age=3, must-revalidate
strict-transport-security: max-age=31536000; includeSubDomains; preload
expect-ct: enforce,max-age=2592000
referrer-policy: strict-origin-when-cross-origin
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
permissions-policy: accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-capture=(),document-domain=("
https://www.facebook.com" self),encrypted-media=(),execution-while-not-rendered=(),execution-while-not-rendered=(),execution-while-
out-of-viewport=(),fullscreen=(),gamepad=(),geolocation=(self),magnetometer=(),gyroscope=(),magnetometer=(),layout-animations=(),le
gacy-image-formats=(self),microphone=(),midi=(),navigation-override=(),oversized-images=(self),payment=(),picture-in-picture=(),pub
lickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unoptimized-images=(self),unsized-media=(self),usb=(),vibrate=(),vr=
(),screen-wake-lock=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=()
content-security-policy: img-src 'self' *.twimg.com *.twitter.com img.youtube.com *.s3waas.gov.in secure.gravatar.com maps.gstatic.
com maps.googleapis.com cbpssubscriber.mygov.in data:;connect-src 'self' *.s3waas.gov.in maps.googleapis.com www.google-analytics.c
om;object-src 'none';media-src 'self' *.s3waas.gov.in data:;child-src *;frame-src *;form-action *.s3waas.gov.in 'self';frame-ancest
ors 'self' *.s3waas.gov.in ;upgrade-insecure-requests;worker-src 'self' *.s3waas.gov.in
```

- **curl -sI https://dehradun.nic.in :** This part of the command uses the curl utility to make an HTTP HEAD request to the specified URL (https://dehradun.nic.in). Here's what each option does:

- **-s:** This option stands for "silent" or "quiet" mode. It suppresses the progress meter and other output information, making the command run in a more quiet or background mode.

- **-I:** This option instructs curl to make a HEAD request instead of the default GET request. A HEAD request is similar to a GET request, but it only asks for the headers of the response, not the actual content. This is useful when you're only interested in the metadata and not the body of the response.

- **|:** This is a pipe operator, and it is used to pass the output of the command on the left side to the command on the right side.

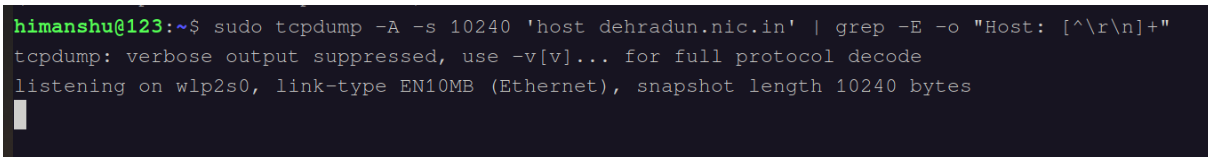
- **grep '^.*:':** This part of the command uses the grep utility to search for lines that match the specified pattern in the input. Here's what the pattern means:

- **^.*::** This is a regular expression pattern. It matches lines that start (^) with any character (.*) followed by a colon (:). In other words, it matches lines that have the format of key-value pairs where the key is followed by a colon.

➢ Task 4. Find requests to non dehradun.nic.in servers:

This command uses tcpdump to capture traffic related to the specified host and then extracts the Host headers to identify requests to other servers.

a. **Command :- tcpdump -A -s 10240 'host dehradun.nic.in' | grep -E -o "Host: [^\r\n]+"**



