Fundamental Skills - Burp Suite

Category	Experience Level
Web	Novice

Contents

Introduction

To properly understand this lesson, we recommend first completing the Web 2 - Understanding HTTP Requests lesson if you are unfamiliar with HTTP requests.

Burp Suite is a powerful tool for inspecting HTTP traffic. It acts as a **proxy** between your *browser* and the *server*. It captures HTTP requests before they are sent to the server, and lets you **view** and **modify** their details on the fly.

What does this mean?

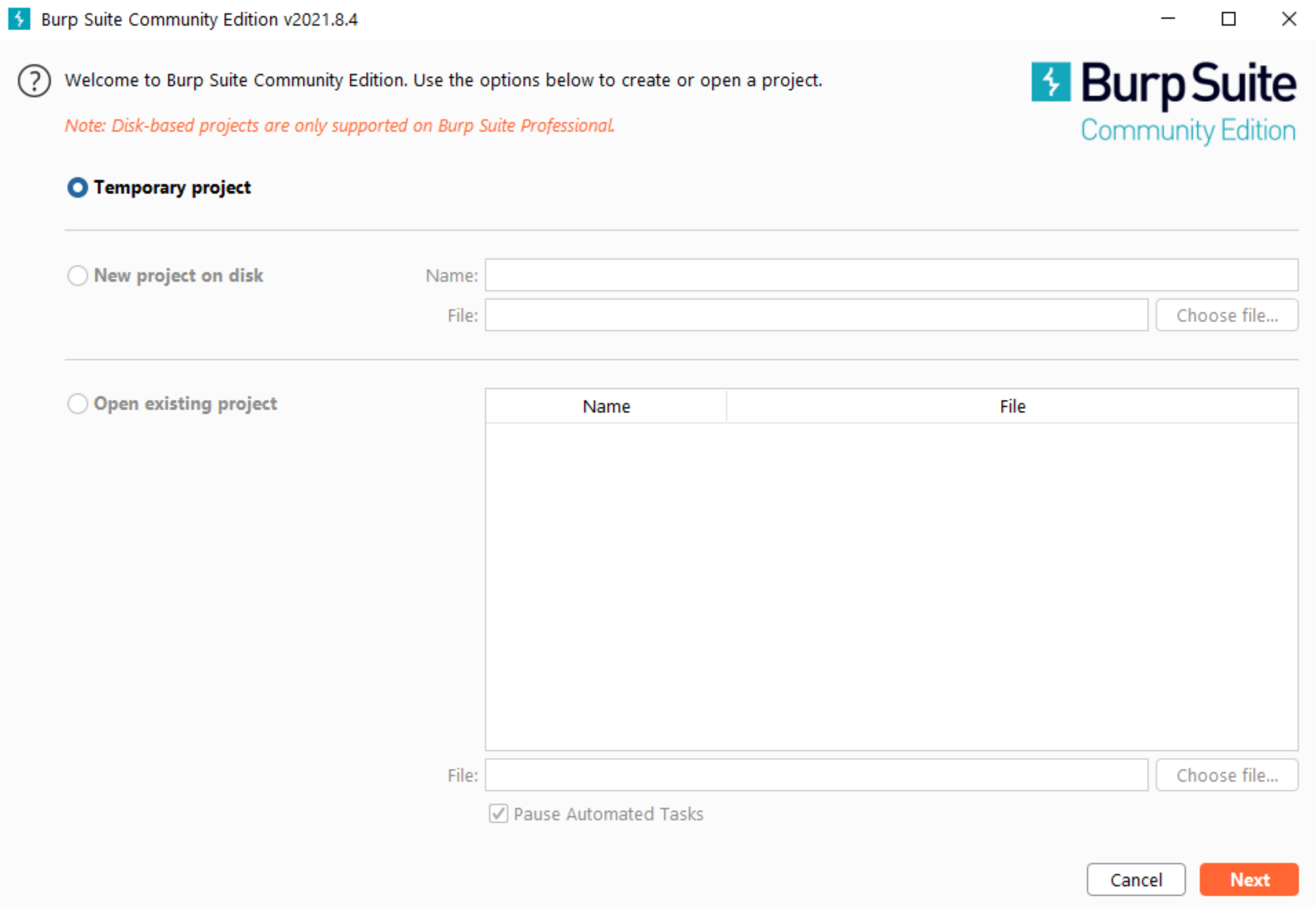
- you can see exactly what is happening when you visit a webpage; this includes request headers added automatically by your browser, request data, and server responses including redirects
- you can see 'behind the scenes requests' that you might not have been aware of
- you can edit requests before they reach the server - this allows you to experiment with site features, and potentially discover broken or unintended functionality on the server

Burp also has many other powerful features, such as the Repeater and Intruder modules which we will address in this lesson.

Setting up Burp Suite

To download the free version of Burp Suite, visit this page, click Download, and choose the most appropriate version for your Operating System. Then run any necessary installers.

When you launch Burp Suite, you will see the following screen:



Burp Suite Community Edition v2021.8.4

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project

○ New project on disk — Name: File:

○ Open existing project

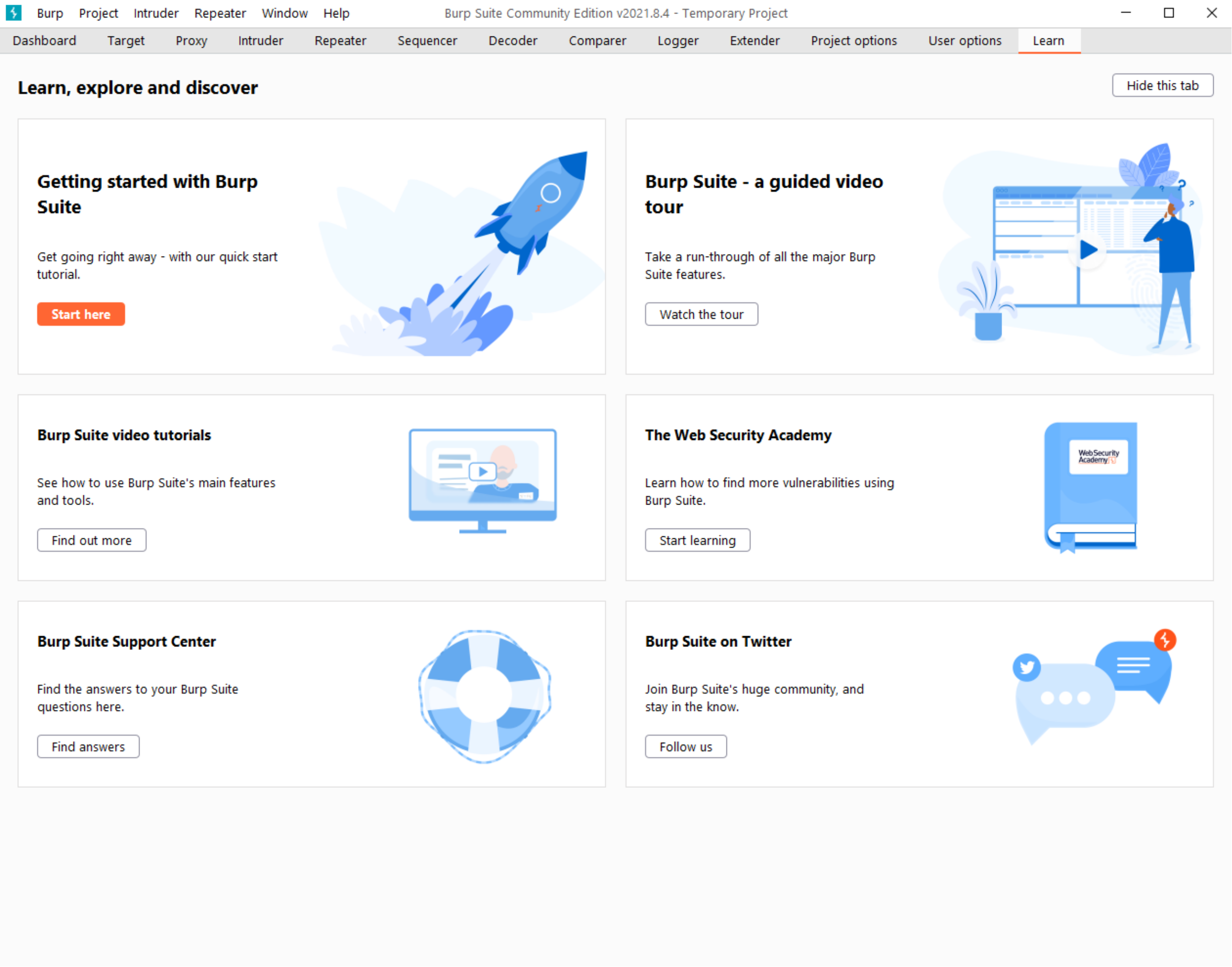
Name	File

File:

☑ Pause Automated Tasks

Click 'Next' to start a temporary project, then 'Start Burp' on the next screen.

You should now see the Burp Homepage:



Learn, explore and discover

Getting started with Burp Suite

Get going right away - with our quick start tutorial.

Burp Suite - a guided video tour

Take a run-through of all the major Burp Suite features.

Burp Suite video tutorials

See how to use Burp Suite's main features and tools.

The Web Security Academy

Learn how to find more vulnerabilities using Burp Suite.

