Burp Suite

3.6 Burp Suite

+ **How does this support my pentesting career?**

  - Web application analysis
  - Finding vulnerabilities
  - Attacks
  - Burp Suite is one of most used pentesting tools

3.6.1 Intercepting Proxies

- Any web application contains many objects like scripts, images, style sheets, client and server-side intelligence.

- Having **tools** that help in the **study** and **analysis** of web application behavior is critical.

3.6.1 Intercepting Proxies

- An **intercepting proxy** is a tool that lets you analyze and modify any request, and any response exchanged between an HTTP client and a server.
- By intercepting HTTP messages, a pentester can study a web application behavior and manually test for vulnerabilities.

3.6.1 Intercepting Proxies

- The most used web application proxies are:
  - The intercepting proxy feature of Burp Suite
  - ZAP

- Proxies are fundamental while analyzing web applications and will become your best friend for web-app testing.

http://portswigger.net/burp/
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

3.6.1 Intercepting Proxies

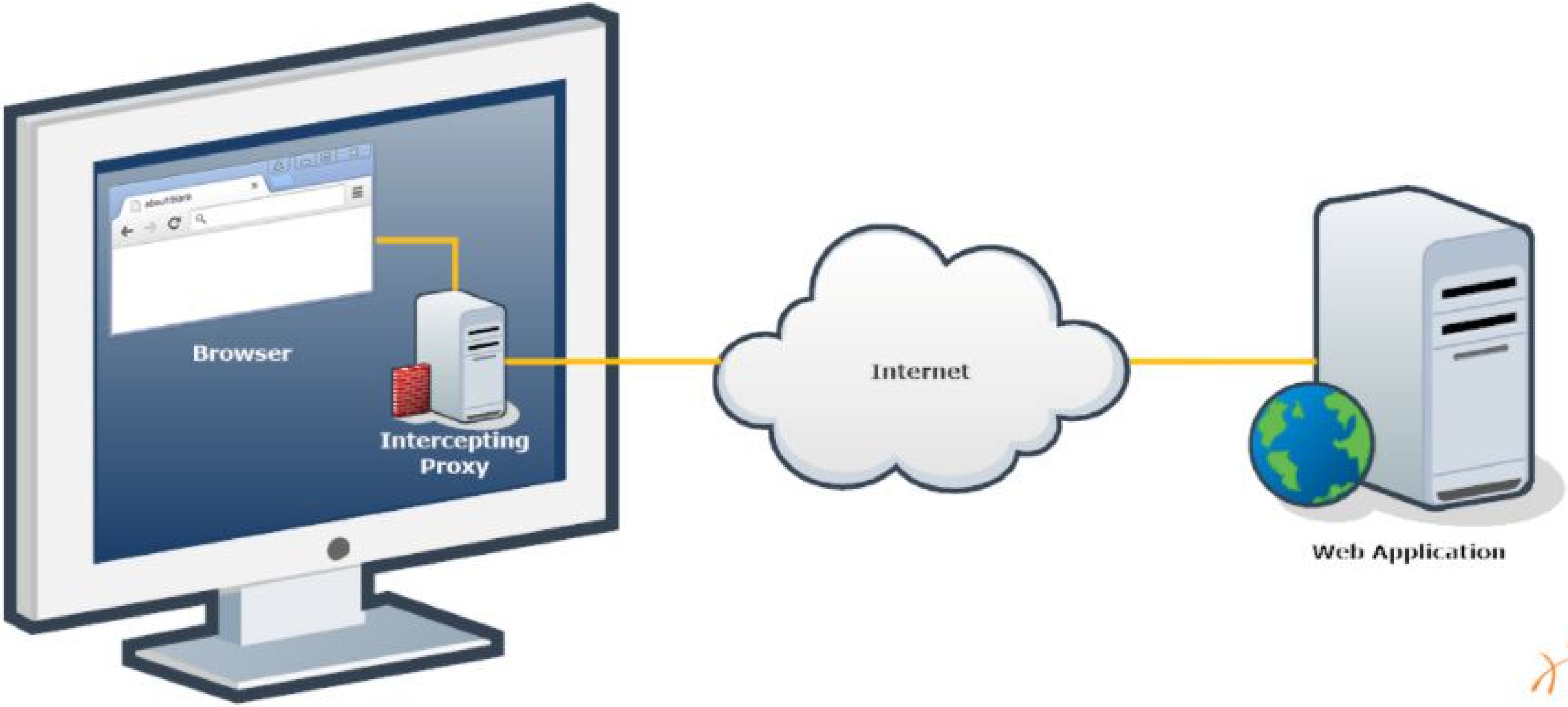
- Do not confuse intercepting proxies with common web proxy servers like Squid. Proxy servers have different purposes: bandwidth optimization, content filtering and more.

- The next two images will make that clearer.

http://www.squid-cache.org/

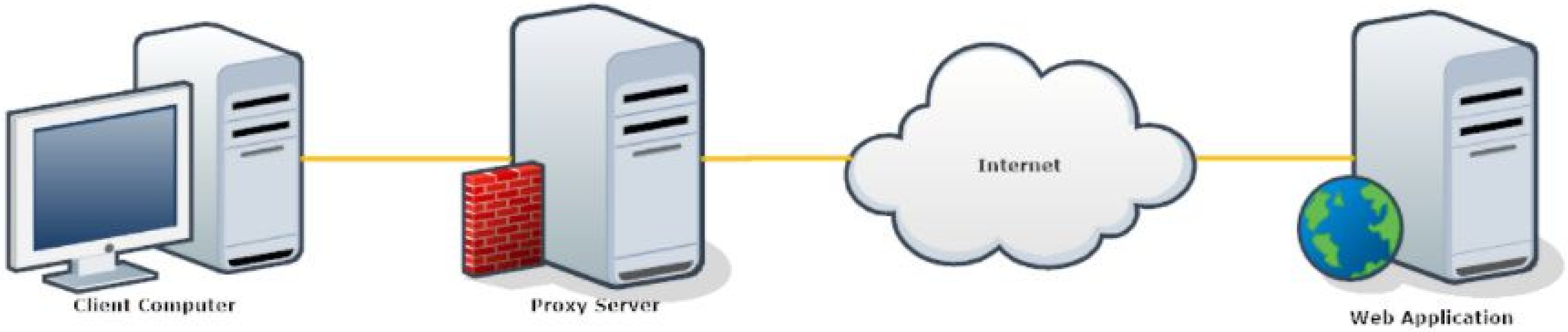
3.6.1.1 Intercepting Proxy Example

Here the proxy is an application which intercepts the penetration tester's browser traffic.



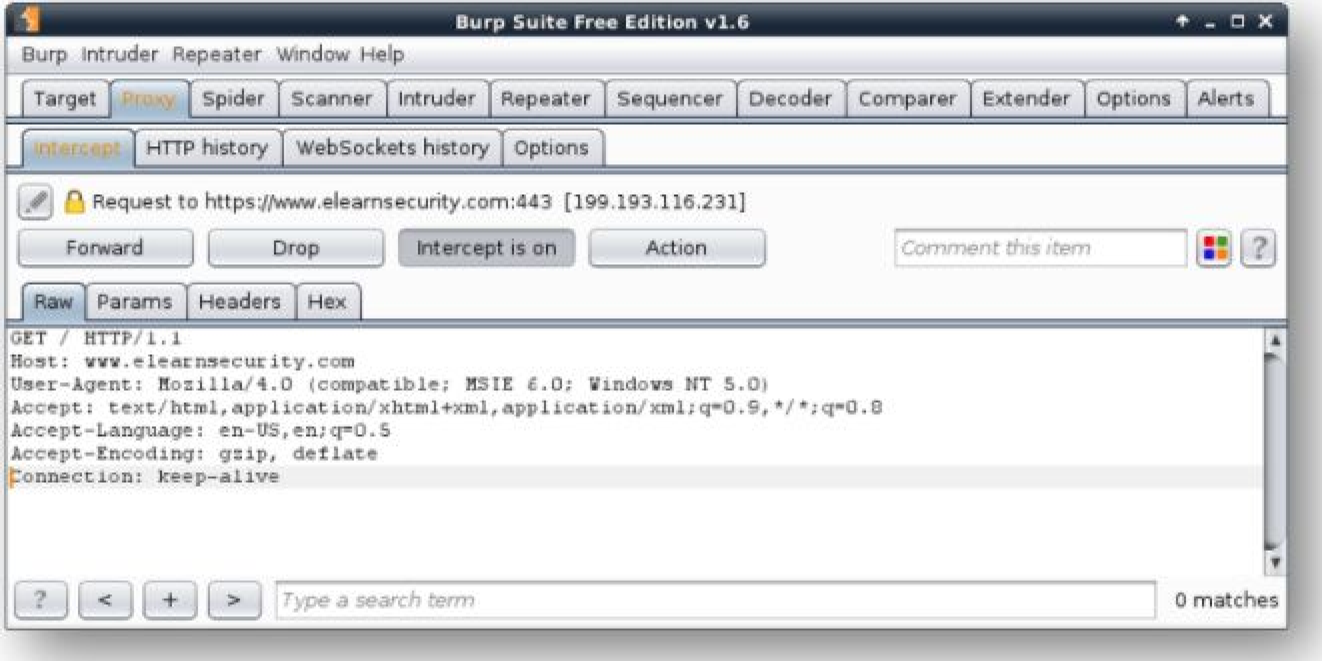
3.6.1.2 Proxy Server Example

Here the proxy server filters all the traffic coming from the internal network.



3.6.2 Burp Proxy

- Burp suite offers one of the best proxies available. You can download the Free Edition here.


