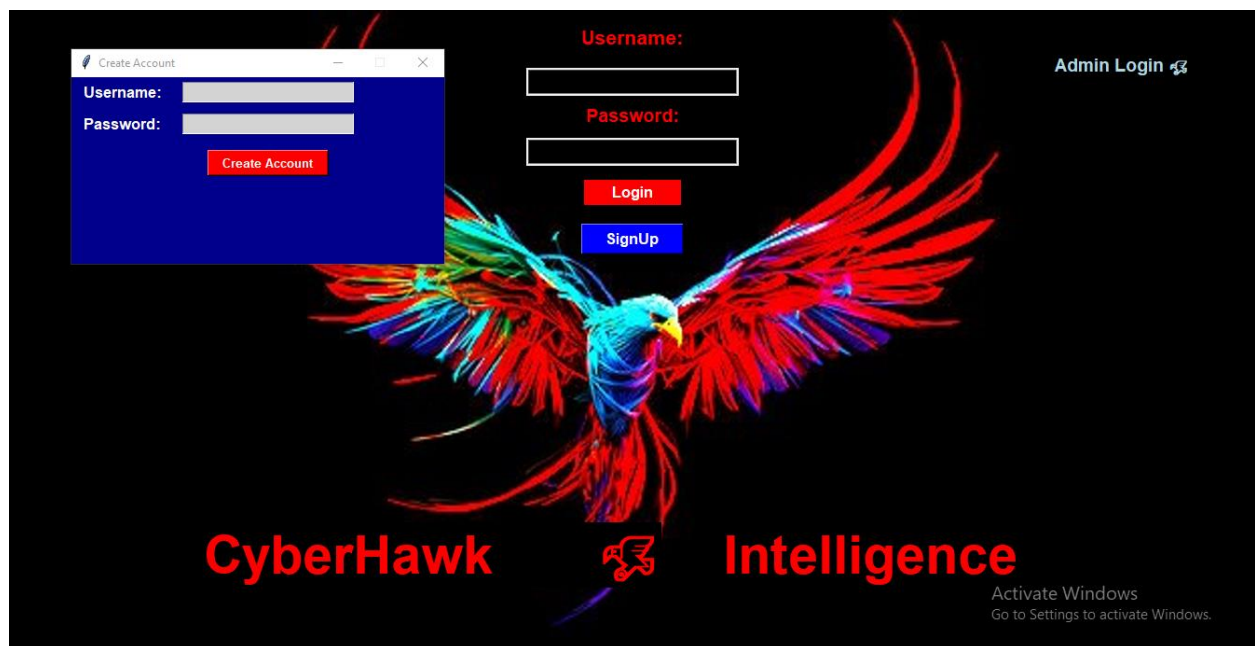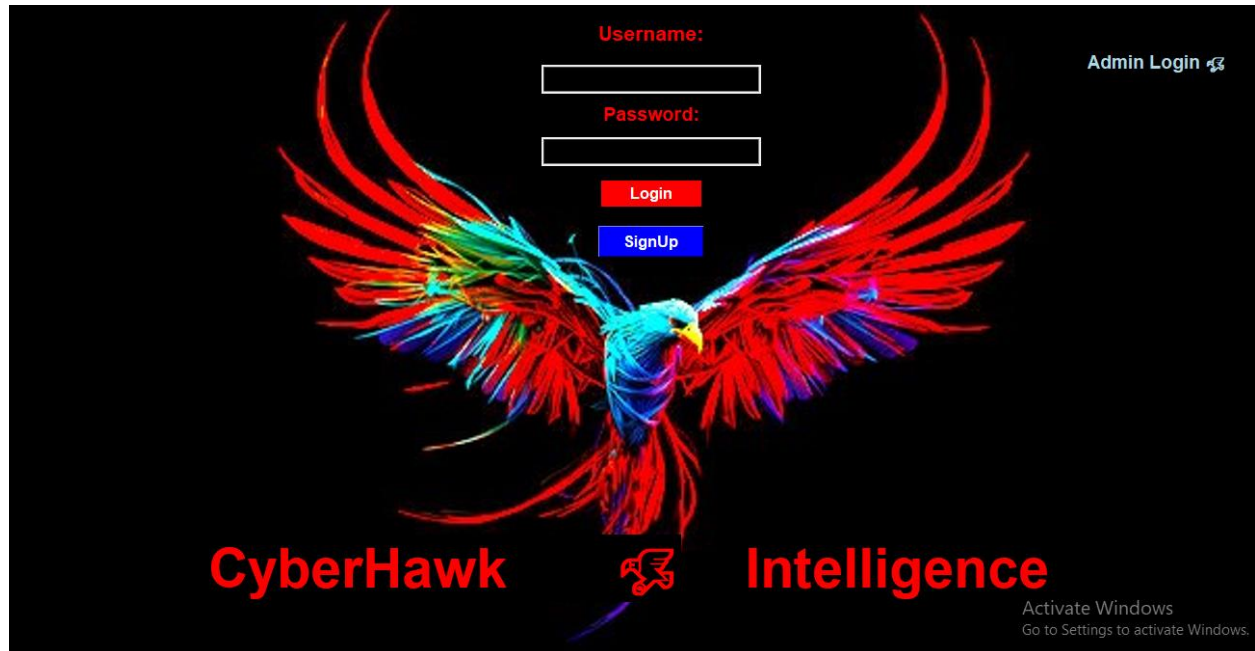# CYBER HAWK INTELLIGENCE

