

No Rate Limit on email verification:

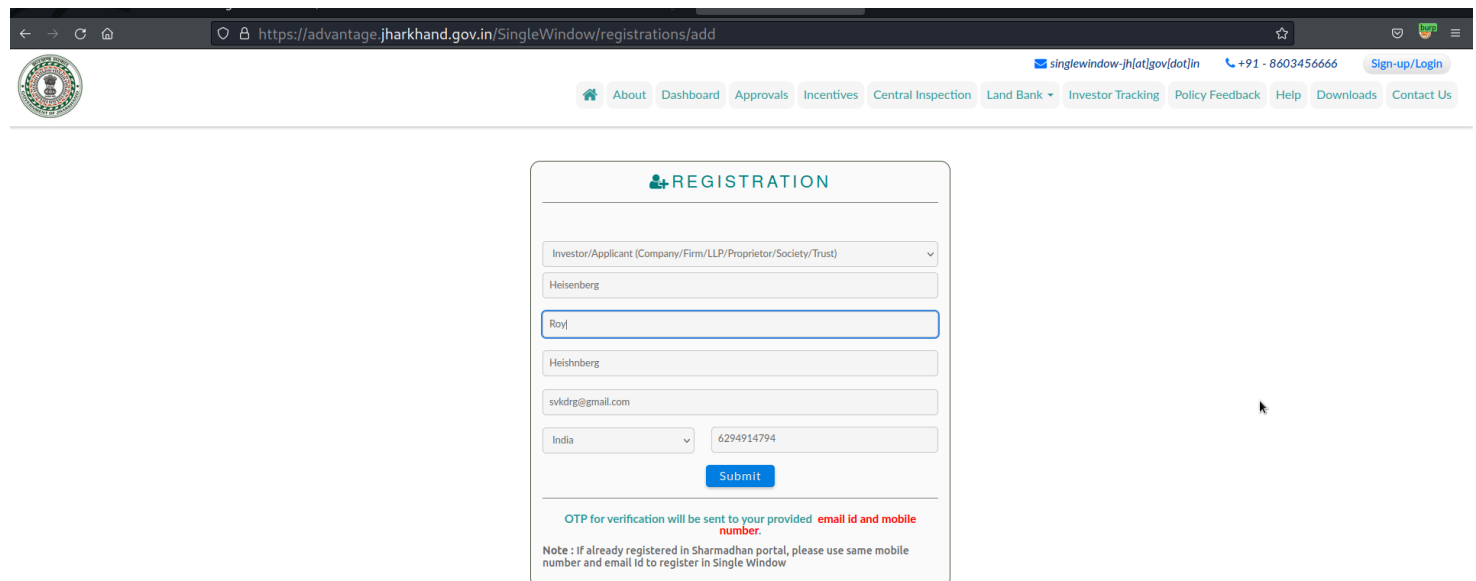
No rate limit on <https://advantage.jharkhand.gov.in/SingleWindow/registrations/add> which leads to tremendous disturbance to the users on the website because huge email bombing can be done by the attackers within seconds.

Summary:

The <https://advantage.jharkhand.gov.in/SingleWindow/registrations/add> endpoint takes any email and if we intercept the request and send it to intruder and repeat it 100 times the target email will have 100 account verification mail.

