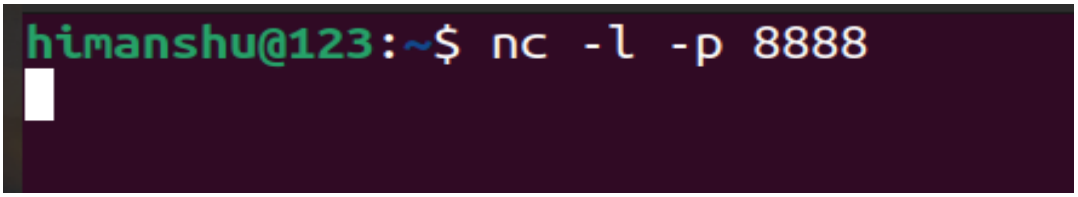
- **What is the nc command and why is it used?**

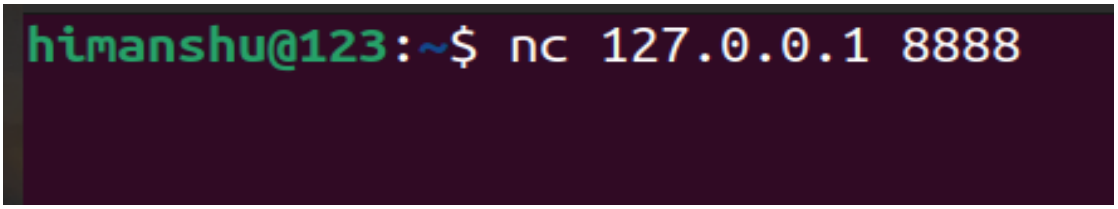
The nc command, short for "netcat," is a versatile networking utility on Linux. It can be used for various network-related tasks, including creating network connections, transferring data, and port scanning. To use it, you typically specify the target IP address and port number, and you can send or receive data through the established connection .

## Practical 1: Basic Bidirectional TCP(Transmission Control Protocol) Communication

- In the first terminal, you are running nc as a server, listening on port 8888 with the command nc -l -p 8888.




- In the second terminal, you are using nc as a client to connect to the server at 127.0.0.1 on port 8888 with the command nc 127.0.0.1 8888.




Initially, there is no output in either terminal because the client and server are connected but not sending any data.

- When you type anything in one of the terminals and press Enter, you will see bidirectional communication because the text you entered is sent to the other terminal and vice versa.

```
himanshu@123:~$ nc -l -p 8888
hello my name is himanshu .
```

```
himanshu@123:~$ nc 127.0.0.1 8888
hello my name is himanshu .
```

- To end the communication, you can press Ctrl + C in either terminal.

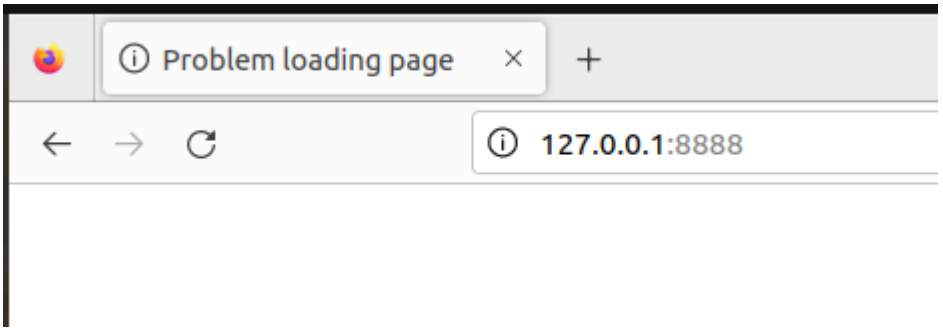
The subject matter of Practical 1 is to demonstrate the basic setup of a TCP client-server communication using nc, showcasing bidirectional data flow.

## Practical 2: Serving HTTP (Hypertext Transfer Protocol ) Content with nc

- In the first terminal, you are running nc as a server, listening on port 8888 with the command nc -l -p 8888.

