# Identifying and securing Firebase vulnerabilities



#### Firebase features

#### Auth

Authentication provider that can be utilized in all Firebase services/products. Similar to AWS Cognito.

Supports multiple handlers: Email & password, social login and more.

#### **Firestore**

NoSQL document database to store data from various sources at scale.

Similar to AWS DynamoDB

#### Firebase Storage

File storage system similar to AWS S3.

#### Research process

#### Manual testing

#### **Targeted testing**

- Custom vulnerable instances to identify
- Targeted organizations testing

#### Open source scan

#### Sourcegraph + GitHub

- Identify potential vulnerable patterns
- Pulled about 15000 repositories that contained firebase API keys.

#### Scan everything

#### **Common Crawl**

- Stored scanned results for web application
- Credit to Andres
   Riancho for
   Blackhat talk on
   AWS Cognito.

# Common Vulnerability Patterns

#### Firebase auth

- Common providers used:
  - Email & password
  - Social providers
    - Twitter
    - Google
    - Facebook
- Commonality with AWS Cognito
  - Anonymous login
  - AWS Cognito: Can be used to get a AWS credential linked to an IAM
  - Firebase Auth: Can be used to retrieve anonymous tokens

### Testing: Firebase anonymous auth

Regular login request

```
POST /v1/accounts:signUp?key=FIREBASE API KEY HTTP/2
Host: identitytoolkit.googleapis.com
Content-Type: application/json
Accept: */*
X-Client-Version: iOS/FirebaseSDK/10.3.0/FirebaseCore-iOS
Accept-Encoding: gzip, deflate
Accept-Language: en
Content-Length: 107
User-Agent: FirebaseAuth.iOS/10.3.0 iPhone/16.0
hw/iPhone13 4
  "returnSecureToken":true,
  "email": "mockuser@example.com",
  "password": "AlphaTangoRomeo#3819"
```

### Testing: Firebase anonymous auth

Anonymous login request

```
POST /v1/accounts:signUp?key=GOOGLE API KEY HTTP/2
Host: identitytoolkit.googleapis.com
                                                               2 Expires: Mon, 01 Jan 1990 00:00:00 GMT
                                                               3 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Content-Type: application/json
Accept: */*
                                                               4 Pragma: no-cache
X-Client-Version: iOS/FirebaseSDK/10.3.0/FirebaseCore-iOS
                                                               5 Date: Fri. 17 Mar 2023 15:54:27 GMT
Accept-Encoding: gzip, deflate
                                                               6 Content-Type: application/json; charset=UTF-8
Accept-Language: en
                                                               7 Vary: Origin
Content-Length: 31
                                                               8 Vary: X-Origin
User-Agent: FirebaseAuth.iOS/10.3.0 iPhone/16.0
                                                              9 Vary: Referer
hw/iPhone13 4
                                                              10 Server: ESF
                                                              11 Content-Length: 1223
                                                             12 X-Xss-Protection: 0
  "returnSecureToken":true
                                                             13 X-Frame-Options: SAMEORIGIN
                                                              14 X-Content-Type-Options: nosniff
                                                             15 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
                                                             17 {
                                                             18 "kind": "identitytoolkit#SignupNewUserResponse",
                                                                   evJhbGci0iJSUzI1NiIsImtpZCI6IiFlOTczZWUwZTE2ZidlZWY0ZikvMW01MGRiniFkNzBiMm"
                                                                  VmZWZjMTkiLCJ0eXAiOiJKV1QifQ.eyJwcm92aWRlcl9pZCI6ImFub255bW91cyIsImlzcyI6Im
                                                                  h0dHBzOi8vc2VjdXJldG9rZW4uZ29vZ2xlLmNvbS90ZXN0ZmlyZXN0b3JlLTc2ZDY0IiwiYXVkI
                                                                  joidGVzdGZpcmVzdG9yZS03NmQ2NCIsImF1dGhfdGltZSI6MTY3OTA2ODQ2NywidXN1c19pZCI6
                                                                  IkluWmhtQkhGTGJSREhFNHB1UU9JRDJPZzhaaTEiLCJzdWIiOiJNblpobUJIRkxiUkRIRTRwdVF
                                                                  PSUOyT2c4WmkxIiwiaWF0IjoxNjc5MDY4NDY3LCJleHAiOjE2NzkwNzIwNjcsImZpcmViYXNlIj
                                                                  p7ImlkZW50aXRpZXMiOnt9LCJzaWduX2luX3Byb3ZpZGVyIjoiYW5vbnltb3VzIn19.d76GmUwQ
                                                                  6xIv690WMeZz9P0q2FAGl0iwXf4lBvyGs4uKm5SEV8uv7NMI2o0pP94WzhQqH8e4NPqxOw5pXMj
                                                                  wI ngssVmwc-D0neg FGHsoDl3P7MvnZ4xa80-3Fi8l5S0LeW38AcA3WYJg3KctXkIWiIS7aNHI
                                                                  CsvCW87FavE sYc3aS2V8VG5Jer2uCV-5 cRx25tKQvFStl5MVx2cOPjJF8GJliqR cPPP2DncZ
                                                                  wxSjvpPzhUMndU-kntphevpgZVI96ltV5wuJRAPAoMa95EC 5fb4Pz-AMG34Z1A2gsBeX7 fZ0K
                                                                  ZAHIsfDXaNxwmt-QxzwBQHtlxCsXLC2KVQ",
                                                             20 "refreshToken":
                                                                   "APJWN8cT9K5cUePXYoG43FMEaPCwg3h-xaOngi2PscF4kVTVnvUWLsba428s5K0p0V3udUY9G2
                                                                  ElkwRNN5UsrfKoufVJmSbDewID 6xF6hAhXP8frOqm DJlG6YItEWLoqtlPHMYeDaYOrdhBfcFc
                                                                  vt6nx9MKdGKbgsqCXOJXjOuhADZJRIow4DqK73AiyvKs6trRPH84V40",
                                                                 "expiresIn":"3600".
                                                             22 "localId": "MnZhmBHFLbRDHE4puQOID20q8Zi1"
                                                             23 }
```

