



Non si lascia il PC sbloccato



DISCLAIMER

L'app che andremo ad analizzare in questo intervento è stata scritta da me
e la chiave che viene utilizzata è la mia

Questo talk è solo a scopo didattico



Di Cosa Parliamo Oggi?



Cos'è il Reverse engineering

Il **reverse engineering** è un processo atto ad analizzare un sistema, software o dispositivo, anche senza accesso al suo codice sorgente, per comprenderne il funzionamento, la logica interna e le strutture.

Si parte **dall'output**, o dal comportamento osservabile, e si lavora a ritroso per ricostruire come è stato realizzato.



Statico vs Dinamico

Statico

Analisi che viene condotta **senza eseguire il codice.**

Vengono utilizzati una **serie di tools e strumenti** per analizzare il programma al fine di **ricavarne lo scopo e le funzionalità.**

Dinamico

Analisi che viene **condotta eseguendo il programma e osservandone il comportamento** monitorando ad esempio il flusso di esecuzione, le interazioni con server e servizi o l'uso della memoria.

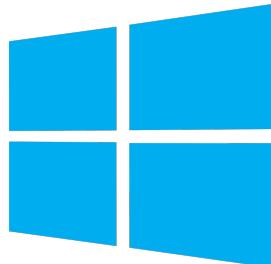


Reverse engineers Statico su un App Android

Abbiamo spiegato cosa vuol dire reversare staticamente un programma, ma su android come funziona?

Prima di tutto dobbiamo avere un [esegibile](#) da studiare.

Se ad esempio su windows abbiamo i .exe e su linux abbiamo .elf, **su android abbiamo gli apk**



Cos'è un APK?

Un APK (**Android Application Package**) è il formato con cui vengono distribuite e installate le applicazioni Android.

Si può pensare come un "pacchetto" che contiene tutto ciò di cui un'app ha bisogno per funzionare: codice compilato, risorse grafiche, file di configurazione e altro.



Quando scarichi un'app, il tuo dispositivo Android "scarta" l'APK e lo installa.





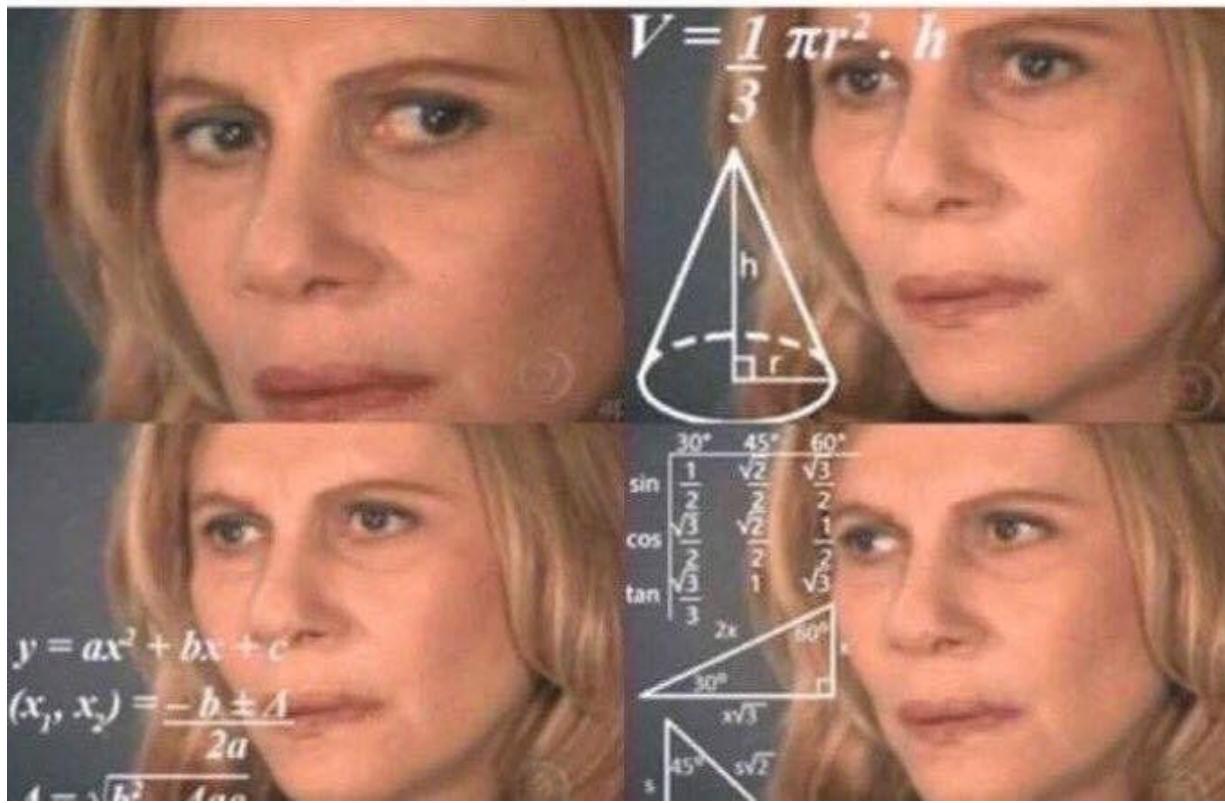
Strumenti



APKTOOL

The word 'APKTOOL' is displayed in large, bold, block letters. The letters are split into two colors: 'APK' is in light green and 'TOOL' is in teal.

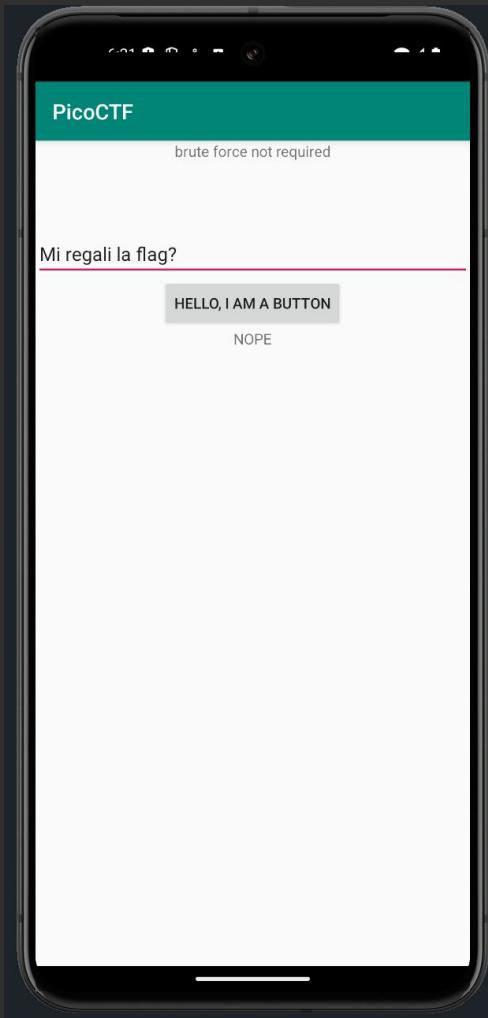
Tutto bellissimo, ma quindi?



