Lab 9: Hacking Web Servers Part 2

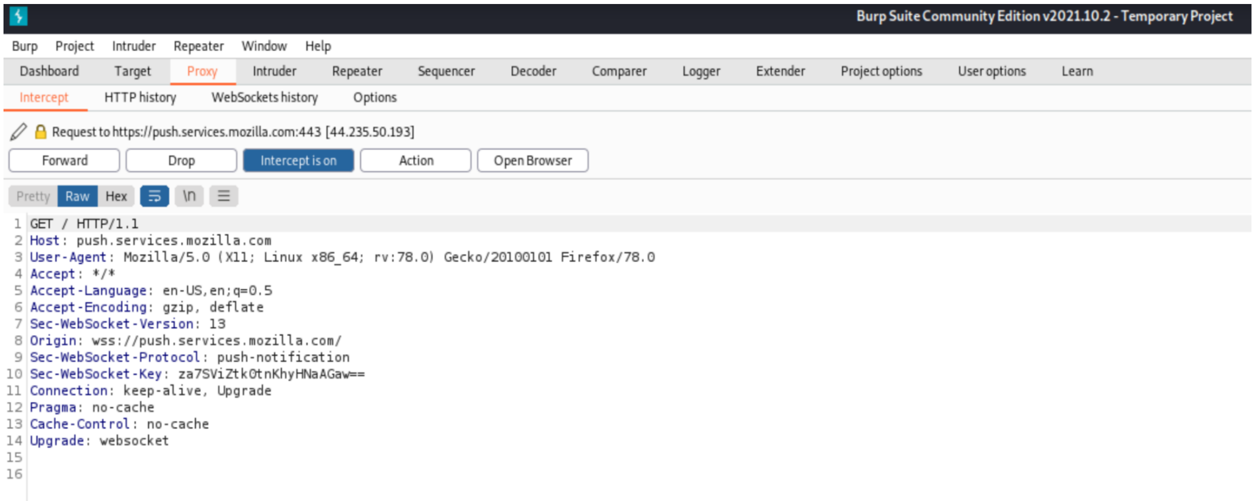
Introduction:

Proxy listeners such as Burp Suite are another incredibly useful tool for hackers and penetration testers to exploit vulnerabilities in web applications. Much like packet sniffers, proxy listeners allow for the capture and analysis of traffic on a network. In this lab, we will demonstrate the use of proxy listeners using Burpsuite Community Edition.

Part 1: Using Burpsuite

Burpsuite comes preinstalled on our kali VM, and can be easily configured to work with our default web browser Firefox. The result is shown below.

Figure 1: Burpsuite Awaiting a Response



Burp Suite Community Edition v2021.10.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex \n

