HTTP Header Analysis of the Chameleon website

By

Usman Tariq

S217034263

S217034263@deakin.edu.au

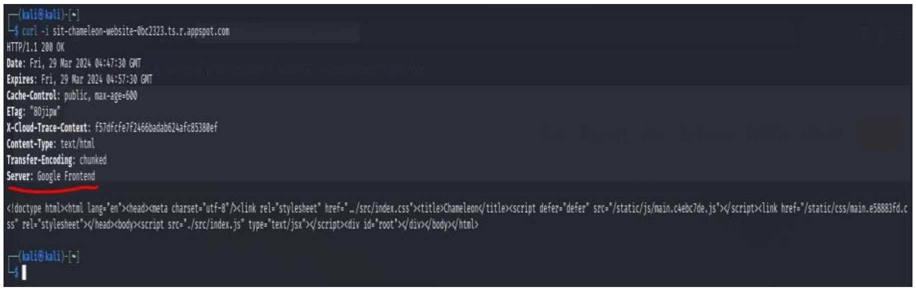
&

Sanchit Mahajan

Using CURl command in terminal

curl -i sit-chameleon-website-0bc2323.ts.r.appspot.com

We need to run the above command in terminal to see HTTP header.

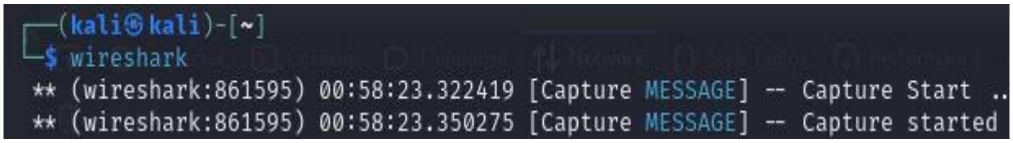


```
┌──(kali㉿kali)-[~]
└─$ curl -i sit-chameleon-website-0bc2323.ts.r.appspot.com
HTTP/1.1 200 OK
Date: Fri, 29 Mar 2024 04:47:30 GMT
Expires: Fri, 29 Mar 2024 04:57:30 GMT
Cache-Control: public, max-age=600
ETag: "80jipw"
X-Cloud-Trace-Context: f57dfcfe7f2466badab624afc85380ef
Content-Type: text/html
Transfer-Encoding: chunked
Server: Google Frontend

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="stylesheet" href="../src/index.css"><title>Chameleon</title><script defer="defer" src="/static/js/main.c4ebc7de.js"></script><link href="/static/css/main.e58883fd.c
ss" rel="stylesheet"></head><body><script src="./src/index.js" type="text/jsx"></script><div id="root"></div></body></html>

┌──(kali㉿kali)-[~]
└─$ 
```

As we can see from the above screenshot server is responding ok and there's no apparent vulnerability.