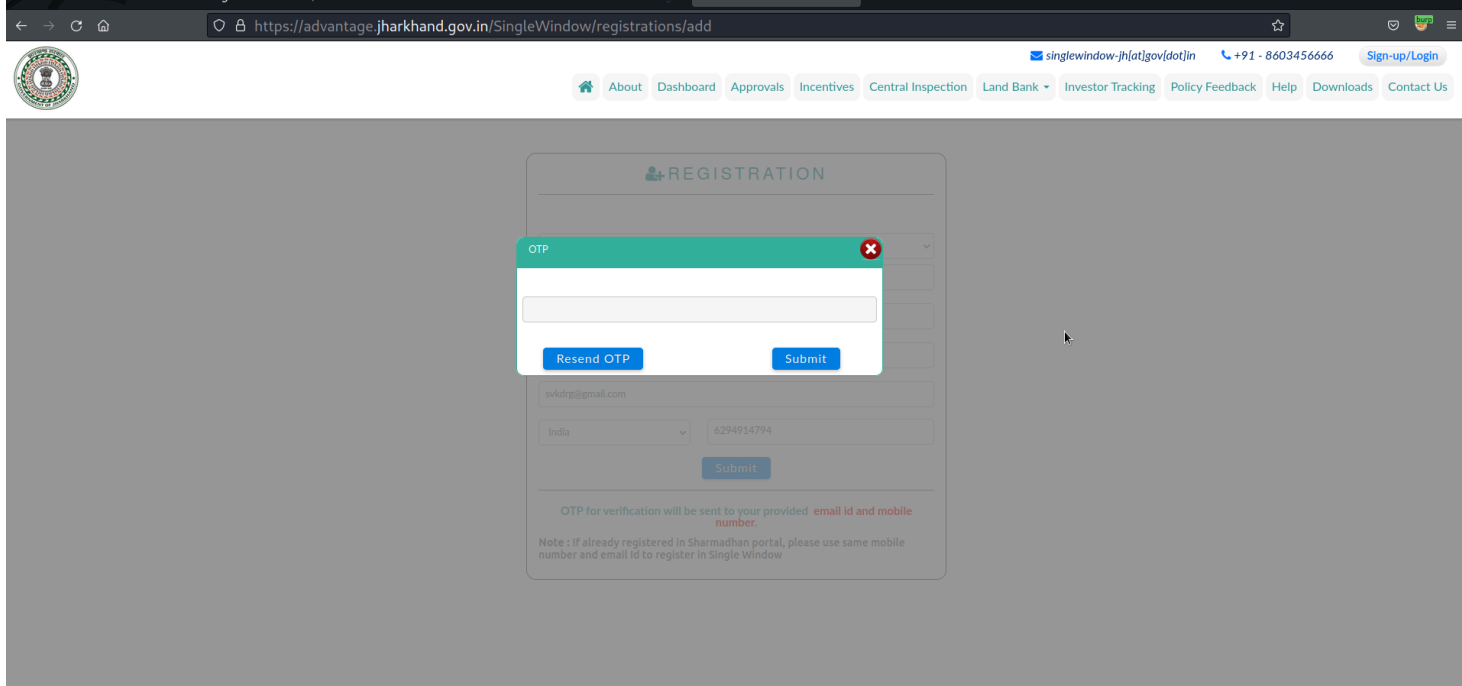
Steps To Reproduce:

1. Go to this link: <https://mahadbtmahait.gov.in/RegistrationLogin/RegistrationLogin> and fill in the required information and put the email you want to get email ID verification.