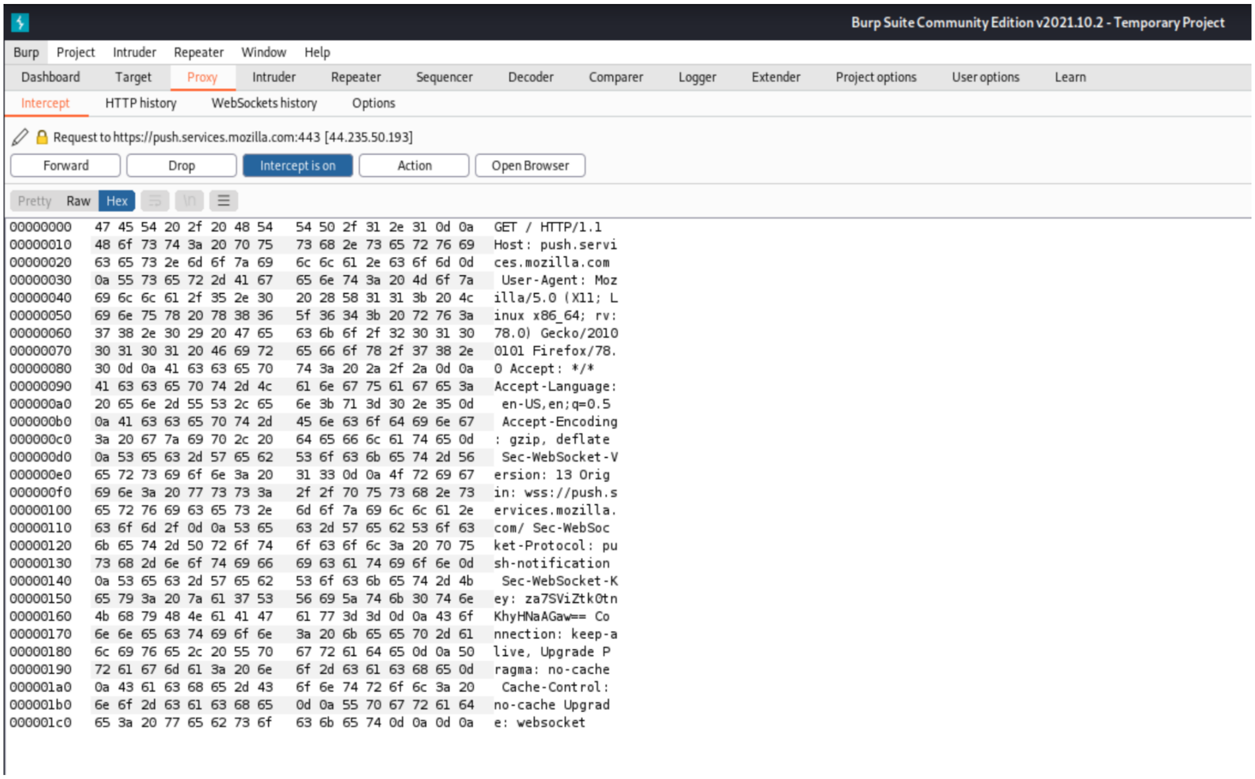
Request to https://push.services.mozilla.com:443 [44.235.50.193]

```
GET / HTTP/1.1
Host: push.services.mozilla.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Sec-WebSocket-Version: 13
Origin: wss://push.services.mozilla.com/
Sec-WebSocket-Protocol: push-notification
Sec-WebSocket-Key: za7SViZtk0tnKhyHNaAGaw==
Connection: keep-alive, Upgrade
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket


```

Here we see the raw request that gets routed through the burp proxy when we open Firefox.

