Rafael Angelo Christianto

Firewall for Portfolio Website

Introduction

I will be adding Firewall for my portfolio website, since it is a good website I can perform experiments on for projects like these. However, one thing to consider is that my portfolio website is a static website means it:

- No backend code
- No database
- No server-side logic

Even though static websites eliminate entire classes of server-side vulnerabilities, they remain exposed to network-level and client-side threats. This project focuses on securing a static web application using edge-based security controls. So attacks like SQL injection, RCE, auth bypass are basically impossible. The real risks are:

- DDoS / traffic abuse
- Bot scraping
- XSS via user input (if you use forms or client-side rendering)
- Asset abuse (hotlinking, bandwidth drain)

Threat Model

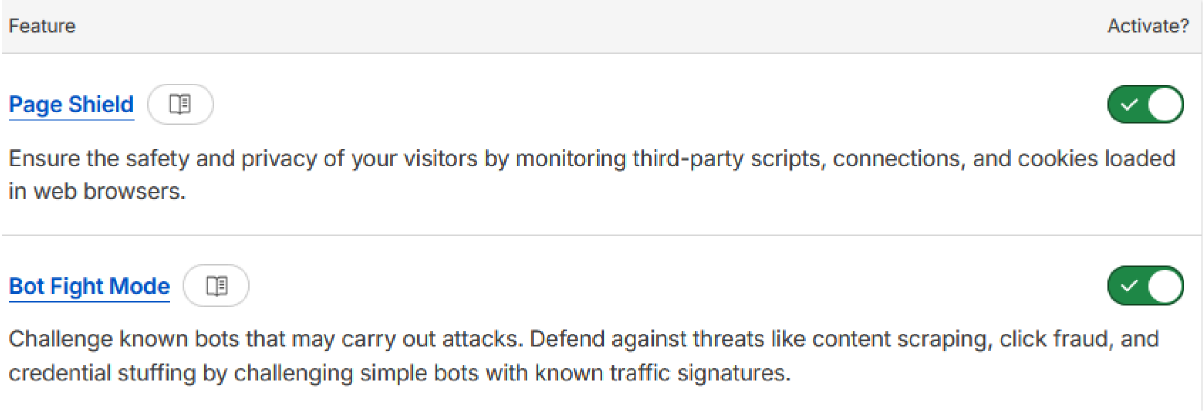
Area	Risk
Network	DDoS, Layer 7 floods
Client-side	XSS (DOM-based), malicious JS injection
Assets	Hotlinking, bandwidth abuse
Crawlers	Bot scraping, automated scanners

Methodology

I bought the domain from Hostinger and hosted it with Cloudflare to connect the domain to my GitHub repository. This provides a cost efficient approach and good for security practices as well.

