



4

## Email enumeration at SignUp page

Share:     State  Resolved (Closed)Disclosed **September 4, 2019 1:12pm +0530**Reported To **Omise**Asset  
go.exchange  
(Domain)

Weakness Information Disclosure

Bounty \$100

Severity  Low (0.1 ~ 3.9)Participants  

Visibility Disclosed (Full)

[Collapse](#)

TIMELINE · EXPORT

**sheerwood** submitted a report to **Omise**.

Aug 3rd (about 1 month ago)

Hi.

There's bad security practise at <https://trade.go.exchange/en/auth/sign-up> against User enumeration.**Description:**At the signup page here <https://trade.go.exchange/en/auth/sign-up>, when you enter an existing user's mail, a msg box says "Email is invalid."[exist.JPG \(F546294\)](#)

The problem is that any used email gets the same error message. while when you enter any other e-mail regardless whether it is fake or not & valid or no it get accepted. which means any Email (could be fake) is valid except registered emails in the database.

so an attacker can compare both responses (success & failure) and enumerate users' emails in large scale.

**Mitigation:**

A better security practise is by simply saying that you sent a link to the e-mail no matter if they have an account already or no. If they have already registered and another process is done, the Email message must say that "someone tried to signup with that Email adress, if that's you please log in."

**Impact**

- Leaking users' emails. / Information Disclosure.

1 attachment:

**F546294:** [exist.JPG](#)**hardymansen** updated the severity from Medium to Low.

Aug 5th (about 1 month ago)

**hardymansen** posted a comment.

Aug 5th (about 1 month ago)

Thank you, Hi,

Thanks for your report.


We are working to verify your findings and will update the report once completed.

This normally is quite fast, expect a answer latest within a few days.


Thank you for your research!  
Omise Security


 [hardymansen](#) changed the status to ○ **Triaged**. Aug 5th (about 1 month ago)

 [sheerwood](#) posted a comment. Aug 5th (about 1 month ago)  
Thanks, I'm waiting.


 [Omise](#) rewarded [sheerwood](#) with a \$100 bounty. Aug 5th (about 1 month ago)  
Ok, we fill fix it. Glve you 100\$ for the research. Thank you very much.  
  
best regards

 [hardymansen](#) closed the report and changed the status to ○ **Resolved**. Aug 5th (about 1 month ago)



 [sheerwood](#) requested to disclose this report. Aug 5th (about 1 month ago)  
Thanks alot for the bounty, Can we move to disclosure?

 [hardymansen](#) posted a comment. Aug 6th (29 days ago)  
Not yet please. We still have the issue in the backlog. Soo any disclosure is totally fine after we fixed it but not before.

 [sheerwood](#) posted a comment. Aug 6th (29 days ago)  
Alright, take your time.

 [hardymansen](#) posted a comment. Aug 6th (29 days ago)  
Thank you, when it is low risk once like these they can take some time since we work in sprints and have a lot of work already planned in feature wise. Usually i want to pay reward after soo hacker can keep us accountable but at the same time i don't want people to have to wait 1 month or something on payment.  
  
Thanks again. And if you find more, let us know.  
  
best regards

 [sheerwood](#) posted a comment. Aug 6th (29 days ago)  
okay no problem, you are good guy.

 [sheerwood](#) posted a comment. Aug 8th (28 days ago)  
Hi, I've found out that the issue is present at this page as well <https://dashboard.omise.co/signup>   
Try signing up with registred email.  
and you get this : [omisesignuperror.JPG \(F549497\)](#)  
I hope you fix it too asap

1 attachment:  
**F549497:** [omisesignuperror.JPG](#)

 This report has been disclosed. Sep 4th (about 1 hr ago)