

Encryption Recommendation for SMEs

User Manual

by

Kewin Skuza

Student ID: C00237361

Project Supervisor: Christopher Staff

Date: 25th April 2022

Contents

Disclaimers	2
Required Files	2
Installation	2
AWS Account	3
Application Use	5
Results	8

Disclaimers

- The application only supports json files exported from PhpMyAdmin at the moment
- The AWS services used are not free, they require a subscription
- It is a good idea to double check any fields that are not detected. Storing sensitive information and not encrypting it properly might lead to fines
- Proper encryption and hashing must be implemented if you want to secure your data. Some algorithms are not considered secure anymore. I would recommend:
 - o For encryption AES with 256-bit keys in CTR mode
 - o For hashing salted SHA-256 hashes

Required Files

The required files for this application to work include:

- Rec-encrypt.py
- AWS.py
- scripts.py
- green.png
- red.png
- requirements.txt

You also require Python 3.9 or higher, pip and an Amazon Web Services account.

The only file format supported is a json database export from PhpMyAdmin.

Installation

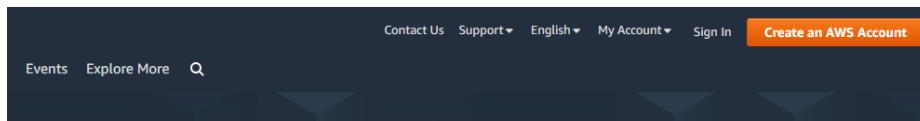
- This application only works on Windows operating systems
- Open command prompt in the folder where you have the application files
- Make sure that Python is installed on your device, and it is the correct version
 - o This can be done by issuing one of the following (depending on installation)
 - Python --version
 - Py --version
- Make sure that pip is installed on your device (Pip is used to download all dependencies for the application to work)
 - o You can check if pip is downloaded by issuing the following command:
 - Pip --version
- Now you can download dependencies by issuing the command:
 - o Pip install -r requirements.txt
- Now you can launch the application

AWS Account

Before you can start using the application you require to create an AWS account. Keep in mind that the services used are not free. They have a fee that you can view here:

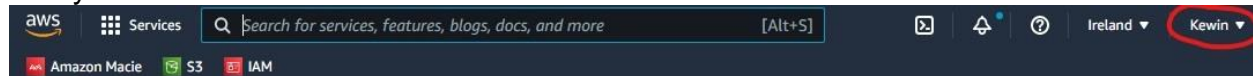
<https://aws.amazon.com/macie/pricing/>.

You can create the account on the AWS website: <https://aws.amazon.com/>.



Once your account is created and you sign in you can generate a key pair to use the application.

On the top right of your AWS console, you will be able to see a drop-down menu button with your username on it.



Once you press it a dropdown menu will appear. In this menu you are looking for an option called “Security Credentials”, press it.

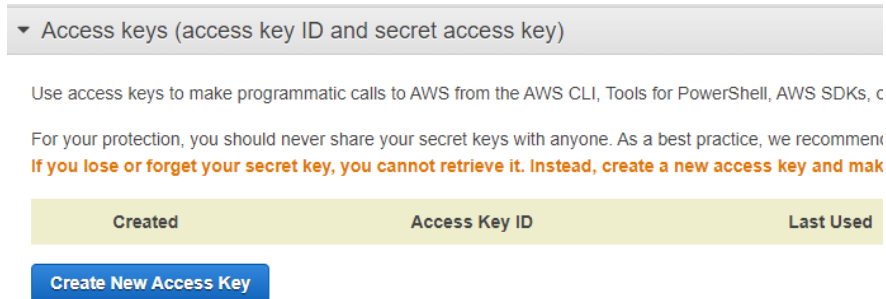


You will be redirected to a page with all your credentials, in this page we can generate our key pair.

Look for a button called "Access keys (access key ID and secret access key)". It should look something like this:



Once you press it you will be able to see a blue button called "Create New Access Key".



Once pressed you will be able to view your access keys. Keep in mind that once you view your keys, you will not be able to view the Secret Access Key again. Make sure to either memorize it or save it in a safe manner. It is also a good idea to delete the keys after use and regenerate them when you need to use them again. If someone gets ahold of those keys they will be able to freely interact with your AWS environment.

