

Week #4

Week 4 – Persistent, Non-Persistent, Authentication, Cookies and Conditional GET

SRN : PES2UG20CS237

Name : P K Navin Shrinivas

Section : D

Task 1 : Setup a apache server

- My setup includes 2 separate linux machines within my network, both running arch linux.
- First packages needed were installed using the following command :

```
[[prod]serveruser@server1 ~]$sudo pacman -S apache php php-apache
warning: apache-2.4.52-1 is up to date -- reinstalling
warning: php-8.1.2-1 is up to date -- reinstalling
warning: php-apache-8.1.2-1 is up to date -- reinstalling
resolving dependencies...
looking for conflicting packages...

Package (3)      Old Version  New Version  Net Change
extra/apache     2.4.52-1    2.4.52-1    0.00 MiB
extra/php        8.1.2-1     8.1.2-1     0.00 MiB
extra/php-apache 8.1.2-1     8.1.2-1     0.00 MiB

Total Installed Size: 44.39 MiB
Net Upgrade Size: 0.00 MiB

:: Proceed with installation? [Y/n]
(3/3) checking keys in keyring
(3/3) checking package integrity
(3/3) loading package files
(3/3) checking for file conflicts
:: Processing package changes...
(1/3) reinstalling apache
(2/3) reinstalling php
(3/3) reinstalling php-apache
:: Running post-transaction hooks...
```

- Apache server was then turned on and its status was checked to be "active" :

```
1: serveruser@server1:~ x + 

[[prod]serveruser@server1 ~]$sudo systemctl enable httpd --now
Created symlink /etc/systemd/system/multi-user.target.wants/
httpd.service → /usr/lib/systemd/system/httpd.service.
[[prod]serveruser@server1 ~]$sudo systemctl status httpd
● httpd.service - Apache Web Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service);>
     Active: active (running) since Thu 2022-02-10 13:46:30>
       Main PID: 243255 (httpd)
          Tasks: 82 (limit: 4575)
        Memory: 7.4M
         CPU: 78ms
        CGroup: /system.slice/httpd.service
                  └─243255 /usr/bin/httpd -k start -DFOREGROUND
                    ├─243256 /usr/bin/httpd -k start -DFOREGROUND
                    ├─243257 /usr/bin/httpd -k start -DFOREGROUND
                    └─243258 /usr/bin/httpd -k start -DFOREGROUND

Feb 10 13:46:30 server1 systemd[1]: Started Apache Web Server.
Feb 10 13:46:30 server1 httpd[243255]: AH00558: httpd: Could not
Lines 1-15/15 (END)
```

- Apache server was configured to allow persistent connections by modifying the /etc/httpd/conf/httpd.conf (specific to distro) was modified like so :

```
1: serveruser@server1:/etc/httpd/conf x + 

#
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
# for a discussion of each configuration directive.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path. If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so "logs/access_log"
# with ServerRoot set to "/usr/local/apache2" will be interpreted by the
# server as "/usr/local/apache2/logs/access_log", whereas "/logs/access_log"
# will be interpreted as '/logs/access_log'.

# For persistent connections

KeepAlive On
MaxKeepAliveRequests 2
```

httpd.conf
"httpd.conf" 548L, 20213C written

- The apache server was restarted after saving changes to the above

file suing : sudo systemctl restart httpd

- Both the system were assigned status ip local addresses from the router itself :

The screenshot shows two terminal windows. The left window is in fish shell (navin) and shows the output of 'ip addr show'. It lists several interfaces: 'lo' (loopback), 'en0', 'en1', and 'wlan0'. The 'wlan0' interface is highlighted with a red box and shows an IP address of 192.168.1.10/24. The right window is in root shell (serveruser) and shows the output of 'ip add show'. It lists 'lo', 'enp2s0', 'wlan0', and 'inet6 fe80'. The 'wlan0' interface is highlighted with a red box and shows an IP address of 192.168.1.11/24. A watermark 'Server IP task' is visible in the center of the image.

```
fish /home/navin
1: fish /home/navin x + 
Welcome to fish, the friendly interactive shell
Type help for instructions on how to use fish
~ ))> ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: en0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether bc:e9:2f:8c:1c:4e brd ff:ff:ff:ff:ff:ff
    altname enp2s0
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether e0:d4:e8:32:73:8c brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
        valid_lft 62433sec preferred_lft 62433sec
        inet6 2401:4900:1f25:c59:7194:3464:c58:daea/64 scope global dynamic noprefixroute
            valid_lft 86202sec preferred_lft 86202sec
            inet6 fe80::7473:30dc:5d7e:ca1a/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
~ ))> 

serveruser@server1:/etc/httpd/conf
1: serveruser@server1:/etc/httpd/conf x + 
[[prod]serveruser@server1 conf]$ip add show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp2s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 8c:16:45:ce:85:43 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 30:24:32:95:a8:b2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.11/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
        valid_lft 45102sec preferred_lft 45102sec
        inet6 2401:4900:1f25:c59:b0e:75:f884:4025/64 scope global dynamic noprefixroute
            valid_lft 86206sec preferred_lft 86206sec
            inet6 fe80::8bdd:fbe1:ac53:b063/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
[[prod]serveruser@server1 conf]$
```

Client : 192.168.1.10

Server : 192.168.1.11

- The Webpage is hosted by copying over the provided photos to the respective folder and writing an index.html file :

