Vulnerability Vector: https://sisudata.com/blog

Vulnerability: Spam & SMTP denial of service vector due to lack of rate limiting & email confirmation on newsletter sign up

Severity: **None⇒Low**

Vulnerability Description:

Lack of email confirmation or validation when signing up for a newsletter or service that involves receiving a constant stream of emails can lead to spamming vectors, and potential backend database/SMTP denial of service potential.

Vulnerability Impact:

A bad actor, or someone who is looking to cause destruction or abuse to the websites services, can take advantage of the lack of confirmation when signing up to the newsletter service, they can:

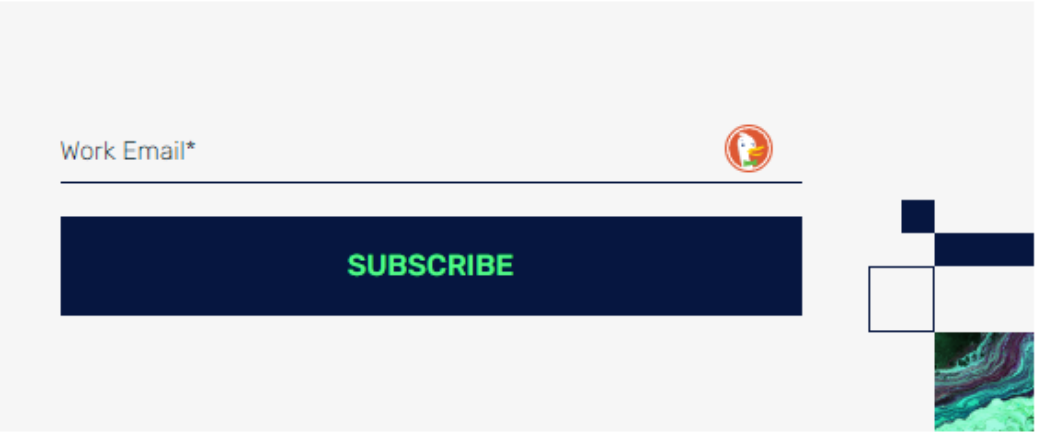
- maliciously sign email addresses/users up without their consent or confirmation, flooding their inbox with unwanted emails and letters

- send false or high amounts of email addresses up to the service, potentially causing a slowdown or complete denial of service when legitimate emails are being sent out to users as part of the newsletter.

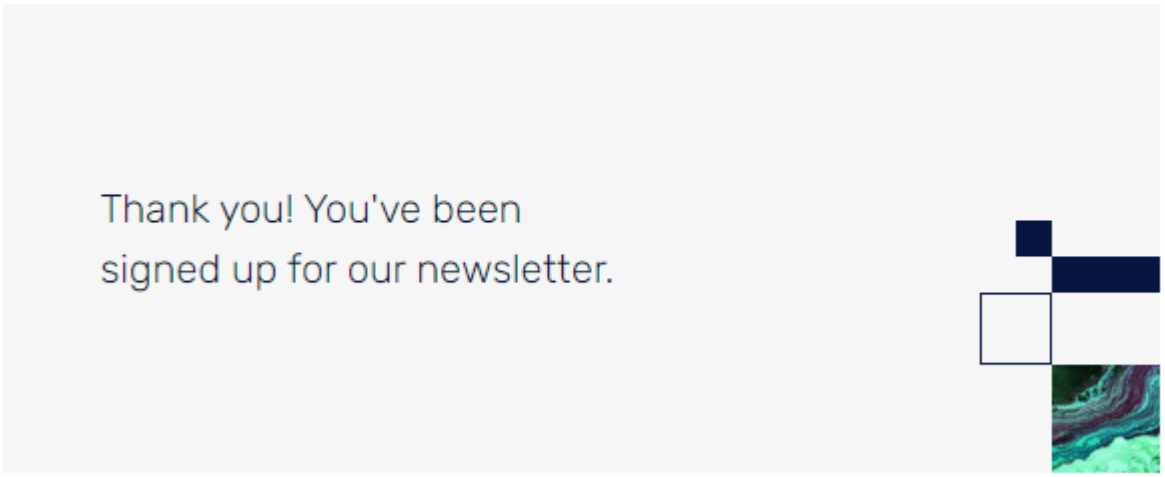
If a threat actor is able to successfully exploit this issue, they may be able to flood a victims inbox with unwanted spam and messages, and or have the email service used for the sending of newsletter emails blacklisted or reported as spam, leading the emails to potentially be listed as spam in the users mailbox, or not being sent to the user at all due to this.

