Two-Factor Authentication Bypass

BY AHMED SALAH ABDALHFAZ (@ELSFA7110)

Agenda

- What is 2fa ?
- Methods to Bypass two factor Authentication

What is 2fa ?

Two-factor authentication (2FA) adds an extra layer of security to your online accounts by asking for a verification code after you sign in with your email address and password.

The verification code is generated by an application on your smartphone. To gain access to your account a potential attacker would need your email address, your password, as well as your phone. Two factor authentication works on the principle of “Something you have” which in most cases is your handheld phone , There are two method using which the one time code is delivered to your phone.

1. Using a text message
2. Using a third party software (Authy, Google Authenticator)

Methods to Bypass two factor Authentication

1-2FA BYPASS BY RESET PASSWORD LINK (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 (Securityweek, 2016). Most of the time, the 2fa system is not implemented on the login function after the password reset. The process flow works in the following way >

Go To Change Password > Request Password Reset Token > Use Password Reset token > Login to the web application without enter 2fa code

Using this technique the attacker can bypass the two factor authentication in online platforms. Basically the password reset token maintains a session with the application just after the reset has token place, which leads to the bypass.

Methods to Bypass two factor Authentication

2-Leaked Token

Check if the token leaked on a response from the web application!

Sometimes attacker can find the code in the server response and it can be encoded and sometimes it is Base64

Check the server response carefully

Methods to Bypass two factor Authentication

3-Bypassing 2fa via rate-limit

Web developers leave a very disdinctive flaw when they forget to put rate limitation on the input fields, in case of 2fa if the field is not rate limited there is a possibility of brute force attacks using which the attacker can brute force the 2fa code sent to the device (Bullock, 2016). 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 forceable using a normal computer

Link to Report: https://hackerone.com/reports/121696

Methods to Bypass two factor Authentication

4-Bypass 2FA With Refer Header (HTTP-HEADER)

Try to navigate to the page which comes after 2FA or any other authenticated page of the application. If there is no success, change the refer header to the 2FA page URL. This may fool application to pretend as if the request came after satisfying 2FA Condition.

Methods to Bypass two factor Authentication

5- Bypass 2FA by server status code (Response Manipulation)

enter any 2fa code > Intercept the POST request in burp and right-click -> "Do intercept to this request".
So, now our burp with Intercept the Response from the server to this request

edit the server response by replace status code header

HTTP/1.1 400 -> HTTP/1.1 200 OK

HTTP/1.1 403 -> HTTP/1.1 200 OK

Methods to Bypass two factor Authentication

6- Chaining CSRF to disable 2FA

So, What is CSRF!

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a
web application in which they're currently authenticated. With a little help of social engineering
(such as sending a link via email or chat), an attacker may trick the users of a web application into
executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their
email address, and so forth. If the victim is an administrative account, CSRF can compromise the
entire web application.

PoC :

https://www.youtube.com/watch?v=WRBJ6-te72g

Methods to Bypass two factor Authentication

7- 2FA bypass by Sending a Blank Code

How to Test For the bug!

Lets take website.com, go to the 2fa verification page and input some random numbers, and intercept the request with a burp. Now remove the random numbers you entered in the input field. Don't Forward the requests. Just Turn off the intercept. Sometimes, with this method, you can bypass 2fa.

Link to Report: https://hackerone.com/reports/897385

Methods to Bypass two factor Authentication

8- Password-Reset >> disable 2fa (Logical Flaw)

* Create an Account and Turn On 2FA.
* Logout from that account.
* Now, Go to forget Password-Reset page.
* Change your password.
* Now try to log in.
* if you are not asked to enter a 2FA code, You can report.

Methods to Bypass two factor Authentication

9- false to true trick (Response Manipulation)

Response body from the server:

modifing json data: "success":"false" -> "success":"true“

Methods to Bypass two factor Authentication

10- Sharing unused tokens

Check if you can get for your account a token and try to use it to bypass the 2FA in a different account.

Methods to Bypass two factor Authentication

11-Enabling 2FA Doesn't Expire Previous Session

1. Login to the application in two different browsers and enable 2FA from 1st session.

2. Use 2nd session and if it is not expired, it could be an issue if there is an insufficient session expiration issue. In this scenario if an attacker hijacks an active session before 2FA, it is possible to carry out all functions without a need for 2FA