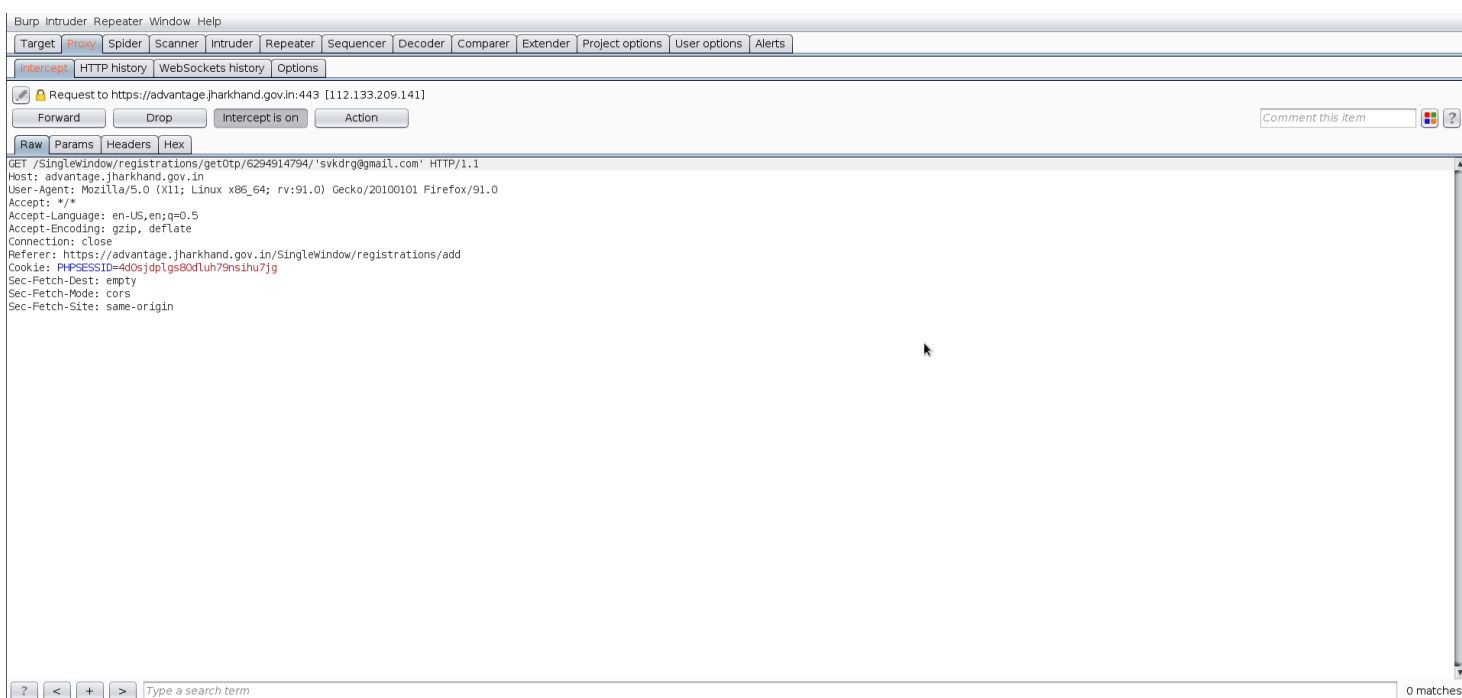


The screenshot shows a web browser window with the URL <https://advantage.jharkhand.gov.in/SingleWindow/registrations/add>. The page features a header with a logo on the left and navigation links (About, Dashboard, Approvals, Incentives, Central Inspection, Land Bank, Investor Tracking, Policy Feedback, Help, Downloads, Contact Us) on the right. A contact email [singlewindow-jh\[at\]gov\[dot\]in](mailto:singlewindow-jh[at]gov[dot]in) and a phone number +91 - 8603456666 are also present, along with a 'Sign-up/Login' button. The main content area is titled 'REGISTRATION' and contains a form with the following fields: a dropdown for 'Investor/Applicant (Company/Firm/LLP/Proprietor/Society/Trust)', text inputs for 'Heisenberg', 'Roy', and 'Heishnberg', an email input 'svkdr@gmail.com', a country dropdown set to 'India', and a mobile number input '6294914794'. A blue 'Submit' button is at the bottom of the form. Below the form, a message states: 'OTP for verification will be sent to your provided email id and mobile number.' A note at the bottom reads: 'Note : If already registered in Sharmadhan portal, please use same mobile number and email id to register in Single Window'.

