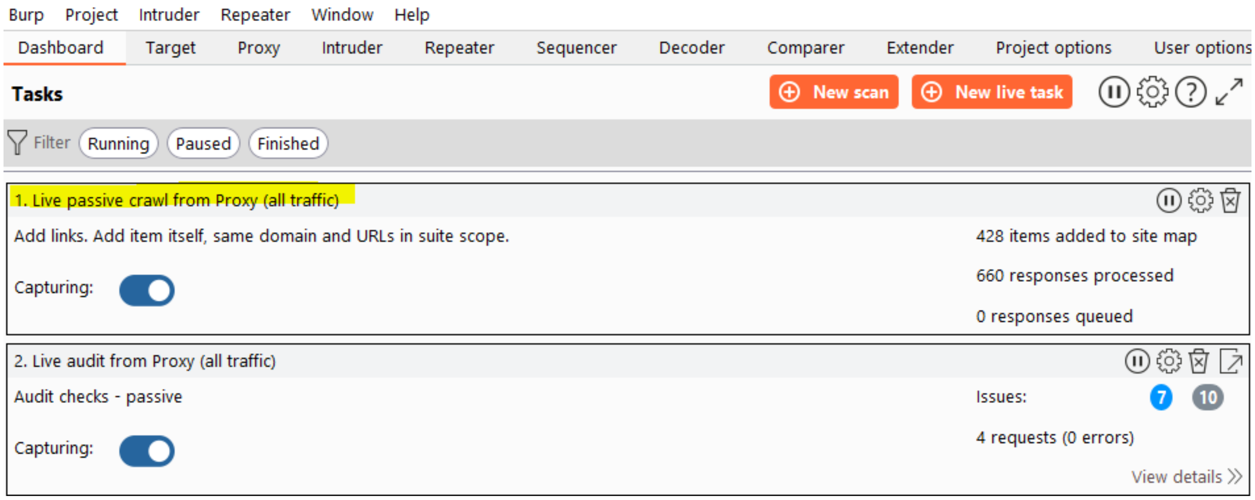
Burp suite: Target

Introduction

In this tab, we can find several useful options that are invaluable in any bug bounty hunters toolbelt in my opinion. I'm not going to bore you with the very basics, i assume you already know those. Instead i am going to show you all the cool tricks we can with this section of burp.

Site map

The site map displays any URL that we visited while browsing the website manually if we have our passive crawling job active in the background to fill the site map.



1. Live passive crawl from Proxy (all traffic)

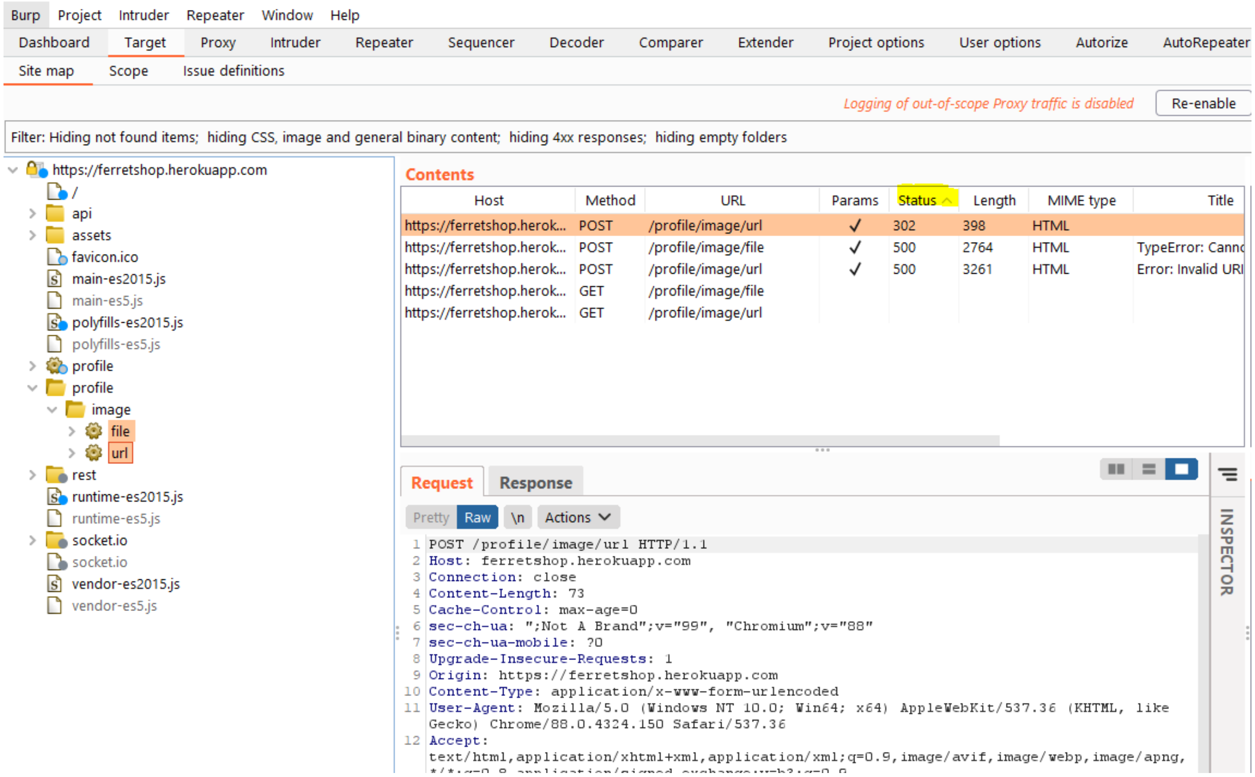
Add links. Add item itself, same domain and URLs in suite scope.

