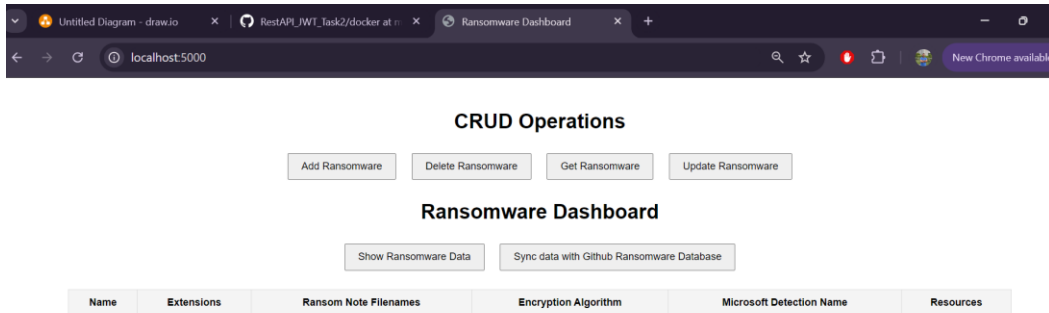
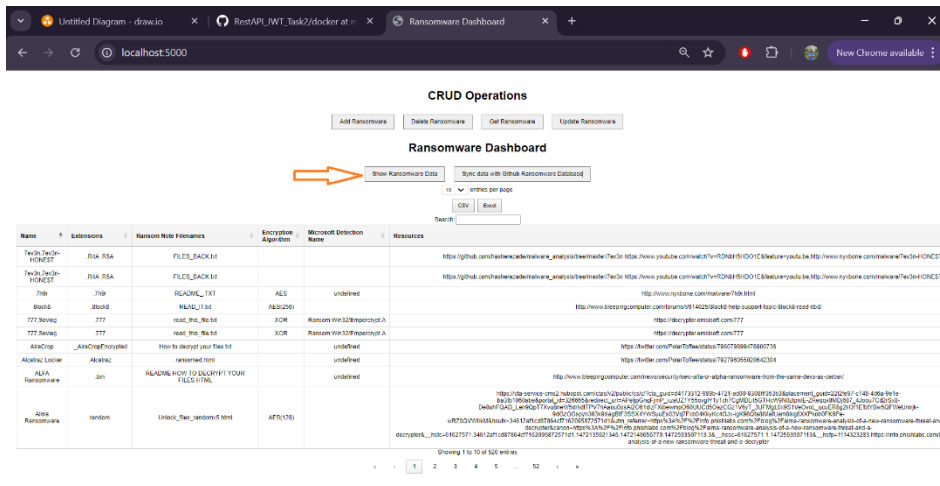


