CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE, INDIA

SP PROJECT

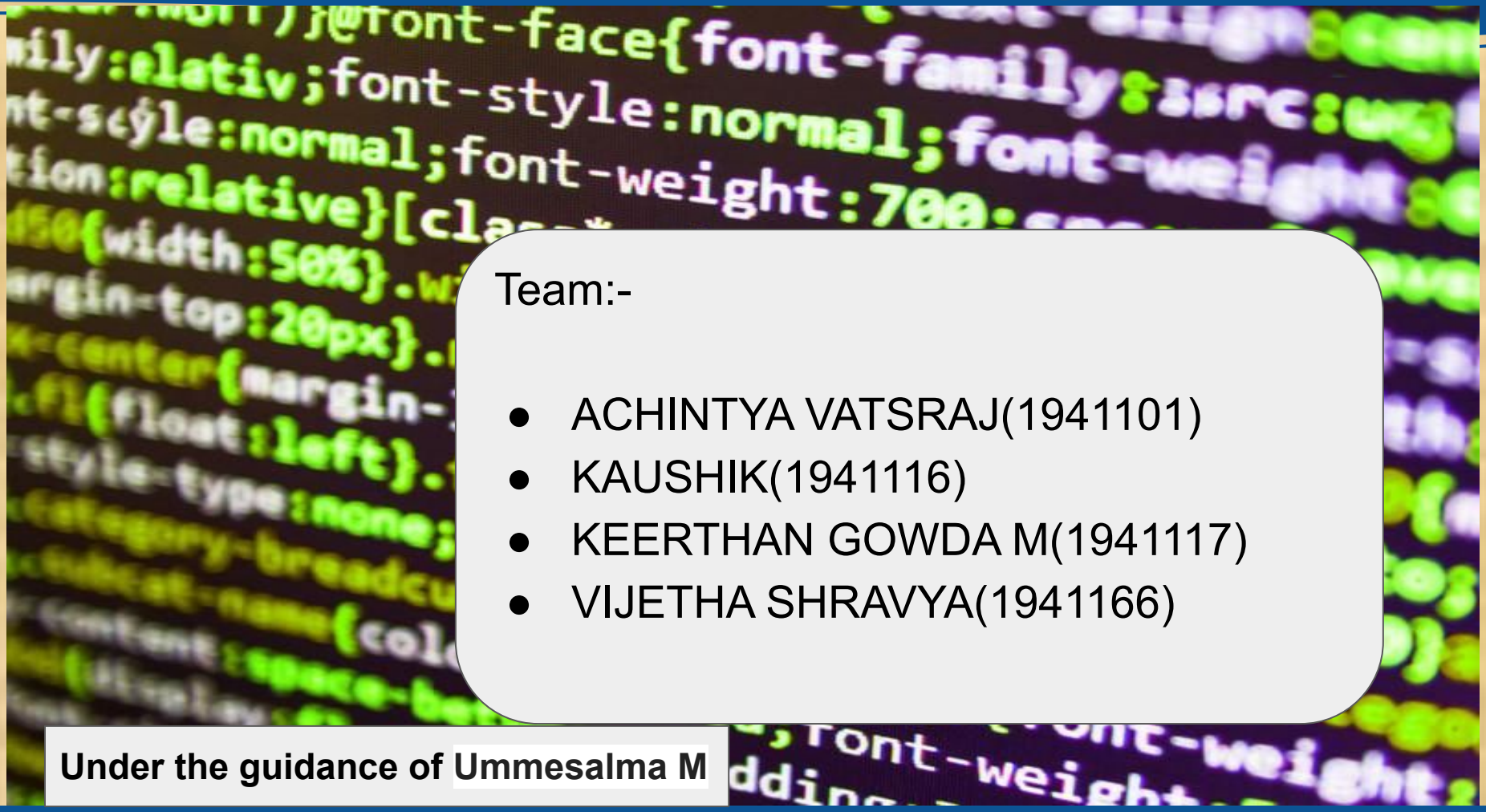
MISSION
CHRIST is a nurturing ground for an individual's holistic development to make effective contribution to the society in a dynamic environment

VISION
Excellence and Service

CORE VALUES
Faith in God | Moral Uprightness
Love of Fellow Beings
Social Responsibility | Pursuit of Excellence

MALSMART

CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE, INDIA



Team:-

- ACHINTYA VATSRAJ(1941101)
- KAUSHIK(1941116)
- KEERTHAN GOWDA M(1941117)
- VIJETHA SHRAVYA(1941166)

Under the guidance of Ummesalma M

Our Domain:- Client Side Cyber Security

Introduction:

Computers are an important part of everyday life to many people across the world. Computers in the hands of consumers who lack the knowledge of protection tools and who have limited administrator skills are vulnerable to virus attacks.A recent trend in attacks has been the attempt to disable security protocols in place at the host machine. This type of attack leaves the host computer completely defenseless and vulnerable to many further exploits through the Internet. To ensure the continuous functioning of the security protocols, a software-based solution is proposed in this thesis.AI and machine learning antivirus leverage sophisticated mathematical algorithms combined with the data from other deployments to understand what the baseline of security is for a given system.

Objective:-

1. To generate a new, effective framework to analyse the behavioural characteristics of the malware family and the mechanics of its operation.
2. To develop a malware detection Toolkit, consisting of a simple structural prototype built from open source software, Implement scanning and content discovery functionality using Python.
3. To conduct an extensive literature review of the different trials associated with malware detection and to identify the parameters for developing the most efficient tools for a live system
4. Develop an ecosystem of Apps across platforms to provide concrete client side security(such as Desktop GUI(tkinter),Mobile App,Chrome Extension.)

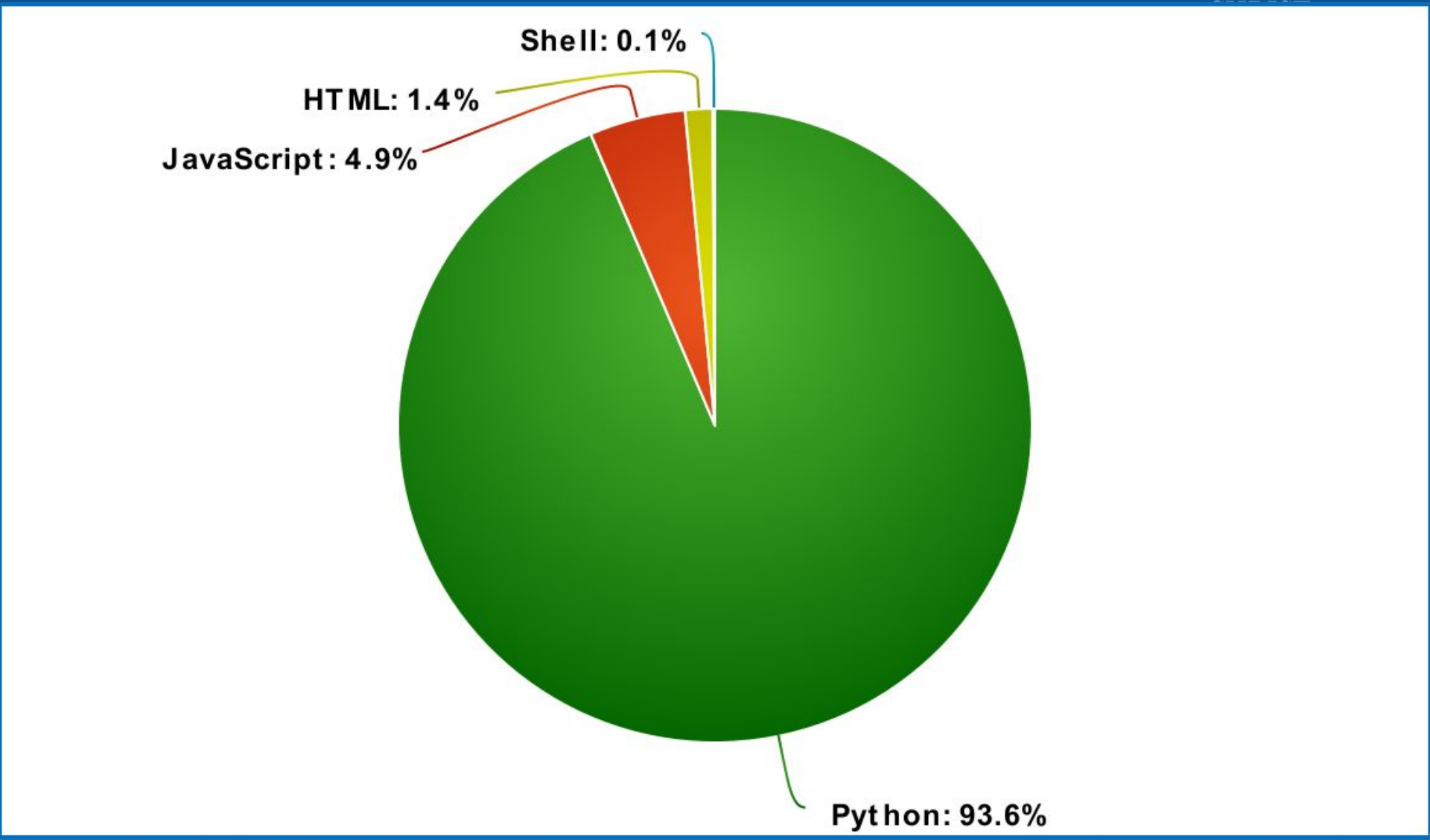
SYSTEM ANALYSIS:-

The Existing Client Side Security solutions do feature one or the other type of detection and Prevention techniques but they do not for the most part try to mix and match the said methods, and no product on the market has both an extension and mobile application to go with their desktop security solution.

Our Project is using the SQL Database Architecture to store data in relational models.

Components of the Project:

1. Desktop Application
2. Backend System
3. AI/ML Model
4. Chrome Extension
5. Mobile APP(NOT YET IMPLEMENTED)


Shell: 0.1%
HTML: 1.4%
JavaScript: 4.9%
Python: 93.6%
Python
JavaScript
HTML
Shell
meta-chart.com

PROFILE OF THE PROBLEM

If you are using a free antivirus program, there is no guarantee that it will provide you the complete protection. Most free antivirus programs out there only offer a basic level of protection. Moreover they are capable of identifying only certain types of threats. In order for acquiring complete level of protection, you have to use a firewall as well.Using an antivirus program means that a lot of resources from the memory and the hard drive is being used. As a result it can drastically slow down overall speed of the computer. Moreover, the process of scanning can also cause lags in the network.

Gantt chart

Start Date	End Date	Description	Feature	Duration(Rough)
31-07-21	03-08-21	Initial Documentation and Prepatory Phase	Basic Python and related technology installation and Port scanner	4
04-08-21	08-08-21	Phase - 1	Firewall,Raw Socket Sniffer and Basic GUI	5
09-08-21	15-08-21	Phase -1	Behaviour and Signature Malware Detection	7
16-08-21	04-09-21	Phase - 1	Design and Build Model for Heuristic-Based Detection With DBMS	20
05-09-21	12-09-21	Phase - 1	Process Monitering and AntiMalware Testing	8
13-09-21	25-09-21	Phase - 1	Sandbox Environment,Web Protection,Threat Score Calculation	13
26-09-21	15-10-21	Phase - 2	Backup Restore,API dev,Cloud Engine Setup,Improve GUI	20
16-10-21	25-10-21	Phase - 3	Further Model Testing and Detailed Documentation	10
26-10-21	31-10-21	Phase - 3	Improve application Logic and develop simple Mobile App with DashBoard(connect with API)	6
01-11-21	10-11-21	Phase - 4	Testing,Demo,Accuracy Data Collection through parellel Container Tests	10
11-11-21	21-11-21	Phase - 4	Publish Product on GitHub and Finish Documentation , in-depth paper on Model as well as Finalise GUI colors	11

SOFTWARE REQUIREMENTS

At Developer Side

Software Used

- HTML
- VISUAL STUDIO CODE
- PYTHON
- SQLITE3 DATABASE
- JAVASCRIPT
- C / Assembly

At System Users Side

Software Requirements

- Browser (IE 7.0 or Above, Mozilla Firefox, Google Chrome
- Browser Must be JavaScript Enabled