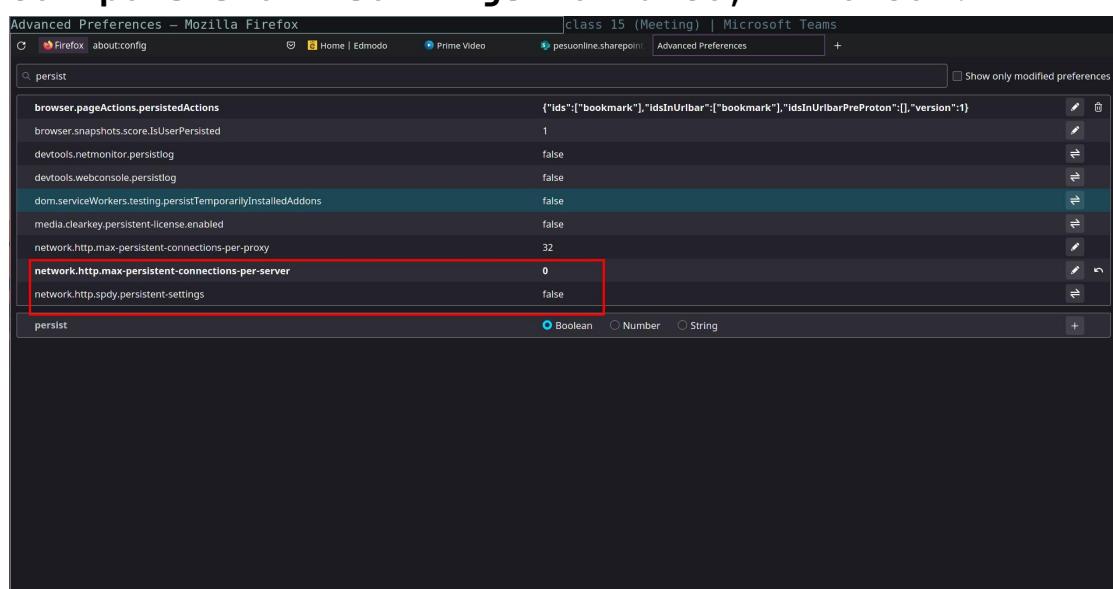
The screenshot shows a terminal window in root shell (serveruser) displaying the contents of 'index.html'. The file contains an HTML document with a title 'Hello world', a heading 'The images', and ten image tags, each pointing to a file named '1.jpg' through '10.jpg'. The entire file is enclosed in HTML and body tags.

```
[[prod]serveruser@server1 http]$ls -a
[ ... 10.jpg 1.jpg 2.jpg 3.jpg 4.jpg 5.jpg 6.jpg 7.jpg 8.jpg 9.jpg .htaccess .htpasswd index.html index.php
[[prod]serveruser@server1 http]$cat index.html
<html>
    <body>
        <h1>Hello world</h1>
        <h2>The images :</h2>
        
        
        
        
        
        
        
        
        
        
    </body>
</html>
[[prod]serveruser@server1 http]$
```

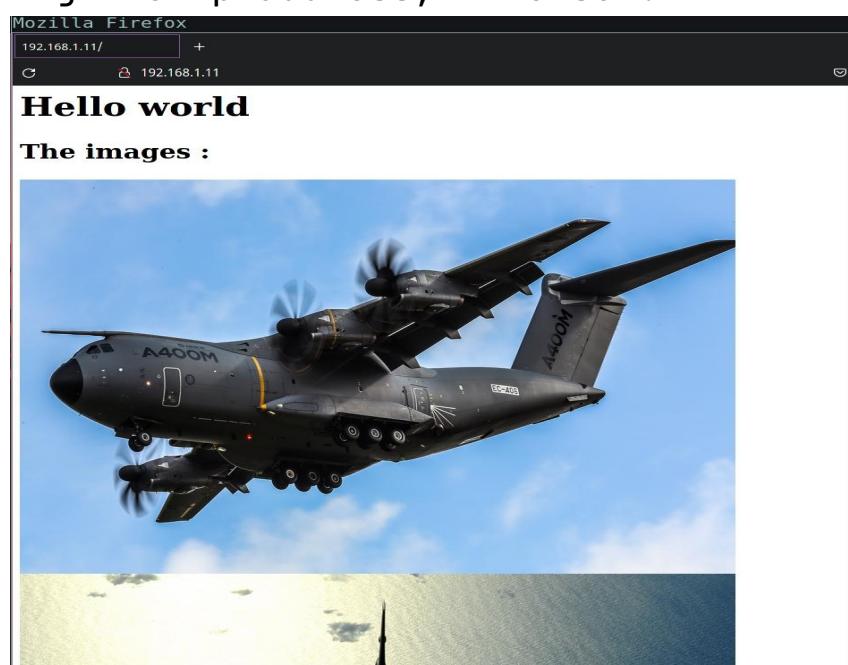
The extra folder are not to confused as they are used in later tasks, only the .jpg and index.html folder is needed for task 1.