By Michael Edmond odongo

Username:

123

Password:

***

Login

Create Account — □ ✕

Username: random

Password: ***

Create Account

dashboard window — □ ✕

🖧 CLI

Fetch CWEs

File [ ] Browse Scan File

URL: [ ] Scan URL

Search: [ ] Search

enter file name Submit Report

Activate Windows
Go to Settings to activate Windows.

CLI

Tkinter CLI — ☐ ✕

Enter 🐢 command:

```
dir
```

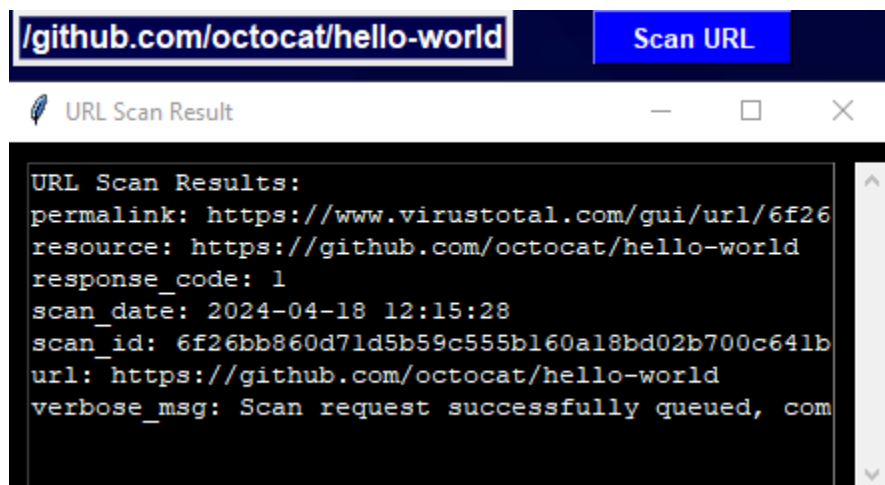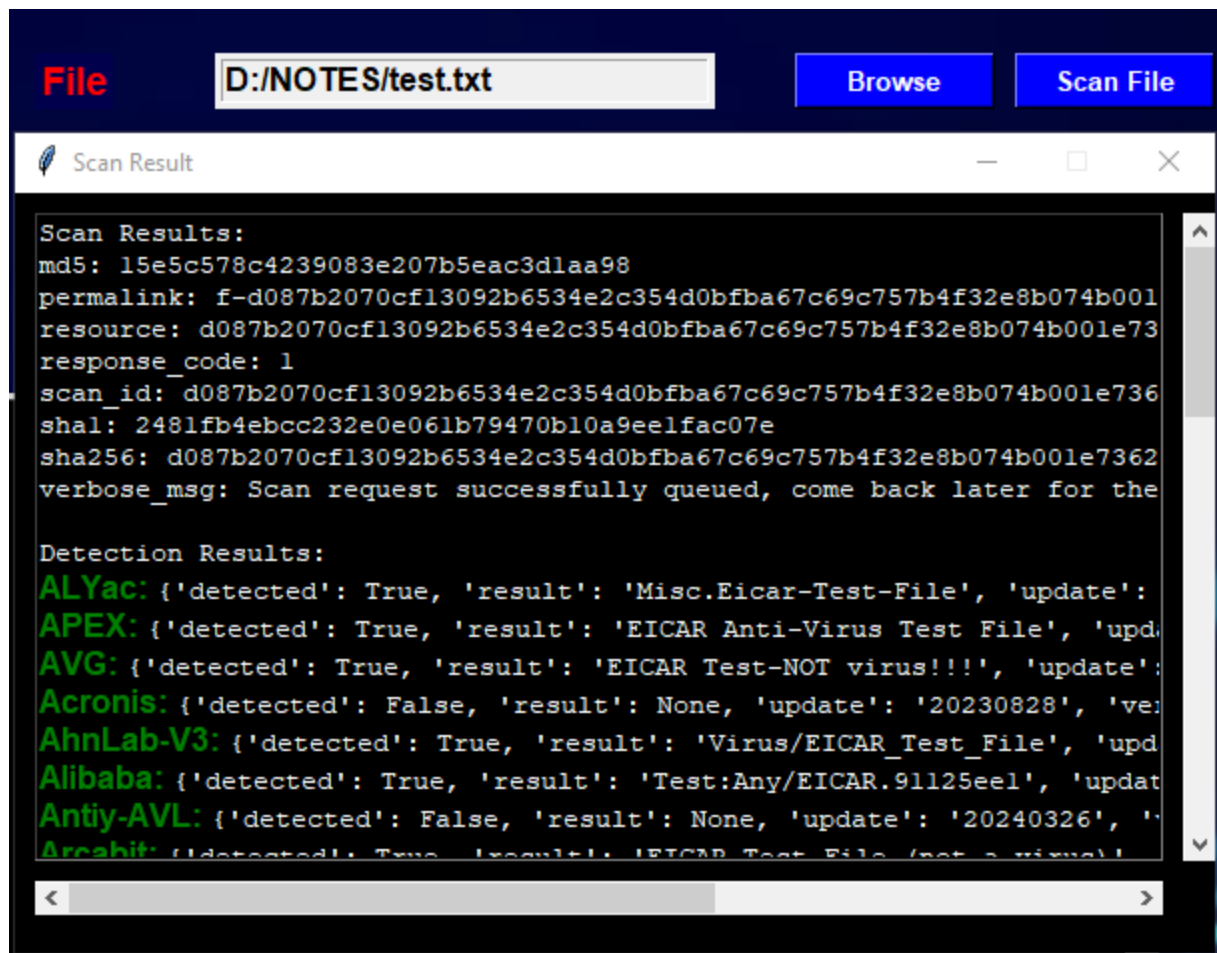**Execute**

```
 Volume in drive C has no label.
 Volume Serial Number is C001-A3AA

 Directory of C:\Users\user\PycharmProjects\MY_INTELLIGENCE
SYSTEM

04/18/2024  02:14 PM    <DIR>          .
04/18/2024  02:14 PM    <DIR>          ..
02/01/2024  12:14 PM    <DIR>          .idea
02/03/2024  01:21 PM           547,792 admin dash2.png
02/03/2024  01:06 PM         1,229,019 admin dashboardl.png
01/31/2024  12:37 PM           334,342 admin_background.png
01/20/2024  10:51 AM           380,929 background6.png
02/01/2024  12:02 PM                85 config.ini
02/03/2024  01:26 PM            80,149 dash_admin.png
```