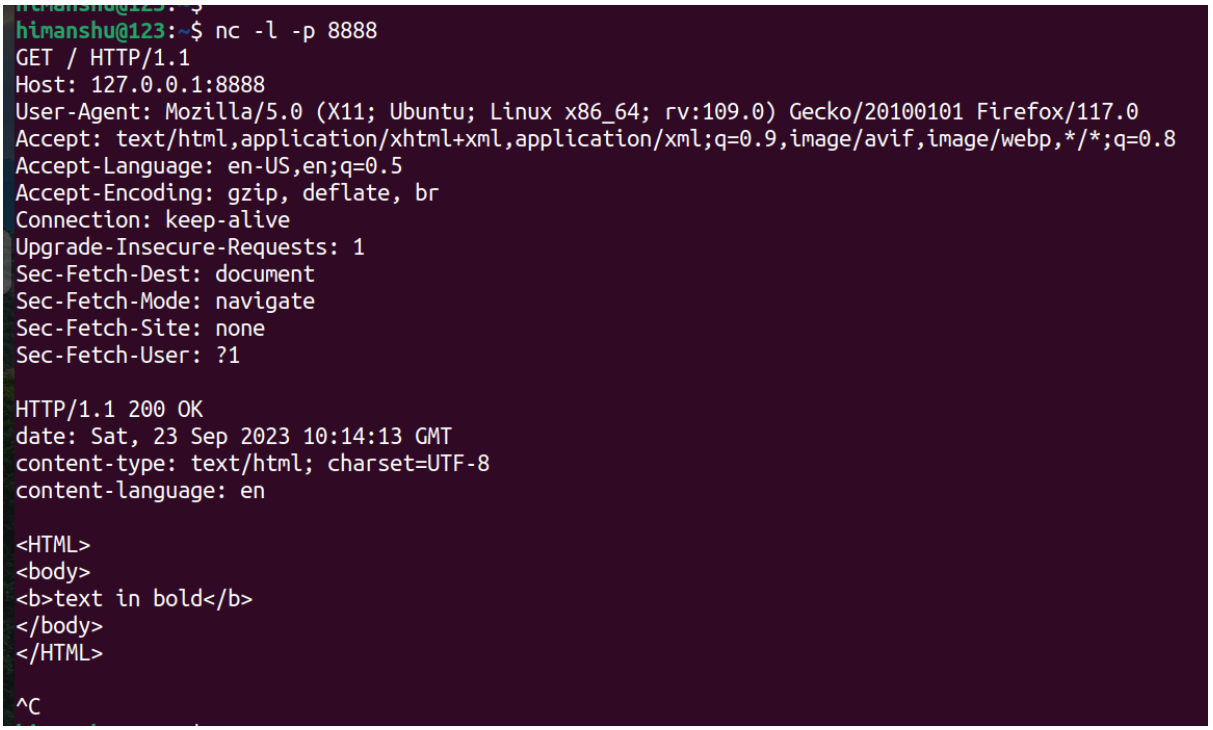
```
himanshu@123:~$ nc -l -p 8888
```

- In your web browser, you open the URL http://127.0.0.1:8888.

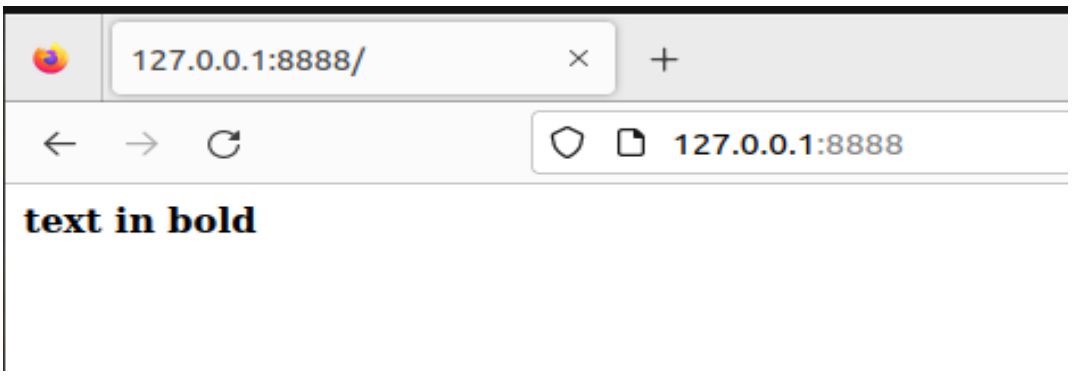


- Immediately after opening the URL in the browser, you paste the following HTTP response headers and HTML content into the terminal running nc:

HTTP/1.1 200 OK
date: Sat, 23 Sep 2023 10:14:13 GMT
content-type: text/html; charset=UTF-8
content-language: en
<HTML>
<body>
text in bold
</body>
</HTML>




- After pasting this content and pressing Enter, you will observe the browser displaying the HTML content with the text "text in bold" in bold.




- To end the communication, you can press Ctrl + C in the terminal running nc.

The subject matter of Practical 2 is to demonstrate how you can use nc as a simple HTTP server by manually sending HTTP response headers and content, allowing you to serve a basic HTML page to a web browser.