#### Firebase Firestore

DocumentDB that can be queried via Rest APIs.

```
GET /v1/projects/test111-cde14/databases/(default)/documents/users?pageSize=1 HTTP/1.1
Host: firestore.googleapis.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: application/json
Accept-Encoding: gzip, deflate
Accept-Language: en-US, en; q=0.9
            Search...
esponse
retty
      Raw
            Hex Render
  "documents":[
      "name": "projects/test111-cde14/databases/(default)/documents/users/19811",
      "fields":{
        "is admin":{
          "booleanValue":true
        },
"joined date":{
          "timestampValue": "2023-08-07T07:00:00.239Z"
        "username":{
          "stringValue": "ok"
        "company name":{
          "stringValue": "LabsTest"
        "email":{
          "stringValue": "john@labstest.localhost"
      "createTime": "2023-07-10T20:56:19.392629Z",
```

#### Firestore: Unauth documents

Sample vulnerable rule

```
service cloud.firestore {
  match /databases/{database}/documents {
    match /{document=**} {
      allow read, write: if true;
    }
  }
}
```

### Firestore: Unauth specific documents

Sample vulnerable rule

```
service cloud.firestore {
 match /databases/{database}/documents {
   match /users/{document=**} {
     allow read, write: if request.auth != null;
   match /organizations/{document=**} {
     allow read, write: if true;
```

# Firestore: Testing document access

- Unauthenticated access Any documents
  - Empty result in non-existent document

```
1 HTTP/1.1 200 OK
 /v1/projects/test111-cde14/databases/(default)/documents/nonexistentdocument?
                                                                                     2 Content-Type: application/json; charset=UTF-8
 pageSize=1 HTTP/1.1
                                                                                     3 Vary: Origin
2 Host: firestore.googleapis.com
                                                                                     4 Vary: X-Origin
3 Upgrade-Insecure-Requests: 1
                                                                                     5 Vary: Referer
                                                                                     6 Date: Fri, 11 Aug 2023 14:40:15 GMT
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36
                                                                                     7 Server: ESF
5 Accept: application/json
                                                                                     8 Cache-Control: private
6 Accept-Encoding: gzip, deflate
                                                                                     9 X-XSS-Protection: 0
7 Accept-Language: en-US, en; g=0.9
                                                                                    10 X-Frame-Options: SAMEORIGIN
                                                                                    11 X-Content-Type-Options: nosniff
                                                                                    12 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
                                                                                    13 Content-Length: 3
                                                                                    15 {
```

### Firestore: Testing document access

Unauthenticated access - Specific Documents

```
GET /v1/projects/test111-cde14/databases/(default)/documents/organizations?pageSize=1 HTTP/1.1
                                                                                                          GET /v1/projects/test111-cde14/databases/(default)/documents/users?pageSize=1 HTTP/1.1
Host: firestore.googleapis.com
                                                                                                          Host: firestore.googleapis.com
Upgrade-Insecure-Requests: 1
                                                                                                           Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
                                                                                                          User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414
Accept: application/ison
                                                                                                           Accept: application/json
Accept-Encoding: gzip, deflate
                                                                                                          Accept-Encoding: gzip, deflate
                                                                                                          Accept-Language: en-US, en; g=0.9
Accept-Language: en-US, en; g=0.9
) \{\hat{o}\} \leftarrow \rightarrow Search..
                                                                                                           esponse
esponse
                                                                                                                Raw Hex Render
retty Raw Hex Render
                                                                                                           HTTP/1.1 403 Forbidden
HTTP/1.1 200 OK
                                                                                                           Vary: Origin
Content-Type: application/json; charset=UTF-8
                                                                                                           Vary: X-Origin
Vary: Origin
                                                                                                           Vary: Referer
Varv: X-Origin
                                                                                                           Content-Type: application/json; charset=UTF-8
Varv: Referer
                                                                                                           Date: Fri, 11 Aug 2023 06:13:56 GMT
Date: Fri, 11 Aug 2023 06:14:32 GMT
                                                                                                           Server: ESF
Server: ESF
                                                                                                          Cache-Control: private
Cache-Control: private
                                                                                                          X-XSS-Protection: 0
X-XSS-Protection: 0
                                                                                                          X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
                                                                                                          X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
                                                                                                          Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
                                                                                                          Content-Length: 127
Content-Length: 409
                                                                                                             "error":{
    "code":403,
  "documents":[
                                                                                                               "message": "Missing or insufficient permissions.",
       "name": "projects/test111-cde14/databases/(default)/documents/organizations/labstest",
                                                                                                                "status": "PERMISSION DENIED"
      "fields":{
         "org admin":{
           "stringValue": "john@labstest.localhost"
         org id":{
```