```
himanshu@123:~$ sudo tcpdump -A -s 10240 'host dehradun.nic.in' | grep -E -o "Host: [^\r\n]+"
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp2s0, link-type EN10MB (Ethernet), snapshot length 10240 bytes
```

- **tcpdump:** This is a packet analyzer that allows the user to display TCP, UDP, and other packets being transmitted or received over a network to which the computer is attached. It's a powerful tool for network troubleshooting and analysis.

- **-A:** This option tells tcpdump to print each packet in ASCII. It is used to display packet contents as text.

- **-s 10240:** This option sets the snaplen parameter to 10240 bytes. Snaplen is the maximum number of bytes to capture for each packet. In this case, it's set to 10240 bytes.

- **'host dehradun.nic.in':** This is a filter expression for tcpdump. It specifies that only packets involving the host with the domain name "dehradun.nic.in" should be captured.

- **|:** This is a pipe symbol, which is used to pass the output of one command as the input to another.

- **grep -E -o "Host:** [^\r\n]+": After capturing the packets using tcpdump, the output is passed to grep. Here's what each part does:

- **grep:** This command is used for searching text using regular expressions.

- **-E:** This option enables extended regular expressions, allowing for more complex pattern matching.

- **-o:** This option tells grep to only print the part of the line that matches the pattern.

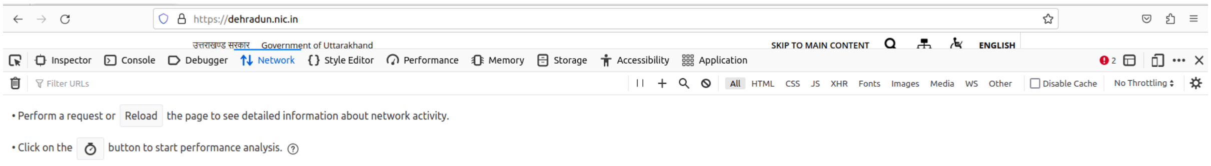
- **"Host: [^\r\n]+":** This is the regular expression pattern. It searches for lines containing "Host:" followed by one or more characters that are not carriage return or newline characters. The [^\r\n]+ part matches one or more characters that are not carriage return or newline.

- **The task I have here is through the graphical user interface (GUI).**

➢ Task 1. List of non-GET requests and determine their request body:

a. Inspect Network Traffic:

- Open the Developer Tools in your browser (usually by pressing Ctrl+Shift+I or Cmd+Option+I).
- Navigate to the "Network" tab.

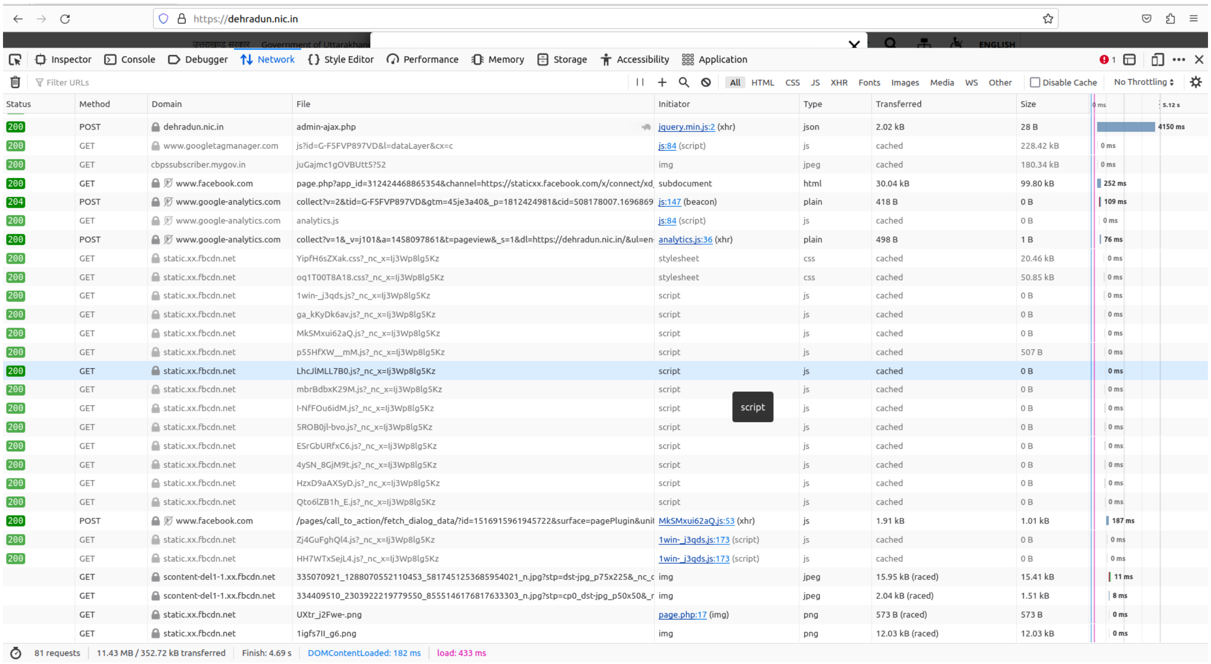


• Perform a request or Reload the page to see detailed information about network activity.

• Click on the button to start performance analysis.

b. Filter Requests:

- Reload the page (Ctrl+R or Cmd+R).
- Look for the requests that are not of type GET (POST, PUT, etc.).

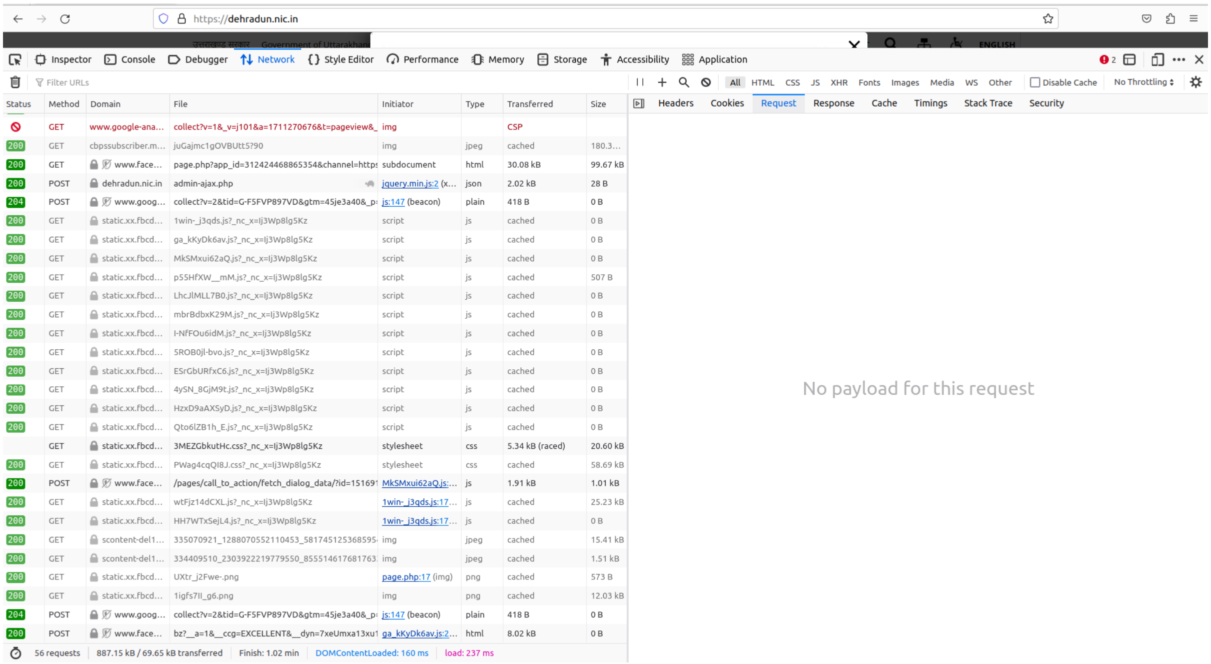


Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms 5.12 s
200	POST	dehradun.nic.in	admin-ajax.php	jquery.min.js:2 (xhr)	json	2.02 kB	28 B	4150 ms
200	GET	www.googletagmanager.com	js?id=G-F5FVP897VD&l=dataLayer&cx=c	js:84 (script)	js	cached	228.42 kB	0 ms
200	GET	cbpssubscriber.mygov.in	juGajmc1gOVBUtt5?52	img	jpeg	cached	180.34 kB	0 ms
200	GET	www.facebook.com	page.php?app_id=312424468865354&channel=https://staticxx.facebook.com/x/connect/xd_	subdocument	html	30.04 kB	99.80 kB	252 ms
204	POST	www.google-analytics.com	collect?v=2&tid=G-F5FVP897VD&gtm=45je3a40&_p=1812424981&cid=508178007.1696869	js:147 (beacon)	plain	418 B	0 B	109 ms
200	GET	www.google-analytics.com	analytics.js	js:84 (script)	js	cached	0 B	0 ms
200	POST	www.google-analytics.com	collect?v=1&_v=j101&a=1458097861&t=pageview&_s=1&dl=https://dehradun.nic.in/&ul=en-	analytics.js:36 (xhr)	plain	498 B	1 B	76 ms
200	GET	static.xx.fbcdn.net	YipfH6sZXak.css?_nc_x=Ij3Wp8lg5Kz	stylesheet	css	cached	20.46 kB	0 ms
200	GET	static.xx.fbcdn.net	oq1T00T8A18.css?_nc_x=Ij3Wp8lg5Kz	stylesheet	css	cached	50.85 kB	0 ms
200	GET	static.xx.fbcdn.net	1win-_j3qds.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B	0 ms
200	GET	static.xx.fbcdn.net	ga_kKyDk6av.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B	0 ms
200	GET	static.xx.fbcdn.net	MkSMxui62aQ.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B	0 ms
200	GET	static.xx.fbcdn.net	p55HfXW__mM.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	507 B	0 ms
200	GET	static.xx.fbcdn.net	LhcJlMLL7B0.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B	0 ms
200	GET	static.xx.fbcdn.net	mbrBdbxK29M.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B	0 ms
200	GET	static.xx.fbcdn.net	I-NfFOu6idM.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B	0 ms
200	GET	static.xx.fbcdn.net	5ROB0jl-bvo.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B	0 ms
200	GET	static.xx.fbcdn.net	ESrGbURfxC6.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B	0 ms
200	GET	static.xx.fbcdn.net	4ySN_8GjM9t.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B	0 ms
200	GET	static.xx.fbcdn.net	HzxD9aAXSyD.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B	0 ms
200	GET	static.xx.fbcdn.net	Qto6lZB1h_E.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B	0 ms
200	POST	www.facebook.com	/pages/call_to_action/fetch_dialog_data/?id=1516915961945722&surface=pagePlugin&unit	MkSMxui62aQ.js:53 (xhr)	js	1.91 kB	1.01 kB	187 ms
200	GET	static.xx.fbcdn.net	Zj4GuFghQl4.js?_nc_x=Ij3Wp8lg5Kz	1win-_j3qds.js:173 (script)	js	cached	0 B	0 ms
200	GET	static.xx.fbcdn.net	HH7WTxSejL4.js?_nc_x=Ij3Wp8lg5Kz	1win-_j3qds.js:173 (script)	js	cached	0 B	0 ms
	GET	scontent-del1-1.xx.fbcdn.net	335070921_1288070552110453_5817451253685954021_n.jpg?stp=dst-jpg_p75x225&_nc_c	img	jpeg	15.95 kB (raced)	15.41 kB	11 ms