1. Loading the Ransomware Data

1. Visit <http://localhost:5000/>

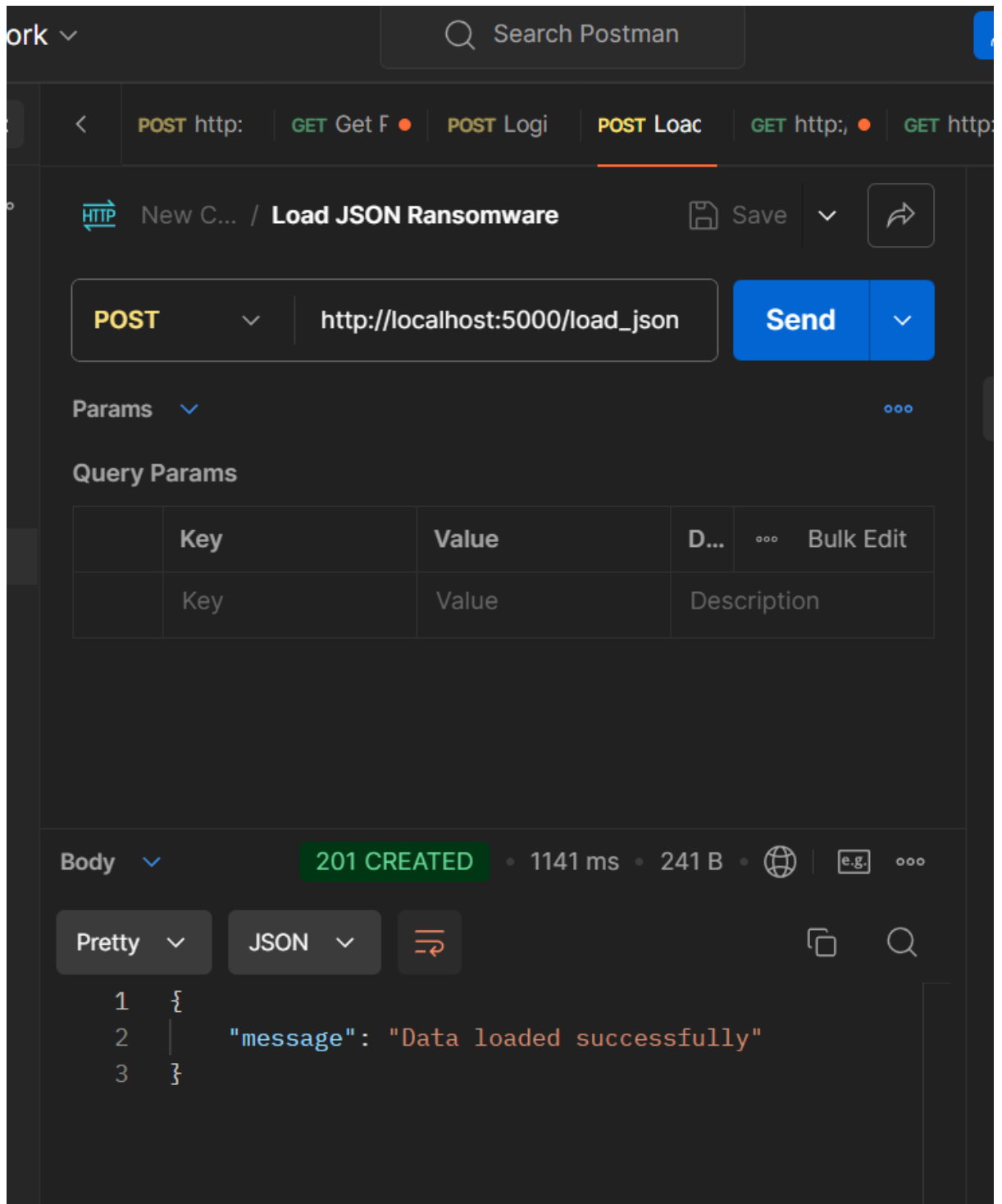


2. Click on Show Ransomware Data



3. If you want to run api to load Data

```
curl --location --request POST 'http://localhost:5000/load_json' \
--header 'Content-Type: application/json'
```



2. Sync Ransomware Data with GitHub

Note : This will download the ransomware json file from [GitHub](#) and sync it with existing data and then will show up in the dashboard with successful message.

Untitled Diagram - draw.io | RestAPI_JWT_Task2/docker at n | Ransomware Dashboard

localhost:5000

CRUD Operations

Add Ransomware Delete Ransomware Get Ransomware Update Ransomware

Ransomware Dashboard

Show Ransomware Data Sync data with Github Ransomware Database

Data downloaded and synched successfully. Displaying the updated data below.

10 entries per page

CSV Excel

Search:

Name	Extensions	Ransom Note Filenames	Encryption Algorithm	Microsoft Detection Name	Resources
7ev3n.7ev3n-HONEST	.R4A, R5A	FILES_BACK.txt			https://github.com/hasherezade/malware_analysis/tree/master/7ev3n https://www.youtube.com/watch?v=RDNBH5HDO1E&feature=youtu.be
7ev3n.7ev3n-HONEST	.R4A, R5A	FILES_BACK.txt			https://github.com/hasherezade/malware_analysis/tree/master/7ev3n https://www.youtube.com/watch?v=RDNBH5HDO1E&feature=youtu.be
7h9r	7h9r	README_.TXT	AES	undefined	http://www.nyxbone.com/malware/7h9r.html
Block8	.Block8	README_.TXT	AES(256)		http://www.bleepingcomputer.com/forums/t/614025/block8-help-support-topic-block8-read-it
777_Sevileg	.777	read_this_file.txt	XOR	Ransom:Win32/Empercrypt.A	https://decrypter.emissoft.com/777
777_Sevileg	.777	read_this_file.txt	XOR	Ransom:Win32/Empercrypt.A	https://decrypter.emissoft.com/777
AiraCrop	_AiraCropEncrypted	How to decrypt your files.txt		undefined	https://twitter.com/PolarTofee/status/796079699478900736
Alcatraz Locker	Alcatraz	ransomed.html		undefined	https://twitter.com/PolarTofee/status/792796055020642304
ALFA Ransomware	.bin	README HOW TO DECRYPT YOUR FILES HTML		undefined	http://www.bleepingcomputer.com/news/security/new-alfa-or-alpha-ransomware-from-the-same-devs-
Alma Ransomware	random	Unlock_files_random.5.html	AES(128)		https://cse-service-cms2.hubspot.com/class/v2/public/csc/c7cta_guid=d4173312-969e-4721-a000-6308f353b3placement_qba3b1006abe&portal_id=326665&redirec_url=ApaPq3naFmF_2a6U21Y55owg1Ty1ch7CgMOLB5GT4Ch19H02zpmE-2R4DeBuhFQAD_Len9OpT7Xu8neV5SndtTPV7hAau0osAZO61didFKbeWmpO6OUUC65OazCQzV8yT_3UfMgLn9S1VeOvL9dQzOGssyn303k9kagBF3SSX4yV5yue503Vq7Frb04KlyKc4GJn-9k96Qab9MaflJam8kg8KKPfo wRZ00VWlIM8shub=34612af1c087864cf7162095872571d1.1472135921345.1472140658779.1472593507113.38__hsc=61627571.1.14725935071138, decrypter&canon=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-ranso analysis-of-a-new-ransomware-threat-and-a-decrypter

Showing 1 to 10 of 520 entries

3. Basic CRUD Operation on Ransomware Data

1. View Ransomware – Click Get Ransomware

CRUD Operations

Add Ransomware Delete Ransomware Get Ransomware Update Ransomware

Ransomware Dashboard

Show Ransomware Data Sync data with Github Ransomware Database

Data downloaded and synched successfully. Displaying the updated data below.

10 entries per page

CSV Excel

Search :

If Exist it shows minimal data

localhost:5000/static/crud/get_ransomware.html

Home

Ransomware Records

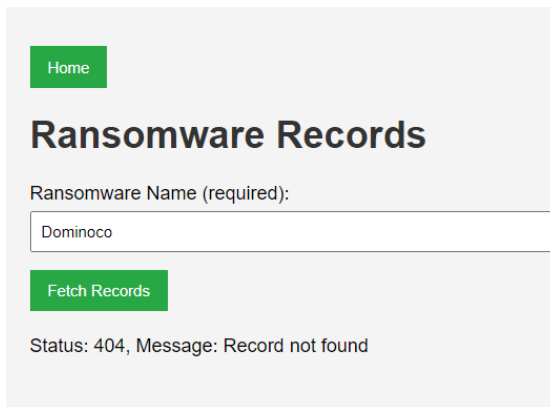
Ransomware Name (required):

