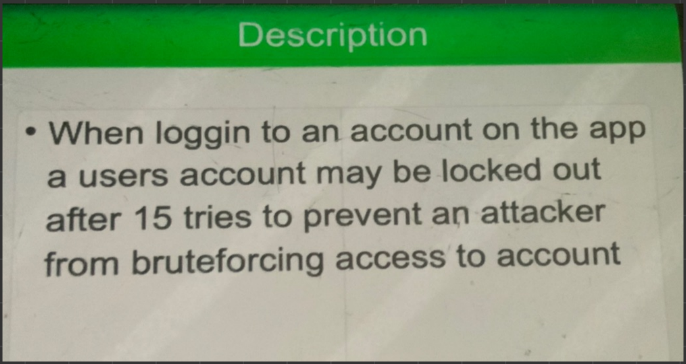
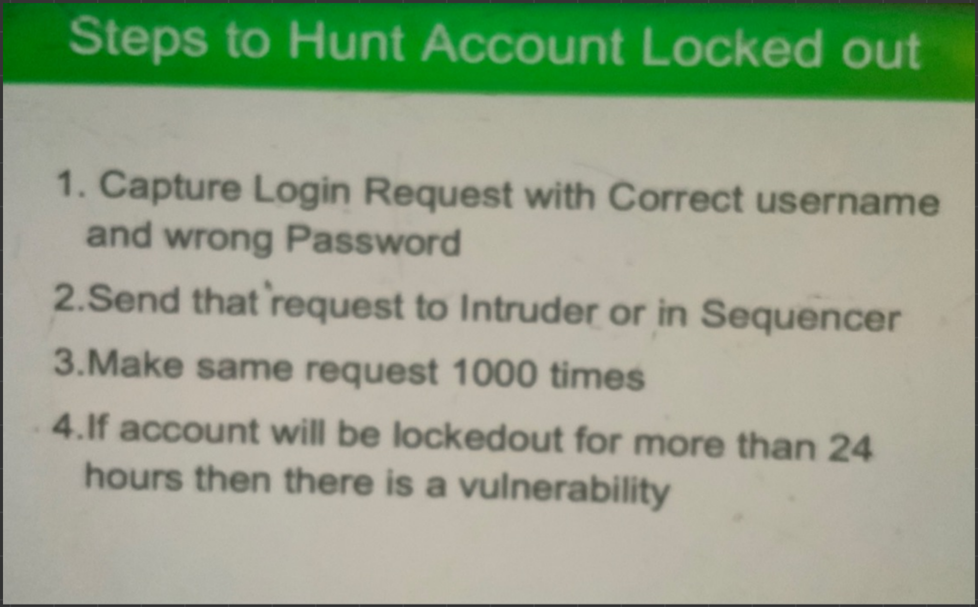


Description

- When loggin to an account on the app a users account may be locked out after 15 tries to prevent an attacker from bruteforcing access to account

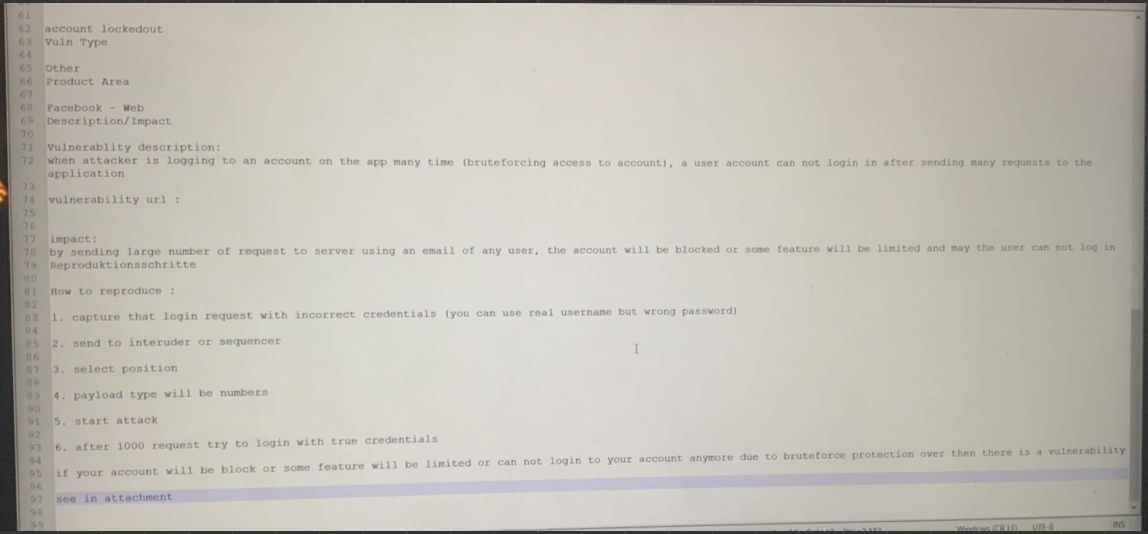
faceBook
↓
login page
↓
{ email:
password:

if bruteforce protection is enable, it will block your account after trying many times



Steps to Hunt Account Locked out

1. Capture Login Request with Correct username and wrong Password
2.Send that request to Intruder or in Sequencer
3.Make same request 1000 times
4.If account will be lockedout for more than 24 hours then there is a vulnerability



account lockedout
Vuln Type

Other
Product Area

Facebook - Web
Description/Impact

Vulnerablity description:
when attacker is logging to an account on the app many time (bruteforcing access to account), a user account can not login in after sending many requests to the application

vulnerability url :

impact:
by sending large number of request to server using an email of any user, the account will be blocked or some feature will be limited and may the user can not log in
Reproduktionsschritte

How to reproduce :

1. capture that login request with incorrect credentials (you can use real username but wrong password)

2. send to interuder or sequencer

3. select position

4. payload type will be numbers

5. start attack

6. after 1000 request try to login with true credentials

if your account will be block or some feature will be limited or can not login to your account anymore due to bruteforce protection over then there is a vulnerability

see in attachment