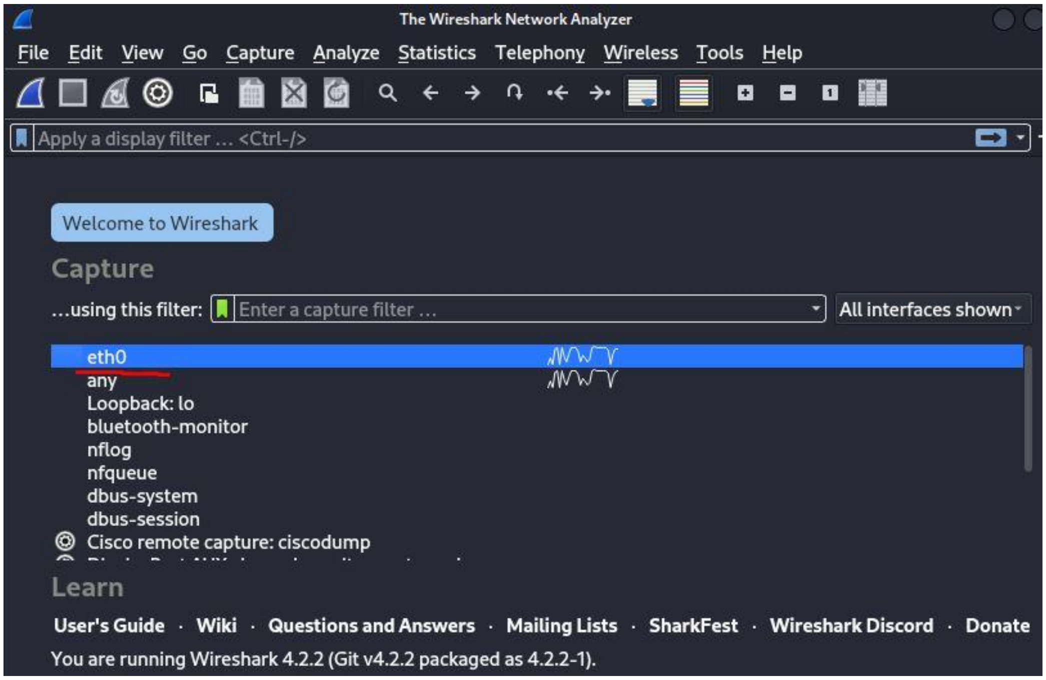
Using wireshark

As we can't find any issues with HTTP header while using 'CURL' command. Now we need to test the same with the wireshark. To do so we need to launch wireshark as shown below.



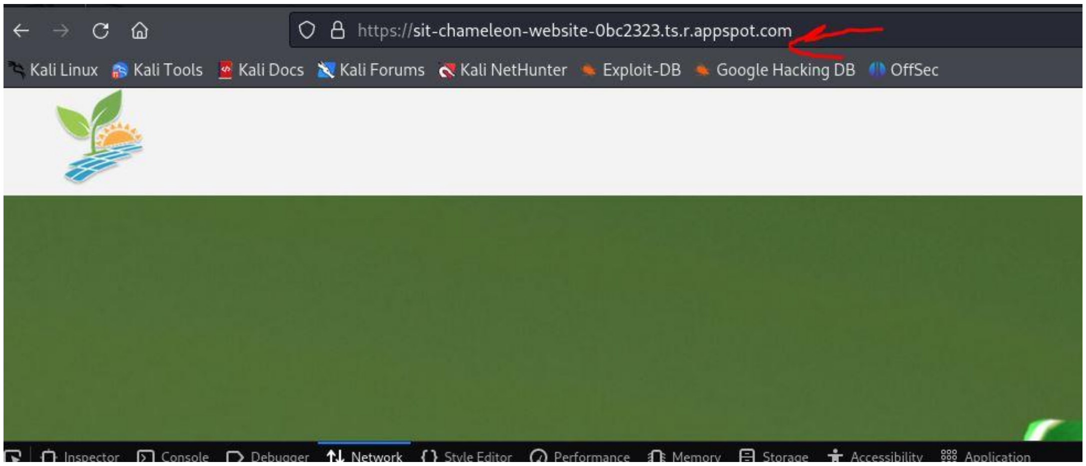
```
┌──(kali㉿kali)-[~]
└─$ wireshark
 ** (wireshark:861595) 00:58:23.322419 [Capture MESSAGE] -- Capture Start ..
 ** (wireshark:861595) 00:58:23.350275 [Capture MESSAGE] -- Capture started
```

We'll get the following screen select the interface 'eth0'