#### Firestore: Authenticated with Anonymous

Anonymous signup + Auth required Firebase = Access to documents

```
GET /v1/projects/test111-cde14/databases/(default)/documents/users?pageSize=1
Host: identitytoolkit.googleapis.com
                                                                           2 Expires: Mon, 01 Jan 1990 00:00:00 GMT
                                                                                                                                                                                                                                            2 Content-Type: application/json; charset=UTF-8
                                                                                                                                             Host: firestore.googleapis.com
                                                                                                                                                                                                                                            3 Vary: Origin
Content-Type: application/json
                                                                           3 Pragma: no-cache
                                                                                                                                             Upgrade-Insecure-Requests: 1
                                                                           4 Date: Fri, 11 Aug 2023 06:35:20 GMT
                                                                                                                                                                                                                                            4 Vary: X-Origin
                                                                          5 Cache-Control: no-cache, no-store, max-age=0, must-re Authorization: Bearer
                                                                                                                                                                                                                                            5 Vary: Referen
X-Client-Version: iOS/FirebaseSDK/10.3.0/FirebaseCore-iOS
                                                                                                                                             eyJhbGciOiJSUzI1NiIsImtpZCI6ImNmM2I1YWRhM2NhMzkxNTQ4ZDM1OTJiMzU5MjkyM2UzNjAxMm
                                                                                                                                                                                                                                            6 Date: Fri, 11 Aug 2023 06:38:55 GMT
                                                                           6 Content-Type: application/json; charset=UTF-8
 Accept-Encoding: gzip, deflate
                                                                                                                                             I5MTQiLCJ0eXAiOiJKV1QifQ.eyJwcm92aWRlcl9pZCI6ImFub255bW91cyIsImlzcyI6Imh0dHBzO
Accept-Language: en
                                                                           7 Vary: Origin
                                                                                                                                                                                                                                             7 Server: ESF
                                                                                                                                             i8vc2VjdXJldG9rzW4uz29vz2x1LmNvbS90zXN0MTexLWNkzTE0IiwiYXVkIjoidGVzdDexMS1jzGU
                                                                                                                                                                                                                                            8 Cache-Control: private
Content-Length: 31
                                                                          8 Vary: X-Origin
                                                                                                                                             xnCIsImFldGhfdGltzSi6mTY5mTcznTcymCwidxnlcl9pZCI6ilnsnlnks05BOGtkeDlwdGlQOTV0n
FozOlYyVzIiLCJzdWIiOiJTUiZTZEtOOThrZHg5cHRDUDkldDraM0JWMlcyIiwiaWF0IioxNikxnZM
                                                                                                                                                                                                                                            9 X-XSS-Protection: 0
User-Agent: FirebaseAuth.iOS/10.3.0 iPhone/16.0
                                                                          9 Vary: Referer
                                                                                                                                                                                                                                            0 X-Frame-Options: SAMEORIGIN
                                                                          10 Server: ESF
                                                                                                                                             lnzīwlCjleHaiOjE2OTE3MzkzMjAsImZpcmViYXNlIjp7ImlkzW50aXRpZXMiOnt9LCJzaWduX2luX
3Byb3zpZGVyIjoiYW5vbnltb3VzIn19.A_yaImRrI67QyyGXEzrlVciqAVB1lvO38vUOLVnle_4vyT
                                                                                                                                                                                                                                            1 X-Content-Type-Options: nosniff
                                                                          11 Content-Length: 1186
                                                                                                                                                                                                                                            12 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
                                                                          12 X-Xss-Protection: 0
                                                                                                                                             swldYcKUPEAoAzKm2VDdlsT88KbyXZm3lnfU349VvNp3G2LYli4QWqDd2FYh9eBnNMeF0LfCoZYmOV
                                                                                                                                                                                                                                             3 Content-Length: 618
   "returnSecureToken":true
                                                                          13 X-Frame-Options: SAMEORIGIN
                                                                                                                                             VXnwwb19DS3HJIyCsRQ75DpzpGeEq8AFbucrtRURm4-WRMoww7RSFjNEJIdTvO1BZr2E0sM1tmtj6z
                                                                          14 X-Content-Type-Options: nosniff
                                                                                                                                             jHuyoaQ4hv0jMvuIU_CdKLOZ8njrd5q7j1j5_J0DXGcrTGDGm154fJ_CsjV49tUJ8sIlCIzhlgxe7W
Y8IkQBUHUn4WPF_X1ZvnDnt1-k WSkaxA9i6X06tu8r8e2pM2ct0tKF7Cn4eqA
                                                                                                                                             User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
                                                                                                                                              (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36
                                                                                                                                                                                                                                                      "name": "projects/test111-cde14/databases/(default)/documents/users/19811",
                                                                                                                                              Accept: application/json
                                                                               "eyJhbGciOiJSUzI1NiIsImtpZCI6ImNmM2I1YWRhM2NhMzkxNT Accept-Encoding: gzip, deriace
Accept-Language: en-US,en;q=0.9
                                                                                                                                                                                                                                                        "email":{
                                                                                                                                                                                                                                                          "stringValue": "john@labstest.localhost"
                                                                                                                                                                                                                                                        "company_name":{
    "stringValue":"LabsTest"
                                                                               DExMS1jZGUxNCIsImFldGhfdGltZSI6MTY5MTczNTcyMCwidXNl
                                                                               eDlwdGlqOTVONFozqlyyVzIiLCJzdWIiOiJTUJZTZEtOQThrZHg
iaWF0IjoxNikxNzMlNzIWLCJleHaiOjE2OTE3MzkzMjAsImZpcm
                                                                              MiOnt9LCJzaWduX2luX3Byb3ZpZGVyIjoiYW5vbnltb3VzIn19.
AVB1lvO38vUOLVnle 4vyTsWldYcKUPEAoAzKm2VDdlsT88KbyX
                                                                              RSFjNEJIdTv01BZr2E0sMltmtj6zjHuyoaQ4hv0jMvuIU_CdKLO:
Gm154fJ CsjV49tUJ8sIlCIzhlqxe7WY8IkOBUHUn4WPF X1Zvn
                                                                                                                                                                                                                                                          "booleanValue":true
                                                                               e2pM2ct0tKF7Cn4eqA",
                                                                                                                                                                                                                                                           "timestampValue":"2023-08-07T07:00:00.239Z"
                                                                                AMf-vBwBIfPNes0jijn-mGl2cYkRw4aKBX8fXuZPYE-7keeiYr
                                                                               dj-gVqyeQ1j8HZ9ccGGEXnymaXiOiqr vfV8Uy-69-BMupXyA5k
                                                                               9T4Sw5Kk 9w-bGfhiAcvuQph5KqIwx7D0U",
                                                                               "localId": "SR6SdKNA8kdx9ptiP95t4Z3BV2W2"
```

