**Vulnerability Name:** No Rate Limit Vulnerability on Subscribe Button at <https://springrecruit.com/>

**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://springrecruit.com/>

**Steps To Reproduce:**

* Go to <https://springrecruit.com/>
* Collect 5 or more emails for testing
* Pick any one email and fill all the details in the signup page.
* Before clicking on the subscribe button make sure burp suite interceptor is on.
* Now click on subscribe your request will captured by burpsuite.
* Select emails id field for attack.

**POST /subscribe/post?u=ca6975e5d8eb9feae8b42d901&id=298078a843 HTTP/1.1**

**Host: springrole.us14.list-manage.com**

**Content-Length: 44**

**Cache-Control: max-age=0**

**Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"**

**Sec-Ch-Ua-Mobile: ?0**

**Upgrade-Insecure-Requests: 1**

**Origin: https://springrecruit.com**

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

**User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36**

**Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9**

**Sec-Fetch-Site: cross-site**

**Sec-Fetch-Mode: navigate**

**Sec-Fetch-User: ?1**

**Sec-Fetch-Dest: document**

**Referer: https://springrecruit.com/**

**Accept-Encoding: gzip, deflate**

**Accept-Language: en-US,en;q=0.9**

**Connection: close**

**EMAIL=§sosodas362%40nefacility.com§&subscribe=**

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

**Impact on Organization:**

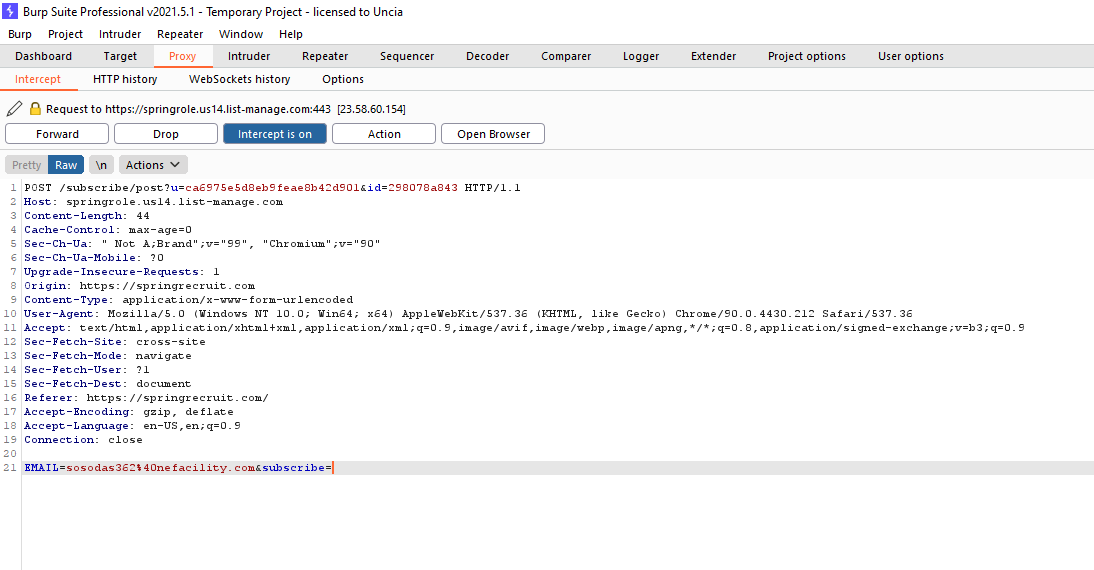
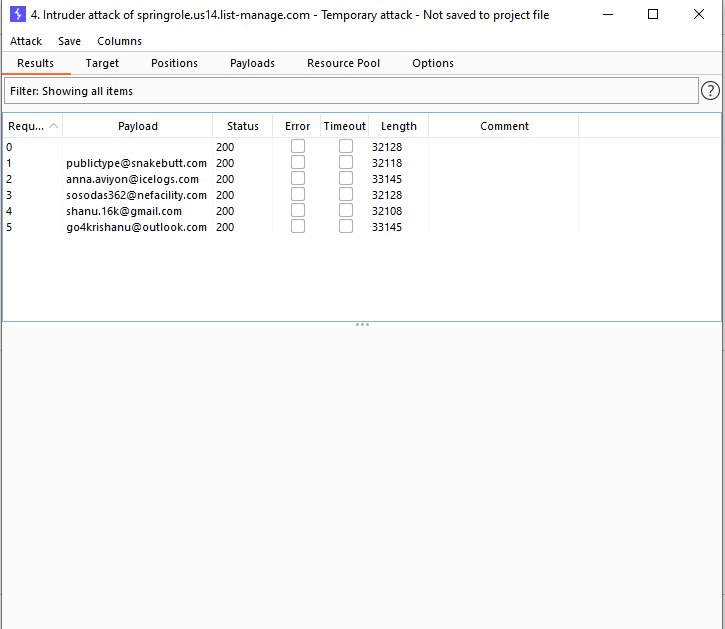
* It can annoy any individual who even did not registered on your organization but got the registration email.
* Mass Emailing will leads to a bad experience for your clients.
* It can lead to financial loss in case any of your business client employees and himself getting these types of mails.
* It can lead to Business risk.
* It can lead to Denial of Service attack which may hard the organization.
* 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**

