**Vulnerability Name:** No Rate Limit Vulnerability on Registration Page & Forget password

**Note**: We are giving the proof of registration page no rate vulnerability. However, we have given the mitigation steps to mitigate the forget password page no rate vulnerability as well.

**Vulnerable URL:** [**https://www.mollie.com/dashboard/signup?lang=en**](https://www.mollie.com/dashboard/signup?lang=en)

**Steps To Reproduce:**

* **Go to** [**https://www.mollie.com/dashboard/signup?lang=en**](https://www.mollie.com/dashboard/signup?lang=en)
* **Collect 5 or more emails for testing**
* **Pick any one email and fill all the details in the signup page.**
* **Before clicking on registration make sure burp suite interceptor is on.**
* **Now click on registration your request will captured by burpsuite.**
* **Select emails id field for attack.**

**POST /dashboard/signup?lang=en HTTP/1.1**

**Host: www.mollie.com**

**User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0**

**Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8**

**Accept-Language: en-US,en;q=0.5**

**Accept-Encoding: gzip, deflate**

**Content-Type: application/x-www-form-urlencoded**

**Content-Length: 679**

**Origin: https://www.mollie.com**

**Connection: close**

**Referer: https://www.mollie.com/dashboard/signup?lang=en**

**Cookie: m\_locale=en; mollieIdTmp=136f41b7998780e75d7c0d1a; \_gcl\_au=1.1.1981080831.1624694102; mp\_mollie=%7B%22distinct\_id%22%3A%20%2217a47509e2864-05a0eb0d9289fe-4c3f2d73-100200-17a47509e29284%22%2C%22%24device\_id%22%3A%20%2217a47509e2864-05a0eb0d9289fe-4c3f2d73-100200-17a47509e29284%22%2C%22%24initial\_referrer%22%3A%20%22%24direct%22%2C%22%24initial\_referring\_domain%22%3A%20%22%24direct%22%7D; \_ga=GA1.2.1894312085.1624694104; \_gid=GA1.2.1231781130.1624694104; m\_session\_type=active; SESSIONID=tltlf61lm9j29pv5q3ksmt3e0l**

**Upgrade-Insecure-Requests: 1**

**\_formtoken=b382d862b802f8a5b557afdf79622b1b172d42d7c1e99876c40a91fdca7a905f6622a345e48e9a48&ga-cid=&onboarding=dashboard&first\_name=Samar&last\_name=yadav&email=§feveme9015%40gamezalo.com§&password=Hadoop%40123.&rcToken=03AGdBq25QMCXfFUW0pgq4a1vO8yhrtkZ3zv1oXOxXFcIygS2IDq6absdqxXf6OZDFctTa9Jqxn1GJMubm3lNdI79RGcCxnTA-LwnN8hYWRoQ6JxJxeB6L1T08BZmF1Z1vaMpgzPm6G9wI7Rl11io9Tnso\_\_XVDIvSudrpLtaueW5QNigyqs-3l5Rxwpy8BXTJELhraXnuC\_la9qIdXdvq10FsR2NPCQpIb9vs37p1zVpxSq2o00UzegMXh02jxKbkJIPVwa98DCrob5UCsaHrJfmyp--2JzPSHsKkWftP\_QDlzFd5A-oxPFcj\_oB9d96wZfXxojYN3Yne-oZ1dHQrjdA9Y7XXl\_iOEUuvcbFYMye2ENgV-VS10FnZ6gv12pjlSID7TiIMP18bOgUw49PR6ZAoa6KAxVIT9MnqozByNsPGBkAtBR3RTda2tohDNqeAZJV\_P4sSXGIw**

* Now go in the payload section, load your email ID, and click on start attack.
* You will observe the multiple emails are getting registered on same time

**Impact on Organization:**

* It can annoy any individual who even did not registered on your organization but got the registration email.
* It can lead to financial loss in case any of your business client employees and himself getting these types of mails.
* It can lead to Business risk.
* The reputation of company can be impacted, as the individual can think that the organization is not concern about their security. SO it will be a negative impact of the organization in people’s mind

**Mitigation/Solution**

* I would recommend you to add captcha on registration page.
* This vulnerability is also on forgot password page, so we should also add captcha at forget password page.
* We can also limit the number of request for forget password.

**POC:**

* **Screenshot has been attached**
* **Video has been attached**