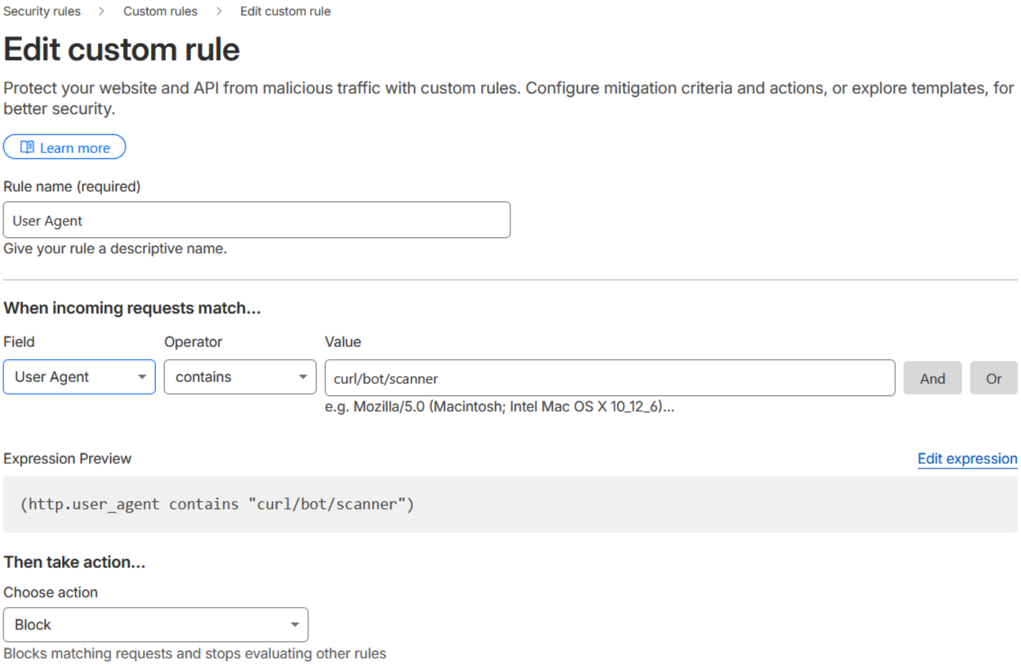
Procedures

Overview



Feature	Activate?
Page Shield Ensure the safety and privacy of your visitors by monitoring third-party scripts, connections, and cookies loaded in web browsers.	✓
Bot Fight Mode Challenge known bots that may carry out attacks. Defend against threats like content scraping, click fraud, and credential stuffing by challenging simple bots with known traffic signatures.	✓

In the custom security rules tab, I set that the User Agent whose containing curl or bot or scanner will be blocked to avoid content scraping without proper user agents.



Security rules > Custom rules > Edit custom rule

Edit custom rule

Protect your website and API from malicious traffic with custom rules. Configure mitigation criteria and actions, or explore templates, for better security.

Rule name (required)

User Agent

Give your rule a descriptive name.

When incoming requests match...

Field	Operator	Value
User Agent	contains	curl/bot/scanner

e.g. Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6)...

Expression Preview

```
(http.user_agent contains "curl/bot/scanner")
```

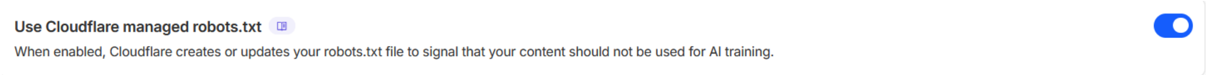
Then take action...

Choose action

Block

Blocks matching requests and stops evaluating other rules

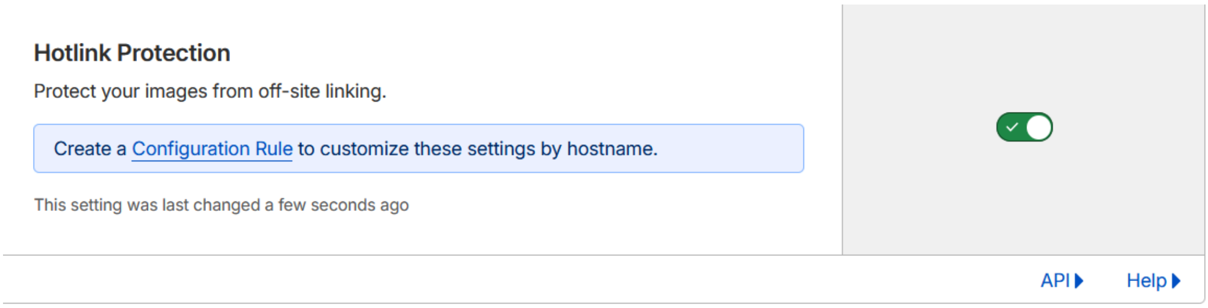
AI Crawl Control makes sure in the robots.txt that the content is the web application will not be crawled by AI and used for AI training.



Use Cloudflare managed robots.txt

When enabled, Cloudflare creates or updates your robots.txt file to signal that your content should not be used for AI training.

Scrape Shield protects the images used in my website so that my bandwidth and resources of my websites will not be consumed because of their usage. So, images will only load if the request comes from your domain