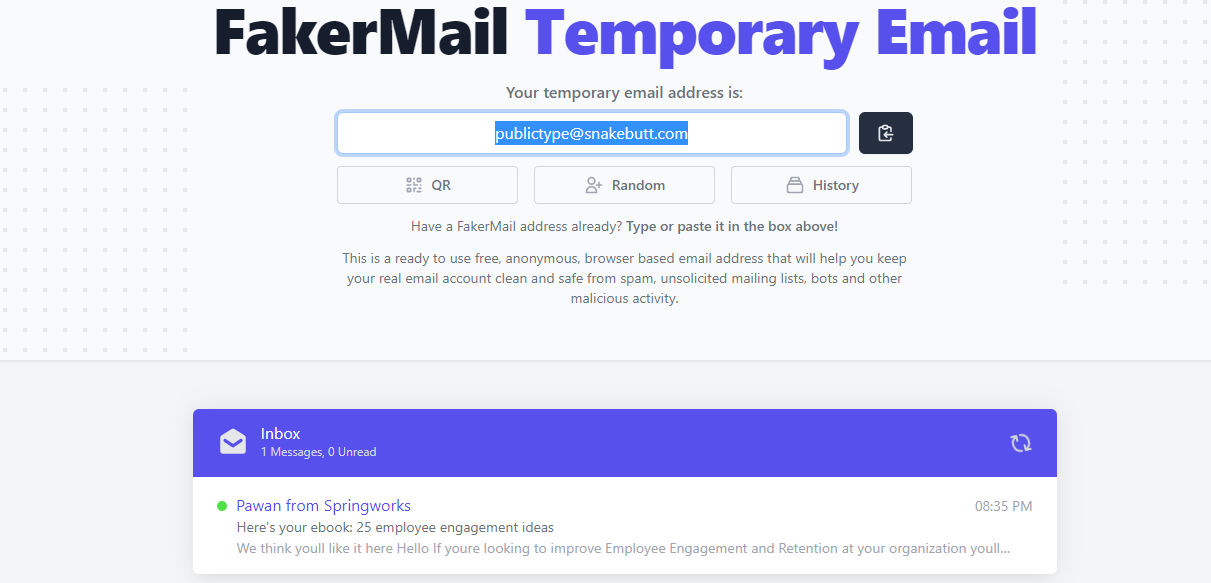
* I would recommend you to add captcha on subscribe page.
* We can also limit the number of request for forget password.
* No fake email should be allowed.