Domino

Fetch Records

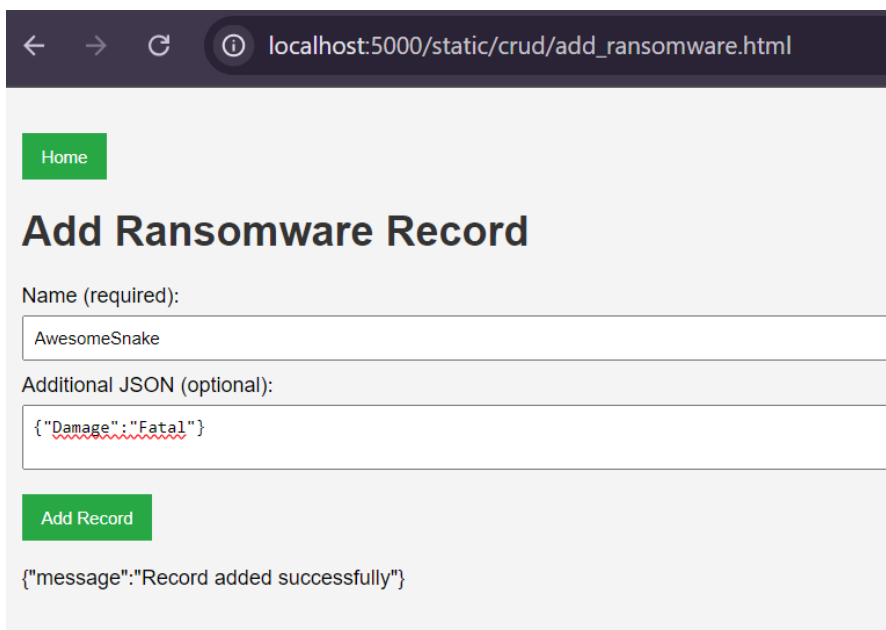
Name	Extensions	Ransom Note Filenames	Encryption Algorithm	Microsoft Detection Name
Domino	.domino	README_TO_RECURE_YOUR_FILES.txt	AES(256)	

Else Give appropriate error



The screenshot shows a web application interface with a green 'Home' button at the top left. Below it is the title 'Ransomware Records'. A form labeled 'Ransomware Name (required):' contains the text 'Dominoco'. A green 'Fetch Records' button is positioned below the form. At the bottom, a status message reads 'Status: 404, Message: Record not found'.

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



The screenshot shows a web browser window with the address bar displaying 'localhost:5000/static/crud/add_ransomware.html'. The page has a green 'Home' button and the title 'Add Ransomware Record'. A form labeled 'Name (required):' contains the text 'AwesomeSnake'. Below it, a form labeled 'Additional JSON (optional):' contains the JSON string '{ "Damage": "Fatal" }'. A green 'Add Record' button is at the bottom. A status message at the bottom reads '{ "message": "Record added successfully" }'.

3. Delete Ransomware record

If exist it deletes

A screenshot of a web browser window with the address bar showing `localhost:5000/static/crud/delete_ransomware.html`. The page has a green 'Home' button in the top left. The main heading is 'Delete Ransomware Record'. Below it is a label 'Ransomware Name' followed by a text input field containing 'AwesomeSnake'. A green 'Delete Record' button is positioned below the input field. At the bottom of the form, a JSON response is displayed: `{"message": "Record deleted successfully"}`.

Else return appropriate response

A screenshot of a web browser window with the address bar showing `localhost:5000/static/crud/delete_ransomware.html`. The page has a green 'Home' button in the top left. The main heading is 'Delete Ransomware Record'. Below it is a label 'Ransomware Name' followed by a text input field containing 'AwesomeSnake'. A green 'Delete Record' button is positioned below the input field. At the bottom of the form, a JSON response is displayed: `{"message": "Record not found"}`.

4. 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

<div> <div>CSV</div> <div>Excel</div> <div>Search: Petya</div> </div>					
Name	Extensions	Ransom Note Filenames	Encryption Algorithm	Microsoft Detection Name	Resources
Chimera	.crypt 4 random characters, e.g., .PzZs, .MKJL	YOUR_FILES_ARE_ENCRYPTED.HTML YOUR_FILES_ARE_ENCRYPTED.TXT .gif		Ransom: Win32/Crowti	http://www.bleepingcomputer.com/news/security/chimera-ransomware-decryption-keys-release
Mischa,"Petya's little brother"		YOUR_FILES_ARE_ENCRYPTED.HTML YOUR_FILES_ARE_ENCRYPTED.TXT			http://www.bleepingcomputer.com/ne
Mischa,"Petya's little brother"		YOUR_FILES_ARE_ENCRYPTED.HTML YOUR_FILES_ARE_ENCRYPTED.TXT			http://www.bleepingcomputer.com/ne
PetrWrap				undefined	https://securelist.com/blog/research/77
Petya,Goldeneye		YOUR_FILES_ARE_ENCRYPTED.TXT	Modified Salsa20	undefined	http://www.thewindowsclub.com/petya-ransomware-decrypt-tool-password-generator ht
Petya,Goldeneye		YOUR_FILES_ARE_ENCRYPTED.TXT	Modified Salsa20	undefined	http://www.thewindowsclub.com/petya-ransomware-decrypt-tool-password-generator ht

