$5000 Google IDOR Vulnerability Writeup

Raidh Ĥere 2 days ago · 3 min read

Hey amazing **Hackers**! its Raidh_Here

After many month, I decided to write writeups regarding my bounty from Google of worth $5000. So without wasting any time, lets begin the story!

The Story :

After getting many duplicates and N/A from **H1** & **Bugcrowd**, I decided to write about my journey and started searching for VDP programs. I got many bugs and reported to them but till then no reply . Finally, I decided to start hunt on google.

Started searching google subdomains using Google dorks. I know its piece of a shit but never mind. I found few domains and nothing work for me. So finally, I decided to test on google cloud.

While scrolling down in the google cloud market place I found an interesting application called **Dialogflow**

again you need to clean up your mind raidh....

I started searching more about the application. Dialogflow is a natural language understanding platform used to design and integrate a conversational user interface into mobile apps, web applications, devices, bots, interactive voice response systems and related uses.

I started searching common bugs like **xss,sqli,htmli**.. etc.

But it didn’t work! :(

After doing a lot of search, I got an interesting Option

and started creating the phone gateway :)

It also has a delete option. I turned on my proxy and started intercepting the requests and I found a request like this .

I sent the request to burp repeater and replace the phoneNumbers/<randomstring> to the victims <randomstring> and submit the request.

its easy to create a wordlist for that random number of strings and able to do brutforce to exploit the vulnerability :)

BHOOOOOOOM!. The victim number got deleted and created a poc and reported to **Google**. But they closed the report as intended Behavior. Then, I was like ??!!

ntended Behavior

After explaining the attacking scenario and impact, they reopened and accepted the bug. Whooo hooo! and rewarded with $5000.

Timeline

May 4, 2021 06:28AM — Reported

May 4, 2021 04:19PM — Status: Won’t Fix (Not Reproducible)

May 7, 2021 06:30PM — Status: Won’t Fix (Intended Behavior)

May 12, 2021 09:10AM — Status: Accepted (reopened)

May 18, 2021 04:20PM — Rewarded $5000 bounty

Aug 28, 2021 01:29AM — fixed.

Infosec Bug Bounty Bugs Cybersecurity Information Technology