**No Rate Limit**

**Summary:** No Rate Limit is a type of computer security vulnerability typically found in web applications. No Rate Limit enables attackers to perform actions on the web application where the attacker can do signup creation, password reset or 2FA of other users. No Rate Limit vulnerability may be used by attackers to bypass access controls such & brute force tokens and passwords without any limiting of any requests. There should be protection on the web application for sensitive actions. Attackers send a high number of requests to perform desirable actions to get access to the application or accounts.

NO RL effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.

**Severity: High**

POST Request

**Complexity: Easy**

**Steps: -**

Getting the post request by filling form



After that intercepting the request and getting the POST request for OTP by entering wrong OTP



Now, setting the parameters to brute force the otp code and starting attack and without any block we got the OTP



**Impact:** An Adversary can carry out No Rate-Limit attack and also can take over the victim Account.

Also, an adversary can manage to login through any other user's account.

**Affected Page**

https://betaaccounts.digitallocker.gov.in/signup/verify\_mobile\_otp

**Recommendations:**

1. There should be a protection on the web application for limiting the user’s simultaneous requests.
2. Any user should be Rate limited if attacker sends or races high amount of requests in a significant amount of time.
3. Set the time limit for entering OTP same as present in Digilocker sign in/up forms

**References:**

https://hackerone.com/reports/743545

https://hackerone.com/reports/385381

https://hackerone.com/reports/297359

**Proof of Concept:**