Vulnerability findings:

When signing up to the newsletter service listed on the website:

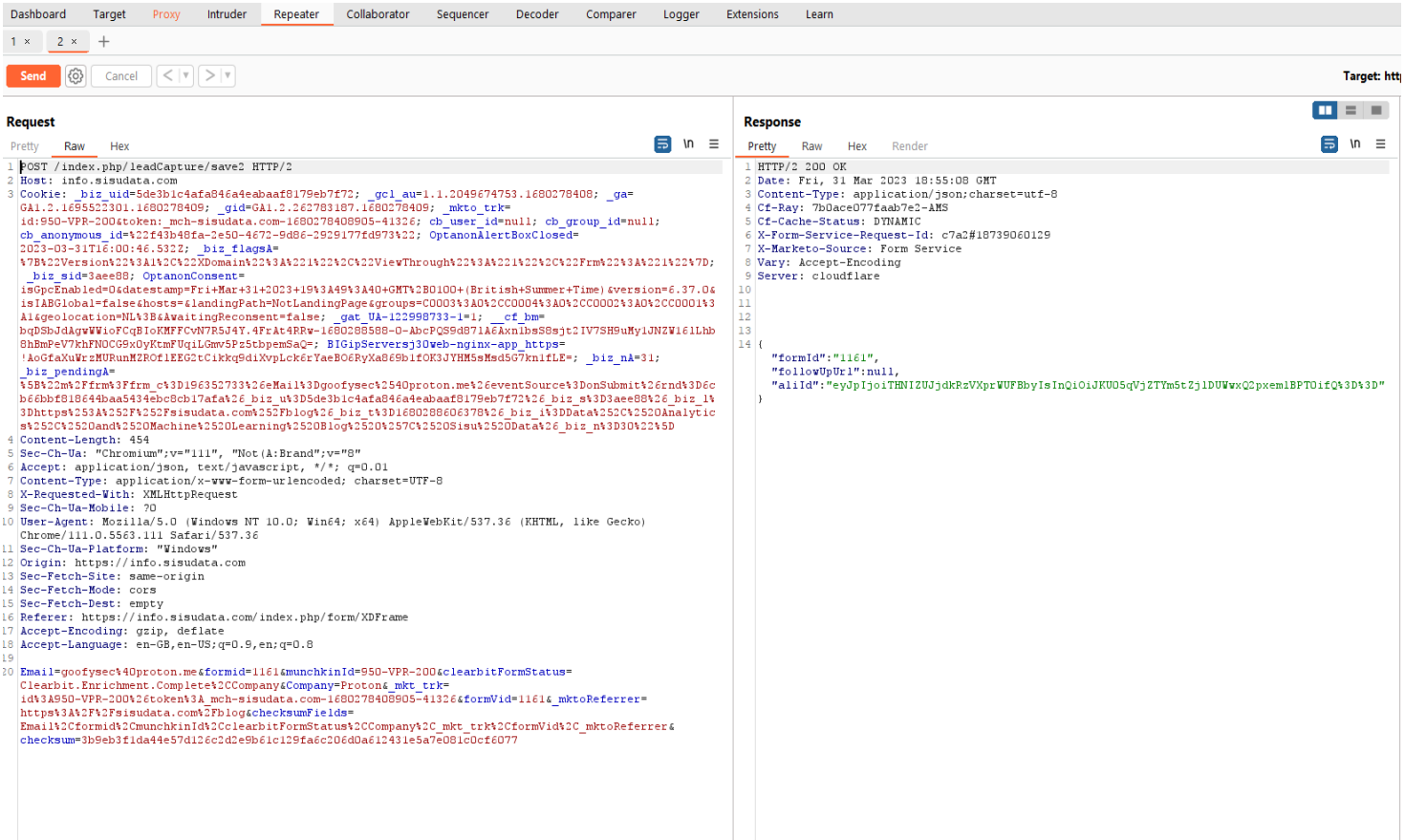


No confirmation is asked to the user, or email sent to the inbox of the user asking for validation when signing up to the newsletter:



Vulnerability Exploitation/POC:

To further validate, and test the lack of rate limiting and confirmation on the newsletter sign up, captured the request being sent to the sign up page from the url listed in the **Vulnerability Vector** and reproduced the request from a different originating email addresses, effectively signing them all up to the newsletter:



Resolution

The company receiving this report decided not to mitigate or take further action relating to this issue, but did note that potentially practises on forms like this would be rate limited in future, depending on severity and need.