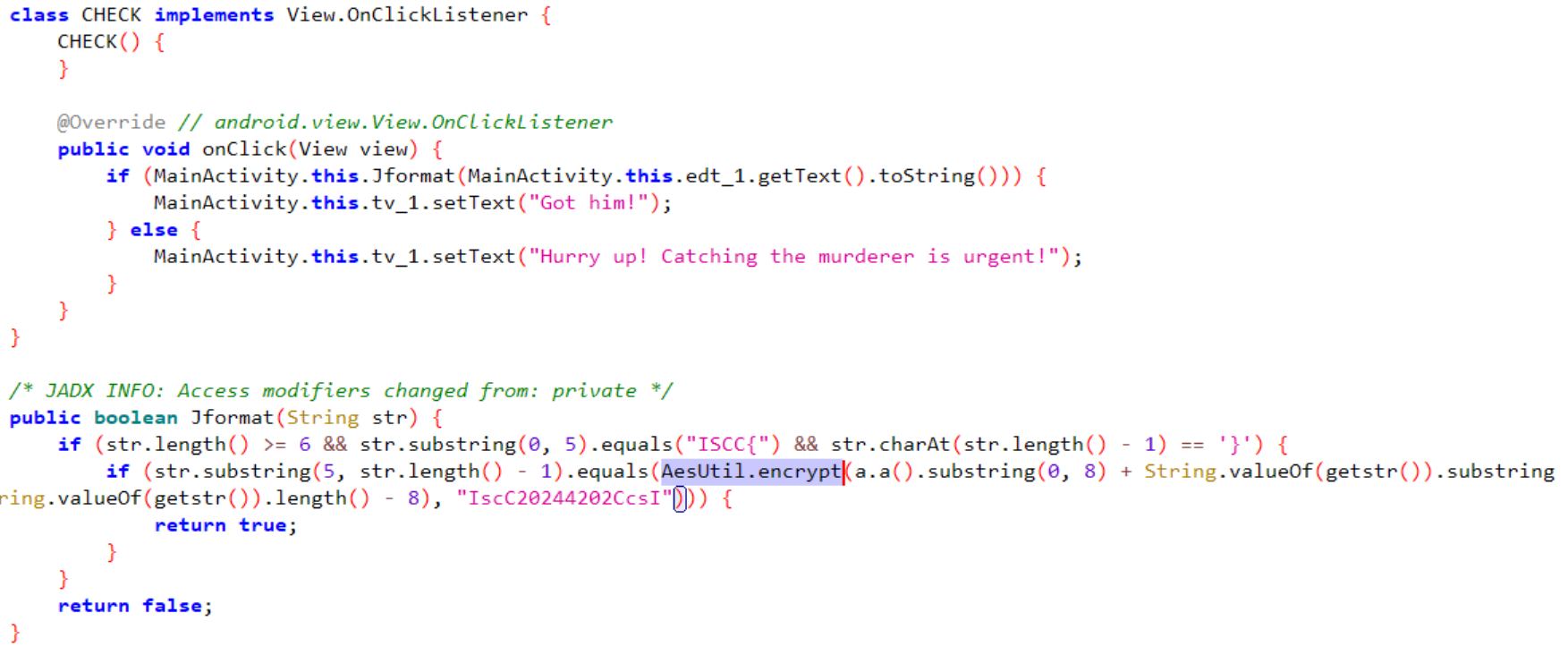
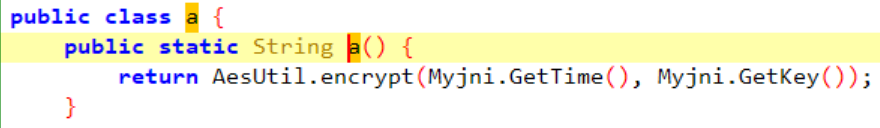
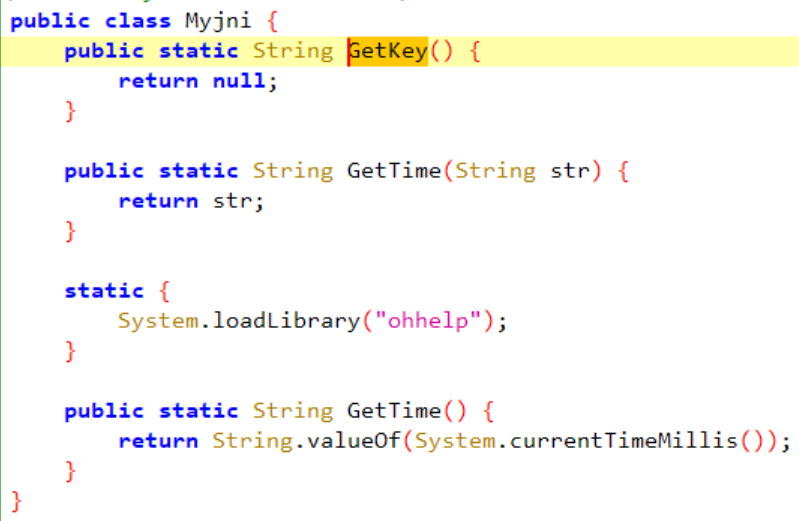
# Mobile+ohHELP

