No Rate Limit on account activation link:

No rate limit on https://www.apprenticeshipindia.gov.in/login/resend-activation-link which leads to tremendous disturbance to the users on the website because huge email bombing can be done by the attackers within seconds.

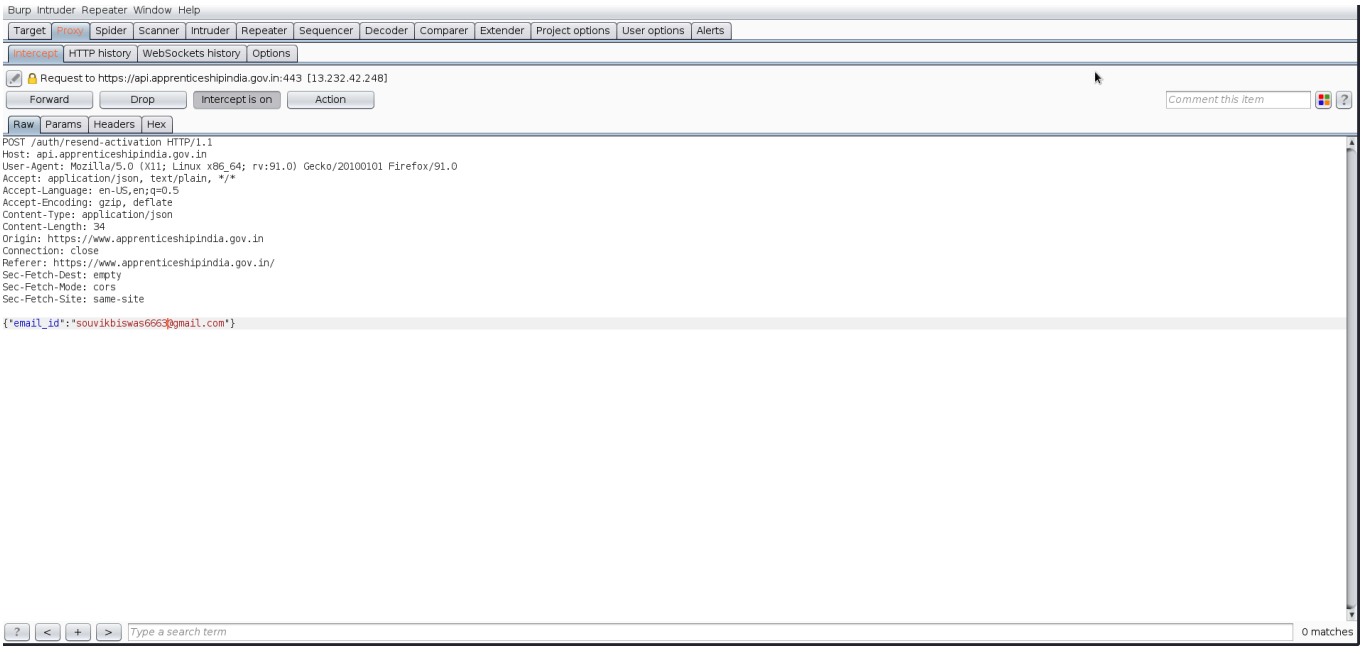
Summary:

The *https://www.apprenticeshipindia.gov.in/login/resend-activation-link* 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 activation email.