428 items added to site map
660 responses processed
0 responses queued

2. Live audit from Proxy (all traffic)

Audit checks - passive

4 requests (0 errors)



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

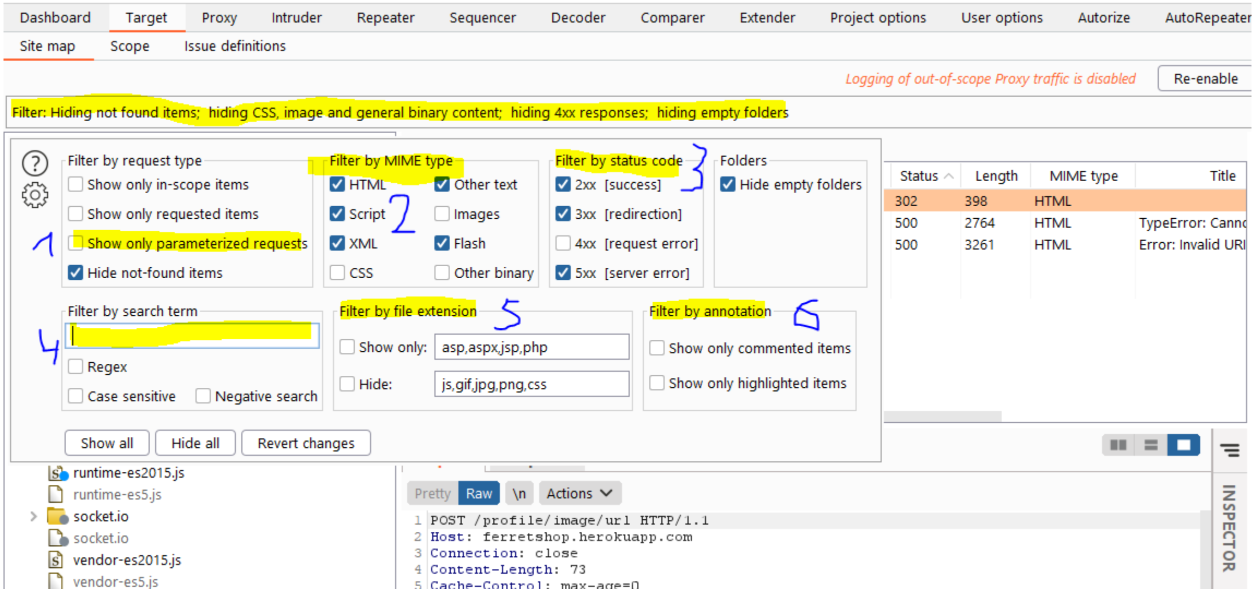
Host	Method	URL	Params	Status	Length	MIME type	Title
https://ferretshop.herok...	POST	/profile/image/url	✓	302	398	HTML	
https://ferretshop.herok...	POST	/profile/image/file	✓	500	2764	HTML	TypeError: Cann
https://ferretshop.herok...	POST	/profile/image/url	✓	500	3261	HTML	Error: Invalid URI
https://ferretshop.herok...	GET	/profile/image/file					
https://ferretshop.herok...	GET	/profile/image/url					

```
POST /profile/image/url HTTP/1.1
Host: ferretshop.herokuapp.com
Connection: close
Content-Length: 73
Cache-Control: max-age=0
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="88"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: https://ferretshop.herokuapp.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/88.0.4324.150 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
```

One thing i will always do is sort my responses via status code. This makes it easier to view the requests that return a 200 status code and then i can judge if they should.