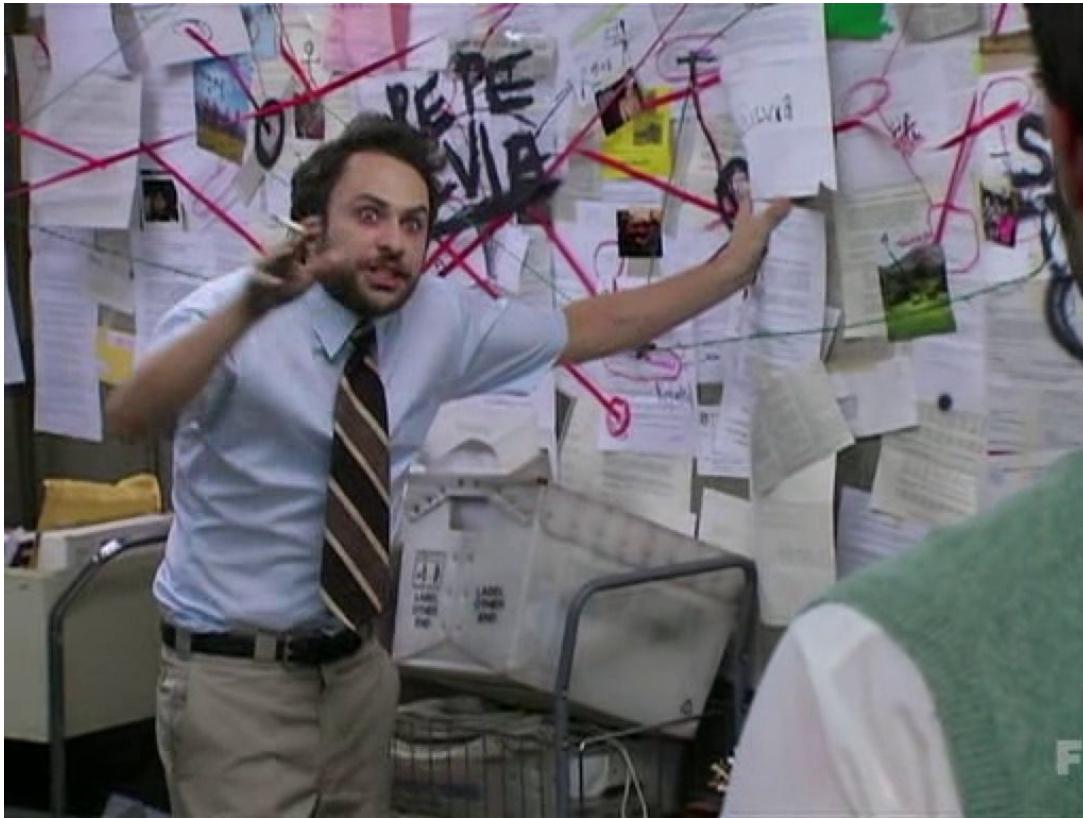
PicoCTF 2019



PicoCTF 2019

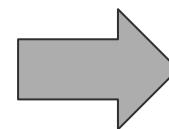
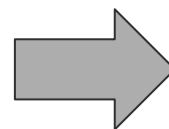


Okay qual è il piano?



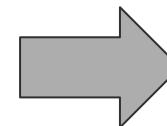
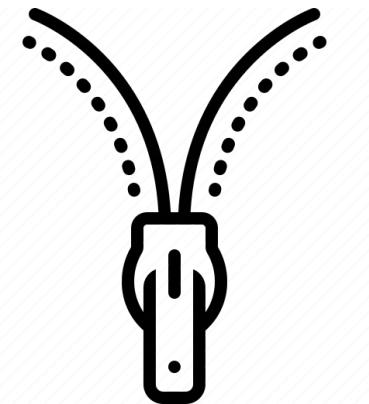
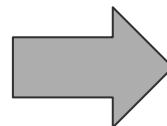


Partiamo dall'APK





Partiamo dall'APK





Estrai ▾ Aggiungi file Trova...

Anteprima

Apri in applicazione esterna

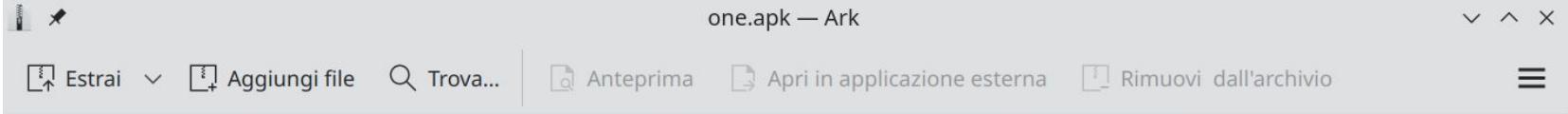
Rimuovi dall'archivio



Nome	Dimensione originale	Dimensione compressa	Codice di con
> META-INF	94,0 KiB		
> lib	59,2 KiB		
> res	322,9 KiB		
AndroidManifest.xml	2,2 KiB	801 B	6C07CEDD
classes.dex	2,1 MiB	995,5 KiB	033DB398
resources.arsc	267,9 KiB	267,9 KiB	952BC759



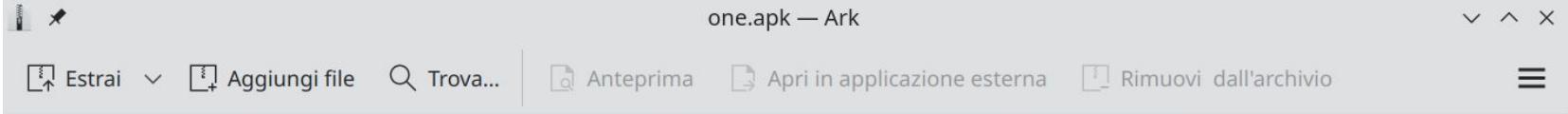
one.apk



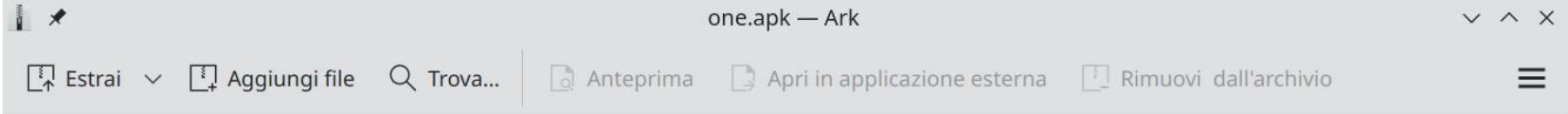
Nome	Dimensione originale	Dimensione compressa	Codice di controllo
➤ META-INF	94,0 KiB		
➤ lib	59,2 KiB		
➤ res	322,9 KiB		
➤ AndroidManifest.xml	2,2 KiB	801 B	6C07CEDD
➤ classes.dex	2,1 MiB	995,5 KiB	033DB398
➤ resources.arsc	267,9 KiB	267,9 KiB	952BC759



one.apk



Nome	Dimensione originale	Dimensione compressa	Codice di controllo
> META-INF	94,0 KiB		
> lib	59,2 KiB		
> res	322,9 KiB		
AndroidManifest.xml	2,2 KiB	801 B	6C07CEDD
classes.dex	2,1 MiB	995,5 KiB	033DB398
resources.arsc	267,9 KiB	267,9 KiB	952BC759



Nome	Dimensione originale	Dimensione compressa	Codice di con...
> META-INF	94,0 KiB		
> lib	59,2 KiB		
res	322,9 KiB		
AndroidManifest.xml	2,2 KiB	801 B	6C07CEDD
classes.dex	2,1 MiB	995,5 KiB	033DB398
resources.arsc	267,9 KiB	267,9 KiB	952BC759



one.apk

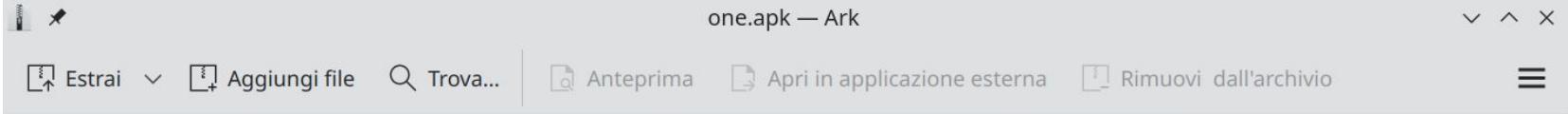
one.apk — Ark

Estrai ▾ Aggiungi file Trova... Anteprima Apri in applicazione esterna Rimuovi dall'archivio

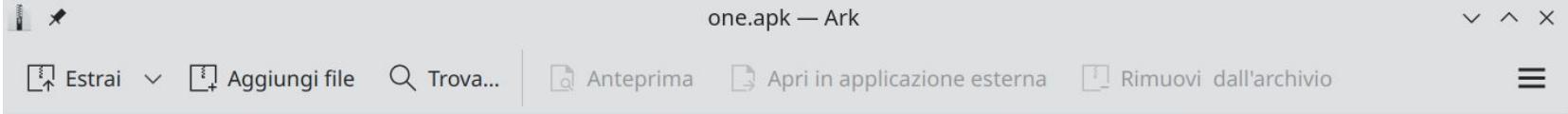
Nome Dimensione originale Dimensione compressa Codice di con

Nome	Dimensione originale	Dimensione compressa	Codice di con
META-INF	94,0 KiB		
lib	59,2 KiB		
res	322,9 KiB		
AndroidManifest.xml	2,2 KiB	801 B	6C07CEDD
classes.dex	2,1 MiB	995,5 KiB	033DB398
resources.arsc	267,9 KiB	267,9 KiB	952BC759

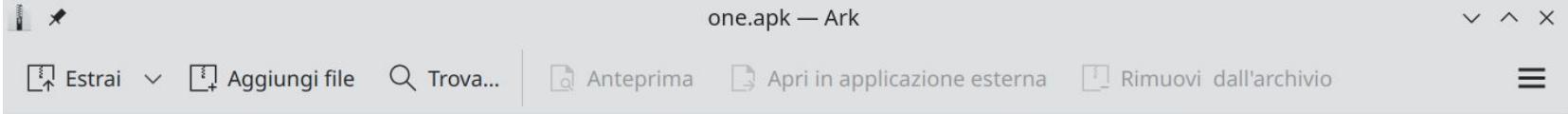
one.apk



one.apk



one.apk

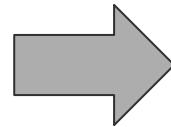


Nome	Dimensione originale	Dimensione compressa	Codice di con...
> META-INF	94,0 KiB		
> lib	59,2 KiB		
> res	322,9 KiB		
-> AndroidManifest.xml	2,2 KiB	801 B	6C07CEDD
-> classes.dex	2,1 MiB	995,5 KiB	033DB398
└ resources.arsc	267,9 KiB	267,9 KiB	952BC759



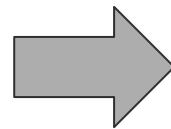
one.apk

Convertire un Dex?



