2FA Bypass

Description:
2FA is an additional layer of security of online accounts but weak implementation of 2FA gives attackers upper hand in carrying out malicious actions.
There are multiple ways to Bypass 2FA

1. Status Code Manipulation : Attackers can manipulate the HTTP status code and try to bypass the 2FA.
Attack Scenario : Attacker changing 4xx to 200 OK status code .

2. No Brute Force Prevention: If the application does not have any bruteforce prevention , then attackers can bruteforce the OTP.
Attack Scenario : Set Payload on 2FA using Burp Suite and start Bruteforce attack, Check the status code .

3. Lack of CSRF Prevention can lead to disabling of 2FA : If there is no/weak implementation of CSRF, then attacker can leverage this to disable the 2FA of Victim account
Attack Scenario: Disable 2FA of Account 1 and create CSRF POC for it . Fire the request from the victim account , If there is no CSRF Protection 2FA will get disabled.

4. Response Manipulation: If there is no proper validation in place , then using response manipulation 2FA can be bypassed
Attack Scenario: Enter correct OTP and capture the request, See the response in Burpsuite and copy the correct response. Now Enter random OTP and capture the request and see it's response , Now Replace incorrect response with correct response and forward it, It will get bypassed.
"Success" : False ---> "Success" : True

5. Using Null/ 000000 : Due to incorrect comparison of entered code with true code, Null can be used to bypass 2FA. Attackers try to bypass 2FA using Null or 000000.

6. JS File Analysis: If any application use Dynamic JS FIles to store/copy OTP, which is matched against the OTP which is entered by User [Client Side Validator]. Hence analyze all JS file when 2FA is triggered .

7. Code Reusability: Due to improper validation/code expiration , attackers can sometimes re-use Same code to bypass 2FA.
Attack Scenario : Request 2FA and use it, After using it , re use the same code , if it works then application is vulnerable.

8. 2FA gets disabled due to Email/Password Change : This can be exploited when 2FA gets disabled when password or email of the account is changed.

9. Backup Code Abuse: Sometimes an application provides some Backup codes to reset things,
Any of the above method can be used to test the weak implementation of Backup code.