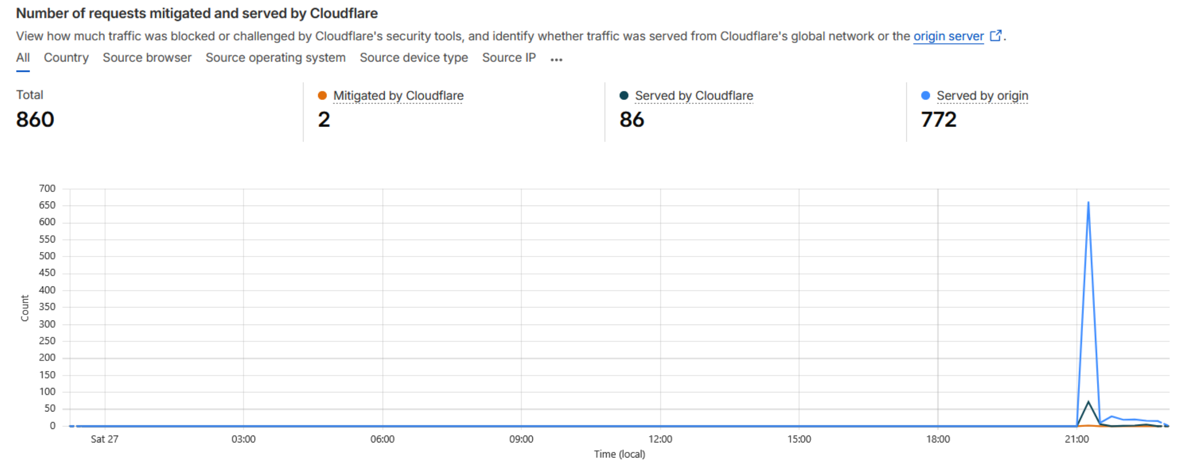
Hotlink Protection

Protect your images from off-site linking.

Create a Configuration Rule to customize these settings by hostname.

This setting was last changed a few seconds ago

Security Analytics indicates that it already mitigated 2 attempts to unknown and unfamiliar requests that it might see as bad.



Number of requests mitigated and served by Cloudflare

View how much traffic was blocked or challenged by Cloudflare's security tools, and identify whether traffic was served from Cloudflare's global network or the origin server.

Total	● Mitigated by Cloudflare	● Served by Cloudflare	● Served by origin
860	2	86	772

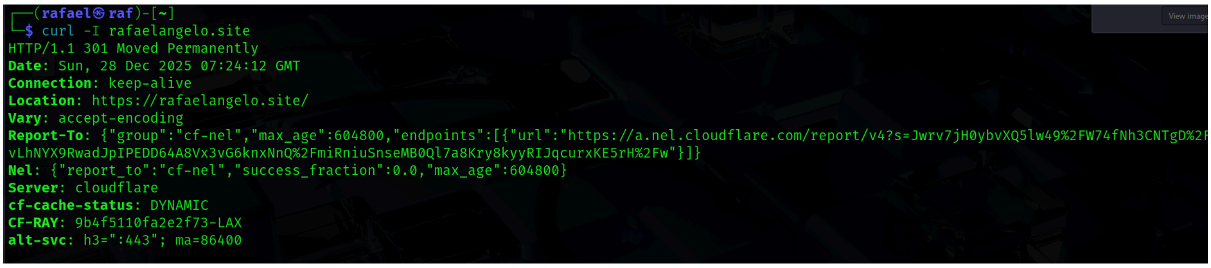
Discussion

Since I deployed the site on Cloudflare, it is already equipped for good security practices like DDoS attacks and others. But then, it lacks coverage for backend security like RCE, SQLi, but then my portfolio website is static and does not contain any forms, file uploads, and others.