HARDWARE REQUIREMENTS

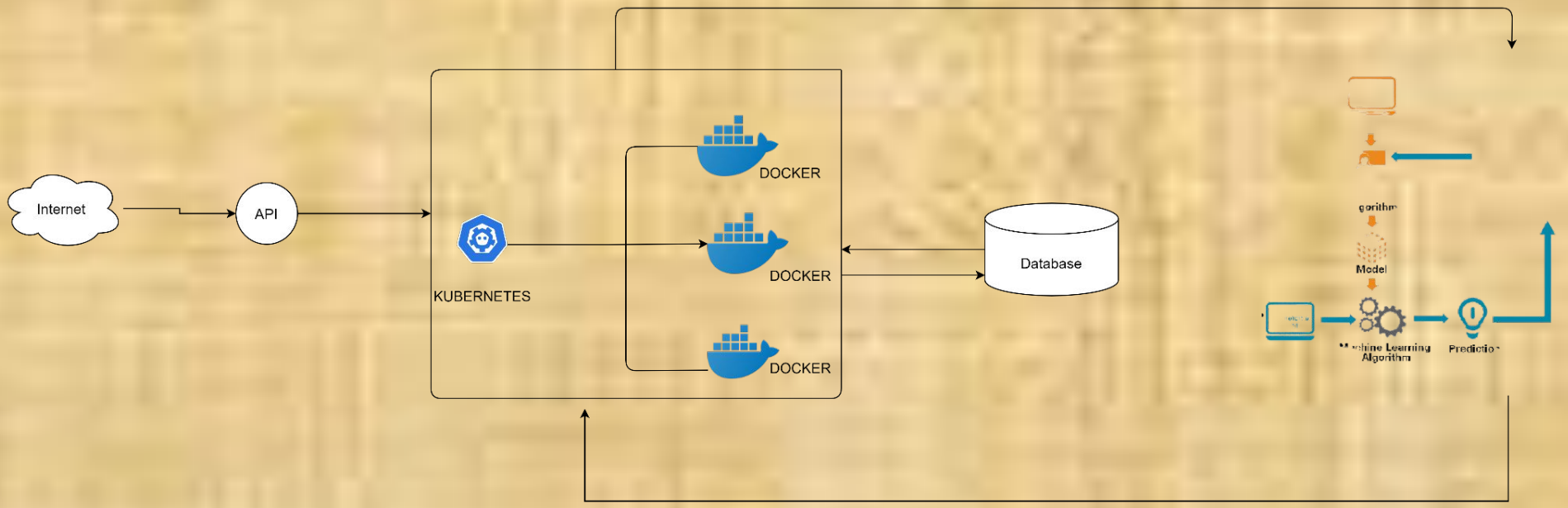
At Developer Side

Hardware Used
- Intel core i5
- Atleast 16 GB RAM.
- O.S. – Windows 10 or *Nix

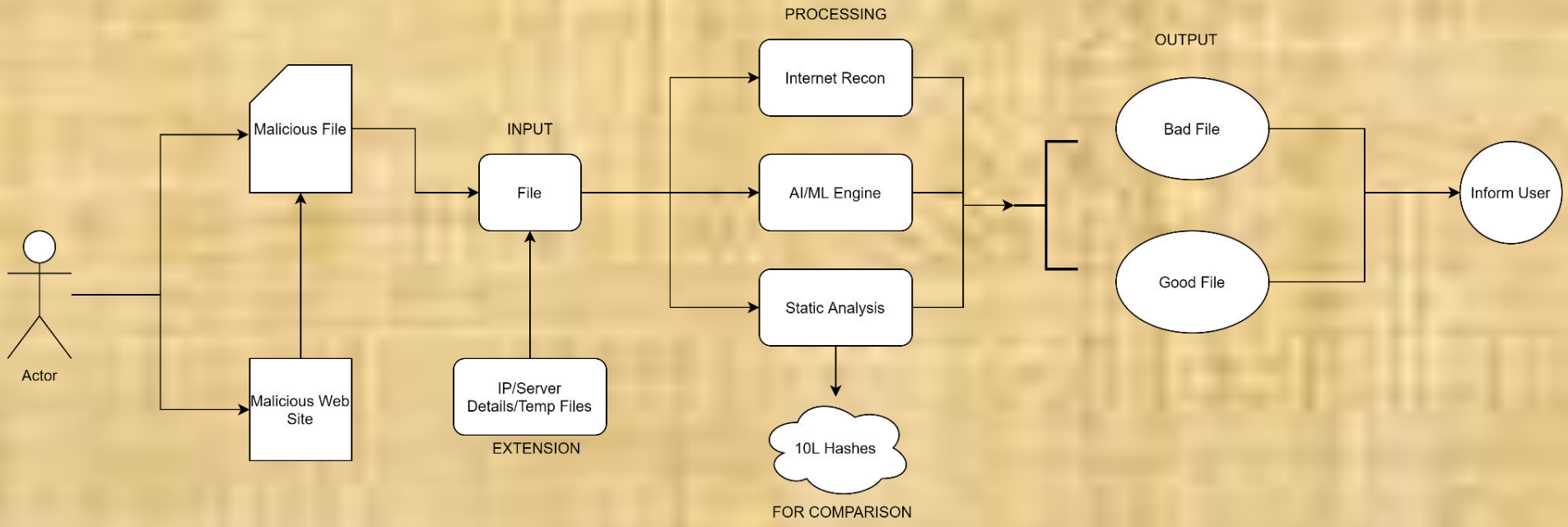
At System Users Side

Hardware Requirements
- Intel Core i3
- O.S. – Windows 10 or *Nix

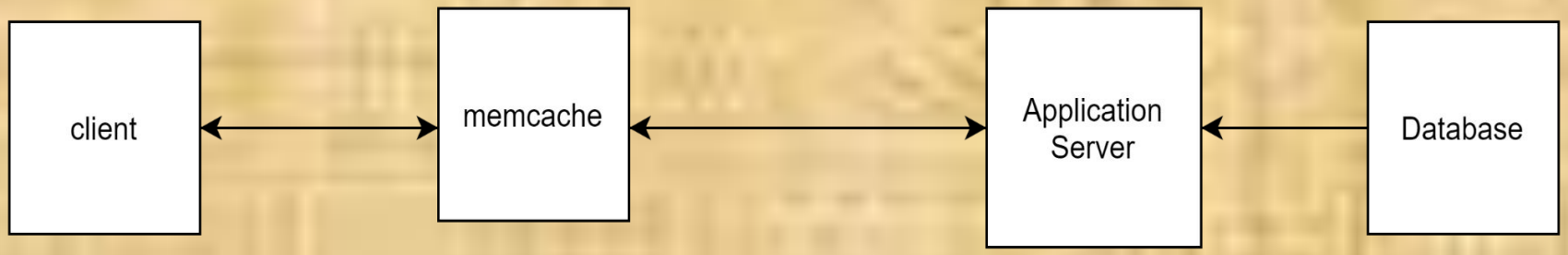
Block diagram:-



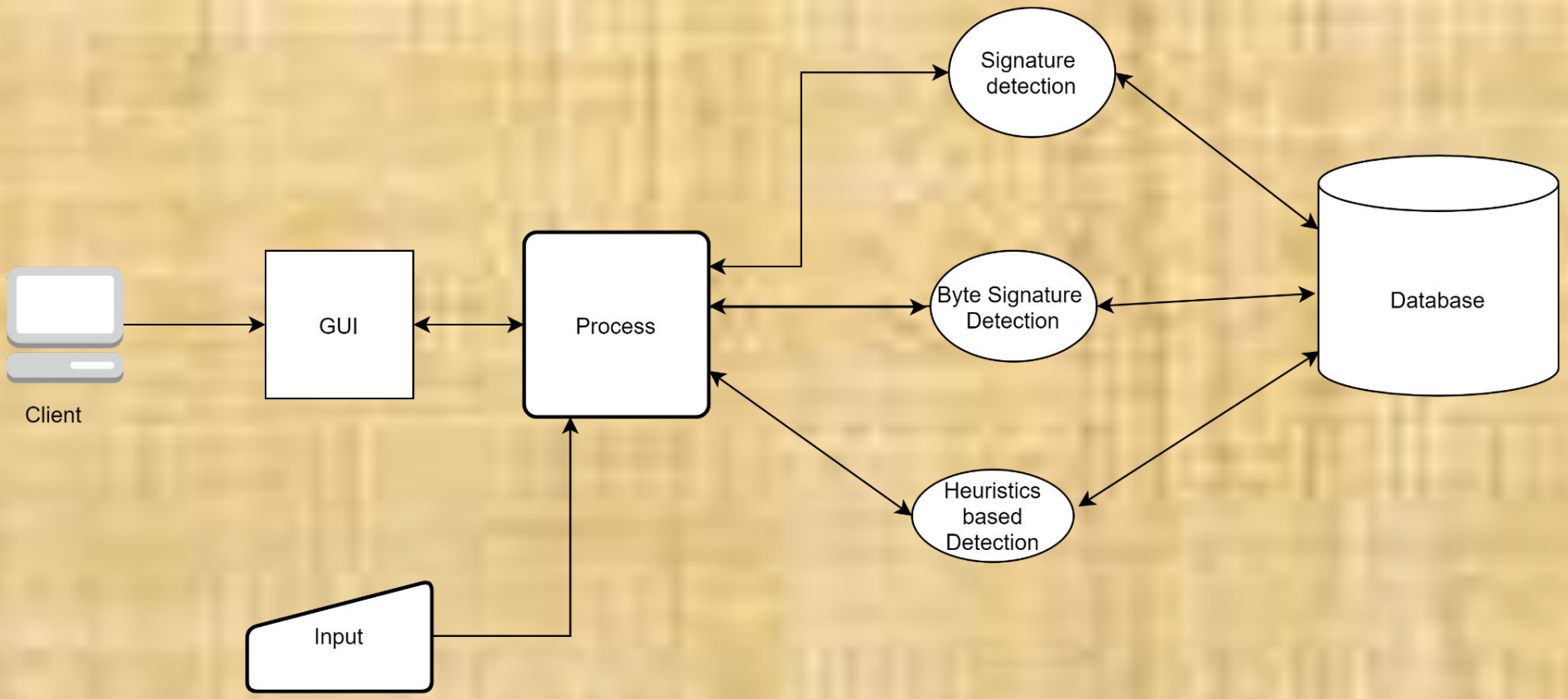
Data Flow Diagram



4 tier architecture

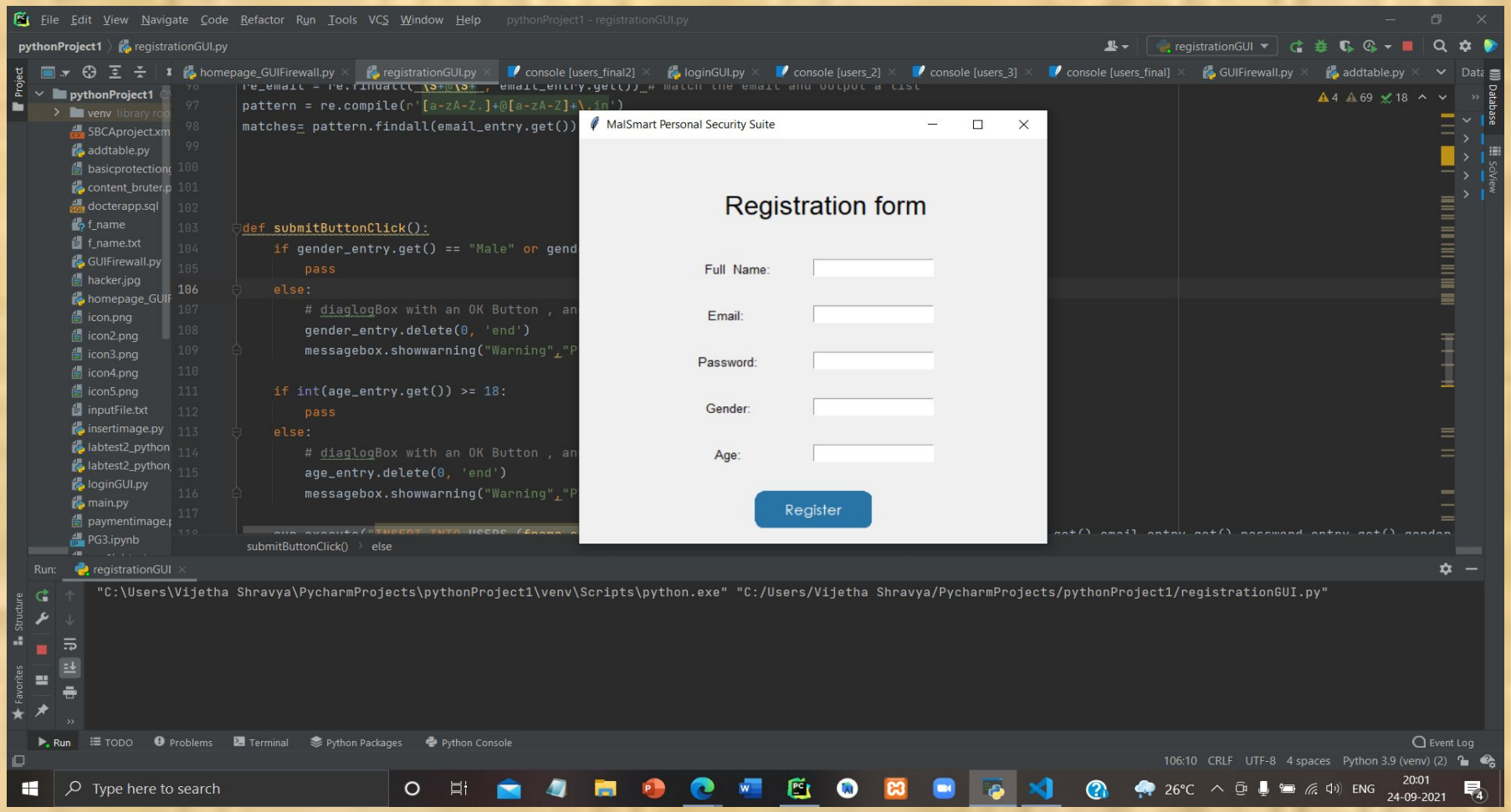


malware detection cycle

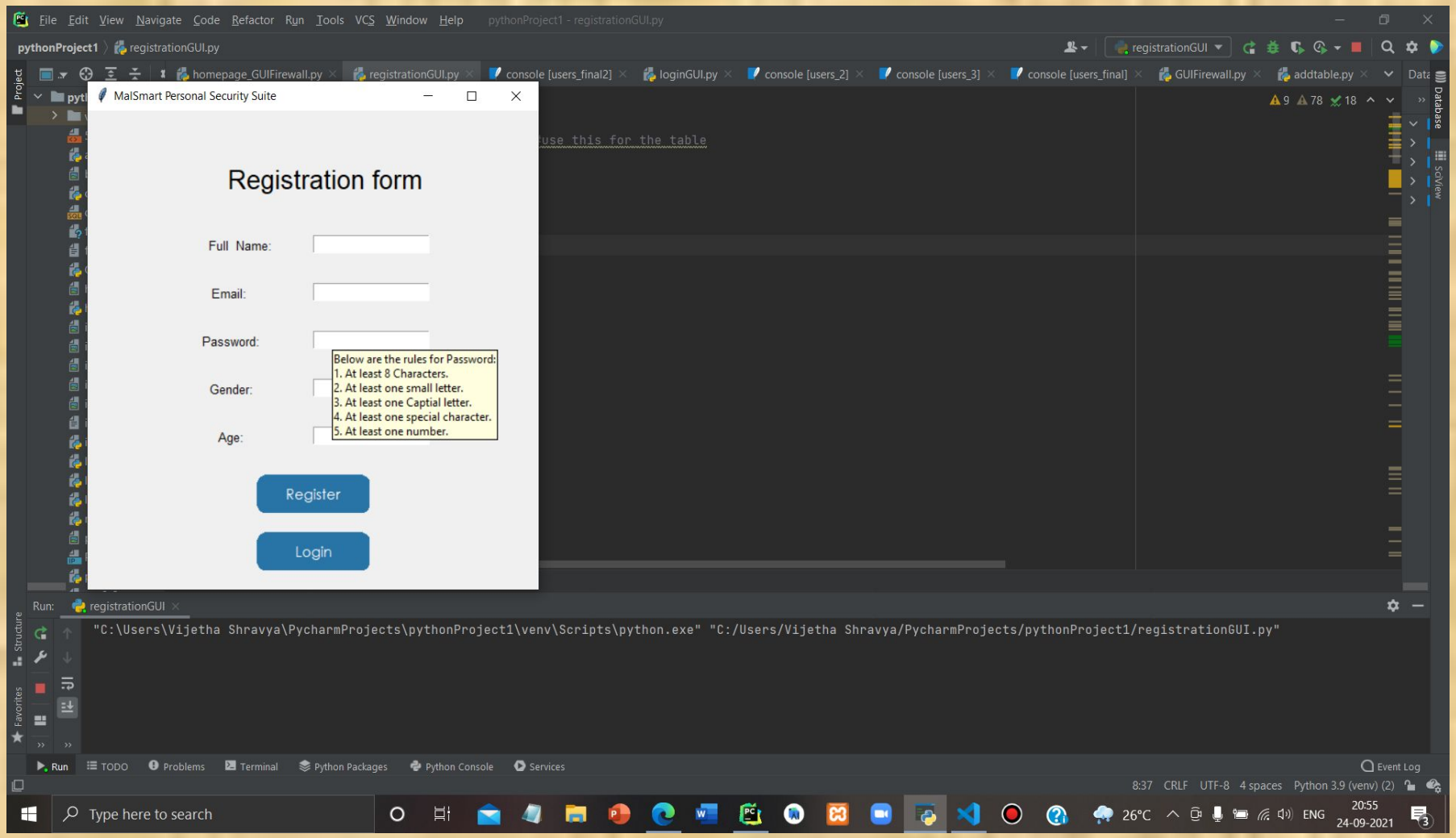


GUI using python tkinter

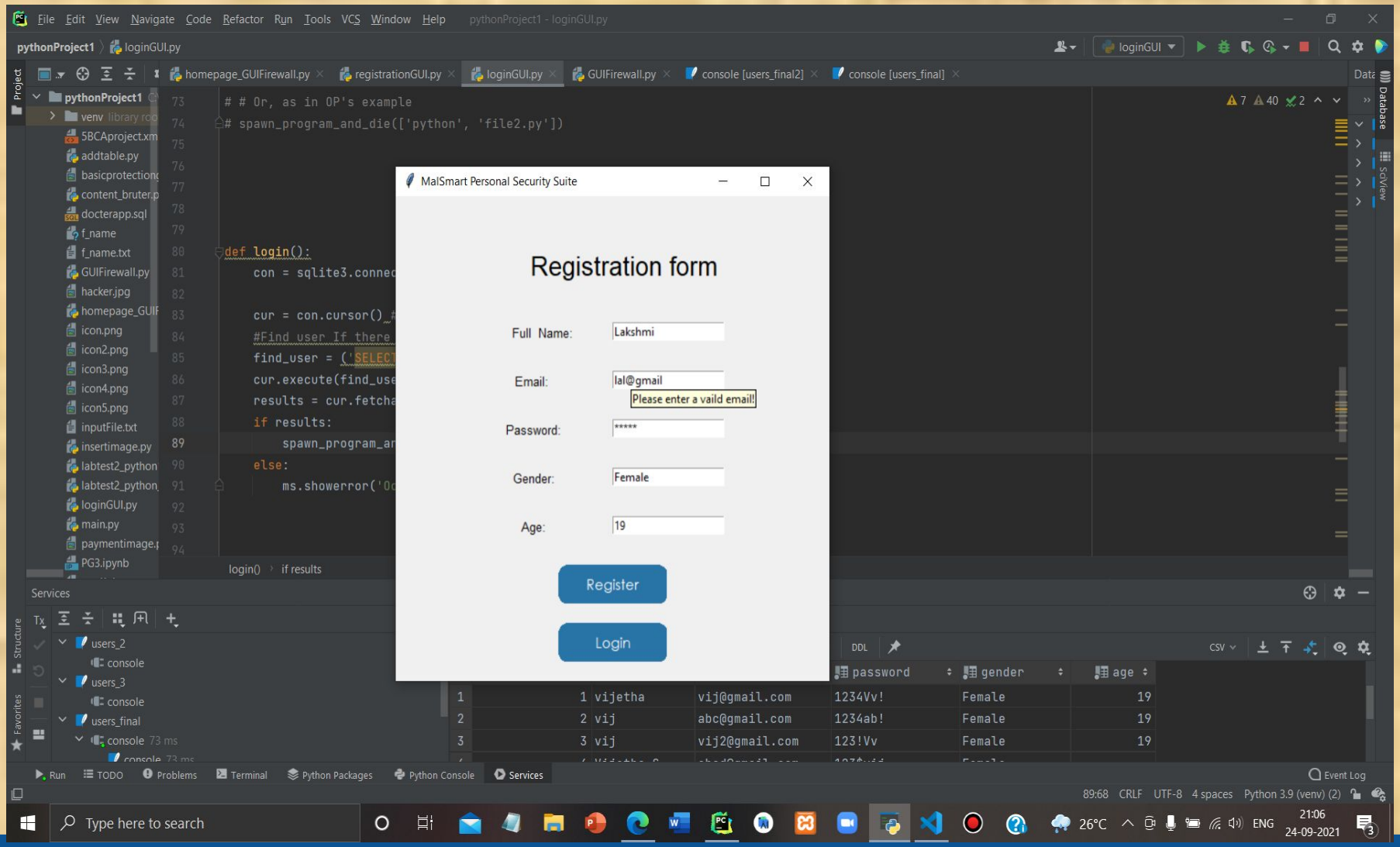
Screenshot 1:



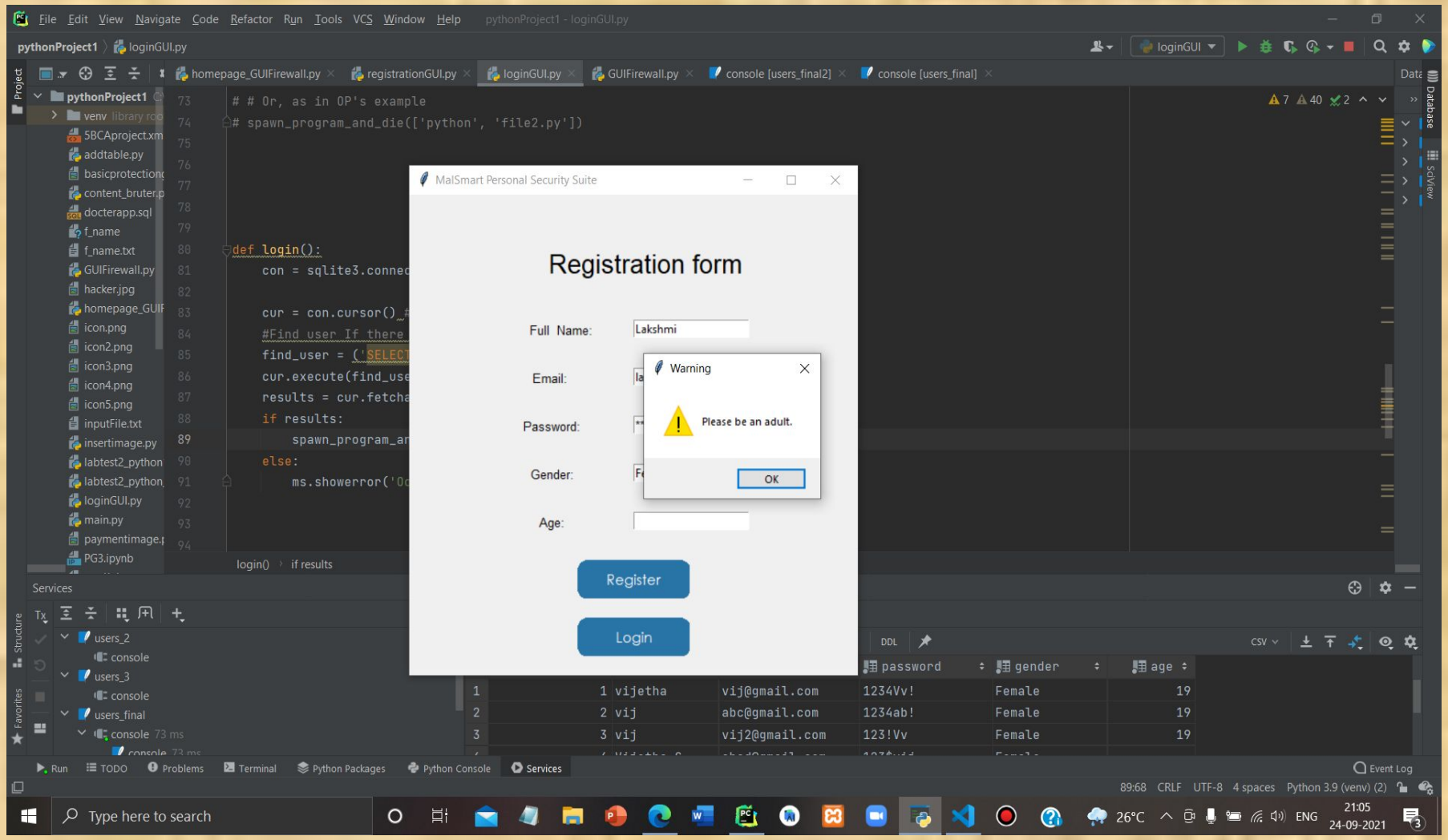
Screenshot 2:



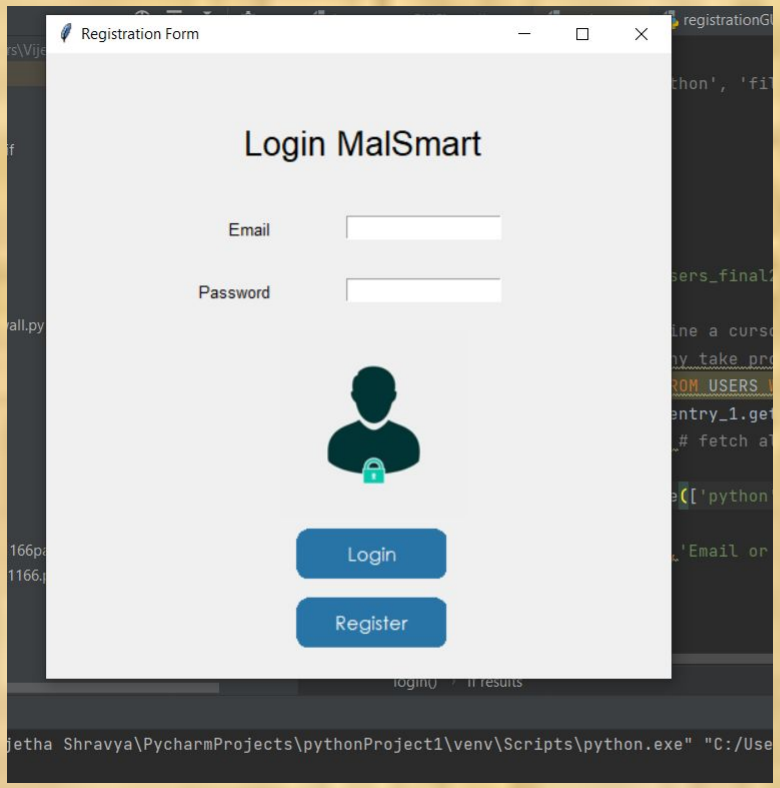
Screenshot 3:



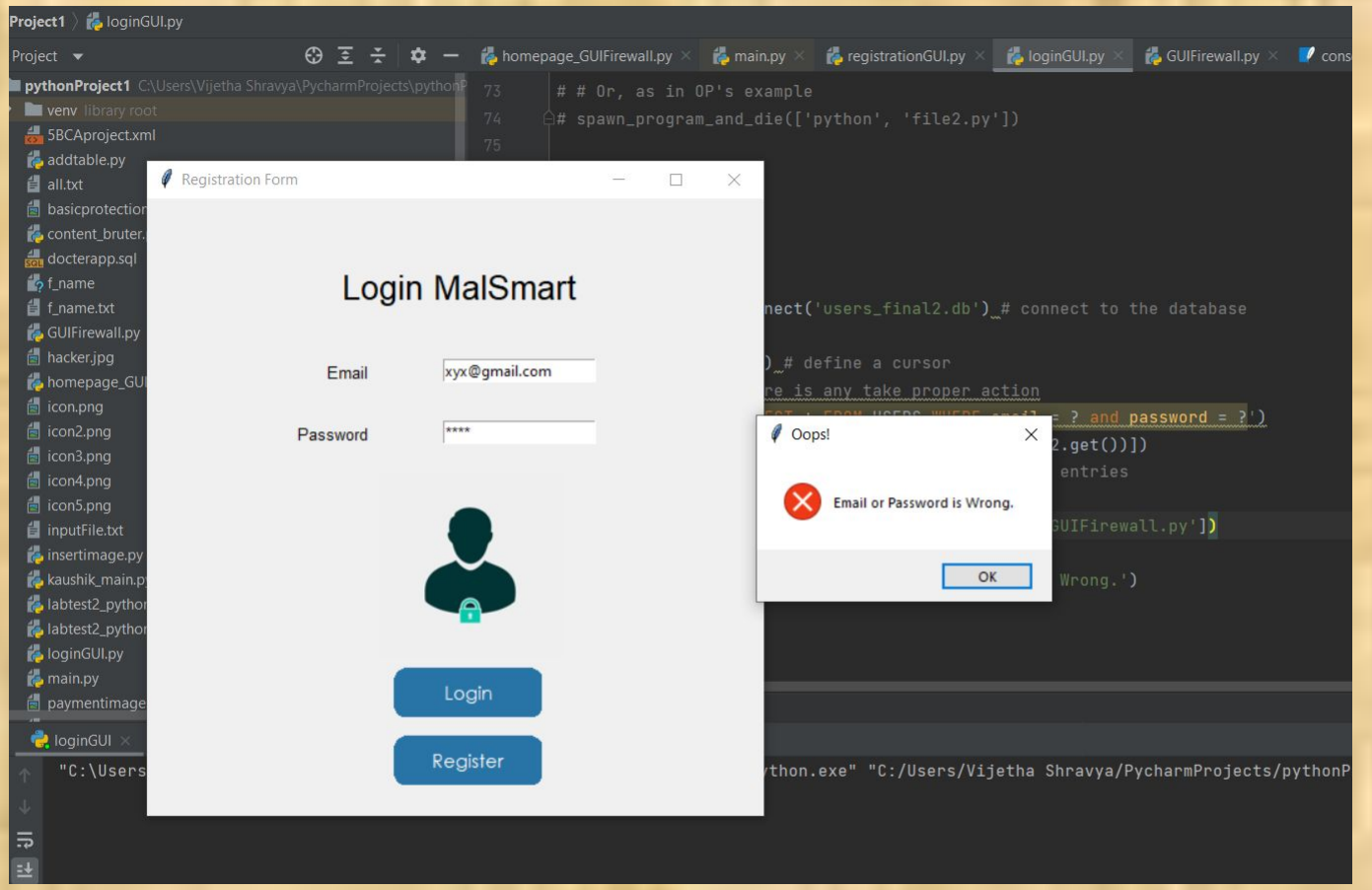
Screenshot 4:



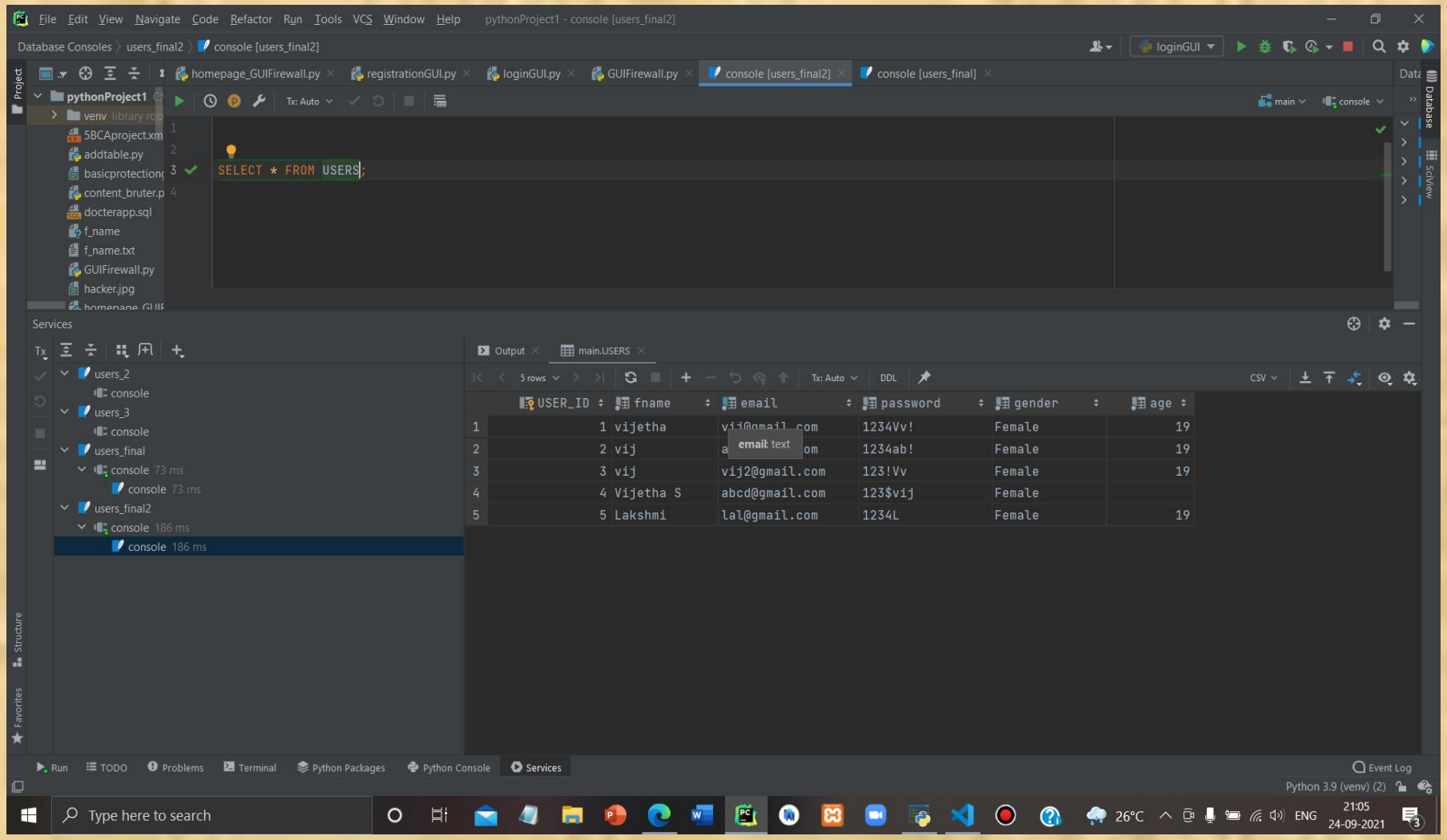
Screenshot :


Registration Form
Login MalSmart
Email
Password
Login
Register
jetha Shravya\PycharmProjects\pythonProject1\venv\Scripts\python.exe" "C:/Use

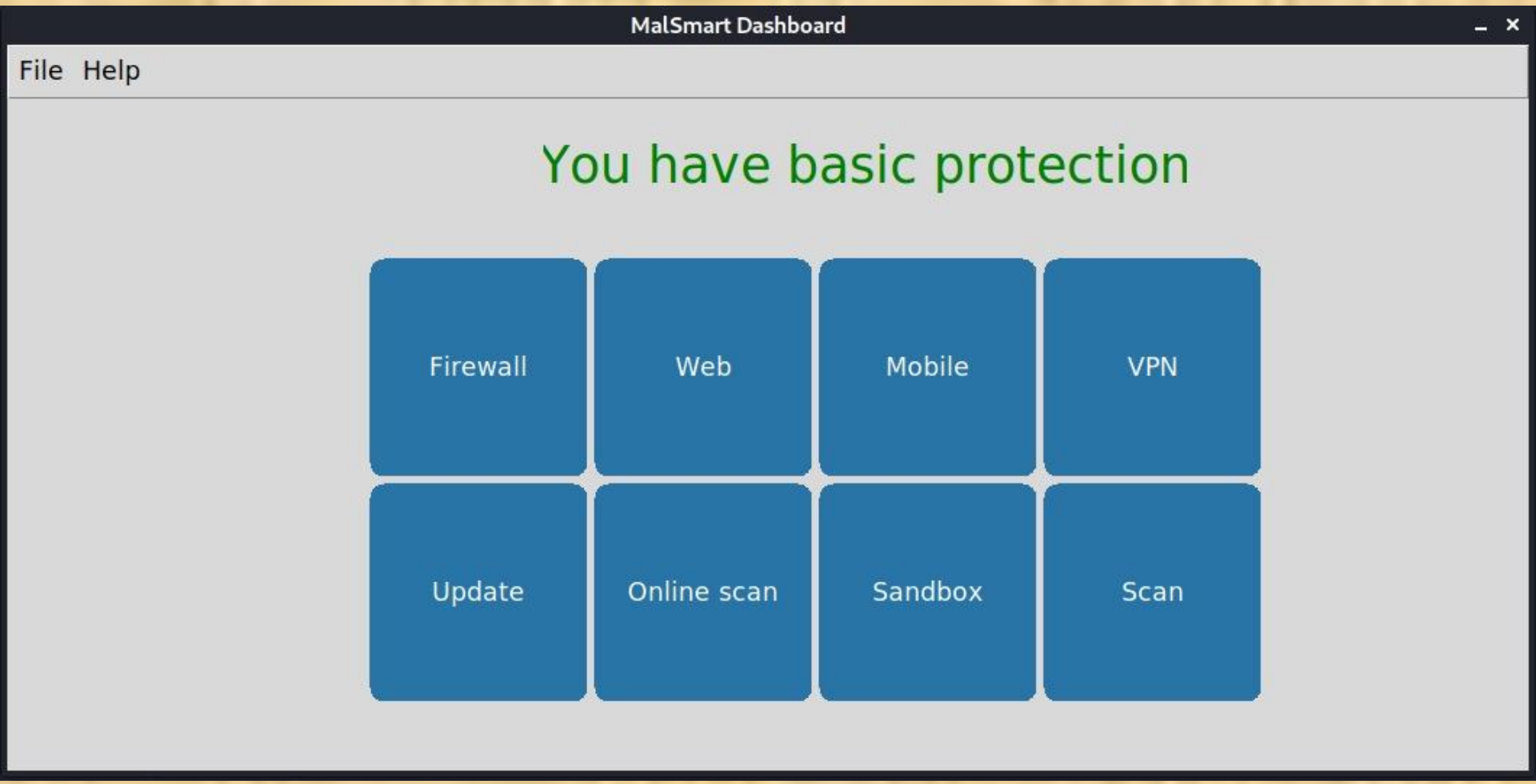
Screenshot :


