

# Quiz

---

## Context:

It's an Android application that displays math questions. The user must answer 500 questions correctly within 60 seconds to obtain the flag.

## Solution:

Let's check the source code of HomeActivity.java with APKLab on vsodium/vscode:

1. Use shortcut : ctrl+maj+P 'APKLAB: Open an APK'
2. Select your apk
3. check '--decompile \_java', '--deobf', '--show-bad-code' and unchecked '--only-main-classes'

Now, go to /java\_src/com/intigriti/quiz/HomeActivity.java :

```
/* renamed from: t */
public final void m2135t(int i) {
    int i2 = this.f1762D;
    if (i != i2) {
        m2133v("Wrong Answer!", false);
        return;
    }
    int i3 = this.f1760B + i2;
    this.f1760B = i3;
    int i4 = this.f1761C + 1;
    this.f1761C = i4;
    if (i4 < this.f1763E.length) {
        m2134u();
        return;
    }
    String valueOf = String.valueOf(i3 + this.f1765G);
    JSONObject jsonObject = new JSONObject();
    jsonObject.put("game_id", this.f1767I);
    jsonObject.put("end_time", valueOf);
    Executors.newSingleThreadExecutor().submit(new RunnableC0379q(this, 5, jsonObject));
}
```

As we can see it : the app checks if user responses are correct.

If responses don't match: the app exits

Else : The app add the result to a variable "i3" "i4" is the user score | number of questions. While the number of question is lower than the number of total questions (500) the quizz continue. At the end application sends a body POST request like this:

```
{"game_id": "23660d0b-3c0c-43cd-a324-d131e6d2e89b", "end_time": 1731825092654+i3}
```

So we can automate the solution.

Here is my python script to get the flag :

```

from re import search
import requests
import time
from json import dumps

time1 = int(time.time())

URL_START = "https://quiz.ctf.intigriti.io/start"
URL_END = "https://quiz.ctf.intigriti.io/submit"

head = {'content-type': "application/json;charset=utf-8", "content-length": "28", "accept-encoding": "gzip", "user-agent": "okhttp/4.12.0"}
solv = 0

rgx = r'(.*)\s(.*)\s(.*)'

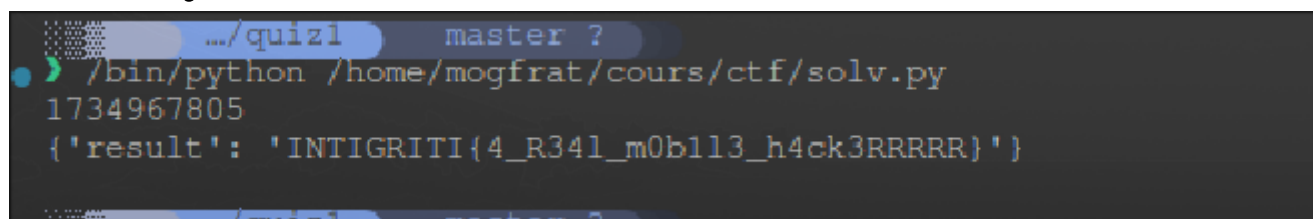
z =
requests.post(URL_START, headers=head, data=dumps({"start_time": time1})).json()
for i in z['equations']:
    a = search(rgx, i).groups()
    if a[1] == '+':
        solv += (int(a[0]) + int(a[2]))
    elif a[1] == '-':
        solv += (int(a[0]) - int(a[2]))
    elif a[1] == '/':
        solv += ((int(a[0]) // int(a[2])))
    else:
        solv += ((int(a[0]) * int(a[2])))

head['content-length'] = '77'
print(requests.post(URL_END, headers=head, data=dumps({"game_id": z['game_id'], "end_time": time1 + solv})).json())

```

Note: The URLs can be found in 'RunnableC0379q.java' and 'RunnableC0406b.java'. I found these with PCAndroid.

Here is the flag :



```

.../quiz1 master ?
$ /bin/python /home/mogfrat/cours/ctf/solv.py
1734967805
{'result': 'INTIGRITI{4_R34l_m0b113_h4ck3RRRRR}'}
.../quiz1 master ?

```