Fetch CWEs

Weakness Types (CWEs) — ☐ ✕

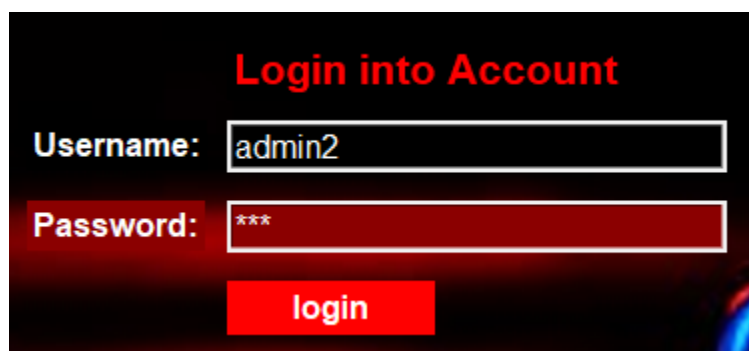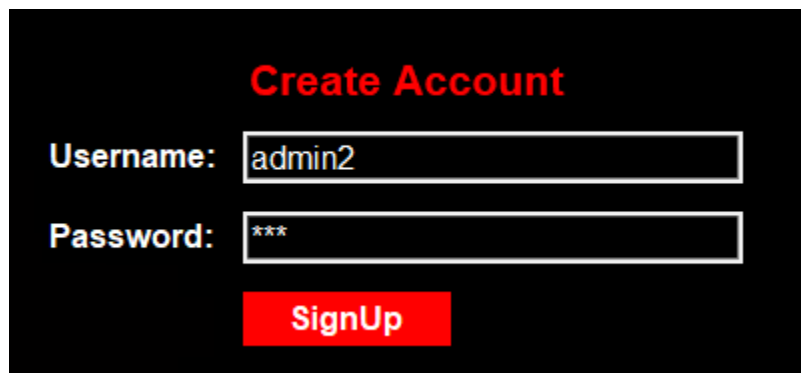| CWE ID	Name	Description
CWE-843	Access of Resource Using Incompati	The program allocates or initializes a
CWE-824	Access of Uninitialized Pointer	The program accesses or uses a poin
CWE-770	Allocation of Resources Without Lim	The software allocates a reusable res
CWE-670	Always-Incorrect Control Flow Imple	The code contains a control flow pat
CWE-294	Authentication Bypass by Capture-re	A capture-replay flaw exists when th
CWE-290	Authentication Bypass by Spoofing	This attack-focused weakness is caus
CWE-639	Authorization Bypass Through User-(	The system's authorization functiona
CWE-120	Buffer Copy without Checking Size o	The program copies an input buffer t
CWE-312	Cleartext Storage of Sensitive Inform	The application stores sensitive infor
CWE-319	Cleartext Transmission of Sensitive Ir	The software transmits sensitive or se

File D:/NOTES/test.txt **Browse** **Scan File**

Scan Result — □ ✕

```
Scan Results:
md5: 15e5c578c4239083e207b5eac3d1aa98
permalink: f-d087b2070cf13092b6534e2c354d0bfba67c69c757b4f32e8b074b001
resource: d087b2070cf13092b6534e2c354d0bfba67c69c757b4f32e8b074b001e73
response_code: 1
scan_id: d087b2070cf13092b6534e2c354d0bfba67c69c757b4f32e8b074b001e736
sha1: 2481fb4ebcc232e0e061b79470b10a9ee1fac07e
sha256: d087b2070cf13092b6534e2c354d0bfba67c69c757b4f32e8b074b001e7362
verbose_msg: Scan request successfully queued, come back later for the

Detection Results:
```
ALYac: {'detected': True, 'result': 'Misc.Eicar-Test-File', 'update':
APEX: {'detected': True, 'result': 'EICAR Anti-Virus Test File', 'upd
AVG: {'detected': True, 'result': 'EICAR Test-NOT virus!!!', 'update':
Acronis: {'detected': False, 'result': None, 'update': '20230828', 've:
AhnLab-V3: {'detected': True, 'result': 'Virus/EICAR_Test_File', 'upd
Alibaba: {'detected': True, 'result': 'Test:Any/EICAR.91125ee1', 'updat
Antiy-AVL: {'detected': False, 'result': None, 'update': '20240326', '
Arcabit: {'detected': True, 'result': 'EICAR Test File (not a virus)'

