Published in InfoSec Write-ups

Sam Follow
Jan 7 · 3 min read · Listen

A TALE OF 5250$: HOW I ACCESSED MILLIONS OF USER'S DATA INCLUDING THEIR ADDRESS AND PERSONAL INFO

Hi, Hope you guys are doing well, And a Happy New Year, YAY! ✨, Let's start the blog without wasting more time.

As usual, I am hunting in Tecno src program for something in the source code of the application, As the scope is huge, So I collected all the applications and decompiled them all at once with apktool with this command: **find . -iname "*.apk" -exec apktool d -o {}_out {} \;**

(Yah it will take a good amount of time to decompile 😳)

FINDING THE BUCKET :

Now I started to look for something juicy in decompiled files, but as there are

about 50+ applications, I can't look at each of them manually right? I just got an idea of nuclei, and boom I knew there are templates for android applications,

I just downloaded them and, started nuclei on the whole directory 😅

Command for that : **nuclei -target /path-to-output-folder/"android testing"/allapks/ -t /path-to-tamplates/mobile-nuclei-templates/**

After 18–19 mins of a run, Nuclei gave an output saying **S3 Bucket Found,** I tried to

just like :

I just simply got access to tecno's data of internal files, Users, and everything they have, I can download everything, Even the whole bucket 😂.

Here is just a glimpse of the data: Now I am damn sure that the bucket is full of juice. Ahh, I wanted to look at more files but as we have to follow bug bounty rules I stopped doing more and directly reported to the team.

Now, After reporting it, I've got one more s3 bucket with nuclei, And it also contained about 4–5 gigs of data 😳

I've reported it too, But don't know why the team said " **both s3 buckets are managed by the same team"** so they merged my report to the previous one 😔, I did not expect something like this 😔, I tried to convince them they cant merge it, But they just did it 😔 But they gave me extra 25 reputations on the program and moved the report to critical, which is still very less for what I just found! Guys, can you say they are right or wrong here for merging different reports? Write down in comments so the team can see 😳, I've rewarded 5250$ for only one report and 0$ for the second one, Even it contained so much sensitive data 😳. I want to say that, I haven't downloaded any file

Links :

Nuclei: https://github.com/projectdiscovery/nuclei **Thanks to projectdiscovery**

Android templates for nuclei: https://github.com/optiv/mobile-nuclei-templates

APKTOOL: https://github.com/iBotPeaches/Apktool

Thanks, guys for reading, I hope you enjoyed it, and please ignore any mistakes and my grammar too 😅, You guys can follow me on Twitter: @__sam0_0

I will publish more writeups soon stay tuned!!! YaY 🔥