Registration Form
Login MalSmart
Email
xyx@gmail.com
Password
****
Login
Register
Oops!
Email or Password is Wrong.
OK

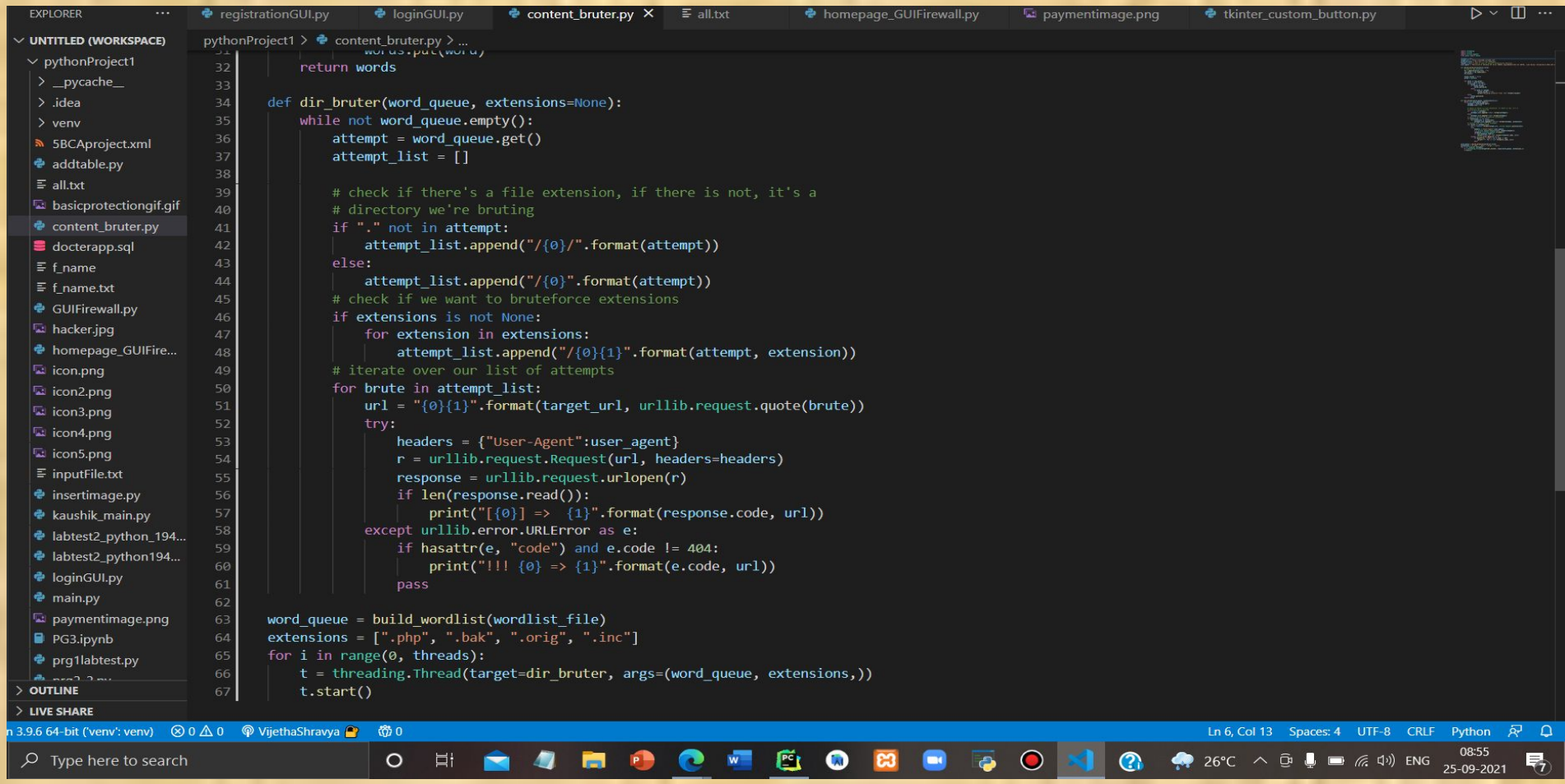
Screenshot 5:



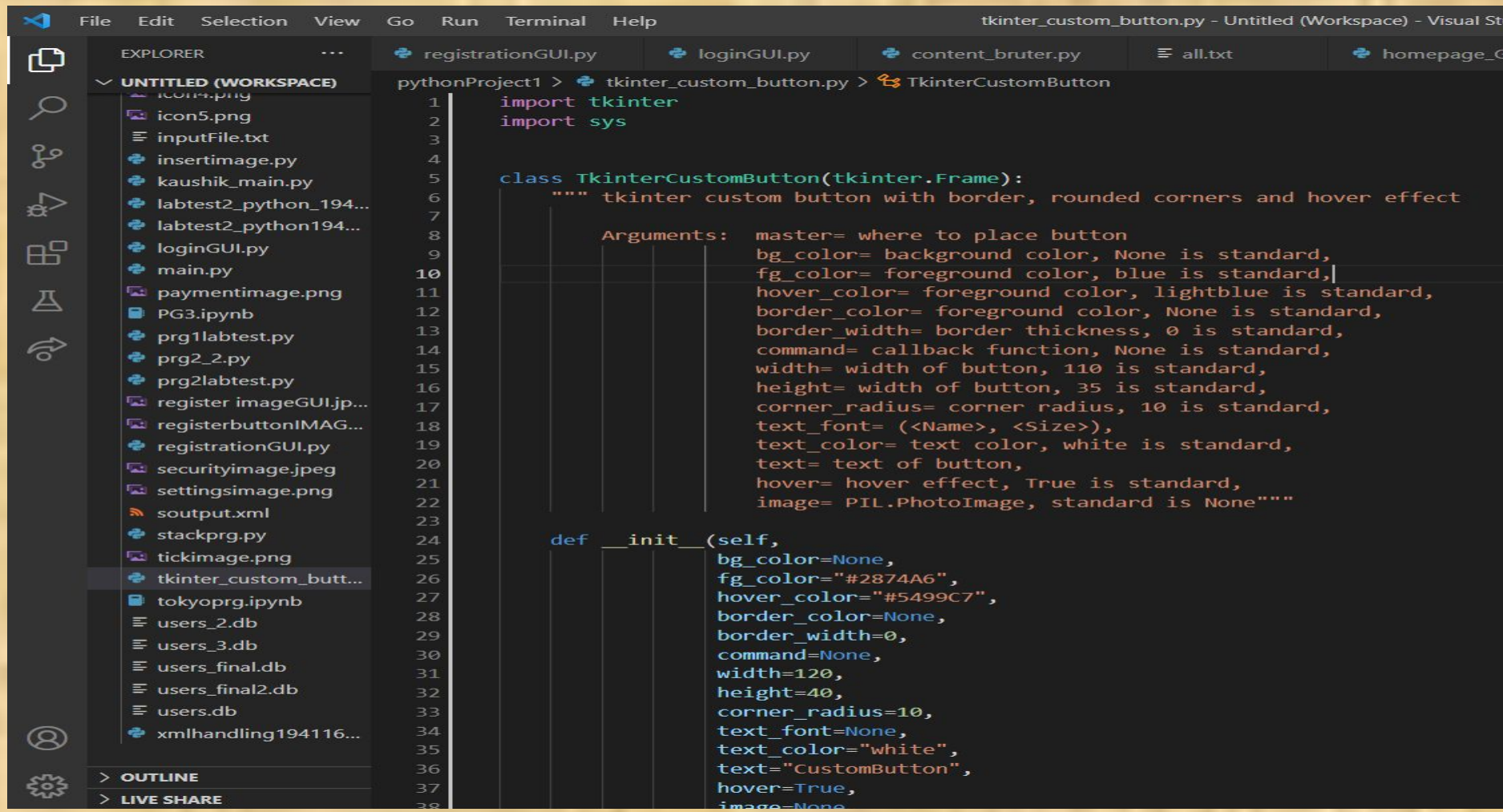
Screenshot 6:



Screenshot :


EXPLORER
registrationGUI.py
loginGUI.py
content_bruter.py
all.txt
homepage_GUIFirewall.py
paymentimage.png
tkinter_custom_button.py
UNTITLED (WORKSPACE)
pythonProject1
__pycache__
.idea
venv
5BCAproject.xml
addtable.py
all.txt
basicprotectiongif.gif
content_bruter.py
docterapp.sql
f_name
f_name.txt
GUIFirewall.py
hacker.jpg
homepage_GUIFire...
icon.png
icon2.png
icon3.png
icon4.png
icon5.png
inputFile.txt
insertimage.py
kaushik_main.py
labtest2_python_194...
labtest2_python194...
loginGUI.py
main.py
paymentimage.png
PG3.ipynb
prg1labtest.py
OUTLINE
LIVE SHARE
pythonProject1 > content_bruter.py > ...
return words
def dir_bruter(word_queue, extensions=None):
while not word_queue.empty():
attempt = word_queue.get()
attempt_list = []
# check if there's a file extension, if there is not, it's a
# directory we're bruting
if "." not in attempt:
attempt_list.append("/{0}/".format(attempt))
else:
attempt_list.append("/{0}".format(attempt))
# check if we want to bruteforce extensions
if extensions is not None:
for extension in extensions:
attempt_list.append("/{0}{1}".format(attempt, extension))
# iterate over our list of attempts
for brute in attempt_list:
url = "{0}{1}".format(target_url, urllib.request.quote(brute))
try:
headers = {"User-Agent":user_agent}
r = urllib.request.Request(url, headers=headers)
response = urllib.request.urlopen(r)
if len(response.read()):
print("[{0}] => {1}".format(response.code, url))
except urllib.error.URLError as e:
if hasattr(e, "code") and e.code != 404:
print("!!! {0} => {1}".format(e.code, url))
pass
word_queue = build_wordlist(wordlist_file)
extensions = [".php", ".bak", ".orig", ".inc"]
for i in range(0, threads):
t = threading.Thread(target=dir_bruter, args=(word_queue, extensions,))
t.start()
n 3.9.6 64-bit ('venv': venv)
VijethaShravya
Ln 6, Col 13
Spaces: 4
UTF-8
CRLF
Python
Type here to search
26°C
ENG
08:55
25-09-2021

Screenshot :


File Edit Selection View Go Run Terminal Help
tkinter_custom_button.py - Untitled (Workspace) - Visual St
EXPLORER
UNTITLED (WORKSPACE)
icon5.png
inputFile.txt
insertimage.py
kaushik_main.py
labtest2_python_194...
labtest2_python194...
loginGUI.py
main.py
paymentimage.png
PG3.ipynb
prg1labtest.py
prg2_2.py
prg2labtest.py
register imageGUI.jp...
registerbuttonIMAG...
registrationGUI.py
securityimage.jpeg
settingsimage.png
soutput.xml
stackprg.py
tickimage.png
tkinter_custom_butt...
tokyoprg.ipynb
users_2.db
users_3.db
users_final.db
users_final2.db
users.db
xmlhandling194116...
OUTLINE
LIVE SHARE
registrationGUI.py
loginGUI.py
content_bruter.py
all.txt
homepage_G
pythonProject1 > tkinter_custom_button.py > TkinterCustomButton
import tkinter
import sys
class TkinterCustomButton(tkinter.Frame):
""" tkinter custom button with border, rounded corners and hover effect
Arguments: master= where to place button
bg_color= background color, None is standard,
fg_color= foreground color, blue is standard,
hover_color= foreground color, lightblue is standard,
border_color= foreground color, None is standard,
border_width= border thickness, 0 is standard,
command= callback function, None is standard,
width= width of button, 110 is standard,
height= width of button, 35 is standard,
corner_radius= corner radius, 10 is standard,
text_font= (<Name>, <Size>),
text_color= text color, white is standard,
text= text of button,
hover= hover effect, True is standard,
image= PIL.PhotoImage, standard is None"""
def __init__(self,
bg_color=None,
fg_color="#2874A6",
hover_color="#5499C7",
border_color=None,
border_width=0,
command=None,
width=120,
height=40,
corner_radius=10,
text_font=None,
text_color="white",
text="CustomButton",
hover=True,

File Edit Selection View Go Run Terminal Help content_bruter.py - Project 1 - Visual Studio Code

Welcome | content_bruter.py | all.txt

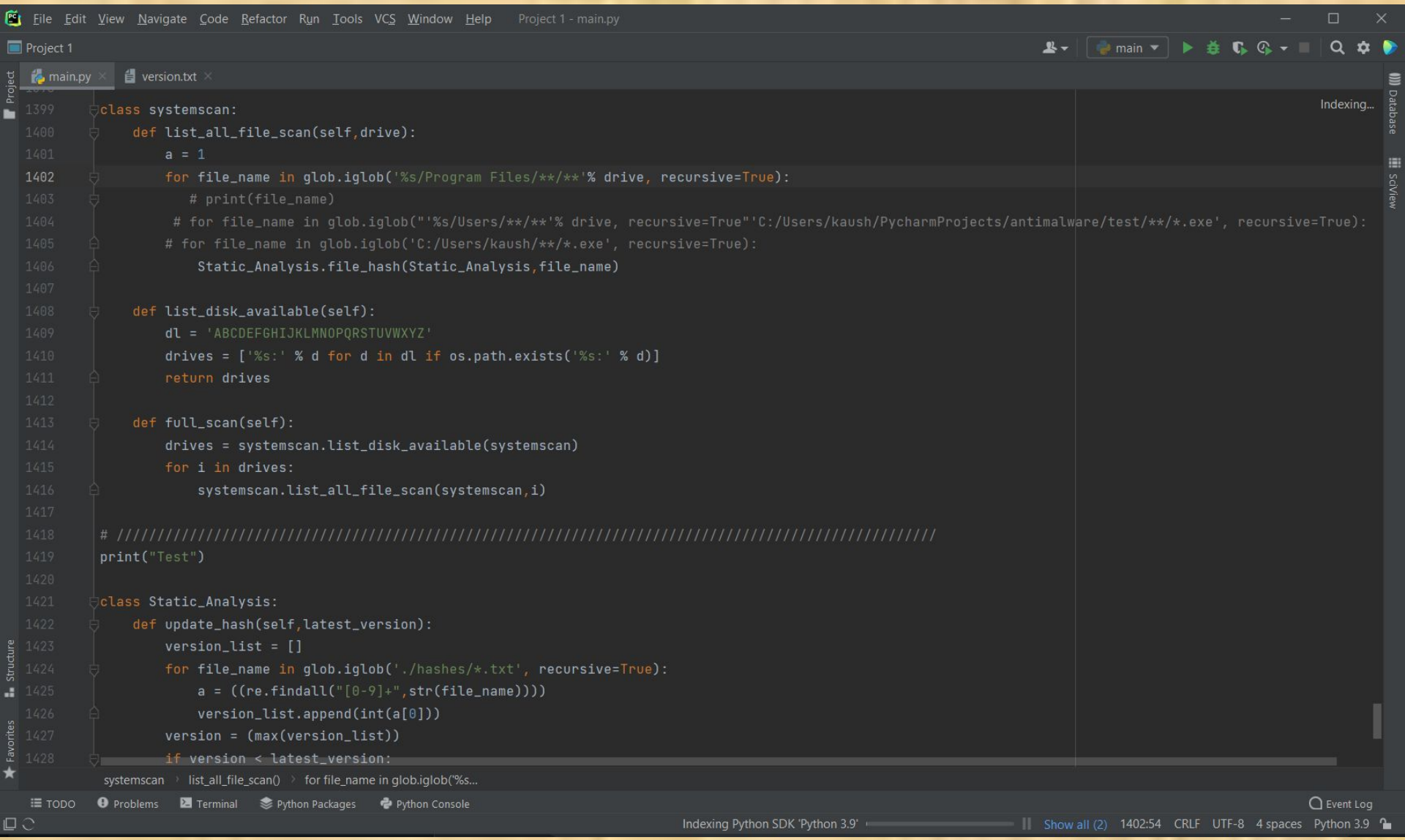
content_bruter_backend > content_bruter.py > ...

```
49          # iterate over our list of attempts
50          for brute in attempt_list:
51              url = "{0}{1}".format(target_url, urllib.request.quote(brute))
52              try:
53                  headers = {"User-Agent":user_agent}
54                  r = urllib.request.Request(url, headers=headers)
55                  response = urllib.request.urlopen(r)
56                  if len(response.read()):
57                      print("[{0}] =>  {1}".format(response.code, url))
58              except urllib.error.URLError as e:
59                  if hasattr(e, "code") and e.code != 404:
60                      print("!!! {0} => {1}".format(e.code, url))
```