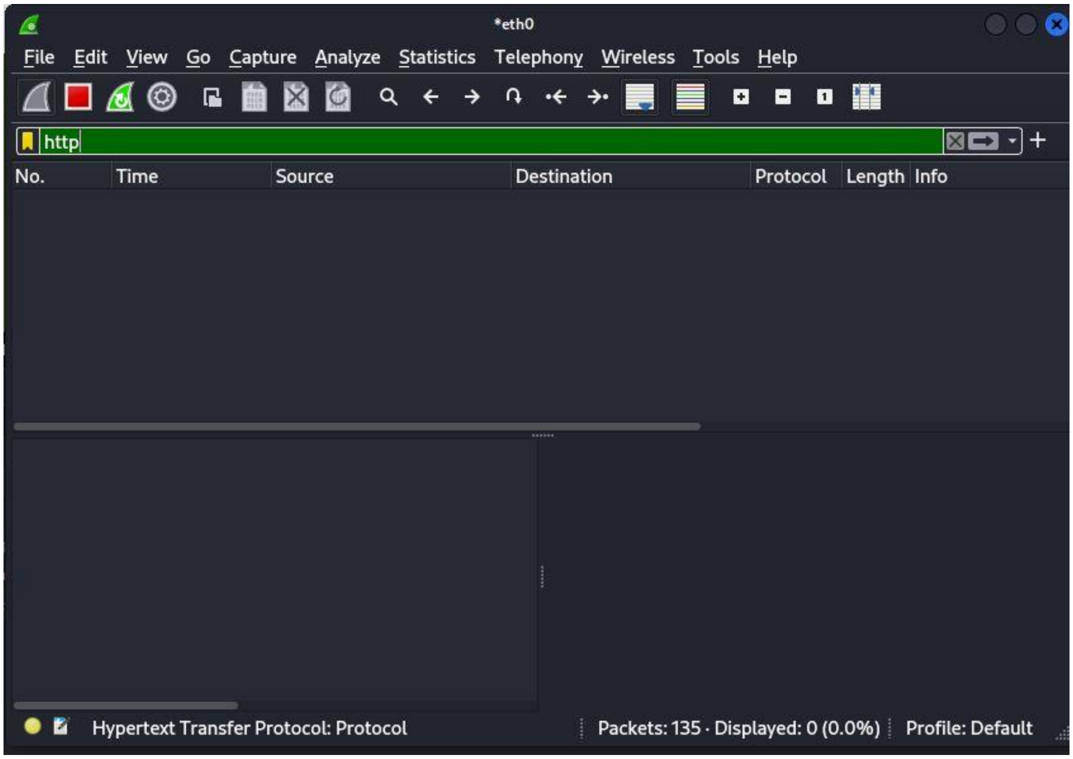

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.2 (Git v4.2.2 packaged as 4.2.2-1).

Also we need to open the website in browser as shown below


https://sit-chameleon-website-0bc2323.ts.r.appspot.com

In filters bar at the top enter ‘http’


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

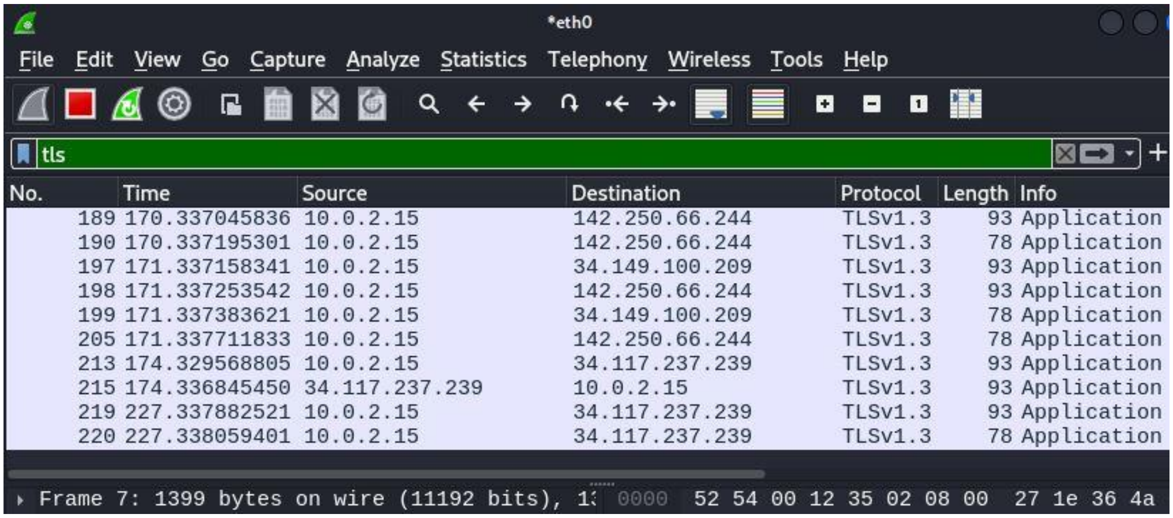
No.	Time	Source	Destination	Protocol	Length	Info

Hypertext Transfer Protocol: Protocol

Packets: 135 · Displayed: 0 (0.0%)