Testing

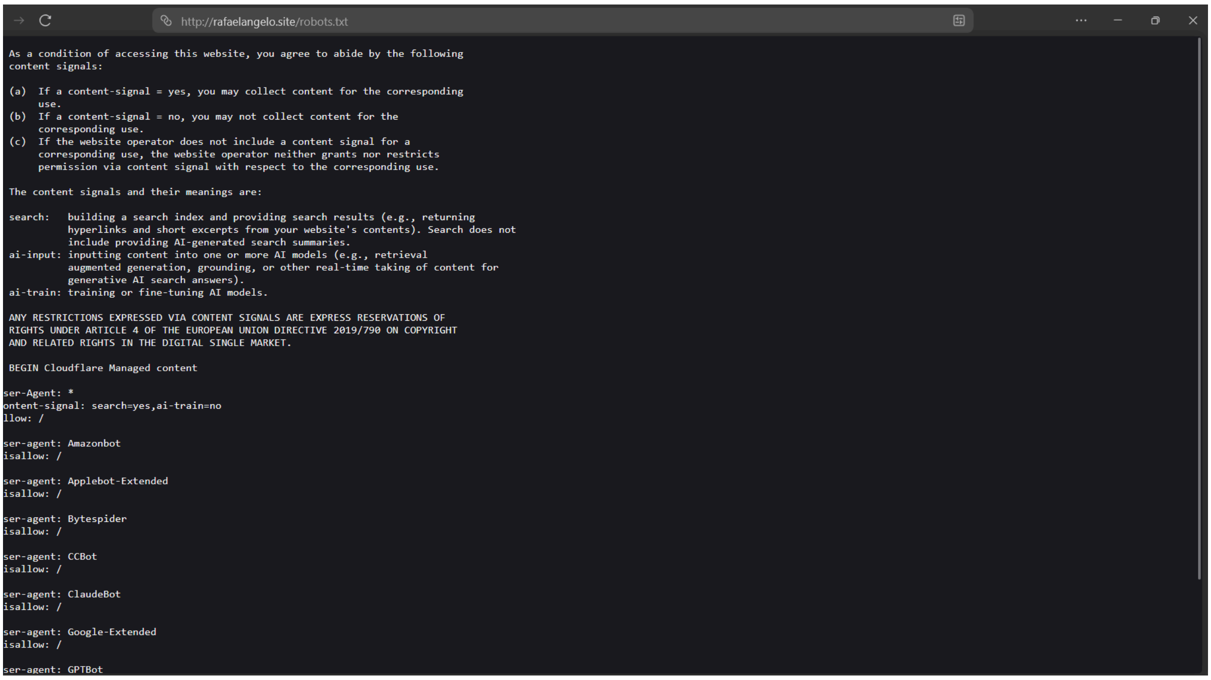
Testing focused on validating edge-based security controls rather than vulnerability exploitation, as the application is fully static. Firewall rules were tested by sending requests with suspicious User-Agent headers and confirming they were blocked. Automated scanning tools triggered Cloudflare security events, confirming bot detection. Hotlink protection was verified by attempting to load images from external origins, which failed as expected. Traffic analytics showed Cloudflare mitigating abnormal request patterns without impacting availability.

The following screenshot demonstrates an example to curl my portfolio website but blocked by Cloudflare known by the 301 status.



```
┌──(rafael㉿raf)-[~]
└─$ curl -I rafaelangelo.site
HTTP/1.1 301 Moved Permanently
Date: Sun, 28 Dec 2025 07:24:12 GMT
Connection: keep-alive
Location: https://rafaelangelo.site/
Vary: accept-encoding
Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=Jwrv7jH0ybvXQ5lw49%2FW74fNh3CNTgD%2F
vLhNYX9RwadJpIPEDD64A8Vx3vG6knxNnQ%2FmiRniuSnseMB0Ql7a8Kry8kyyRIJqcurxKE5rH%2Fw"}]}
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Server: cloudflare
cf-cache-status: DYNAMIC
CF-RAY: 9b4f5110fa2e2f73-LAX
alt-svc: h3=":443"; ma=86400
```

