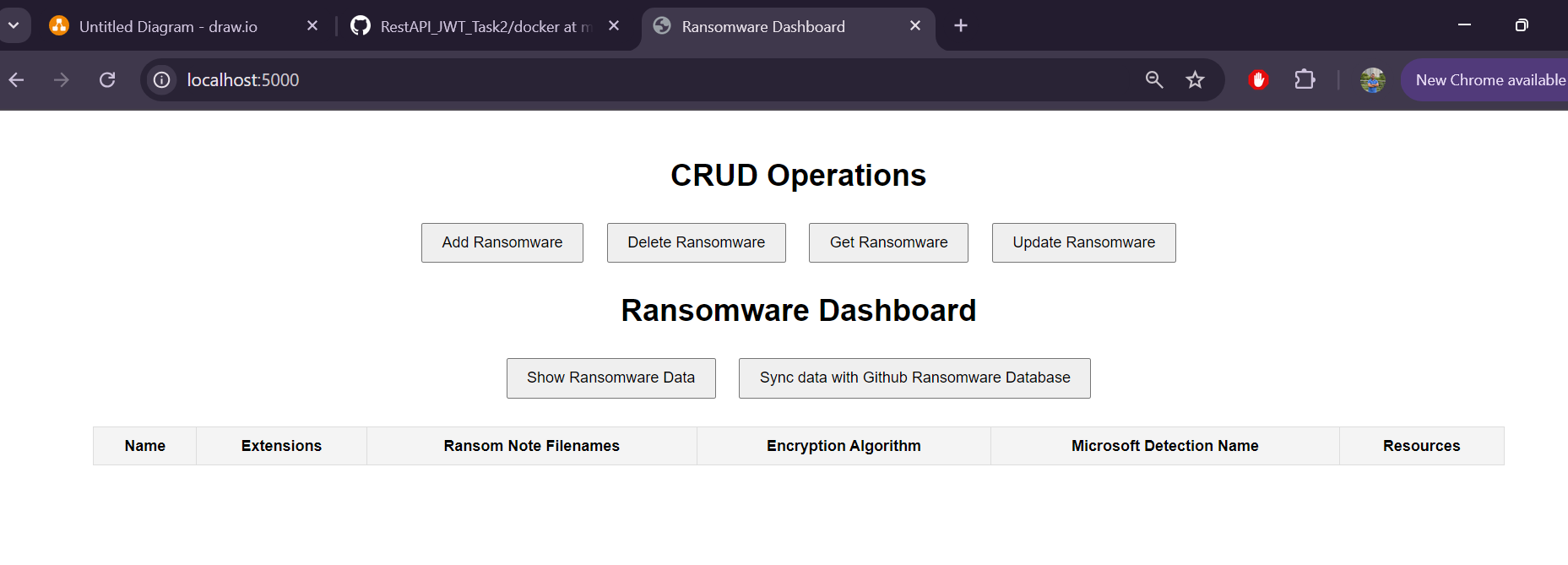
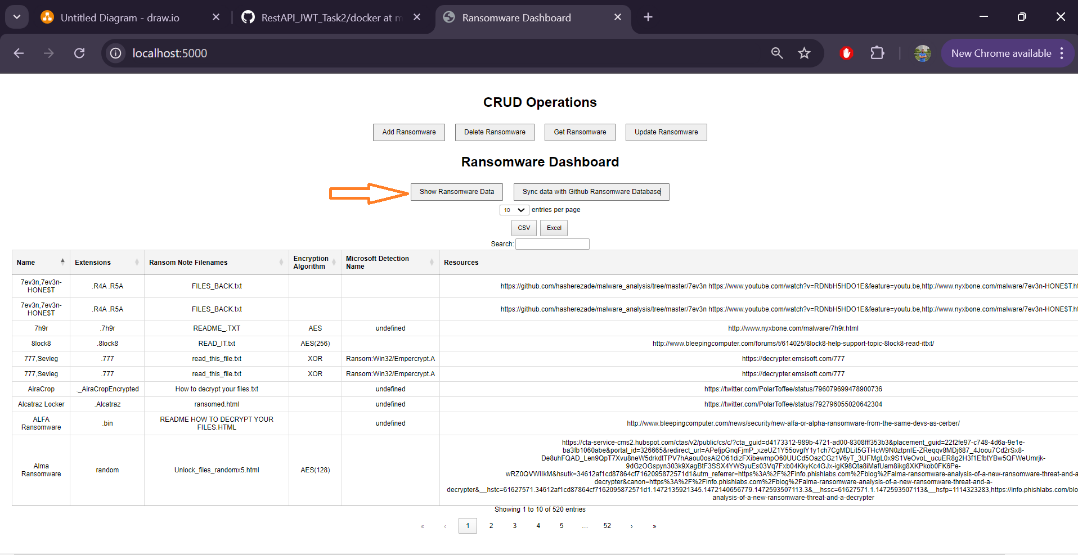
# Loading the Ransomware Data