Profile: Default

After typing 'http' in filters bar we got no packets. As shown above. This indicates all packets are secured they might be running on 'https' so we need to change the filter to 'tls'.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

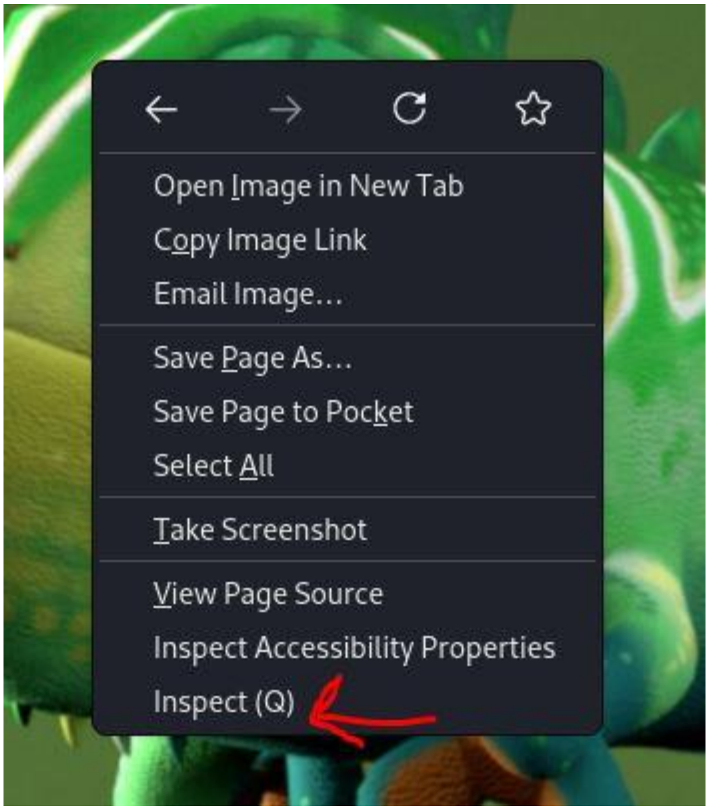
No.	Time	Source	Destination	Protocol	Length	Info
189	170.337045836	10.0.2.15	142.250.66.244	TLSv1.3	93	Application
190	170.337195301	10.0.2.15	142.250.66.244	TLSv1.3	78	Application
197	171.337158341	10.0.2.15	34.149.100.209	TLSv1.3	93	Application
198	171.337253542	10.0.2.15	142.250.66.244	TLSv1.3	93	Application
199	171.337383621	10.0.2.15	34.149.100.209	TLSv1.3	78	Application
205	171.337711833	10.0.2.15	142.250.66.244	TLSv1.3	78	Application
213	174.329568805	10.0.2.15	34.117.237.239	TLSv1.3	93	Application
215	174.336845450	34.117.237.239	10.0.2.15	TLSv1.3	93	Application
219	227.337882521	10.0.2.15	34.117.237.239	TLSv1.3	93	Application
220	227.338059401	10.0.2.15	34.117.237.239	TLSv1.3	78	Application

```
› Frame 7: 1399 bytes on wire (11192 bits), 1:  0000  52 54 00 12 35 02 08 00  27 1e 36 4a
```

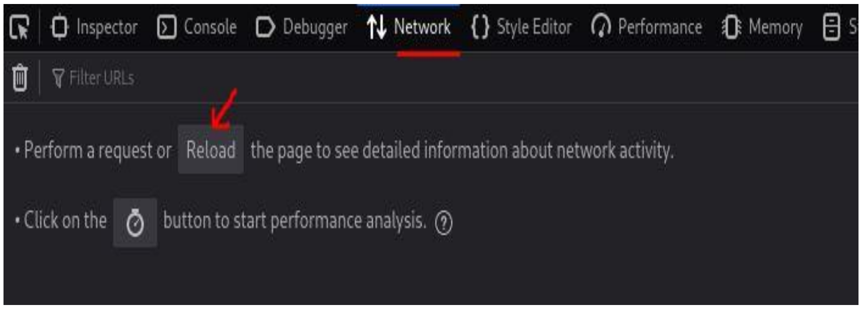
This indicates that http header is responding ok and there is no apparent vulnerability.