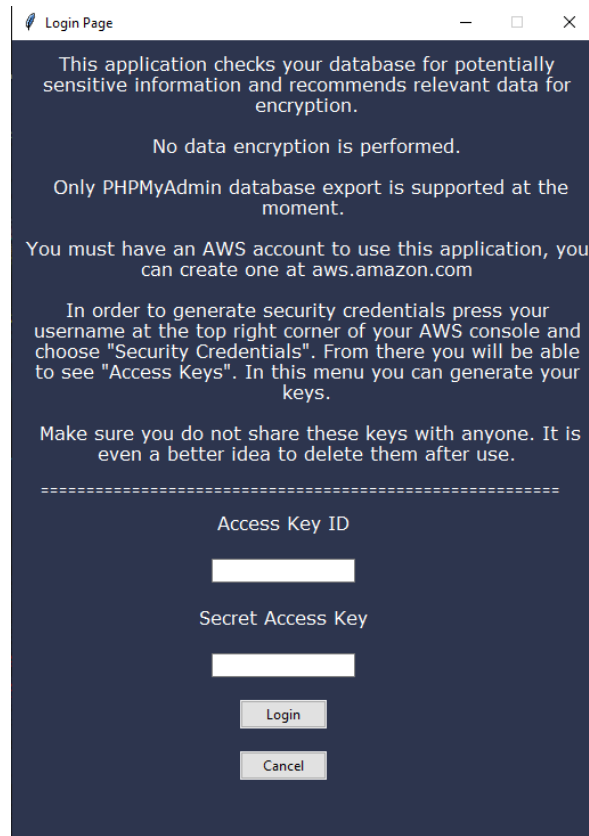
You can view your access keys by pressing "Show Access Key".

Now that you have a valid Access Key pair you can log into the application.



Application Use

Once you launch the application you will be greeted with a login screen. This login screen has some information about restrictions within the application and a guide on how to obtain your AWS Access Keys.



Once you log in you will be redirected to a home page, which gives you some basic information about the application.



The application screen has four different buttons to choose from. The “Home” button will take you back to the home screen.

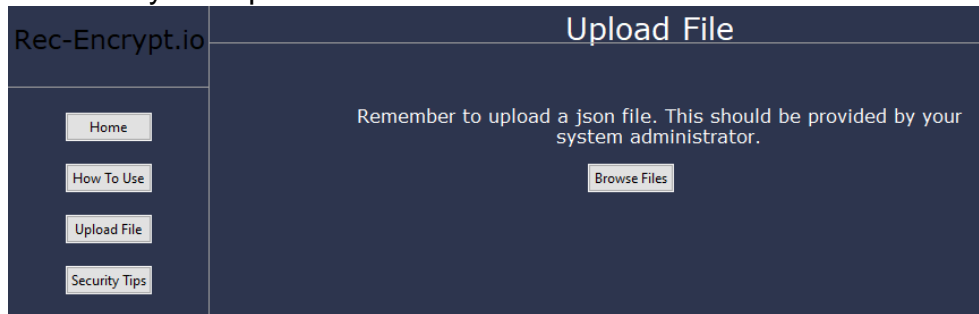
The “How To Use” button will take you to a page explaining how use the application.

The screenshot shows the 'How To Use' page of the Rec-Encrypt.io application. On the left is a dark sidebar with the application name 'Rec-Encrypt.io' at the top and four buttons: 'Home', 'How To Use', 'Upload File', and 'Security Tips'. The main content area has a dark background with white text. The title 'How To Use' is centered at the top. The text explains the process of logging in with AWS credentials, creating a user, and the steps for uploading a file to check for sensitive information. It details the file upload process, the processing time (up to 15 minutes), and the results, which are color-coded: green for non-sensitive fields and red for sensitive fields that have been encrypted.

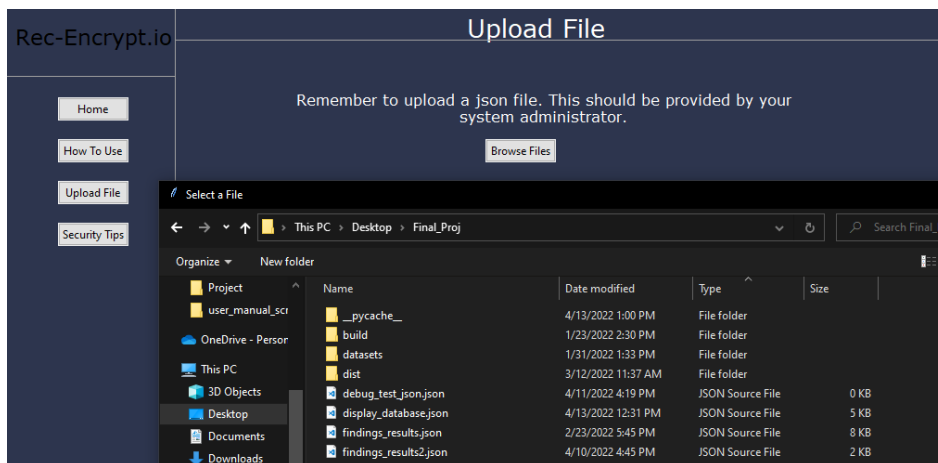
The “Security Tips” page will give you some pointers on how to encrypt your data and things to look out for.