	GET	scontent-del1-1.xx.fbcdn.net	334409510_2303922219779550_8555146176817633303_n.jpg?stp=cp0_dst-jpg_p50x50&_r	img	jpeg	2.04 kB (raced)	1.51 kB	8 ms
	GET	static.xx.fbcdn.net	UXtr_j2Fwe-.png	page.php:17 (img)	png	573 B (raced)	573 B	0 ms
	GET	static.xx.fbcdn.net	1igfs7II_g6.png	img	png	12.03 kB (raced)	12.03 kB	0 ms

81 requests | 11.43 MB / 352.72 kB transferred | Finish: 4.69 s | DOMContentLoaded: 182 ms | load: 433 ms

c. View Request Body:

- Click on the non-GET request.
- Navigate to the "Request" or "Headers" tab to view the request body.



https://dehradun.nic.in

Status	Method	Domain	File	Initiator	Type	Transferred	Size
⊘	GET	www.google-ana...	collect?v=1&_v=j101&a=1711270676&t=pageview&_	img		CSP	
200	GET	cbpssubscriber.m...	juGajmc1gOVBUtt5?90	img	jpeg	cached	180.3...
200	GET	www.face...	page.php?app_id=312424468865354&channel=https	subdocument	html	30.08 kB	99.67 kB
200	POST	dehradun.nic.in	admin-ajax.php	jquery.min.js:2 (x...	json	2.02 kB	28 B
204	POST	www.goog...	collect?v=2&tid=G-F5FVP897VD&gtm=45je3a40&_p:	js:147 (beacon)	plain	418 B	0 B
200	GET	static.xx.fbcd...	1win-_j3qds.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.fbcd...	ga_kKyDk6av.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.fbcd...	MkSMxui62aQ.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.fbcd...	p55HfXW__mM.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	507 B
200	GET	static.xx.fbcd...	LhcJlMLL7B0.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.fbcd...	mbrBdbxK29M.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.fbcd...	I-NfFOu6idM.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.fbcd...	5ROB0jl-bvo.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.fbcd...	ESrGbURfxC6.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.fbcd...	4ySN_8GjM9t.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.fbcd...	HzxD9aAXSyD.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.fbcd...	Qto6lZB1h_E.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
	GET	static.xx.fbcd...	3MEZGbkutHc.css?_nc_x=Ij3Wp8lg5Kz	stylesheet	css	5.34 kB (raced)	20.60 kB
200	GET	static.xx.fbcd...	PWag4cqQI8J.css?_nc_x=Ij3Wp8lg5Kz	stylesheet	css	cached	58.69 kB
200	POST	www.face...	/pages/call_to_action/fetch_dialog_data/?id=151691	MkSMxui62aQ.js:...	js	1.91 kB	1.01 kB
200	GET	static.xx.fbcd...	wtFjz14dCXL.js?_nc_x=Ij3Wp8lg5Kz	1win-_j3qds.js:17...	js	cached	25.23 kB
200	GET	static.xx.fbcd...	HH7WTxSejL4.js?_nc_x=Ij3Wp8lg5Kz	1win-_j3qds.js:17...	js	cached	0 B
200	GET	scontent-del1...	335070921_1288070552110453_581745125368595	img	jpeg	cached	15.41 kB
200	GET	scontent-del1...	334409510_2303922219779550_855514617681763	img	jpeg	cached	1.51 kB
200	GET	static.xx.fbcd...	UXtr_j2Fwe-.png	page.php:17 (img)	png	cached	573 B
200	GET	static.xx.fbcd...	1igfs7II_g6.png	img	png	cached	12.03 kB
204	POST	www.goog...	collect?v=2&tid=G-F5FVP897VD&gtm=45je3a40&_p:	js:147 (beacon)	plain	418 B	0 B
200	POST	www.face...	bz?__a=1&__ccg=EXCELLENT&__dyn=7xeUmxa13xu1	ga_kKyDk6av.js:2...	html	8.02 kB	0 B

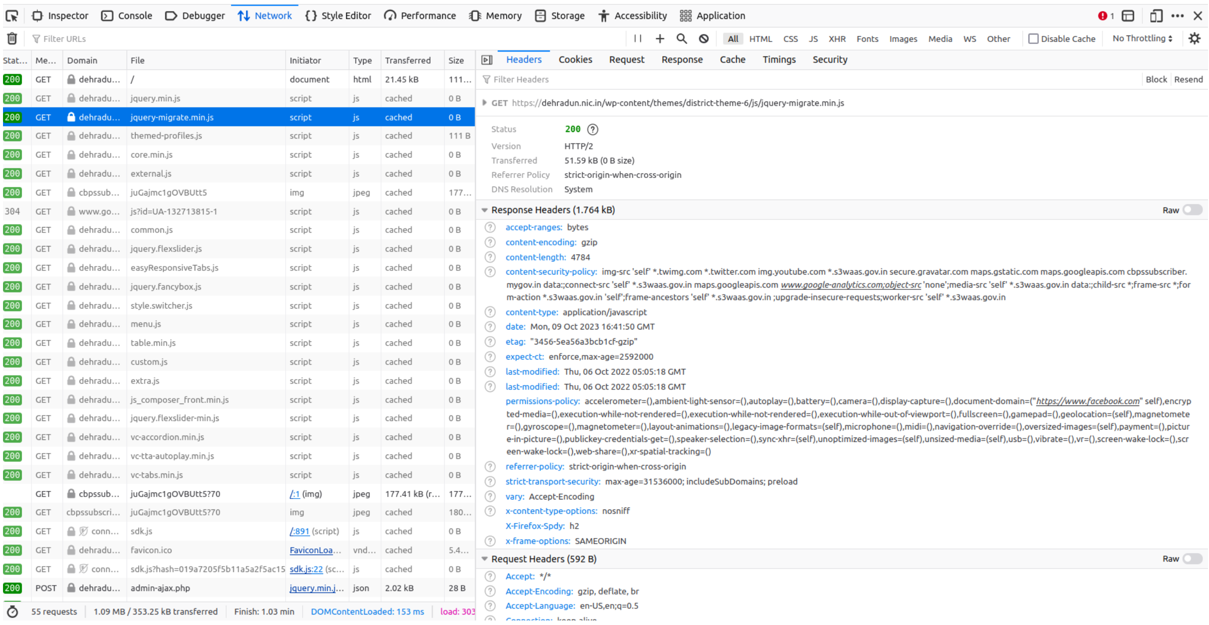
56 requests | 887.15 kB / 69.65 kB transferred | Finish: 1.02 min | DOMContentLoaded: 160 ms | load: 237 ms

No payload for this request

➢ Task 2. List of non-200 responses:

a. Inspect Network Traffic:

- Follow the steps mentioned in the first task to open Developer Tools and navigate to the "Network" tab.



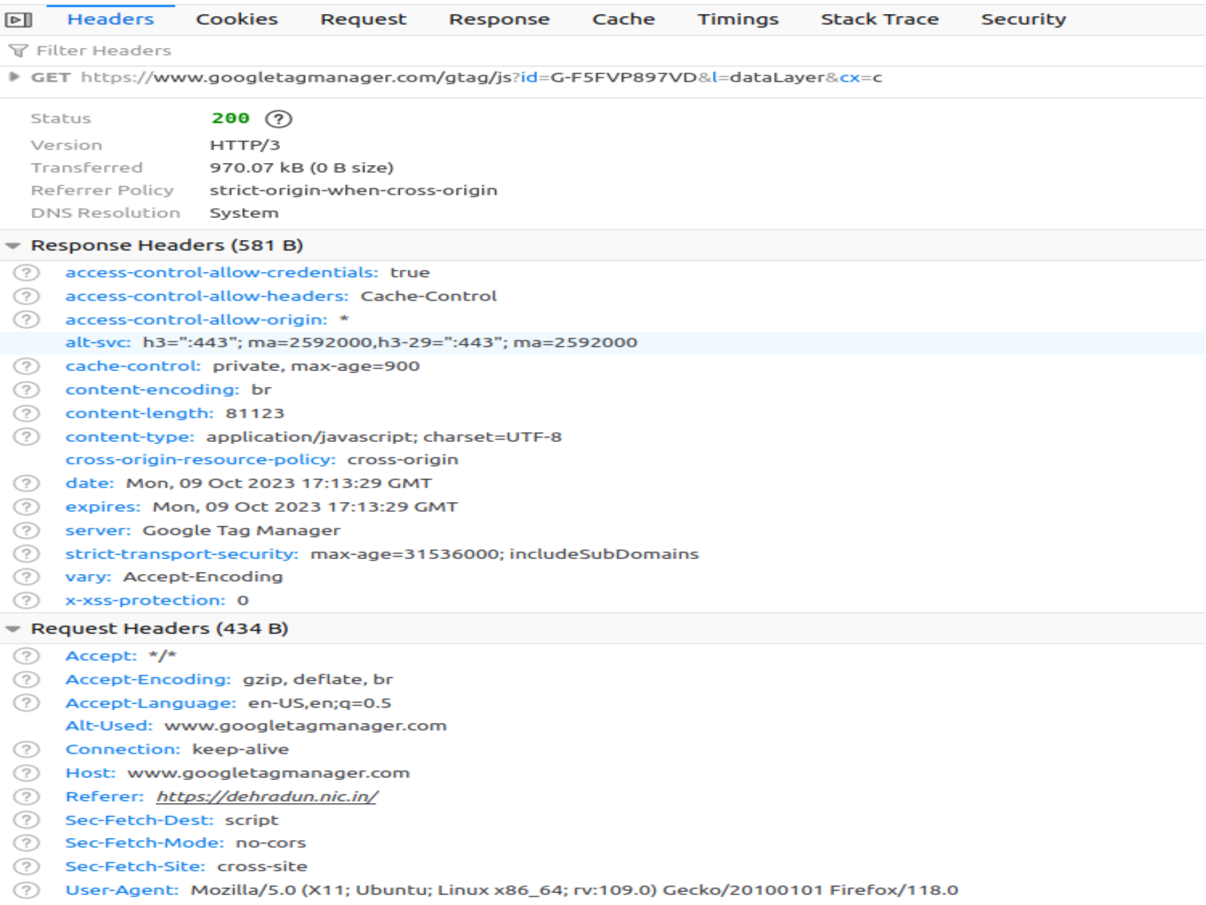
Stat…	Me…	Domain	File	Initiator	Type	Transferred	Size
200	GET	dehradu…	/	document	html	21.45 kB	111…
200	GET	dehradu…	jquery.min.js	script	js	cached	0 B
200	GET	dehradu…	jquery-migrate.min.js	script	js	cached	0 B
200	GET	dehradu…	themed-profiles.js	script	js	cached	111 B
200	GET	dehradu…	core.min.js	script	js	cached	0 B
200	GET	dehradu…	external.js	script	js	cached	0 B
200	GET	cbpssub…	juGajmc1gOVBUtt5	img	jpeg	cached	177…
304	GET	www.go…	js?id=UA-132713815-1	script	js	cached	0 B
200	GET	dehradu…	common.js	script	js	cached	0 B
200	GET	dehradu…	jquery.flexslider.js	script	js	cached	0 B
200	GET	dehradu…	easyResponsiveTabs.js	script	js	cached	0 B
200	GET	dehradu…	jquery.fancybox.js	script	js	cached	0 B
200	GET	dehradu…	style.switcher.js	script	js	cached	0 B
200	GET	dehradu…	menu.js	script	js	cached	0 B
200	GET	dehradu…	table.min.js	script	js	cached	0 B
200	GET	dehradu…	custom.js	script	js	cached	0 B
200	GET	dehradu…	extra.js	script	js	cached	0 B
200	GET	dehradu…	js_composer_front.min.js	script	js	cached	0 B
200	GET	dehradu…	jquery.flexslider-min.js	script	js	cached	0 B
200	GET	dehradu…	vc-accordion.min.js	script	js	cached	0 B
200	GET	dehradu…	vc-tta-autoplay.min.js	script	js	cached	0 B
200	GET	dehradu…	vc-tabs.min.js	script	js	cached	0 B
	GET	cbpssub…	juGajmc1gOVBUtt5?70	/:1 (img)	jpeg	177.41 kB (r…	177…
200	GET	cbpssubscri…	juGajmc1gOVBUtt5?70	img	jpeg	cached	180…
200	GET	conn…	sdk.js	/:891 (script)	js	cached	0 B
200	GET	dehradu…	favicon.ico	FaviconLoa…	vnd…	cached	5.4…
200	GET	conn…	sdk.js?hash=019a7205f5b11a5a2f5ac15	sdk.js:22 (sc…	js	cached	0 B
200	POST	dehradu…	admin-ajax.php	jquery.min.j…	json	2.02 kB	28 B

55 requests | 1.09 MB / 353.25 kB transferred | Finish: 1.03 min | DOMContentLoaded: 153 ms | load: 303