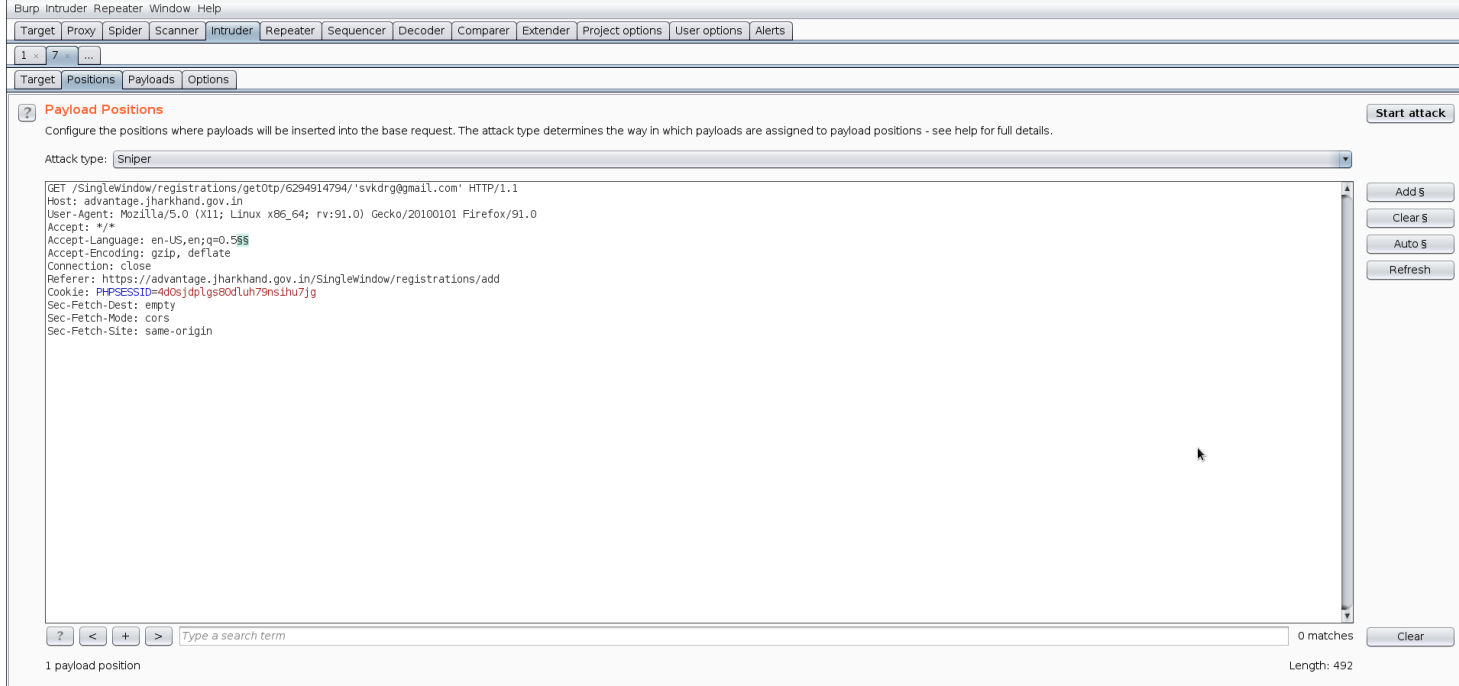
2. You'll be prompted to page to verify the OTP.



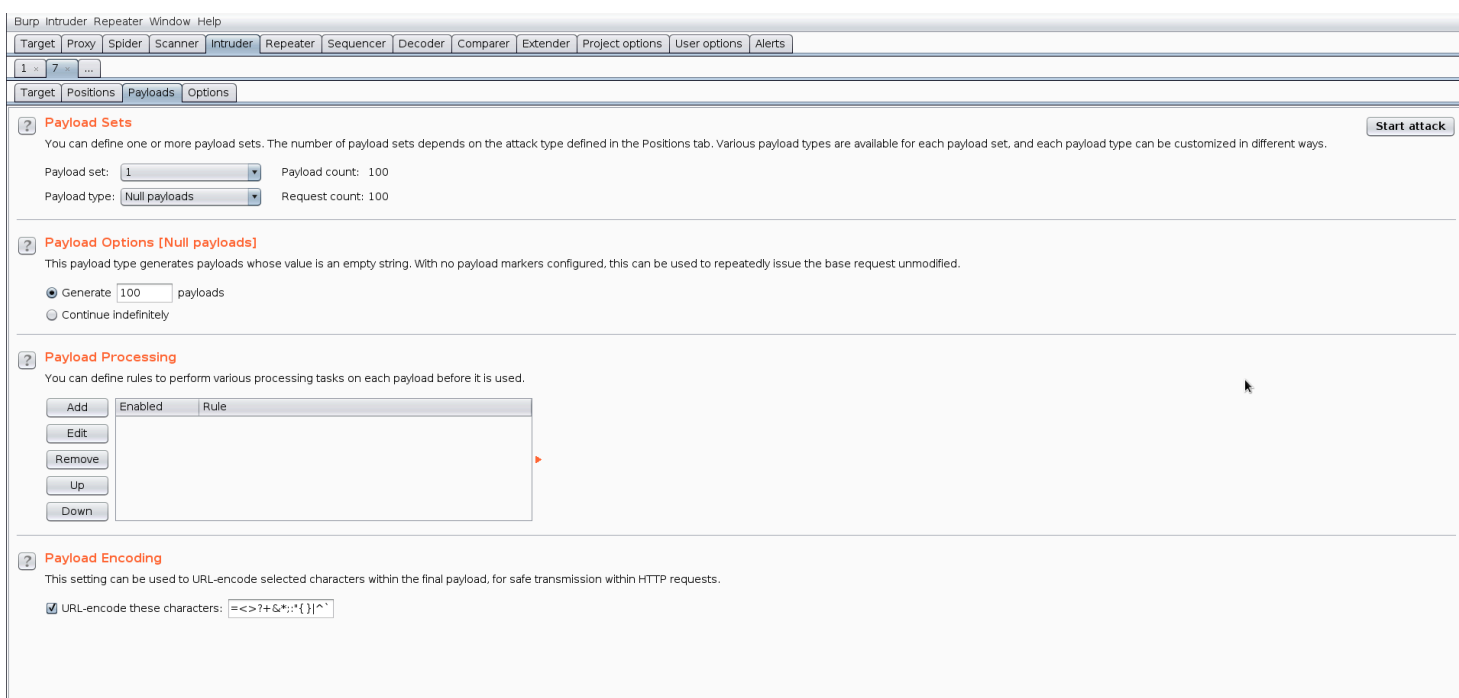
3. Turn on interception in burpsuite and click the **Resend OTP** and capture the request.



