Bypassing two factor authentication

Saturday, December 21, 2019 7:05 PM

1. Bypassing 2fa using conventional session management

This method is about bypassing the two factor authentication mechanism using password reset functions. In almost all web applications the **password reset function automatically logs the user into the application** after the reset procedure is completed

To Change Password > Request Password Reset Token > Use Password Reset token > Login to the web application

---

2. Bypassing 2fa Via OAuth mechanism

As it is observed that in this process flow there is no intervention of 2fa. An attacker can potentially abuse this mechanism and utilize a **OAuth integration to log into the web application** rather than using the username and password to do so (Shah, 2014).

Note:
For this bypass to work the attacker must have access to the OAuth integration account to login on behalf of the user

Site.com requests Facebook for OAuth token > Facebook verifies user account > Facebook send callback code > Site.com logs user in

---

3. Bypassing 2fa via brute force

Usually the length of the 2fa code is 4 to 6 characters which often is numbers, and that makes to a possibility 151,800 which in real world scenario is easily brute force able using a normal computer (**NO RATE LIMITING**)

---

4. Bypassing 2fa using race conditions (RARE)

An attacker can **utilize previously used or un used values of tokens to verify the device**. However this technique requires the attacker to have access to the previous generated values, which can be done via reversing the algorithm of the code generation app or intercepting a previously known code.

---

5. Bypassing 2fa using modifies response (Kishan)

Enter correct OTP -> Intercept & capture the response -> logout -> enter wrong OTP -> Intercept & change the response with successful previous response -> logged in

---

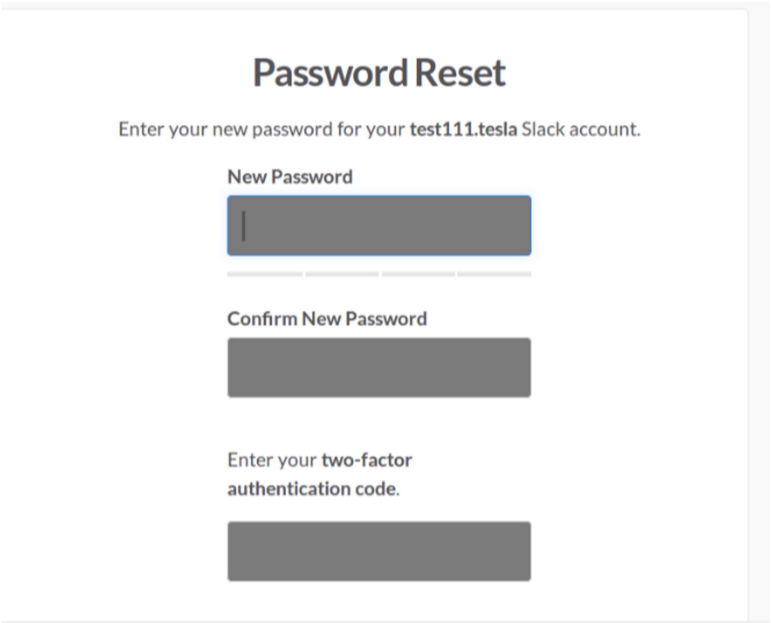
6. Bypassing 2fa using Activation link (RARE)

Able to login with activation link (Activation link is vulnerable and token not expiring)

---

7. Bypassing 2fa in password reset page

Go the password reset page with password reset link



No RATE LIMIT in 2FA

---

8. Bypassing 2fa using backup code request & response (Try your own logic stuffs)

I quickly moved to backup code generation part. So at the account setting page the following sample API request is used to get backup codes.

So the above API request fired in 2nd case of session scenario (defined above) since we are logged in to account. Now what if we fire the same API request using 1st session scenario i.e. when user provide valid email and password but not 2FA code.

So I quickly logged out and logged in again with valid email and password. As expected bountyplease.com redirected me to 2FA page. This time I provided the wrong OTP code and captured the request and made following two changes in request -

1. Replace the original Destination to POST /api/totp_auth HTTP/1.1 2. Replace the original parameters to
{"action":"backup_codes","clusterNum":"000","accountId":"test123","email":"test123@gmail.com"}
And in response I got all the backup codes. Now attacker can put these backup code at 2FA place and get into victim's account.

Thanks,
Surendiran S