```
GET https://dehradun.nic.in/wp-content/themes/district-theme-6/js/jquery-migrate.min.js

Status              200
Version             HTTP/2
Transferred         51.59 kB (0 B size)
Referrer Policy     strict-origin-when-cross-origin
DNS Resolution      System

Response Headers (1.764 kB)                                                    Raw
accept-ranges: bytes
content-encoding: gzip
content-length: 4784
content-security-policy: img-src 'self' *.twimg.com *.twitter.com img.youtube.com *.s3waas.gov.in secure.gravatar.com maps.gstatic.com maps.googleapis.com cbpssubscriber.mygov.in data:;connect-src 'self' *.s3waas.gov.in maps.googleapis.com www.google-analytics.com;object-src 'none';media-src 'self' *.s3waas.gov.in data:;child-src *;frame-src *;form-action *.s3waas.gov.in 'self';frame-ancestors 'self' *.s3waas.gov.in ;upgrade-insecure-requests;worker-src 'self' *.s3waas.gov.in
content-type: application/javascript
date: Mon, 09 Oct 2023 16:41:50 GMT
etag: "3456-5ea56a3bcb1cf-gzip"
expect-ct: enforce,max-age=2592000
last-modified: Thu, 06 Oct 2022 05:05:18 GMT
last-modified: Thu, 06 Oct 2022 05:05:18 GMT
permissions-policy: accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-capture=(),document-domain=("https://www.facebook.com" self),encrypted-media=(),execution-while-not-rendered=(),execution-while-not-rendered=(),execution-while-out-of-viewport=(),fullscreen=(),gamepad=(),geolocation=(self),magnetometer=(),gyroscope=(),magnetometer=(),layout-animations=(),legacy-image-formats=(self),microphone=(),midi=(),navigation-override=(),oversized-images=(self),payment=(),picture-in-picture=(),publickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unoptimized-images=(self),unsized-media=(self),usb=(),vibrate=(),vr=(),screen-wake-lock=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=()
referrer-policy: strict-origin-when-cross-origin
strict-transport-security: max-age=31536000; includeSubDomains; preload
vary: Accept-Encoding
x-content-type-options: nosniff
X-Firefox-Spdy: h2
x-frame-options: SAMEORIGIN

Request Headers (592 B)                                                        Raw
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
```

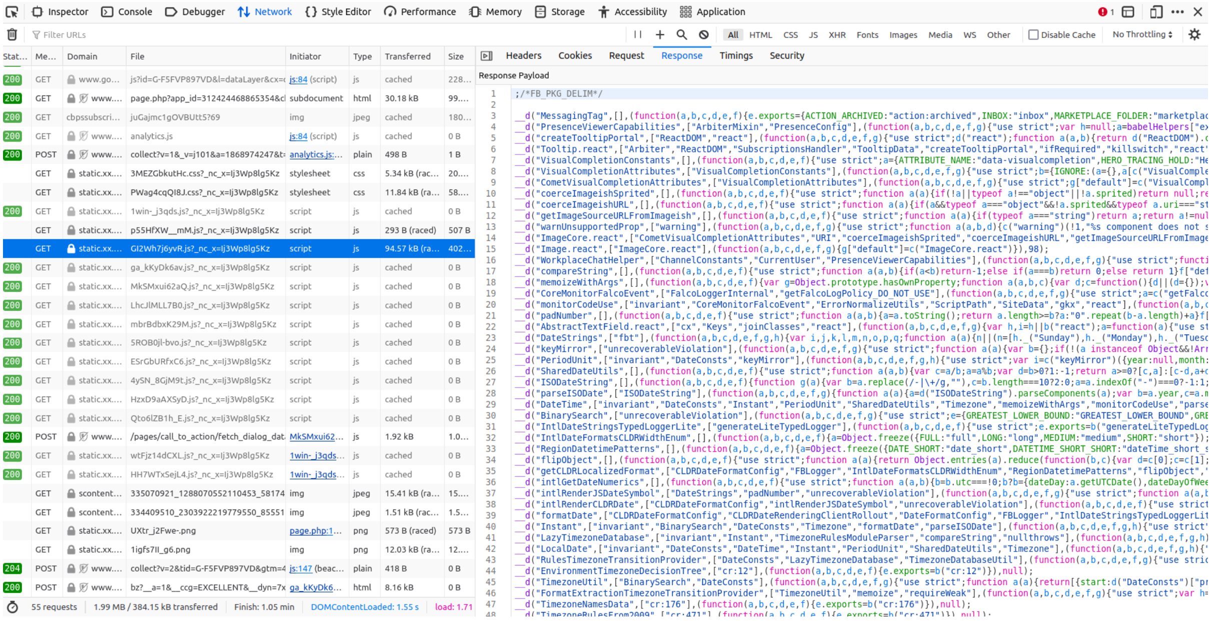
b. Filter Responses:

- Look for responses with a status code other than 200.



```
GET https://www.googletagmanager.com/gtag/js?id=G-F5FVP897VD&l=dataLayer&cx=c

Status              200
Version             HTTP/3
Transferred         970.07 kB (0 B size)
Referrer Policy     strict-origin-when-cross-origin
DNS Resolution      System

Response Headers (581 B)
access-control-allow-credentials: true
access-control-allow-headers: Cache-Control
access-control-allow-origin: *
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
cache-control: private, max-age=900
content-encoding: br
content-length: 81123
content-type: application/javascript; charset=UTF-8
cross-origin-resource-policy: cross-origin
date: Mon, 09 Oct 2023 17:13:29 GMT
expires: Mon, 09 Oct 2023 17:13:29 GMT
server: Google Tag Manager
strict-transport-security: max-age=31536000; includeSubDomains
vary: Accept-Encoding
x-xss-protection: 0

Request Headers (434 B)
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Alt-Used: www.googletagmanager.com
Connection: keep-alive
Host: www.googletagmanager.com
Referer: https://dehradun.nic.in/
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/118.0
```

- Click on the response to view details in the "Response" or "Headers" tab.



Stat…	Me…	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.go…	js?id=G-F5FVP897VD&l=dataLayer&cx=c	js:84 (script)	js	cached	228…
200	GET	www.…	page.php?app_id=312424468865354&cl	subdocument	html	30.18 kB	99.…
200	GET	cbpssubscri…	juGajmc1gOVBUtt5?69	img	jpeg	cached	180…
200	GET	www.…	analytics.js	js:84 (script)	js	cached	0 B
200	POST	www.…	collect?v=1&_v=j101&a=1868974247&t=	analytics.js:…	plain	498 B	1 B
	GET	static.xx.…	3MEZGbkutHc.css?_nc_x=Ij3Wp8lg5Kz	stylesheet	css	5.34 kB (rac…	20.…
	GET	static.xx.…	PWag4cqQI8J.css?_nc_x=Ij3Wp8lg5Kz	stylesheet	css	11.84 kB (ra…	58.…
200	GET	static.xx.…	1win-_j3qds.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
	GET	static.xx.…	p55HfXW__mM.js?_nc_x=Ij3Wp8lg5Kz	script	js	293 B (raced)	507 B
	GET	static.xx.…	GI2Wh7j6yvR.js?_nc_x=Ij3Wp8lg5Kz	script	js	94.57 kB (ra…	402…
200	GET	static.xx.…	ga_kKyDk6av.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.…	MkSMxui62aQ.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.…	LhcJlMLL7B0.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.…	mbrBdbxK29M.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.…	5ROB0jl-bvo.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.…	ESrGbURfxC6.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.…	4ySN_8GjM9t.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.…	HzxD9aAXSyD.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	GET	static.xx.…	Qto6lZB1h_E.js?_nc_x=Ij3Wp8lg5Kz	script	js	cached	0 B
200	POST	www.…	/pages/call_to_action/fetch_dialog_dat:	MkSMxui62…	js	1.92 kB	1.0…
200	GET	static.xx.…	wtFjz14dCXL.js?_nc_x=Ij3Wp8lg5Kz	1win-_j3qds…	js	cached	0 B
200	GET	static.xx.…	HH7WTxSejL4.js?_nc_x=Ij3Wp8lg5Kz	1win-_j3qds…	js	cached	0 B
	GET	scontent…	335070921_1288070552110453_58174	img	jpeg	15.41 kB (ra…	15.…
	GET	scontent…	334409510_2303922219779550_85551	img	jpeg	1.51 kB (rac…	1.5…
	GET	static.xx.…	UXtr_j2Fwe-.png	page.php:1…	png	573 B (raced)	573 B
	GET	static.xx.…	1igfs7II_g6.png	img	png	12.03 kB (ra…	12.…
204	POST	www.…	collect?v=2&tid=G-F5FVP897VD&gtm=4	js:147 (beac…	plain	418 B	0 B
200	POST	www.…	bz?__a=1&__ccg=EXCELLENT&__dyn=7x	ga_kKyDk6…	html	8.16 kB	0 B

55 requests | 1.99 MB / 384.15 kB transferred | Finish: 1.05 min | DOMContentLoaded: 1.55 s | load: 1.71

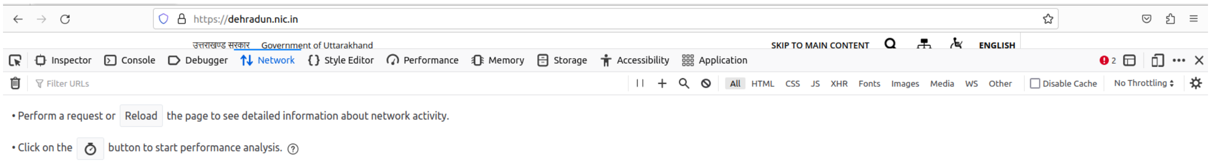
Response Payload