The screenshot shows the 'Security Tips' page of the Rec-Encrypt.io application. The sidebar is identical to the previous page. The main content area has a dark background with white text. The title 'Security Tips' is centered at the top. The text provides several important considerations for data encryption, such as using secure algorithms (AES), key size, research, key security, and the importance of encrypting data both at rest and in transit. It also mentions that encryption is not ideal for password fields and that salted hashes are preferred. Finally, it notes that sensitive data in a database should be encrypted and that non-compliance with GDPR can lead to fines.

And lastly the “Upload File” button will take you to the page with the actual functionality of this application. The page itself has only one button named “Browse Files” and a reminder of the file you require.



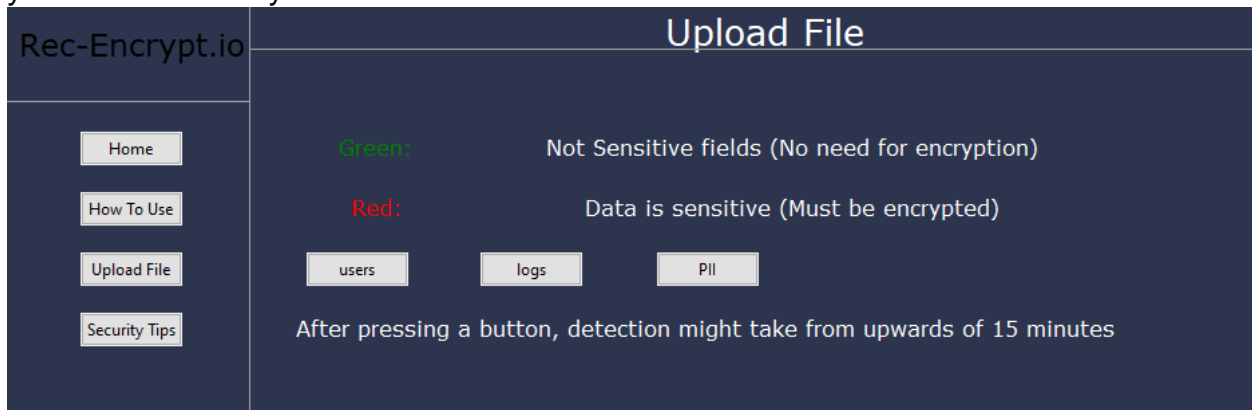
Once the “Browse Files” button is pressed you will be greeted with the familiar file explorer interface. You can traverse through your directory structure and choose the file that you want to check for sensitive information.



Remember that only files exported from PhpMyAdmin are supported at the moment.

Once you upload a file the results legend will be displayed and a button for every field in your database. Simply press any of the buttons to start processing.

Processing might take from upwards of 15 minutes depending on the amount of data you want to classify.



Results

Once the processing is finished the results will be displayed to screen in a table. Above the legend there will be a notification approximating the amount of time it would take to encrypt your data. Keep in mind that this application does not encrypt your data. It simply identifies which fields are sensitive and should be encrypted.

There are going to be multiple buttons allowing you to go between each table. The table with your results will have a colored strip above every field. This strip indicates if the data inside that field is sensitive or not.

Green coloring means that the field contains no sensitive information and does not need to be encrypted.

Red coloring on the other hand means that sensitive information is present, and the field should be encrypted. Remember that password fields should not be encrypted. They should be salted and hashed instead.

The screenshot shows the 'Rec-Encrypt.io' application interface. At the top, there is a title 'Upload File'. Below the title, a notification states: 'If you were to encrypt this data it would take approximately: 0.001997709274291992 seconds'. Below this, there is a legend with two entries: 'Green: Not Sensitive fields (No need for encryption)' and 'Red: Data is sensitive (Must be encrypted)'. There are three buttons labeled 'Users', 'logs', and 'PII'. The 'Users' button is highlighted with a dashed border. Below the legend, there is a table with four columns: 'id', 'Name', 'SSN', and 'Credit_Card_Number'. The first row has a green header, and the subsequent rows have red headers. The data in the table is as follows:

id	Name	SSN	Credit_Card_Number
1	Robert Aragon	489-36-8350	4929-3813-3266-4295
2	Ashley Borden	514-14-8905	5370-4638-8881-3020
3	Thomas Conley	690-05-5315	4916-4811-5814-8111
4	Susan Davis	421-37-1396	4916-4034-9269-8783
5	Christopher Diaz	458-02-6124	5299-1561-5689-1938
6	Rick Edwards	612-20-6832	5293-8502-0071-3058
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664
7	Victor Faulkner	300-62-3266	5548-0246-6336-5664

The results displayed above are not actual data. It is generated dummy data used for testing.