How I hacked worldwide Tiktok users

s3c Sep 14 · 2 min read

Hello everyone,

In this write up I am sharing a TikTok vulnerability reported via TikTok's bug bounty program

While I was testing the Tiktok app to find a vulnerability I saw a part called family pairing and it's let parents control account their younger users like turn off/on the search bar and turn off/on account to private/public and many more things like the direct message, comments, liked videos….

I thought it's a good position for testing because these functions are complex in the backend app so I start testing in this part

I created 2 accounts 1 for **parents 1 for children and then linked it, and I was turn on my burp suite to catch the** requests,

In the parent account, I tried to change my children account from public to private so once I clicked the turn on button private I catch the request in the burp suite

Let's see what's happening in this request,
I saw there are some parameters each of them does different actions like

restriction_type and **restriction_value** and **child_user_id**

Type is for parts like
Number 1 for direct message
Number 2 for liked videos
Number 3 for comments
Number 4 for public/private account

And Value for if this turn on/off/noone
Like 1 or 2 or 3 or 0

And **child_user_id** for your children account id

So i thought what happens if i change the **child_user_id** to another user id so i changed it and i see **BoOM** it worked😱

Now I can change sensitive settings of any account just by user id of the account 😨

proof of content

impact
an attacker would have potentially been able to collect all users id of Tiktok and change all users from public to private accounts and stop all lives and videos on the ForYou page and all comments…etc

So I quickly reported it to Tiktok and they resolved the issue quickly.

> *Timeline:*
>
> *Reported — Aug 2nd*
>
> *Awarded $$$$— Aug 6th*
>
> *Resolved — Aug 13th*
>
> *Thank you for reading.*

Twitter: @s3c_krd

Hacking Infosec Tik Tok Security Cybersecurity