# Firebase Storage

Sample auth rules

```
rules_version = '2';
service firebase.storage {
 match /b/{bucket}/o {
   match /{allPaths=**} {
      allow read: if request.auth != null;
```

# Firebase Storage

Sample Unauth rules

```
rules_version = '2';
service firebase.storage {
 match /b/{bucket}/o {
    match /{allPaths=**} {
      allow read: if true;
```

### Firebase Storage: Authenticated Access

```
GET /v0/b/test111-cde14.appspot.com/o/ HTTP/2
Host: firebasestorage.googleapis.com
Accept-Language: en-US, en; q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
```

```
1 HTTP/2 403 Forbidden
 2 X-Guploader-Uploadid:
  ADPycdsw2v0sz8K4xIzJ3BtMWa0fPj1MmWfd9nS0
  U70jXbpbdrxfV5Ap
3 X-Content-Type-Options: nosniff
 4 Content-Type: application/json; charset=
 5 Access-Control-Expose-Headers: Content-F
 6 Access-Control-Allow-Origin: *
 7 Date: Fri, 11 Aug 2023 06:51:24 GMT
 8 Expires: Fri, 11 Aug 2023 06:51:24 GMT
 9 Cache-Control: private, max-age=0
10 Content-Length: 73
11 Server: UploadServer
12 Alt-Svc: h3=":443"; ma=2592000,h3-29=":4
13
14 {
    "error":{
       "code":403,
16
       "message": "Permission denied."
17
18
19 }
```

# Firebase Storage: Unauthenticated Access

```
1 HTTP/2 200 OK
GET /v0/b/test111-cde14.appspot.com/o/ HTTP/2
                                                        2 X-Guploader-Uploadid:
Host: firebasestorage.googleapis.com
Accept-Language: en-US, en; g=0.5
                                                          ADPycdvH3Bq7KrGfuthsGS2ec9VHDTaCoMVKR7873RRx-aRvU-idD6nG-5tqV4AC uBX8t
Accept-Encoding: gzip, deflate
                                                           ar6hCnm9A
                                                        3 X-Content-Type-Options: nosniff
Upgrade-Insecure-Requests: 1
                                                        4 Content-Type: application/json; charset=UTF-8
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
                                                        5 Access-Control-Expose-Headers: Content-Range, X-Firebase-Storage-XSRF
                                                        6 Access-Control-Allow-Origin: *
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
                                                        7 Date: Fri, 11 Aug 2023 06:53:40 GMT
Te: trailers
                                                        8 Expires: Fri, 11 Aug 2023 06:53:40 GMT
                                                        9 Cache-Control: private, max-age=0
                                                       10 Content-Length: 126
                                                       11 Server: UploadServer
                                                       12 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
                                                            "prefixes":[
                                                            "items":[
                                                                "name": "ok\u202eok.txt",
                                                                "bucket": "test111-cde14.appspot.com"
                                                       22 }
```