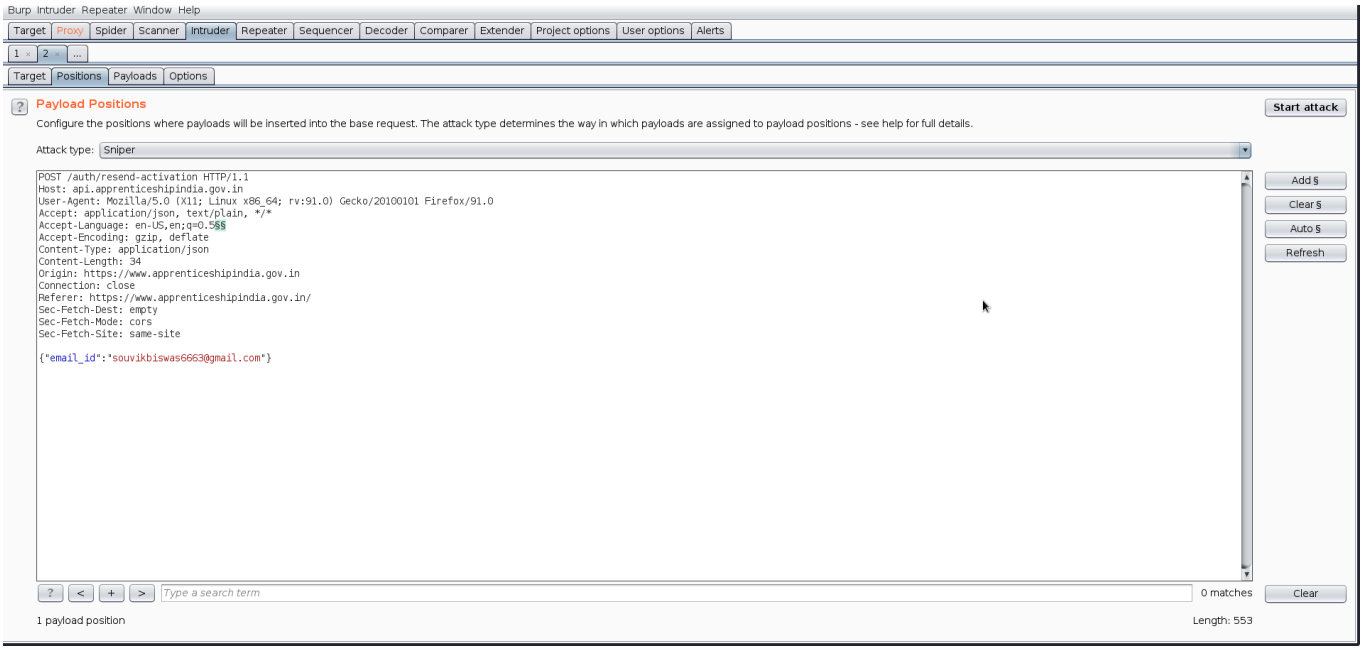
Steps To Reproduce:

First register here https://www.apprenticeshipindia.gov.in/candidate-registration with a valid email and any phone number

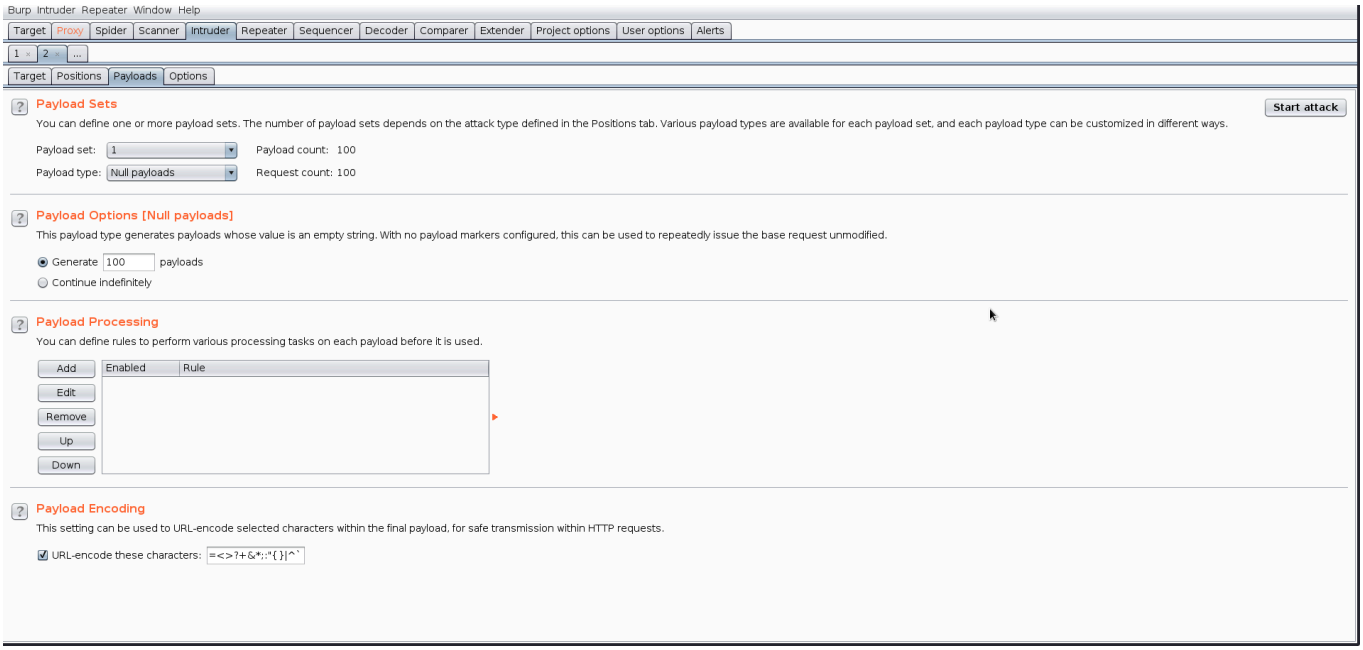
1. Go to https://www.apprenticeshipindia.gov.in/login/resend-activation-link and enter the registered email then click send.
2. Intercept the request in burp suite.