Figure 2: Burpsuite Hex Dump



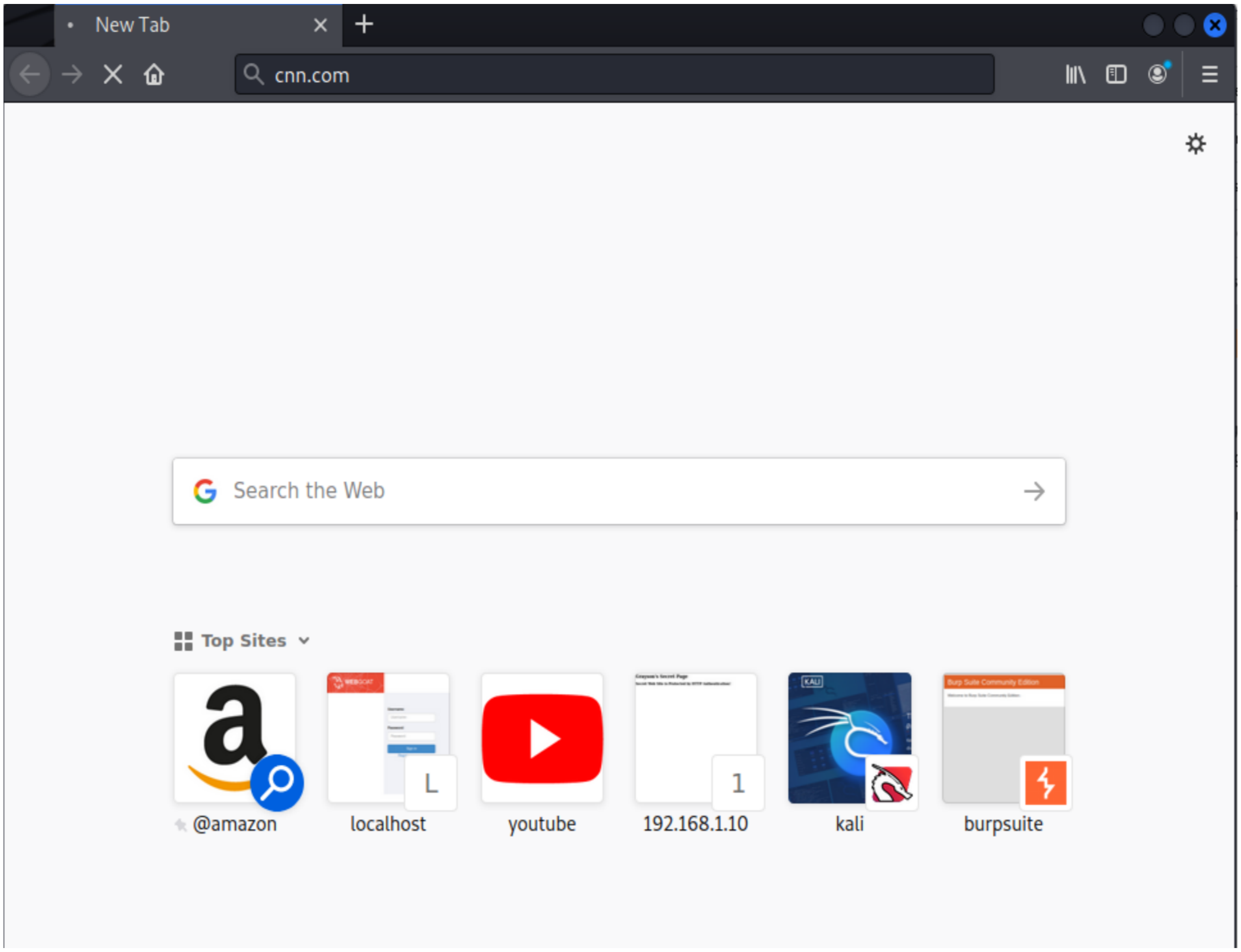
Burp Suite Community Edition v2021.10.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex

