2FA Bugs

@h0tak88r

2FA Setup/Implementation

- 2FA Secret Cannot be Rotated
- 2FA Secret Remains Obtainable After 2FA is Enabled
- Logic Bug in 2FA setup leads to account damage (1)
- Previously created sessions continue being valid after MFA activation
- Enable 2FA without verifying the email
- IDOR to ATO

2FA Bypass

- 2FA Code Leakage in Response
- JS File Analysis
- 2FA Code Reusability
- Lack of Brute-Force Protection
- Lack of rate limit in the user's account when logged in
- Old 2FA Code is Not Invalidated After New Code is Generated
- 2FA Code is Not Updated After New Code is Requested
- Missing 2FA Code Integrity Validation
- Bypass 2FA with null or 000000 or Blanc
- 2FA Referrer Check Bypass | Direct Request
- Misconfiguration of Session permission
- Target use JSON?
- change MFA mode from sms To email
- Bypass Using OAUTH
- Random timeout issue on a Two-Step Verification endpoint

Disable 2FA

- Lack of Brute-Force Protection Disable 2FA
- Disable 2FA via CSRF (Leads to 2FA Bypass)
- Clickjacking on 2FA Disabling Page
- Backup Code Abuse
- Password Reset/Email Check → Disable 2FA
- 2FA can be disabled when logged in without confirming account password (2)
- Logic Bug Disable 2FA