1. Visit http://localhost:5000/

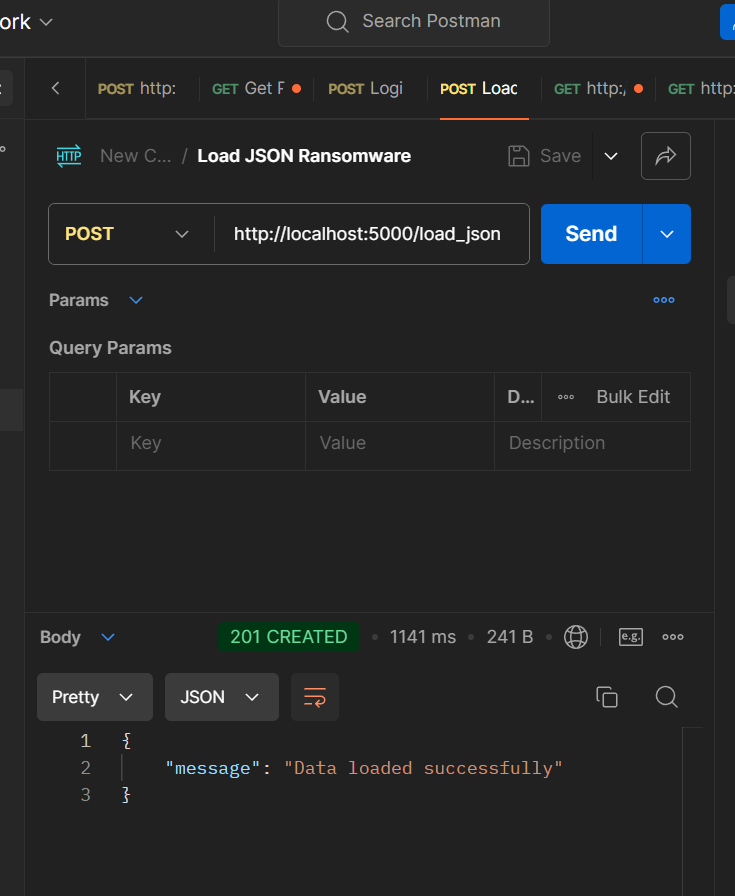


1. Click on Show Ransomware Data



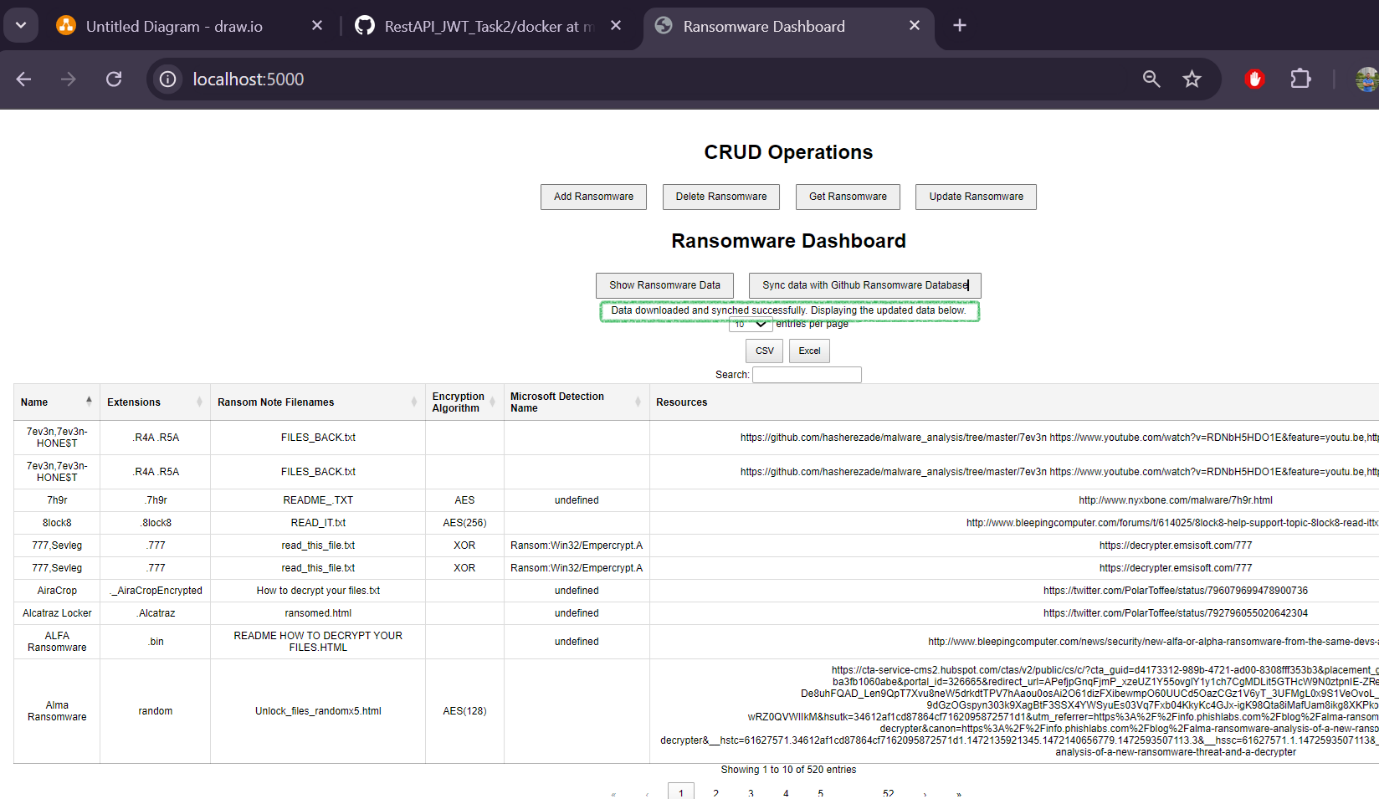
1. If you want to run api to load Data

|  |
| --- |
| curl --location --request POST 'http://localhost:5000/load\_json' \  --header 'Content-Type: application/json' |



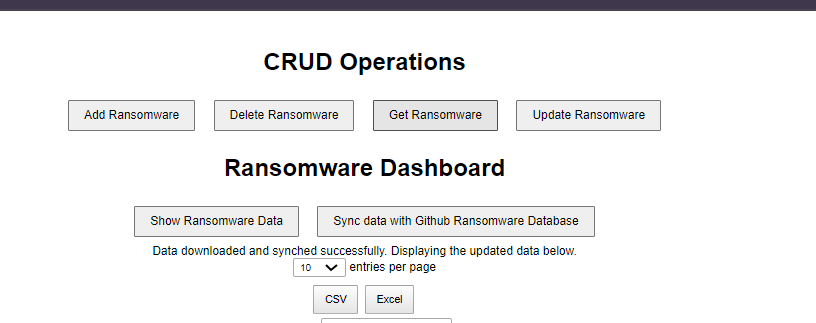
# Sync Ransomware Data with GitHub

Note : This will download the ransomware json file from [GitHub](https://github.com/codingo/Ransomware-Json-Dataset/blob/master/ransomware_overview.json) and sync it with existing data and then will show up in the dashboard with successful message.