Request to https://push.services.mozilla.com:443 [44.235.50.193]

```
00000000   47 45 54 20 2f 20 48 54   54 50 2f 31 2e 31 0d 0a   GET / HTTP/1.1
00000010   48 6f 73 74 3a 20 70 75   73 68 2e 73 65 72 76 69   Host: push.servi
00000020   63 65 73 2e 6d 6f 7a 69   6c 6c 61 2e 63 6f 6d 0d   ces.mozilla.com
00000030   0a 55 73 65 72 2d 41 67   65 6e 74 3a 20 4d 6f 7a    User-Agent: Moz
00000040   69 6c 6c 61 2f 35 2e 30   20 28 58 31 31 3b 20 4c   illa/5.0 (X11; L
00000050   69 6e 75 78 20 78 38 36   5f 36 34 3b 20 72 76 3a   inux x86_64; rv:
00000060   37 38 2e 30 29 20 47 65   63 6b 6f 2f 32 30 31 30   78.0) Gecko/2010
00000070   30 31 30 31 20 46 69 72   65 66 6f 78 2f 37 38 2e   0101 Firefox/78.
00000080   30 0d 0a 41 63 63 65 70   74 3a 20 2a 2f 2a 0d 0a   0 Accept: */*
00000090   41 63 63 65 70 74 2d 4c   61 6e 67 75 61 67 65 3a   Accept-Language:
000000a0   20 65 6e 2d 55 53 2c 65   6e 3b 71 3d 30 2e 35 0d    en-US,en;q=0.5
000000b0   0a 41 63 63 65 70 74 2d   45 6e 63 6f 64 69 6e 67    Accept-Encoding
000000c0   3a 20 67 7a 69 70 2c 20   64 65 66 6c 61 74 65 0d   : gzip, deflate
000000d0   0a 53 65 63 2d 57 65 62   53 6f 63 6b 65 74 2d 56    Sec-WebSocket-V
000000e0   65 72 73 69 6f 6e 3a 20   31 33 0d 0a 4f 72 69 67   ersion: 13 Orig
000000f0   69 6e 3a 20 77 73 73 3a   2f 2f 70 75 73 68 2e 73   in: wss://push.s
00000100   65 72 76 69 63 65 73 2e   6d 6f 7a 69 6c 6c 61 2e   ervices.mozilla.
00000110   63 6f 6d 2f 0d 0a 53 65   63 2d 57 65 62 53 6f 63   com/ Sec-WebSoc
00000120   6b 65 74 2d 50 72 6f 74   6f 63 6f 6c 3a 20 70 75   ket-Protocol: pu
00000130   73 68 2d 6e 6f 74 69 66   69 63 61 74 69 6f 6e 0d   sh-notification
00000140   0a 53 65 63 2d 57 65 62   53 6f 63 6b 65 74 2d 4b    Sec-WebSocket-K
00000150   65 79 3a 20 7a 61 37 53   56 69 5a 74 6b 30 74 6e   ey: za7SViZtk0tn
00000160   4b 68 79 48 4e 61 41 47   61 77 3d 3d 0d 0a 43 6f   KhyHNaAGaw== Co
00000170   6e 6e 65 63 74 69 6f 6e   3a 20 6b 65 65 70 2d 61   nnection: keep-a
00000180   6c 69 76 65 2c 20 55 70   67 72 61 64 65 0d 0a 50   live, Upgrade P
00000190   72 61 67 6d 61 3a 20 6e   6f 2d 63 61 63 68 65 0d   ragma: no-cache
000001a0   0a 43 61 63 68 65 2d 43   6f 6e 74 72 6f 6c 3a 20    Cache-Control:
000001b0   6e 6f 2d 63 61 63 68 65   0d 0a 55 70 67 72 61 64   no-cache Upgrad
000001c0   65 3a 20 77 65 62 73 6f   63 6b 65 74 0d 0a 0d 0a   e: websocket
```

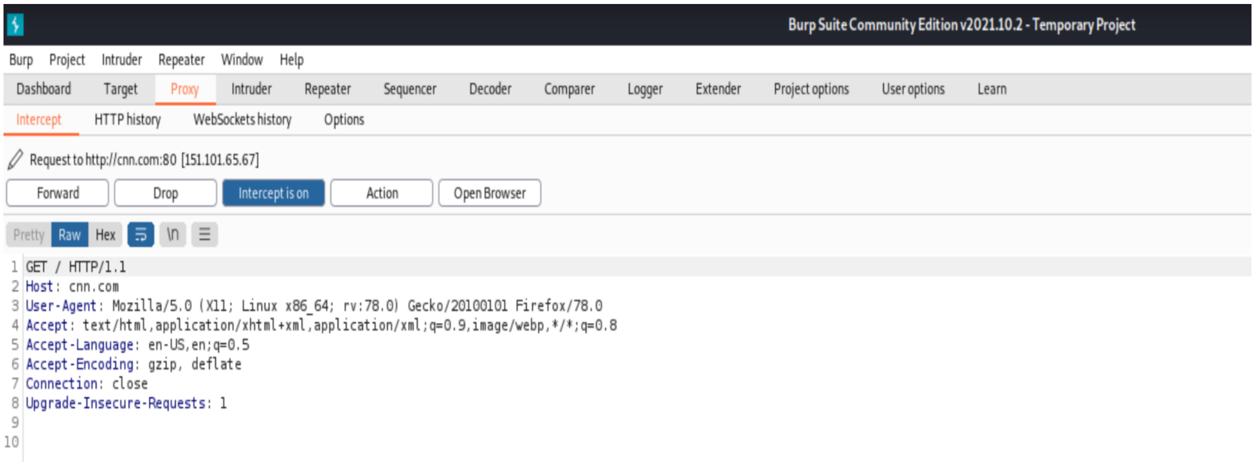
We can also view a hexdump of the request if needed