## Practical 3 :Send the website uk.nic.in the following data over port 80 --

The provided data represents an HTTP request intended for the server of the website uk.nic.in. This request is structured to reach the server through port 80, which is the standard port for HTTP communication.

There are two ways to do this .

1. **Using cURL**
2. **Using Telnet**

**Step 1. Using cURL:** curl -v http://uk.nic.in

```
<link rel='stylesheet' id='flexslider-css' href='https://uk.nic.in/wp-content/plugins/js_composer/assets/lib/bower/flexslider/flexslider.min.css?ver=6.1'
 media='all' />
<link rel='stylesheet' id='custom-flexslider-css' href='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/css/custom-flexslider.css?ver=6.3' med
ia='all' />
<link rel='stylesheet' id='news-ticker-style-css' href='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/css/news-ticker.css?ver=6.3' media='al
l' />
<link rel='stylesheet' id='card-style-css' href='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/css/card.css?ver=6.3' media='all' />
<link rel='stylesheet' id='component-helper-css' href='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/css/component-helper.css?ver=6.3' media
='all' />
<link rel='stylesheet' id='home-gallery-css' href='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/css/photo-gallery-home.css?ver=6.3' media='
all' />
<link rel='stylesheet' id='list-style-css' href='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/css/list-style.min.css?ver=6.3' media='all' /
>
<link rel='stylesheet' id='ad-banner-css-css' href='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/css/ad-banner.css?ver=6.3' media='all' />
<link rel='stylesheet' id='holiday-css-css' href='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/css/holiday-calendar.css?ver=6.3' media='all
' />
<link rel='stylesheet' id='footer-style-css' href='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/css/footer-logo-carousel.css?ver=6.3' media
='all' />
<script type='text/javascript' id='jquery-common-js-js-extra'>
/* <![CDATA[ */
var AwaasData = {"ajaxUrl":"https:\/\/uk.nic.in\/wp-admin\/admin-ajax.php"};
/* ]]> */
</script>
<script src='https://uk.nic.in/wp-content/plugins/common_utility//js/common.js?ver=1.1' id='jquery-common-js-js'></script>
<script src='https://uk.nic.in/wp-includes/js/jquery/ui/core.min.js?ver=1.13.2' id='jquery-ui-core-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/ui/jquery.flexslider.js?ver=1.1' id='jquery-flexslider-js-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/easyResponsiveTabs.js?ver=1.1' id='jseasyResponsiveTabs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/jquery.fancybox.js?ver=1.1' id='jqueryfancyboxjs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/style.switcher.js?ver=1.1' id='styleswitcherjs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/menu.js?ver=1.1' id='menujs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/table.min.js?ver=1.1' id='tablejs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/jquery.treeview.js?ver=1.1' id='treeviewjs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/custom.js?ver=1.1' id='custom-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/extra.js?ver=1.1' id='extrajs-js'></script>
<script src='https://uk.nic.in/wp-content/plugins/js_composer/assets/js/dist/js_composer_front.min.js?ver=6.1' id='wpb_composer_front_js-js'></script>
<script src='https://uk.nic.in/wp-content/plugins/js_composer/assets/lib/bower/flexslider/jquery.flexslider-min.js?ver=6.1' id='flexslider-js'></script>
<script src='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/js/holiday-calendar.js?ver=1.0.0' id='holiday-js-js'></script>
<script>
jQuery(document).ready(function($){
```