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
? < + >
Type a search term
0 matches

Request to https://www.elearnsecurity.com:443 [199.193.116.231]

```
GET / HTTP/1.1
Host: www.elearnsecurity.com
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

https://portswigger.net/burp/communitydownload

3.6.2 Burp Proxy

- Burp suite will let you:
  - Intercept requests and responses between your browser and the web server.
  - Build requests manually.
  - Crawl a website by automatically visiting every page in a website.
  - Fuzz web applications by sending them patterns of valid and invalid inputs to test their behavior.

3.6.2 Burp Proxy

- By using Burp, you can **intercept and modify** requests coming from your browsers **before** they are sent to the remote server.

- You can modify the **header** and the **body** of a message **by hand or automatically**.

3.6.2.1 Burp Proxy Configuration

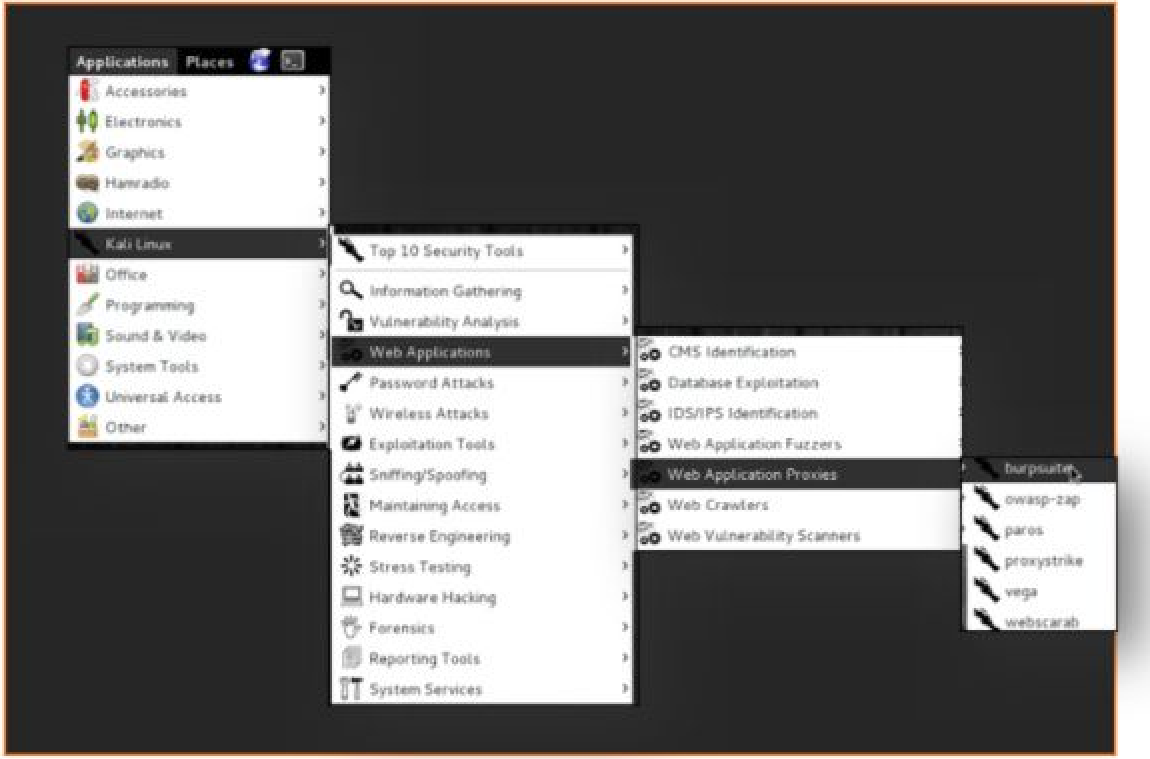
- In the following slides, you will see how to launch, configure and use Burp Suite with your browser.

- Try to understand all the settings by trying them on your computer!

3.6.2.1 Burp Proxy Configuration

Launch Burp Suite:

- In Kali you will find it under *Kali Linux > Web Applications > Web Application Proxies > burpsuite*.



3.6.2.1 Burp Proxy Configuration

If you want to run it on another operating system, you can download it from the Portswigger website.

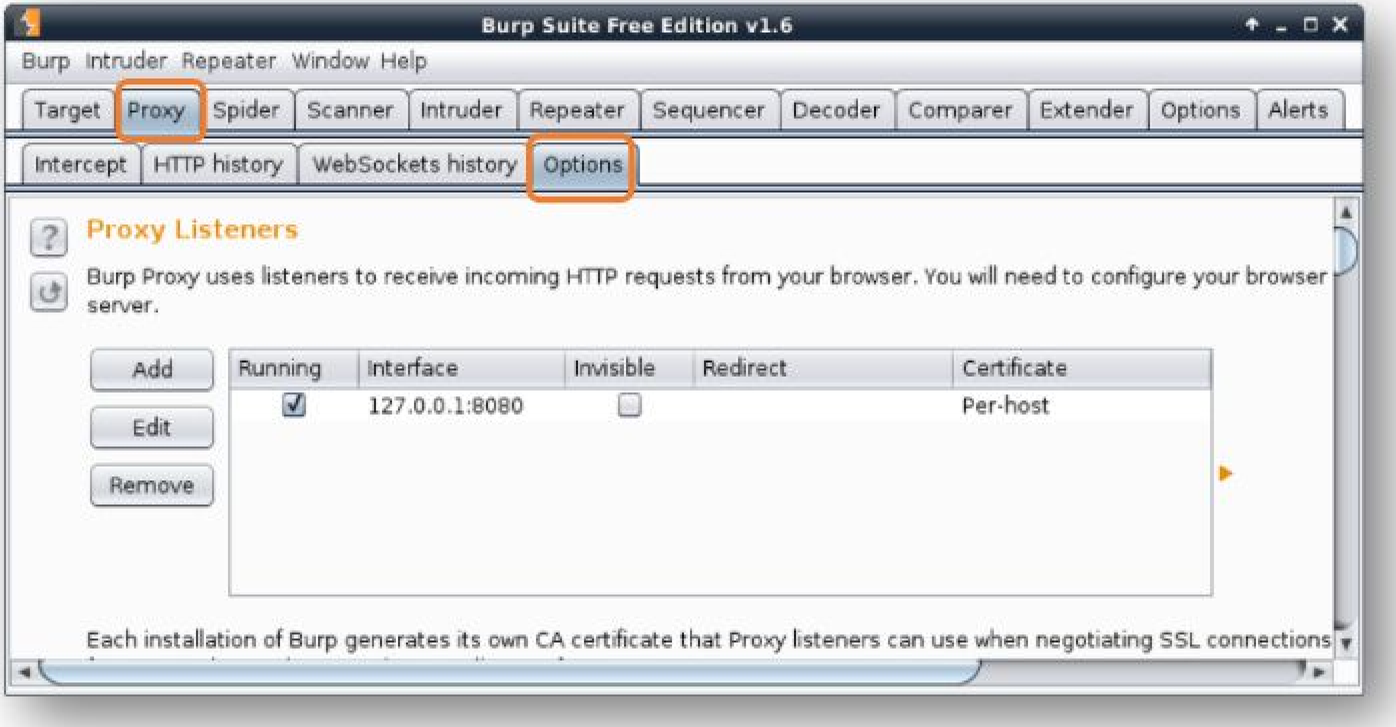
To run Burp, double click on the jar file you downloaded or run the below from the console:

```
java -jar burpsuite_free_v1.6.jar
```

https://portswigger.net/burp/communitydownload

3.6.2.1 Burp Proxy Configuration

- Now, go to the *Proxy* tab and then to the *Options* sub-tab.


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Add
Edit
Remove

Proxy Listeners

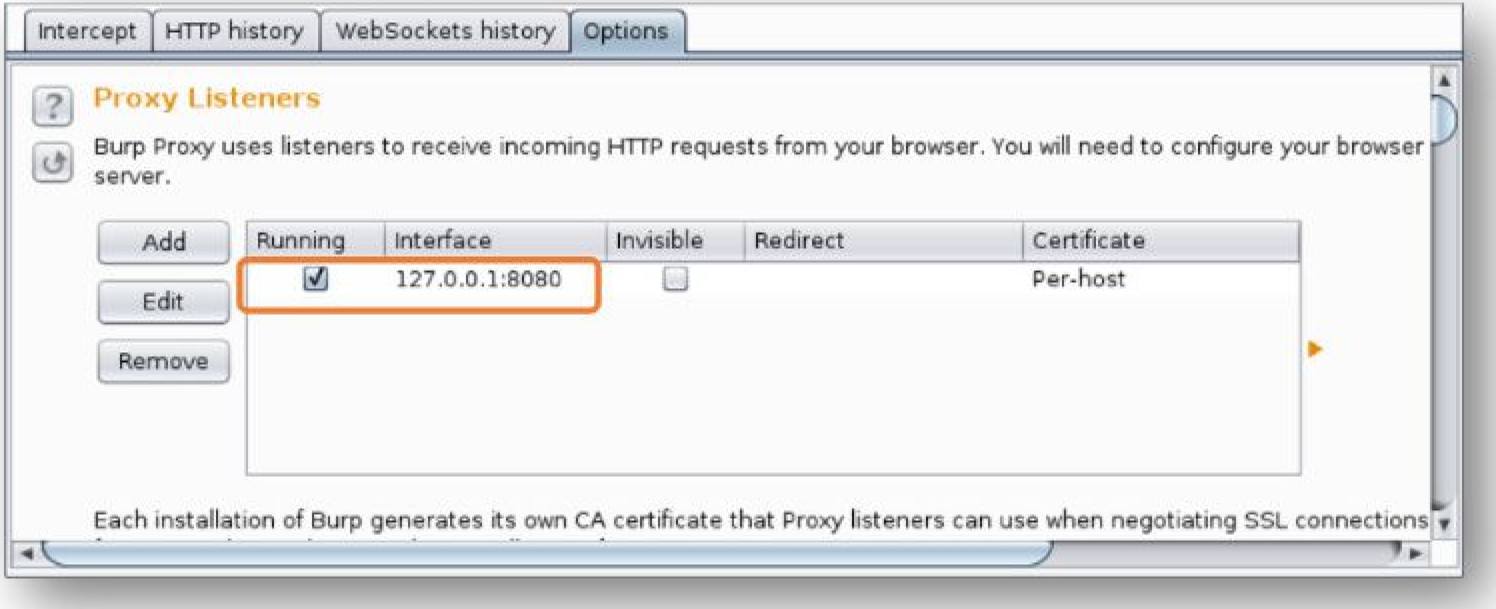
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser server.

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080	☐		Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections

3.6.2.1 Burp Proxy Configuration

- Here you can start and stop the proxy and configure the *host:port* pair on which burp will listen.



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser server.

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080	□		Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections

3.6.2.1 Burp Proxy Configuration

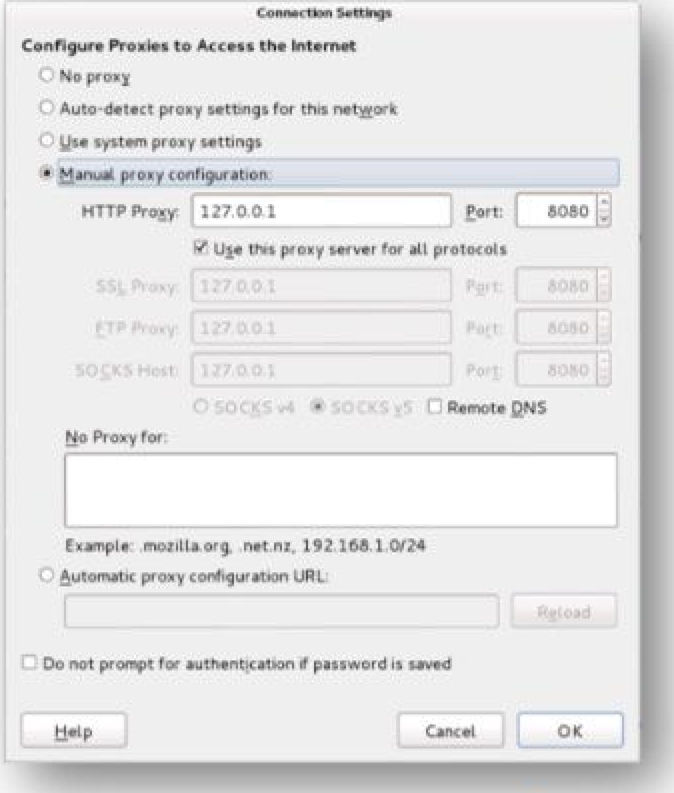
- Scrolling down you can find other configuration items to fine tune, which messages to intercept, how to automatically change message content and more.

- For now, just leave the default options as they are, you will see how to use those features later on.

3.6.2.1 Burp Proxy Configuration

- Once Burp Proxy is configured, you have to configure your browser to use it as the proxy for every protocol.

- In Firefox, you have to open the *Preferences* window, go to the advanced tab, click on the *Network* sub-tab and finally open the *Connection settings* window.



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 8080

☑ Use this proxy server for all protocols

SSL Proxy: 127.0.0.1 Port: 8080

FTP Proxy: 127.0.0.1 Port: 8080

SOCKS Host: 127.0.0.1 Port: 8080

○ SOCKS v4 ● SOCKS v5 □ Remote DNS

No Proxy for:

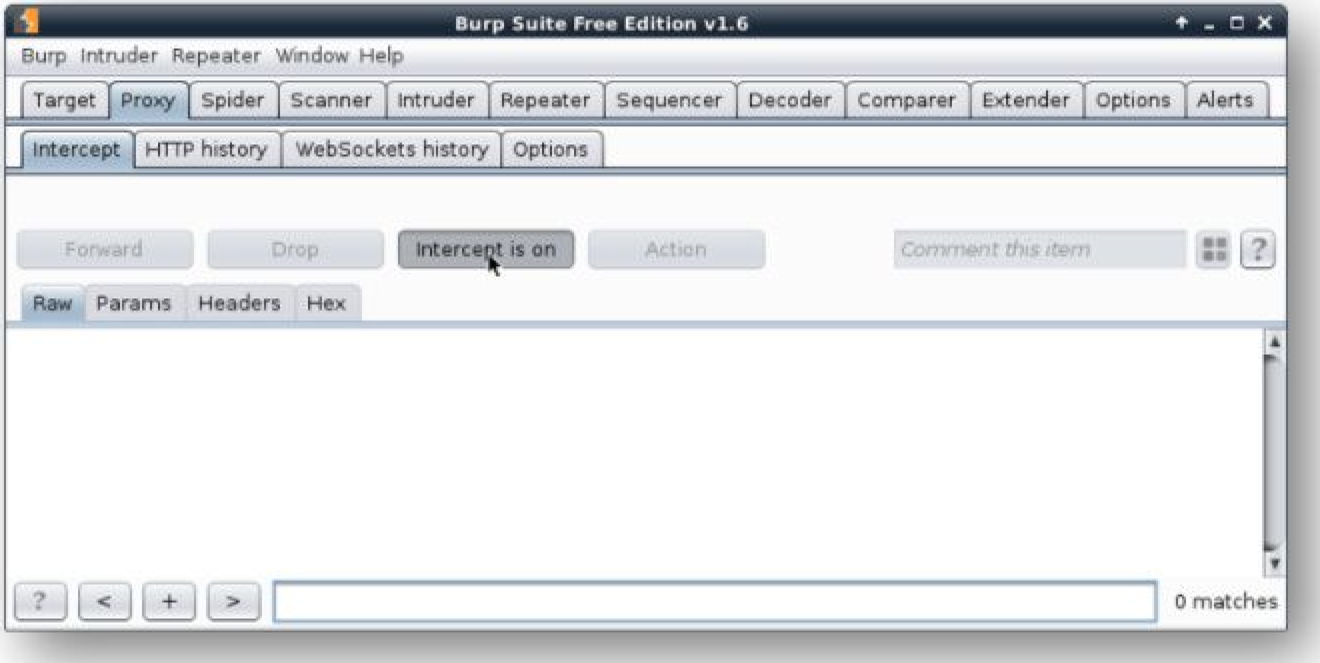
Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

□ Do not prompt for authentication if password is saved

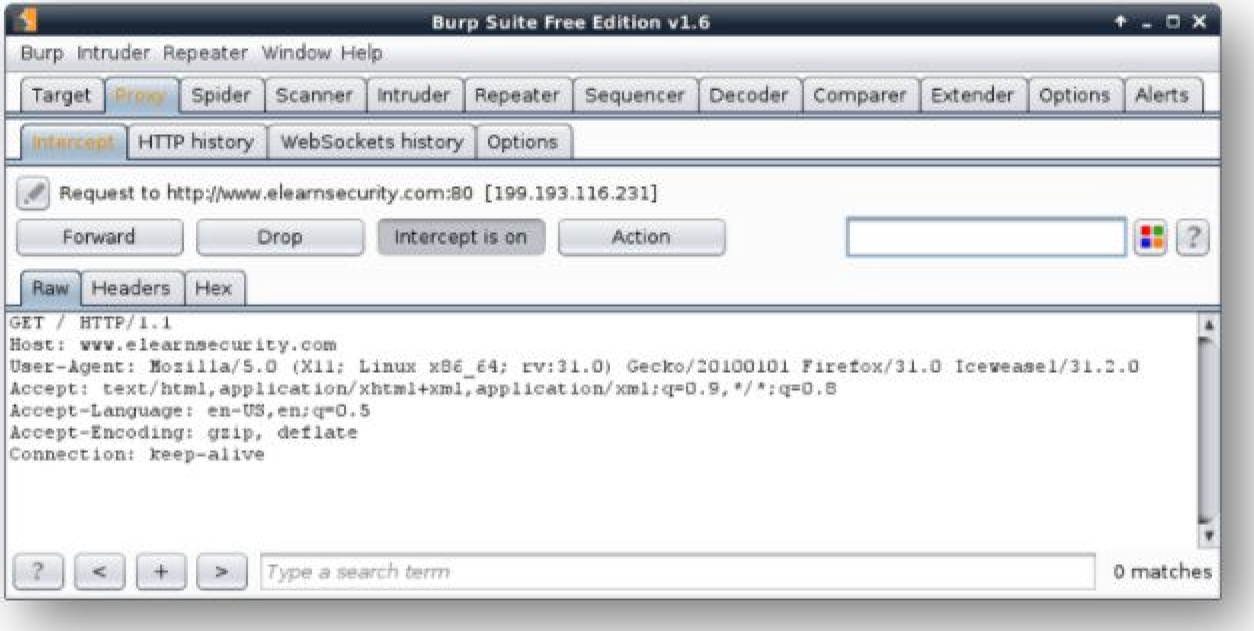
3.6.2.1 Burp Proxy Configuration

- To intercept traffic, switch to Burp and go to *Proxy > Intercept* and click on the *Intercept is off* button to enable interception.


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
? < + >
0 matches

3.6.2.1 Burp Proxy Configuration

- Now open a website with your browser; Burp will pop up intercepting the request. Optionally, you can modify and then forward it by clicking on *Forward*.

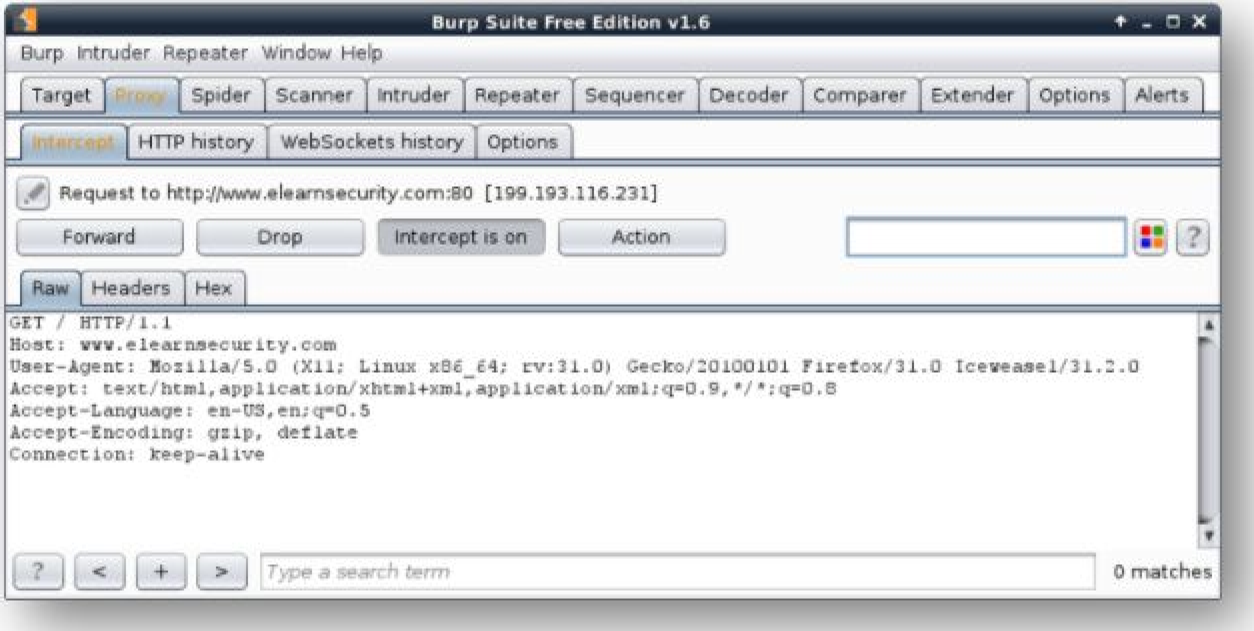

Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Headers Hex
?
<
+
>
Type a search term
0 matches

Request to http://www.elearnsecurity.com:80 [199.193.116.231]