Figure 3: Firefox Waiting For Forwarded Request



When we try to access a URL, the Firefox hangs because it has not yet received the request. The request at this point has been intercepted by burp, and will only be received by Firefox when it is forwarded by the proxy.

Figure 4: Request Awaiting Forwarding


Burp Suite Community Edition v2021.10.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex
\n

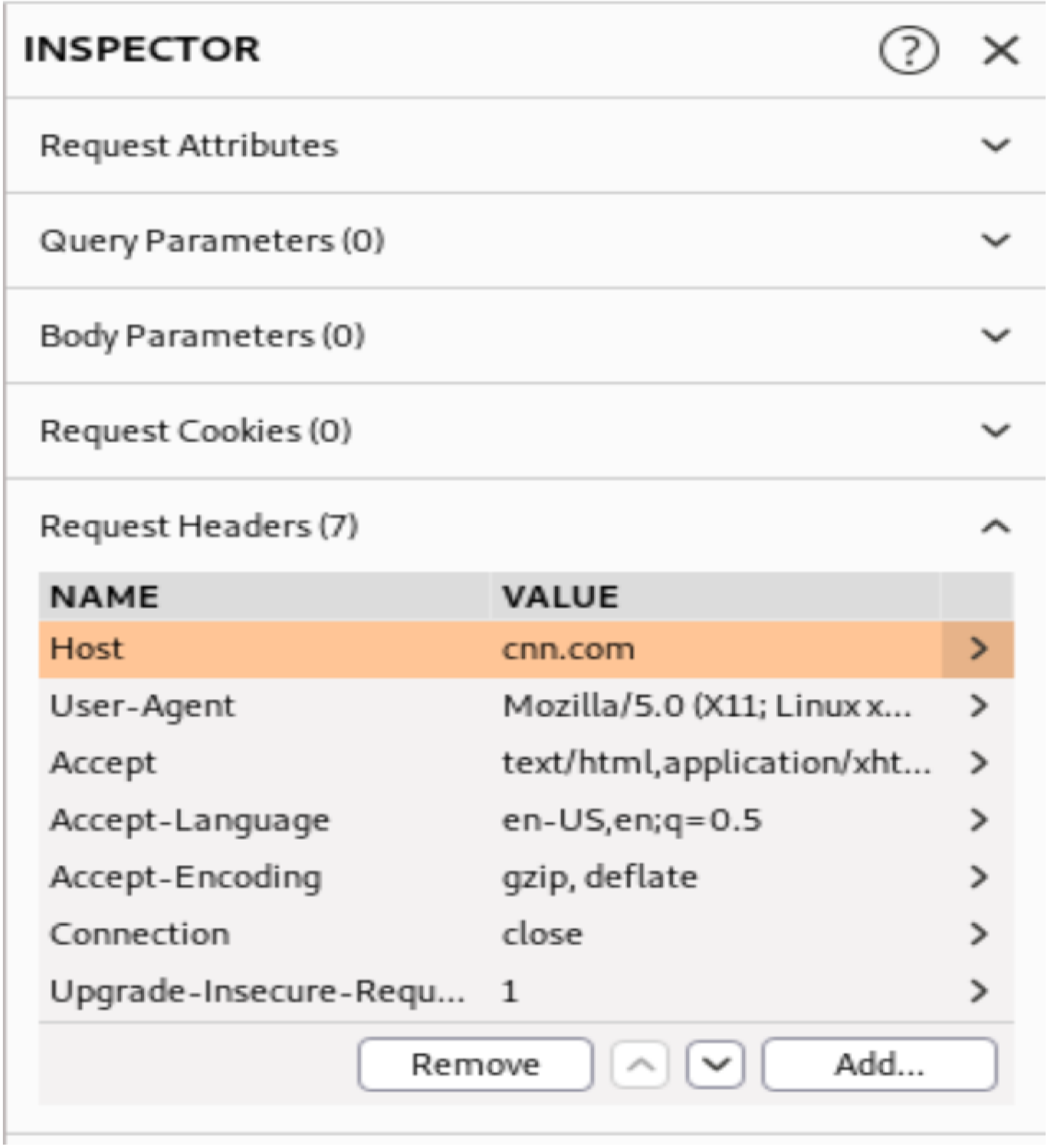
Request to http://cnn.com:80 [151.101.65.67]

```
GET / HTTP/1.1
Host: cnn.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1