# Firebase Storage: request.auth vulnerability

```
GET /v0/b/test111-cde14.appspot.com/o/ HTTP/2
Host: identitytoolkit.googleapis.com
                                                                                                                         2 Expires: Mon, 01 Jan 1990 00:00:00 GMT
                                                                                                                                                                                                                                                      Host: firebasestorage.googleapis.com
                                                                                                                                                                                                                                                                                                                                                                                                   2 X-Guploader-Uploadid:
Content-Type: application/json
                                                                                                                         3 Pragma: no-cache
                                                                                                                                                                                                                                                      Accept-Language: en-US, en; g=0.5
                                                                                                                                                                                                                                                                                                                                                                                                       ADPvcdu0XfhCLexKkpp4WxPMWOVhNwh1T5X57ovmojKUHvYU
                                                                                                                         4 Date: Fri, 11 Aug 2023 06:35:20 GMT
X-Client-Version: iOS/FirebaseSDK/10.3.0/FirebaseCore-iOS
                                                                                                                         5 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Authorization: Bearer
                                                                                                                                                                                                                                                                                                                                                                                                       cvruVkh87A
                                                                                                                         6 Content-Type: application/json; charset=UTF-8
Accept-Encoding: gzip, deflate
                                                                                                                                                                                                                                                      evJhbGciOiJSUzI1NiIsImtpZCI6ImNmM2I1YWRhM2NhMzkxNTO
                                                                                                                                                                                                                                                                                                                                                                                                   3 X-Content-Type-Options: nosniff
                                                                                                                                                                                                                                                                                                                                                                                                   4 Content-Type: application/json; charset=UTF-8
                                                                                                                                                                                                                                                      4ZDM1OTJiMzU5MjkvM2UzNjAxMmI5MTOiLCJ0eXAiOiJKV1OifO
Content-Length: 31
                                                                                                                         8 Vary: X-Origin
                                                                                                                                                                                                                                                      .eyJwcm92aWRlc19pZCI6ImFub255bW91cyIsImlzcyI6Imh0dH
                                                                                                                                                                                                                                                                                                                                                                                                   5 Access-Control-Expose-Headers: Content-Range, X-
User-Agent: FirebaseAuth.iOS/10.3.0 iPhone/16.0
                                                                                                                         9 Vary: Referer
hw/iPhone13 4
                                                                                                                       10 Server: ESF
                                                                                                                                                                                                                                                      BzOi8vc2VjdXJldG9rZW4uZ29vZ2xlLmNvbS90ZXN0MTExLWNkZ
                                                                                                                                                                                                                                                                                                                                                                                                   6 Access-Control-Allow-Origin: *
                                                                                                                       11 Content-Length: 1186
                                                                                                                                                                                                                                                      TE0IiwiYXVkIjoidGVzdDExMS1jZGUxNCIsImF1dGhfdGltZSI6
                                                                                                                                                                                                                                                                                                                                                                                                   7 Date: Fri, 11 Aug 2023 06:59:37 GMT
                                                                                                                       12 X-Xss-Protection: 0
                                                                                                                                                                                                                                                                                                                                                                                                   8 Expires: Fri, 11 Aug 2023 06:59:37 GMT
                                                                                                                                                                                                                                                      MTY5MTczNTcyMCwidXNlcl9pZCI6IlNSNlNkS05BOGtkeDlwdGl
    "returnSecureToken":true
                                                                                                                       13 X-Frame-Options: SAMEORIGIN
                                                                                                                       14 X-Content-Type-Options: nosniff
                                                                                                                                                                                                                                                      OOTVONFozOlyvVzIiLCJzdWIiOiJTUiZTZEtOOThrZHq5cHRpUD
                                                                                                                                                                                                                                                                                                                                                                                                   9 Cache-Control: private, max-age=0