```
GET / HTTP/1.1
Host: www.elearnsecurity.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.2.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

3.6.2.1 Burp Proxy Configuration

- When *Intercept* is on, every browser request stops at Burp Proxy. You can modify the entire request or just its headers.

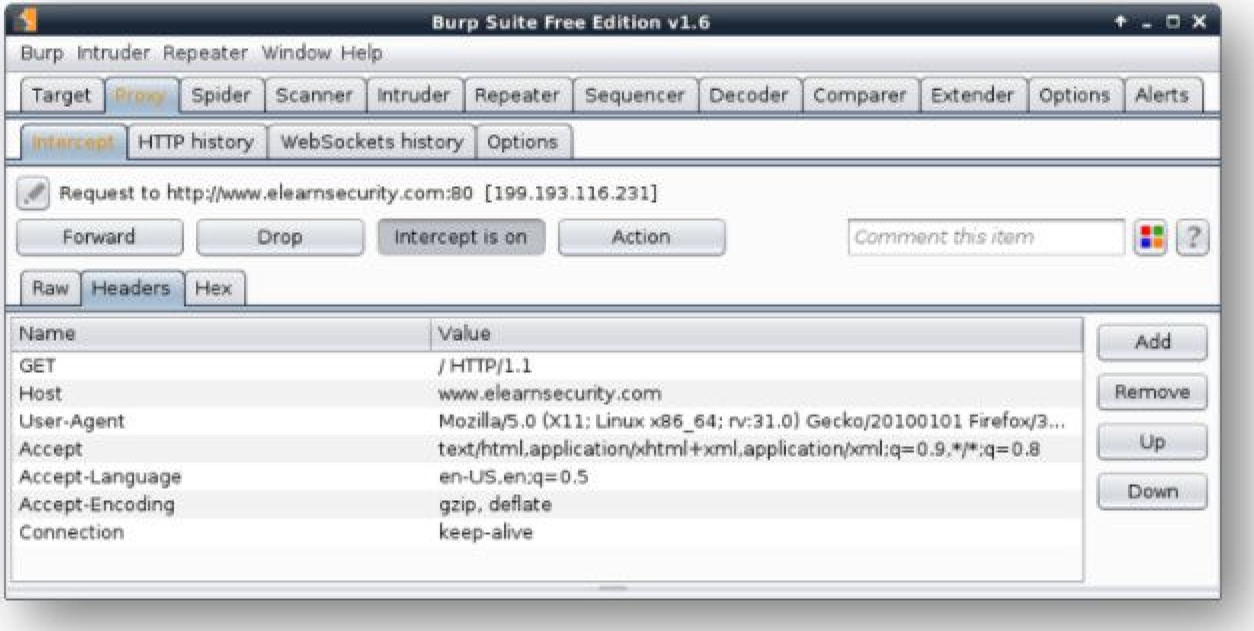


Request to http://www.elearnsecurity.com:80 [199.193.116.231]

```
GET / HTTP/1.1
Host: www.elearnsecurity.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.2.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

3.6.2.1 Burp Proxy Configuration

- You can modify the headers both in the *Raw* tab or in the *Headers* tab. Remember to forward the request after editing it!


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
?
Raw Headers Hex
Add
Remove
Up
Down

Request to http://www.elearnsecurity.com:80 [199.193.116.231]

Name	Value
GET	/ HTTP/1.1
Host	www.elearnsecurity.com
User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/3...
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Connection	keep-alive

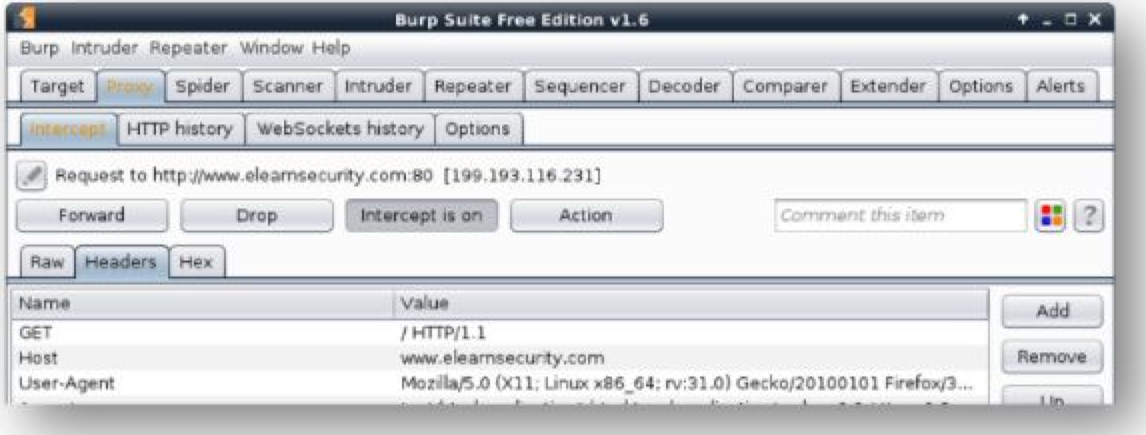
3.6.2.1 Burp Proxy Configuration

Q

What is the difference between the Raw *and the* Headers *tab?*

A

They present the very same information with a different format. The Headers *tab simply presents the headers in a tabular manner.*



Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
?
Raw Headers Hex
Add
Remove
Up

Request to http://www.elearnsecurity.com:80 [199.193.116.231]

Name	Value
GET	/ HTTP/1.1
Host	www.elearnsecurity.com
User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/3...

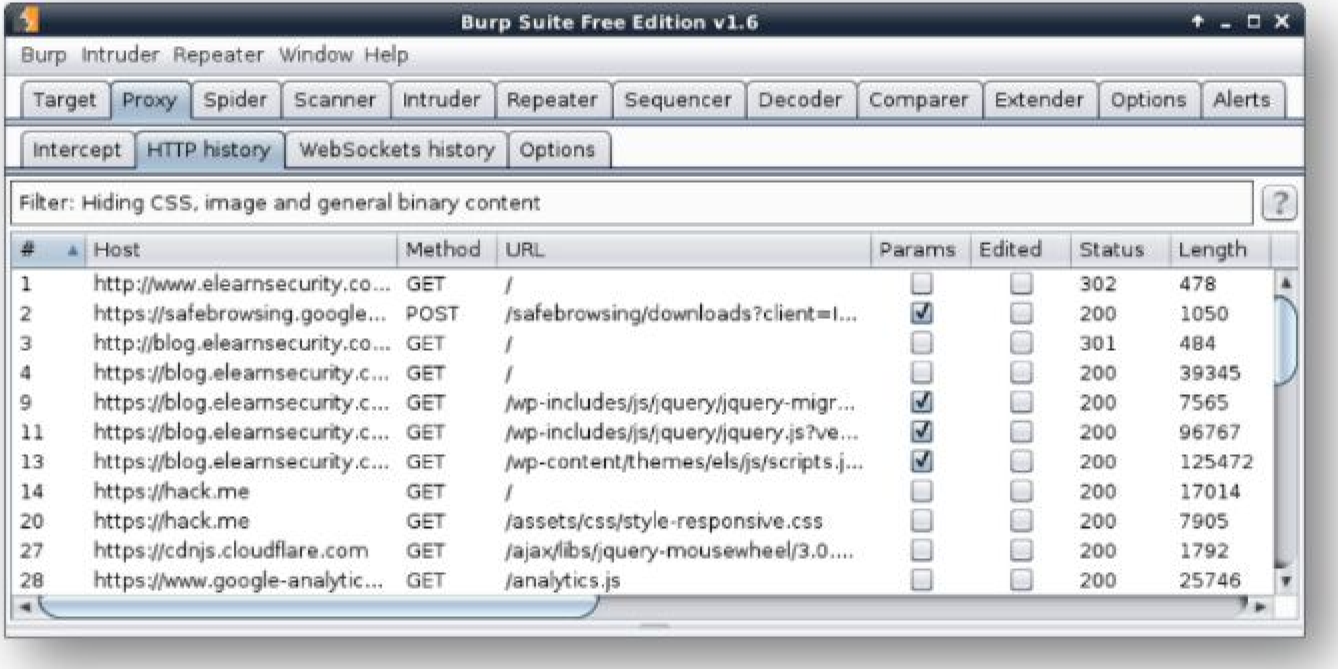
3.6.2.1 Burp Proxy Configuration

- You do not need to manually intercept and forward every request though. Even if you leave the master interception off, Burp will still collect information on the HTTP traffic coming to and from your browser.

- You can check what Burp is collecting in two ways:
  - On the *Proxy > History* tab
  - In the *Target > Site Map* tab

3.6.2.1 Burp Proxy Configuration

Burp Suite *Proxy* tab contains an *HTTP history* sub tab.

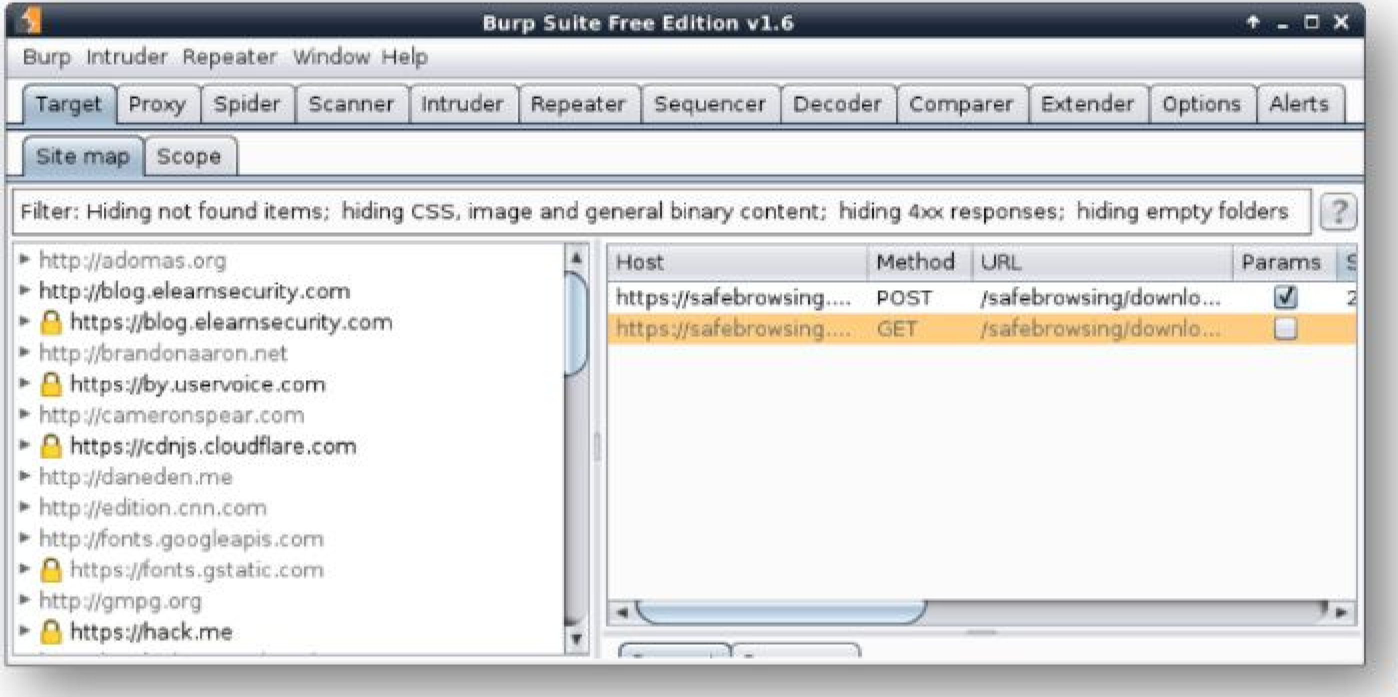

Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