Please note that by default items with a response code of 4xx (i.e. 403) are not shown in the site tree. We can enable those in the filtering, that's where the real fun starts.

filtering



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

Filter by request type
☐ Show only in-scope items
☐ Show only requested items
☐ Show only parameterized requests
☑ Hide not-found items

Filter by MIME type
☑ HTML
☑ Script
☑ XML
☐ CSS
☑ Other text
☐ Images
☑ Flash
☐ Other binary

Filter by status code
☑ 2xx [success]
☑ 3xx [redirection]
☐ 4xx [request error]
☑ 5xx [server error]

Folders
☑ Hide empty folders

Filter by search term
☐ Regex
☐ Case sensitive
☐ Negative search

Filter by file extension
☐ Show only: asp,aspx,jsp,php
☐ Hide: js,gif,jpg,png,css

Filter by annotation
☐ Show only commented items
☐ Show only highlighted items

Status	Length	MIME type	Title
302	398	HTML	
500	2764	HTML	TypeError: Cannc
500	3261	HTML	Error: Invalid URI

runtime-es2015.js
runtime-es5.js
socket.io
socket.io
vendor-es2015.js
vendor-es5.js

```
POST /profile/image/url HTTP/1.1
Host: ferretshop.herokuapp.com
Connection: close
Content-Length: 73
Cache-Control: max-age=0
```

If we click the filter bar at the top of the screen, we can some very useful filters.

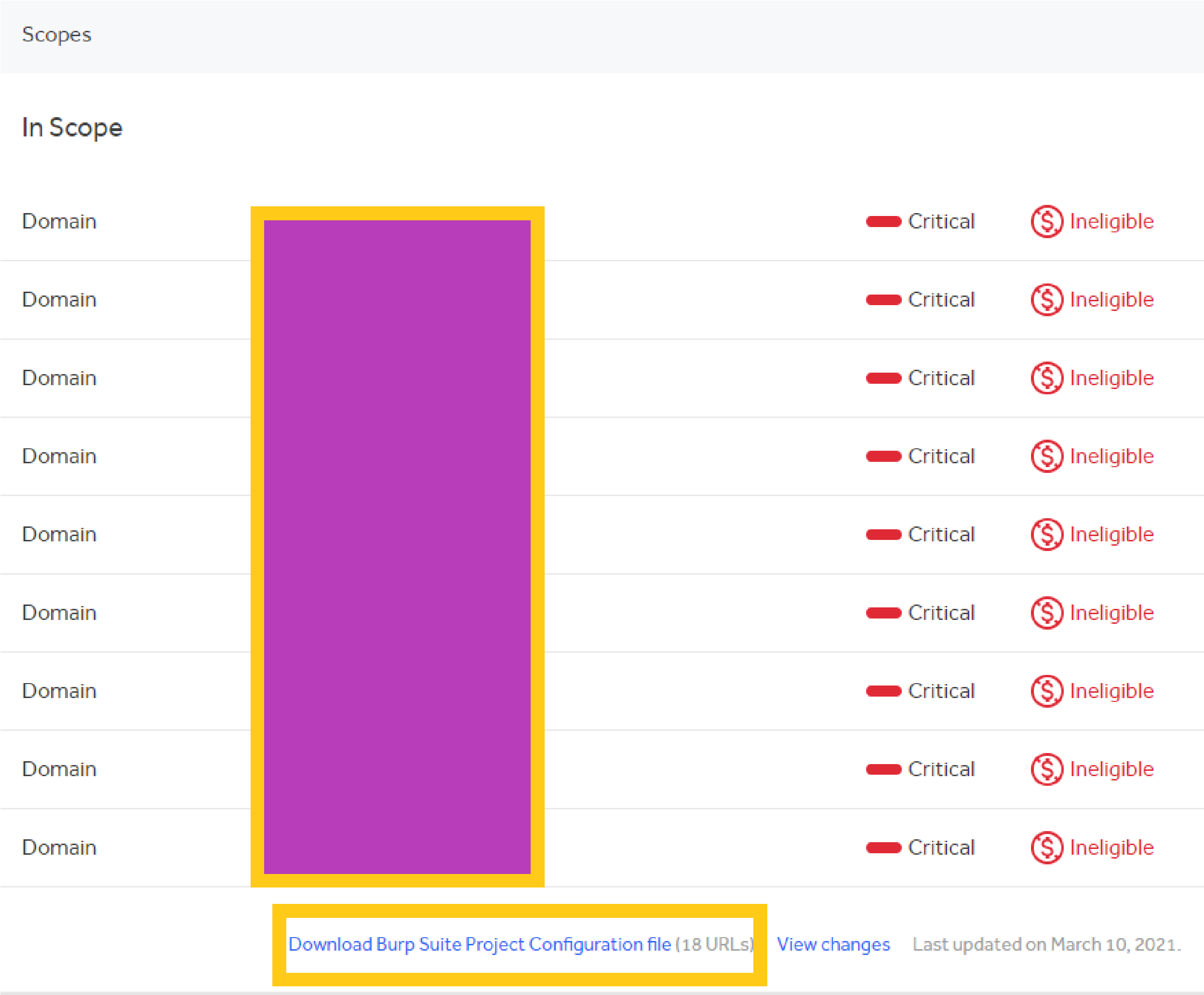
1. Showing only the paramterised requests will show us all the requests that allow us some kind of interaction with the server. These are the requests that i care about mosts as they talk to the API.
2. Filtering by mime type allows us to include or exclude certain types of files such as scripts or CSS files by checking or unchecking the checkbox respectively.
3. If we want to show or hide certain status codes, that's also possible like the 4xx status codes which are disabled by default
4. If we want to search for specific terms, that also possible. We can do this in negative search as well, which would mean that we would **exclude** requests with the search term in it.
5. If we want to hide or show certain file types, that's also possible but we can't use both together as they would cancel eachother out
6. We can also annote or comment certain requests by right clicking them in the site map, repeater or proxy history and then we can filter on those requests.