```

Here we can see the raw text for our request to access cnn.com We can also modify the request if we like by opening the inspector tab on the right.

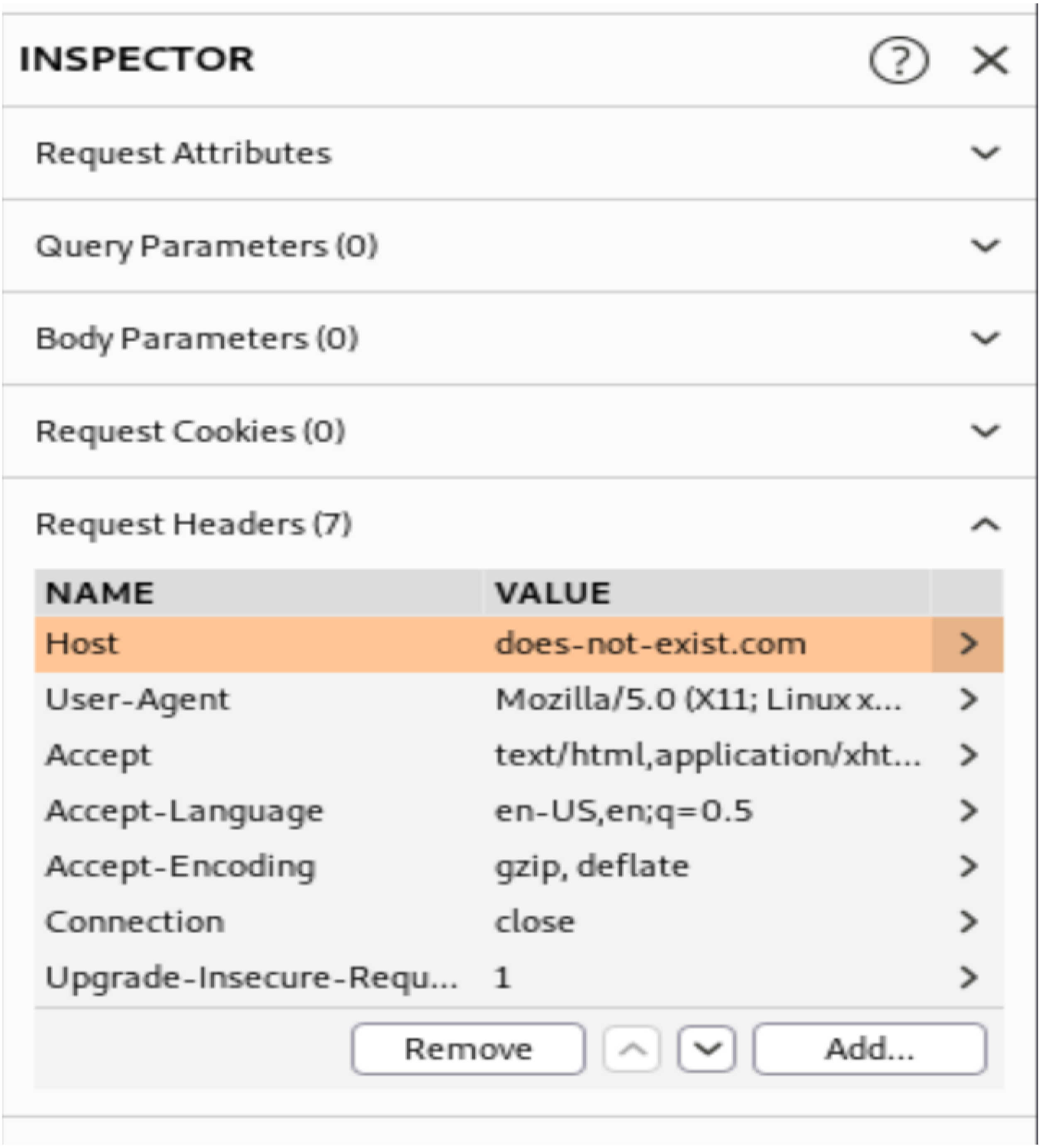
Figure 5: Viewing Request Details With Burp Inspector