Using Browser Developer tools

After analyzing 'HTTP header' using two tools we can use another tool. Which is built in the most modern web browsers. To access it we need to do the following.



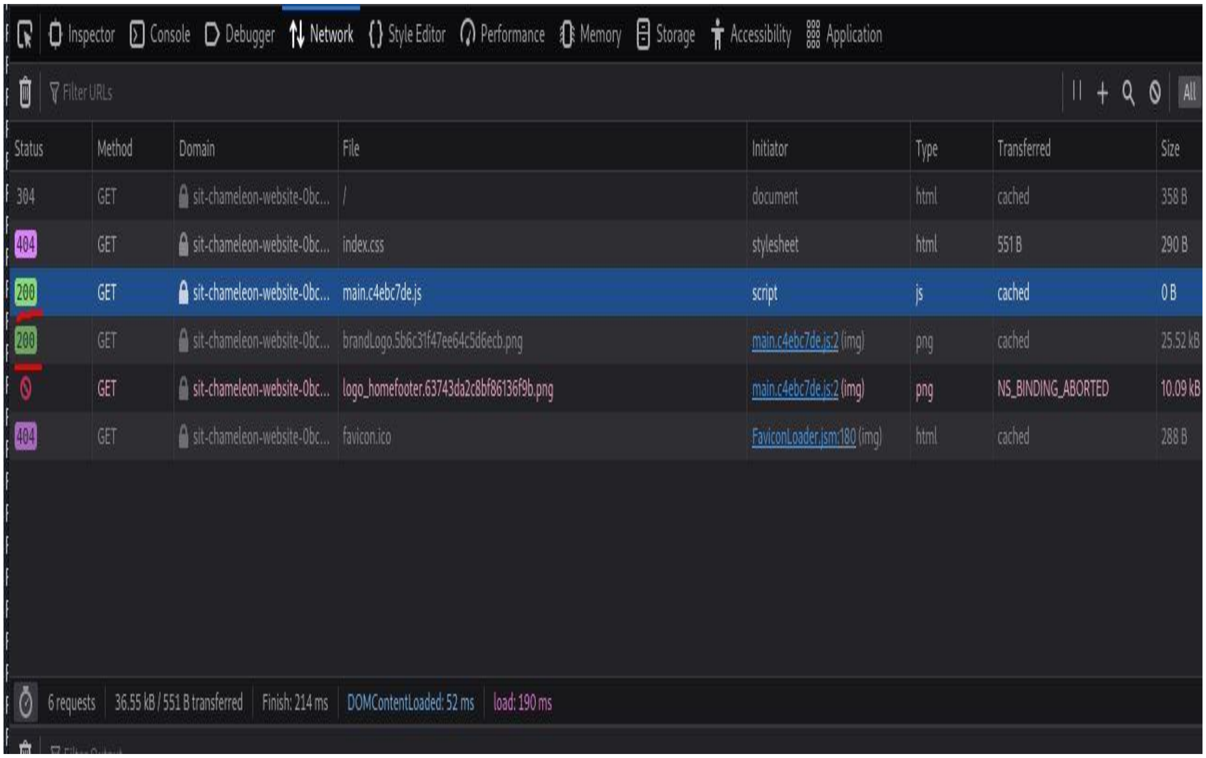
As we can see from above screenshot we need to right click on any part of the page and go to the inspect option. We'll get the following.



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

• Click on the button to start performance analysis.