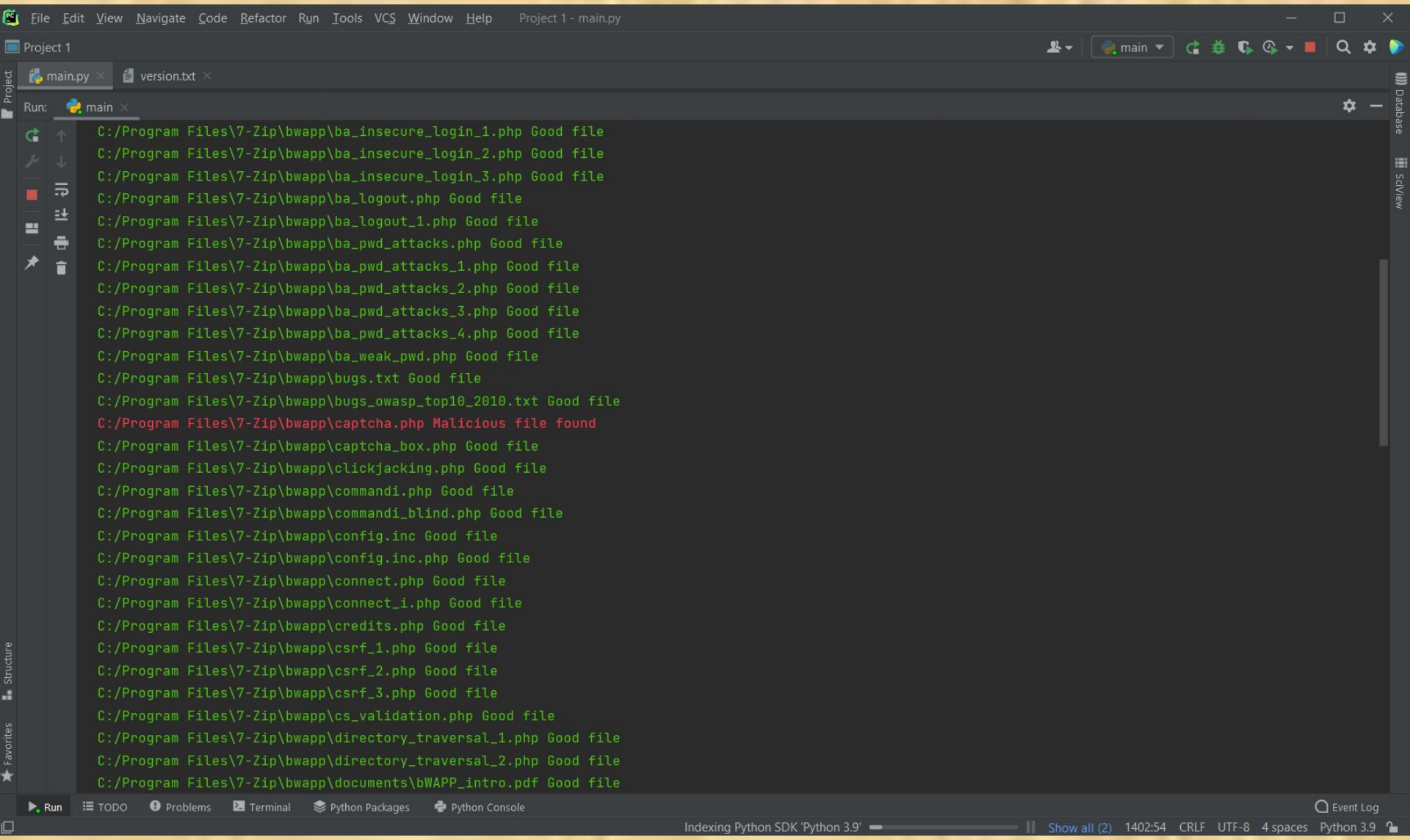
PROBLEMS OUTPUT TERMINAL SQL CONSOLE DEBUG CONSOLE powershell

```
[200] =>  http://testphp.vulnweb.com/index.php
[200] =>  http://testphp.vulnweb.com/index.bak
[200] =>  http://testphp.vulnweb.com/search.php
[200] =>  http://testphp.vulnweb.com/login.php
[200] =>  http://testphp.vulnweb.com/login.php
[200] =>  http://testphp.vulnweb.com/images/
[200] =>  http://testphp.vulnweb.com/index.php
[200] =>  http://testphp.vulnweb.com/logout.php
[200] =>  http://testphp.vulnweb.com/categories.php
[200] =>  http://testphp.vulnweb.com/404.php
[200] =>  http://testphp.vulnweb.com/categories.php
[200] =>  http://testphp.vulnweb.com/signup.php
[200] =>  http://testphp.vulnweb.com/comment.php
```

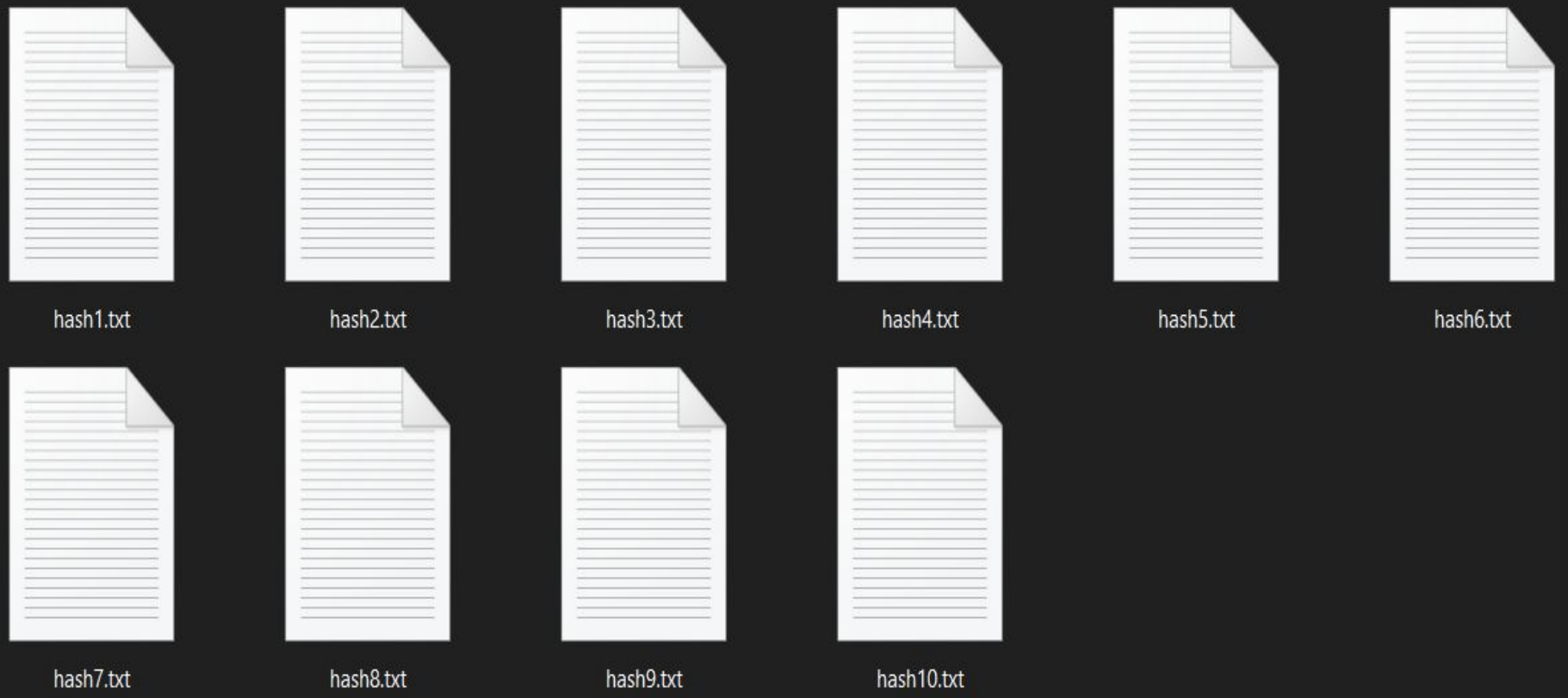
Python 3.9.7 64-bit ⊗ 0 ⚠ 0 Connect AchintyaVatsraj Live Share Ln 5, Col 1 Spaces: 4 UTF-8 CRLF MagicPython Go Live Prettier



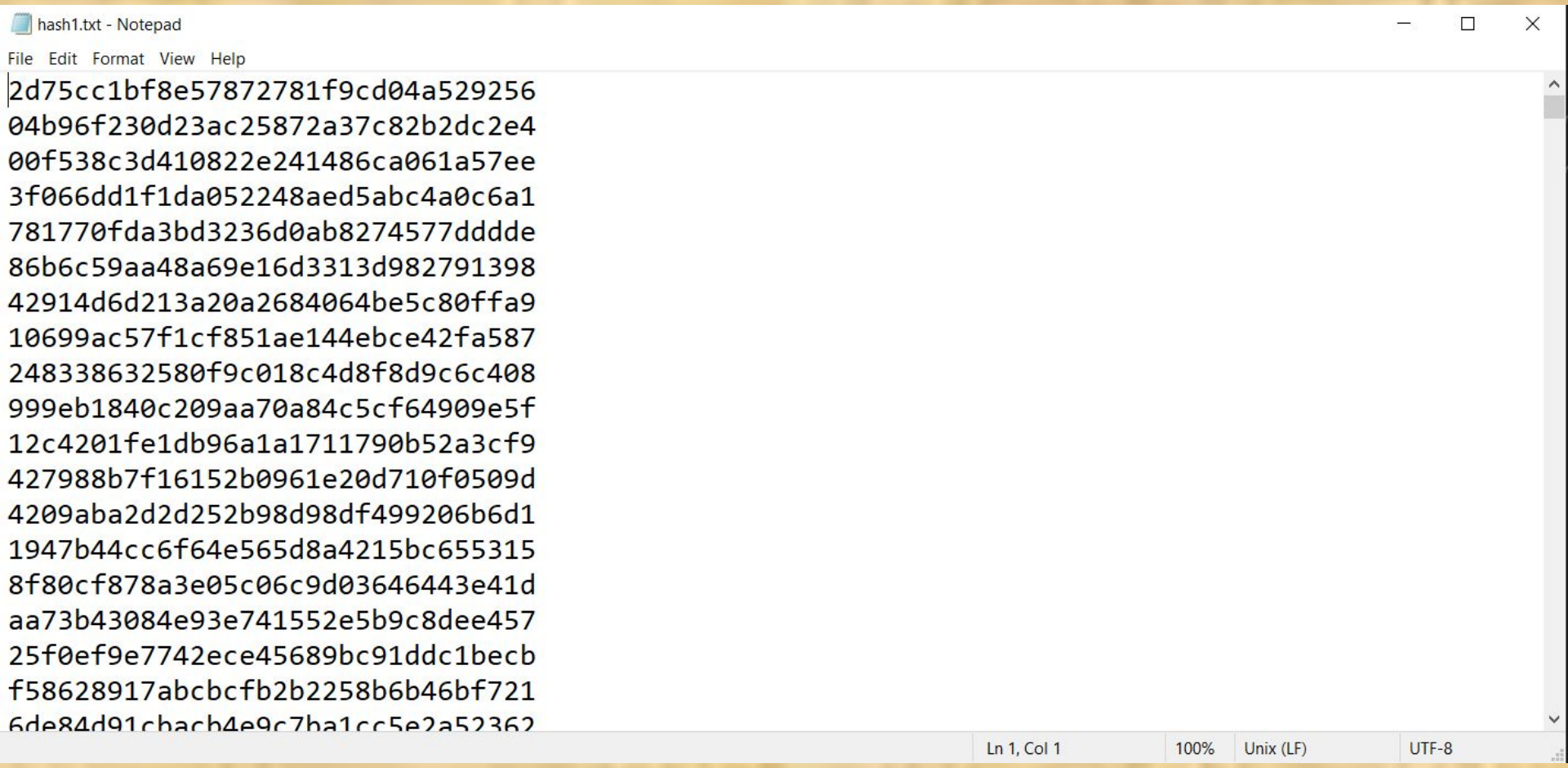

```
1399  class systemscan:
1400      def list_all_file_scan(self,drive):
1401          a = 1
1402          for file_name in glob.iglob('%s/Program Files/**/**'% drive, recursive=True):
1403             # print(file_name)
1404           # for file_name in glob.iglob("'%s/Users/**/**'% drive, recursive=True"'C:/Users/kaush/PycharmProjects/antimalware/test/**/*.exe', recursive=True):
1405          # for file_name in glob.iglob('C:/Users/kaush/**/*.exe', recursive=True):
1406              Static_Analysis.file_hash(Static_Analysis,file_name)
1407
1408      def list_disk_available(self):
1409          dl = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
1410          drives = ['%s:' % d for d in dl if os.path.exists('%s:' % d)]
1411          return drives
1412
1413      def full_scan(self):
1414          drives = systemscan.list_disk_available(systemscan)
1415          for i in drives:
1416              systemscan.list_all_file_scan(systemscan,i)
1417
1418  # ////////////////////////////////////////////////////////////////////////////////////////////////////////////
1419  print("Test")
1420
1421  class Static_Analysis:
1422      def update_hash(self,latest_version):
1423          version_list = []
1424          for file_name in glob.iglob('./hashes/*.txt', recursive=True):
1425              a = ((re.findall("[0-9]+",str(file_name))))
1426              version_list.append(int(a[0]))
1427          version = (max(version_list))
1428          if version < latest_version:
```


File Edit View Navigate Code Refactor Run Tools VCS Window Help
Project 1 - main.py
Project 1
main
main.py
version.txt
Run:
main
C:/Program Files\7-Zip\bwapp\ba_insecure_login_1.php Good file
C:/Program Files\7-Zip\bwapp\ba_insecure_login_2.php Good file
C:/Program Files\7-Zip\bwapp\ba_insecure_login_3.php Good file
C:/Program Files\7-Zip\bwapp\ba_logout.php Good file
C:/Program Files\7-Zip\bwapp\ba_logout_1.php Good file
C:/Program Files\7-Zip\bwapp\ba_pwd_attacks.php Good file
C:/Program Files\7-Zip\bwapp\ba_pwd_attacks_1.php Good file
C:/Program Files\7-Zip\bwapp\ba_pwd_attacks_2.php Good file
C:/Program Files\7-Zip\bwapp\ba_pwd_attacks_3.php Good file
C:/Program Files\7-Zip\bwapp\ba_pwd_attacks_4.php Good file
C:/Program Files\7-Zip\bwapp\ba_weak_pwd.php Good file
C:/Program Files\7-Zip\bwapp\bugs.txt Good file
C:/Program Files\7-Zip\bwapp\bugs_owasp_top10_2010.txt Good file
C:/Program Files\7-Zip\bwapp\captcha.php Malicious file found
C:/Program Files\7-Zip\bwapp\captcha_box.php Good file
C:/Program Files\7-Zip\bwapp\clickjacking.php Good file
C:/Program Files\7-Zip\bwapp\commandi.php Good file
C:/Program Files\7-Zip\bwapp\commandi_blind.php Good file
C:/Program Files\7-Zip\bwapp\config.inc Good file
C:/Program Files\7-Zip\bwapp\config.inc.php Good file
C:/Program Files\7-Zip\bwapp\connect.php Good file
C:/Program Files\7-Zip\bwapp\connect_i.php Good file
C:/Program Files\7-Zip\bwapp\credits.php Good file
C:/Program Files\7-Zip\bwapp\csrf_1.php Good file
C:/Program Files\7-Zip\bwapp\csrf_2.php Good file
C:/Program Files\7-Zip\bwapp\csrf_3.php Good file
C:/Program Files\7-Zip\bwapp\cs_validation.php Good file
C:/Program Files\7-Zip\bwapp\directory_traversal_1.php Good file
C:/Program Files\7-Zip\bwapp\directory_traversal_2.php Good file
C:/Program Files\7-Zip\bwapp\documents\bWAPP_intro.pdf Good file
Run
TODO
Problems
Terminal
Python Packages
Python Console
Event Log
Indexing Python SDK 'Python 3.9'
Show all (2)
1402:54
CRLF
UTF-8
4 spaces
Python 3.9

Screenshot :


hash1.txt
hash2.txt
hash3.txt
hash4.txt
hash5.txt
hash6.txt
hash7.txt
hash8.txt
hash9.txt
hash10.txt

Screenshot :


hash1.txt - Notepad
File Edit Format View Help
2d75cc1bf8e57872781f9cd04a529256
04b96f230d23ac25872a37c82b2dc2e4
00f538c3d410822e241486ca061a57ee
3f066dd1f1da052248aed5abc4a0c6a1
781770fda3bd3236d0ab8274577dddde
86b6c59aa48a69e16d3313d982791398
42914d6d213a20a2684064be5c80ffa9
10699ac57f1cf851ae144ebce42fa587
248338632580f9c018c4d8f8d9c6c408
999eb1840c209aa70a84c5cf64909e5f
12c4201fe1db96a1a1711790b52a3cf9
427988b7f16152b0961e20d710f0509d
4209aba2d2d252b98d98df499206b6d1
1947b44cc6f64e565d8a4215bc655315
8f80cf878a3e05c06c9d03646443e41d
aa73b43084e93e741552e5b9c8dee457
25f0ef9e7742ece45689bc91ddc1becb
f58628917abcbcfb2b2258b6b46bf721
Ln 1, Col 1
100%
Unix (LF)
UTF-8

Interesting Fact about Analysis

We have 10L+ Hashes to do comparison that we will regularly improve/update to get better results and accuracy in Analysis.

