Scan Book

In this challenge we were given the task of finding the flag in a website that generated QR Codes based on user input. These codes could then be uploaded to the website to retrieve the original message. For this challenge I noticed that when creating a QR Code you would get an image that was stored in https://scanbook.chall.pwnoh.io/static/codes/#.png where # would be the file number. Seeing this I decided to create a script that would search all possible files present in the site by using HTTP requests with that parameter hardcoded.

Welcome to Scanbook

Scanbook is a **secure storage platform** for all of your valuable plaintext.

How does it work? Simple:

Submit your content
Save your ticket
Use your ticket to retrieve your content

It's just that easy!

Make a Post

Enter your plaintext below:

fortnite travis scott burger

Post

View a Post

Upload your ticket to retrieve your plaintext:

Browse… No file selected. Scan

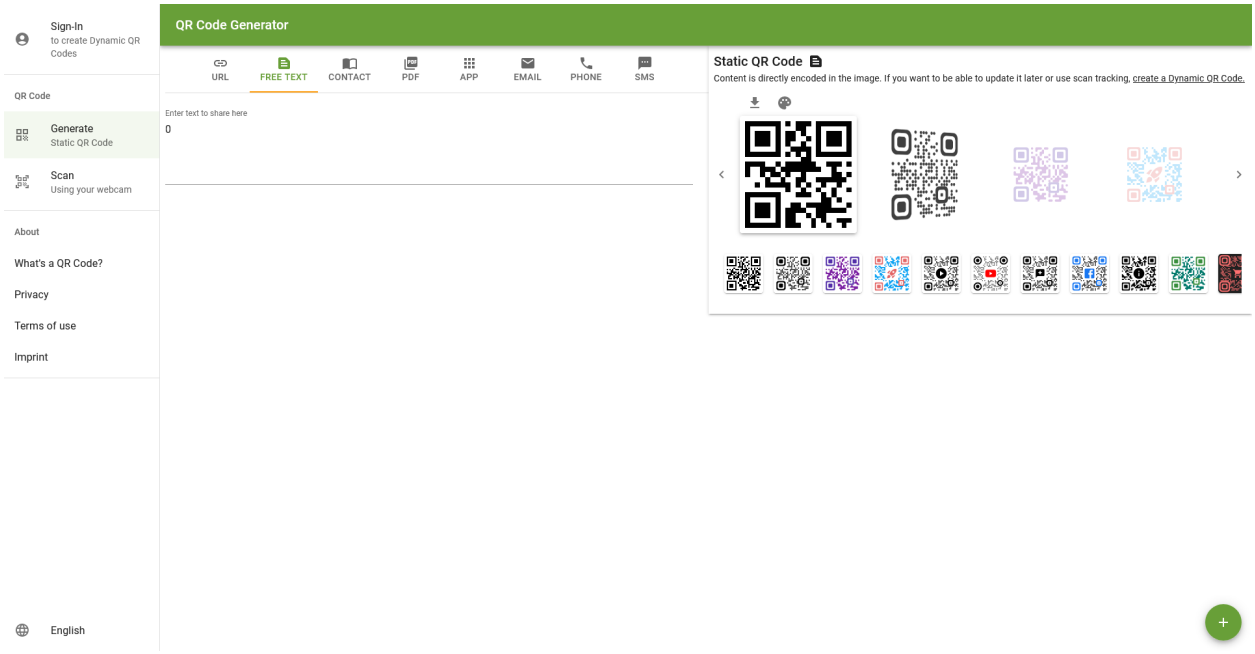
Scanbook

fortnite travis scott burger

Here's your ticket:

Post Challenge Edit

The HTTP request method was incorrect given that the amount of files present in the website were impossible to be searched given that there were two million entries. The correct way to find the flag would be to generate a QRCode with the value of 0 using outside tools such that you can use it to find the first element entered into the website.



Scanbook

buckeye{4n_1d_numb3r_15_N07_4_p455w0rd}

Images taken from https://f0rtis1.github.io/posts/scanbook/ due to the fact that this write-up was done after the websites were down.