**POC:**

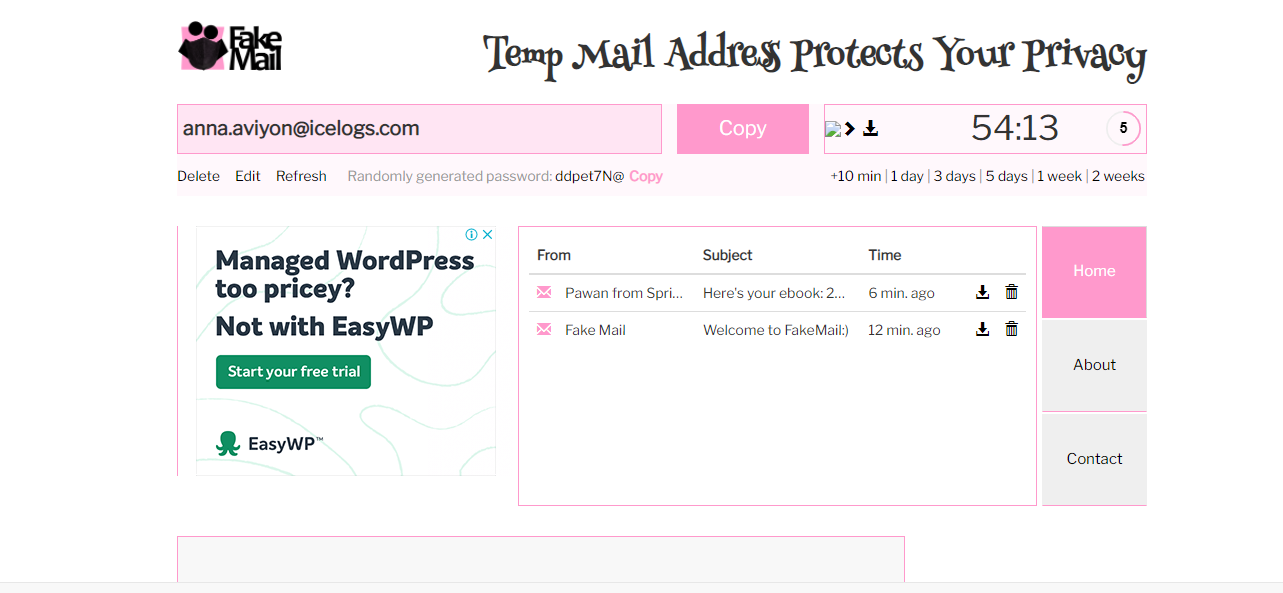
* **Screenshot has been attached**

****

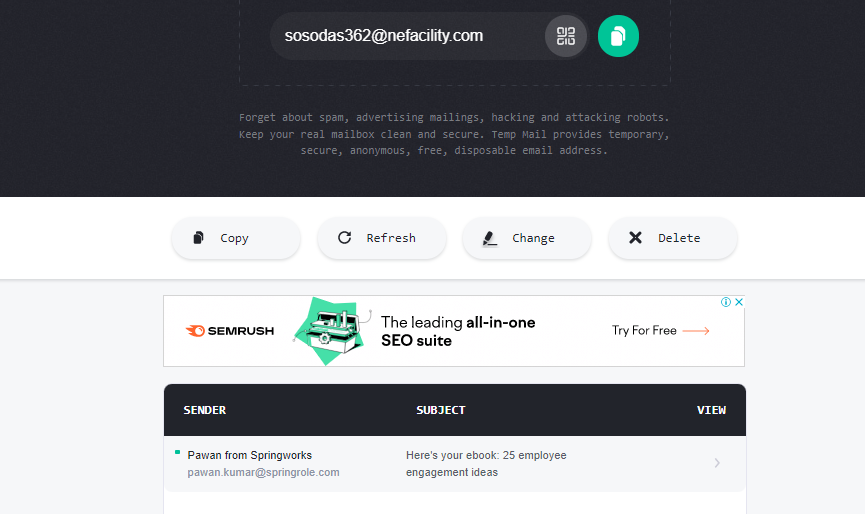
**Email 1 :**

****