Task 2 :Non-Persistent Connections

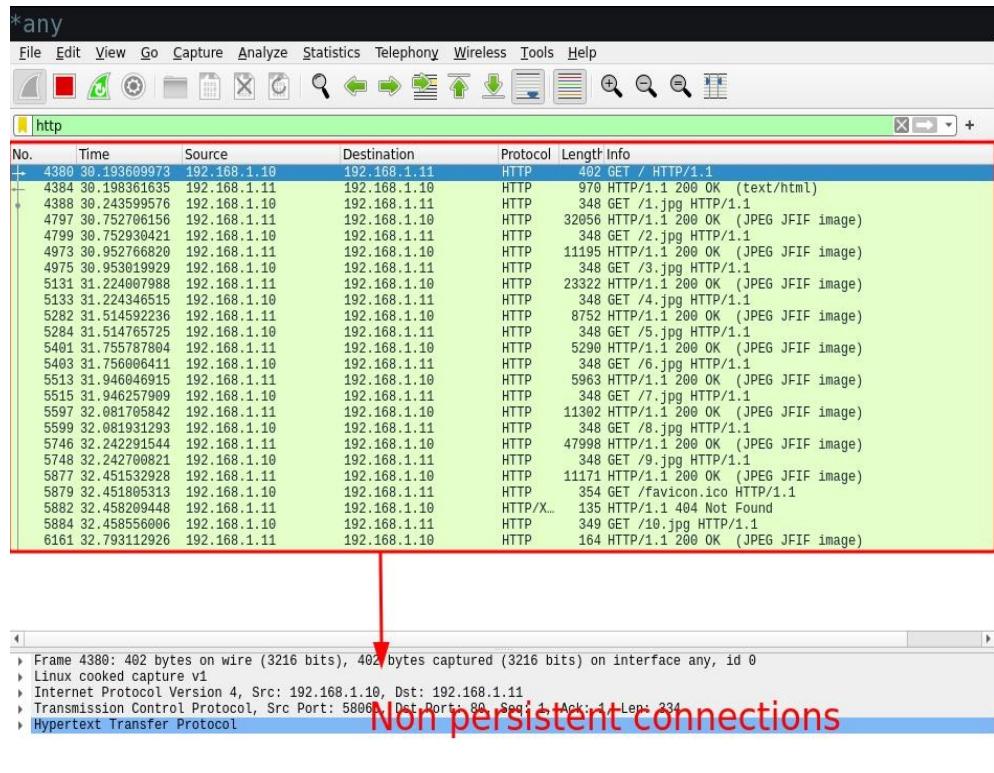
- Open firefox and enter address `about:config` , and press accpet risk and continue if asked.
- Once done, search for persist and set :
max-persistent-connections-per-server to 0 and set **persistent-settings** to false, like so :



- Now, ping your server from firefox by simply entering the ip address, like so :

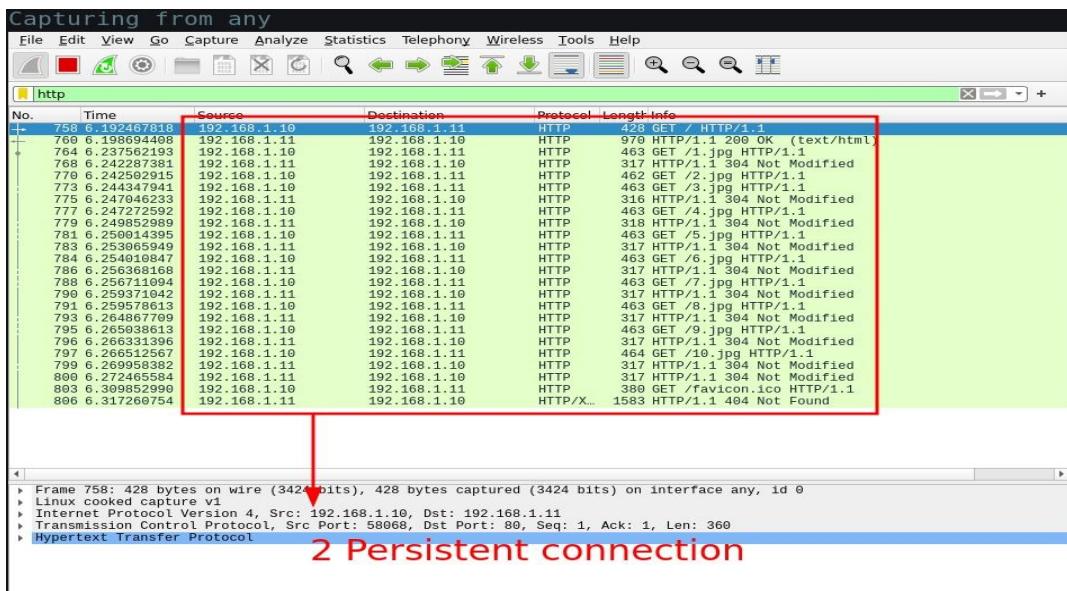


- Analysing the packets in wirehark make it clear that we are handling non persistent connections :

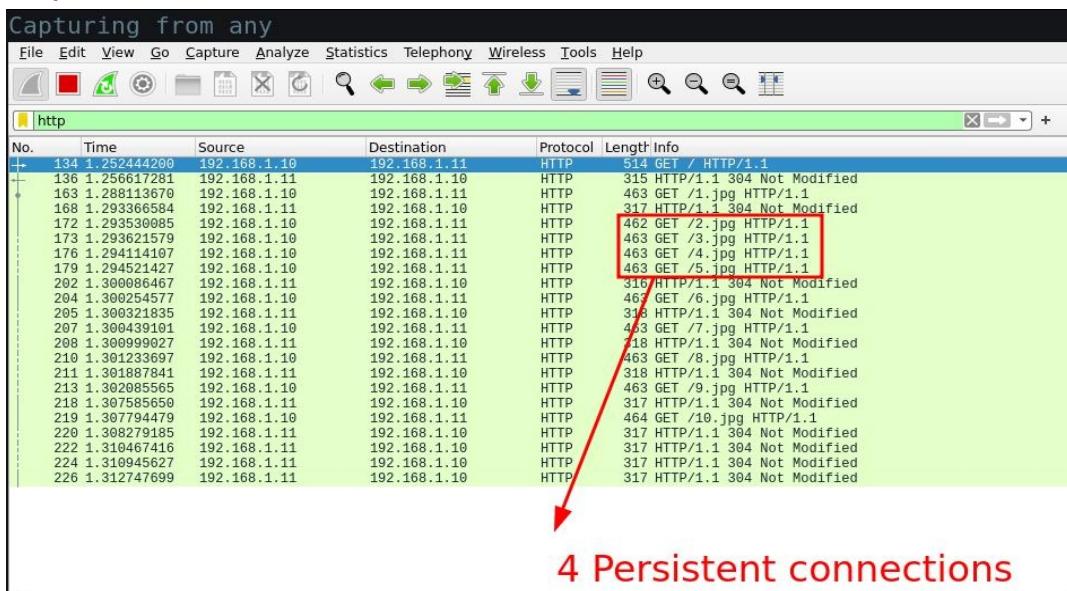


Task 3 : Persistent Connections

- Open firefox again and got to about:config and set:
max-persistent-connections-per-server to 2,4,6..
persistent-settings to true
- 2 persist connections