Burp Suite Support Center

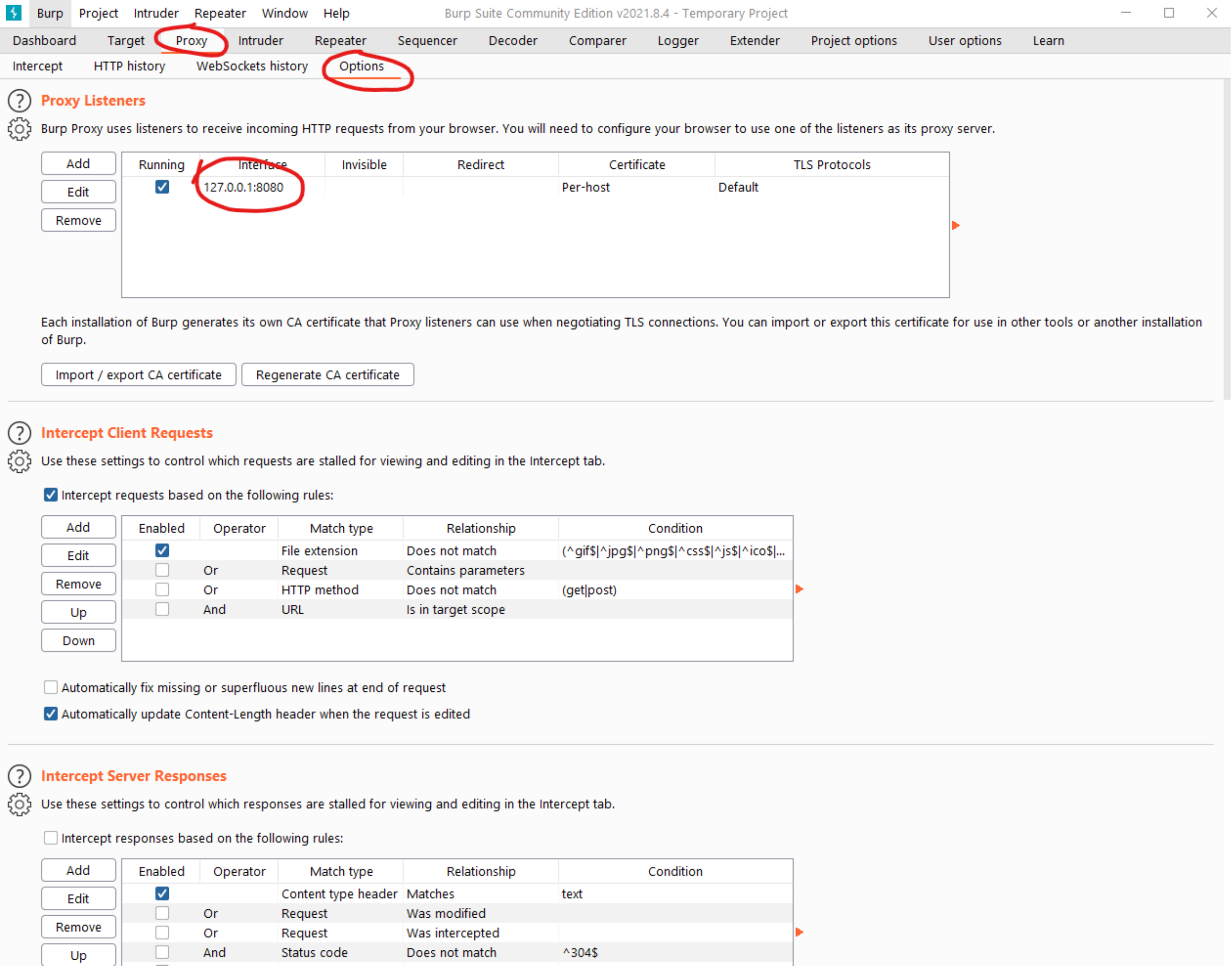
Find the answers to your Burp Suite questions here.

Burp Suite on Twitter

Join Burp Suite's huge community, and stay in the know.

Proxying Traffic

By default, Burp sets up a HTTP proxy on address 127.0.0.1 (aka localhost, the address of your computer) and port 8080. You can see the proxy settings in the *Proxy > Options* tab:



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$|...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

□ Automatically fix missing or superfluous new lines at end of request

☑ Automatically update Content-Length header when the request is edited

Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

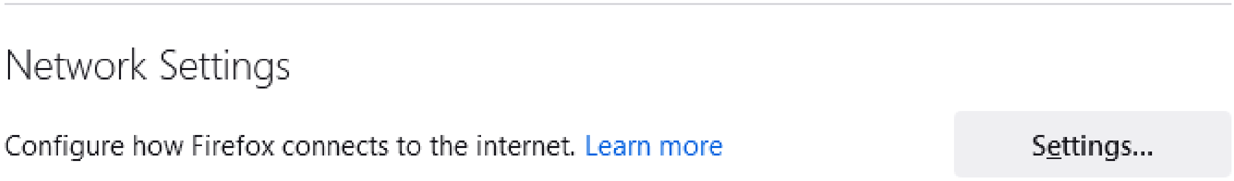
□ Intercept responses based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		Content type header	Matches	text
□	Or	Request	Was modified	
□	Or	Request	Was intercepted	
□	And	Status code	Does not match	^304$

There are lots of options, but we will focus on the first one. This lets us set the port and address to listen on. We can add, edit, and remove proxies with the buttons on the left, and enable/disable them with the checkbox.

To direct requests from your browser to your proxy, you must instruct the browser to point at Burp. I will show Firefox in this lesson, but PortSwigger have written a guide for Google Chrome if that's the browser you prefer.

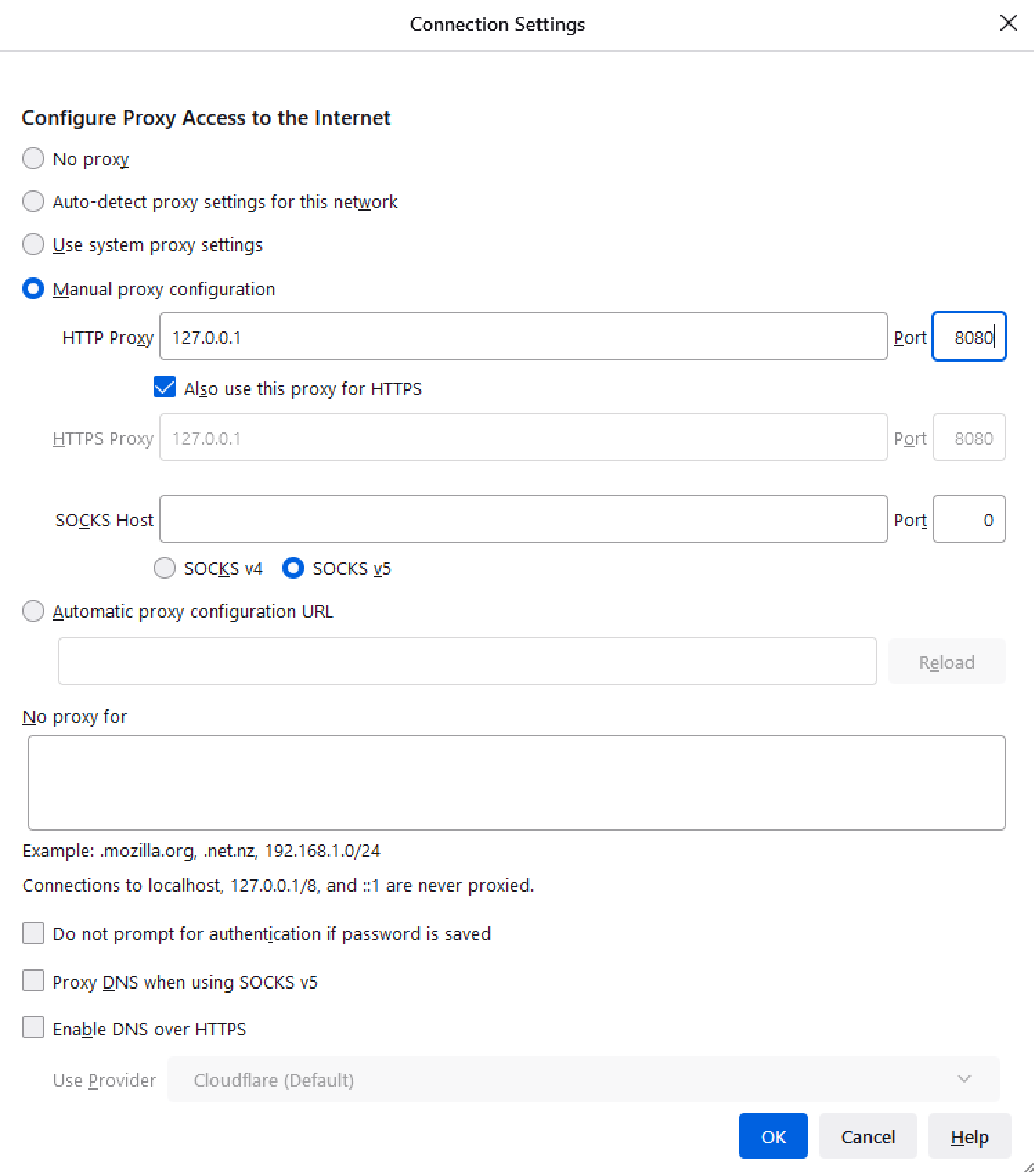
In Firefox, navigate to `about:preferences` in the URL bar. This will open your settings menu. Scroll to the bottom where the Network Settings are, and click 'Settings':



Network Settings

Configure how Firefox connects to the internet. Learn more

Now add proxy settings to match the Proxy Listener settings in Burp:



Connection Settings

Configure Proxy Access to 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

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload

No proxy for

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

Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

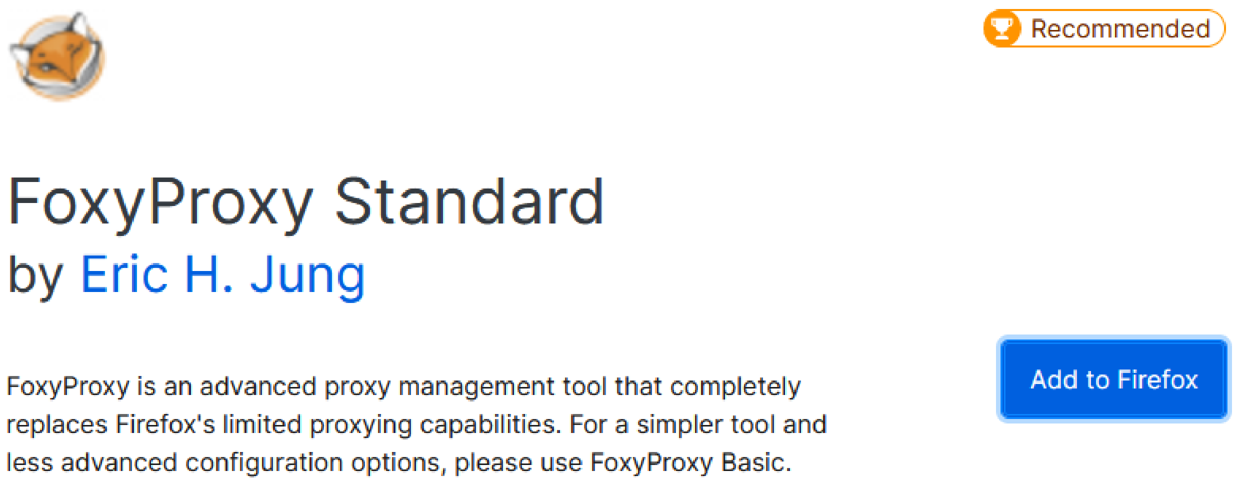
□ Do not prompt for authentication if password is saved

