As the title of the challenge suggests, we are asked to perform a recon of this web application.

Besides other things, I ran gobuster to see if there are any hidden files and I found that the source file is called index.php. This could have also been done manually since it's one of the most common filenames. However, the fact that it's a php file and not a .html means there might be some hidden logic behind it.

At this point I got a bit stuck, so I started to look online to get ideas. On https://hak2learn.gitbook.io/hak2learn/webapp/recon-checklist I found "*Identify hidden parameters & headers (Paraminer – Burp Extension)*". This refers to the fact that sometimes php files contain logic connected to parameters, like /index.php?a=test would reveal something extra. I ran **ffuf -u 'http://34.107.95.209:31876/index.php?FUZZ=test' -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -fs 76** to see if there is anything worth noting, and turns out parameter **m** is the magic parameter.

Made with love by: AndreiCat