开始以为hook掉AesUtil.encrypt拿返回值就行了



check发现a.a()会异常，原因是GetKey返回了null





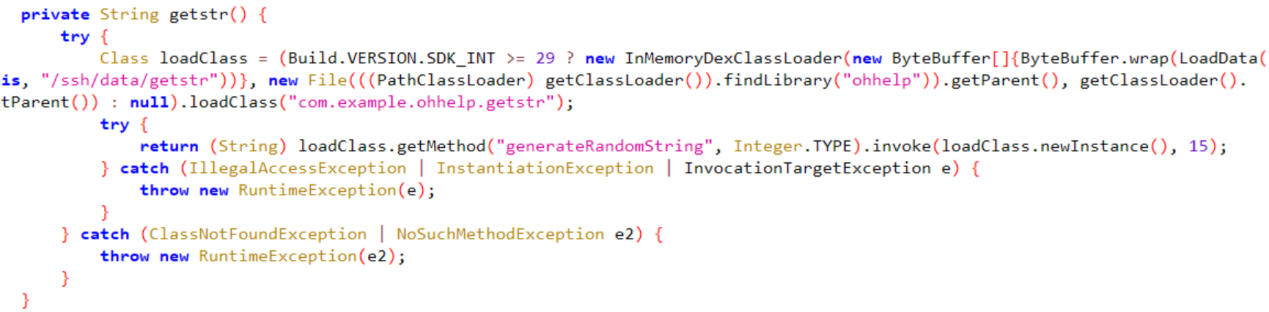
在assets->ssh翻到一个word，镜像后得到”PUDzbflthjqxlJVW”，应该就是GetKey的返回值