                                                                                                                       15 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
                                                                                                                                                                                                                                                      k1dDRaM0JWMlcyIiwiaWF0IjoxNjkxNzM1NzIwLCJleHAi0jE20
                                                                                                                                                                                                                                                                                                                                                                                                  10 Content-Length: 126
                                                                                                                                                                                                                                                      TE3MzkzMjAsImZpcmViYXNlIjp7ImlkZW50aXRpZXMiOnt9LCJz
                                                                                                                                                                                                                                                                                                                                                                                                11 Server: UploadServer
                                                                                                                                "kind": "identitytoolkit#SignupNewUserResponse",
                                                                                                                                                                                                                                                                                                                                                                                                12 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=
                                                                                                                                                                                                                                                      aWduX2luX3Byb3ZpZGVyIjoiYW5vbnltb3VzIn19.A yaImRrI6
                                                                                                                                                                                                                                                      7QyyGXEZr1VciqAVB11v038vUOLVn1e 4vyTsW1dYcKUPEAoAzK
                                                                                                                                 eyJhbGciOiJSUzI1NiIsImtpZCI6ImNmM2I1YWRhM2NhMzkxNTQ4ZDM1OTJ"
                                                                                                                                AXMMISMTQiLCJ0eXAiOiJKVl0ifQ.eyJwcm92aWRlcl9pZCT6ImFub255bw91m2VDdlsT88KbyXZm3lnfU349VVNp3G2LY1i4QWqDd2FYh9eBnNM
                                                                                                                                                                                                                                                                                                                                                                                                14 {
                                                                                                                                h0dHbzoi8vc2VjdXJldG9rzW4uz29vz2x1LmNvbS90ZXN0MTEXLWNkZTE0IiveF0LfCoZYmOVVXnwwb19DS3HJIyCsRO75DpzpGeEg8AFbucrtRU
                                                                                                                                                                                                                                                                                                                                                                                                              "prefixes":[
                                                                                                                                                                                                                                                     Rm4-WRMoww7RSFjNEJIdTvO1BZr2E0sMltmtj6zjHuyoaQ4hv0j
                                                                                                                                iawf0ijoxnjkxnzminziwLCJleHaiojE2OTE3MzkzmjaSimwpcmVixmlijp7MvuIU CdKLOZ8njrd5q7j1j5 J0DXGcrTGDGm154fJ CsjV49tU
                                                                                                                                                                                                                                                                                                                                                                                                              "items":[
                                                                                                                                MiOnt91CJzaWduX2luX3Byb3ZpZgVyIjoiYW5vbnltb3VzIn19.A_yaImRr16J8sIlCIzhlgxe7WY8IkQBUHUn4WPF X1ZvnDntl-k WSkaxA9i6
                                                                                                                               NIONEYILGZZANGUNZTUKJENYGJEZEN 1 1 JANUARY NIONE NIONE
                                                                                                                                                                                                                                                                                                                                                                                                                        "name": "ok\u202eok.txt",
                                                                                                                                qDd2FYh9eBnNMeF0LfCoZYmOVVXnwwb19DS3HJIyCsRQ75DpzpGeEq8AFbu
                                                                                                                                godzr ingeminderolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimovolitozimov
                                                                                                                                                                                                                                                                                                                                                                                                                        "bucket": "test111-cde14.appspot.com"
                                                                                                                                                                                                                                                      Sec-Fetch-Dest: document
                                                                                                                                "AMf-vBwBIfPNes0jijn-mGl2cYkRw4aKBX8fXuZPYE-7keeiYrElvgoFsMvfSec-Fetch-Mode: navigate
                                                                                                                                                                                                                                                                                                                                                                                                22 }
                                                                                                                                dj-gVqyeQlj8HZ9ccGGEXnymaXi0iqr_vfV8Uy-69-BMupXyA5k7KYWVYFMewSec-Fetch-Site: none
                                                                                                                                9T4Sw5Kk 9w-bGfhiAcvuOph5KgIwx7D0U",
                                                                                                                                                                                                                                                      Sec-Fetch-User: ?1
                                                                                                                                "expiresIn": "3600",
                                                                                                                                                                                                                                                      Te: trailers
                                                                                                                               "localId": "SR6SdKNA8kdx9ptiP95t4Z3BV2W2'
```