□ Proxy DNS when using SOCKS v5

□ Enable DNS over HTTPS

Use Provider Cloudflare (Default)

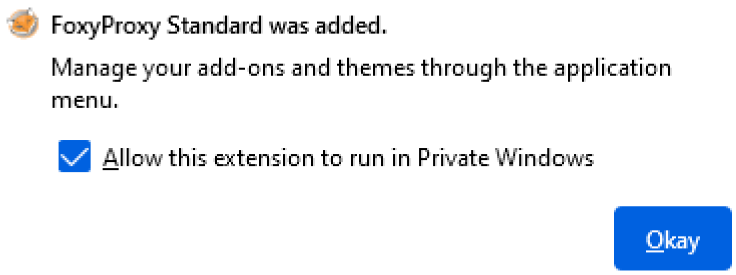
You can also use the browser extension FoxyProxy to more easily configure, enable, and disable proxies - install it by visiting the extension page and clicking 'Add to Firefox':



FoxyProxy Standard
by Eric H. Jung

FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.

If you commonly use private browsing mode, you must also enable it to run in those windows:

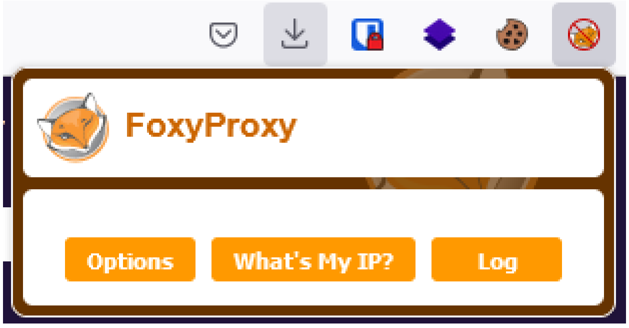


FoxyProxy Standard was added.

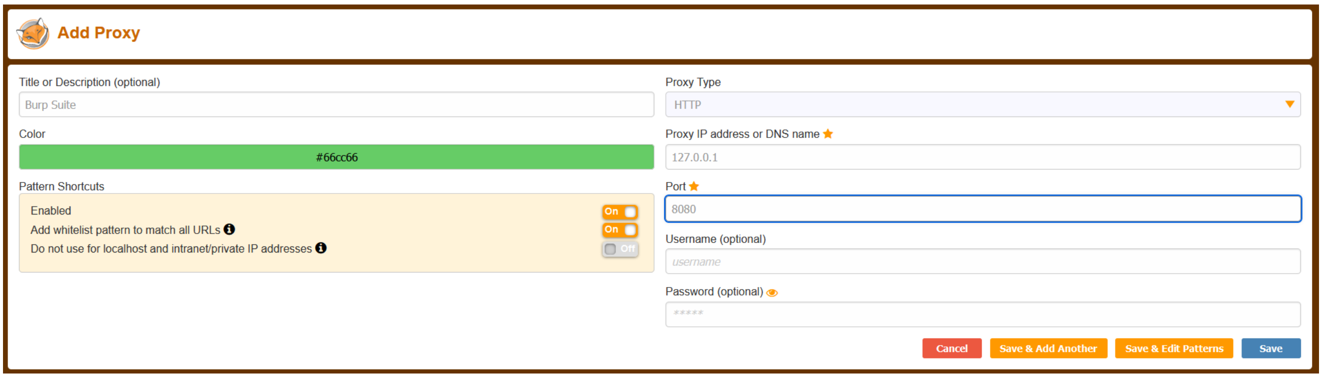
Manage your add-ons and themes through the application menu.

☑ Allow this extension to run in Private Windows

You can close the window that opens, then click the extension in the top-right:



Click 'Options' to add a proxy, then fill in the details to match the listener:



Add Proxy

Title or Description (optional): Burp Suite

Color: #66cc66

Pattern Shortcuts

Enabled — On

Add whitelist pattern to match all URLs — On

Do not use for localhost and intranet/private IP addresses — Off

Proxy Type: HTTP

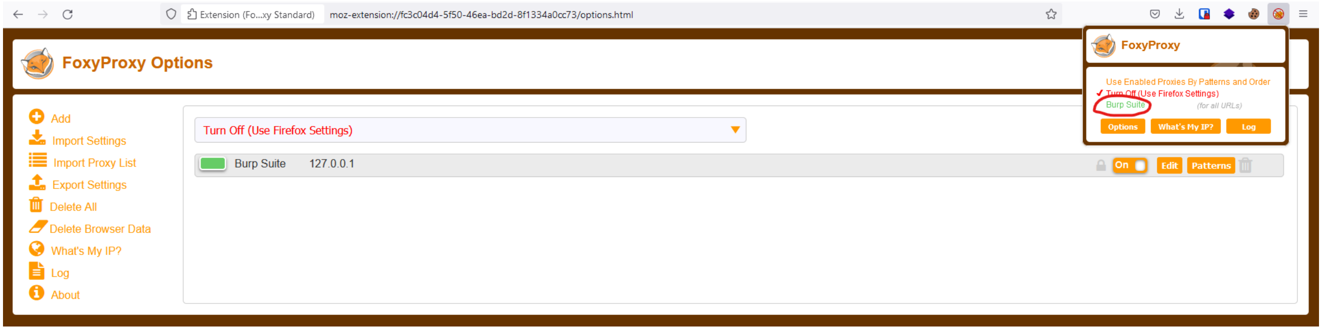
Proxy IP address or DNS name ★: 127.0.0.1

Port ★: 8080

Username (optional): username

Password (optional): *****

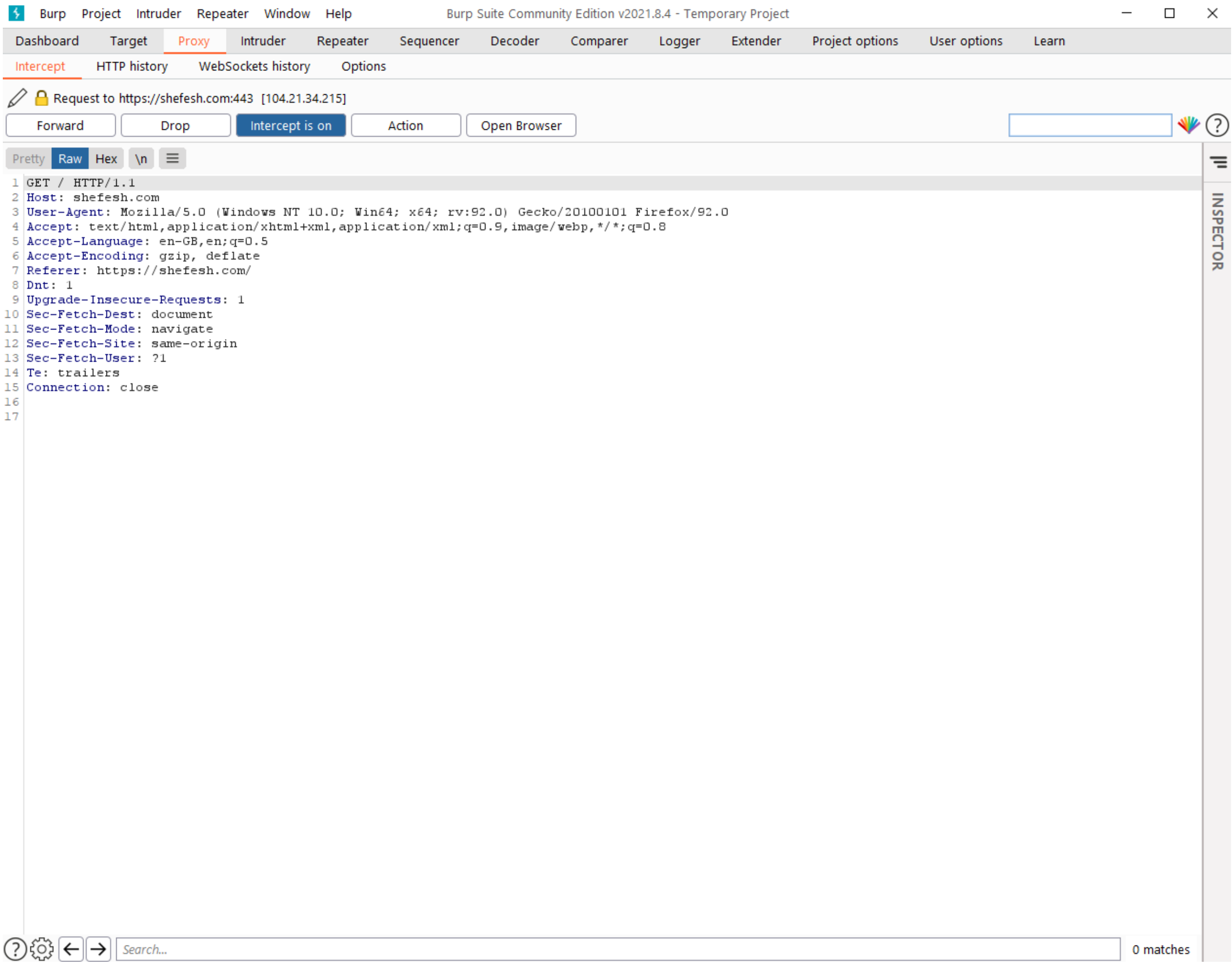
Click 'Save', then you can click the extension again and click your new proxy to enable it and start directing traffic:



Turn Off (Use Firefox Settings)

🟩 Burp Suite 127.0.0.1

Now, when you visit a webpage you will see the request pop up in the Burp Suite *Proxy > Intercept* window:



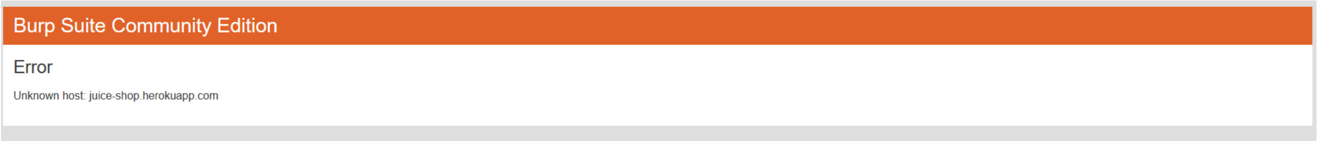
Request to https://shefesh.com:443 [104.21.34.215]

```
GET / HTTP/1.1
Host: shefesh.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://shefesh.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close


```

Burp will now 'hold' the traffic until you either click 'Forward' or turn Intercept off. After it passes through Burp it will go to the server, and you can view the history in the 'HTTP History' tab. We'll cover Intercept in more detail later in this lesson.

If you get a message in your browser (or any other tool) saying that the "Proxy Server is refusing connections", you probably haven't launched Burp or enabled the proxy listener.

If you see an 'Unknown Host' error, you might not have an internet connection:


Burp Suite Community Edition

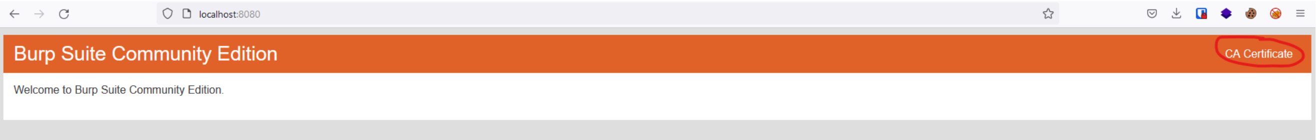
Error

Unknown host: juice-shop.herokuapp.com

Adding the Certificate

If you try to visit a HTTPS website with Burp Suite running, you may be warned by your browser or Antivirus that the certificate is untrustworthy.

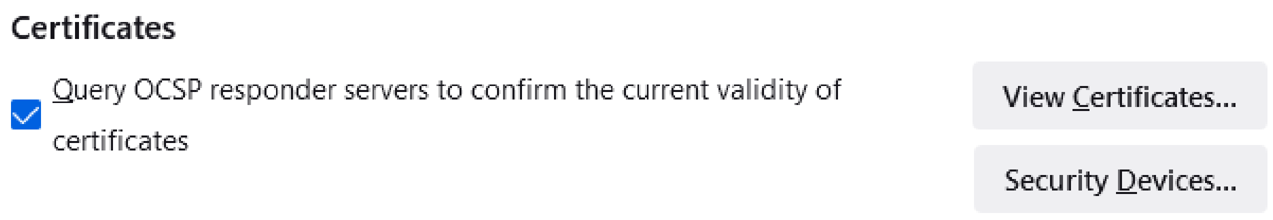
To avoid this warning, you must import Burp's certificate into your browser. To get the certificate, navigate to `localhost:8080` in your browser while Burp is running (or `localhost:[PORT]` if you're using a different port to listen on) and click the 'CA Certificate' button:



Burp Suite Community Edition

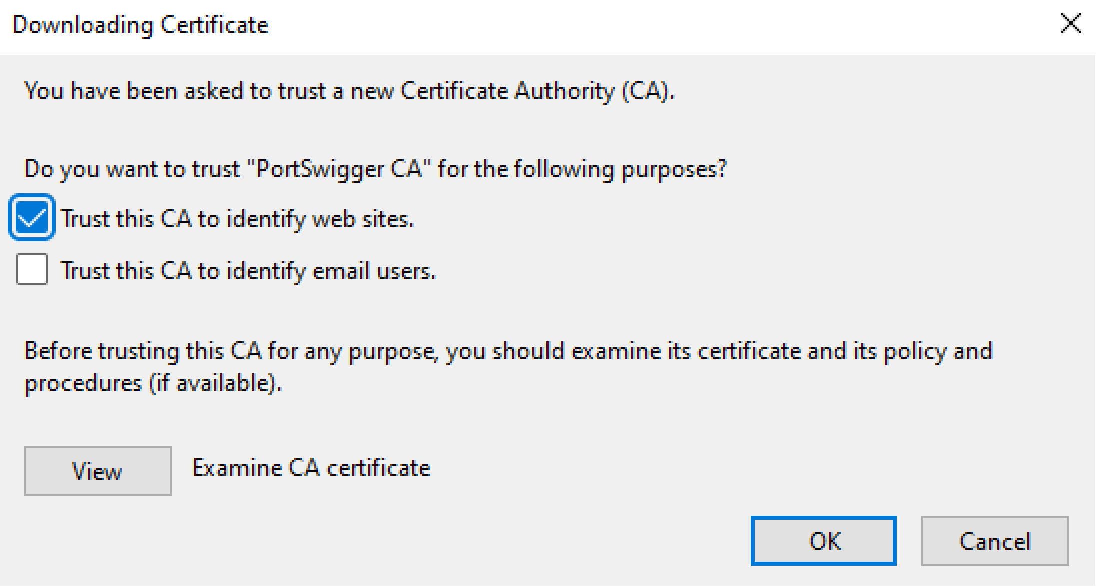
Welcome to Burp Suite Community Edition.

This will download the `cacert.der` file. You can now import this into your browser by navigating to `about:preferences#privacy` in browser and scrolling to the Certificates section:


Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates

Click 'View Certificates', then 'Import', then select the downloaded certificate and tell Firefox to trust it to identify websites:


Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "PortSwigger CA" for the following purposes?

☑ Trust this CA to identify web sites.

□ Trust this CA to identify email users.

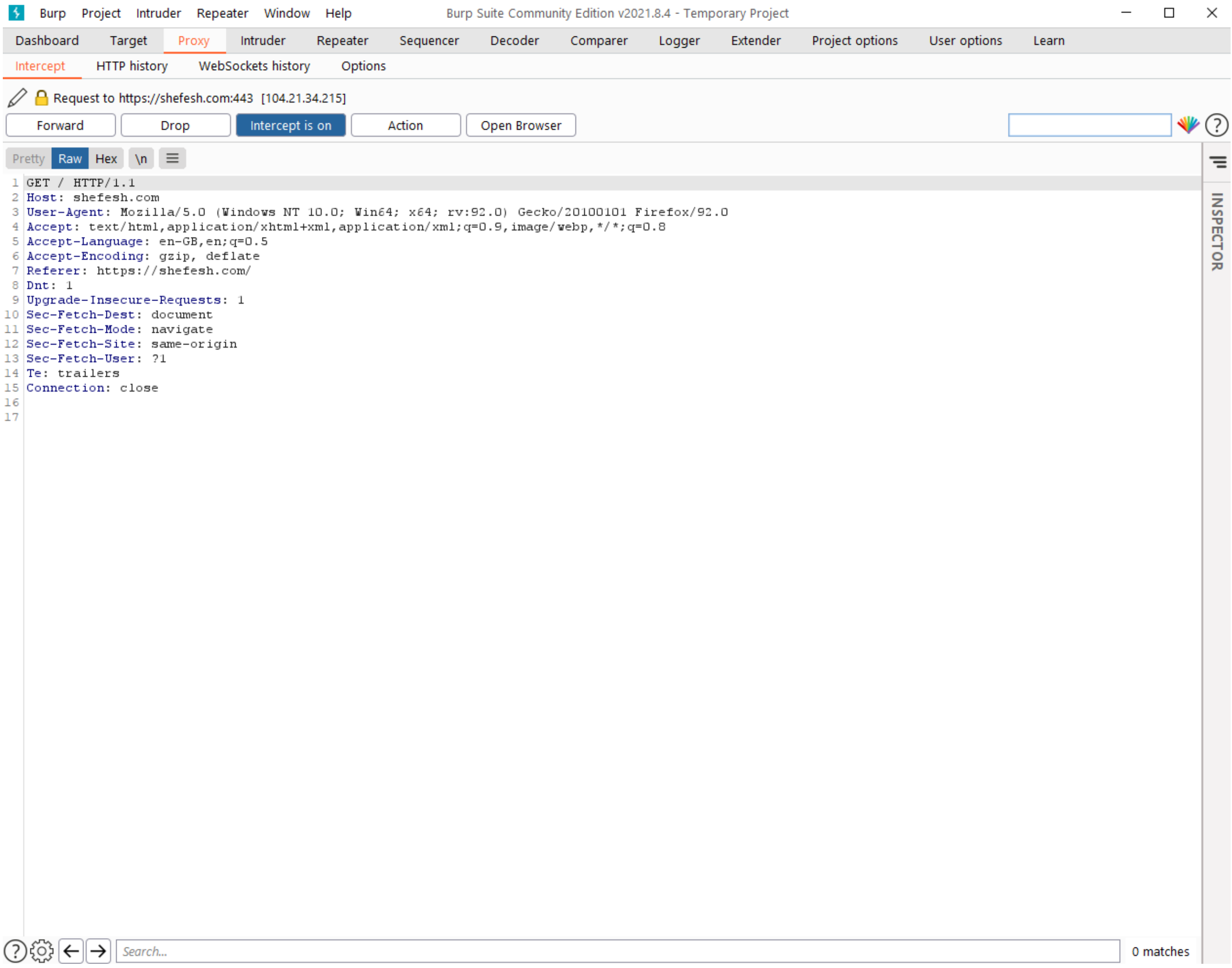
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Click 'OK'. Burp should now work normally over HTTPS.