?

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length
1	http://www.elearnsecurity.co...	GET	/	☐	☐	302	478
2	https://safebrowsing.google...	POST	/safebrowsing/downloads?client=l...	☑	☐	200	1050
3	http://blog.elearnsecurity.co...	GET	/	☐	☐	301	484
4	https://blog.elearnsecurity.c...	GET	/	☐	☐	200	39345
9	https://blog.elearnsecurity.c...	GET	/wp-includes/js/jquery/jquery-migr...	☑	☐	200	7565
11	https://blog.elearnsecurity.c...	GET	/wp-includes/js/jquery/jquery.js?ve...	☑	☐	200	96767
13	https://blog.elearnsecurity.c...	GET	/wp-content/themes/els/js/scripts.j...	☑	☐	200	125472
14	https://hack.me	GET	/	☐	☐	200	17014
20	https://hack.me	GET	/assets/css/style-responsive.css	☐	☐	200	7905
27	https://cdnjs.cloudflare.com	GET	/ajax/libs/jquery-mousewheel/3.0....	☐	☐	200	1792
28	https://www.google-analytic...	GET	/analytics.js	☐	☐	200	25746

3.6.2.1 Burp Proxy Configuration

You can also check what Burp is collecting on *Target > Site Map*.


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
?

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- http://adomas.org
- http://blog.elearnsecurity.com
- 🔒 https://blog.elearnsecurity.com
- http://brandonaaron.net
- 🔒 https://by.uservoice.com
- http://cameronspear.com
- 🔒 https://cdnjs.cloudflare.com
- http://daneden.me
- http://edition.cnn.com
- http://fonts.googleapis.com
- 🔒 https://fonts.gstatic.com
- http://gmpg.org
- 🔒 https://hack.me

Host	Method	URL	Params	S
https://safebrowsing....	POST	/safebrowsing/downlo...	☑	2
https://safebrowsing....	GET	/safebrowsing/downlo...	□	

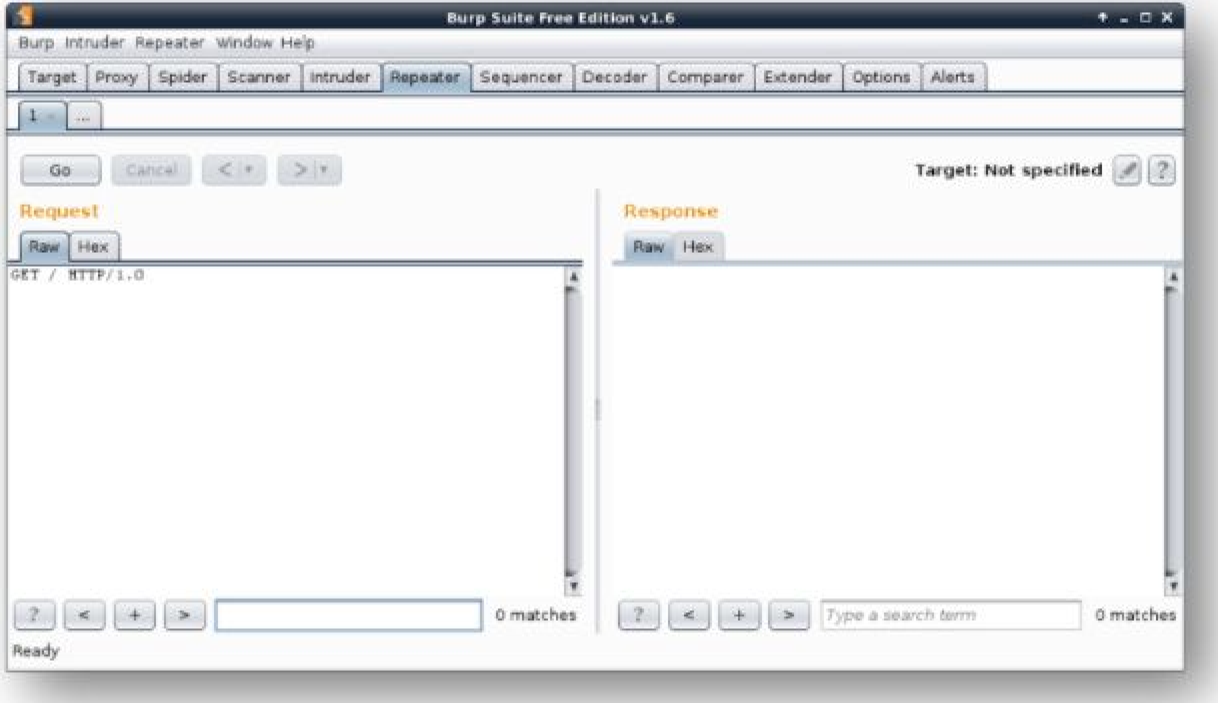
3.6.3 Burp Repeater

- Another feature is **Burp Repeater**, which lets you manually build raw HTTP requests.

- You can do the same thing by using other tools such as *netcat* or *telnet*, but *Burp* provides you:
  - Syntax highlighting
  - Raw and rendered responses
  - Integration with other Burp tools

3.6.3 Burp Repeater

- To create a request, first set your target by clicking on the pencil icon in the upper right corner of the tab.


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 ...
Go Cancel < >
Request
Raw Hex
Response
Raw Hex
? < + >
Type a search term

Target: Not specified