/github.com/octocat/hello-world **Scan URL**

URL Scan Result — □ ✕

```
URL Scan Results:
permalink: https://www.virustotal.com/gui/url/6f26
resource: https://github.com/octocat/hello-world
response_code: 1
scan_date: 2024-04-18 12:15:28
scan_id: 6f26bb860d71d5b59c555b160a18bd02b700c641b
url: https://github.com/octocat/hello-world
verbose_msg: Scan request successfully queued, com
```
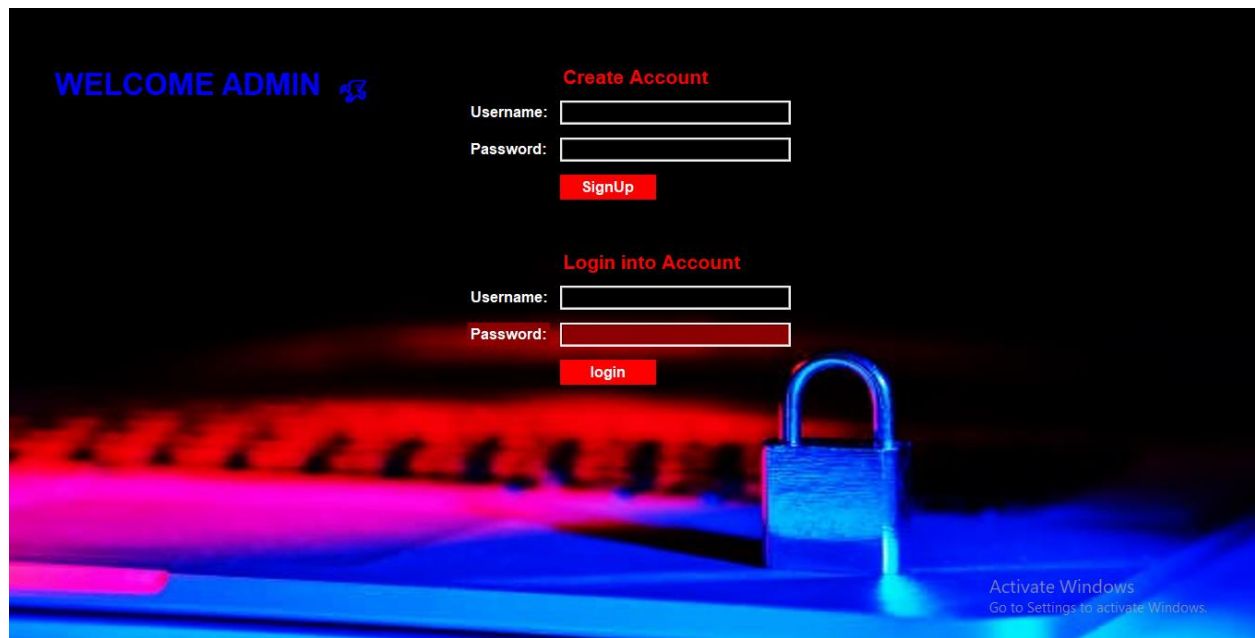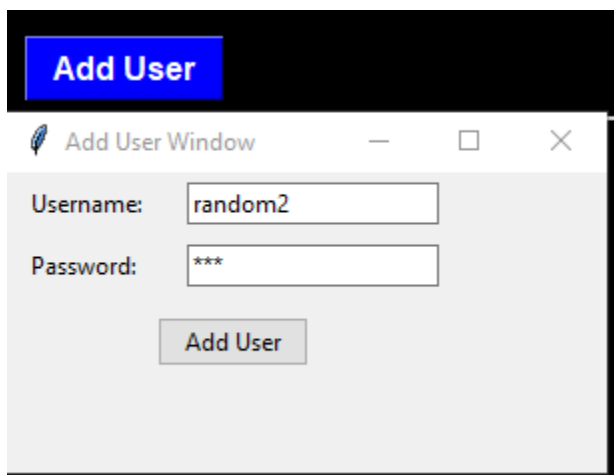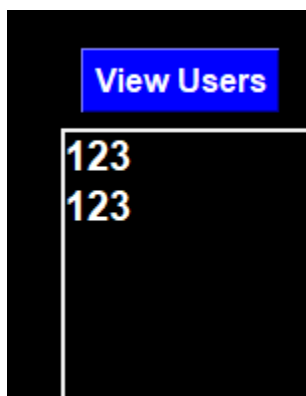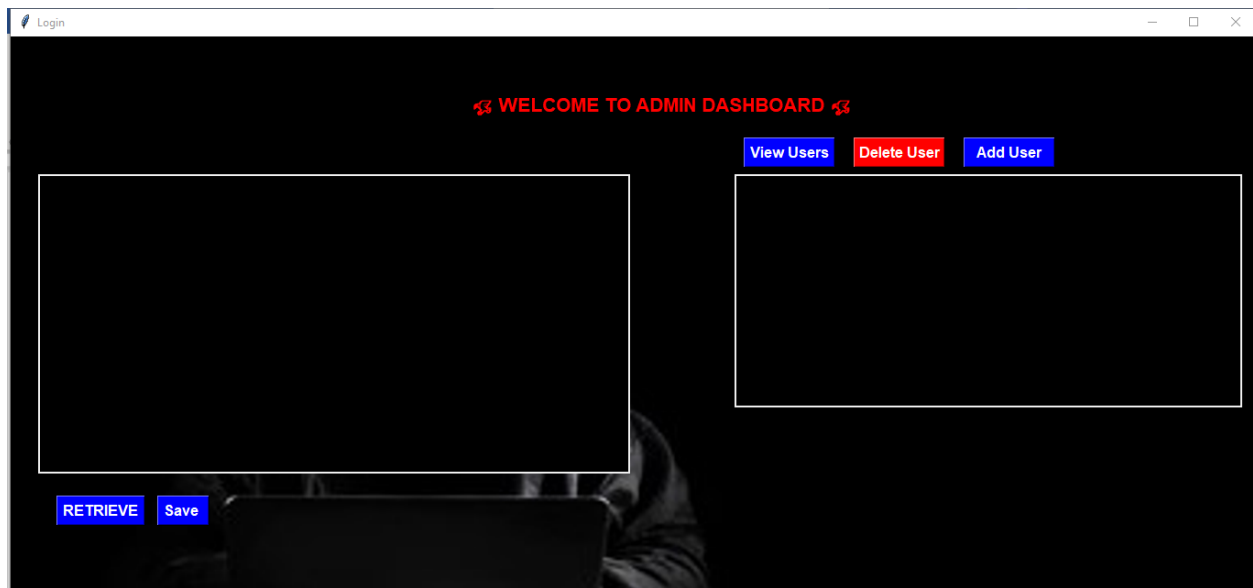
Search: example.com [Search]

