Pre-Account Takeover via Insecure Logic Registration Flow

Summary:

A **Pre-Account Takeover** vulnerability exists in the registration flow due to missing email ownership verification. An attacker can register an account using the victim's email address and **enable 2FA (Two-Factor Authentication)** on the account. When the victim later tries to register or reset their password, they are blocked by the 2FA configured by the attacker, effectively locking them out of their own account.

Vulnerability Type:

Pre-Account Takeover with 2FA Lockout

CWE-287: Improper Authentication

Severity: HIGH

Steps to Reproduce (Full Exploit Chain):

1. **Attacker registers an account using their own email**
    a. Go to the registration page.
    b. Use an attacker-controlled email like `attacker@example.com`.
    c. Set any password and complete the registration.
    d. You will find a confirmation link sent to your inbox
    e. Log in successfully.
2. **Attacker accesses profile settings**
    a. Navigate to the account/profile settings page.
    b. Confirm that email address can be updated manually.
    c. There is no any authentication for the new account that I added manually.

3. **Add the 2FA on the edit of profile**
    a. After replacing the victim email with the attacker email
    b. In profile settings before saving add a 2FA
    c. Follow the instructions of the 2FA on the authenticator app
4. **Email verification bypass achieved**
    a. The attacker now owns a fully active account using the victim's email address.
    b. The pending verification flow for the victim's signup becomes useless.
    c. The victim can no longer register or use the email.

PoC Video:
https://drive.google.com/file/d/1bKiQ4h_WuyMmYSSYCjznrYyIiNIJIsOj/view?usp=drivesdk

Final Result:

The attacker fully takes over an account associated with the victim's email address.
The victim is unable to register or reset the account.
The attacker gains persistent control via 2FA.
No proof of email ownership is ever verified.

Impact:

Permanent account takeover before the legitimate user signs up.
Victim is locked out of the account, even with password reset.
Brand trust & legal implications (e.g., GDPR violations).

Recommendations:

1. **Enforce strict email ownership verification before account activation**
    a. Do **not allow login**, access to settings, or 2FA setup until the email is fully verified.
    b. Pending registrations should not be usable until email confirmation is completed.
2. **Prevent email change without ownership validation**
    a. When a user updates their email in the profile:

        i. Send a verification link to the new email address.
        ii. Only apply the change after the user clicks the link and confirms ownership.
        iii. Until then, keep the old email active.
3. **Bind email verification tokens to session or user ID**
    a. Tokens should not be generic or guessable.
    b. A verification token issued to one registration flow **must not** work for a different session or logged-in account.
4. **Restrict 2FA activation until after email verification**
    a. Users should only be allowed to enable 2FA after confirming email ownership to prevent account lockout abuse.
5. **Prevent duplicate email registration or changes across active accounts**
    a. Enforce uniqueness and verify ownership before allowing any email to be reused in any form (registration or profile update).
6. **Invalidate all sessions and 2FA after password reset**
    a. In case a legitimate user resets the password, all previous sessions and 2FA setups should be invalidated unless re-verified.
7. **Notify both old and new email addresses of any change**
    a. If an email is changed, notify both the old and new addresses about the change and offer a way to revert if unauthorized.