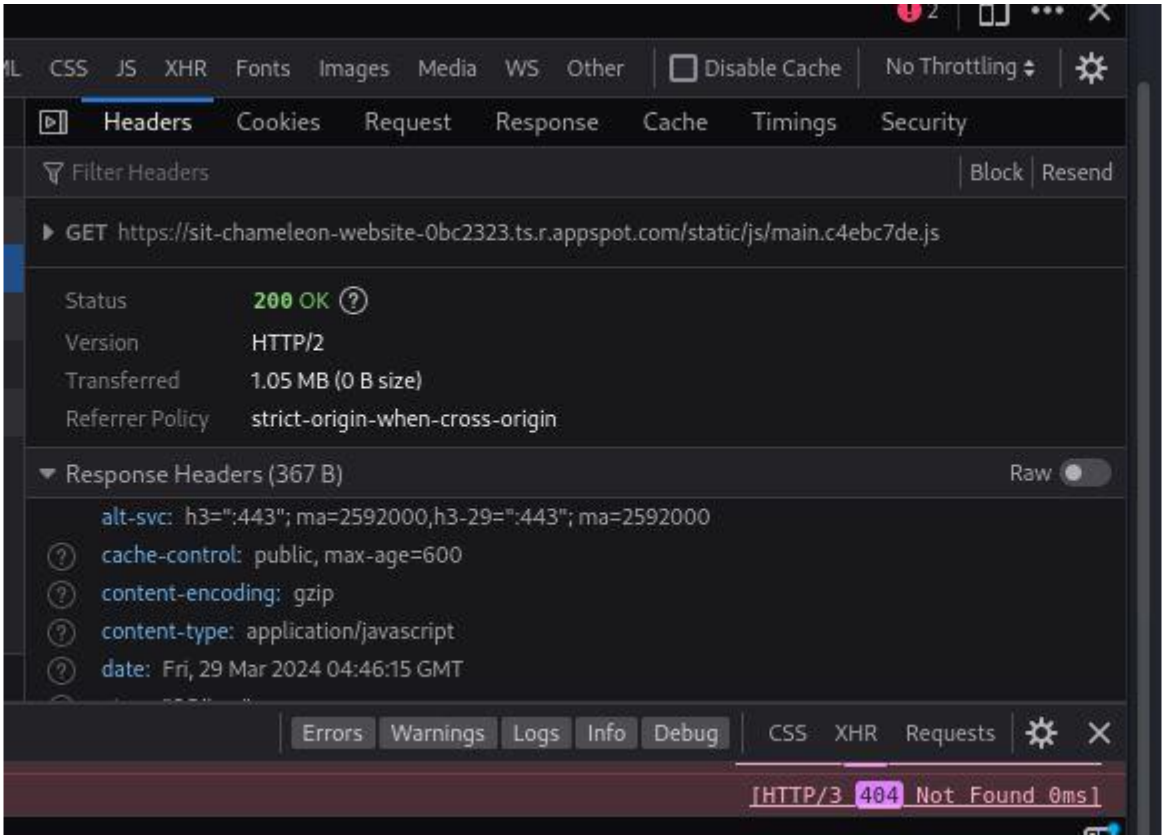
After that we need to go to the 'Network' tab and click 'Reload' as shown in above screenshot. We'll see the following screen.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
304	GET	sit-chameleon-website-0bc...	/	document	html	cached	358 B
404	GET	sit-chameleon-website-0bc...	index.css	stylesheet	html	551 B	290 B
200	GET	sit-chameleon-website-0bc...	main.c4ebc7de.js	script	js	cached	0 B
200	GET	sit-chameleon-website-0bc...	brandLogo.5b6c31f47ee64c5d6ecb.png	main.c4ebc7de.js:2 (img)	png	cached	25.52 kB
⊘	GET	sit-chameleon-website-0bc...	logo_homefooter.63743da2c8bf86136f9b.png	main.c4ebc7de.js:2 (img)	png	NS_BINDING_ABORTED	10.09 kB
404	GET	sit-chameleon-website-0bc...	favicon.ico	FaviconLoader.jsm:180 (img)	html	cached	288 B

6 requests | 36.55 kB / 551 B transferred | Finish: 214 ms | DOMContentLoaded: 52 ms | load: 190 ms

Now we need to click on '200' under status option. We'll get the following on the right side of the screen.



GET https://sit-chameleon-website-0bc2323.ts.r.appspot.com/static/js/main.c4ebc7de.js

Status 200 OK
Version HTTP/2
Transferred 1.05 MB (0 B size)
Referrer Policy strict-origin-when-cross-origin