```
;/*FB_PKG_DELIM*/

__d("MessagingTag",[],(function(a,b,c,d,e,f){e.exports={ACTION_ARCHIVED:"action:archived",INBOX:"inbox",MARKETPLACE_FOLDER:"marketplac
__d("PresenceViewerCapabilities",["ArbiterMixin","PresenceConfig"],(function(a,b,c,d,e,f,g){"use strict";var h=null;a=babelHelpers["ex
__d("createTooltipPortal",["ReactDOM","react"],(function(a,b,c,d,e,f,g){"use strict";d("react");function a(a,b){return d("ReactDOM").c
__d("Tooltip.react",["Arbiter","ReactDOM","SubscriptionsHandler","TooltipData","createTooltipPortal","ifRequired","killswitch","react"
__d("VisualCompletionConstants",[],(function(a,b,c,d,e,f){"use strict";a={ATTRIBUTE_NAME:"data-visualcompletion",HERO_TRACING_HOLD:"He
__d("VisualCompletionAttributes",["VisualCompletionConstants"],(function(a,b,c,d,e,f,g){"use strict";b={IGNORE:(a={},a[c("VisualComple
__d("CometVisualCompletionAttributes",["VisualCompletionAttributes"],(function(a,b,c,d,e,f,g){"use strict";g["default"]=c("VisualCompl
__d("coerceImageishSprited",[],(function(a,b,c,d,e,f){"use strict";function a(a){if(!a||typeof a!=="object"||!a.sprited)return null;re
__d("coerceImageishURL",[],(function(a,b,c,d,e,f){"use strict";function a(a){if(a&&typeof a==="object"&&!a.sprited&&typeof a.uri==="st
__d("getImageSourceURLFromImageish",[],(function(a,b,c,d,e,f){"use strict";function a(a){if(typeof a==="string")return a;return a!=nul
__d("warnUnsupportedProp",["warning"],(function(a,b,c,d,e,f,g){"use strict";function a(a,b,d){c("warning")(!1,"%s component does not s
__d("ImageCore.react",["CometVisualCompletionAttributes","URI","coerceImageishSprited","coerceImageishURL","getImageSourceURLFromImage
__d("Image.react",["ImageCore.react"],(function(a,b,c,d,e,f,g){g["default"]=c("ImageCore.react")}),98);
__d("WorkplaceChatHelper",["ChannelConstants","CurrentUser","PresenceViewerCapabilities"],(function(a,b,c,d,e,f,g){"use strict";functi
__d("compareString",[],(function(a,b,c,d,e,f){"use strict";function a(a,b){if(a<b)return-1;else if(a===b)return 0;else return 1}f["def
__d("memoizeWithArgs",[],(function(a,b,c,d,e,f){var g=Object.prototype.hasOwnProperty;function a(a,b,c){var d;c=function(){d||(d={});v
__d("CoreMonitorFalcoEvent",["FalcoLoggerInternal","getFalcoLogPolicy_DO_NOT_USE"],(function(a,b,c,d,e,f,g){"use strict";a=c("getFalco
__d("monitorCodeUse",["invariant","CoreMonitorFalcoEvent","ErrorNormalizeUtils","ScriptPath","SiteData","gkx","react"],(function(a,b,c
__d("padNumber",[],(function(a,b,c,d,e,f){"use strict";function a(a,b){a=a.toString();return a.length>=b?a:"0".repeat(b-a.length)+a}f[
__d("AbstractTextField.react",["cx","Keys","joinClasses","react"],(function(a,b,c,d,e,f,g){var h,i=h||b("react");a=function(a){"use st
__d("DateStrings",["fbt"],(function(a,b,c,d,e,f,g,h){var i,j,k,l,m,n,o,p,q;function a(a){n||(n=[h._("Sunday"),h._("Monday"),h._("Tuesc
__d("keyMirror",["unrecoverableViolation"],(function(a,b,c,d,e,f,g){"use strict";function a(a){var b={};if(!(a instanceof Object&&!Arr
__d("PeriodUnit",["invariant","DateConsts","keyMirror"],(function(a,b,c,d,e,f,g,h){"use strict";var i=c("keyMirror")({year:null,month:
__d("SharedDateUtils",[],(function(a,b,c,d,e,f){"use strict";function a(a,b){var c=a/b;a=a%b;var d=b>0?1:-1;return a>=0?[c,a]:[c-d,a+c
__d("ISODateString",[],(function(a,b,c,d,e,f){function g(a){var b=a.replace(/-|\+/g,""),c=b.length===10?2:0;a=a.indexOf("-")===0?