# Automating at scale

### Vuln scanning

#### Identify API type

- Not all Google API keys are Firebase.
- Identify if a Firebase key is using Identity Toolkit.

#### Test Firestore

#### **Auth and Unauth access**

- Identify project for a given API key
- Test if firestore is access without authentication
- Test firestore with anonymous token

# Test Firebase storage

#### Auth and unauth access

- Identify project for given API key.
- Access Firebase Storage without authentication.

#### Identify API type

- Accessing the identity toolkit API to list project's domains tells us if the project is using identity toolkit.
- If identity toolkit is enabled, get project name: project-name.firebaseapp.com

```
1 GET /v1/projects?key=AIzaSyDu0VfJe0PFTOrGLFhQObibMzzJQR6XbT4 HTTP/2
2 Host: identitytoolkit.googleapis.com
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) C
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/a
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Te: trailers

? Search...
```

# Test authentication - Is Anonymous enabled?

While not a vulnerability, anonymous signup could be used later on.

```
POST /v1/accounts:signUp?key=
AlzaSyDu0VfJe0PFTOrGLFhQObibMzzJQR6XbT4 HTTP/2
                                                                                                                                                             AlzaSyDu0VfJe0PFTOrGLFhQObibMzzJQR6XbT4 HTTP/2
                                                                                                                                                                                                                               2 Expires: Mon, 01 Jan 1990 00:00:00 GMT
                                                                             2 Date: Fri, 11 Aug 2023 06:34:58 GMT
                                                                                                                                                            2 Host: identitytoolkit.googleapis.com
                                                                                                                                                                                                                               3 Pragma: no-cache
2 Host: identitytoolkit.googleapis.com
                                                                             3 Pragma: no-cache
                                                                                                                                                            3 Content-Type: application/json
                                                                                                                                                                                                                               4 Date: Fri, 11 Aug 2023 06:35:20 GMT
3 Content-Type: application/json
                                                                             4 Expires: Mon, 01 Jan 1990 00:00:00 GMT
                                                                                                                                                                                                                               5 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
4 Accept: */*
                                                                             5 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
                                                                                                                                                            5 X-Client-Version: iOS/FirebaseSDK/10.3.0/FirebaseCore-iOS
                                                                                                                                                                                                                               6 Content-Type: application/json; charset=UTF-8
5 X-Client-Version: iOS/FirebaseSDK/10.3.0/FirebaseCore-iOS
                                                                             6 Vary: Origin
                                                                                                                                                            6 Accept-Encoding: gzip, deflate
                                                                                                                                                                                                                               7 Vary: Origin
Accept-Encoding: gzip, deflate
                                                                             7 Vary: X-Origin
                                                                                                                                                                                                                               8 Vary: X-Origin
                                                                             8 Vary: Referer
                                                                                                                                                            8 Content-Length: 31
                                                                                                                                                                                                                               9 Vary: Referer
 Accept-Language: en
                                                                                                                                                            9 User-Agent: FirebaseAuth.iOS/10.3.0 iPhone/16.0
                                                                                                                                                                                                                              10 Server: ESF
8 Content-Length: 31
                                                                             9 Content-Type: application/json; charset=UTF-8
                                                                                                                                                                                                                              11 Content-Length: 1186
User-Agent: FirebaseAuth.iOS/10.3.0 iPhone/16.0
                                                                            10 Server: ESF
                                                                                                                                                                                                                              12 X-Xss-Protection: 0
                                                                            11 Content-Length: 214
                                                                                                                                                                                                                              13 X-Frame-Options: SAMEORIGIN
                                                                            12 X-Xss-Protection: 0
                                                                                                                                                                "returnSecureToken":true
                                                                                                                                                                                                                              14 X-Content-Type-Options: nosniff
                                                                                                                                                                                                                              15 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
                                                                           13 X-Frame-Options: SAMEORIGIN
    "returnSecureToken":true
                                                                           14 X-Content-Type-Options: nosniff
                                                                            15 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
                                                                                                                                                                                                                                  "idToken":
                                                                                  "error":{
                                                                                    "code":400,
                                                                                    "message": "ADMIN_ONLY_OPERATION",
                                                                                                                                                                                                                                  eDlwdGlQOTV0NFozQlYyVzIiLCJzdWIiOiJTUjZTZEtQQThrZHg5cHRpUDkldDRaM0JWMlcyIiv
                                                                                                                                                                                                                                  iaWF0IjoxnjkxnzMlnzlwLCJleHAiOjE2OTE3MzkzMjAsImZpcmViYXNlIjp7ImlkZW50aXRpZ
MiOnt9LCJzaWduX2luX3Byb3ZpZGVyIjoiYW5vbnltb3VzIn19.A_yaImRrI67QyyGXEZr1Vcic
                                                                                         "message": "ADMIN_ONLY_OPERATION",
                                                                                                                                                                                                                                  AVB11vO38vUOLVnle 4vyTsW1dYcKUPEAoAzKm2VDdlsT88KbyXZm3lnfu349VvNp3G2LY1i4Qi
                                                                                         "domain": "global",
                                                                                                                                                                                                                                  qDd2FYh9eBnNMeF0LTCo2YmOVVXnwwb19DS3HJIyCsRQ75DpzpGeEq8AFbucrtRURm4-WRMoww7RSFjNEJIdTv01BZr2E0sMltmtj6zjHuyoaQ4hv0jMvuIU_CdKLOZ8njrd5q7j1j5_J0DXGcrTGD
                                                                                         "reason": "invalid'
                                                                                                                                                                                                                                  Gm154fJ_CsjV49tUJ8sIlCIzhlgxe7WY8IkQBUHUn4WPF_X1ZvnDntl-k WSkaxA9i6X06tu8r8
                                                                                                                                                                                                                                  e2pM2ct0tKF7Cn4eqA",
                                                                                                                                                                                                                                   "refreshToken":
                                                                                                                                                                                                                                  dj-gVqyeQ1j8HZ9ccGGEXnymaXiOiqr vfV8Uy-69-BMupXyA5k7KYWVYFMewr5zkQj5SsapVH
                                                                                                                                                                                                                                   9T4Sw5Kk 9w-bGfhiAcvuQph5KqIwx7D0U",
                                                                                                                                                                                                                                  "expiresIn": "3600",
"localId": "SR6SdKNA8kdx9ptiP95t4Z3BV2W2"
```

#### Firestore - Check unauthenticated access

- Project name from identity toolkit API.
- API call:

https://content-firestore.googleapis.com/v1/projects/test111-cde14/databas es/(default)/documents/nonexistdocument

- If 200 with empty result:
  - All documents are accessible without authentication
- If Missing or insufficient permissions.
  - All documents may require authentication
  - Some documents may still be accessible without authentication

#### Firestore - Check authenticated access

- Project name from identity toolkit API.
- If API returned "Access Denied" and Anonymous signup is enabled
- API call:

https://content-firestore.googleapis.com/v1/projects/test111-cde14/databas es/(default)/documents/nonexistdocument with Authorization header