- 4 persist connections



- 6 persist connections

Capturing from any						
No.	Time	Source	Destination	Protocol	Length	Info
179	1.455928726	192.168.1.10	192.168.1.11	HTTP	514	GET / HTTP/1.1
181	1.459506306	192.168.1.11	192.168.1.10	HTTP	315	HTTP/1.1 304 Not Modified
182	1.490196592	192.168.1.11	192.168.1.10	HTTP	463	GET /1.jpg HTTP/1.1
184	1.48376306	192.168.1.10	192.168.1.11	HTTP	621	HTTP/1.1 304 Not Modified
185	1.48376306	192.168.1.10	192.168.1.11	HTTP	462	GET /2.jpg HTTP/1.1
187	1.4902073186	192.168.1.10	192.168.1.11	HTTP	463	GET /3.jpg HTTP/1.1
188	1.4902073186	192.168.1.10	192.168.1.11	HTTP	463	GET /4.jpg HTTP/1.1
189	1.4902073186	192.168.1.10	192.168.1.11	HTTP	463	GET /5.jpg HTTP/1.1
190	1.492279719	192.168.1.10	192.168.1.11	HTTP	463	GET /6.jpg HTTP/1.1
191	1.492279719	192.168.1.10	192.168.1.11	HTTP	463	GET /7.jpg HTTP/1.1
192	1.49561919	192.168.1.10	192.168.1.11	HTTP	314	HTTP/1.1 304 Not Modified
193	1.500368221	192.168.1.11	192.168.1.10	HTTP	311	HTTP/1.1 304 Not Modified
194	1.500369129	192.168.1.11	192.168.1.10	HTTP	318	HTTP/1.1 304 Not Modified
195	1.500369129	192.168.1.11	192.168.1.10	HTTP	318	HTTP/1.1 304 Not Modified
196	1.500406774	192.168.1.11	192.168.1.10	HTTP	318	HTTP/1.1 304 Not Modified
197	1.500692569	192.168.1.10	192.168.1.11	HTTP	63	GET /8.jpg HTTP/1.1
198	1.500777986	192.168.1.10	192.168.1.11	HTTP	463	GET /9.jpg HTTP/1.1
199	1.5008837562	192.168.1.10	192.168.1.11	HTTP	464	GET /10.jpg HTTP/1.1
200	1.500941468	192.168.1.11	192.168.1.10	HTTP	318	HTTP/1.1 304 Not Modified
201	1.502010241	192.168.1.11	192.168.1.10	HTTP	318	HTTP/1.1 304 Not Modified
202	1.505676057	192.168.1.11	192.168.1.10	HTTP	317	HTTP/1.1 304 Not Modified
203	1.505377454	192.168.1.11	192.168.1.10	HTTP	317	HTTP/1.1 304 Not Modified
204	1.505635731	192.168.1.11	192.168.1.10	HTTP	317	HTTP/1.1 304 Not Modified

6 Persistent connections

- 8 persist connections

http						
No.	Time	Source	Destination	Protocol	Length	Info
113	1.169938378	192.168.1.10	192.168.1.11	HTTP	514	GET / HTTP/1.1
138	1.164772640	192.168.1.11	192.168.1.10	HTTP	315	HTTP/1.1 304 Not Modified
141	1.190477268	192.168.1.10	192.168.1.11	HTTP	463	GET /1.jpg HTTP/1.1
142	1.190475451	192.168.1.10	192.168.1.11	HTTP	462	GET /2.jpg HTTP/1.1
143	1.194842924	192.168.1.10	192.168.1.11	HTTP	463	GET /3.jpg HTTP/1.1
151	1.194834940	192.168.1.10	192.168.1.11	HTTP	463	GET /4.jpg HTTP/1.1
152	1.198423578	192.168.1.10	192.168.1.11	HTTP	463	GET /5.jpg HTTP/1.1
162	1.198590362	192.168.1.10	192.168.1.11	HTTP	463	GET /6.jpg HTTP/1.1
163	1.199008981	192.168.1.10	192.168.1.11	HTTP	317	HTTP/1.1 304 Not Modified
164	1.199008981	192.168.1.10	192.168.1.11	HTTP	463	GET /7.jpg HTTP/1.1
174	2.206225059	192.168.1.10	192.168.1.11	HTTP	463	GET /8.jpg HTTP/1.1
175	1.206800257	192.168.1.11	192.168.1.10	HTTP	317	HTTP/1.1 304 Not Modified
183	1.206981777	192.168.1.10	192.168.1.11	HTTP	463	GET /9.jpg HTTP/1.1
184	1.207055323	192.168.1.10	192.168.1.11	HTTP	463	GET /10.jpg HTTP/1.1
185	1.207055323	192.168.1.10	192.168.1.11	HTTP	463	GET /11.jpg HTTP/1.1
189	1.211833724	192.168.1.11	192.168.1.10	HTTP	318	HTTP/1.1 304 Not Modified
190	1.211849997	192.168.1.11	192.168.1.10	HTTP	317	HTTP/1.1 304 Not Modified
194	1.213217859	192.168.1.11	192.168.1.10	HTTP	317	HTTP/1.1 304 Not Modified
196	1.214575733	192.168.1.11	192.168.1.10	HTTP	318	HTTP/1.1 304 Not Modified
201	1.217213329	192.168.1.11	192.168.1.10	HTTP	317	HTTP/1.1 304 Not Modified
202	1.217875923	192.168.1.11	192.168.1.10	HTTP	318	HTTP/1.1 304 Not Modified
204	1.218523719	192.168.1.11	192.168.1.10	HTTP	318	HTTP/1.1 304 Not Modified

