

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.

The image is a composite of three screenshots illustrating a security vulnerability. The leftmost screenshot shows a web browser at <https://192.168.3.44/signup> displaying the 'SocialSphere' signup form. The form has two steps: 'Enter Details' and 'Verify Email'. The 'Enter Details' step is active, showing fields for Email (PARISHAMEERUT@GMAIL.COM), Username (parisha), Full Name (parisha), and Password (masked with dots). There is a 'Send OTP' button and a 'Continue with Google' link. The middle screenshot is a terminal window showing a Python script using pynput and logging to create a keylogger. The script logs key presses to 'keylog.txt'. The output shows several key presses: '5', '8', '3', '1', '9', and '4'. The rightmost screenshot shows the 'SocialSphere' OTP verification page. It indicates 'OTP sent successfully! Please check your email.' and has an 'Enter OTP' field. There are 'Back' and 'Verify OTP & Create Account' buttons. A 'Log in' link is at the bottom.

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.