```
GET / HTTP/1.0
```

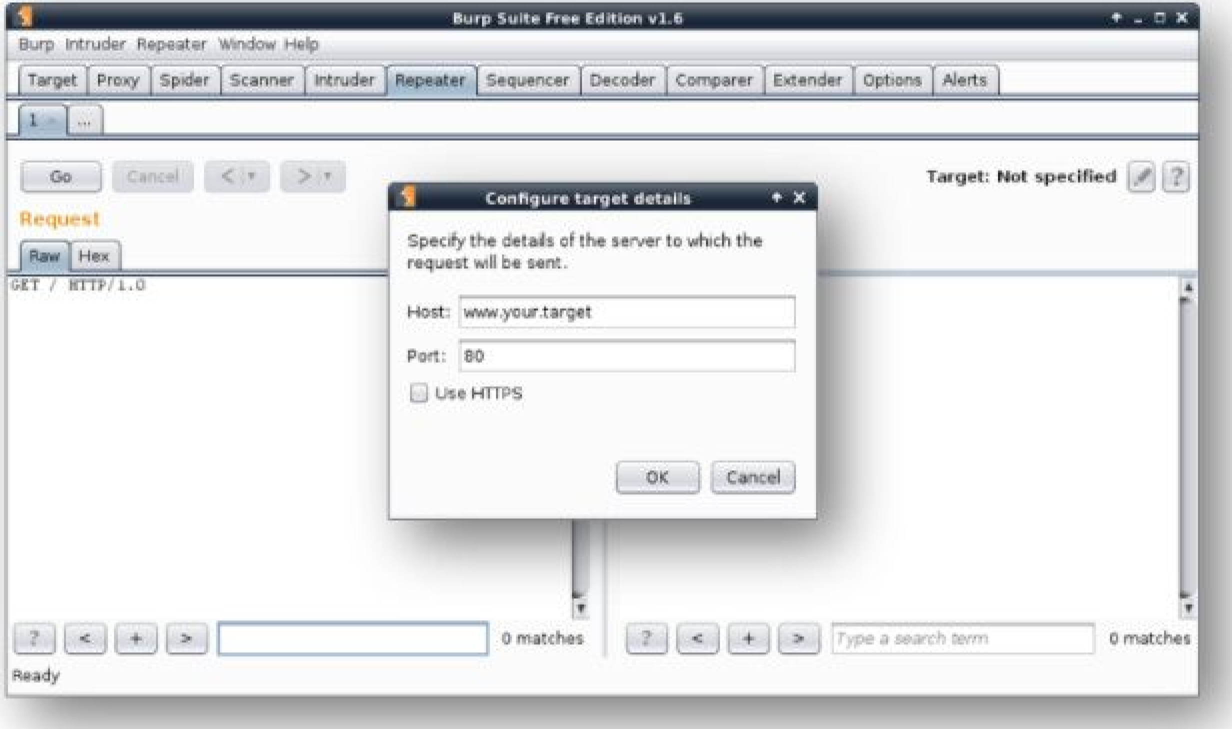
0 matches

0 matches

Ready

3.6.3 Burp Repeater

- You can then set your target host and port.



Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 ...
Go Cancel < >
Request
Raw Hex
? < + >
0 matches
Type a search term
Ready
OK Cancel

Target: Not specified

```
GET / HTTP/1.0
```

Configure target details

Specify the details of the server to which the request will be sent.

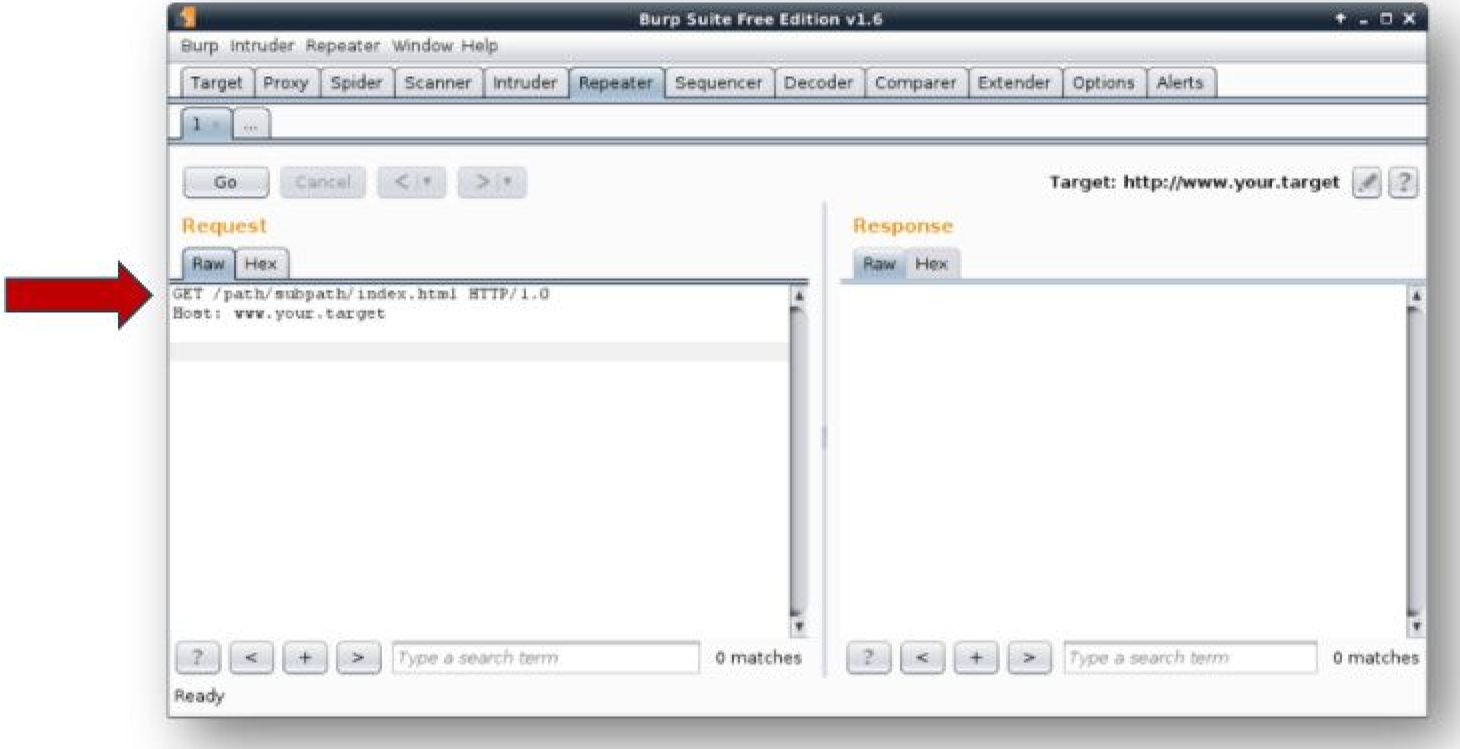
Host: www.your.target

Port: 80

□ Use HTTPS

3.6.3 Burp Repeater

You can define your request by using this text area. Every request must have at least an **HTTP VERB** (GET, POST, HEAD, ...)



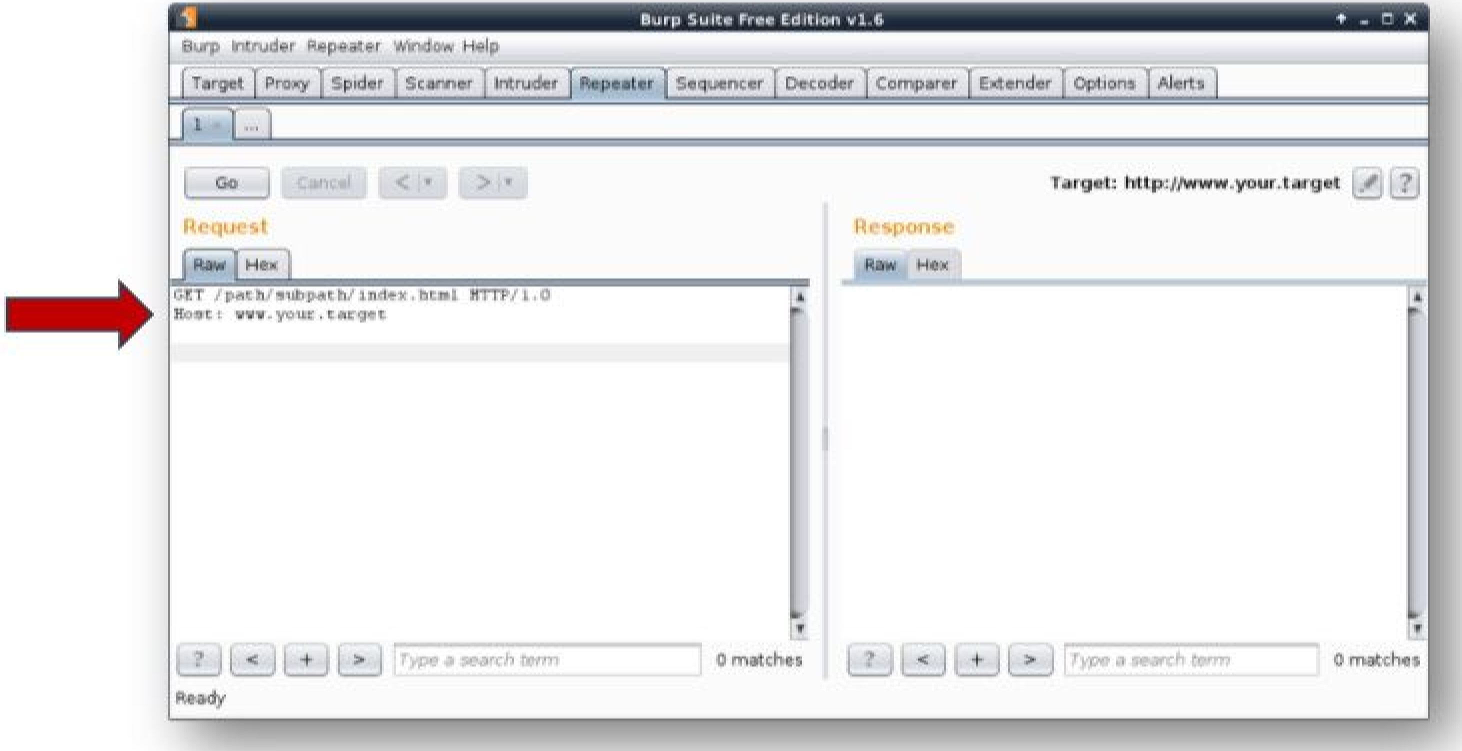
Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 ...
Go Cancel < >
Request
Raw Hex
Response
Raw Hex
? < + > Type a search term 0 matches
Ready

Target: http://www.your.target

