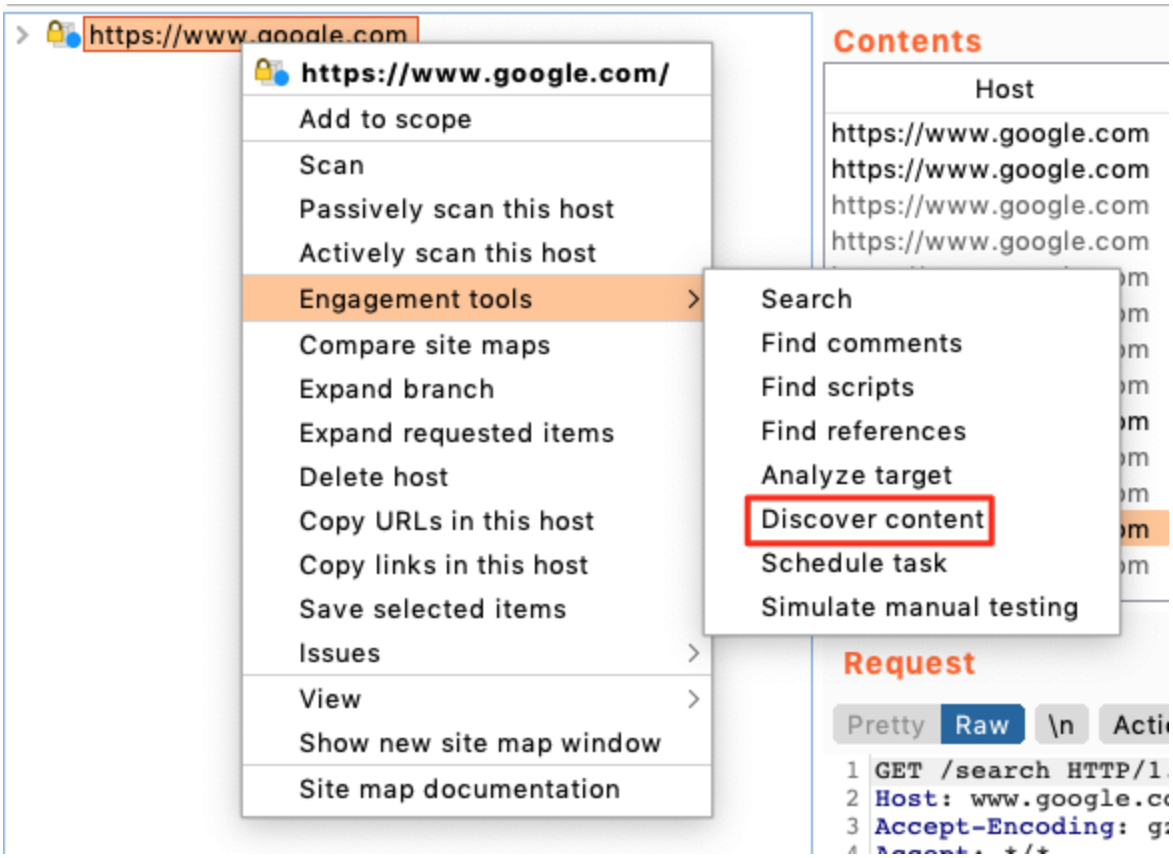
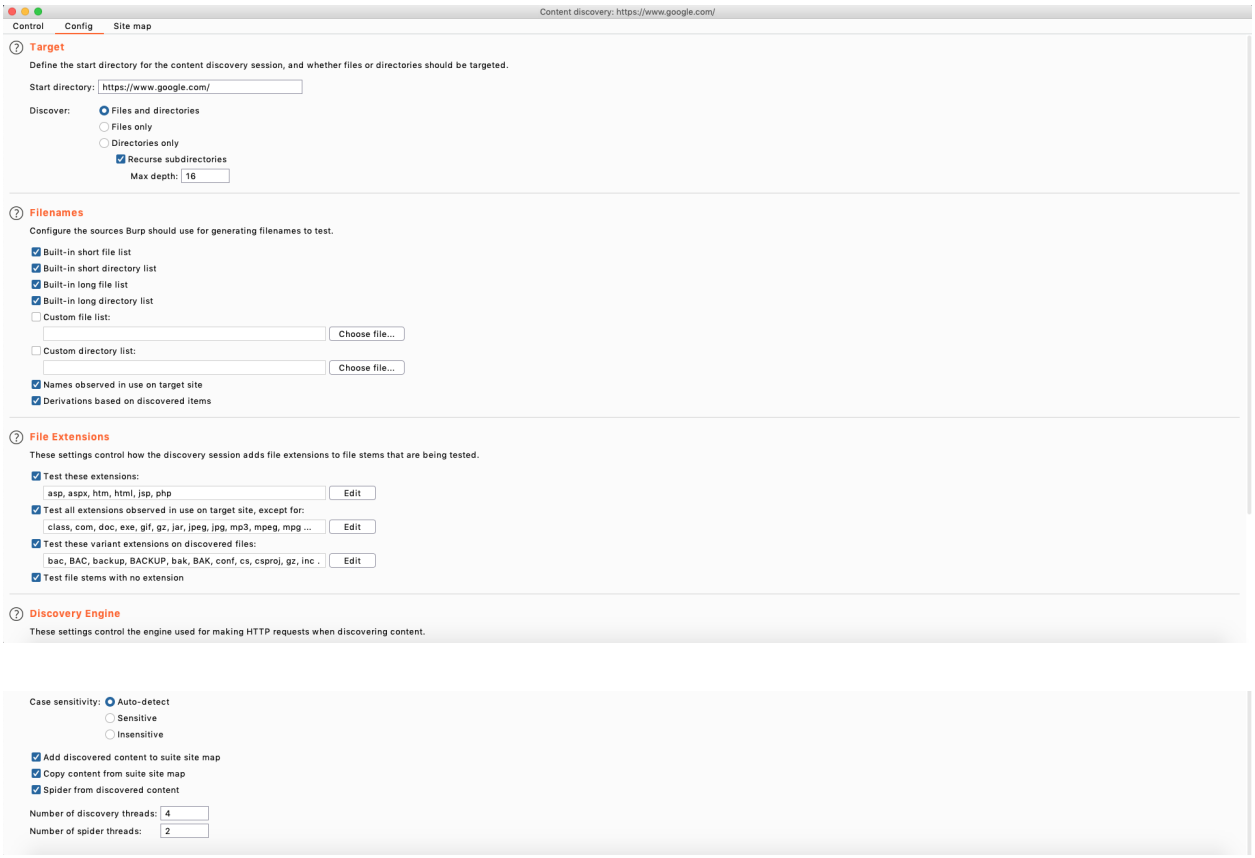
Burp Suite: Content discovery

