Bug Bounty

Issue No. 1

Impact

It leads to page admin disclosure which is a serious issue.

A page admin will post a story to their personal account instead of the Page when messaging from the Page inbox on FBLite and hitting "Add to Story"

Steps

1.UserA sends a photo to UserB through the page.

2. UserA clicks on Add to story option

3. The photo is added to the UserA's story instead of Page's story which is leading to page admin disclosure.

Issue No. 2

Steps :

1. User A goes to his PageX's inbox through fblite and sees UserB's message thread

2. UserA messages to User B

3.User B receives the text message done by UserA through page's id

4. UserA now sends photo to UserB through the page inbox.

5. UserB receives the photo message through UserA's personal profile id instead of the page id which leads to page admin disclosure.

Noticed Facebook bugs:

Bug 1

My friend had started a Facebook page to post funny videos.

One video was very funny. I knew his fb id and also that he is the admin of the page.

Example admin id- xxxx

While viewing a video, I simply right clicked, View Page Source, searched xxxx.

Boom! One result found.

The page source was leaking the id of the person who was the content owner.

Bug 2

Users could have made a messenger call to the victim's account and then receive the call from the victim's locked Android phone to use the 'Watch Together' feature from the call screen without unlocking the phone thus allowing the intruder to get access to all of the saved videos & Watch History of the Facebook user. So, basically; the vulnerability here was that Facebook was allowing users to use such a sensitive feature like Watch Together even from a locked state of the device. Facebook patched this one along with similar such vulnerabilities by asking first to unlock the phone before using such sensitive features from a locked Android phone.

Bug 3

We can create fundraisers for nonprofits and personal causes on Facebook. We can add our friends as organizers in the fundraisers we created. They need to approve our invitation to become an organizer. Once they approved the invitation an attacker was able to block the victim and thus victim was unable access the fundraiser and remove themself as an organizer from the fundraiser. An attacker could use this for their personal benefits.

Steps:

1)Attacker creates a fundraiser and invites victim as an organizer

2) Once victim accepts the invitation, attacker blocks the victim..

3) Victim is now unable to access the fundraiser but others can still see the victim as an organizer of the fundraiser.