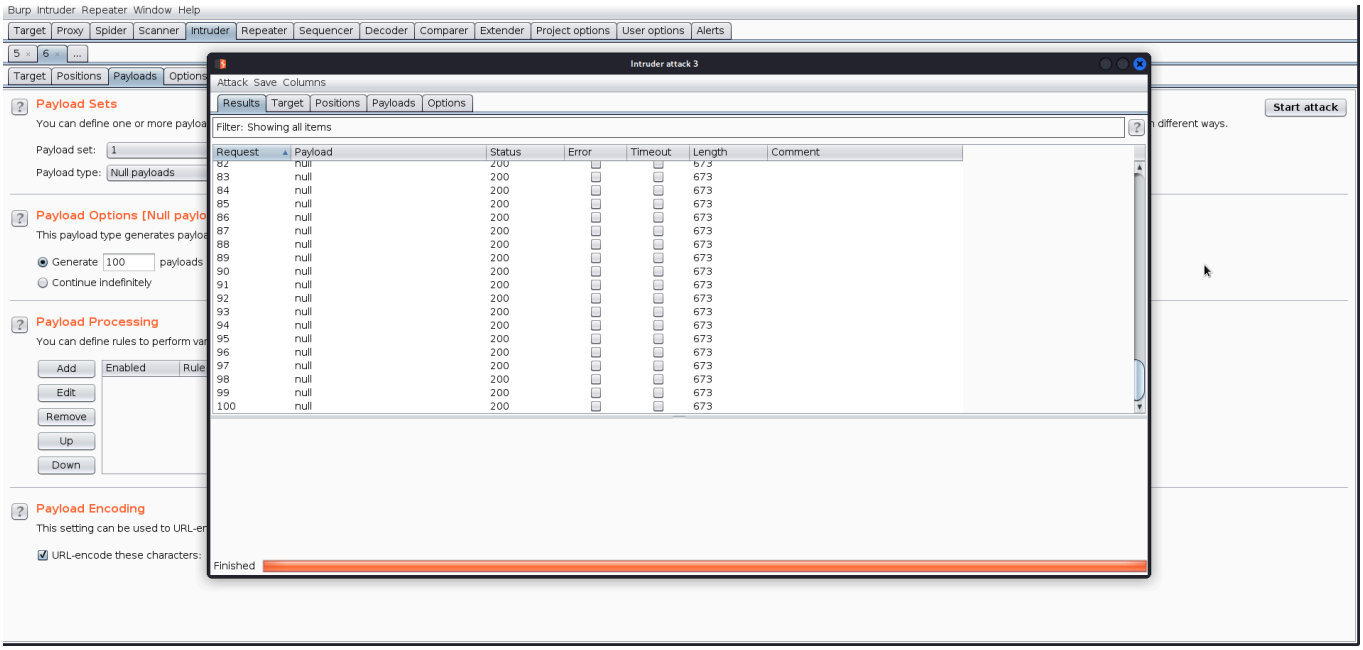
3. Send it to intruder and then turn off the interception.
4. Go to position tab and clear then add any random position.