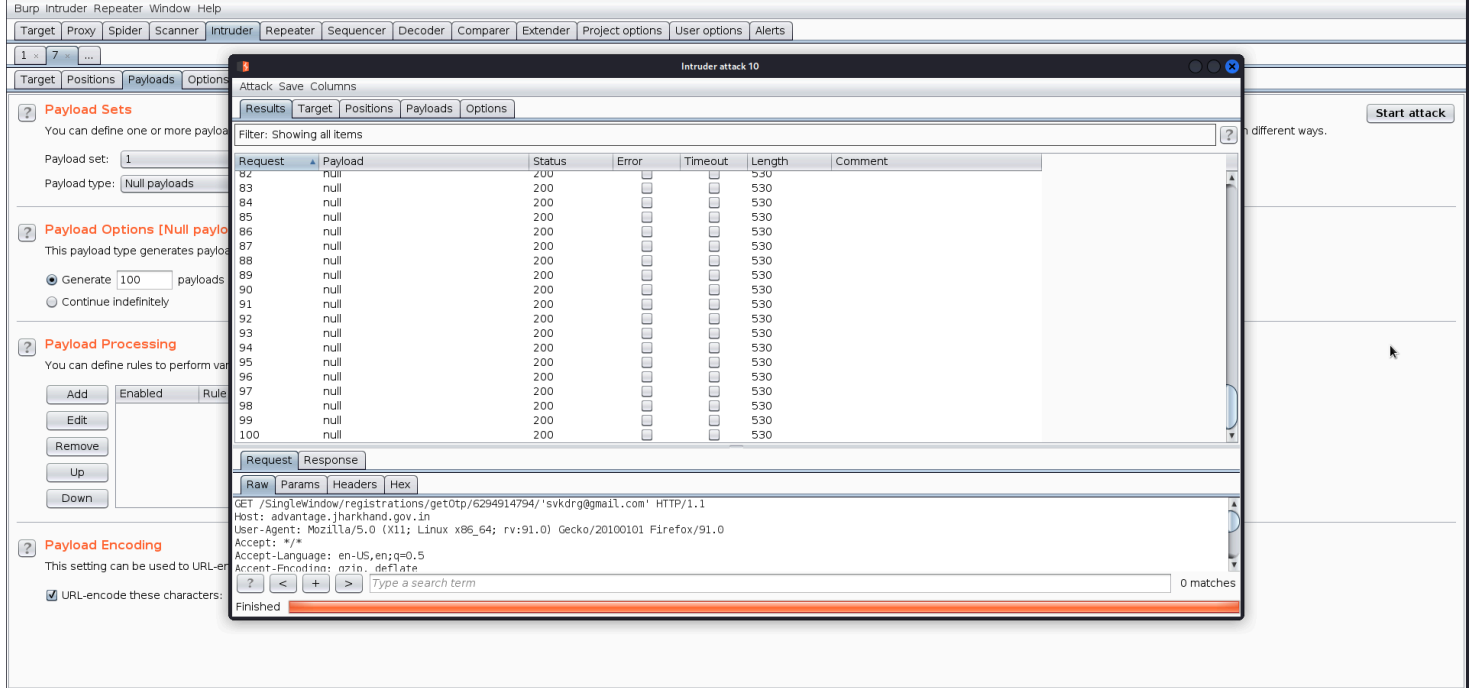
4. Send it to intruder and then turn off the interception.
5. Go to position tab and clear then add any random position.