#### Firestore - Check authenticated access

- Project name from identity toolkit API.
- If API returned "Access Denied" and Anonymous signup is enabled
- API call:

https://content-firestore.googleapis.com/v1/projects/test111-cde14/databas es/(default)/documents/nonexistdocument with Authorization header

```
1 GET /v1/projects/test111-cde14/databases/(default)/documents/users?pageSize=1
 HTTP/1.1
2 Host: firestore.googleapis.com
3 Upgrade-Insecure-Requests: 1
4 Authorization: Bearer
 eyJhbGciOiJSUzI1NiIsImtpZCI6ImNmM2I1YWRhM2NhMzkxNTQ4ZDM1OTJiMzU5MjkyM2UzNjAxMm
 I5MTQiLCJ0eXAiOiJKV1QifQ.eyJwcm92aWRlc19pZCI6ImFub255bW91cyIsIm1zcyI6Imh0dHBzO
 i8vc2VjdXJldG9rZW4uZ29vZ2xlLmNvbS90ZXN0MTExLWNkZTE0IiwiYXVkIjoidGVzdDExMS1jZGU
 xNCIsImF1dGhfdGltZSI6MTY5MTczNTcyMCwidXNlc19pZCI6I1NSN1NkS05BOGtkeDlwdGlQOTV0N
 FozQlYyVzIiLCJzdWIiOiJTUjZTZEtOQThrZHq5cHRpUDkldDRaM0JWMlcyIiwiaWF0IjoxNjkxNzM
 1NzIwLCJleHAiOjE2OTE3MzkzMjAsImZpcmViYXNlIjp7ImlkZW50aXRpZXMiOnt9LCJzaWduX2luX
 3Byb3ZpZGVyIjoiYW5vbnltb3VzIn19.A yaImRrI67QyyGXEZr1VciqAVB1lvO38vUOLVn1e 4vyT
 sWldYcKUPEAoAzKm2VDdlsT88KbyXZm3lnfU349VvNp3G2LY1i4OWgDd2FYh9eBnNMeF0LfCoZYmOV
 VXnwwbl9DS3HJIyCsRO75DpzpGeEg8AFbucrtRURm4-WRMoww7RSFjNEJIdTvO1BZr2E0sMltmtj6z
 jHuyoaQ4hv0jMvuIU CdKLOZ8njrd5q7j1j5 J0DXGcrTGDGm154fJ CsjV49tUJ8sIlCIzhlgxe7W
 Y8IkQBUHUn4WPF X1ZvnDntl-k WSkaxA9i6X06tu8r8e2pM2ct0tKF7Cn4eqA
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36
6 Accept: application/json
 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US, en; q=0.9
```

#### Storage - Check unauthenticated access

- Project name from identity toolkit API.
- API call:

https://firebasestorage.googleapis.com/v0/b/project-name.appspot.com/o/

- If vulnerable: Lists all files in a given storage
- o If Permission Denied and anonymous sign up enabled
  - Re-send request with Authorization header

#### **Automation Final**

```
rojanrijal@rojanrijal-1175 firebase-test-codes % python3.9 main.py --api AIzaSyCjQ_Gq5p03UCaIxt9mWhakHv4tfadDREs INFO: > Auditing AIzaSyCjQ_Gq5p03UCaIxt9mWhakHv4tfadDREs INFO: >> Following projects were guessed for this API Key. testfirestore-76d64 WARNING: >> Anonymous signup is allowed with this API Key. INFO: >> Testing access for testfirestore-76d64 WARNING: >> Vulnerability: Logged in users (Anonymous) can access firestore collections. WARNING: >> Vulnerability: Buckets can be dumped by any logged in user (ex: Anonymous user). rojanrijal@rojanrijal-1175 firebase-test-codes % python3.9 main.py --api AIzaSyDu0VfJe0PFTOrGLFhQ0bibMzzJQR6XbT4 INFO: >> Auditing AIzaSyDu0VfJe0PFTOrGLFhQ0bibMzzJQR6XbT4 INFO: >> Following projects were guessed for this API Key. test111-cde14 WARNING: >> Anonymous signup is allowed with this API Key. INFO: >> Testing access for test111-cde14 WARNING: >> Vulnerability: Logged in users (Anonymous) can access firestore collections. WARNING: >> Vulnerability: Buckets can be dumped by any logged in user (ex: Anonymous user). rojanrijal@rojanrijal-1175 firebase-test-codes %
```

# Scanning the web

# Sourcegraph Scans

- 15,000 Google API keys extracted.
- 4498 Unique API keys.
- 1705 Identity toolkit enabled
- 249 had Anonymous Sign up
- 35 Unauthenticated Firestore accessible
- 20 Unauth Firebase storage accessible
- 10 Firestore accessible with auth
- 5 Firebase storage accessible with auth

# Commoncrawl

- 1000 unique Firebase api keys
- 692 Identity Toolkit enabled
- 80 out of 692 Anonymous sign up enabled
- 55 Unauthenticated Firestore
   DB
- **15** Unauthenticated Storage buckets
- 10 Firestore DB accessible with anonymous login
- 10 Firebase Storage
   accessible with anonymous
   login

# Common vulnerable categories

- Early stage startups
- New AI applications built on top of conversational APIs from OpenAI
- Demo applications with real users

#### Conclusions & References

- It is common for new companies to mis-configure their firebase instances.
- Securing instances:
  - Strict rules than just request.auth != null for example requiring cross-checking data with logged in users' ID.
- AWS Cognito Talk:
  - https://www.youtube.com/watch?v=\_Ek0F-Xh57w
- Social Media
  - Twitter/X: @uraniumhacker / @TinderEng