8 persistent connection

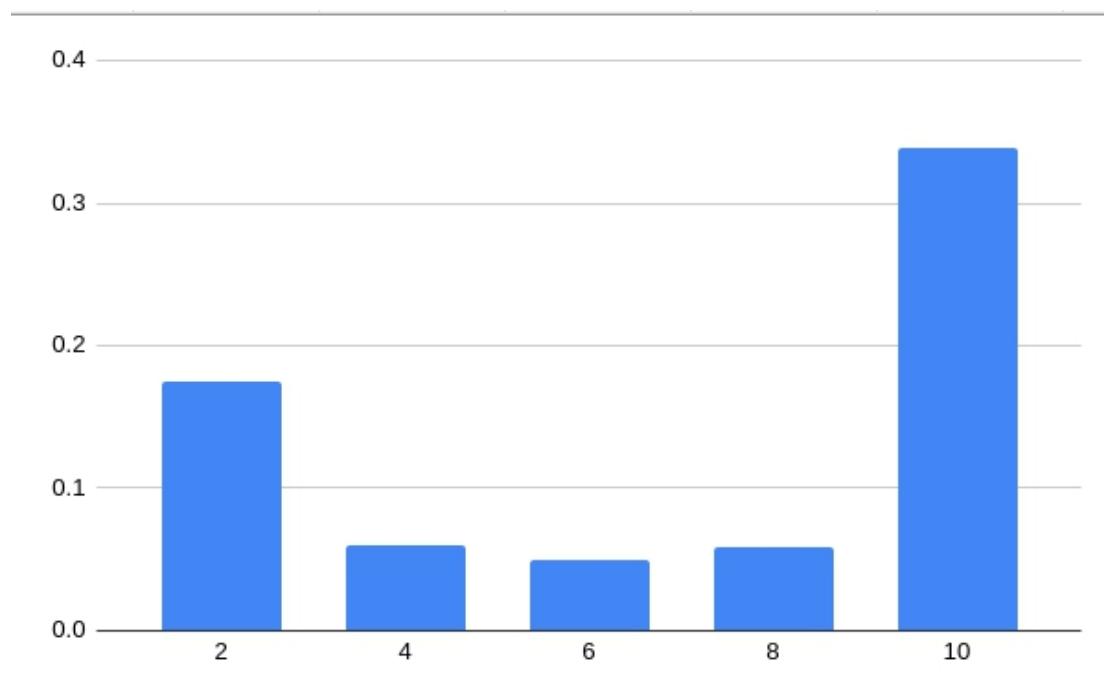
- 10connections

http						
No.	Time	Source	Destination	Protocol	Length	Info
1082	11.165031000	192.168.1.10	192.168.1.11	HTTP	402	GET / HTTP/1.1
1086	11.172109644	192.168.1.11	192.168.1.10	HTTP/X...	306	HTTP/1.1 401 Unauthorized
2375	23.862790858	192.168.1.10	192.168.1.11	HTTP	449	GET / HTTP/1.1
2377	23.871089226	192.168.1.11	192.168.1.10	HTTP/X...	1754	HTTP/1.1 401 Unauthorized
3590	33.554736747	192.168.1.10	192.168.1.11	HTTP	445	GET / HTTP/1.1
3598	33.5549114314	192.168.1.10	192.168.1.11	HTTP	445	GET / HTTP/1.1
3600	33.554696590	192.168.1.11	192.168.1.10	HTTP	911	HTTP/1.1 200 OK (text/html)
3615	33.767843305	192.168.1.10	192.168.1.11	HTTP	480	GET /1.jpg HTTP/1.1
3626	33.79671659	192.168.1.10	192.168.1.11	HTTP	479	GET /2.jpg HTTP/1.1
3629	33.799416506	192.168.1.11	192.168.1.11	HTTP	480	GET /3.jpg HTTP/1.1
3633	33.800413713	192.168.1.10	192.168.1.11	HTTP	480	GET /4.jpg HTTP/1.1
3636	33.800636020	192.168.1.10	192.168.1.11	HTTP	480	GET /5.jpg HTTP/1.1
3641	33.802438507	192.168.1.10	192.168.1.11	HTTP	480	GET /6.jpg HTTP/1.1
3642	33.802518546	192.168.1.10	192.168.1.11	HTTP	480	GET /7.jpg HTTP/1.1
3644	33.804487537	192.168.1.11	192.168.1.10	HTTP	327	HTTP/1.1 304 Not Modified
3646	33.804790835	192.168.1.11	192.168.1.10	HTTP	327	HTTP/1.1 304 Not Modified
3653	33.811041015	192.168.1.11	192.168.1.10	HTTP	328	HTTP/1.1 304 Not Modified
3656	33.812108715	192.168.1.11	192.168.1.10	HTTP	328	HTTP/1.1 304 Not Modified
3658	33.812206494	192.168.1.11	192.168.1.10	HTTP	328	HTTP/1.1 304 Not Modified
3660	33.814096143	192.168.1.11	192.168.1.10	HTTP	328	HTTP/1.1 304 Not Modified
3662	33.815098239	192.168.1.11	192.168.1.10	HTTP	328	HTTP/1.1 304 Not Modified
3664	33.816744000	192.168.1.10	192.168.1.11	HTTP	480	GET /8.jpg HTTP/1.1
3665	33.817563249	192.168.1.10	192.168.1.11	HTTP	480	GET /9.jpg HTTP/1.1
3666	33.818690431	192.168.1.10	192.168.1.11	HTTP	481	GET /10.jpg HTTP/1.1
3669	33.823464842	192.168.1.11	192.168.1.10	HTTP	327	HTTP/1.1 304 Not Modified
3671	33.823480557	192.168.1.11	192.168.1.10	HTTP	327	HTTP/1.1 304 Not Modified
3674	33.823731081	192.168.1.11	192.168.1.10	HTTP	327	HTTP/1.1 304 Not Modified
3687	33.8892986369	192.168.1.10	192.168.1.11	HTTP	397	GET /favicon.ico HTTP/1.1
3693	33.9000127940	192.168.1.11	192.168.1.10	HTTP/X...	155	HTTP/1.1 404 Not Found