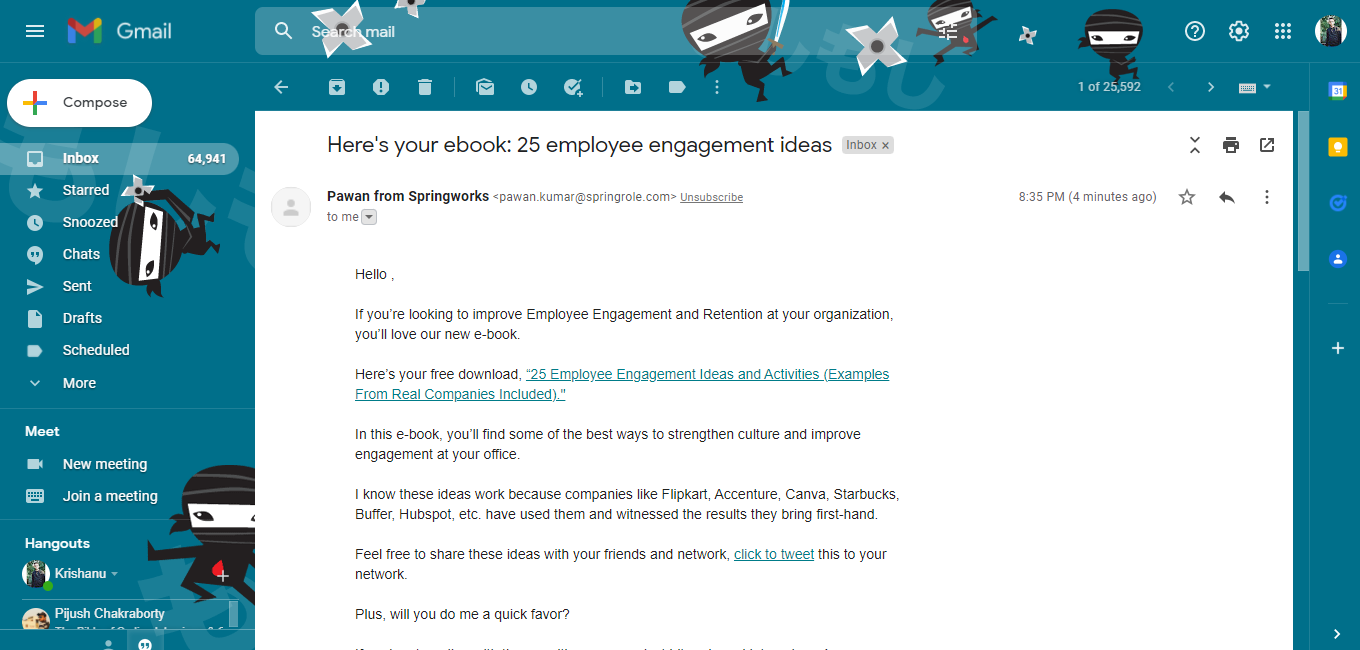
**Email 2 :**

****

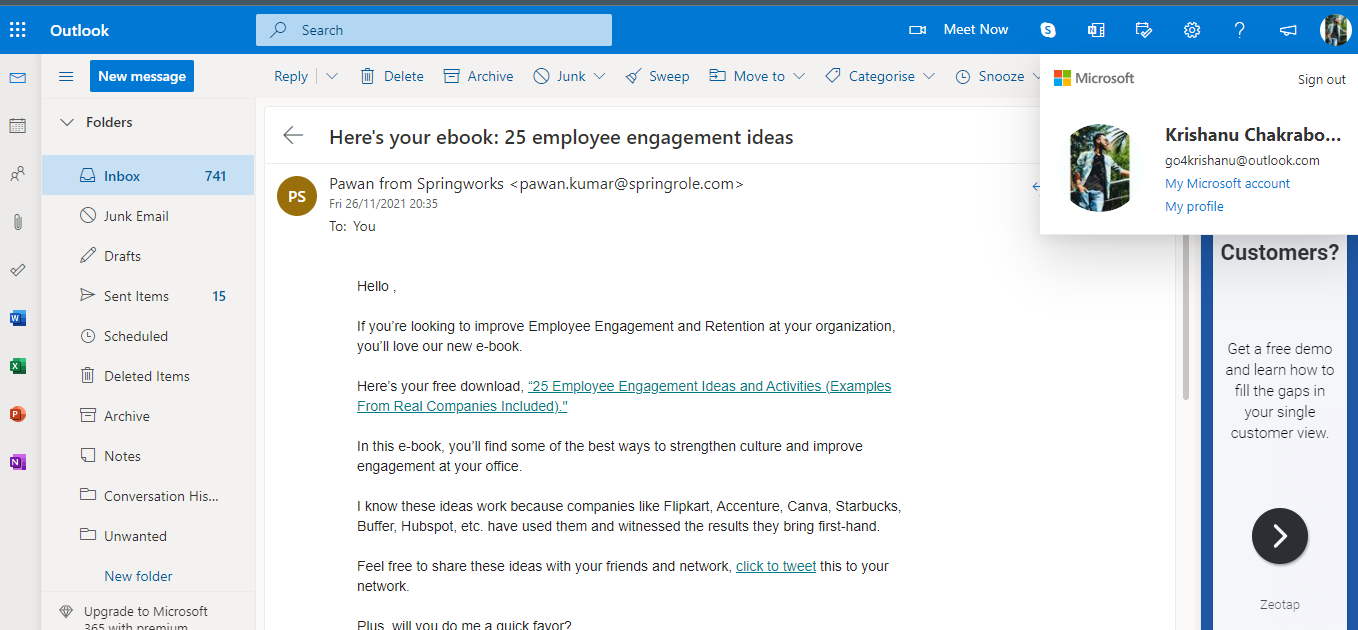
**Email 3 :**

****

**Email 4 :**

****

**Email 5 :**

****