Scope

In here, we set our scope as the name says 🙂 it might not seem like it, but this insignifficant section is the most important one of our whole project. If we don't set our scope properly we risk of testing targets which are not covered in our program. These targets can be neferious but they can also be 3rd parties which don't like all the hacker attention.

On the other hand, set the scope wrong or too strict and you are missing a ton of potential requests.

Hackerone has configuration files for burp you can download.



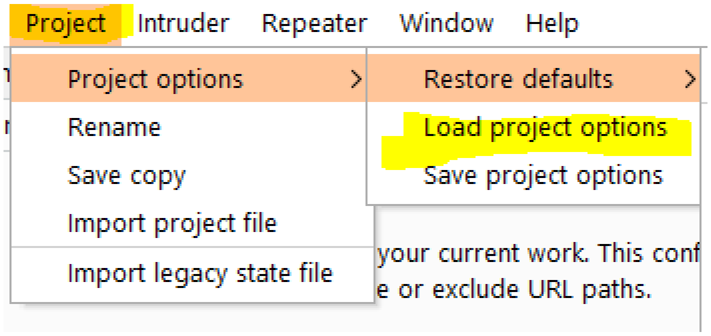
Scopes

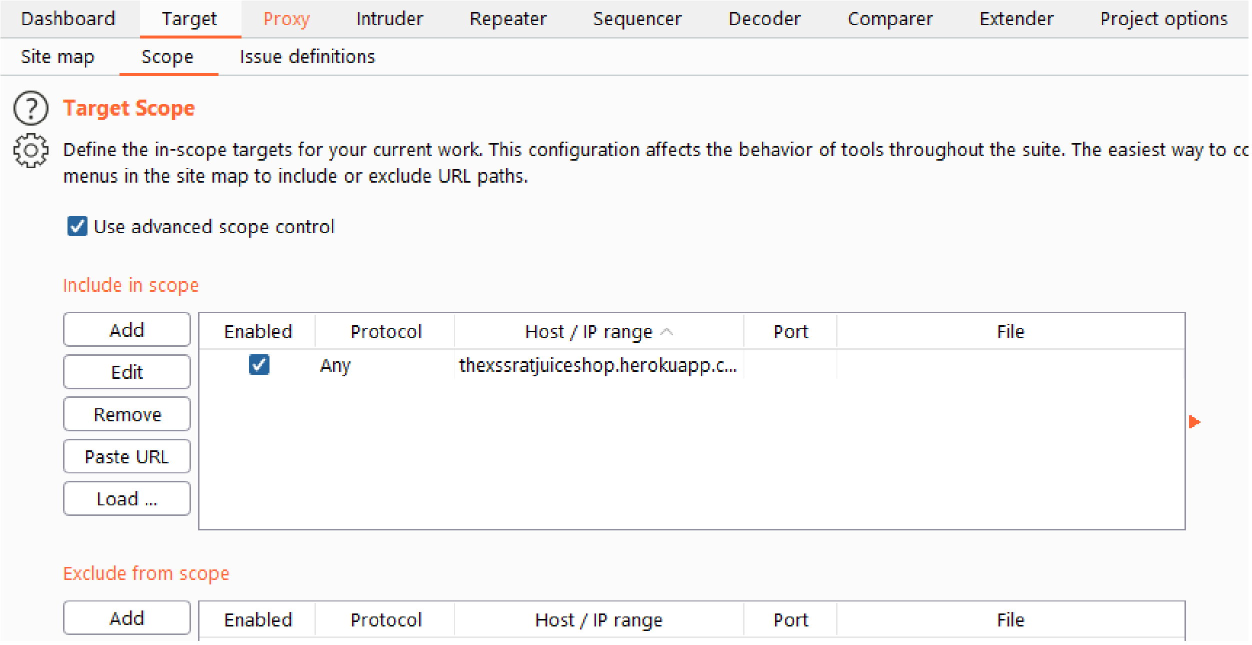
In Scope

Domain	[redacted]	Critical	Ineligible
Domain	[redacted]	Critical	Ineligible
Domain	[redacted]	Critical	Ineligible
Domain	[redacted]	Critical	Ineligible
Domain	[redacted]	Critical	Ineligible
Domain	[redacted]	Critical	Ineligible
Domain	[redacted]	Critical	Ineligible
Domain	[redacted]	Critical	Ineligible
Domain	[redacted]	Critical	Ineligible

Download Burp Suite Project Configuration file (18 URLs) View changes Last updated on March 10, 2021.

You can then import this file via the project options import functionality under "Project > Project options > Load Project options"





Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to cc menus in the site map to include or exclude URL paths.

☑ Use advanced scope control

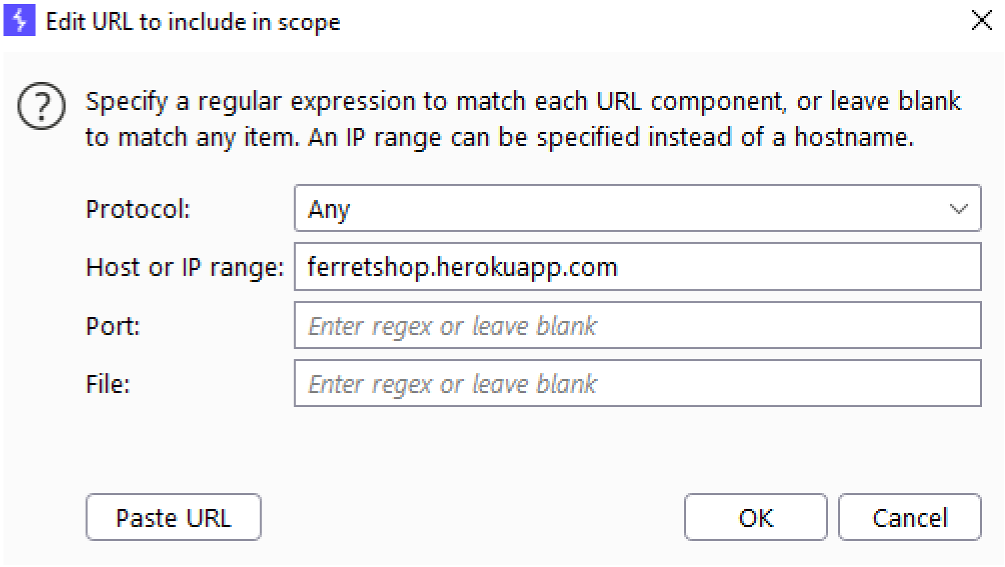
Include in scope

Enabled	Protocol	Host / IP range	Port	File
☑	Any	thexssratjuiceshop.herokuapp.c...		

Exclude from scope

Enabled	Protocol	Host / IP range	Port	File

I always use the "Advanced scope control" myself which allows you to enter regular expressions. Make sure you don't include the protocol (HTTPS:// or HTTP://) in the host or ip range as that is a seperate field.



Specify a regular expression to match each URL component, or leave blank to match any item. An IP range can be specified instead of a hostname.

Protocol: Any

Host or IP range: ferretshop.herokuapp.com

Port: Enter regex or leave blank

File: Enter regex or leave blank

Make note of the fact that you can also exclude URLs from the scope. This can be very useful if you have certain subdirectories for example that are out of scope or if you are at an assignment that only provides out of scope URLs and a *.target.com in scope URL.

Issue definitions

This is just a list of all issues that can be detected by burp and their descriptions.