Intercept

The Intercept tab is where you can inspect HTTP/S traffic before forwarding it to the server.

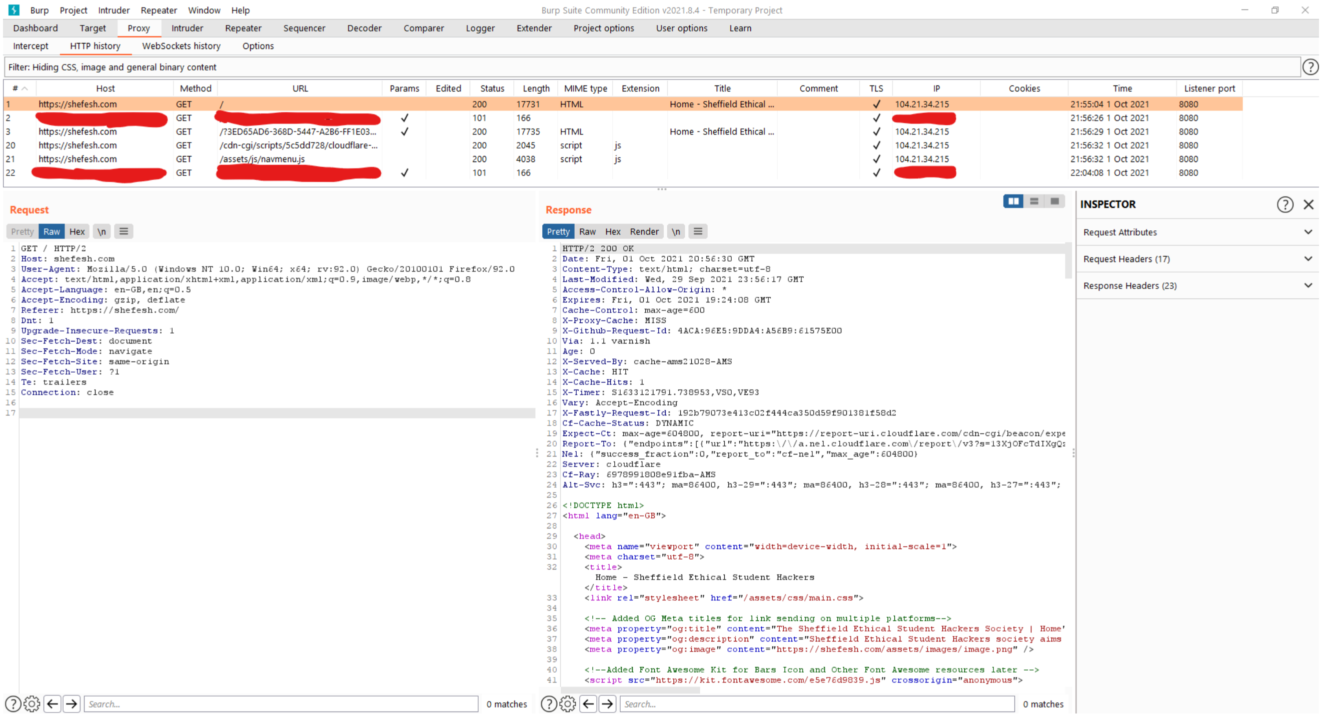
In the tab you can view all elements of the request, including headers and request body:


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2021.8.4 - Temporary Project
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
INSPECTOR
Search...
0 matches

Request to https://shefesh.com:443 [104.21.34.215]

```
GET / HTTP/1.1
Host: shefesh.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://shefesh.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close


```

The HTTP history tab shows *all* previous requests, and their responses:


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2021.8.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
INSPECTOR
Request Attributes
Request Headers (17)
Response Headers (23)
Search...
0 matches
Search...
0 matches

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
1	https://shefesh.com	GET	/			200	17731	HTML		Home - Sheffield Ethical ...		✓	104.21.34.215		21:55:04 1 Oct 2021	8080
2	[redacted]	GET	[redacted]	✓		101	166					✓	[redacted]		21:56:26 1 Oct 2021	8080
3	https://shefesh.com	GET	/?3ED65AD6-368D-5447-A2B6-FF1E03...	✓		200	17735	HTML		Home - Sheffield Ethical ...		✓	104.21.34.215		21:56:29 1 Oct 2021	8080
20	https://shefesh.com	GET	/cdn-cgi/scripts/5c5dd728/cloudflare-...			200	2045	script	js			✓	104.21.34.215		21:56:32 1 Oct 2021	8080
21	https://shefesh.com	GET	/assets/js/navmenu.js			200	4038	script	js			✓	104.21.34.215		21:56:32 1 Oct 2021	8080
22	[redacted]	GET	[redacted]	✓		101	166					✓	[redacted]		22:04:08 1 Oct 2021	8080

```
GET / HTTP/2
Host: shefesh.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://shefesh.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close


```

```
HTTP/2 200 OK
Date: Fri, 01 Oct 2021 20:56:30 GMT
Content-Type: text/html; charset=utf-8
Last-Modified: Wed, 29 Sep 2021 23:56:17 GMT
Access-Control-Allow-Origin: *
Expires: Fri, 01 Oct 2021 19:24:08 GMT
Cache-Control: max-age=600
X-Proxy-Cache: MISS
X-Github-Request-Id: 4ACA:96E5:9DDA4:A56B9:61575E00
Via: 1.1 varnish
Age: 0
X-Served-By: cache-ams21028-AMS
X-Cache: HIT
X-Cache-Hits: 1
X-Timer: S1633121791.738953,VS0,VE93
Vary: Accept-Encoding
X-Fastly-Request-Id: 192b79073e413c02f444ca350d59f901381f58d2
Cf-Cache-Status: DYNAMIC
Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expe
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=13XjOFcTdIXgQz
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 6978991808e91fba-AMS
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443";

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

  <head>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta charset="utf-8">
    <title>
      Home - Sheffield Ethical Student Hackers
    </title>
    <link rel="stylesheet" href="/assets/css/main.css">

    <!-- Added OG Meta titles for link sending on multiple platforms-->
    <meta property="og:title" content="The Sheffield Ethical Student Hackers Society | Home'
    <meta property="og:description" content="Sheffield Ethical Student Hackers society aims
    <meta property="og:image" content="https://shefesh.com/assets/images/image.png" />

    <!--Added Font Awesome Kit for Bars Icon and Other Font Awesome resources later -->
    <script src="https://kit.fontawesome.com/e5e76d9839.js" crossorigin="anonymous">
```

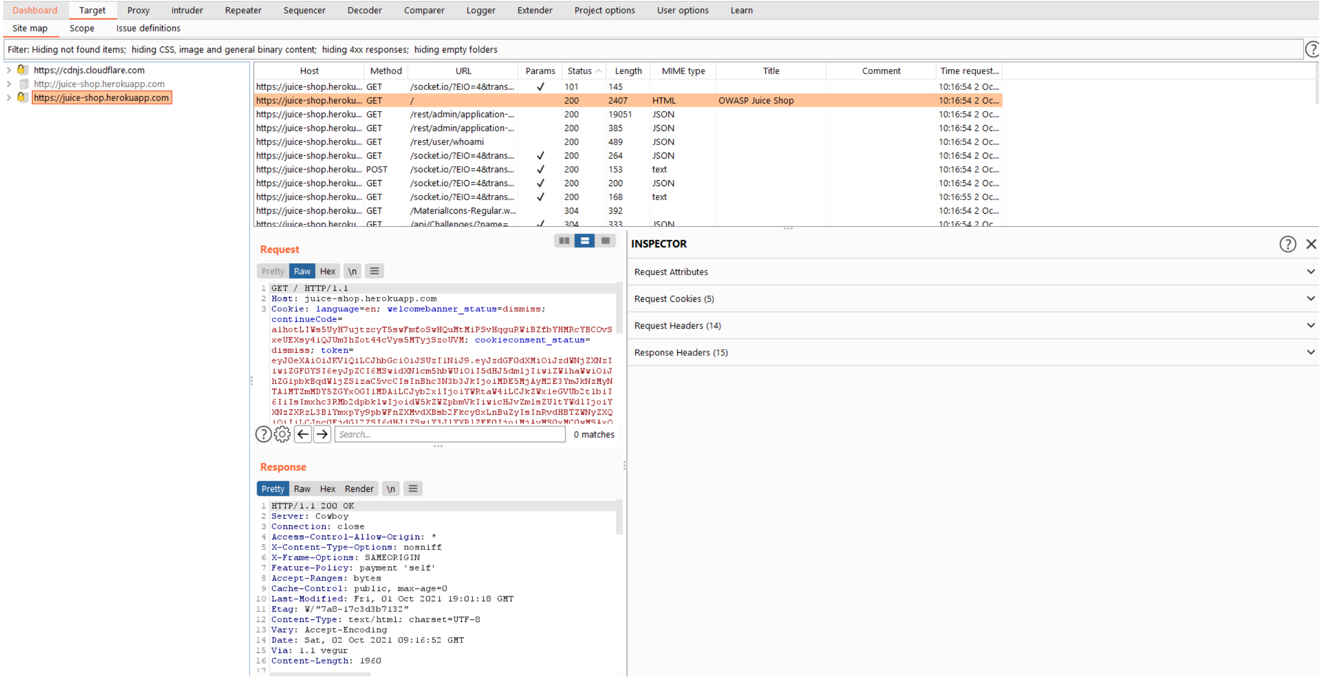
To modify a request before it hits the server, you can hold it in the Intercept tab (by leaving Intercept on and not forwarding the request), then send it to the Repeater by pressing `Ctrl + R`. Once your request is in the Repeater, click drop on the Intercept tab to stop the original request from sending. You can now modify the request.

For a practical example of this, watch [this video]() on the Academy HacktheBox machine.

Traffic Filtering

You may find that your HTTP History gets clogged with a lot of other requests, especially if you're using Burp Suite from your day-to-day machine.