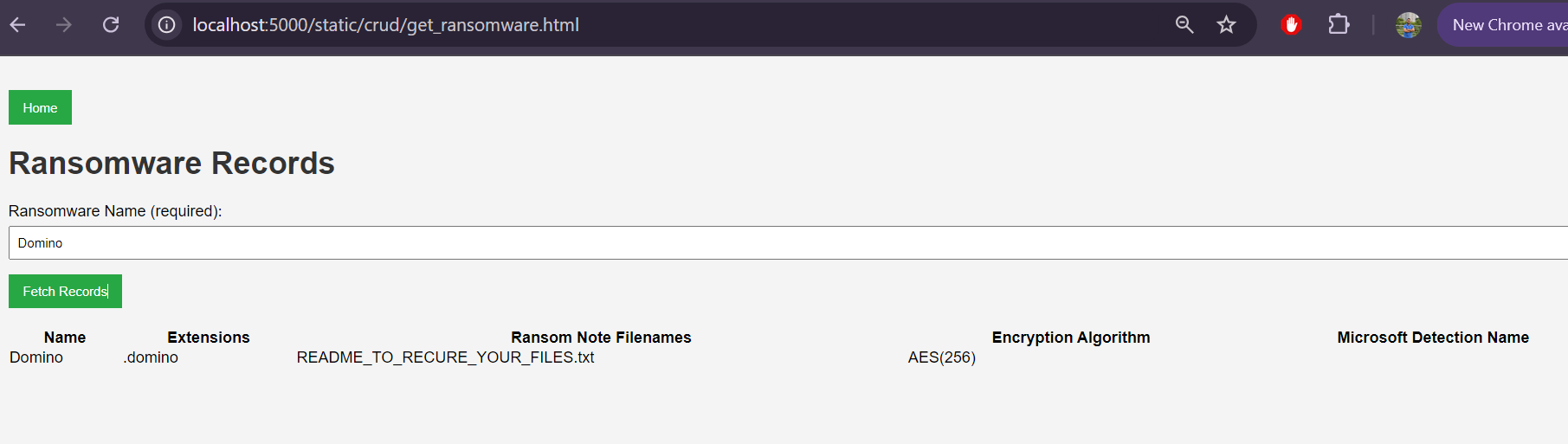
# Basic CRUD Operation on Ransomware Data

1. View Ransomware – Click Get Ransomware

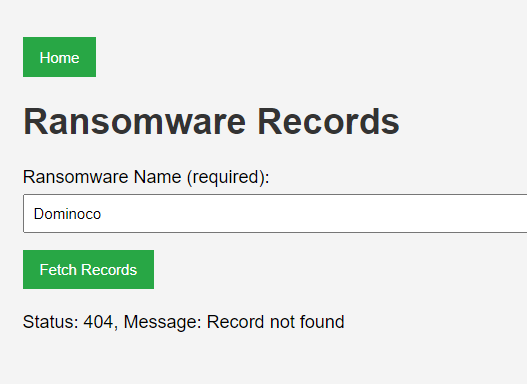


Search :