Screenshot of Database Creation:

```
### Database Code

con = sqlite3.connect('users_final2.db')

cur = con.cursor()

cur.execute('''CREATE TABLE IF NOT EXISTS USERS(
    USER_ID INTEGER PRIMARY KEY AUTOINCREMENT,
    fname text NOT NULL,
    email text UNIQUE NOT NULL,
    password text NOT NULL,
    gender text NOT NULL,
    age INTEGER NOT NULL
)
''')

con.commit() # add the table if not already existing.
###
```

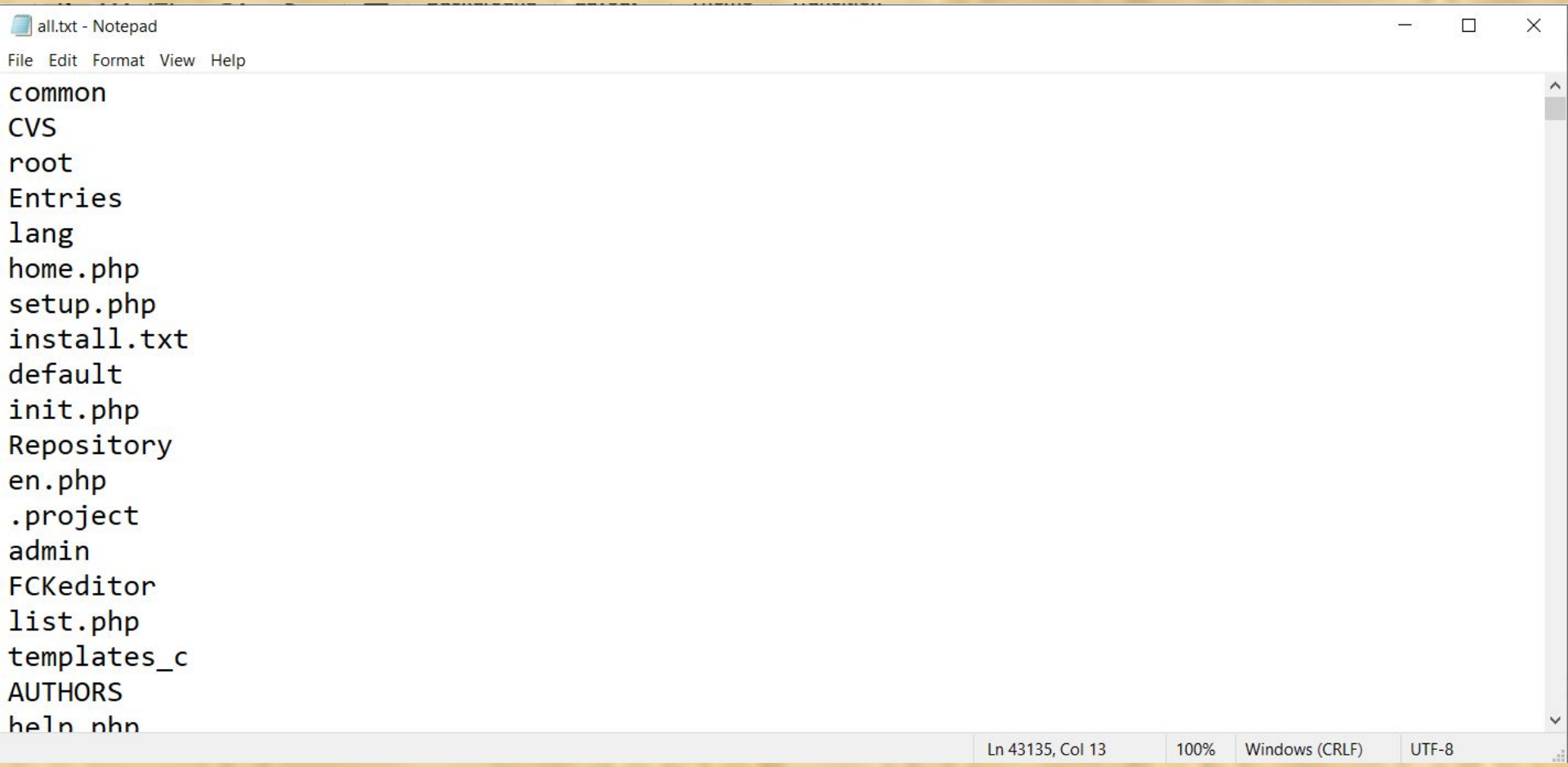
Screenshot of Imports for the Project:

```
from tkinter_custom_button import *
from tkinter import *
import sqlite3
import tkinter as tk
import awesometkinter as atk
from idlelib.tooltip import Hovertip
from tkinter import messagebox
from tkinter import messagebox as ms
import re
import subprocess
import sys

from PIL import ImageTk
from PIL import Image
```

Screenshots:

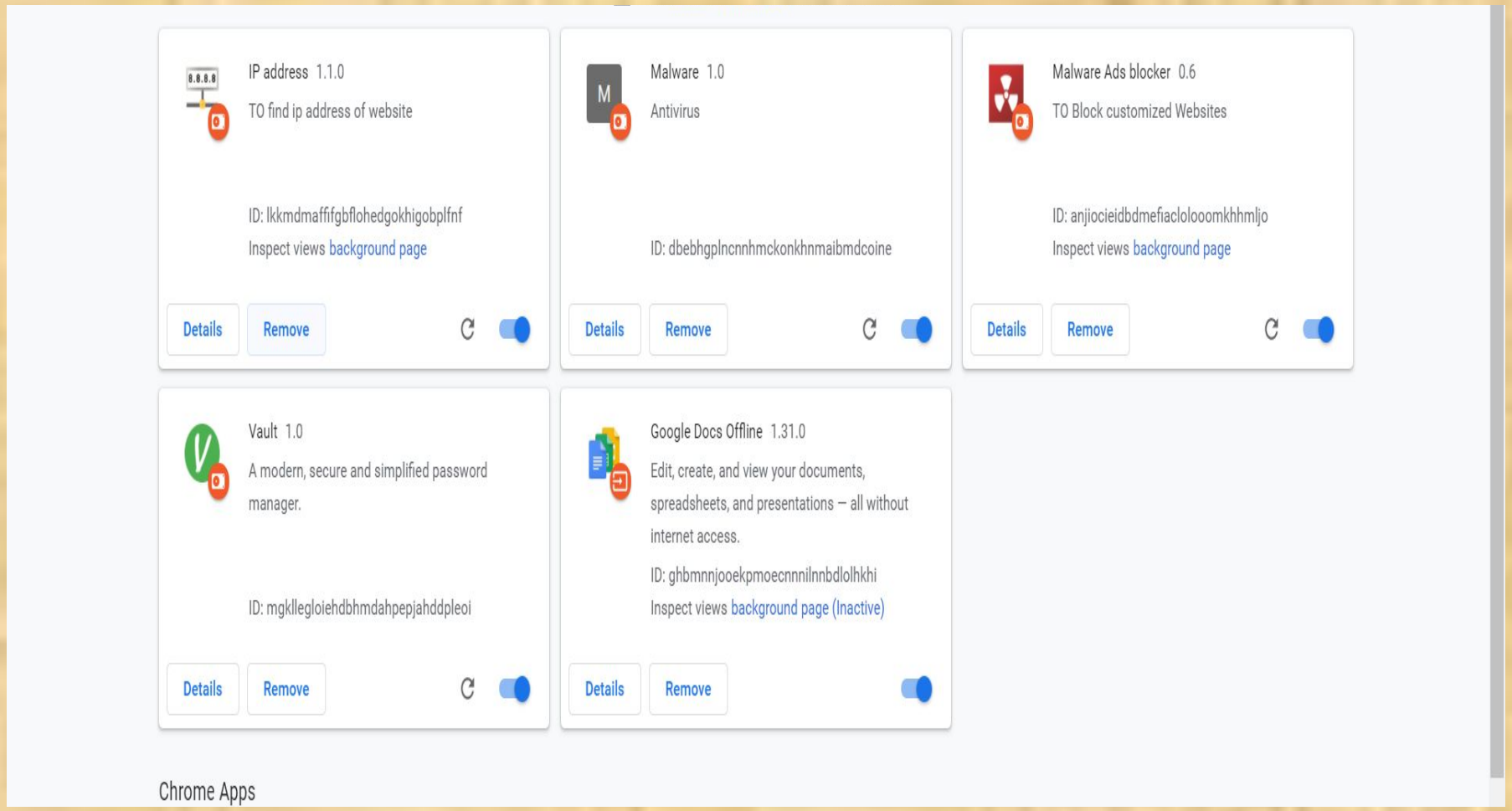
```
def login():
    con = sqlite3.connect('users_final2.db') # connect to the database

    cur = con.cursor() # define a cursor
    #Find user If there is any take proper action
    find_user = ('SELECT * FROM USERS WHERE email = ? and password = ?')
    cur.execute(find_user,[(entry_1.get()),(entry_2.get())])
    results = cur.fetchall() # fetch all the found entries
    if results:
        spawn_program_and_die(['python','homepage_GUIFirewall.py'])
    else:
        ms.showerror('Oops!','Email or Password is Wrong.')
```

Screenshots for Content/Folder BruteForcing:



Chrome extension screenshots

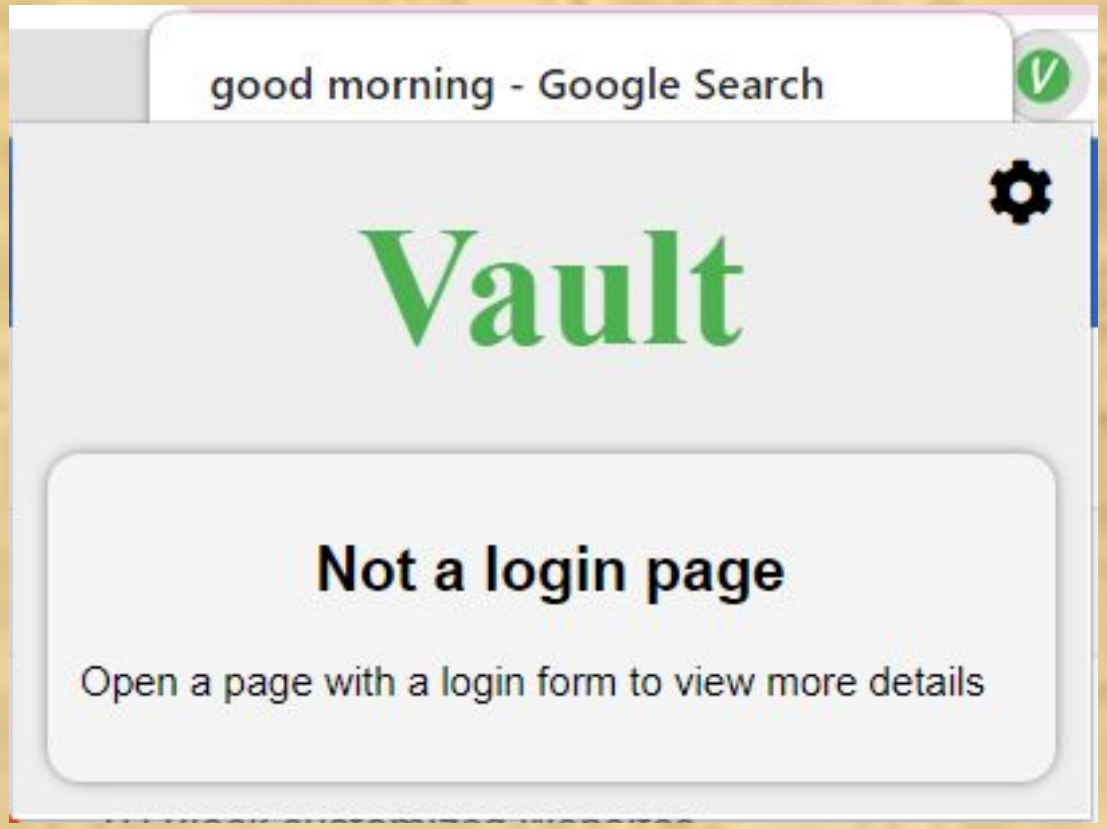
Screenshot 1:



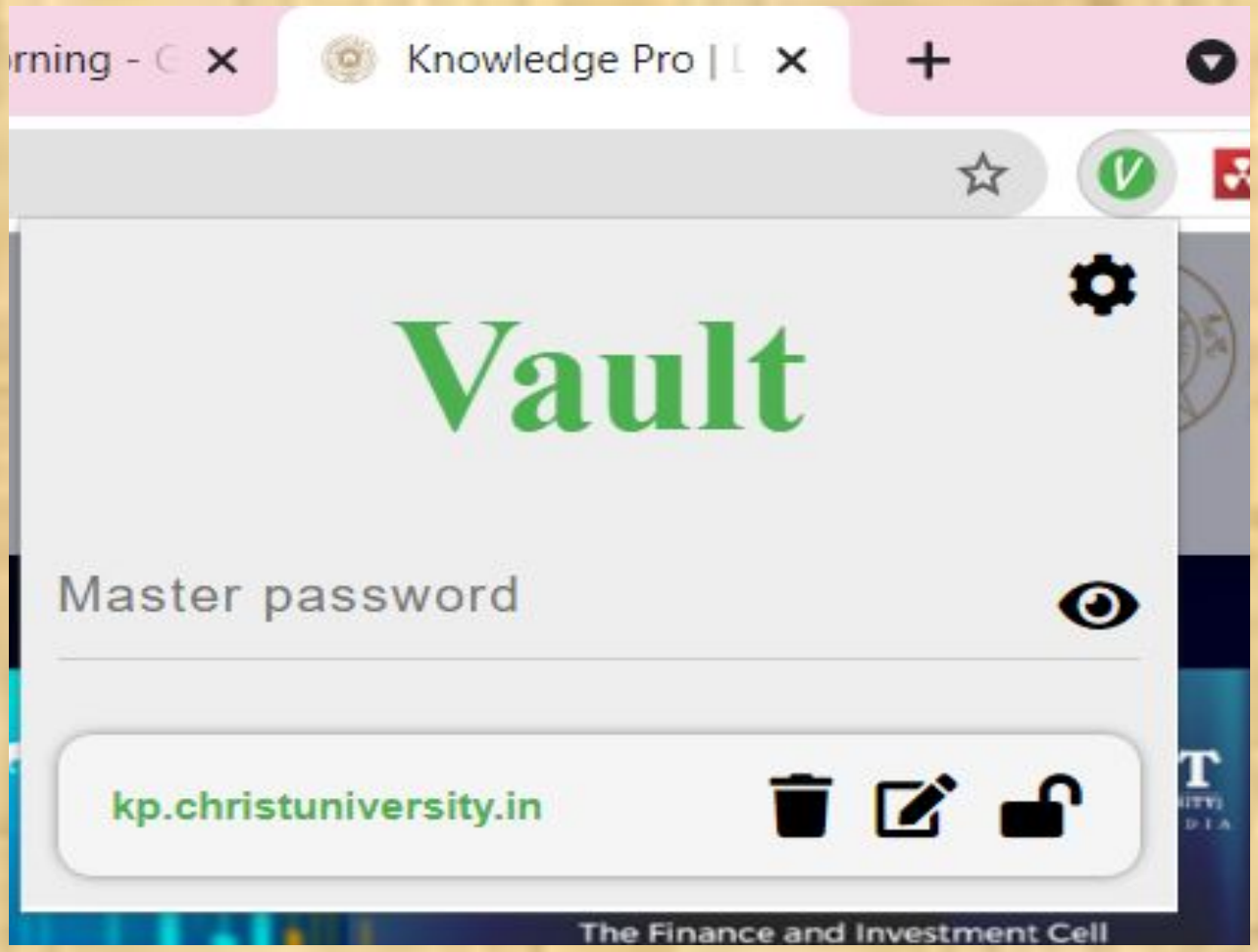
Screenshot 2:

Screenshot 3:

Screenshot 4:

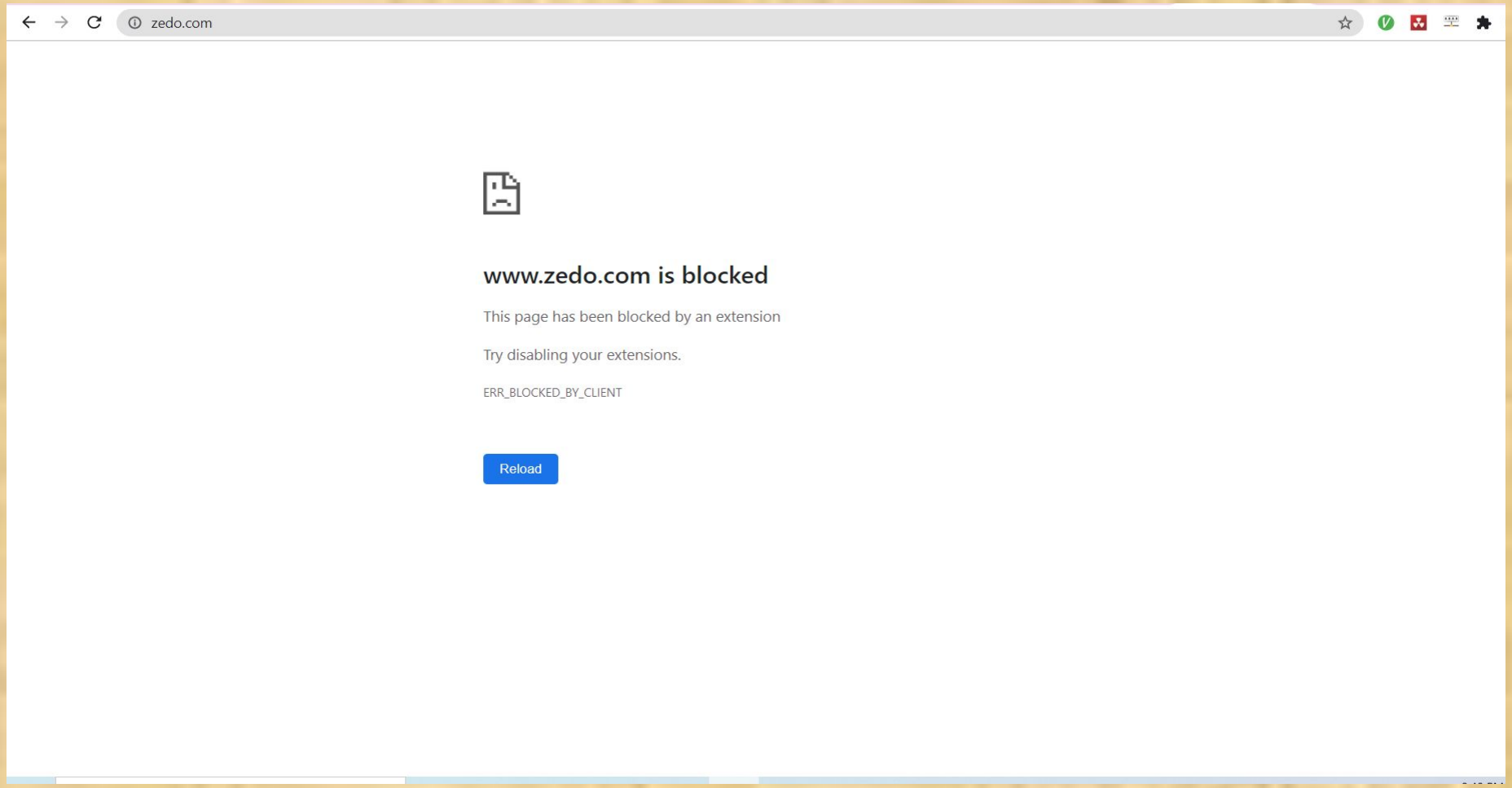


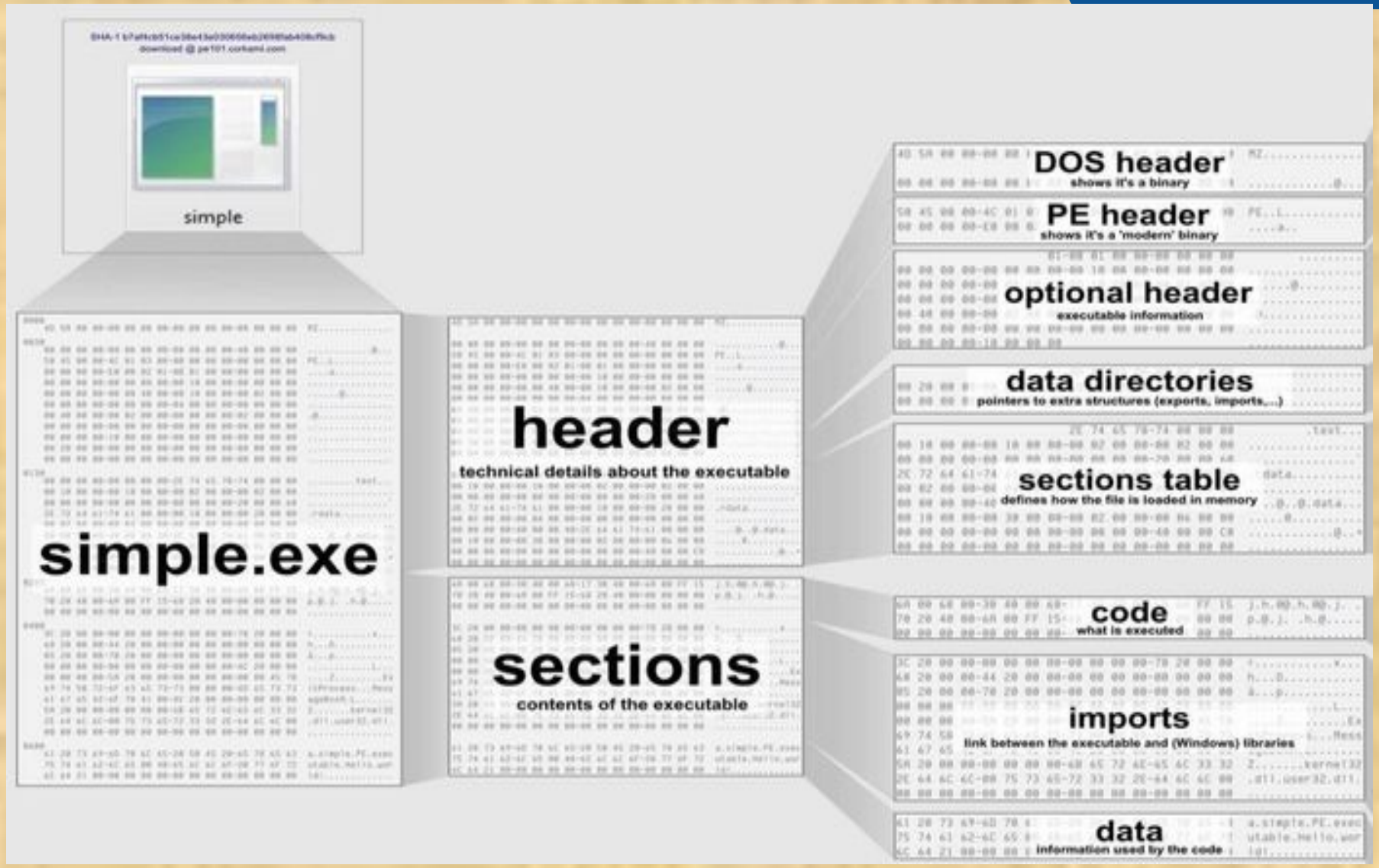
Screenshot 5:



Screenshot 7:

Screenshot 6:




simple
simple.exe
header
technical details about the executable
sections
contents of the executable
DOS header
shows it's a binary
PE header
shows it's a 'modern' binary
optional header
executable information
data directories
pointers to extra structures (exports, imports,...)
sections table
defines how the file is loaded in memory
code
what is executed
imports
link between the executable and (Windows) libraries
data
information used by the code

```
----------DOS_HEADER----------

[IMAGE_DOS_HEADER]
0x0         0x0   e_magic:                       0x5A4D
0x2         0x2   e_cblp:                        0x78
0x4         0x4   e_cp:                          0x1
0x6         0x6   e_crlc:                        0x0
0x8         0x8   e_cparhdr:                     0x4
0xA         0xA   e_minalloc:                    0x0
0xC         0xC   e_maxalloc:                    0x0
0xE         0xE   e_ss:                          0x0
0x10        0x10  e_sp:                          0x0
0x12        0x12  e_csum:                        0x0
0x14        0x14  e_ip:                          0x0
0x16        0x16  e_cs:                          0x0
0x18        0x18  e_lfarlc:                      0x40
0x1A        0x1A  e_ovno:                        0x0
0x1C        0x1C  e_res:
0x24        0x24  e_oemid:                       0x0
0x26        0x26  e_oeminfo:                     0x0
0x28        0x28  e_res2:
0x3C        0x3C  e_lfanew:                      0x78

----------NT_HEADERS----------

[IMAGE_NT_HEADERS]
```

In [15]:
```
from sklearn.model_selection import train_test_split
```

In [16]:
```
# Features
x
# Labels
y = data.label
```

In [17]:
```
X_train, X_test, y_train, y_test = train_test_split(x, y, test_size=0.33, random_state=42)
```

In [18]:
```
from sklearn.naive_bayes import MultinomialNB
clf = MultinomialNB()
clf.fit(X_train,y_train)
clf.score(X_test,y_test)
```

Out[18]:
```
0.9722674661631376
```

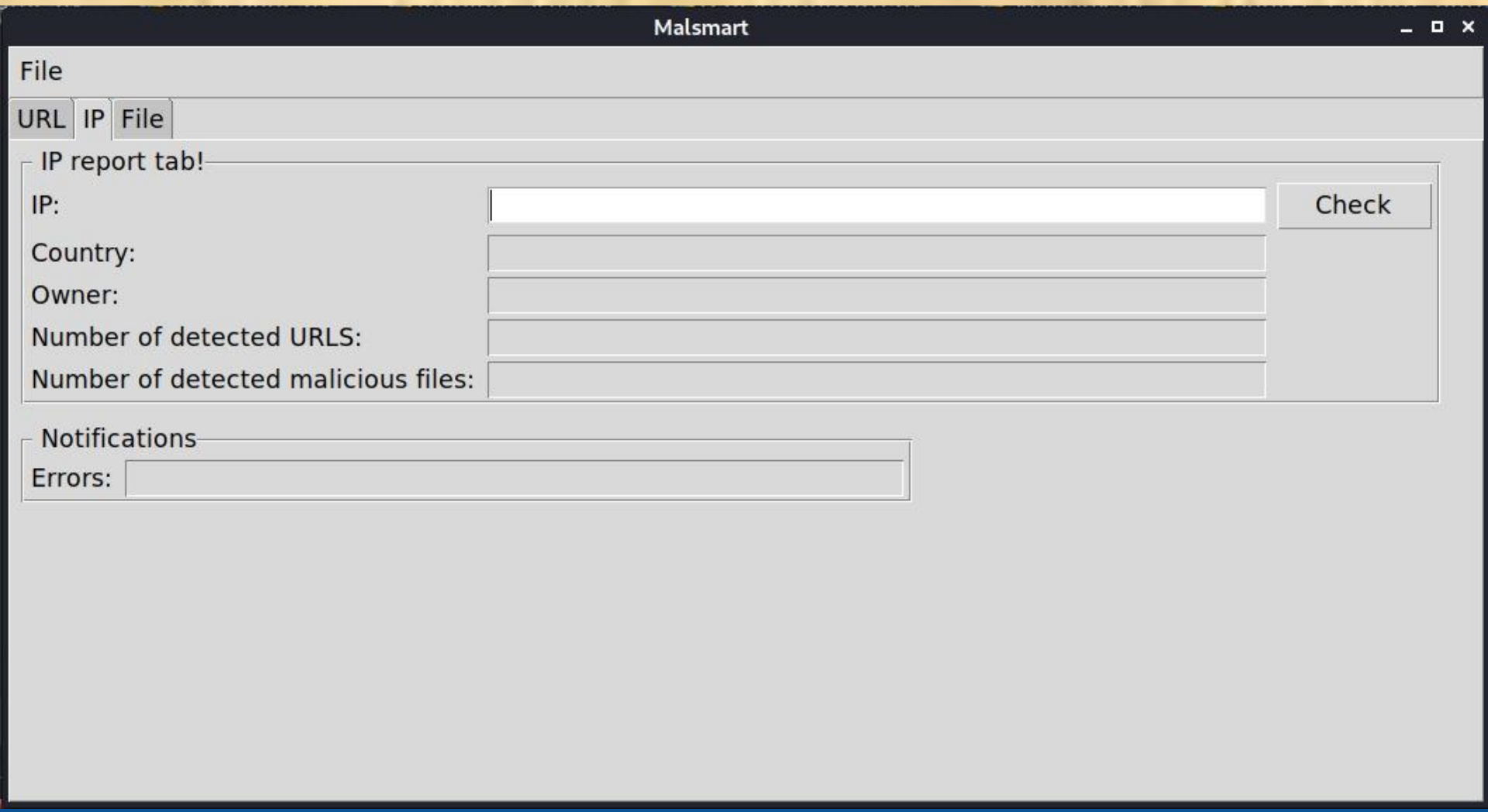
In [19]:
```
print("Accuracy of Model",clf.score(X_test,y_test)*100,"%")
```

```
Accuracy of Model 97.22674661631376 %
```

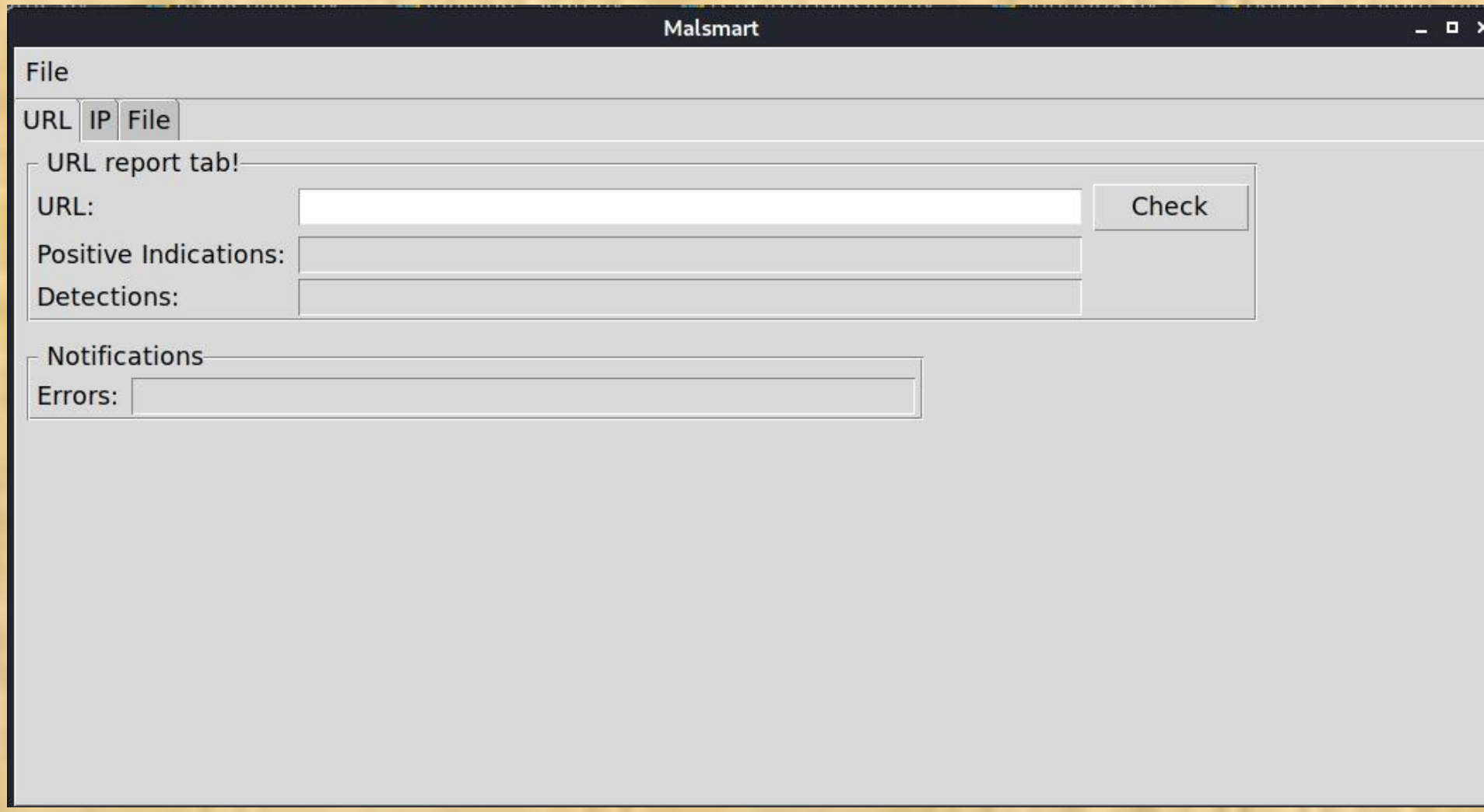
In [20]:
```
sample_url = ["buyfakebillsonlinee.blogspot.com"]
vect = cv.transform(sample_url).toarray()
```

```
Accuracy of Model 97.22674661631376 %
google.com/ not malicious
Accuracy of Model 97.22674661631376 %
google.com/ not malicious
Accuracy of Model 97.22674661631376 %
google.com/ not malicious
Accuracy of Model 97.22674661631376 %
google.com/ not malicious
Accuracy of Model 97.22674661631376 %
radsport-voggel.de/wp-admin/includes/log.exe malicious
Accuracy of Model 97.22674661631376 %
radsport-voggel.de/wp-admin/includes/log.exe malicious
Accuracy of Model 97.22674661631376 %
radsport-voggel.de/wp-admin/includes/log.exe malicious
Accuracy of Model 97.22674661631376 %
radsport-voggel.de/wp-admin/includes/log.exe malicious
Accuracy of Model 97.22674661631376 %
radsport-voggel.de/wp-admin/includes/log.exe malicious
Accuracy of Model 97.22674661631376 %
```