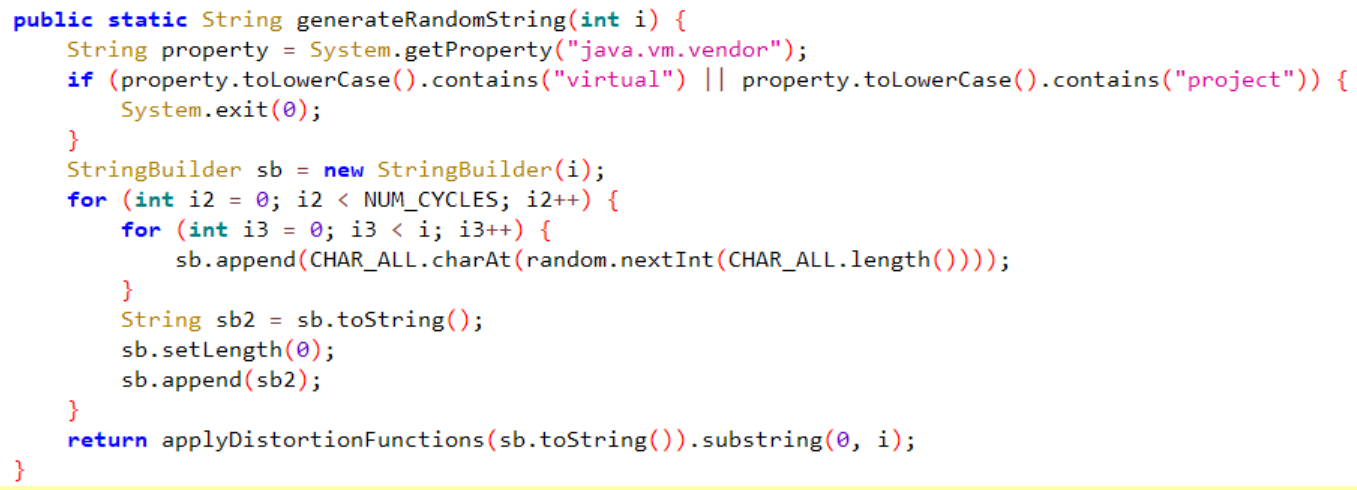
frida设置GetKey返回值

|  |
| --- |
| let Myjni = Java.use("com.example.ohhelp.MyJNI.Myjni");  Myjni["GetKey"].implementation = function () {  console.log('GetKey is called');  let ret = this.GetKey();  console.log('GetKey ret value is ' + ret);  return "PUDzbflthjqxlJVW";  }; |

getstr反射调用com.example.ohhelp.getstr.generateRandomString



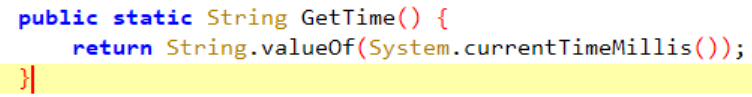
发现校验property时会退出



frida设置System.getProperty返回值

|  |
| --- |
| let System = Java.use('java.lang.System');  System.getProperty.overload('java.lang.String').implementation = function (propertyName) {  var returnValue = this.getProperty(propertyName);  console.log("System.getProperty called with propertyName: " + propertyName + ", returned: " + returnValue);  if (propertyName === "java.vm.vendor") {  return "";  }  return returnValue;  }; |

之后hook AesUtil.encrypt就不会退出了



GetTime返回的是当前时间戳 根据题目描述拿到正确时间戳



frida设置GetTime返回值

|  |
| --- |
| let Myjni = Java.use("com.example.ohhelp.MyJNI.Myjni");  Myjni["GetTime"].overload().implementation = function () {  console.log('GetTime is called');  let ret = this.GetTime();  console.log('GetTime ret value is ' + ret);  return "1055853128000";  }; |

之后hook AesUtil.encrypt拿到的返回值即为flag

|  |
| --- |
| function hook() {  Java.perform(function () {  let Myjni = Java.use("com.example.ohhelp.MyJNI.Myjni");  Myjni["GetTime"].overload().implementation = function () {  console.log('GetTime is called');  let ret = this.GetTime();  console.log('GetTime ret value is ' + ret);  return "1055853128000";  };  Myjni["GetKey"].implementation = function () {  console.log('GetKey is called');  let ret = this.GetKey();  console.log('GetKey ret value is ' + ret);  return "PUDzbflthjqxlJVW";  };  let AesUtil = Java.use("com.example.ohhelp.AesUtil");  AesUtil["encrypt"].overload('java.lang.String', 'java.lang.String').implementation = function (str, str2) {  console.log('encrypt is called' + ', ' + 'str: ' + str + ', ' + 'str2: ' + str2);  let ret = this.encrypt(str, str2);  console.log('encrypt ret value is ' + ret);  return ret;  };  let System = Java.use('java.lang.System');  System.getProperty.overload('java.lang.String').implementation = function (propertyName) {  var returnValue = this.getProperty(propertyName);  console.log("System.getProperty called with propertyName: " + propertyName + ", returned: " + returnValue);  if (propertyName === "java.vm.vendor") {  return "";  }  return returnValue;  };  })  }  hook() |

hook结果，此时flag即为ISCC{VJS6yUGcQNC3K3lZ5BeYng==}

|  |
| --- |
| GetTime is called  GetTime ret value is 1715746657421  GetKey is called  GetKey ret value is null  encrypt is called, str: 1055853128000, str2: PUDzbflthjqxlJVW  encrypt ret value is UPwDHuXQBoInrKpj0VcdGA==  System.getProperty called with propertyName: java.library.path, returned: /system/lib64:/system/system\_ext/lib64:/system/product/lib64:/vendor/lib64  System.getProperty called with propertyName: java.vm.vendor, returned: The Android Project  System.getProperty called with propertyName: java.library.path, returned: /system/lib64:/system/system\_ext/lib64:/system/product/lib64:/vendor/lib64  System.getProperty called with propertyName: java.vm.vendor, returned: The Android Project  encrypt is called, str: UPwDHuXQOQgM2Fxv, str2: IscC20244202CcsI  encrypt ret value is VJS6yUGcQNC3K3lZ5BeYng== |