-1:1;
__d("parseISODate",["ISODateString"],(function(a,b,c,d,e,f,g){function a(a){a=d("ISODateString").parseComponents(a);var b=a.year,c=a.m
__d("DateTime",["invariant","DateConsts","Instant","PeriodUnit","SharedDateUtils","Timezone","memoizeWithArgs","monitorCodeUse","parse
__d("BinarySearch",["unrecoverableViolation"],(function(a,b,c,d,e,f,g){"use strict";e={GREATEST_LOWER_BOUND:"GREATEST_LOWER_BOUND",GRE
__d("IntlDateStringsTypedLoggerLite",["generateLiteTypedLogger"],(function(a,b,c,d,e,f){"use strict";e.exports=b("generateLiteTypedLog
__d("IntlDateFormatsCLDRWidthEnum",[],(function(a,b,c,d,e,f){a=Object.freeze({FULL:"full",LONG:"long",MEDIUM:"medium",SHORT:"short"});
__d("RegionDatetimePatterns",[],(function(a,b,c,d,e,f){a=Object.freeze({DATE_SHORT:"date_short",DATETIME_SHORT_SHORT:"dateTime_short_s
__d("flipObject",[],(function(a,b,c,d,e,f){"use strict";function a(a){return Object.entries(a).reduce(function(b,c){var d=c[0];c=c[1];
__d("getCLDRLocalizedFormat",["CLDRDateFormatConfig","FBLogger","IntlDateFormatsCLDRWidthEnum","RegionDatetimePatterns","flipObject","
__d("intlGetDateNumerics",[],(function(a,b,c,d,e,f){"use strict";function a(a,b){b=b.utc===!0;b?b={dateDay:a.getUTCDate(),dateDayOfWee
__d("intlRenderJSDateSymbol",["DateStrings","padNumber","unrecoverableViolation"],(function(a,b,c,d,e,f,g){"use strict";function a(a,b
__d("intlRenderCLDRDate",["CLDRDateFormatConfig","intlRenderJSDateSymbol","unrecoverableViolation"],(function(a,b,c,d,e,f){"use strict
__d("formatDate",["CLDRDateFormatConfig","CLDRDateRenderingClientRollout","DateFormatConfig","FBLogger","IntlDateStringsTypedLoggerLit
__d("Instant",["invariant","BinarySearch","DateConsts","Timezone","formatDate","parseISODate"],(function(a,b,c,d,e,f,g,h){"use strict"
__d("LazyTimezoneDatabase",["invariant","Instant","TimezoneRulesModuleParser","compareString","nullthrows"],(function(a,b,c,d,e,f,g,h)
__d("LocalDate",["invariant","DateConsts","DateTime","Instant","PeriodUnit","SharedDateUtils","Timezone"],(function(a,b,c,d,e,f,g,h){"
__d("RulesTimezoneTransitionProvider",["DateConsts","LazyTimezoneDatabase","TimezoneDatabaseUtil"],(function(a,b,c,d,e,f,g){"use stric
__d("EnvironmentTimezoneDecisionTree",["cr:12"],(function(a,b,c,d,e,f){e.exports=b("cr:12")}),null);
__d("TimezoneUtil",["BinarySearch","DateConsts"],(function(a,b,c,d,e,f,g){"use strict";function a(a){return[{start:d("DateConsts")["pr
__d("FormatExtractionTimezoneTransitionProvider",["TimezoneUtil","memoize","requireWeak"],(function(a,b,c,d,e,f,g){"use strict";var h=
__d("TimezoneNamesData",["cr:176"],(function(a,b,c,d,e,f){e.exports=b("cr:176")}),null);
__d("TimezoneRulesFrom2009",["cr:471"],(function(a,b,c,d,e,f){e.exports=b("cr:471")}),null);
```

➢ Task 3. Find common headers in all requests:

a. Inspect Network Traffic:

- Follow the steps mentioned in the first task to open Developer Tools and navigate to the "Network" tab.



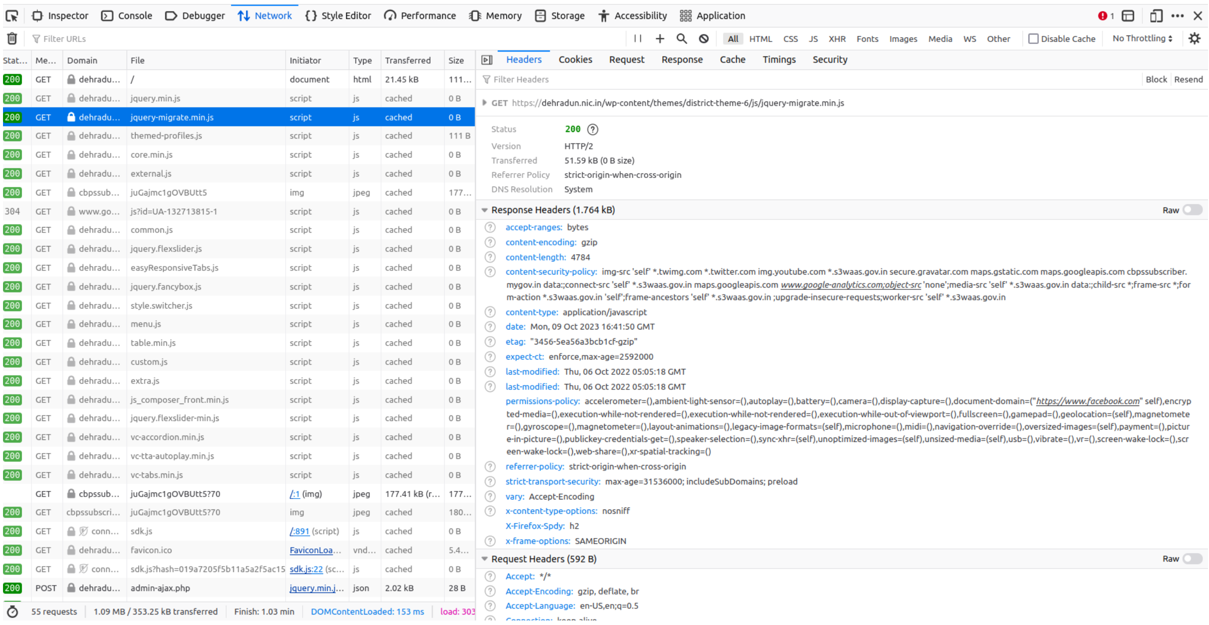
• Perform a request or Reload the page to see detailed information about network activity.

• Click on the button to start performance analysis.

b. View Headers:

- Click on any request.

- Look for the "Headers" tab.



Stat…	Me…	Domain	File	Initiator	Type	Transferred	Size
200	GET	dehradu…	/	document	html	21.45 kB	111…
200	GET	dehradu…	jquery.min.js	script	js	cached	0 B
200	GET	dehradu…	jquery-migrate.min.js	script	js	cached	0 B
200	GET	dehradu…	themed-profiles.js	script	js	cached	111 B
200	GET	dehradu…	core.min.js	script	js	cached	0 B
200	GET	dehradu…	external.js	script	js	cached	0 B
200	GET	cbpssub…	juGajmc1gOVBUtt5	img	jpeg	cached	177…
304	GET	www.go…	js?id=UA-132713815-1	script	js	cached	0 B
200	GET	dehradu…	common.js	script	js	cached	0 B
200	GET	dehradu…	jquery.flexslider.js	script	js	cached	0 B
200	GET	dehradu…	easyResponsiveTabs.js	script	js	cached	0 B
200	GET	dehradu…	jquery.fancybox.js	script	js	cached	0 B
200	GET	dehradu…	style.switcher.js	script	js	cached	0 B
200	GET	dehradu…	menu.js	script	js	cached	0 B
200	GET	dehradu…	table.min.js	script	js	cached	0 B
200	GET	dehradu…	custom.js	script	js	cached	0 B
200	GET	dehradu…	extra.js	script	js	cached	0 B
200	GET	dehradu…	js_composer_front.min.js	script	js	cached	0 B
200	GET	dehradu…	jquery.flexslider-min.js	script	js	cached	0 B
200	GET	dehradu…	vc-accordion.min.js	script	js	cached	0 B
200	GET	dehradu…	vc-tta-autoplay.min.js	script	js	cached	0 B