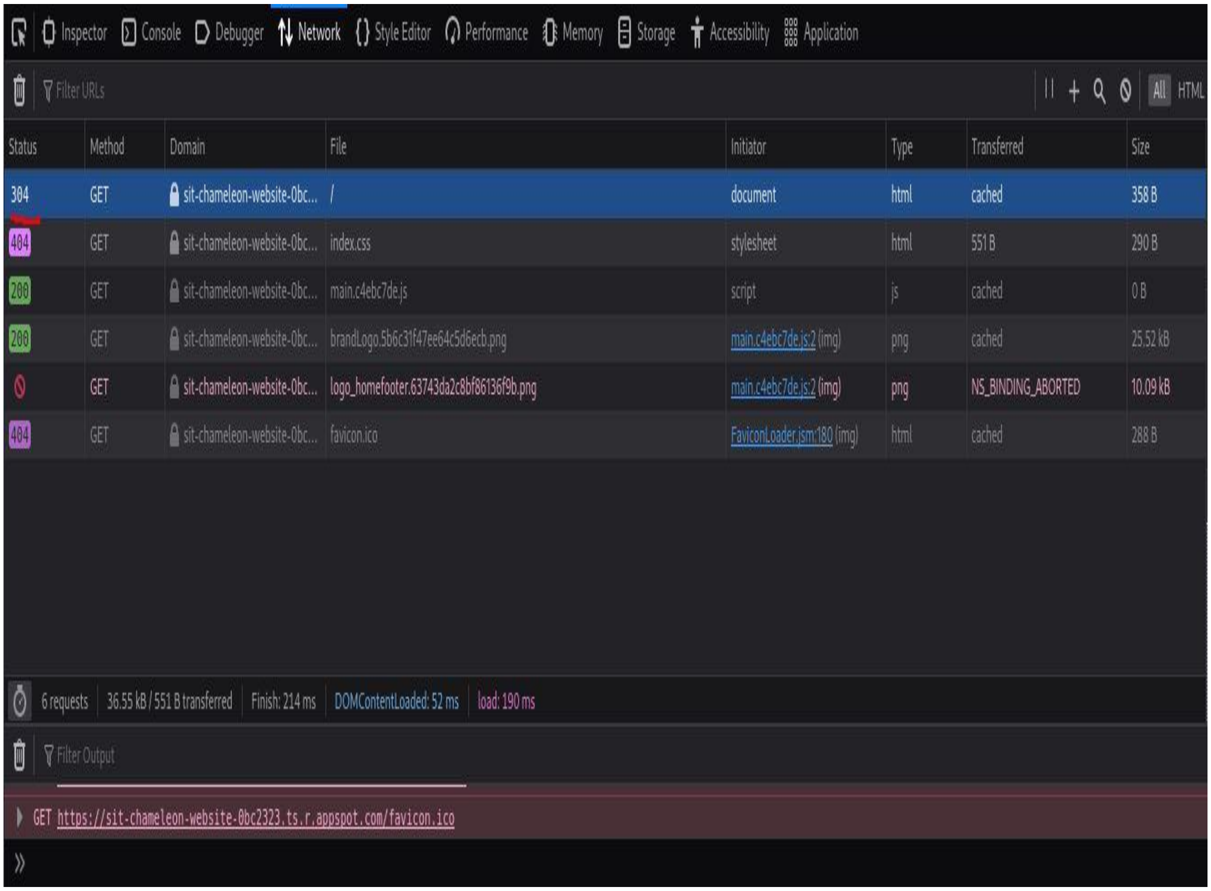
Response Headers (367 B)

alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
cache-control: public, max-age=600
content-encoding: gzip
content-type: application/javascript
date: Fri, 29 Mar 2024 04:46:15 GMT

[HTTP/3 404 Not Found 0ms]

This above screen indicates that communication with the server was successful and secure.