- Observations from task 3 :

Calculations and tabulating load time using wireshark :

Persistence	First GET time	Last Response	Load time
0	30.19360	32.71399	2.52039
2	6.14296	6.31726	0.1743
4	1.25244	1.31274	0.0603
6	1.45592	1.50563	0.04971
8	1.16003	1.21852	0.05849
10	33.55469	33.89298	0.33829



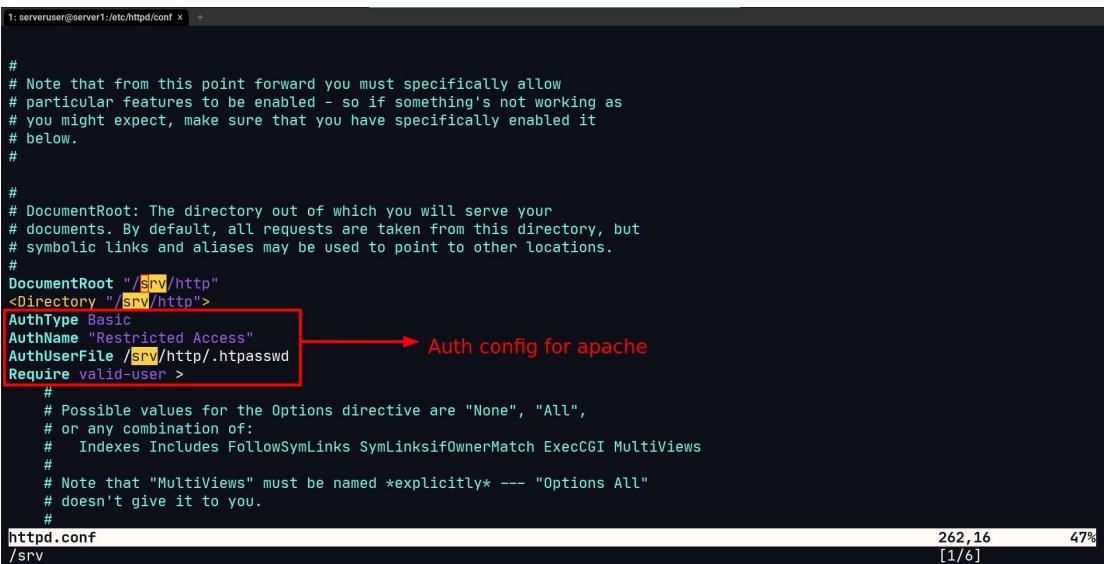
It is observed that the best number of persistent connection is 6.

Task 4 : Authentication in Apache server

- Create a .htpasswd file in any place in the system preferably outside the server root. Like so :

```
[[prod]serveruser@server1 conf]$sudo htpasswd -c /srv/http/.htpasswd navin
New password:
Re-type new password:
Adding password for user navin
[[prod]serveruser@server1 conf]$
```

- Edit the apache config file in /etc/httpd/conf/httpd.conf file as so :



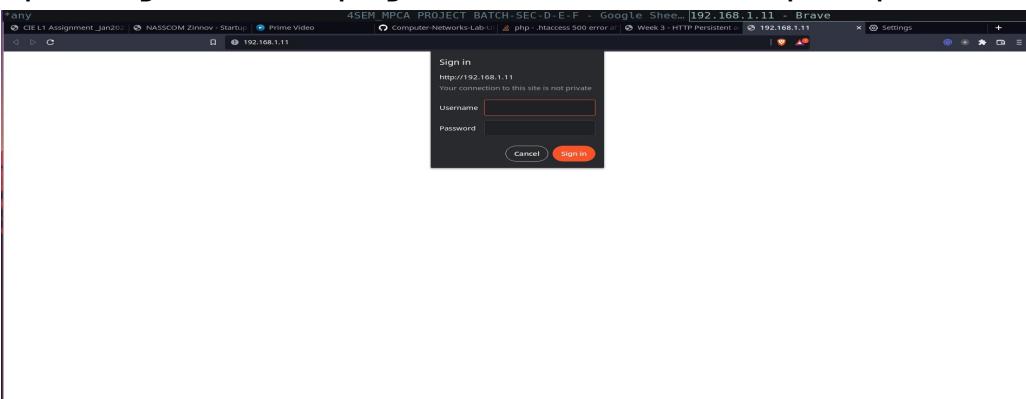
```
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
# DocumentRoot "/srv/http"
<Directory "/srv/http">
AuthType Basic
AuthName "Restricted Access"
AuthUserFile /srv/http/.htpasswd
Require valid-user >
#
# Possible values for the Options directive are "None", "All",
# or any combination of:
#   Indexes Includes FollowSymLinks SymLinksIfOwnerMatch ExecCGI MultiViews
#
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
#