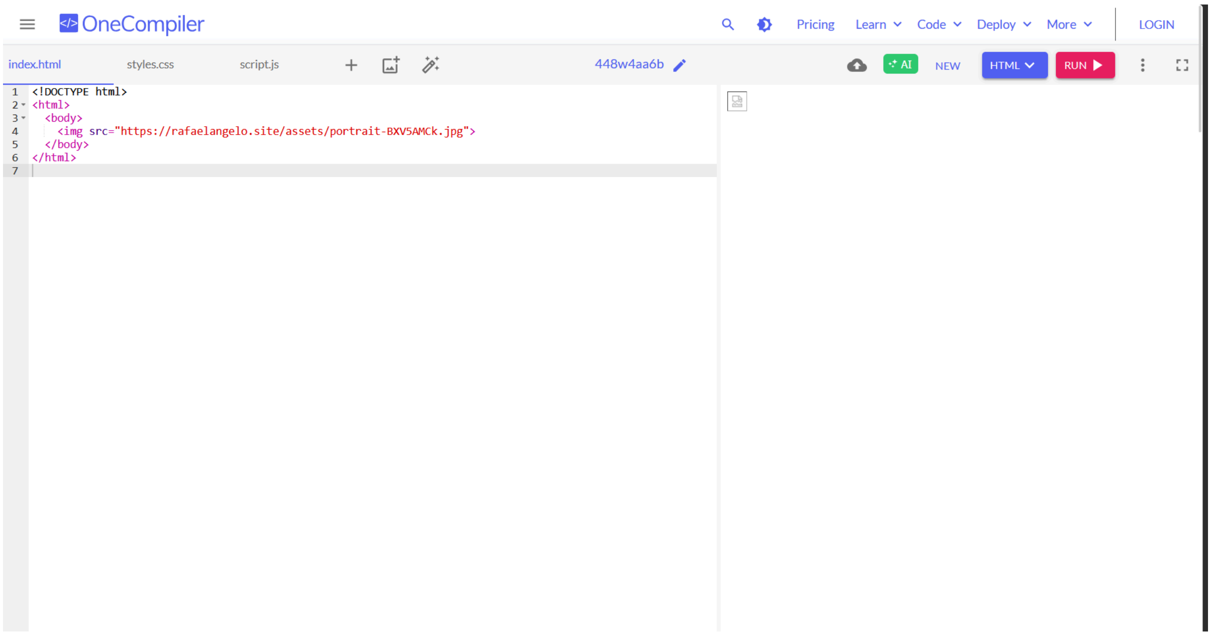
If we go from the normal browser search bar and type in robots.txt for my website, it will return the unallowed AI to crawl my site.



```
As a condition of accessing this website, you agree to abide by the following
content signals:

(a)  If a content-signal = yes, you may collect content for the corresponding
     use.
(b)  If a content-signal = no, you may not collect content for the
     corresponding use.
(c)  If the website operator does not include a content signal for a
     corresponding use, the website operator neither grants nor restricts
     permission via content signal with respect to the corresponding use.

The content signals and their meanings are:

search:   building a search index and providing search results (e.g., returning
          hyperlinks and short excerpts from your website's contents). Search does not
          include providing AI-generated search summaries.
ai-input: inputting content into one or more AI models (e.g., retrieval
          augmented generation, grounding, or other real-time taking of content for
          generative AI search answers).
ai-train: training or fine-tuning AI models.

ANY RESTRICTIONS EXPRESSED VIA CONTENT SIGNALS ARE EXPRESS RESERVATIONS OF
RIGHTS UNDER ARTICLE 4 OF THE EUROPEAN UNION DIRECTIVE 2019/790 ON COPYRIGHT
AND RELATED RIGHTS IN THE DIGITAL SINGLE MARKET.

BEGIN Cloudflare Managed content

ser-Agent: *
ontent-signal: search=yes,ai-train=no
llow: /

ser-agent: Amazonbot
isallow: /

ser-agent: Applebot-Extended
isallow: /

ser-agent: Bytespider
isallow: /

ser-agent: CCBot
isallow: /

ser-agent: ClaudeBot
isallow: /

ser-agent: Google-Extended
isallow: /

ser-agent: GPTBot
```