Burp suite pro users have a range of engagement tools available to them, one of them and a very important one for that matter would be the content discovery tool. This is one of the most sophisticated spiders i ever found and it's the one i use most, however it is limited to content and directory brute forcing, it can not fuzz parameters.



Burp Suite Pro version content discovery



There are a lot of options in here that most people don't ever touch which is a big shame! Ofcourse the default options are fine, but i am a big proponent of tweaking your attack strategy for every target. This includes setting custom settings for our attack tools, blindly running the same tool against a range of different targets is not a good idea. Let's have a look at what we can tweak here.

- Start directory: We can play with this if we don't want to test the root of a website for example
- Discover: Here we can pick if we want to find only files, directories or both (Default option), The recursive subdirectories option allows us to set how deep the spider will crawl. By default if the spider has gone 16 links deep into a website it will stop but we can tweak this.
- Filenames: Burp suite has some filename lists built in by default and it will use the short and long list by default which makes the scan quite lengthy if the spider can go 16 levels deep. I usually start out with the small list and if i don't find what i need, i will go on to the big list, and ofcourse we can never forget about custom lists either. They are the diesel to our engines!

- File extensions is something you ALWAYS have to tune to your target, just open your target, open wappalyzer(browser plugin) and see what the server is running. Don't waste time trying to brute force ASPX servers with PHP files. Don't be a dumbass.
- Discovery engine: This will determine how the crawler engine will behave towards your target. The default options are good here unless you know for sure your target is case (in)sensitive. The number of threads determine how many children burp suite will spawn (that sounds brutal) to start crawling and discovering content. If your target requires you to keep it low and slow, ofcourse do change these values.

When everything is configured correctly, burp suite can start running.