NAME	VALUE
Host	cnn.com
User-Agent	Mozilla/5.0 (X11; Linux x...
Accept	text/html,application/xht...
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Connection	close
Upgrade-Insecure-Requ...	1

We see here a wealth of information about the request, and can modify certain fields.

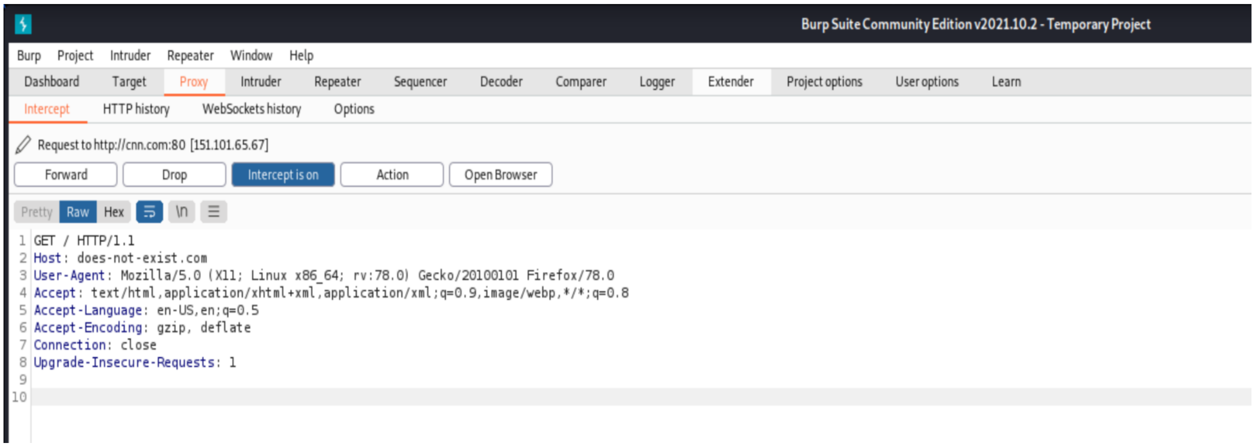
Figure 6: Modifying Request With Burp



NAME	VALUE
Host	does-not-exist.com
User-Agent	Mozilla/5.0 (X11; Linux x...
Accept	text/html,application/xht...
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Connection	close
Upgrade-Insecure-Requ...	1

We change the host field of the request to a domain that does not exist.