```

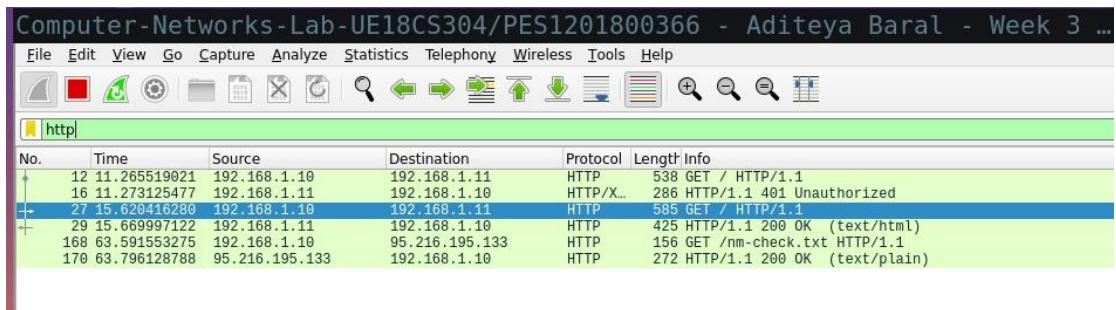
- Create an .htaccess file in the server route with the following contents :

```
[[prod]serveruser@server1 http]$ls -a
.. 10.jpg 1.jpg 2.jpg 3.jpg 4.jpg 5.jpg 6.jpg 7.jpg 8.jpg 9.jpg .htaccess .htpasswd index.html index.php
[[prod]serveruser@server1 http]$cat .htaccess
AuthType Basic
AuthName "Restricted Access"
AuthUserFile /srv/http/.htpasswd
Require valid-user >
```

- Opening the webpage should lead to prompt :



- Analyzing the packets in wireshark :



```

48
If you think this is a server error, please contact
the <a href="mailto:
28
you@example.com">webmaster</a>.

11
</p>
<h2>Error
21
401</h2>
<address>
<a href="/">
1f
192.168.1.11</a><br />
<span>
37
Apache/2.4.52 (Unix)</span>
</address>
</body>
</html>

1

0

GET / HTTP/1.1
Host: 192.168.1.11
Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic bmF2aW46a2FrYw5hMDcxMTI5
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-GPC: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

HTTP/1.1 200 OK
Date: Thu, 10 Feb 2022 10:39:00 GMT
Server: Apache/2.4.52 (Unix)
Last-Modified: Thu, 10 Feb 2022 10:38:35 GMT
ETag: "4d-5d7a78d62238d"
Accept-Ranges: bytes
Content-Length: 77
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html

<html>
  <body>
    <h1>Hello world</h1>
    <h2>The images :</h2>
  </body>
</html>

```

- Analyzing base64 Auth cipher text :

As the Authentication follows a base 64 addressing, each letter in cipher is of 6 bits and which can later be converted to ascii of 8 bits each, this gives us :

011011 100110 000101 110110 011010 010110 111000 111010

011011 100110 000101 110110 011010 010110 111000 110001

001100 100011 001100 110100

rearranging to ascii 8 bits :

01101110 01100001 01110110 01101001 01101110 00111010

01101110 01100001 01110110 01101001 01101110 00110001

00110010 00110011 00110100

This leads to : navin:navin1234, whcih was indeed my
username:password

Task 5 : Cookies using PHP

- For this a new index.php file is created in the server root, which has html content with php embedded, like so :

```
[[prod]serveruser@server1 http]$ls -a
[... 10.jpg 1.jpg 2.jpg 3.jpg 4.jpg 5.jpg 6.jpg 7.jpg 8.jpg 9.jpg .htaccess .htpasswd index.html index.php
[[prod]serveruser@server1 http]$cat index.php
<html>
<?php
    setcookie("SRN","PES2UG20CS237");
    setcookie("Name","Navin Shrinivas",time()+125);
?>
<body>
<h1>Hello world</h1>
</body>
</html>
[[prod]serveruser@server1 http]$
```

- PHP is enabled in the apache server by editing the conf file, like so :

```
1: serveruser@server1:/etc/httpd/conf x +
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
LoadModule php_module modules/libphp.so
AddHandler php-script .php
Include conf/extr/php_module.conf
```

Configuring for apache
after installing php package

```
#LoadModule mpm_event_module modules/mod_mpm_event.so
LoadModule mpm_prefork_module modules/mod_mpm_prefork.so
#LoadModule mpm_worker_module modules/mod_mpm_worker.so
LoadModule authn_file_module modules/mod_authn_file.so
#LoadModule authn_dbm_module modules/mod_authn_dbm.so
#LoadModule authn_anon_module modules/mod_authn_anon.so
#LoadModule authn_dbd_module modules/mod_authn_dbd.so
#LoadModule authn_socache_module modules/mod_authn_socache.so
LoadModule authn_core_module modules/mod_authn_core.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_groupfile_module modules/mod_authz_groupfile.so
LoadModule authz_user_module modules/mod_authz_user.so
#LoadModule authz_dbm_module modules/mod_authz_dbm.so
#LoadModule authz_owner_module modules/mod_authz_owner.so
httpd.conf
```

91,1 12%

- The PHP file is then accessed from the client and wireshark packets are analysed, the **set-cookie** can be seen :

```
GET /index.php HTTP/1.1
Host: 192.168.1.11
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.8
Sec-GPC: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
HTTP/1.1 200 OK
Date: Thu, 10 Feb 2022 12:22:00 GMT
Server: Apache/2.4.52 (Unix) PHP/8.1.2
X-Powered-By: PHP/8.1.2
Set-Cookie: SRN=PES2UG20CS237
Set-Cookie: Name=Navin%20Shrinivas; expires=Thu, 10-Feb-2022 12:24:05 GMT; Max-Age=125
Content-Length: 73
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<html>
    <body>
        <h1>Hello world</h1>
    </body>
</html>
```