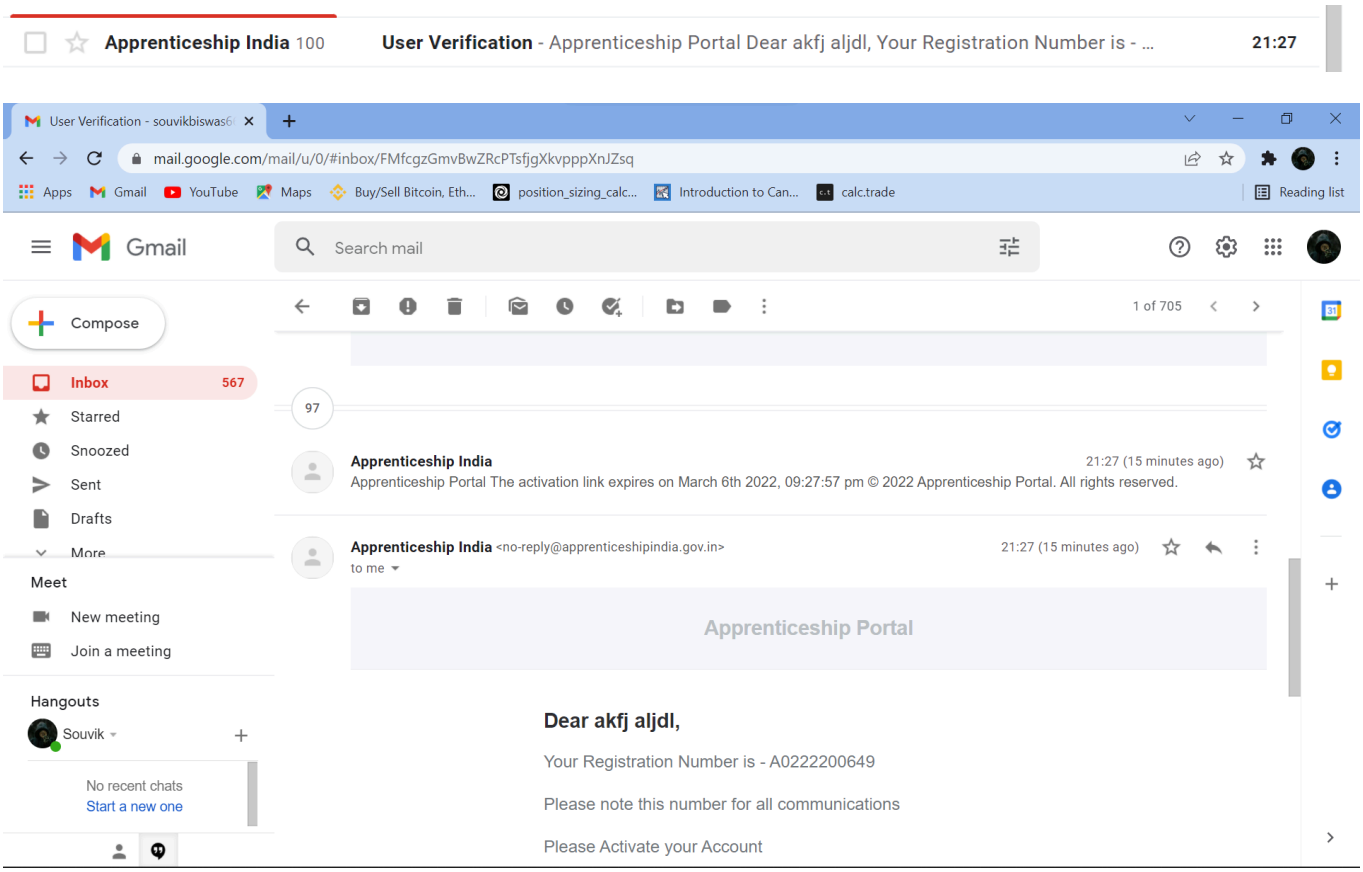
6. Then Select null payload in payload type and generate 100.



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



8. POC: As a result I got 100 emails within seconds.



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.