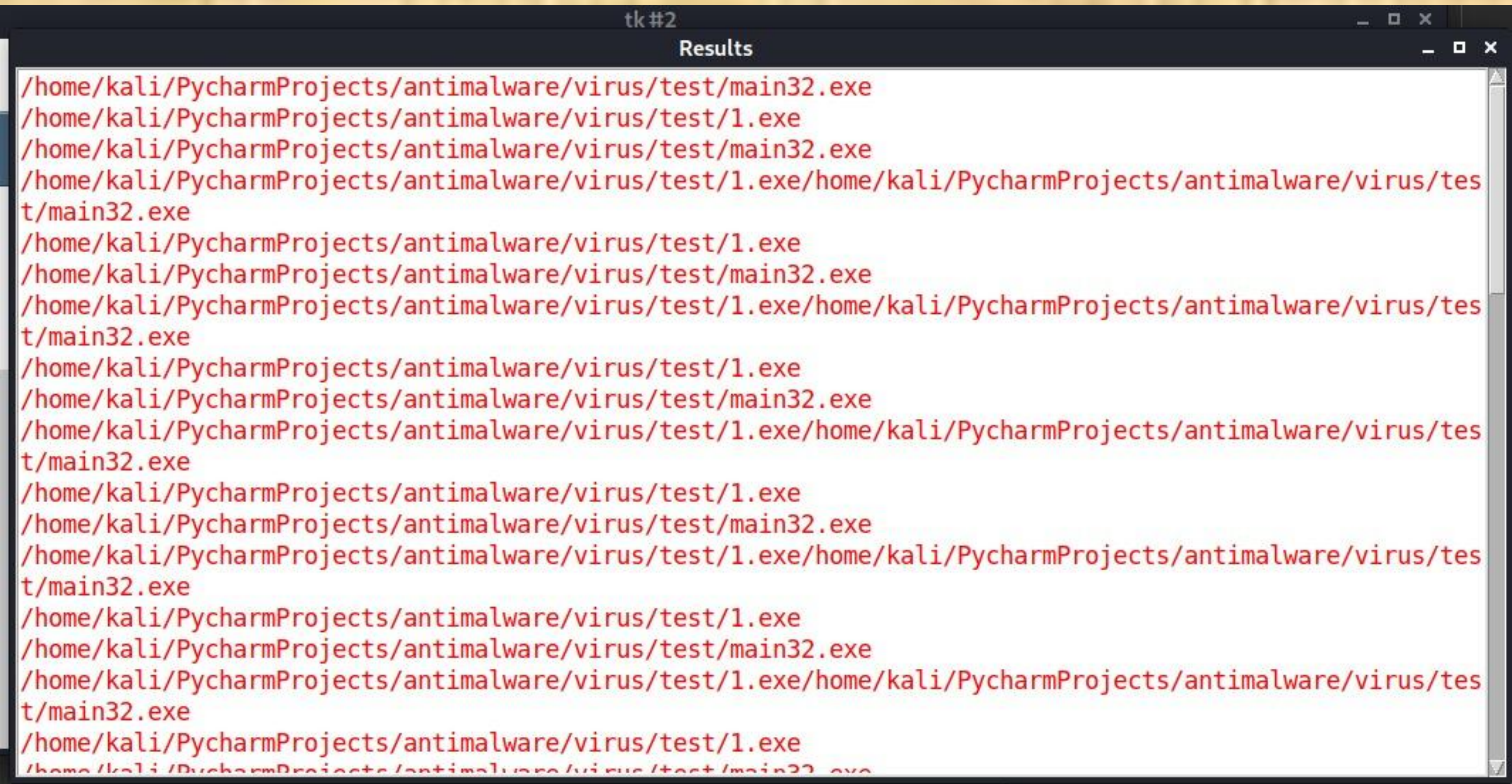
Screenshot 7:



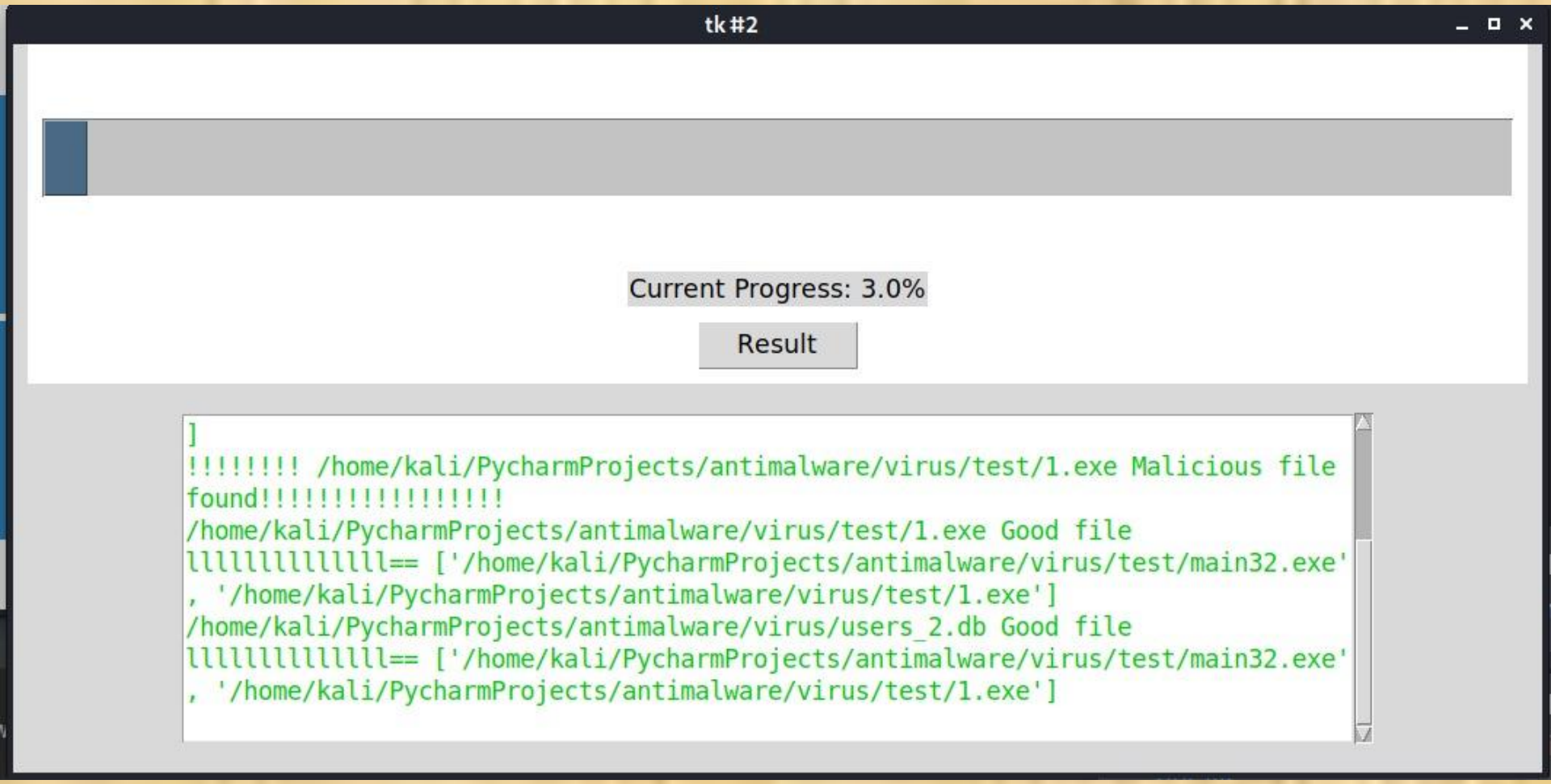
Screenshot 8:



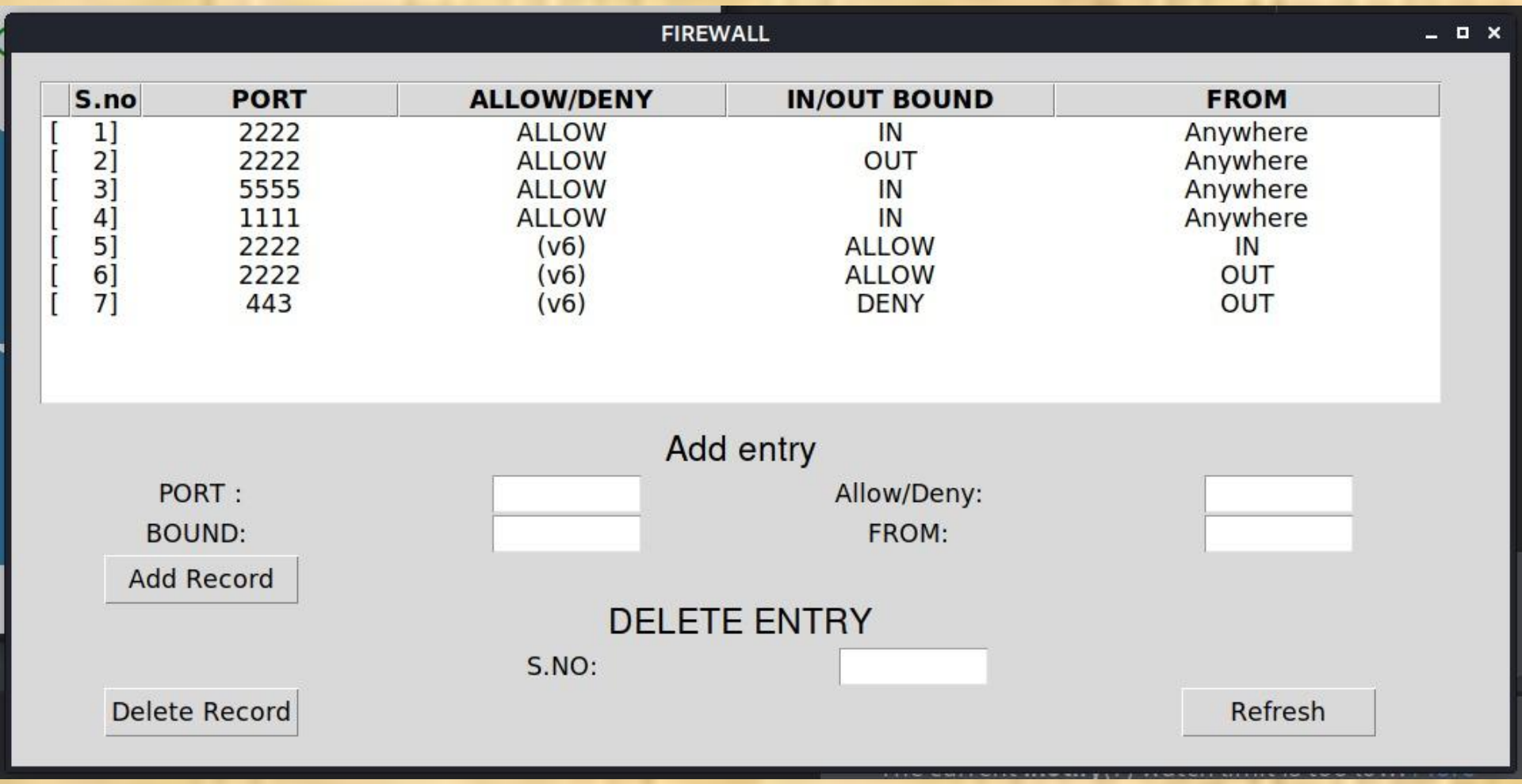
Screenshot 9:



Screenshot 10:



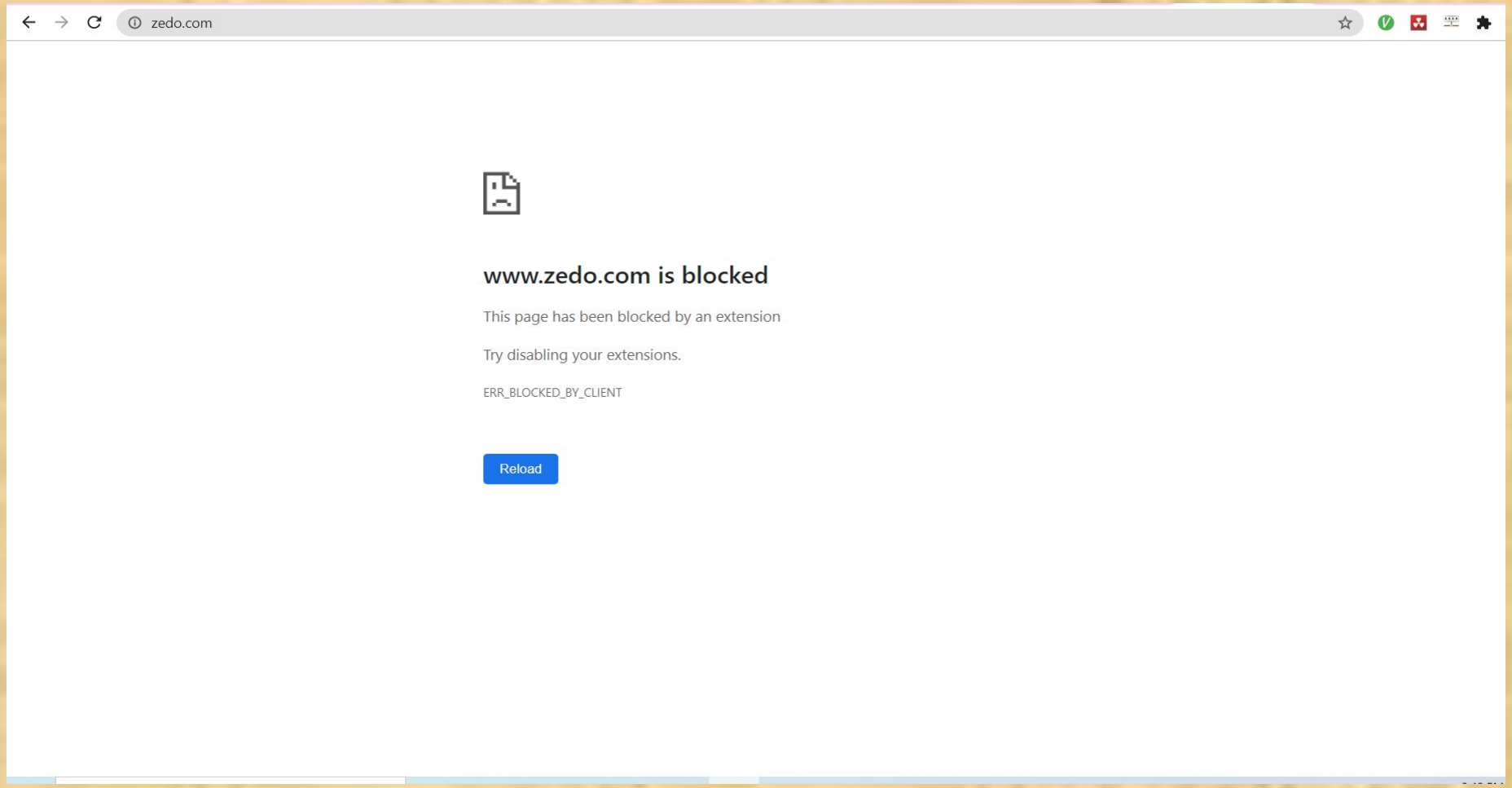
Screenshot 11:



Screenshot 12:

```
class TkinterCustomButton(tkinter.Frame):
    """ tkinter custom button with border, rounded corners and hover effect

        Arguments:  master= where to place button
                    bg_color= background color, None is standard,
                    fg_color= foreground color, blue is standard,
                    hover_color= foreground color, lightblue is standard,
                    border_color= foreground color, None is standard,
                    border_width= border thickness, 0 is standard,
                    command= callback function, None is standard,
                    width= width of button, 110 is standard,
                    height= width of button, 35 is standard,
                    corner_radius= corner radius, 10 is standard,
                    text_font= (<Name>, <Size>),
                    text_color= text color, white is standard,
                    text= text of button,
                    hover= hover effect, True is standard,
                    image= PIL.PhotoImage, standard is None"""
```

Screenshot 13:



Github LInk

https://github.com/AchintyaVatsraj/MalSmart


ANY
QUESTION
?


THANK
YOU