```
GET /path/subpath/index.html HTTP/1.0
Host: www.your.target
```

3.6.3 Burp Repeater

- Here is the **Host** header.

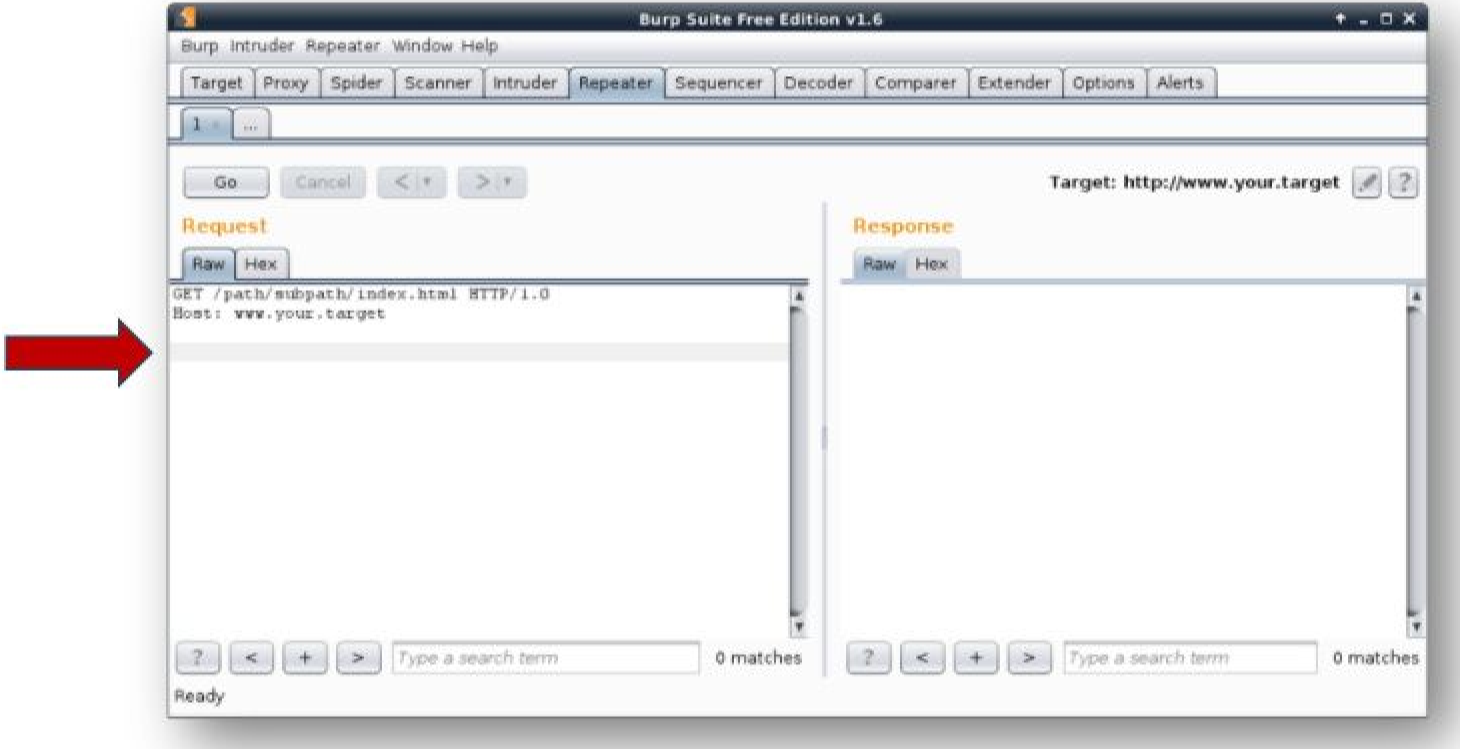


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 ...
Go Cancel
Target: http://www.your.target
Request
Raw Hex
Response
Raw Hex
Type a search term
0 matches
Type a search term
0 matches
Ready

```
GET /path/subpath/index.html HTTP/1.0
Host: www.your.target
```

3.6.3 Burp Repeater

- And here we see **two empty lines** after the headers.

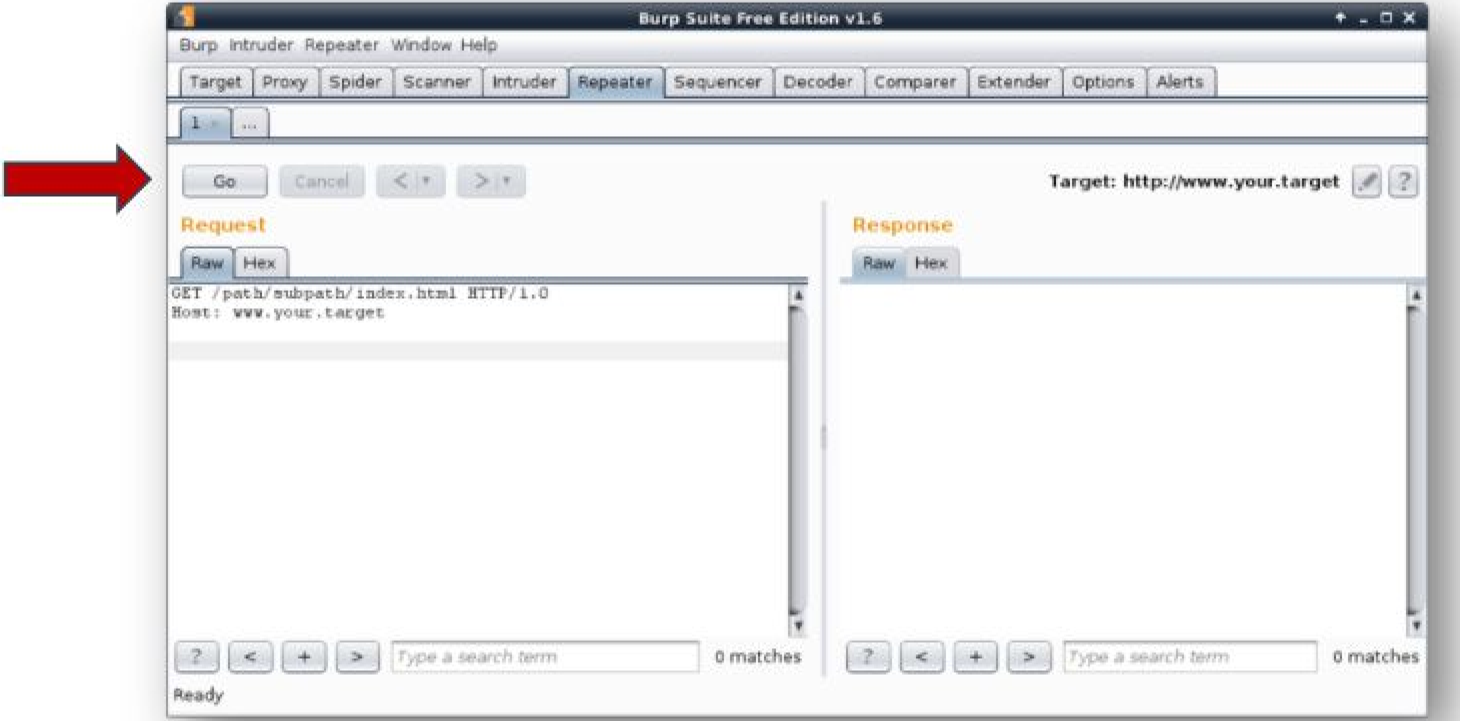


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 ...
Go Cancel < >
Target: http://www.your.target
Request
Raw Hex
Response
Raw Hex
Type a search term
0 matches
Type a search term
0 matches
Ready