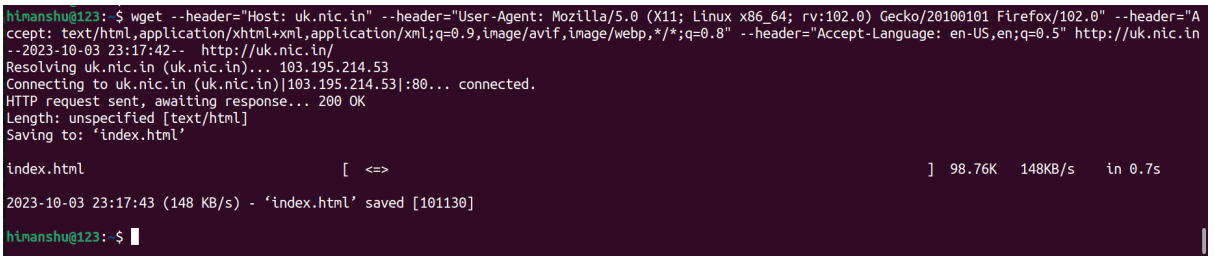
```
' />
<link rel='stylesheet' id='footer-style-css' href='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/css/footer-logo-carousel.css?ver=6.3' media
='all' />
<script type='text/javascript' id='jquery-common-js-js-extra'>
/* <![CDATA[ */
var AwaasData = {"ajaxUrl":"https:\/\/uk.nic.in\/wp-admin\/admin-ajax.php"};
/* ]]> */
</script>
<script src='https://uk.nic.in/wp-content/plugins/common_utility//js/common.js?ver=1.1' id='jquery-common-js-js'></script>
<script src='https://uk.nic.in/wp-includes/js/jquery/ui/core.min.js?ver=1.13.2' id='jquery-ui-core-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/ui/jquery.flexslider.js?ver=1.1' id='jquery-flexslider-js-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/easyResponsiveTabs.js?ver=1.1' id='jseasyResponsiveTabs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/jquery.fancybox.js?ver=1.1' id='jqueryfancyboxjs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/style.switcher.js?ver=1.1' id='styleswitcherjs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/menu.js?ver=1.1' id='menujs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/table.min.js?ver=1.1' id='tablejs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/jquery.treeview.js?ver=1.1' id='treeviewjs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/custom.js?ver=1.1' id='custom-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/extra.js?ver=1.1' id='extrajs-js'></script>
<script src='https://uk.nic.in/wp-content/plugins/js_composer/assets/js/dist/js_composer_front.min.js?ver=6.1' id='wpb_composer_front_js-js'></script>
<script src='https://uk.nic.in/wp-content/plugins/js_composer/assets/lib/bower/flexslider/jquery.flexslider-min.js?ver=6.1' id='flexslider-js'></script>
<script src='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/js/holiday-calendar.js?ver=1.0.0' id='holiday-js-js'></script>
<script>
jQuery(document).ready(function($){
  jQuery('body').find('a.flex-pause').attr('href',"javascript:void(0)");
    $('.flex-direction-nav a.flex-prev').attr({'title' : 'पिछला','aria-label':'पिछला'});
    $('.flex-pauseplay a.flex-pause').attr({'title' : 'चालू करें / रोकें','aria-label':'चालू करें / रोकें'});
    $('.flex-direction-nav a.flex-next').attr({'title' : 'आला','aria-label':'आला'});
});
</script>
</body>
</html>

<!-- Dynamic page generated in 21.981 seconds. -->
<!-- Cached page generated by WP-Super-Cache on 2023-09-22 19:49:36 -->

* Connection #0 to host uk.nic.in left intact
<!-- super cache -->himanshu@123:~$
```

- curl: Command-line tool for making HTTP requests.
- -v: Verbose mode, which displays additional information during the request.
- http://uk.nic.in : The URL to which the GET request is sent.

- wget --header="Host: uk.nic.in" --header="User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" --header="Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8" --header="Accept-Language: en-US,en;q=0.5" http://uk.nic.in...




1. wget: This is the command itself, indicating that you want to use the wget utility.

2. --header="Host: uk.nic.in": This option specifies an HTTP header to be included in the request. In this case, it sets the "Host" header to "uk.nic.in". This is often necessary when the server requires a specific host header for the request to be valid.

3. --header="User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0": This sets the "User-Agent" header, which is used to identify the client making the request. In this case, it's set to mimic the Firefox web browser running on a Linux system.

4. --header="Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8": The "Accept" header specifies the types of content that the client can understand. This header indicates that the client prefers HTML and XML, but it can accept other types of content as well.

5. --header="Accept-Language: en-US,en;q=0.5": The "Accept-Language" header indicates the preferred language for the response. In this case, it prefers English (United States) with a lower preference for generic English.

6. ` http://uk.nic.in...: This is the URL from which wget will download the content. The URL is truncated in your provided command, and it ends with "...", so the actual URL is not complete.

- Here is the link to the downloaded file

- **Link :-** [Index.html]

**Step 2. Using Telnet :** telnet uk.nic.in 80

- telnet uk.nic.in 80: Initiates a Telnet connection to the specified server (uk.nic.in) on port 80.

```
himanshu@123:~$ telnet uk.nic.in 80
Trying 103.195.214.53...
Connected to s3fb2e203234df6dee15934e448ee88971.s3waas.gov.in.
Escape character is '^]'.
```

- Paste this code and press enter .
  GET / HTTP/1.1
  Host: uk.nic.in
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
  Accept-Language: en-US,en;q=0.5