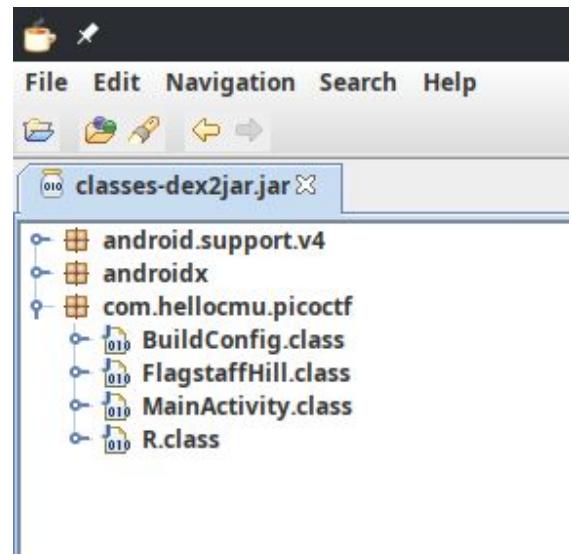
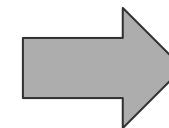
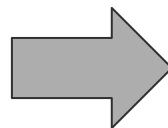


Convertire un Dex?

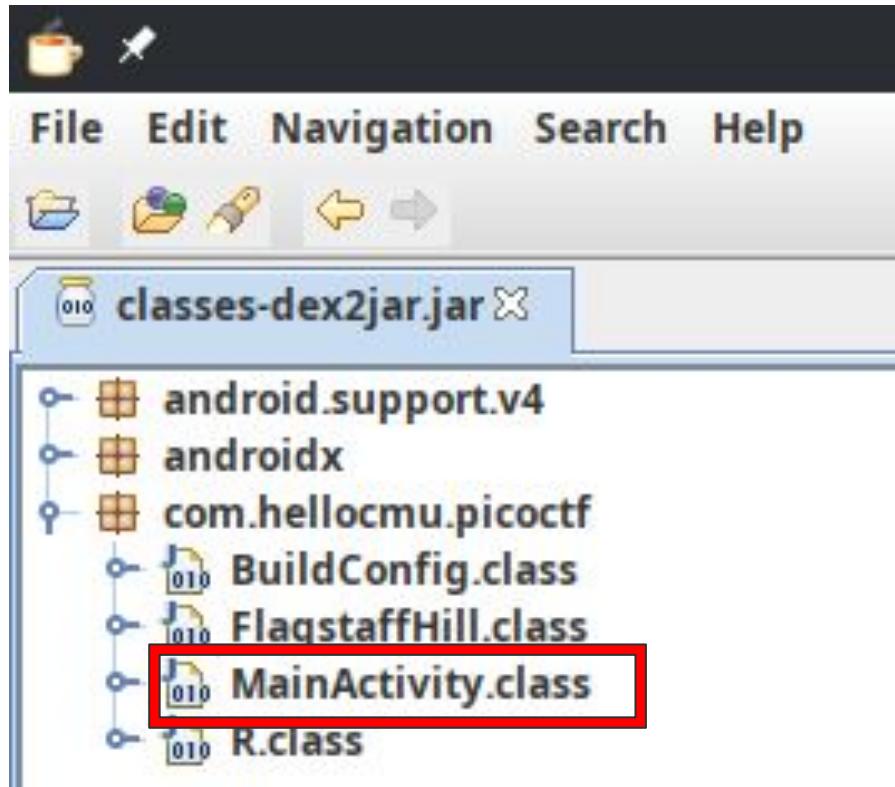




Come apriamo un jar?



JD-GUI



```
>MainActivity.class
```

```
package com.hellocmu.picoctf;

import android.content.Context;
import android.os.Bundle;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.TextView;
import androidx.appcompat.app.AppCompatActivity;

public class MainActivity extends AppCompatActivity {
    Button button;

    Context ctx;

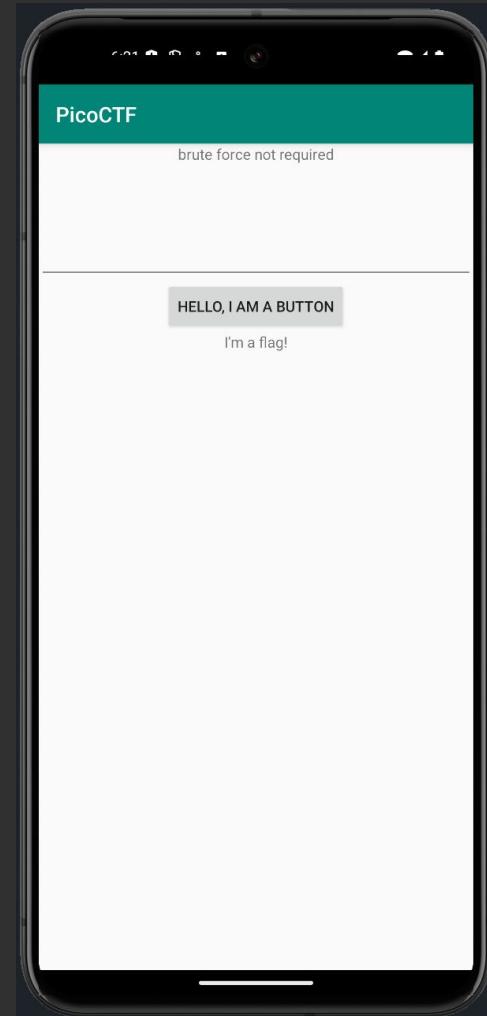
    TextView text_bottom;

    EditText text_input;

    TextView text_top;

    public void buttonClick(View paramView) {
        String str = this.text_input.getText().toString();
        this.text_bottom.setText(FlagstaffHill.getFlag(str, this.ctx));
    }

    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2131296284);
        this.text_top = (TextView)findViewById(2131165322);
        this.text_bottom = (TextView)findViewById(2131165320);
        this.text_input = (EditText)findViewById(2131165321);
        this.ctx = getApplicationContext();
        System.loadLibrary("hellojni");
        this.text_top.setText(2131427372);
    }
}
```



```
MainActivity.class FlagstaffHill.class  
package com.hellocmu.picoctf;  
  
import android.content.Context;  
  
public class FlagstaffHill {  
    public static native String fenugreek(String paramString);  
  
    public static String getFlag(String paramString, Context paramContext) {  
        return paramString.equals(paramContext.getString(2131427375)) ? fenugreek(paramString) : "NOPE";  
    }  
}
```



(paramContext.getString(2131427375))