Search Result — □ ✕

 Search Results:
Alexa domain info: example.com is one of the top 10,000 sites in the w
BitDefender domain info: This URL domain/host was seen to host badware
WOT domain info: {'Child safety': 'Excellent', 'Privacy': 'Excellent',
Webutation domain info: {'Adult content': 'no', 'Safety score': 100, '
detected_communicating_samples: [{'date': '2024-04-16 14:52:08', 'posi
detected_downloaded_samples: []
detected_referrer_samples: [{'date': '2024-04-18 12:12:57', 'positives
detected_urls: [{'positives': 1, 'scan_date': '2023-10-22 06:02:22', '
domain_siblings: []
pcaps: ['bc9cdc432eeedf0d60014e23306bcb24bf947ff176fcf87a8d7e53bb86657
resolutions: [{'ip_address': '1.1.1.1', 'last_resolved': '2023-03-09 1
response_code: 1
subdomains: ['www.example.com', 'ns2.example.com', 'ns1.example.com',
undetected_communicating_samples: [{'date': '2024-04-14 15:47:12', 'po
undetected_downloaded_samples: [{'date': '2024-04-17 15:28:34', 'posit
undetected_referrer_samples: [{'date': '2024-04-18 12:15:52', 'positiv
undetected_urls: [['http://example.com/', '2a1b402420ef46577471cdc7409
verbose_msg: Domain found in dataset
whois: Creation Date: 1995-08-14T04:00:00Z

this is my report

report name [Submit Report]

WELCOME ADMIN

Create Account

Username: [   ]

Password: [   ]

[SignUp]

Login into Account

Username: [   ]

Password: [   ]

[login]

Create Account

Username: [admin2]

Password: [***]

[SignUp]

Login into Account

Username: [admin2]

Password: [***]

[login]

random2

```
myreport: this is my report

REVIEW: i did the scan and generated the following report  for review

scan: this is my scan
```

RETRIEVE **Save**

File name:		∨
Save as type:	Text files	∨
Folders		Save	Cancel

Save

```
38 | admin2   | $2b$12$XMHSU1M7fF1FRQOM2Frz6uy.pJqWw4TM.9Q/U11BJE7EV1194eQh1 | admin |
39 | random2  | $2b$12$YMujh.fNZ9XkEcF5o/tEUOSzXchV2sKo33xMz4j4eBDhl.lSShsbO | user  |
----+---------+--------------------------------------------------------------+------+
```