- GET / HTTP/1.1: Specifies the HTTP request method, path ("/" indicates the root), and HTTP version.
- Host: uk.nic.in: Informs the server about the intended host.
- User-Agent: Mozilla/5.0 ...: Provides information about the user agent (browser).
- Accept: ...: Communicates the types of content that the client can process.
- Accept-Language: ...: Indicates the preferred languages for the response.

```
himanshu@123:~$ telnet uk.nic.in 80
Trying 103.195.214.53...
Connected to s3fb2e203234df6dee15934e448ee88971.s3waas.gov.in.
Escape character is '^]'.
GET / HTTP/1.1
Host: uk.nic.in
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
</ul></div>            </div>
        </div>
    </div>
    <div class="footer-bottom">
        <div class="container">
            <div class="row">
                <div class="col-xs-12 text-center">

                    <div class="copyRights">

                        <div class="copyRightsText">
                                                    <p>© उत्तरा खंड रा जय वेंहर , <a href="http://www.nic.in/" target="_blank">रा ष्ट्री य सूचना -वि ज्ञान वेंहर</a>,<br>
<a href="http://meity.gov.in/" target="_blank">इलेक्ट्रॉनि क्स औ सूचना प्रौ द्यो गि की मंत्रा लय</a>, भारत सरकार, द्वा रा वि कसित औ हो स्ट्रेड</p>
                            <p>अंति म अद्यतन तिथि: <strong>May 24, 2023</strong></p>                                </div>

                        <div class="copyRightsLogos">
                            <a href="https://s3waas.gov.in/"><img src="https://uk.nic.in/wp-content/themes/sdo-theme/images/s3waas.png"  alt="Secure, Sca
lable and Sugamya Website as a Service"></a>
                            <!--<a href="http://www.nic.in/"><img src="https://uk.nic.in/wp-content/themes/sdo-theme/images/nicLogo.png"  alt="रा ष्ट्री य सू
ना -वि ज्ञान वेंहर"></a>-->
                            <a href="http://www.digitalindia.gov.in/"><img src="https://uk.nic.in/wp-content/themes/sdo-theme/images/digitalIndia.png" al
t="Digital India"></a>
                        </div>
                    </div>
                </div>
            </div>
        </div>
    </div>
</footer>
```

```
<script src='https://uk.nic.in/wp-content/plugins/common_utility//js/common.js?ver=1.1' id='jquery-common-js-js'></script>
<script src='https://uk.nic.in/wp-includes/js/jquery/ui/core.min.js?ver=1.13.2' id='jquery-ui-core-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/ui/jquery.flexslider.js?ver=1.1' id='jquery-flexslider-js-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/easyResponsiveTabs.js?ver=1.1' id='jseasyResponsiveTabs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/jquery.fancybox.js?ver=1.1' id='jqueryfancyboxjs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/style.switcher.js?ver=1.1' id='styleswitcherjs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/menu.js?ver=1.1' id='menujs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/table.min.js?ver=1.1' id='tablejs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/jquery.treeview.js?ver=1.1' id='treeviewjs-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/custom.js?ver=1.1' id='custom-js'></script>
<script src='https://uk.nic.in/wp-content/themes/sdo-theme/js/extra.js?ver=1.1' id='extrajs-js'></script>
<script src='https://uk.nic.in/wp-content/plugins/js_composer/assets/js/dist/js_composer_front.min.js?ver=6.1' id='wpb_composer_front_js-js'></script>
<script src='https://uk.nic.in/wp-content/plugins/js_composer/assets/lib/bower/flexslider/jquery.flexslider-min.js?ver=6.1' id='flexslider-js'></script>
<script src='https://uk.nic.in/wp-content/plugins/awas-shortcode/assets/js/holiday-calendar.js?ver=1.0.0' id='holiday-js-js'></script>
<script>
jQuery(document).ready(function($){
  jQuery('body').find('a.flex-pause').attr('href',"javascript:void(0)");
    $('.flex-direction-nav a.flex-prev').attr
1ec
({'title' : 'पि छला','aria-label':'पि छला'});
    $('.flex-pauseplay a.flex-pause').attr({'title' : 'चालू करे / रो के','aria-label':'चालू करे / रो के'});
    $('.flex-direction-nav a.flex-next').attr({'title' : 'अला','aria-label':'अला'});
});
</script>
</body>
</html>

<!-- Dynamic page generated in 21.981 seconds. -->
<!-- Cached page generated by WP-Super-Cache on 2023-09-22 19:49:36 -->

<!-- super cache -->
0
```

- Type **quit** or you will be Exited .


- **The same output will be displayed here as was shown when curl was executed.**

## Interpretation of Data:

The data includes a GET request for a web page, specifies the host, and provides information about the user agent and accepted content types.

## Check the Response:

After running the command, you can observe the response received from the server, which may include information about the requested web page.