Paypal bug $10K - All Secondary users account takeover leads to unauthorized money transfer from paypal business accounts

In the name of Allah the beneficient the most merciful.

It's been quite long time i wrote a blog due to some commitments , Today i would like to disclose one of my findings in Paypal which was reported via Hackerone.

This bug allowed me to takeover all secondary accounts of any paypal business account , there was an IDOR bug which gave me control over any secondary user account i want.

Paypal business accounts are used by millions of organizations worldwide and business owners
assign various privileges to secondary user accounts so as to ease their task. One of the privilege business owners give to secondary user is transfer money from paypal business account to any other account they like . So, i used this particular privilege in describing the issue which if exploited it would have given attacker unauthorized access to transfer money from any paypal business account by taking over secondary account of users having privilege as "Transfer money".

Steps:
Two different business accounts were needed for POC.

-> From victim@gmail.com business account i created secondary user having username as victim1234

-> From attacker@gmail.com business account i created secondary user having username as attacker1234

-> From attacker account after going to secondary user account here
https://www.paypal.com/businessmanage/users/16609711757912450 38
(this id is for attacker1234 , from attacker@gmail.com) and then captured the request
to edit the permission like this

PUT /businessmanage/users/api/v1/users? HTTP/1.1
Host: www.paypal.com
Connection: close

[{"id":"16609711757912450 38","accessPoint":{"privileges":
["MANUAL_REFERENCE_TXN","VIEW_CUSTOMERS","SEND_MONEY"],"id"
:"4446113495","accounts":
["attacker@gmail.com"]},"roleID":0,"roleName":"CUSTOM","privilegeChan ged":true,"privilegeSecondaryName":"ttt ttts"}]

-> Now in the above PUT request the first id "it can be anything" i entered
id:"asdfjdsf"(some dummy value) and in the second id:446113495 , is the actual id of each secondary user which was vulnerable to IDOR.

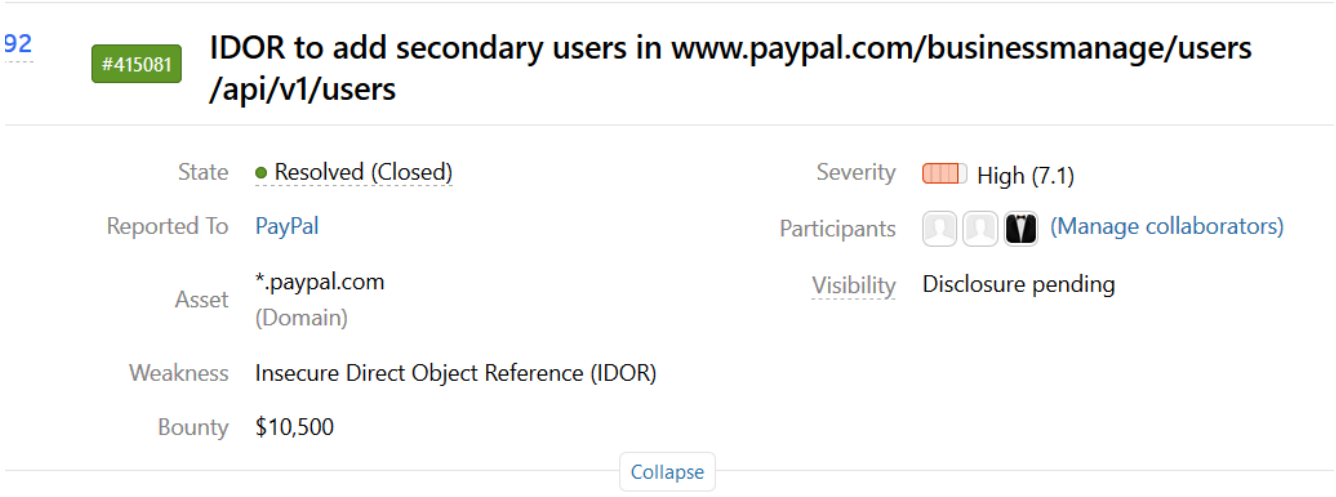
-> This second id is incremental and enumerable as it's only numbers. If attacker would have changed it to 44613496(lets suppose it is id of victim1234) then the associated secondary user account i.e., victim1234 would have been listed to him in
https://www.paypal.com/businessmanage/users .

-> This way if attacker would have just enumerated from 44613495 to 44613999 then all these secondary accounts would have been showed to him in Manage users section of attackers business account , then attacker just needed to change the password of user via Manage users section and Game over!!
Complete takeover of any secondary account.

-> After this attacker could have login to any secondary user account having privilege as "Transfer Money" and then it would have allowed him transfer money from victim account to attacker own account .

Now Paypal remediated the issue and found no evidence of any kind of abuse associated with it.

Summary by Paypal in hackerone about the issue.



92 #415081 **IDOR to add secondary users in www.paypal.com/businessmanage/users /api/v1/users**

State	Resolved (Closed)	Severity	High (7.1)
Reported To	PayPal	Participants	(Manage collaborators)
Asset	*.paypal.com (Domain)	Visibility	Disclosure pending
Weakness	Insecure Direct Object Reference (IDOR)		
Bounty	$10,500		

Collapse

SUMMARY BY PAYPAL

PayPal Business Accounts allow account owners to create multiple secondary users with specific privileges assigned to their employees. This submission identified a method that made it possible for a Business Account owner to assign secondary users from other accounts. The new secondary user would be granted access to the login allowing for unauthorized access to the functions of that single user login. PayPal remediated the vulnerability and found no evidence of abuse associated with it.

Thanks for reading.

Hope you enjoyed reading it.

P.S: Iam looking for infosec job in Hyderabad or remotely, please let me know if any.

Regards
Mohd Haji
https://www.linkedin.com/in/mohd-haji-490960a0/