Loaded Cookies

Task 6 : Conditional get

- A conditional HTTP request that carries data only if data has been modified. Apache servers are configured by default to do this
- Code 304 is for not modified, 200 is when the data is actually fetched successfully.
- Below is a demonstration of Conditional get using refreshing pages and wireshark :

Io.	Time	Source	Destination	Protocol	Length	Info
-	313	6.371231942	192.168.1.10	192.168.1.11	512	HTTP / 1.1
-	315	6.378657910	192.168.1.11	192.168.1.10	1754	HTTP/1.1 401 Unauthorized
336	11.093263393	192.168.1.10	192.168.1.11	HTTP	585	GET / HTTP/1.1
349	11.097224631	192.168.1.11	192.168.1.10	HTTP/X..	305	HTTP/1.1 401 Unauthorized
780	15.229525932	192.168.1.10	192.168.1.11	HTTP	504	GET / HTTP/1.1
822	15.262305240	192.168.1.11	192.168.1.10	HTTP	1026	HTTP/1.1 200 OK (text/html)
844	15.298691120	192.168.1.10	192.168.1.11	HTTP	490	GET /1.jpg HTTP/1.1
860	15.301822563	192.168.1.10	192.168.1.11	HTTP	490	GET /2.jpg HTTP/1.1
946	15.358457290	192.168.1.10	192.168.1.11	HTTP	490	GET /3.jpg HTTP/1.1
947	15.358564679	192.168.1.10	192.168.1.11	HTTP	490	GET /4.jpg HTTP/1.1
948	15.358620623	192.168.1.10	192.168.1.11	HTTP	490	GET /5.jpg HTTP/1.1
953	15.361985988	192.168.1.10	192.168.1.11	HTTP	490	GET /6.jpg HTTP/1.1
1912	16.239861980	192.168.1.11	192.168.1.10	HTTP	13989	HTTP/1.1 200 OK (JPEG JFIF image)
1917	16.231927360	192.168.1.10	192.168.1.11	HTTP	490	GET /7.jpg HTTP/1.1
2075	16.385961728	192.168.1.10	192.168.1.11	HTTP	490	GET /8.jpg HTTP/1.1
2082	16.388990923	192.168.1.10	192.168.1.11	HTTP	490	GET /9.jpg HTTP/1.1
2123	16.423195980	192.168.1.11	192.168.1.10	HTTP	7315	HTTP/1.1 200 OK (JPEG JFIF image)
2128	16.424825887	192.168.1.10	192.168.1.11	HTTP	490	GET /10.jpg HTTP/1.1
2464	16.770485349	192.168.1.11	192.168.1.10	HTTP	12761	HTTP/1.1 200 OK (JPEG JFIF image)
2684	16.950966080	192.168.1.11	192.168.1.10	HTTP	13256	HTTP/1.1 200 OK (JPEG JFIF image)
2921	17.161851756	192.168.1.11	192.168.1.10	HTTP	11181	HTTP/1.1 200 OK (JPEG JFIF image)
3209	17.419650550	192.168.1.11	192.168.1.10	HTTP	18998	HTTP/1.1 200 OK (JPEG JFIF image)
6928	47.313003136	192.168.1.10	192.168.1.11	HTTP	667	GET / HTTP/1.1
6930	47.317779920	192.168.1.11	192.168.1.10	HTTP	325	HTTP/1.1 304 Not Modified
6998	54.488352280	192.168.1.10	95.216.195.133	HTTP	100	GET /image-check.txt HTTP/1.1
7001	54.689551061	95.216.195.133	192.168.1.10	HTTP	272	HTTP/1.1 200 OK (text/plain)

Frame 313: 512 bytes on wire (4096 bits), 512 bytes captured (4096 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.11
Transmission Control Protocol, Src Port: 58408, Dst Port: 80, Seq: 1, Ack: 1, Len: 444
HyperText Transfer Protocol
 GET / HTTP/1.1\r\n Host: 192.168.1.11\r\n Connection: keep-alive\r\n Upgrade-Insecure-Requests: 1\r\n User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
 Sec-GPC: 1
 Accept-Encoding: gzip, deflate
 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

When refreshing, 304

Wire shark overlook

```
</html>
GET / HTTP/1.1
Host: 192.168.1.11
Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic bmF2aW46bmF2aW4xMjM0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-GPC: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

HTTP/1.1 200 OK
Date: Thu, 10 Feb 2022 12:29:09 GMT
Server: Apache/2.4.52 (Unix) PHP/8.1.2
Last-Modified: Thu, 10 Feb 2022 11:19:23 GMT
ETag: "29a-5d7a1f4bf0a9"
Accept-Ranges: bytes
Content-Length: 666
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html

<?php
    setcookie("SRN", "PES2UG20CS237");
    setcookie("Name", "Navin Shrinivas", time() + 125);
```

200 status on first load after clearing cache

```
GET / HTTP/1.1
Host: 192.168.1.11
Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic bmF2aW46bmF2aW4xMjM0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-GPC: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
If-None-Match: "29a-5d7a81f4bf0a9"
If-Modified-Since: Thu, 10 Feb 2022 11:19:23 GMT

HTTP/1.1 304 Not Modified
Date: Thu, 10 Feb 2022 12:29:41 GMT
Server: Apache/2.4.52 (Unix) PHP/8.1.2
Last-Modified: Thu, 10 Feb 2022 11:19:23 GMT
ETag: "29a-5d7a81f4bf0a9"
Accept-Ranges: bytes
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

304 not modified

304 not modified status after refreshing