To prevent this, you can add a certain website to your 'scope'. Visit the 'Target' tab, where you can see all websites that Burp has captured traffic for:



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

- https://cdnjs.cloudflare.com
- http://juice-shop.herokuapp.com
- https://juice-shop.herokuapp.com

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time request...
https://juice-shop.heroku...	GET	/socket.io/?EIO=4&trans...	✓	101	145				10:16:54 2 Oc...
https://juice-shop.heroku...	GET	/		200	2407	HTML	OWASP Juice Shop		10:16:54 2 Oc...
https://juice-shop.heroku...	GET	/rest/admin/application-...		200	19051	JSON			10:16:54 2 Oc...
https://juice-shop.heroku...	GET	/rest/admin/application-...		200	385	JSON			10:16:54 2 Oc...
https://juice-shop.heroku...	GET	/rest/user/whoami		200	489	JSON			10:16:54 2 Oc...
https://juice-shop.heroku...	GET	/socket.io/?EIO=4&trans...	✓	200	264	JSON			10:16:54 2 Oc...
https://juice-shop.heroku...	POST	/socket.io/?EIO=4&trans...	✓	200	153	text			10:16:54 2 Oc...
https://juice-shop.heroku...	GET	/socket.io/?EIO=4&trans...	✓	200	200	JSON			10:16:54 2 Oc...
https://juice-shop.heroku...	GET	/socket.io/?EIO=4&trans...	✓	200	168	text			10:16:55 2 Oc...
https://juice-shop.heroku...	GET	/MaterialIcons-Regular.w...		304	392				10:16:54 2 Oc...
https://juice-shop.heroku...	GET	/api/Challenges/?name=	✓	304	333	JSON			10:16:54 2 Oc

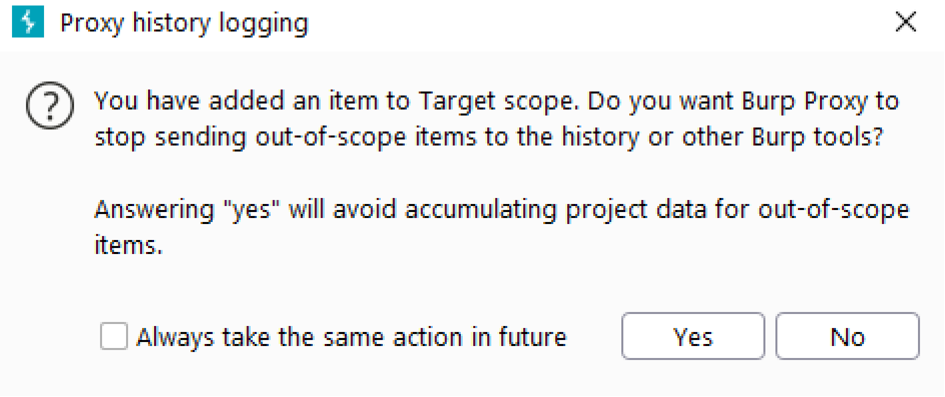
Request

```
GET / HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss;
continueCode=
a1hotLIWs5UyH7ujtzcyT5swFmfoSwHQuMtMiPSvHqguRWiBZfbYHMRcYBCOvS
xeUEXsy4iQJUm3hZot44cVys5MTyjSzoUVM; cookieconsent_status=
dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzI
iwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiI5dHJ5dmljIiwiZW1haWwiOiJ
hZG1pbkBqdW1jZS1zaC5vcCIsInBhc3N3b3JkIjoiMDE5MjAyM2E3YmJkNzMyN
TA1MTZmMDY5ZGYxOGI1MDAiLCJyb2xlIjoiYWRtaW4iLCJkZWx1eGVUb2tlbiI
6IiIsImxhc3RMb2dpbklwIjoidW5kZWZpbmVkIiwicHJvZmlsZUltYWdlIjoiY
XNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy8xLnBuZyIsInRvdHBTZWNyZXQ
```

Response

```
HTTP/1.1 200 OK
Server: Cowboy
Connection: close
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 01 Oct 2021 19:01:18 GMT
Etag: W/"7a8-17c3d3b7132"
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
Date: Sat, 02 Oct 2021 09:16:52 GMT
Via: 1.1 vegur
Content-Length: 1960
```

Right-click the website you are testing (in this case, juice-shop.herokuapp.com) and click 'Add to scope':



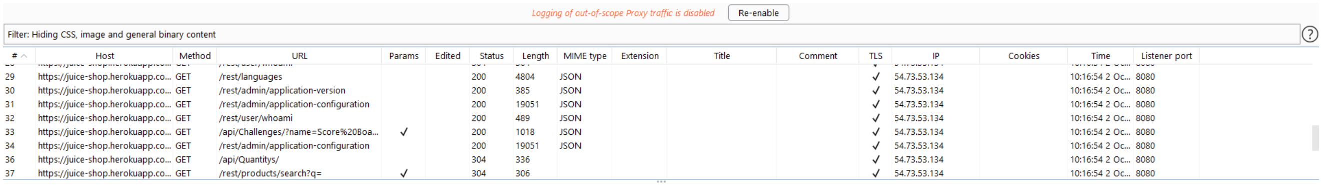
You have added an item to Target scope. Do you want Burp Proxy to stop sending out-of-scope items to the history or other Burp tools?

Answering "yes" will avoid accumulating project data for out-of-scope items.

□ Always take the same action in future

Click yes, and Burp should stop logging traffic from other sites.

Your history tab will now be much cleaner:



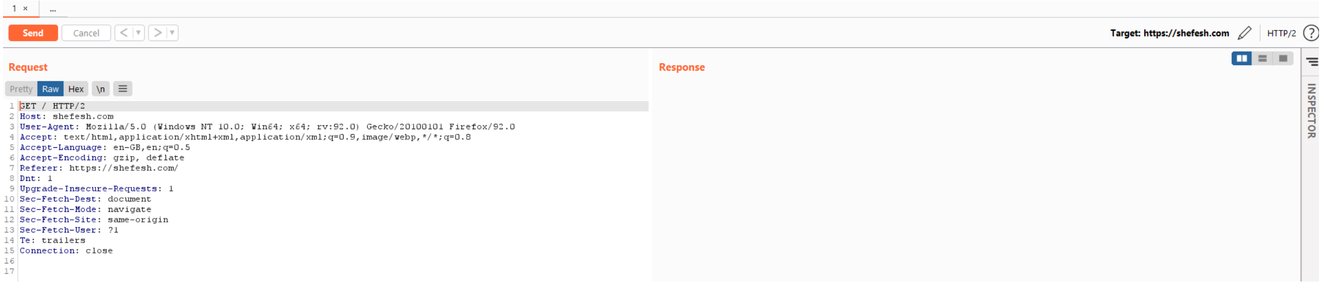
Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
29	https://juice-shop.herokuapp.co...	GET	/rest/languages			200	4804	JSON				✓	54.73.53.134		10:16:54 2 Oc...	8080
30	https://juice-shop.herokuapp.co...	GET	/rest/admin/application-version			200	385	JSON				✓	54.73.53.134		10:16:54 2 Oc...	8080
31	https://juice-shop.herokuapp.co...	GET	/rest/admin/application-configuration			200	19051	JSON				✓	54.73.53.134		10:16:54 2 Oc...	8080
32	https://juice-shop.herokuapp.co...	GET	/rest/user/whoami			200	489	JSON				✓	54.73.53.134		10:16:54 2 Oc...	8080
33	https://juice-shop.herokuapp.co...	GET	/api/Challenges/?name=Score%20Boa...	✓		200	1018	JSON				✓	54.73.53.134		10:16:54 2 Oc...	8080
34	https://juice-shop.herokuapp.co...	GET	/rest/admin/application-configuration			200	19051	JSON				✓	54.73.53.134		10:16:54 2 Oc...	8080
36	https://juice-shop.herokuapp.co...	GET	/api/Quantitys/			304	336					✓	54.73.53.134		10:16:54 2 Oc...	8080
37	https://juice-shop.herokuapp.co...	GET	/rest/products/search?q=	✓		304	306					✓	54.73.53.134		10:16:54 2 Oc...	8080

Repeater

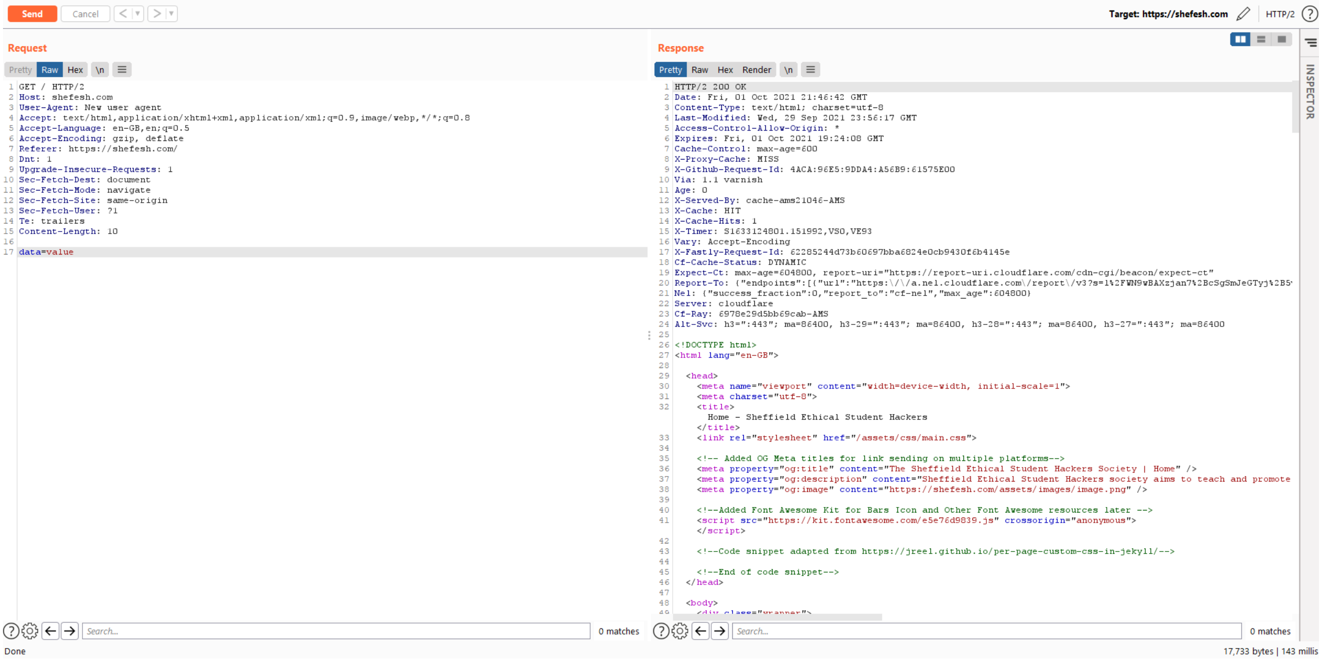
The Repeater tab can be used to Edit & Resend requests, similar to with the Developer Tools.