200	GET	dehradu…	vc-tabs.min.js	script	js	cached	0 B
	GET	cbpssub…	juGajmc1gOVBUtt5?70	/:1 (img)	jpeg	177.41 kB (r…	177…
200	GET	cbpssubscri…	juGajmc1gOVBUtt5?70	img	jpeg	cached	180…
200	GET	conn…	sdk.js	/:891 (script)	js	cached	0 B
200	GET	dehradu…	favicon.ico	FaviconLoa…	vnd…	cached	5.4…
200	GET	conn…	sdk.js?hash=019a7205f5b11a5a2f5ac15	sdk.js:22 (sc…	js	cached	0 B
200	POST	dehradu…	admin-ajax.php	jquery.min.j…	json	2.02 kB	28 B

55 requests | 1.09 MB / 353.25 kB transferred | Finish: 1.03 min | DOMContentLoaded: 153 ms | load: 303

GET https://dehradun.nic.in/wp-content/themes/district-theme-6/js/jquery-migrate.min.js

Status 200

Version HTTP/2

Transferred 51.59 kB (0 B size)

Referrer Policy strict-origin-when-cross-origin

DNS Resolution System

Response Headers (1.764 kB)

accept-ranges: bytes

content-encoding: gzip

content-length: 4784

content-security-policy: img-src 'self' *.twimg.com *.twitter.com img.youtube.com *.s3waas.gov.in secure.gravatar.com maps.gstatic.com maps.googleapis.com cbpssubscriber.mygov.in data:;connect-src 'self' *.s3waas.gov.in maps.googleapis.com www.google-analytics.com;object-src 'none';media-src 'self' *.s3waas.gov.in data:;child-src *;frame-src *;form-action *.s3waas.gov.in 'self';frame-ancestors 'self' *.s3waas.gov.in ;upgrade-insecure-requests;worker-src 'self' *.s3waas.gov.in

content-type: application/javascript

date: Mon, 09 Oct 2023 16:41:50 GMT

etag: "3456-5ea56a3bcb1cf-gzip"

expect-ct: enforce,max-age=2592000

last-modified: Thu, 06 Oct 2022 05:05:18 GMT

last-modified: Thu, 06 Oct 2022 05:05:18 GMT

permissions-policy: accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-capture=(),document-domain=("https://www.facebook.com" self),encrypted-media=(),execution-while-not-rendered=(),execution-while-not-rendered=(),execution-while-out-of-viewport=(),fullscreen=(),gamepad=(),geolocation=(self),magnetometer=(),gyroscope=(),magnetometer=(),layout-animations=(),legacy-image-formats=(self),microphone=(),midi=(),navigation-override=(),oversized-images=(self),payment=(),picture-in-picture=(),publickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unoptimized-images=(self),unsized-media=(self),usb=(),vibrate=(),vr=(),screen-wake-lock=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=()

referrer-policy: strict-origin-when-cross-origin

strict-transport-security: max-age=31536000; includeSubDomains; preload

vary: Accept-Encoding

x-content-type-options: nosniff

X-Firefox-Spdy: h2

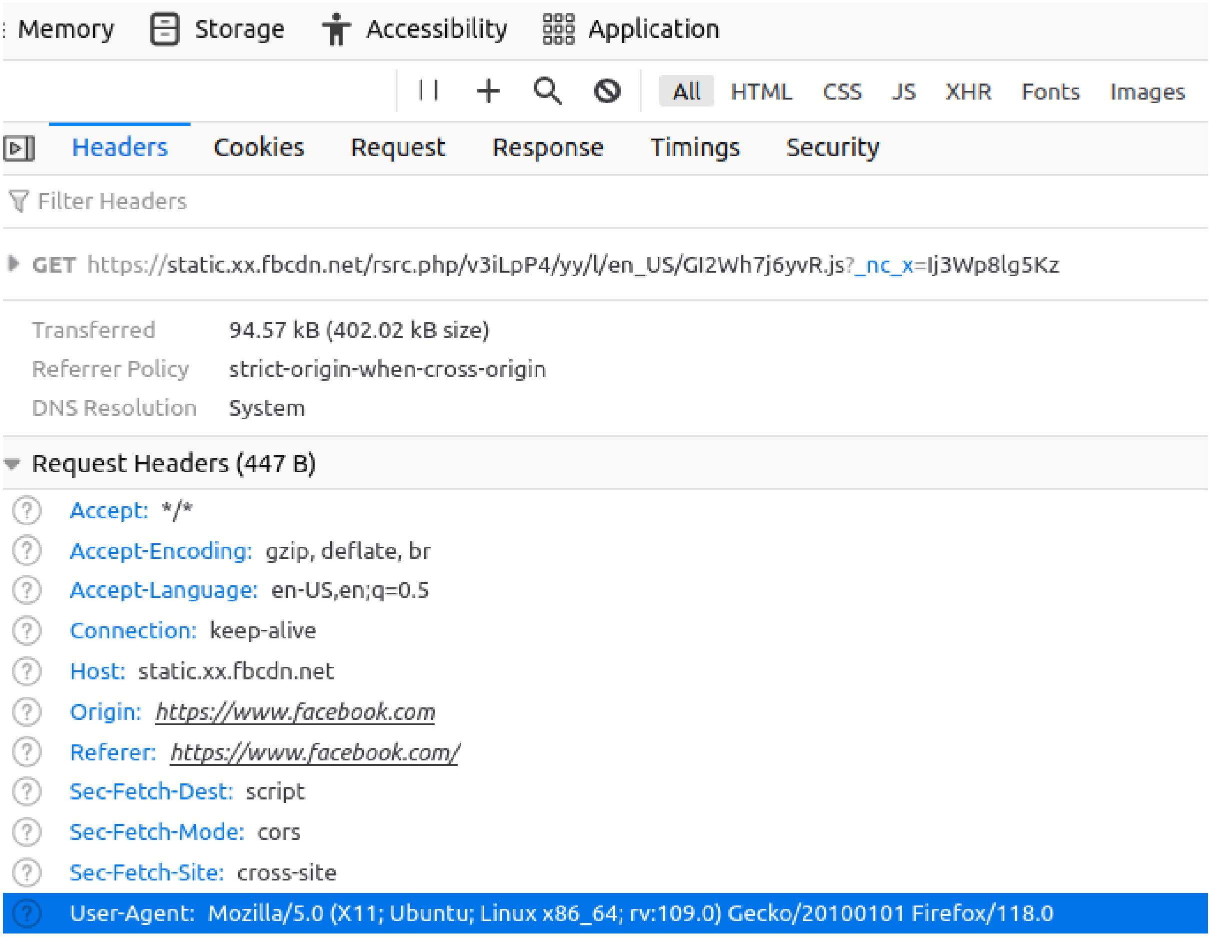
x-frame-options: SAMEORIGIN

Request Headers (592 B)

Accept: */*

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.5



GET https://static.xx.fbcdn.net/rsrc.php/v3iLpP4/yy/l/en_US/GI2Wh7j6yvR.js?_nc_x=Ij3Wp8lg5Kz

Transferred 94.57 kB (402.02 kB size)

Referrer Policy strict-origin-when-cross-origin

DNS Resolution System

Request Headers (447 B)

Accept: */*

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.5

Connection: keep-alive

Host: static.xx.fbcdn.net

Origin: https://www.facebook.com

Referer: https://www.facebook.com/

Sec-Fetch-Dest: script

Sec-Fetch-Mode: cors

Sec-Fetch-Site: cross-site

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/118.0

Note down common headers across all requests.

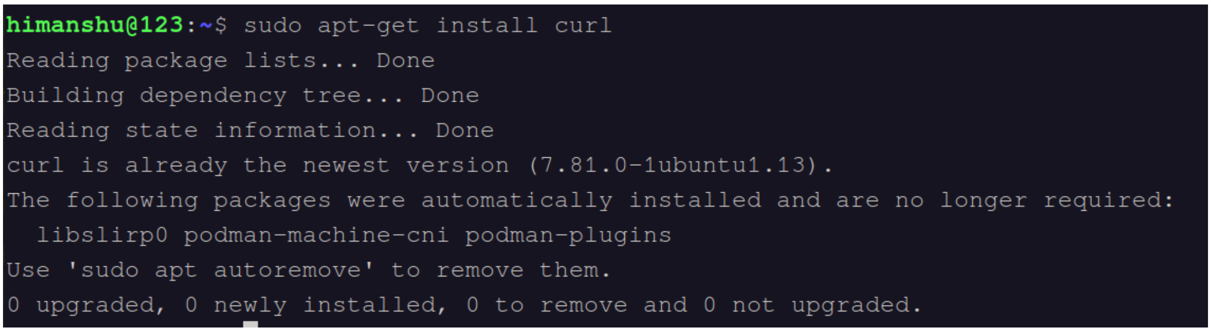
➢ Task 4. Find requests to non-dehradun.nic.in servers:

a. Using curl in Terminal:

- Open the Terminal on Ubuntu.

b. Capture Traffic:

- Install curl if not already installed (sudo apt-get install curl).
  - **Command :- sudo apt-get install curl**



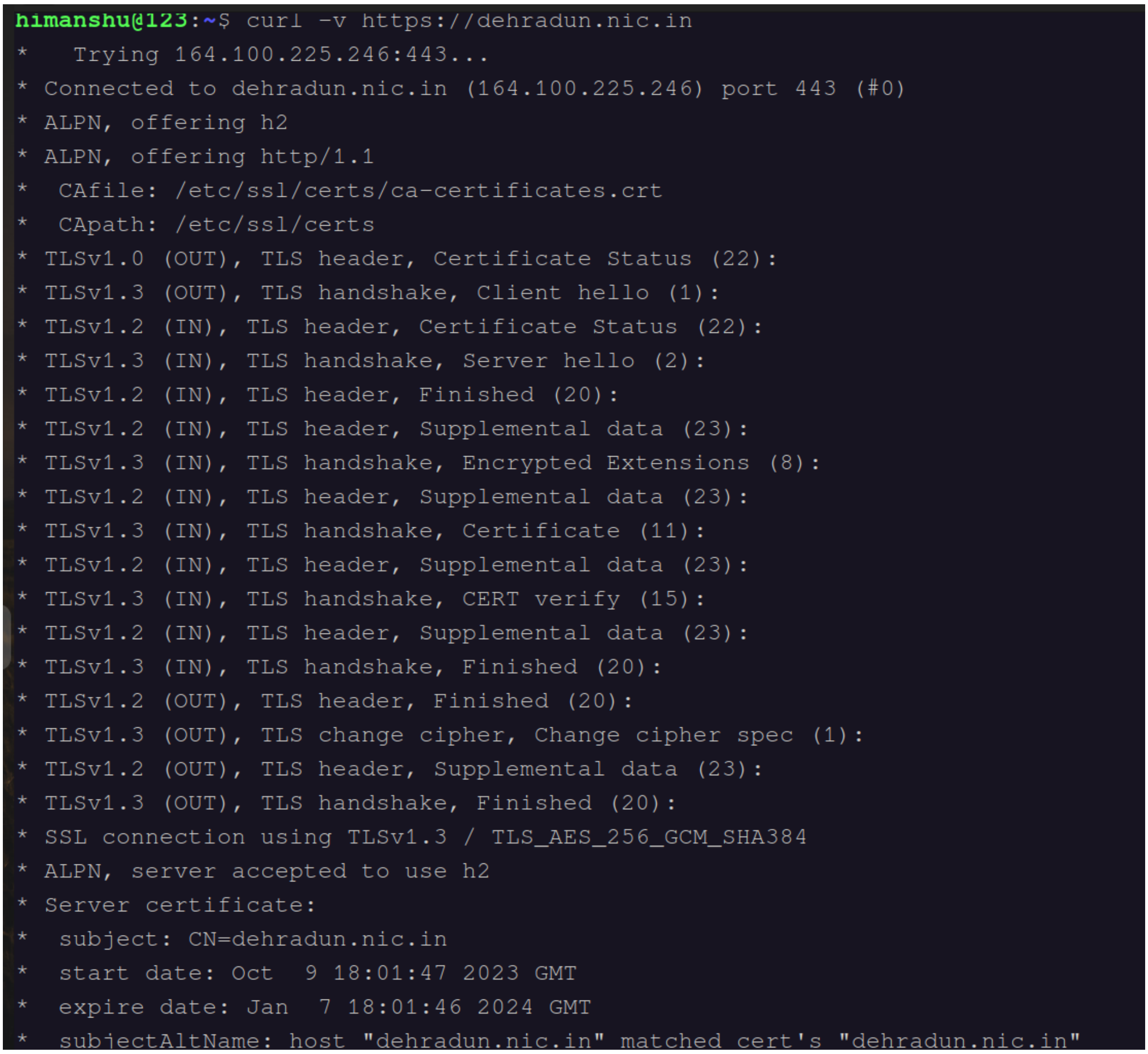
```
himanshu@123:~$ sudo apt-get install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (7.81.0-1ubuntu1.13).
The following packages were automatically installed and are no longer required:
  libslirp0 podman-machine-cni podman-plugins
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