```
GET /path/subpath/index.html HTTP/1.0
Host: www.your.target


```

3.6.3 Burp Repeater

- When your request is complete, you can click the **Go** button to send it to the server.

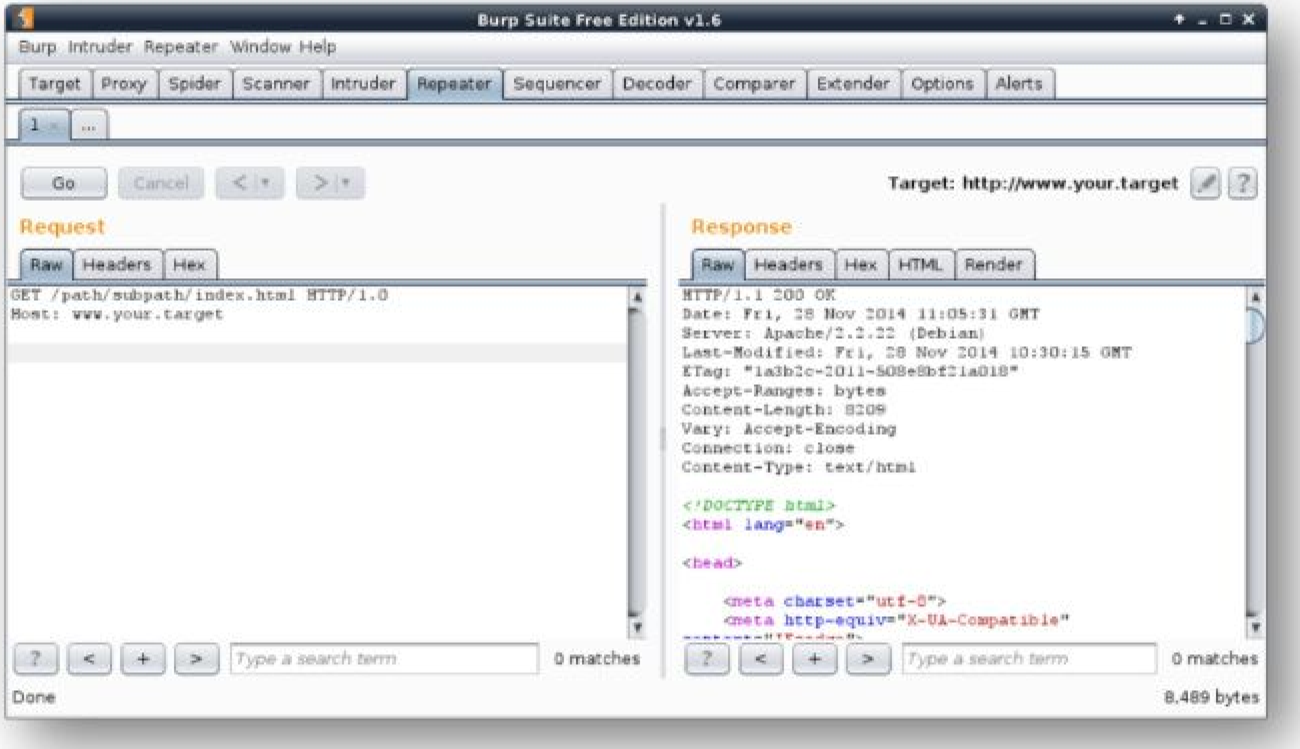


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 ...
Go Cancel < >
Target: http://www.your.target
Request
Raw Hex
Response
Raw Hex
Type a search term
0 matches
Type a search term
0 matches
Ready

```
GET /path/subpath/index.html HTTP/1.0
Host: www.your.target
```

3.6.3 Burp Repeater

- Burp will then display the response in the **Response** panel.



Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 ×
...
Go
Cancel
<
>
Request
Raw
Headers
Hex
Response
Raw
Headers
Hex
HTML
Render
?
<
+
>
Type a search term
0 matches
Done

Target: http://www.your.target

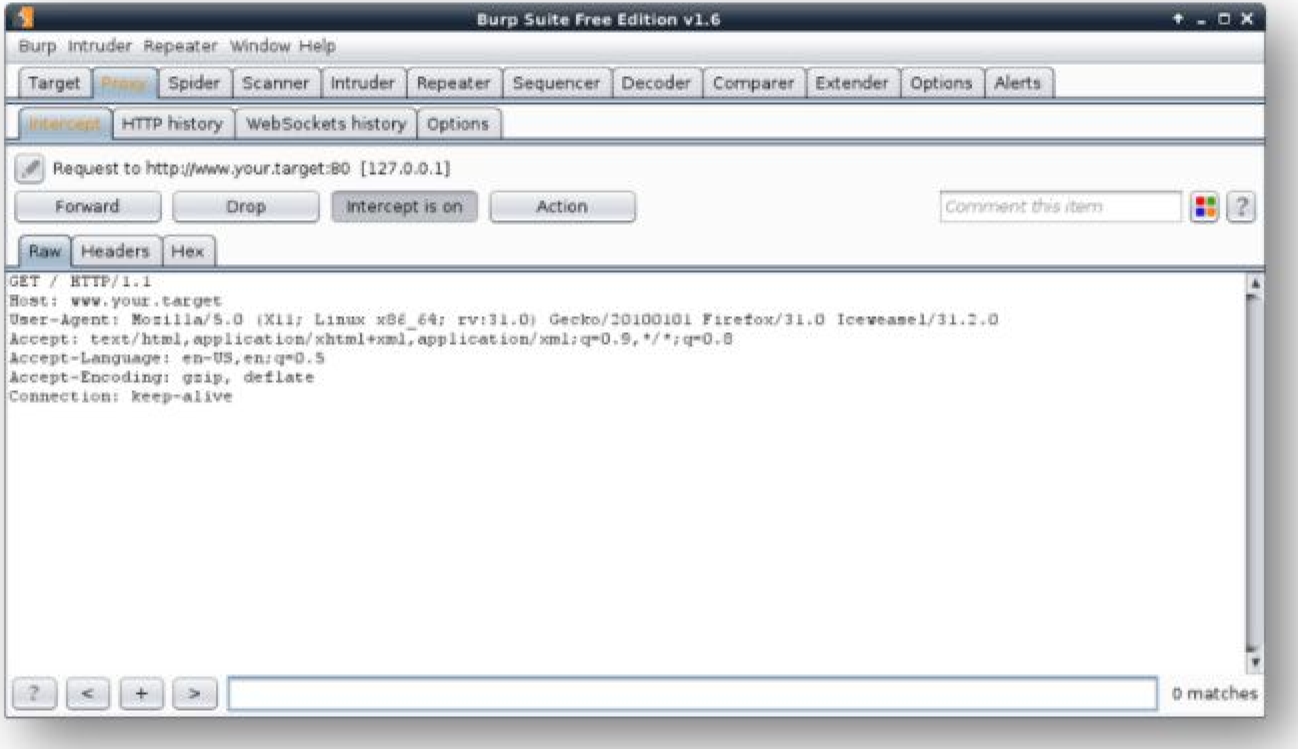
```
GET /path/subpath/index.html HTTP/1.0
Host: www.your.target
```

```
HTTP/1.1 200 OK
Date: Fri, 28 Nov 2014 11:05:31 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Fri, 28 Nov 2014 10:30:15 GMT
ETag: "1a3b2c-2011-508e8bf21a018"
Accept-Ranges: bytes
Content-Length: 8209
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">

<head>

    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible"
```

8,489 bytes

3.6.3 Burp Repeater

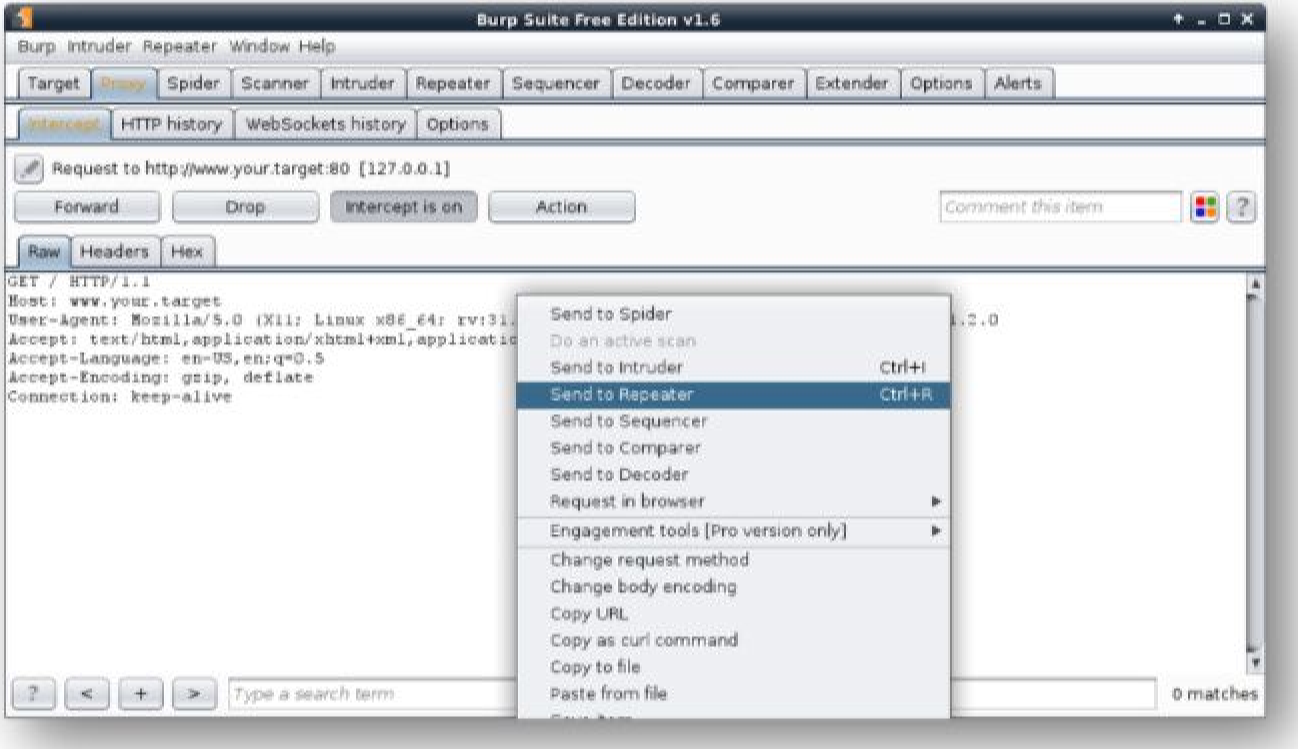
- An easier method to build requests is to intercept a browser request with the proxy and send it to the Repeater function.



```
GET / HTTP/1.1
Host: www.your.target
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.2.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

3.6.3 Burp Repeater

- You can do that with the **Ctrl+R** shortcut or by right-clicking in the request body and selecting **Send to Repeater**.



```
GET / HTTP/1.1
Host: www.your.target
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.                    .2.0
Accept: text/html,application/xhtml+xml,applicatio
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

References

- Burp Suite: http://portswigger.net/burp/
- Burp Suite Download: https://portswigger.net/burp/communitydownload
- Squid: http://www.squid-cache.org/
- ZAP: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project