MainActivity.class FlagstaffHill.class BuildConfig.class R.class ResultReceiver.class AccessibilityNodeInfoCompat.class

```
public static final int abc_toolbar_collapse_description = 2131427366;

public static final int app_name = 2131427367;

public static final int bat = 2131427368;

public static final int bear = 2131427369;

public static final int cottentail = 2131427370;

public static final int gopher = 2131427371;

public static final int hint = 2131427372;

public static final int manatee = 2131427373;

public static final int myotis = 2131427374;

public static final int password = 2131427375; 2131427375;

public static final int porcupine = 2131427376;

public static final int porpoise = 2131427377;

public static final int search_menu_title = 2131427378;

public static final int skunk = 2131427379;

public static final int status_bar_notification_info_overflow = 2131427380;

public static final int vole = 2131427381;

}

public static final class style {
    public static final int AlertDialog_AppCompat = 2131492864;

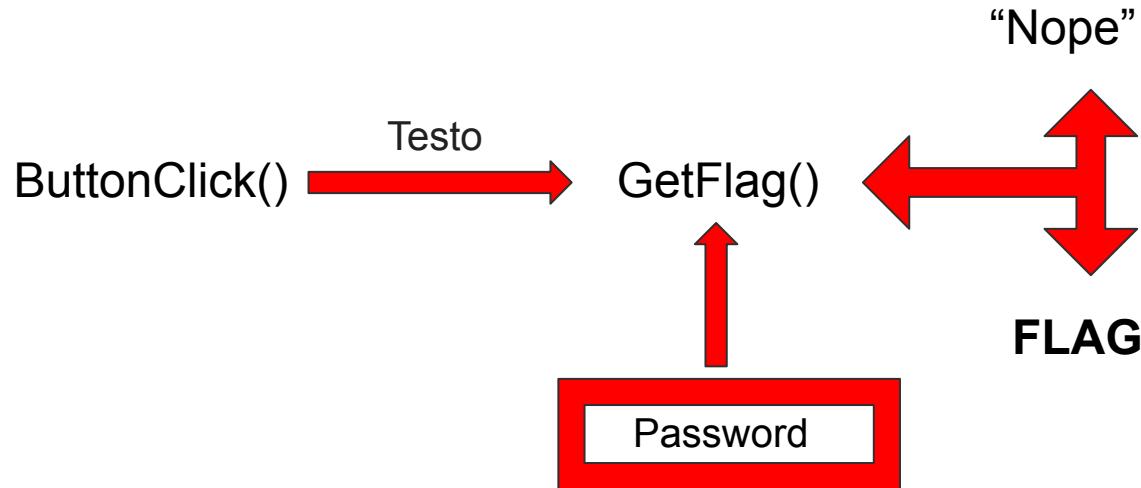
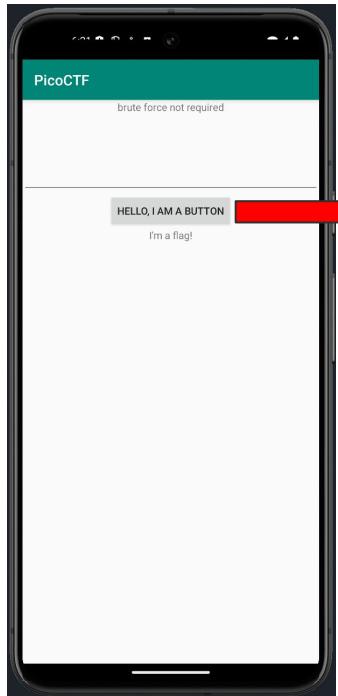
    public static final int AlertDialog_AppCompat_Light = 2131492865;
}
```

Next Previous Case sensitive

Ci siamo quasi...

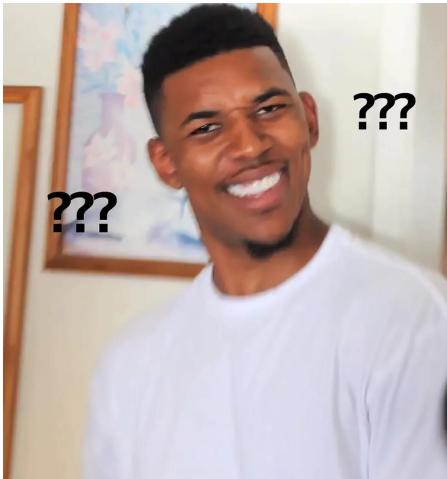


Riassumendo in breve:



Estrai ▾ Aggiungi file Trova...

Nome	Dimensione or
META-INF	94,0 KiB
lib	59,2 KiB
res	322,9 KiB
AndroidManifest.xml	2,2 KiB
classes.dex	2,1 MiB
resources.arsc	267,9 KiB

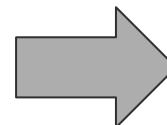
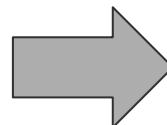


Nome	Modificato
mipmap-xxxhdpi-v4	13/12/01 alle 21:45
mipmap-xxhdpi-v4	13/12/01 alle 21:45
mipmap-xhdpi-v4	13/12/01 alle 21:45
mipmap-mdpi-v4	13/12/01 alle 21:45
mipmap-hdpi-v4	13/12/01 alle 21:45
mipmap-anydpi-v26	13/12/01 alle 21:45
layout-watch-v20	13/12/01 alle 21:45
layout-v26	13/12/01 alle 21:45
layout-v22	13/12/01 alle 21:45
layout-v21	13/12/01 alle 21:45
layout-v17	13/12/01 alle 21:45
layout-v16	13/12/01 alle 21:45
layout	13/12/01 alle 21:45
drawable-xxxhdpi-v4	13/12/01 alle 21:45
drawable-xxhdpi-v4	13/12/01 alle 21:45
drawable-xhdpi-v4	13/12/01 alle 21:45
drawable-watch-v20	13/12/01 alle 21:45
drawable-v24	13/12/01 alle 21:45
drawable-v23	13/12/01 alle 21:45
drawable-v21	13/12/01 alle 21:45
drawable-mdpi-v4	13/12/01 alle 21:45
drawable-lldrtl-xxxhdpi-v17	13/12/01 alle 21:45
drawable-lldrtl-xxhdpi-v17	13/12/01 alle 21:45
drawable-lldrtl-xhdpi-v17	13/12/01 alle 21:45
drawable-lldrtl-mdpi-v17	13/12/01 alle 21:45
drawable-lldrtl-hdpi-v17	13/12/01 alle 21:45
drawable-lldrtl-v4	13/12/01 alle 21:45
drawable-hdpi-v4	13/12/01 alle 21:45
drawable-anydpi-v21	13/12/01 alle 21:45
drawable	13/12/01 alle 21:45
color-v23	13/12/01 alle 21:45
color-v21	13/12/01 alle 21:45
color	13/12/01 alle 21:45
anim	13/12/01 alle 21:45



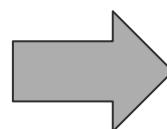


Torniamo all'APK

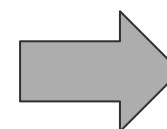




Torniamo all'APK



 **APKTOOL**

The word 'APKTOOL' is written in a bold, sans-serif font. The 'A' and 'P' are in green, while 'KTOOL' is in teal. An Android smartphone icon is integrated into the letter 'A'.

Qualcosa di nuovo?

 res	15 minuti fa
 original	15 minuti fa
 lib	15 minuti fa
 smali	15 minuti fa
 apktool.yml	15 minuti fa
 AndroidManifest.xml	15 minuti fa



File Modifica Selezione Visualizza Vai Esegui Terminale Guida

CERCA

password

Sostituisci AB ...

20 risultati in 9 file - Apri nell'editor

- ✓ public.xml res/values ...public type="string" name="password" id="0x7f0b002f" /...
- ✓ strings.xml res/values <string name="password">opossum</string>
- ✗ AppCompatTextHelper.smali smali/androidx/appcompat/widget ...v9, Landroid/text/method/PasswordTransformationMethod; ...AccessibilityNodeInfoCompat.smali smali/androidx/core/view/accessibility .method public isPassword()Z ...AccessibilityNodeInfo; ->isPassword()Z .method public setPassword(Z)V .param p1, "password" # Z ...AccessibilityNodeInfo; ->setPassword(Z)V const-string v2, ":" password: ...AccessibilityNodeInfoCompat; ->isPassword()Z
- ✗ AccessibilityRecordCompat.smali smali/androidx/core/view/accessibility .method public isPassword()Z ...accessibility/AccessibilityRecord; ->isPassword()Z .method public setPassword(Z)V .param p1, "isPassword" # Z .../AccessibilityRecord; ->setPassword(Z)V
- ✗ TextViewCompat.smali smali/androidx/core/widget ...v0, Landroid/text/method/PasswordTransformationMethod; ...AccessibilityNodeInfoCompat; ->isPassword()Z ...accessibility/AccessibilityEvent; ->setPassword(Z)V
- ✗ FlagstaffHill.smali smali/com/hellocmu/picoctf .local v0, "password":Ljava/lang/String; ...field public static final password:I = 0x7f0b002f

strings.xml x

res > values > strings.xml > resources > string

```
<resources>
    <string name="abc_menu_snift_shortcut_label">Snift+</string>
    <string name="abc_menu_space_shortcut_label">space</string>
    <string name="abc_menu_sym_shortcut_label">Sym+</string>
    <string name="abc_prepend_shortcut_label">Menu+</string>
    <string name="abc_search_hint">Search...</string>
    <string name="abc_searchview_description_clear">Clear query</string>
    <string name="abc_searchview_description_query">Search query</string>
    <string name="abc_searchview_description_search">Search</string>
    <string name="abc_searchview_description_submit">Submit query</string>
    <string name="abc_searchview_description_voice">Voice search</string>
    <string name="abc_shareactionprovider_share_with">Share with</string>
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
    <string name="abc_toolbarCollapse_description">Collapse</string>
    <string name="app_name">PicoCTF</string>
    <string name="bat">mink</string>
    <string name="bear">margay</string>
    <string name="cottontail">shrew</string>
    <string name="gopher">armadillo</string>
    <string name="hint">brute force not required</string>
    <string name="manatee">caribou</string>
    <string name="password">opossum</string>
    <string name="porpoise">mouflon</string>
    <string name="search_menu_title">Search</string>
    <string name="skunk">elk</string>
    <string name="status_bar_notification_info_overflow">999+</string>
    <string name="vole">beaver</string>
</resources>
```