- Use the following command to capture requests:

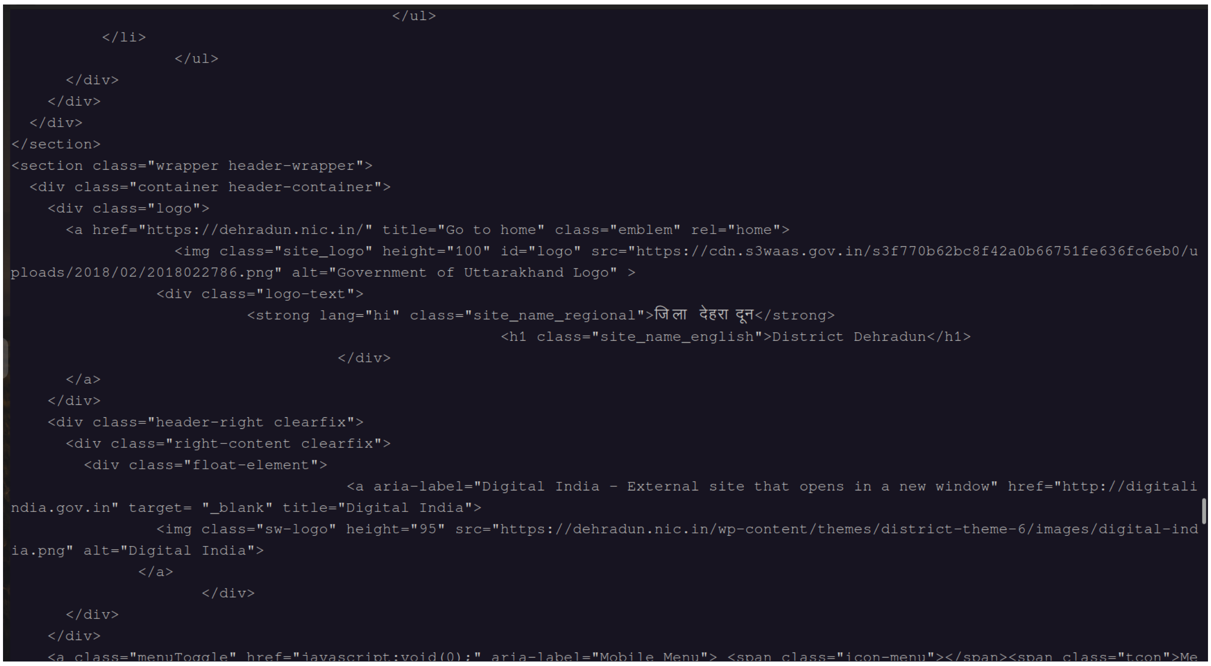
Command :- curl -v https://dehradun.nic.in
This will display verbose information about the requests, including headers.

c. Analyse Output:

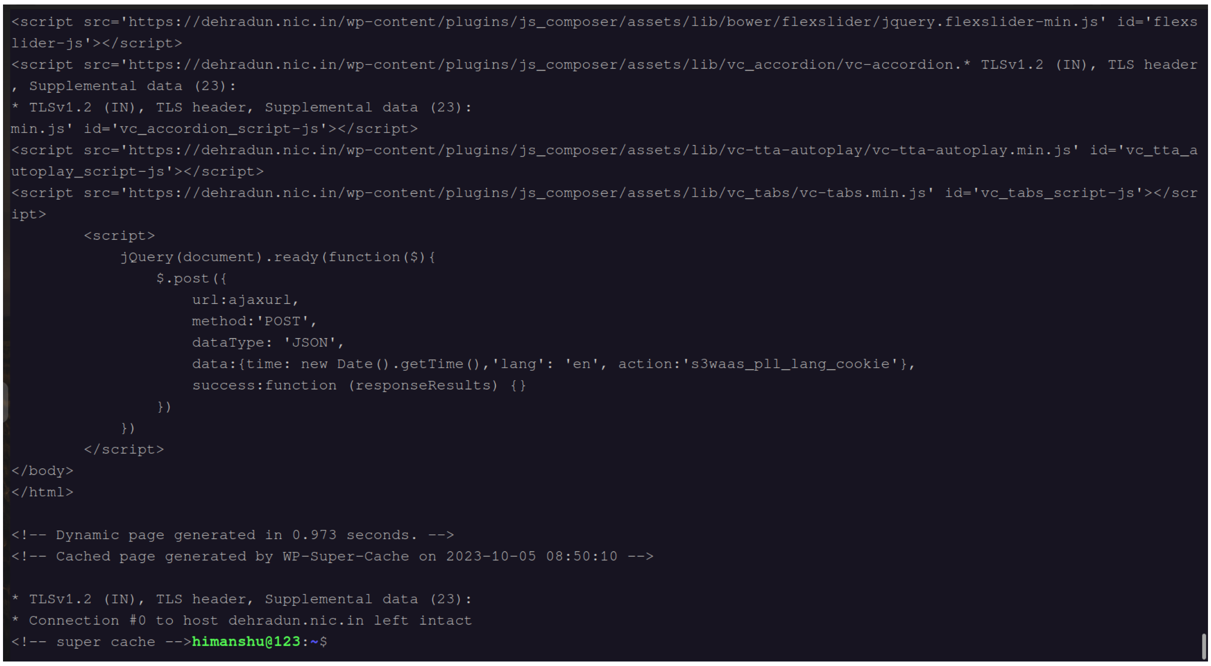
- Look for requests to servers other than dehradun.nic.in.



```
himanshu@123:~$ curl -v https://dehradun.nic.in
*   Trying 164.100.225.246:443...
* Connected to dehradun.nic.in (164.100.225.246) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
*  CAfile: /etc/ssl/certs/ca-certificates.crt
*  CApath: /etc/ssl/certs
* TLSv1.0 (OUT), TLS header, Certificate Status (22):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS header, Finished (20):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.2 (OUT), TLS header, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server accepted to use h2
* Server certificate:
*  subject: CN=dehradun.nic.in
*  start date: Oct  9 18:01:47 2023 GMT
*  expire date: Jan  7 18:01:46 2024 GMT
*  subjectAltName: host "dehradun.nic.in" matched cert's "dehradun.nic.in"
```



```
                                          </ul>
          </li>
                  </ul>
      </div>
    </div>
  </div>
</section>
<section class="wrapper header-wrapper">
  <div class="container header-container">
    <div class="logo">
      <a href="https://dehradun.nic.in/" title="Go to home" class="emblem" rel="home">
                  <img class="site_logo" height="100" id="logo" src="https://cdn.s3waas.gov.in/s3f770b62bc8f42a0b66751fe636fc6eb0/u
ploads/2018/02/2018022786.png" alt="Government of Uttarakhand Logo" >
                <div class="logo-text">
                          <strong lang="hi" class="site_name_regional">जिला देहरा दून</strong>
                                                <h1 class="site_name_english">District Dehradun</h1>
                                    </div>
      </a>
    </div>
    <div class="header-right clearfix">
      <div class="right-content clearfix">
        <div class="float-element">
                                     <a aria-label="Digital India - External site that opens in a new window" href="http://digitali
ndia.gov.in" target= "_blank" title="Digital India">
                <img class="sw-logo" height="95" src="https://dehradun.nic.in/wp-content/themes/district-theme-6/images/digital-ind
ia.png" alt="Digital India">
              </a>
                     </div>
      </div>
    </div>
    <a class="menuToggle" href="javascript:void(0);" aria-label="Mobile Menu"> <span class="icon-menu"></span><span class="tcon">Me
```



```
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/bower/flexslider/jquery.flexslider-min.js' id='flexs
lider-js'></script>
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/vc_accordion/vc-accordion.* TLSv1.2 (IN), TLS header
, Supplemental data (23):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
min.js' id='vc_accordion_script-js'></script>
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/vc-tta-autoplay/vc-tta-autoplay.min.js' id='vc_tta_a
utoplay_script-js'></script>
<script src='https://dehradun.nic.in/wp-content/plugins/js_composer/assets/lib/vc_tabs/vc-tabs.min.js' id='vc_tabs_script-js'></scr
ipt>
        <script>
            jQuery(document).ready(function($){
                $.post({
                    url:ajaxurl,
                    method:'POST',
                    dataType: 'JSON',
                    data:{time: new Date().getTime(),'lang': 'en', action:'s3waas_pll_lang_cookie'},
                    success:function (responseResults) {}
                })
            })
        </script>
</body>
</html>

<!-- Dynamic page generated in 0.973 seconds. -->
<!-- Cached page generated by WP-Super-Cache on 2023-10-05 08:50:10 -->

* TLSv1.2 (IN), TLS header, Supplemental data (23):
* Connection #0 to host dehradun.nic.in left intact
<!-- super cache -->himanshu@123:~$
```

- **curl:** The command itself, used for making HTTP requests.

- **-v:** The verbose option, which displays additional information about the request and response. This can include details like the request headers, response headers, and other diagnostic information.

- **https://dehradun.nic.in :** The URL you're making the request to.