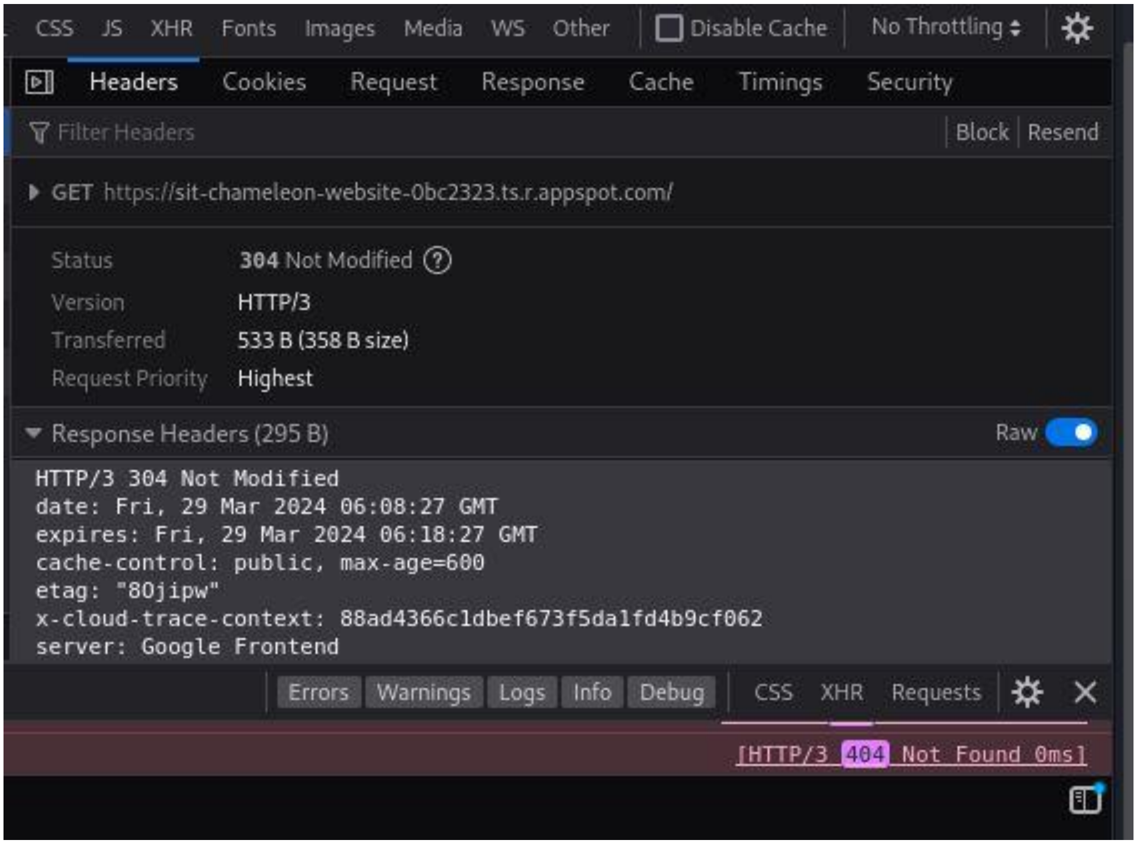
We also got the following which indicates that resource hasn’t been modified since the last request. Which indicates that there was no unnecessary data transfer.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
304	GET	sit-chameleon-website-0bc...	/	document	html	cached	358 B
404	GET	sit-chameleon-website-0bc...	index.css	stylesheet	html	551 B	290 B
200	GET	sit-chameleon-website-0bc...	main.c4ebc7de.js	script	js	cached	0 B
200	GET	sit-chameleon-website-0bc...	brandLogo.5b6c31f47ee64c5d6ecb.png	main.c4ebc7de.js:2 (img)	png	cached	25.52 kB
⊘	GET	sit-chameleon-website-0bc...	logo_homefooter.63743da2c8bf86136f9b.png	main.c4ebc7de.js:2 (img)	png	NS_BINDING_ABORTED	10.09 kB
404	GET	sit-chameleon-website-0bc...	favicon.ico	FaviconLoader.jsm:180 (img)	html	cached	288 B

6 requests | 36.55 kB / 551 B transferred | Finish: 214 ms | DOMContentLoaded: 52 ms | load: 190 ms

```
GET https://sit-chameleon-website-0bc2323.ts.r.appspot.com/favicon.ico
```



GET https://sit-chameleon-website-0bc2323.ts.r.appspot.com/

Status 304 Not Modified

Version HTTP/3

Transferred 533 B (358 B size)

Request Priority Highest

Response Headers (295 B)

```
HTTP/3 304 Not Modified
date: Fri, 29 Mar 2024 06:08:27 GMT
expires: Fri, 29 Mar 2024 06:18:27 GMT
cache-control: public, max-age=600
etag: "80jipw"
x-cloud-trace-context: 88ad4366c1dbef673f5da1fd4b9cf062
server: Google Frontend
```

```
[HTTP/3 404 Not Found 0ms]
```