Here we see the request for the shefesh page that was sent to the Repeater by pressing `Ctrl + R`:



```
GET / HTTP/2
Host: shefesh.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://shefesh.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close


```

We can edit any values in the request, such as headers and data, then press 'Send' and view the results of the response:



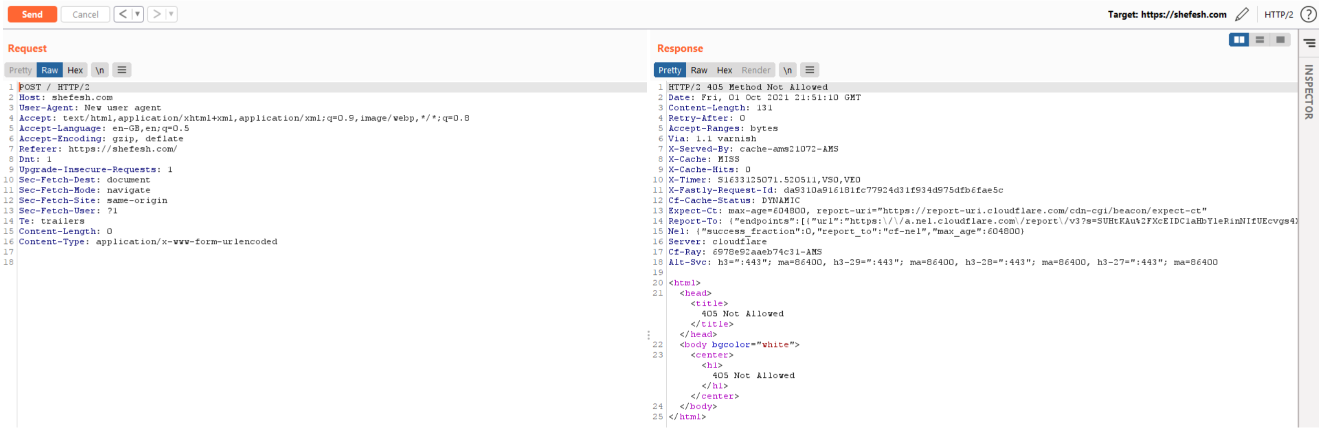
```
GET / HTTP/2
Host: shefesh.com
User-Agent: New user agent
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://shefesh.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Content-Length: 10

data=value
```

```
HTTP/2 200 OK
Date: Fri, 01 Oct 2021 21:46:42 GMT
Content-Type: text/html; charset=utf-8
Last-Modified: Wed, 29 Sep 2021 23:56:17 GMT
Access-Control-Allow-Origin: *
Expires: Fri, 01 Oct 2021 19:24:08 GMT
Cache-Control: max-age=600
X-Proxy-Cache: MISS
X-Github-Request-Id: 4ACA:96E5:9DDA4:A56B9:61575E00
Via: 1.1 varnish
Age: 0
X-Served-By: cache-ams21046-AMS
X-Cache: HIT
X-Cache-Hits: 1
X-Timer: S1633124801.151992,VS0,VE93
Vary: Accept-Encoding
X-Fastly-Request-Id: 62285244d73b60697bba6824e0cb9430f6b4145e
Cf-Cache-Status: DYNAMIC
Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=1%2FWN9wBAXzjan7%2BcSgSmJeGTyj%2B5
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 6978e29d5bb69cab-AMS
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

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

  <head>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta charset="utf-8">
    <title>
      Home - Sheffield Ethical Student Hackers
    </title>
    <link rel="stylesheet" href="/assets/css/main.css">

    <!-- Added OG Meta titles for link sending on multiple platforms-->
    <meta property="og:title" content="The Sheffield Ethical Student Hackers Society | Home" />
    <meta property="og:description" content="Sheffield Ethical Student Hackers society aims to teach and promote
    <meta property="og:image" content="https://shefesh.com/assets/images/image.png" />

    <!--Added Font Awesome Kit for Bars Icon and Other Font Awesome resources later -->
    <script src="https://kit.fontawesome.com/e5e76d9839.js" crossorigin="anonymous">
    </script>

    <!--Code snippet adapted from https://jreel.github.io/per-page-custom-css-in-jekyll/-->

    <!--End of code snippet-->
  </head>

  <body>
    <div class="wrapper">
```

17,733 bytes | 143 millis

The size of the response is shown in the bottom-right corner - checking whether this changes is a good indicator of whether the changes you made had any impact.

We can also change the HTTP request method (right-click + 'Change request method') from the repeater tab, to conveniently turn a GET request for a specific resource into a POST request:



```
POST / HTTP/2
Host: shefesh.com
User-Agent: New user agent
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://shefesh.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Content-Length: 0
Content-Type: application/x-www-form-urlencoded

```

```
HTTP/2 405 Method Not Allowed
Date: Fri, 01 Oct 2021 21:51:10 GMT
Content-Length: 131
Retry-After: 0
Accept-Ranges: bytes
Via: 1.1 varnish
X-Served-By: cache-ams21072-AMS
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1633125071.520511,VS0,VE0
X-Fastly-Request-Id: da9310a916181fc77924d31f934d975dfb6fae5c
Cf-Cache-Status: DYNAMIC
Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=SUHtKAu%2FXcEIDC1aHbYleRinNIfUEcvgs4
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 6978e92aaeb74c31-AMS
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

<html>
  <head>
    <title>
      405 Not Allowed
    </title>
  </head>
  <body bgcolor="white">
    <center>
      <h1>
        405 Not Allowed
      </h1>
    </center>
  </body>
</html>
```

You can use this tab to experiment with different values in parameters, try to send requests that may trigger errors in the application, try to exploit IDOR-style vulnerabilities, and resend payloads to web shells - the possibilities are endless.

Intruder

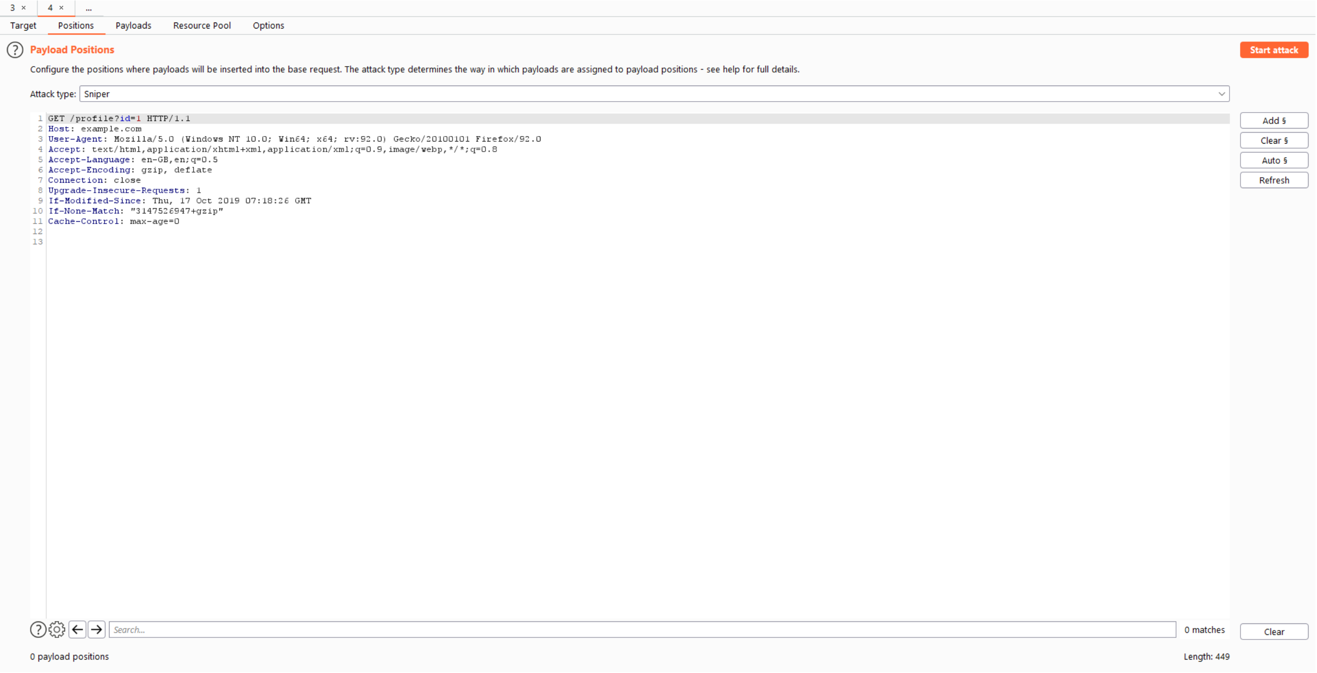
The Intruder tab is similar to the Repeater tab, in that it can resend HTTP requests. The extra feature of the Intruder tab is its ability to automate the sending of HTTP requests within a certain scheme, automatically replacing parts of the request with a sequence of predefined values.

What does this mean? It means you can take a captured Burp request - for example, a GET request to `http://example.com/profile?id=1` - and select a portion of the URL to modify according to a ruleset.

You may, for example, want to perform a brute force attack against the website and see if you can discover any other user profiles by their ID. You could do this by hand, visiting `http://example.com/profile?id=2` and `http://example.com/profile?id=3` until you find a match - or you could tell the Intruder to do it for you.