Duo 🔍 Ri 50, col 27 (8 selezionate) Spazi: 4 UTF-8 LF XML 🔍

PicoCTF

brute force not required

opossum

HELLO, I AM A BUTTON

picoCTF{pining.for.the.fjords}



strings.xml - one - Visual Studio Code

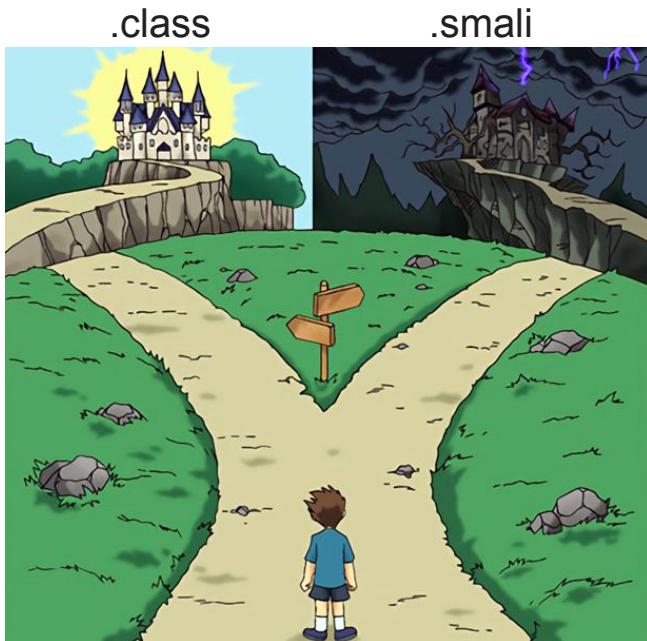
values > strings.xml > resources > string

```
<resources>
    <string name="abc_menu_shortcut_label">Shift+</string>
    <string name="abc_menu_space_shortcut_label">space</string>
    <string name="abc_menu_sym_shortcut_label">Sym+</string>
    <string name="abc_prepend_shortcut_label">Menu+</string>
    <string name="abc_search_hint">Search...</string>
    <string name="abc_searchview_description_clear">Clear query</string>
    <string name="abc_searchview_description_query">Search query</string>
    <string name="abc_searchview_description_search">Search</string>
    <string name="abc_searchview_description_submit">Submit query</string>
    <string name="abc_searchview_description_voice">Voice search</string>
    <string name="abc_shareactionprovider_share_with">Share with</string>
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
    <string name="abc_toolbarCollapse_description">Collapse</string>
    <string name="app_name">PicoCTF</string>
    <string name="bat">mink</string>
    <string name="bear">margay</string>
    <string name="cottontail">shrew</string>
    <string name="gopher">armadillo</string>
    <string name="hint">brute force not required</string>
    <string name="manatee">caribou</string>
    <string name="password">opossum</string>
    <string name="porpoise">mouflon</string>
    <string name="search_menu_title">Search</string>
    <string name="skunk">elk</string>
    <string name="status_bar_notification_info_overflow">999+</string>
    <string name="vole">beaver</string>
</resources>
```

Ri 50, col 27 (8 selezionate) Spazi: 4 UTF-8 LF XML G

A large circular logo for muhack.org. It features a stylized lowercase 'uh' in white on a black background, with the website address 'muhack.org' written in a smaller white sans-serif font below it.

Prima di andare oltre



ma3e.github.io/brains

Leggere i sorgenti



Leggere .class



Leggere .smali



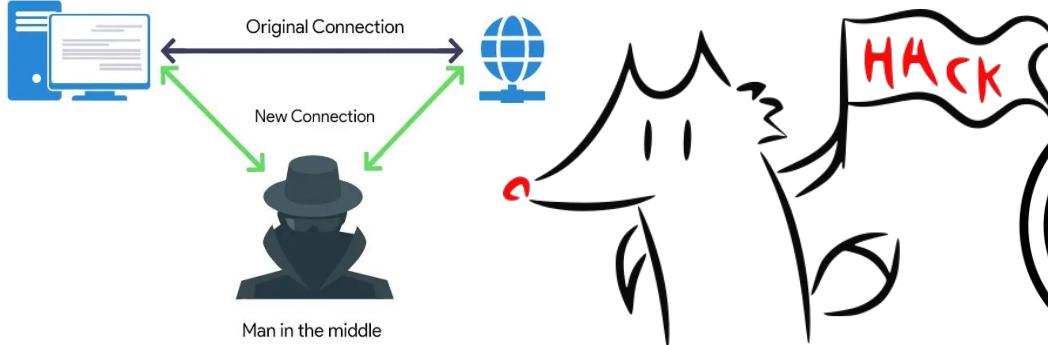
Spegnere il computer



Reverse Dinamico su Android

Il **reverse engineering dinamico** su Android consiste nell'**analisi di un'applicazione durante la sua esecuzione**.

Si utilizza per **monitorare** chiamate a metodi, **intercettare e modificare** il traffico di rete attraverso un **proxy** e **aggirare protezioni** come il pinning SSL.



Strumentopoli Pt.2



 Burp Suite

FRIDA

Il mio Setup

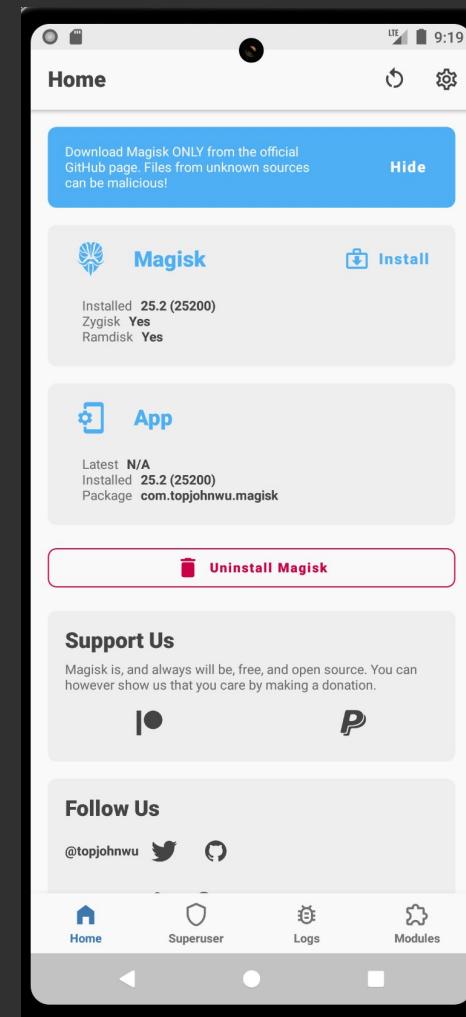
Emulatore Pixel 7a

-> API 26

-> Android 8 x86 Oreo

Per i permessi di root:

<https://github.com/newbit1/rootAVD>

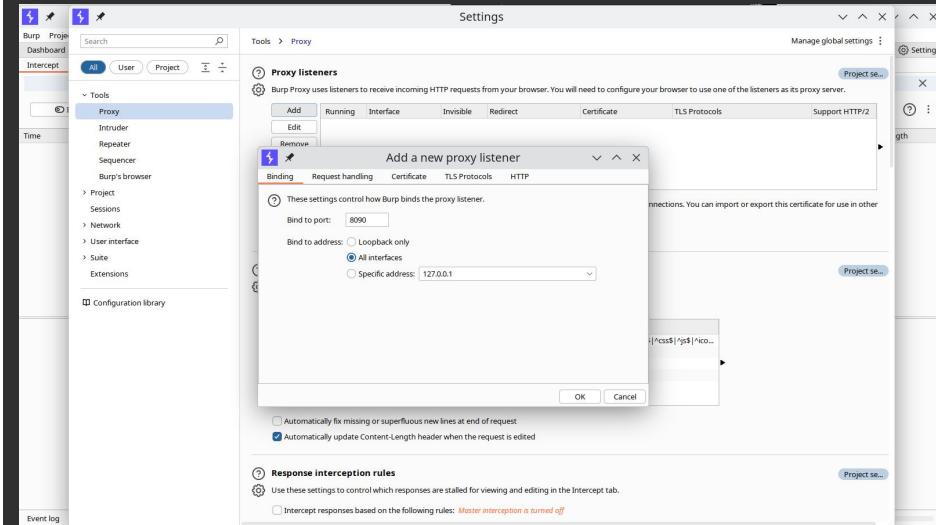


Proxy Setup

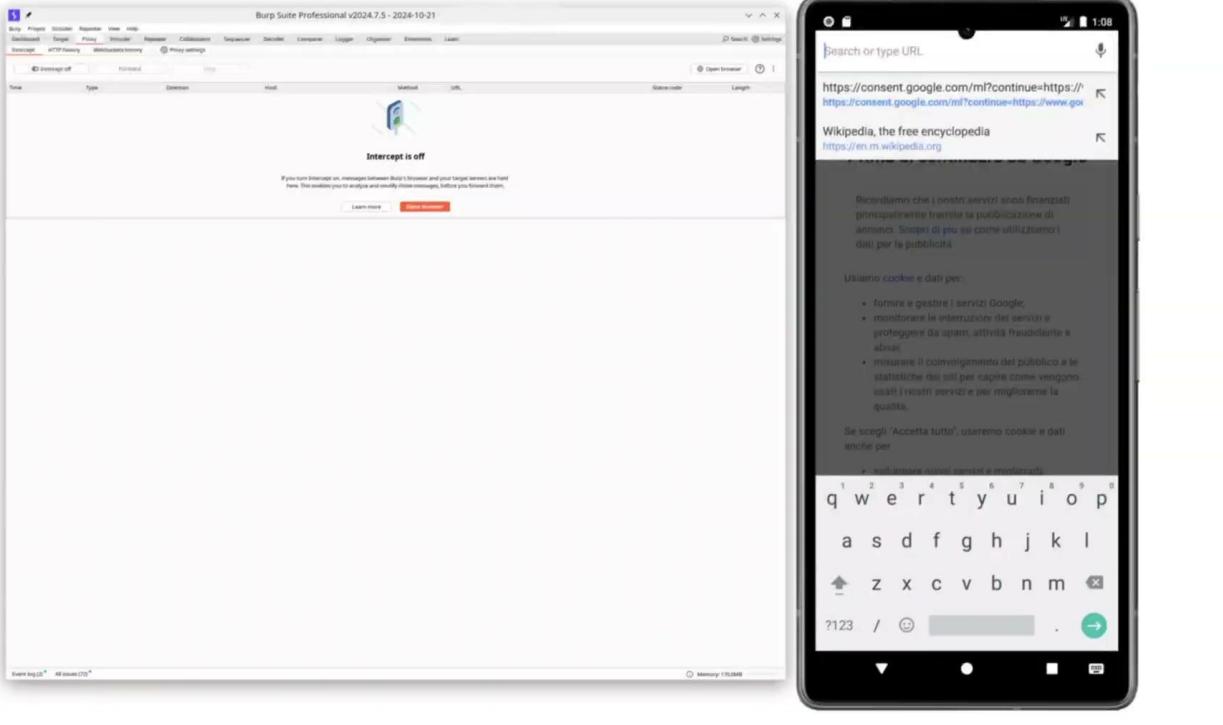
Configurare il proxy con Burp e installare i certificati sull'emulatore può essere abbastanza tedioso

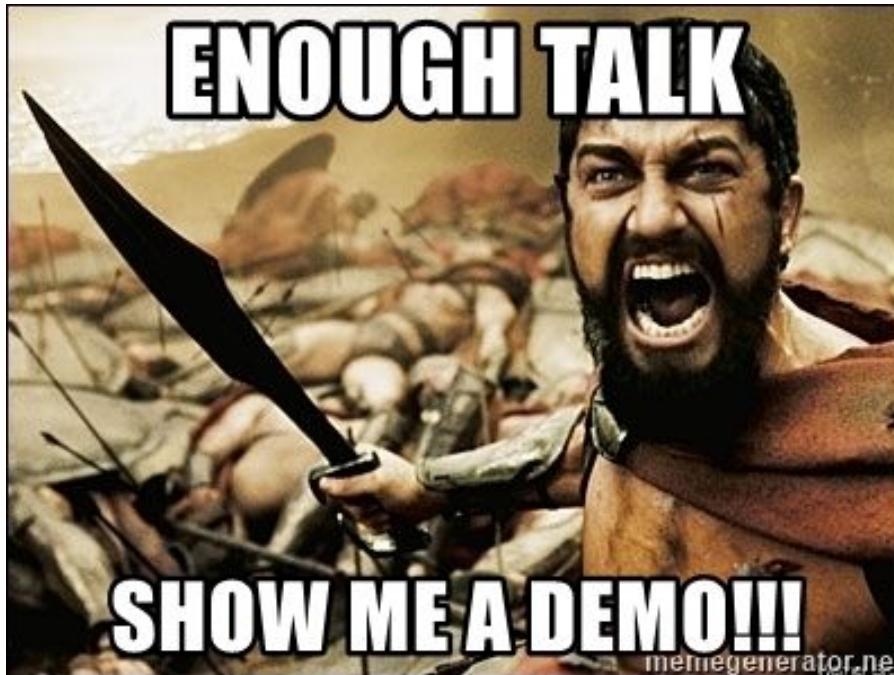
Quindi vi lascio un po' di doc che può aiutare se volete provare:

- > <https://portswigger.net/burp/documentation/desktop/mobile/config-android-device>
- > <https://www.youtube.com/watch?v=qQicUW0svB8>



Se siete stati bravi







Quindi?



Proxy per la
versione
Base



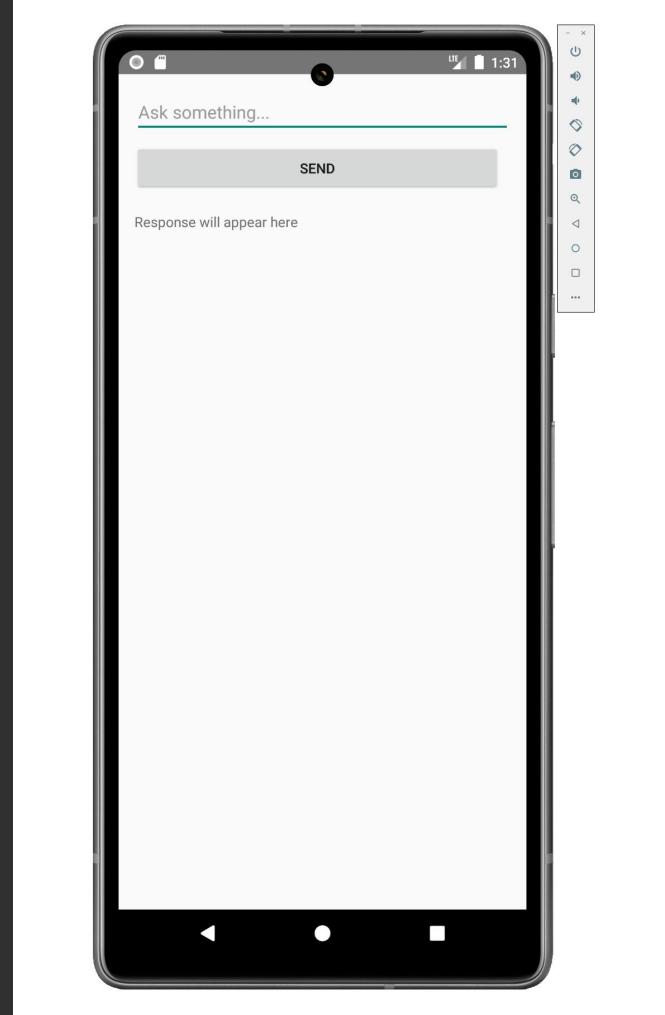
Proxy per la
versione pro,
Why doesn't
work?