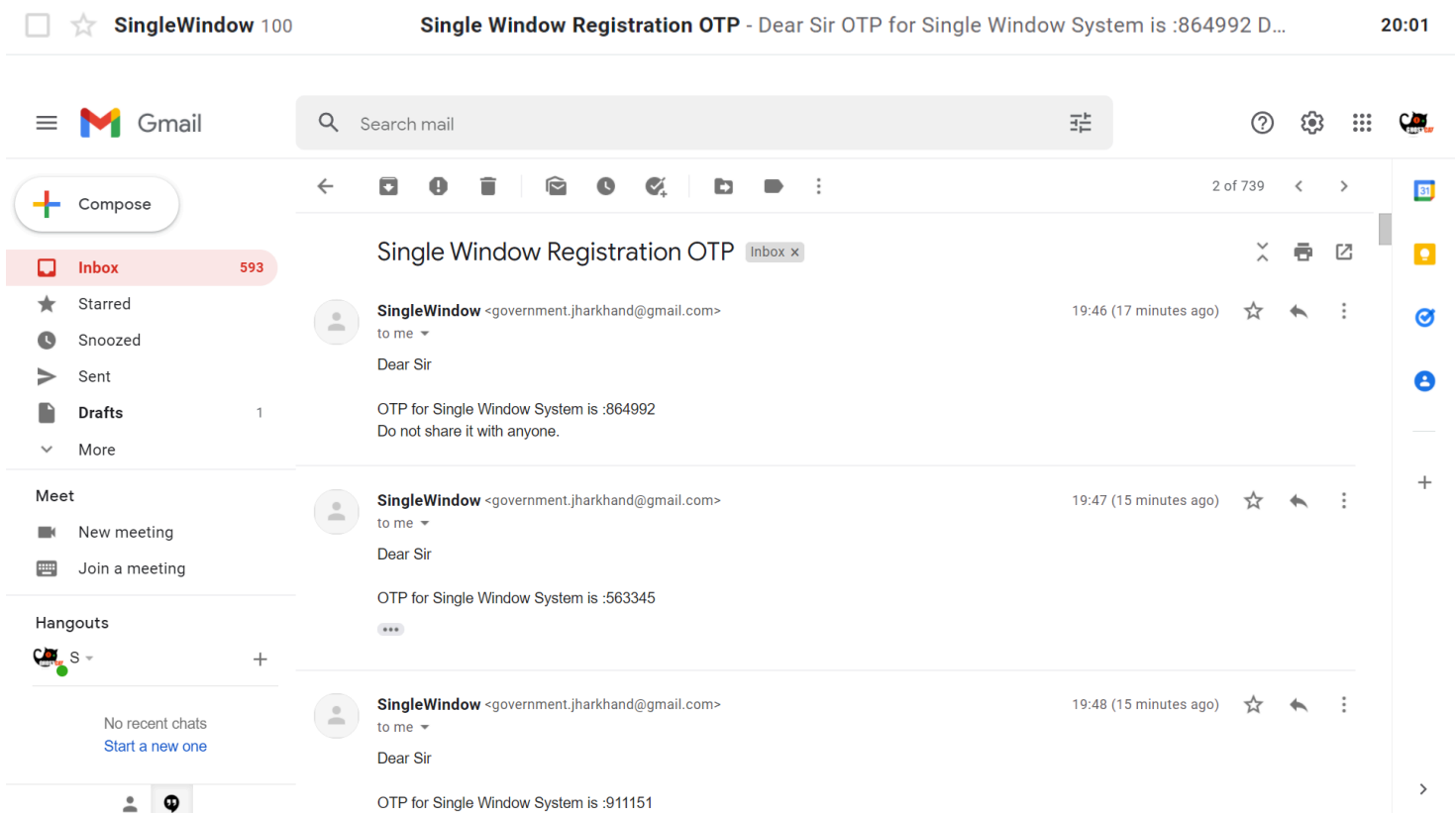
6. Then Select null payload in payload type and generate 100.



7. You'll get 200 OK status code even on the 100th request.



8. POC: As a result I got 100 emails.(Please be patient because it takes a little bit time to generate 100 emails.)



Impact:

Trouble to the users on the website because of huge email bombing by the attackers within seconds.

Mitigation:

- Use CAPTCHA verification if many requests are sent.
- Reducing the number of requests.
- Monitoring API activity against your rate limit.