> Important note: the following example is purely illustrative. We are not performing a vulnerability assessment on example.com, and there is no intention of causing undesired effects. The URL /profile does not exist on example.com, so the requests will have no impact besides a small amount of traffic - they merely illustrate what the Intruder could be used for. Remember you can only perfom a vulnerability assessment on a site that you have explicit permission to do so on, such as juice-shop.herokuapp.com.

Press `Ctrl + I` to send a request to the Intruder:



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

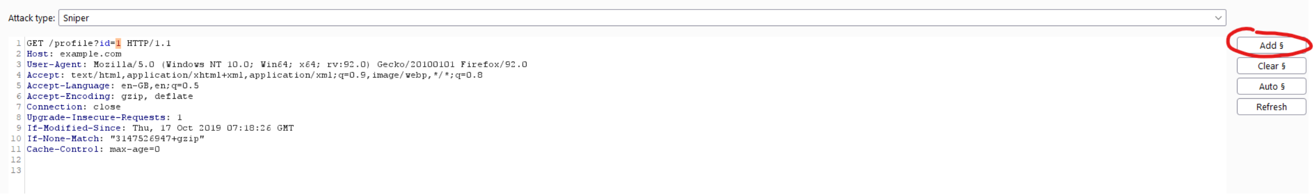
```
GET /profile?id=1 HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Thu, 17 Oct 2019 07:18:26 GMT
If-None-Match: "3147526947+gzip"
Cache-Control: max-age=0
```

0 payload positions

Length: 449

The default attack type is 'Sniper', which will insert values into the desired 'positions'.

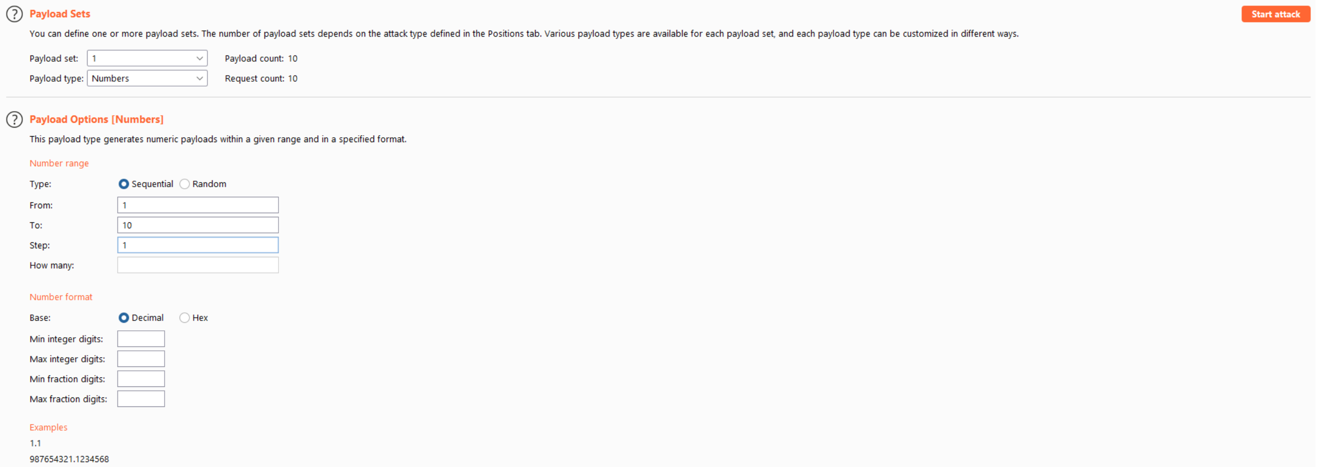
Now we need to define these positions - we can do so by highlighting the text we want to be replaced, and clicking the 'Add' button on the side:


Attack type: Sniper

```
GET /profile?id=1 HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Thu, 17 Oct 2019 07:18:26 GMT
If-None-Match: "3147526947+gzip"
Cache-Control: max-age=0
```

This adds two characters round the text, indicating it will be replaced: `§1§`

We then go to the Payloads tab and tell Burp which values should replace the text in each position. The most simple payload type is 'Numbers', for which we can fill out the numbers 1-10 sequentially, with a step of 1 (meaning the numbers will increase by one with each request):



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1   Payload count: 10

Payload type: Numbers   Request count: 10

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

From: 1

To: 10

Step: 1

How many:

Number format

Base: ● Decimal ○ Hex

Min integer digits:

Max integer digits:

Min fraction digits:

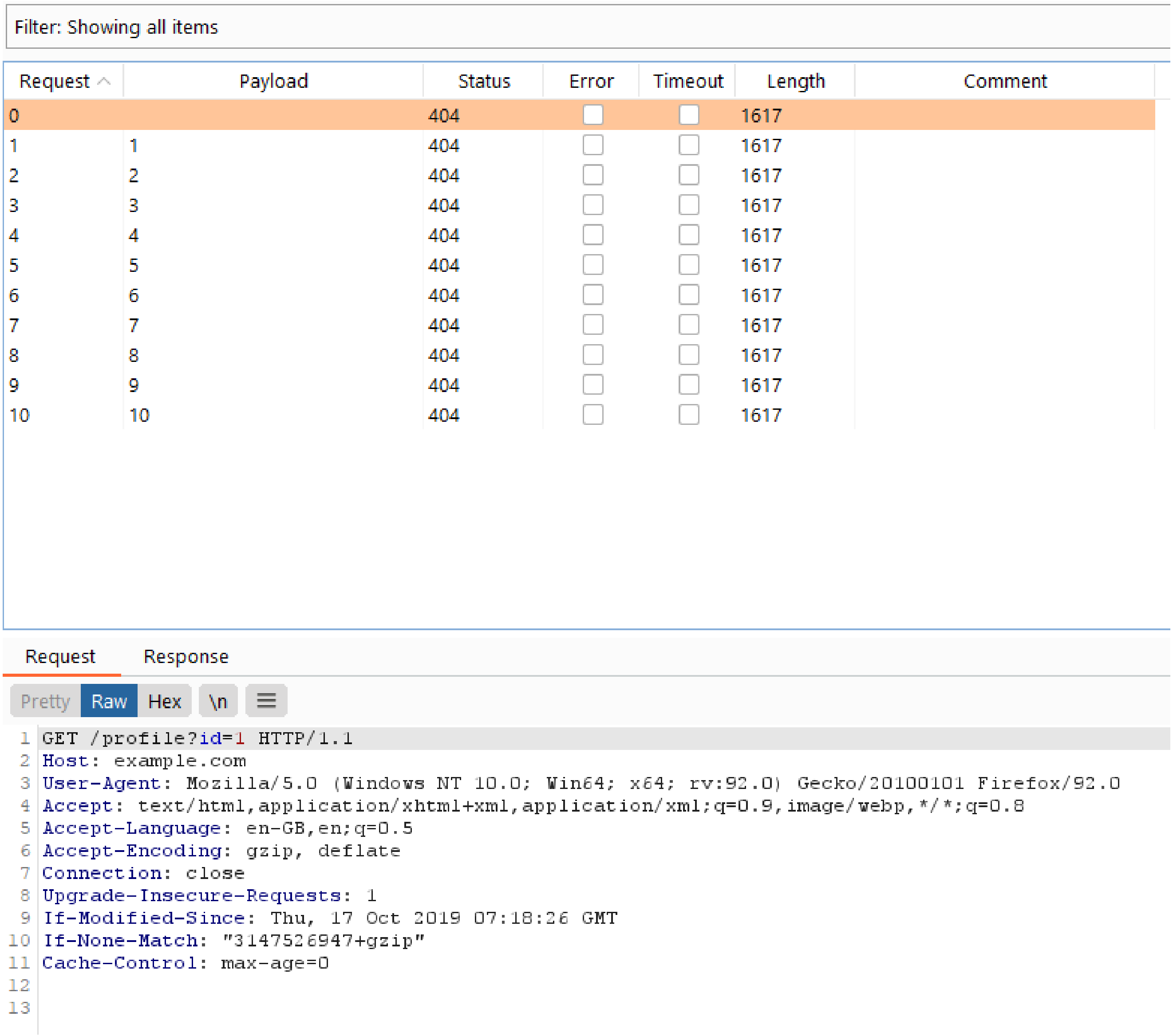
Max fraction digits:

Examples

1.1

987654321.1234568

Then click 'Start Attack' - this will re-make these requests, replacing the `id` parameter with a new number each time. Clicking a request shows it in more detail:



Request	Payload	Status	Error	Timeout	Length	Comment
0		404	□	□	1617	
1	1	404	□	□	1617	
2	2	404	□	□	1617	
3	3	404	□	□	1617	
4	4	404	□	□	1617	
5	5	404	□	□	1617	
6	6	404	□	□	1617	
7	7	404	□	□	1617	
8	8	404	□	□	1617	
9	9	404	□	□	1617	
10	10	404	□	□	1617	

```
GET /profile?id=1 HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Thu, 17 Oct 2019 07:18:26 GMT
If-None-Match: "3147526947+gzip"
Cache-Control: max-age=0


```

Using this method we could look for a page that returns a non-404 status code, indicating we had found a profile.

This method is often called fuzzing. It can be done much better by other tools, but the concept is important and sometimes the intruder can be helpful for small-scale fuzzing. We will teach you about more efficient fuzzing tools as the semester goes on.

> If you wanted to reuse a request captured by Burp, perhaps in a `curl` command or to pass to a specialised fuzzing program, then you can right-click the request and click 'Copy as curl command'

Cheatsheet

`Ctrl + R` to send a request to the Repeater.

`Ctrl + I` to send a request to the Intruder.

Worksheet

1. Visit https://juice-shop.herokuapp.com/-and-proxy-the-traffic-to-burp-suite.-add-an-item-to-your-basket,-and-see-if-you-can-identify-which-request-adds-the-item-(hint:-it's-a-post-request)
2. After identifying this request, send it to the Repeater tab. Can you modify it so the item is added to another user's basket? (hint: it might not be as simple as changing one value - an error message in the response might tell you more)
3. View your basket, and identify the request that returns the basket data. Can you modify this request to *view* another user's basket? Use this to verify the previous exercise