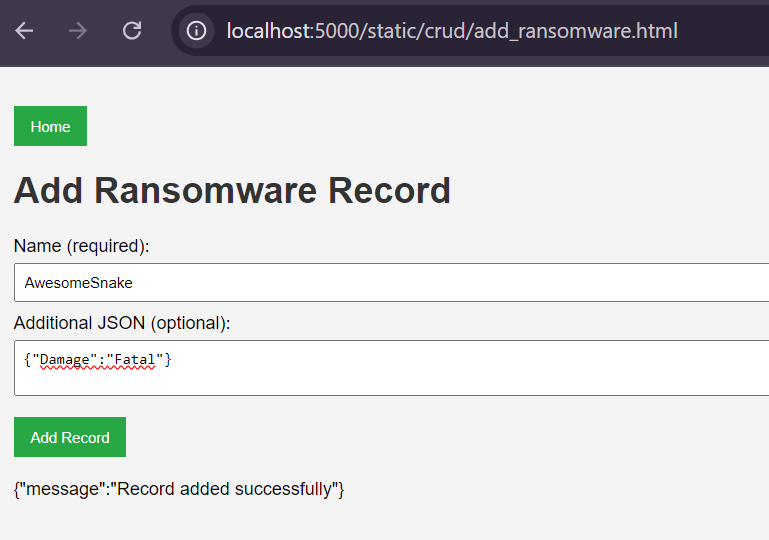
If Exist it shows minimal data



Else Give appropriate error

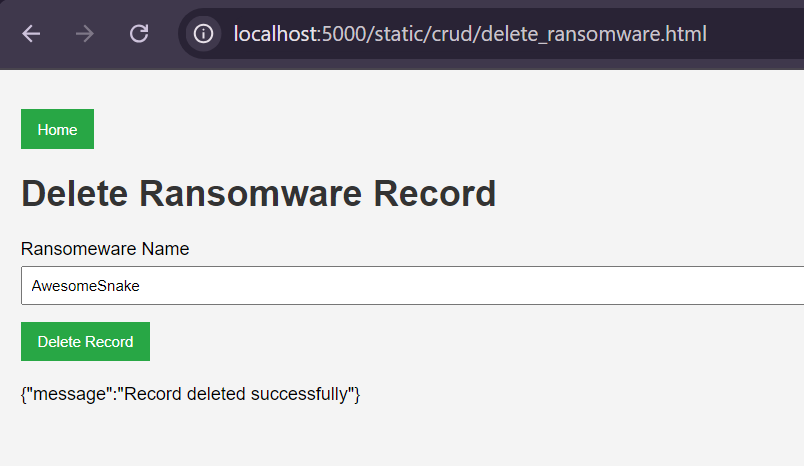


1. Create A ransomware Record (Similarly you can update the existing record in Update Record section)

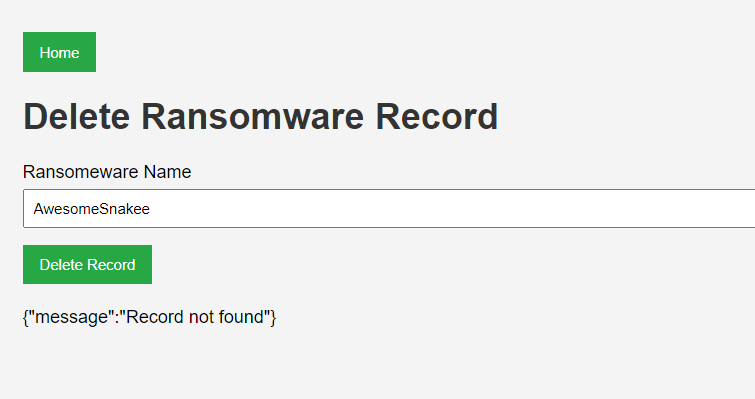


1. Delete Ransomware record

If exist it deletes



Else return appropriate response



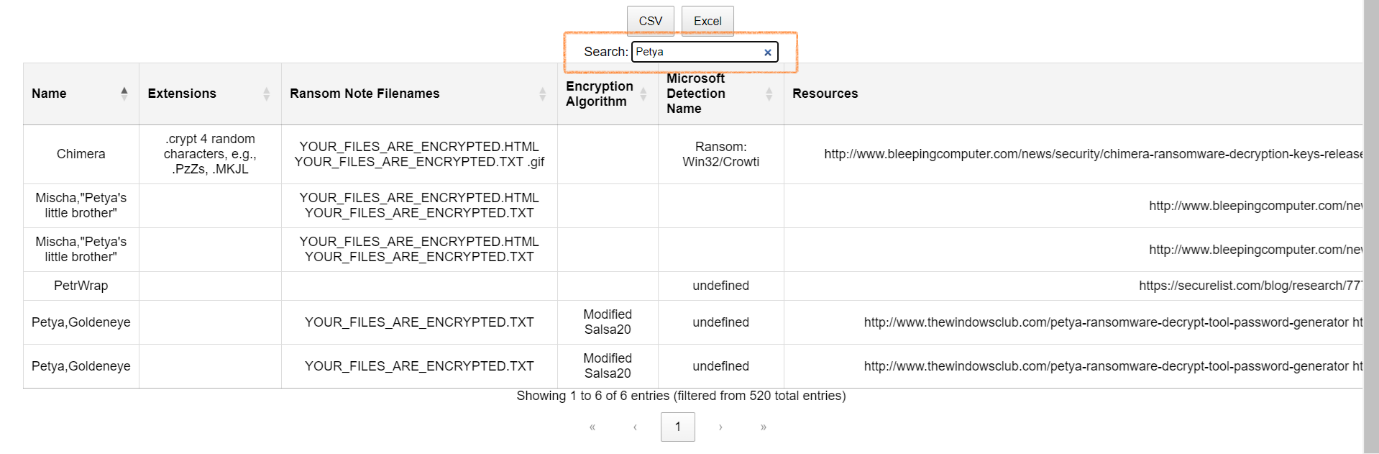
# Working with dashboard

Dashboard gives lot of good feature , you can search , sort and download record in csv or excel

You can also expand the pages for easy navigation. It is simple yet powerful to look into the data.

Note: The Table has been truncated to show most relevant information , we can include columns with bit tweaking in JavaScript

1. Search – Just put any test to search the table – it will search the whole table and show columns matching with data



1. Download CSV or Excel