Showing 1 to 6 of 6 entries (filtered from 520 total entries)

2. Download CSV or Excel

CRUD Operations

Ransomware Dashboard

100 entries per page

Search:

Name	Extensions	Ransom Note Filenames
7ev3n.7ev3n-HONE\$T	.R4A .R5A	FILES_BACK.txt
7ev3n.7ev3n-HONE\$T	.R4A .R5A	FILES_BACK.txt
7h9r	.7h9r	README_.TXT
Block8	.Block8	READ_IT.txt
777,Sevleg	.777	read_this_file.txt
777,Sevleg	.777	read_this_file.txt
AiraCrop	..AiraCropEncrypted	How to decrypt your file
Alcatraz Locker	.Alcatraz	ransomed.html

Save As

File name: Ransomware Dashboard.csv

Save as type: Microsoft Excel Comma Separated Values File (*.csv)

Save Cancel

Ransomware Dashboard.csv - Excel

FileHomeInsertPage LayoutFormulasDataReviewViewHelpTell me what you want to do

Get External Data

New Query

Recent Sources

Get & Transform

Refresh All

Connections

Properties

Edit Links

Connections

Refresh All

Queries & Connections

Properties

Workbook Links

Queries & Connections

Sort

Filter

Advanced

Sort & Filter

Text to Columns

Data Tools

D6

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	Extension: Ransom N Encryptor Microsoft Resources											
2	7ev3n,7ev3n-HONEŠT	.R4A .RSA	FILES_BACK.txt			https://github.com/hasherezade/malware_analysis/tree/master/7ev3n	https://wv						
3	7ev3n,7ev3n-HONEŠT	.R4A .RSA	FILES_BACK.txt			https://github.com/hasherezade/malware_analysis/tree/master/7ev3n	https://wv						
4	7h9r	.7h9r	README_AES	undefined	http://www.nyxbone.com/malware/7h9r.html								
5	8lock8	.8lock8	READ_IT.t AES(256)		http://www.bleepingcomputer.com/forums/t/614025/8lock8-help-support-topic-8								
6	777,Sevleg	0.777	read_this_XOR	Ransom:V	https://decrypter.emsisoft.com/777								
7	777,Sevleg	0.777	read_this_XOR	Ransom:V	https://decrypter.emsisoft.com/777								
8	AiraCrop	._AiraCrop	How to decrypt your	undefined	https://twitter.com/PolarToffee/status/796079699478900736								
9	Alcatraz Locker	.Alcatraz	ransomed.html	undefined	https://twitter.com/PolarToffee/status/792796055020642304								
10	ALFA Ransomware	.bin	README HOW TO D	undefined	http://www.bleepingcomputer.com/news/security/new-alfa-or-alpha-ransomwar								
11	Alma Ransomware	random	Unlock_fil AES(128)		https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-98								
12	Al-Namrood	.unavailab	Read_Me.Txt	undefined	https://decrypter.emsisoft.com/al-namrood								
13	Al-Namrood	.unavailab	Read_Me.Txt	undefined	https://decrypter.emsisoft.com/al-namrood								
14	Alphabet			undefined	https://twitter.com/PolarToffee/status/812331918633172992								
15	Alpha Ransomware,AlphaLoi.encrypt		Read Me (AES(256)	undefined	http://download.bleepingcomputer.com/demonslay335/AlphaDecrypter.zip,http:/								
16	Alpha Ransomware,AlphaLoi.encrypt		Read Me (AES(256)	undefined	http://download.bleepingcomputer.com/demonslay335/AlphaDecrypter.zip,http:/								
17	Alpha Ransomware,AlphaLoi.encrypt		Read Me (AES(256)	undefined	http://download.bleepingcomputer.com/demonslay335/AlphaDecrypter.zip,http:/								