Frida hello world PART #1

بسم الله الرحمن الرحيم اليوم بناخذ نبذة عن frida

What is frida

ايش ممكن تسوي لنا frida؟ باختصار تتيح لنا امكانية تعديل على طريقة عمل البرنامج خلوني اعطيكم مثال بسيط

```
function login(){
is_admin = false
if(is_admin){
print("Welcome admin")
}
}
```

هذا كود بسيط كتبته عشان يكون الشرح اسهل باختصار فنكشن login بتسوي متغير is_admin و المتغير ذا دايم false باستخدام frida اقدر اخليه true و امشي طبيعي

Install firda

قبل اي شي لازم تعرف معلومات من ال android vm حقك

```
adb shell getprop ro.product.cpu.abi
```

اذا طبقت الامر هذا من ال adb بتعرف ال arch حق جهازك و منه تقدر تحمل ال frida server اللي تبيه من هنا بعد https://github.com/frida/frida/releases

بعد ما تحمله و تحمل ادوات ال frida باستخدام pip

```
pip install frida
pip install frida-tools
```

و بعد ما تحمله حط ال package name و ال path حق js file حقك

```
frida -U -f <package name> -l <js file >
```

و منها تقدر تستخدم frida بدون اي مشكلة ممكن تقرا frida docs اذا فيه شي مو واضح او طلعت لك مشكلة

Solve challenge 1

1. Change class challenge_01's variable 'chall01' to: 1
2. Run chall02()
3. Make chall03() return true
4. Send "frida" to chall04()
5. Always send "frida" to chall05()
6. Run chall06() after 10 seconds with correct value
7. Bruteforce check07Pin() then confirm with chall07()
8. Change 'check' button's text value to 'Confirm'

هنا عندنا برنامج fridalab ممكن نطبق عليه فيه اكثر من تحدي اول تحدي يبي الكلاس حق challenge_01 نغير قيمت chall01 الى 1

```java
package uk.rossmarks.fridalab;

/* loaded from: classes.dex */
public class challenge_01 {
    static int chall01;

    public static int getChall01Int() {
        return chall01;
    }
}
```

هذا الكود جدا بسيط الحين بكتب frida سكربت يسوي اللي يبغاه بالسؤال

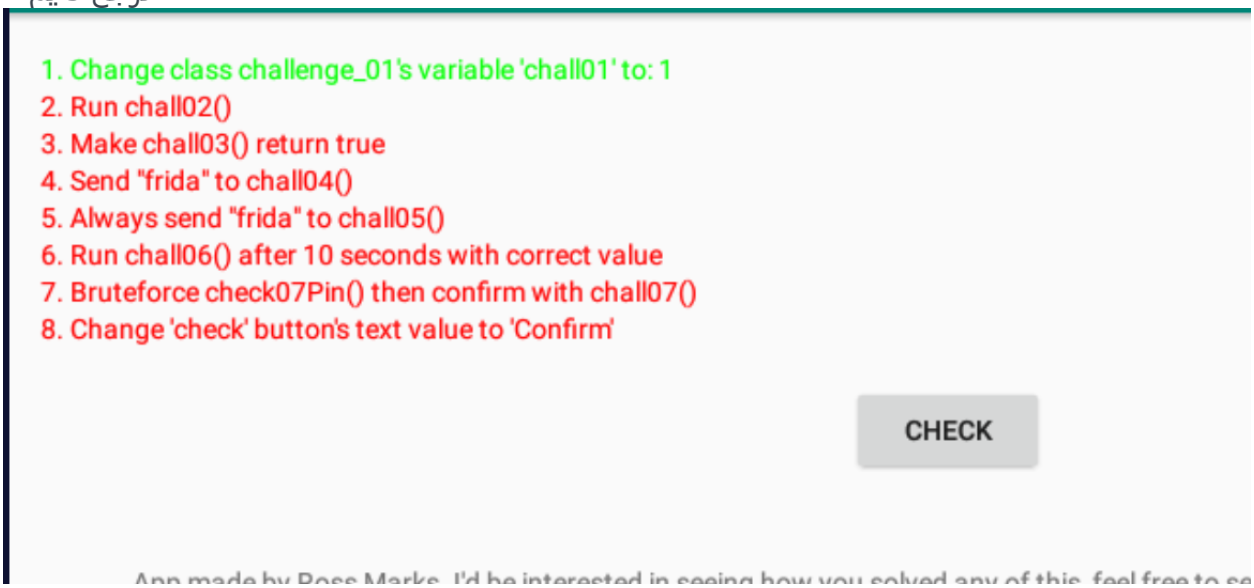
```
Java.perform(function(){
                var mainapp =
Java.use("uk.rossmarks.fridalab.challenge_01");
                mainapp.getChall01Int.implementation = function(){
                    return 1
                };


});
```

```
var mainapp = Java.use("uk.rossmarks.fridalab.challenge_01");
```