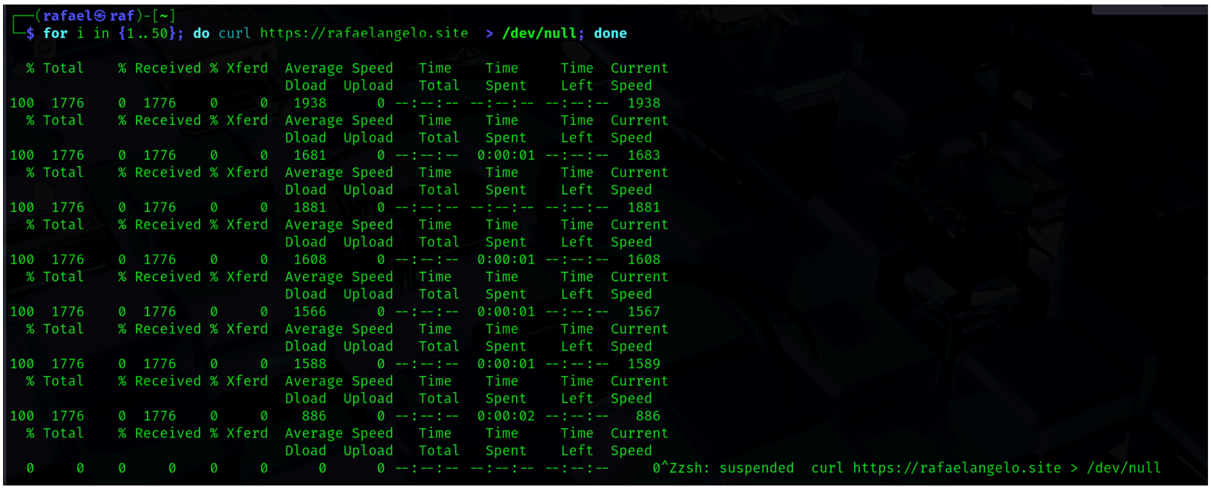
Rafael Angelo Christianto

The following screenshot below shows us in an HTML compiler with simple compiler code, shows that the image in my portfolio website cannot be used in a link like shown in the image.



```html
<!DOCTYPE html>
<html>
  <body>
    <img src="https://rafaelangelo.site/assets/portrait-BXV5AMCk.jpg">
  </body>
</html>
```

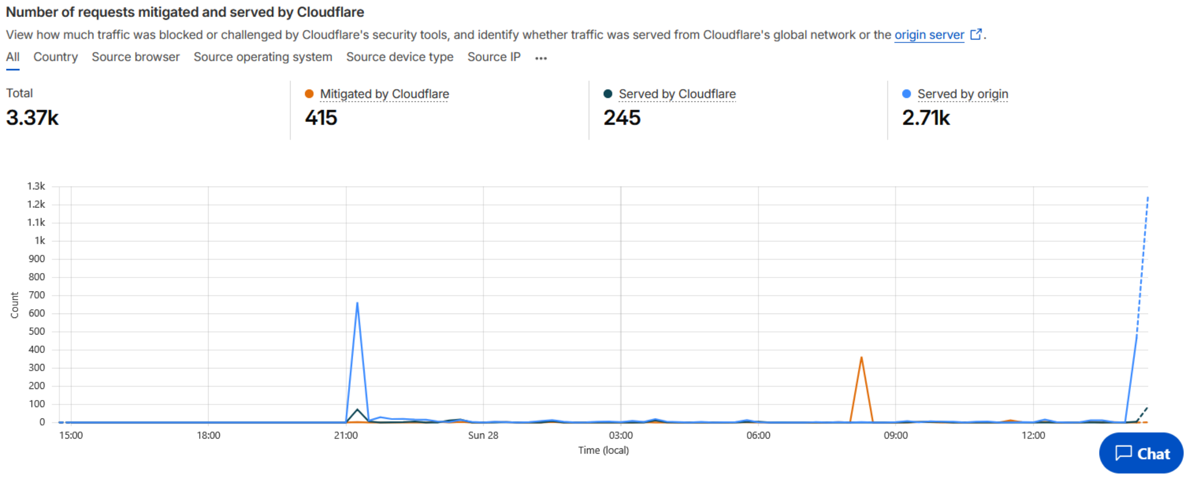
The screenshot below demonstrates a DDoS attack on my portfolio website, but I will not actually flood it until it goes down. But from the picture below, it is observable that the current speed decreases as more requests get on.



```
┌──(rafael㉿raf)-[~]
└─$ for i in {1..50}; do curl https://rafaelangelo.site  > /dev/null; done

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1776    0  1776    0     0   1938      0 --:--:-- --:--:-- --:--:--  1938
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1776    0  1776    0     0   1681      0 --:--:--  0:00:01 --:--:--  1683
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1776    0  1776    0     0   1881      0 --:--:-- --:--:-- --:--:--  1881
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1776    0  1776    0     0   1608      0 --:--:--  0:00:01 --:--:--  1608
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1776    0  1776    0     0   1566      0 --:--:--  0:00:01 --:--:--  1567
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1776    0  1776    0     0   1588      0 --:--:--  0:00:01 --:--:--  1589
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1776    0  1776    0     0    886      0 --:--:--  0:00:02 --:--:--   886
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0^Zzsh: suspended  curl https://rafaelangelo.site > /dev/null
```

Rafael Angelo Christianto

From the DDoS attack previously we can see there are a lot of requests mitigated by Cloudflare, and perhaps some or most of the requests are coming from the DDoS attack we performed previously



Number of requests mitigated and served by Cloudflare

View how much traffic was blocked or challenged by Cloudflare's security tools, and identify whether traffic was served from Cloudflare's global network or the origin server.

Total	● Mitigated by Cloudflare	● Served by Cloudflare	● Served by origin
3.37k	415	245	2.71k