Figure 7: Raw Text of Modified Request


Burp Suite Community Edition v2021.10.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex \n

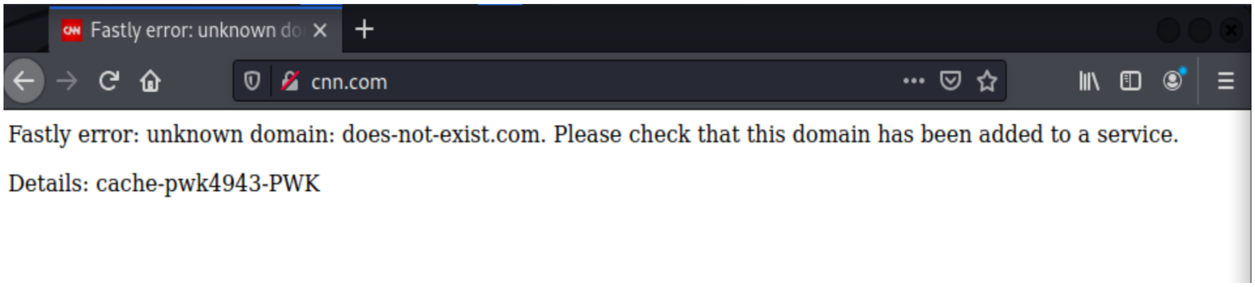
Request to http://cnn.com:80 [151.101.65.67]

```
GET / HTTP/1.1
Host: does-not-exist.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

```

When we forward this request to the browser, the result should be a page not found error of some sort.

Figure 8: Forwarding Modified Request to Firefox

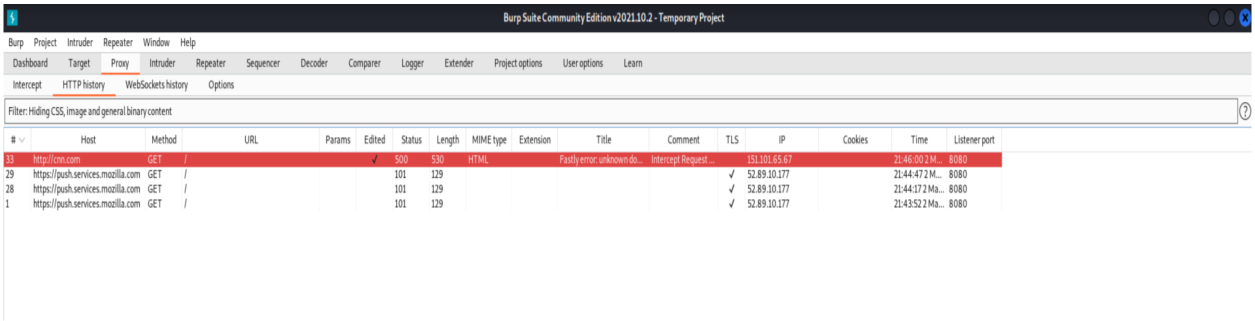


Fastly error: unknown domain: does-not-exist.com. Please check that this domain has been added to a service.

Details: cache-pwk4943-PWK

As expected, there is an error when the request is forwarded because it was intercepted and modified.

Figure 9: Burp HTTP History



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
33	http://cnn.com	GET	/		✓	500	530	HTML		Fastly error: unknown do...	Intercept Request ...		151.101.65.67		21:46:00 2 M...	8080
29	https://push.services.mozilla.com	GET	/			101	129					✓	52.89.10.177		21:44:47 2 M...	8080
28	https://push.services.mozilla.com	GET	/			101	129					✓	52.89.10.177		21:44:17 2 Ma...	8080
1	https://push.services.mozilla.com	GET	/			101	129					✓	52.89.10.177		21:43:52 2 Ma...	8080

We see here that the HTTP history tab in burp allows us to highlight certain requests and make comments on them. A very valuable feature when a large volume of requests are coming in.