بالبداية بناخذ ال path حق الكلاس اللي نبيه ف نحط الباث كامل عشان نقدر نغير في طريقة عمل الفنكشن اللي نبيها

```
mainapp.getChall01Int.implementation = function(){
                    return 1
                };
```

هنا اخذت الفنكشن و سويت لها زي ال overwrite ف صرت اتحكم بطريقة عملها و اخلي الفنكشن ترجع دايم 1



بكل سهوله حلينا التحدي رقم 1 مع ان فيه طريقة اسهل من كذا بس و هذا الكود حقها

```
var challenge_01 = Java.use('uk.rossmarks.fridalab.challenge_01');
challenge_01.chall01.value = 1;
```

هذا الكود بيغير قيمه ال chall01 في الكلاس نفس النتيجة بس الطريقة تختلف

Solve Challenge 2

1. Change class challenge_01's variable 'chall01' to: 1
2. Run chall02()
3. Make chall03() return true
4. Send "frida" to chall04()
5. Always send "frida" to chall05()
6. Run chall06() after 10 seconds with correct value
7. Bruteforce check07Pin() then confirm with chall07()
8. Change 'check' button's text value to 'Confirm'

التحدي الثاني يبينا بس نسوي call لفنكشن معينة

```
Java.perform(function(){
var mainapp = Java.use("uk.rossmarks.fridalab.MainActivity");
mainapp.chall02()

});
```

هذا الكود بيسوي call ل ال chall02 من ال MainActivity لأن الفنكشن متواجدة في هذاك الكلاس

```
[SM-G965N::uk.rossmarks.fridalab ]-> Error: chall02: cannot call instance method without an instance
    at value (frida/node_modules/frida-java-bridge/lib/class-factory.js:1135)
    at e (frida/node_modules/frida-java-bridge/lib/class-factory.js:606)
    at <anonymous> (/mnt/c/Users/kira2/Desktop/aaa.js:3)
    at <anonymous> (frida/node_modules/frida-java-bridge/lib/vm.js:12)
    at _performPendingVmOps (frida/node_modules/frida-java-bridge/index.js:250)
    at <anonymous> (frida/node_modules/frida-java-bridge/index.js:242)
    at apply (native)
    at ne (frida/node_modules/frida-java-bridge/lib/class-factory.js:673)
    at <anonymous> (frida/node_modules/frida-java-bridge/lib/class-factory.js:651)
```

و لكن اذا شغلنا frida بيطلع لنا cannot call instance method without an instance Error لازم نسوي instance اول

```
Java.perform(function() {

var main;
Java.choose('uk.rossmarks.fridalab.MainActivity', {
  onMatch: function(instance) {
    main = instance;
  },
  onComplete: function() {}
});
```

```
main.chall02();
})
```

هنا حلينا المشكلة و سويت call بدون اي مشكلة

Solve challenge 3

```
package uk.rossmarks.fridalab;

import android.os.Bundle;
import android.support.p000v4.internal.view.SupportMenu;
import android.support.p003v7.app.AppCompatActivity;
import android.view.View;
import android.widget.Button;
import android.widget.TextView;
import java.util.Random;
import java.util.Timer;
import java.util.TimerTask;

/* loaded from: classes.dex */
public class MainActivity extends AppCompatActivity {
    public int[] completeArr = {0, 0, 0, 0, 0, 0, 0, 0};

    public boolean chall03() {
        return false;
    }
```

بالتحدي هذا يبينا نخلي ال false ل true بنسوي زي التحدي الاول بالضبط بس بنغير ال 1 الى true مع تغيير ال class path

```
Java.perform(function(){
    var mainapp = Java.use("uk.rossmarks.fridalab.MainActivity");
    mainapp.chall03.implementation = function(){
        return true
    };
});
```

1. Change class challenge_01's variable 'chall01' to: 1
2. Run chall02()
3. Make chall03() return true
4. Send "frida" to chall04()
5. Always send "frida" to chall05()
6. Run chall06() after 10 seconds with correct value
7. Bruteforce check07Pin() then confirm with chall07()
8. Change 'check' button's text value to 'Confirm'

و بكذا حلينا اول 3 تحديات من fridalab ان شاء الله فكره frida واضحة انها تخليك تعدل على الفنكشنز كأنك قاعد تعيد برمجتها من جديد او بشكل اصح تسوي hooking عليها و ال hooking هو تعديل على طريقة عمل الفنكشن