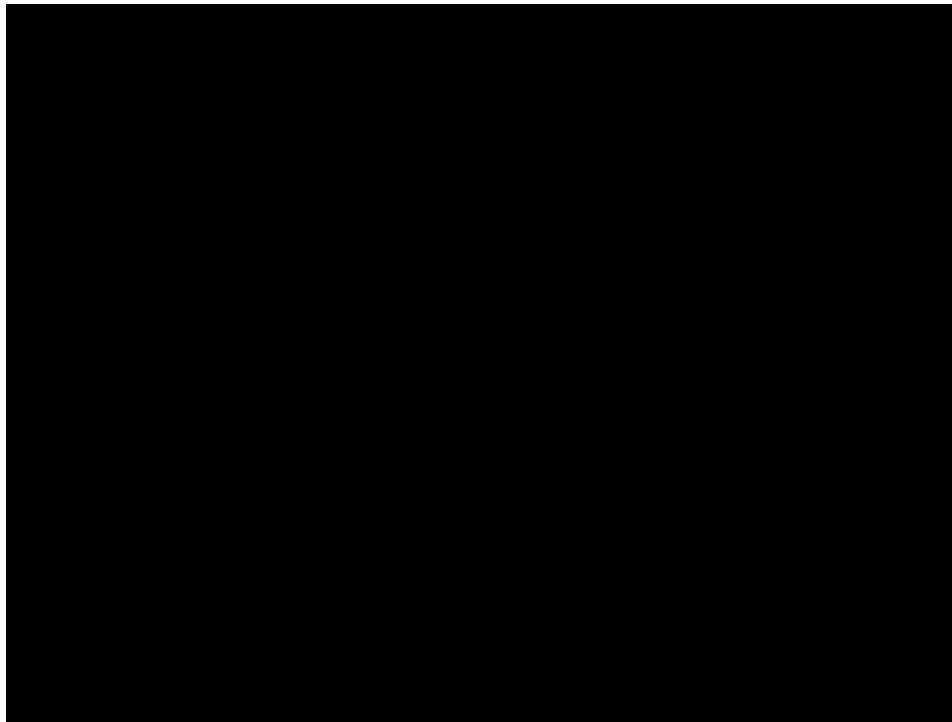
Bypass del
pinning SSL

La nostra app di test

Versione Base



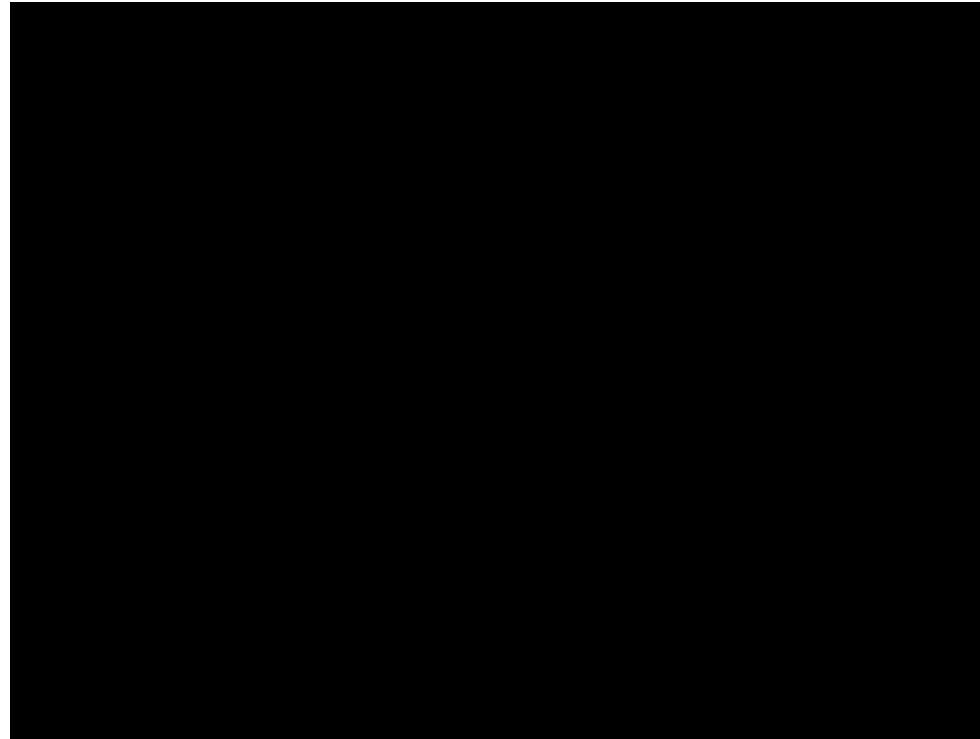
Come funziona



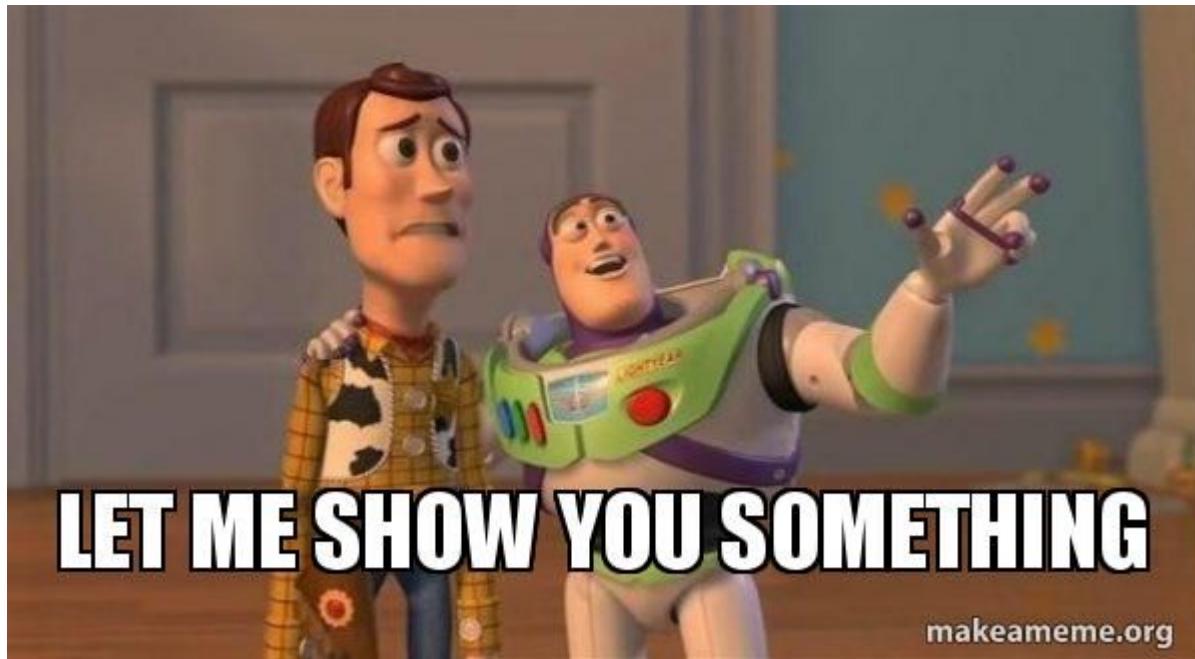
Proxy



Se tutto il setup iniziale con Burp è andato a buon fine il risultato finale è questo:



But First

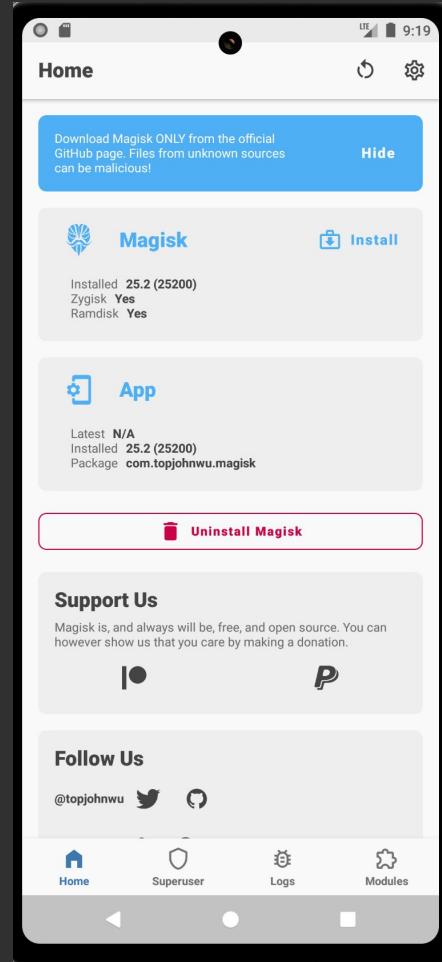
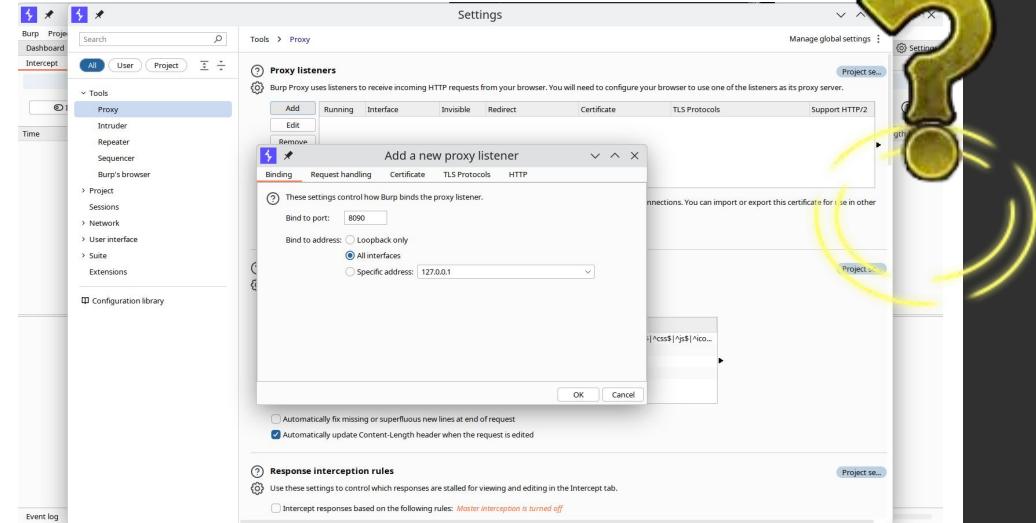


LET ME SHOW YOU SOMETHING

makeameme.org

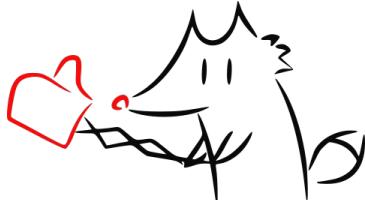
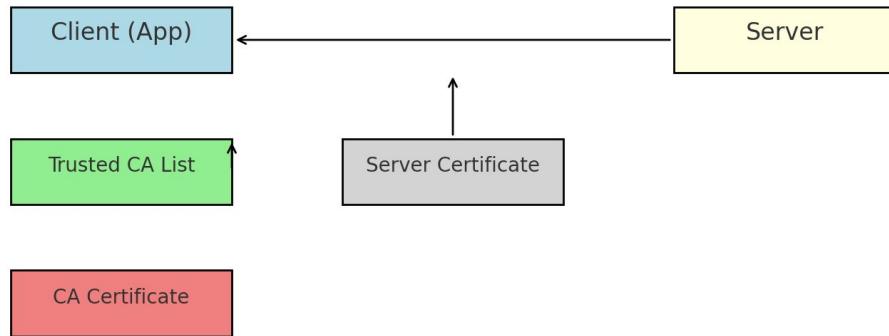


Torniamo indietro



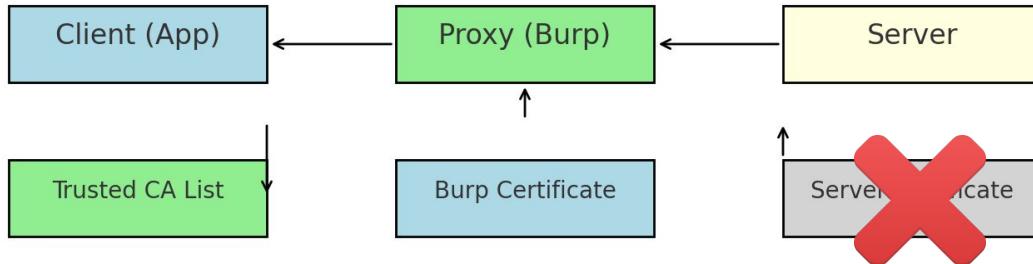
Https e Certificati

Connection Flow with Trusted CA List on Client



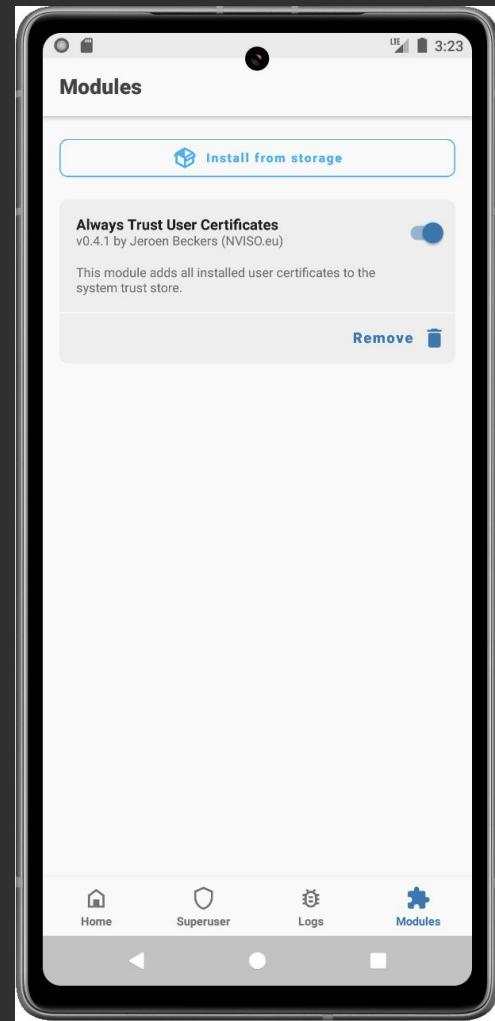
Proxy e Burp

Flow with Burp Intercepting and Presenting Its Own Certificate



Certificato e permessi di root

Android per motivi di sicurezza non ci permette di installare **certificati** che sono in una **partizione di sola lettura**, quindi se vogliamo installare il nostro certificato abbiamo bisogno dei **permessi di root**





Ma torniamo al nostro esempio



Proxy per la
versione
Base



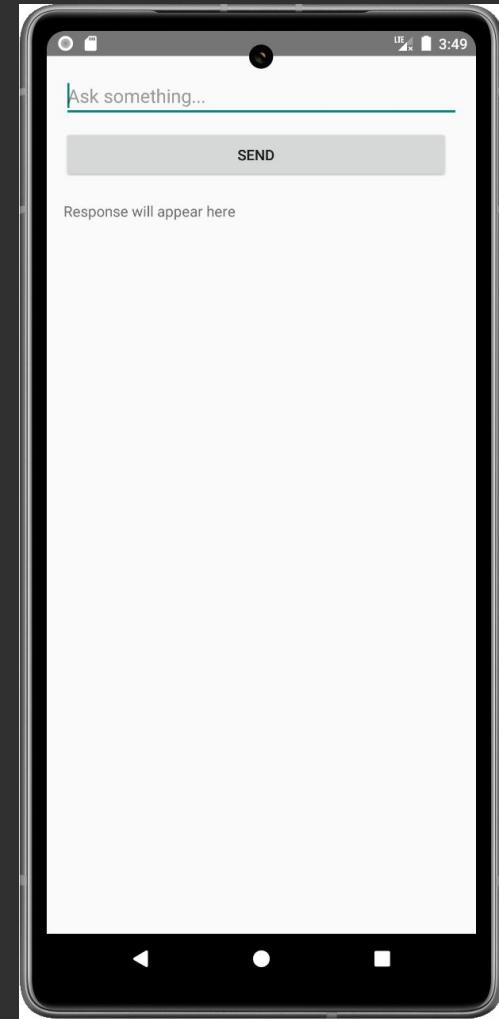
Proxy per la
versione pro,
Why doesn't
work?



Bypass del
pinning SSL

La nostra app di test

Versione PRO





O quasi...

Burp Suite Professional v2024.7.5 - 2024-10-21 - licensed to h3110w0r1d

File Project Import Reporter View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Computer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history ⚙️ Proxy settings

Intercept on: [Forward] [Drop]

Time	Type	Direction	Host	Method	URL	Status code	Length

Intercept is on

Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

[Learn more] [Open browser]

Event log (2) All issues (91)

Memory: 185.3MB

The screenshot shows the Burp Suite Professional interface. The 'Intercept' tab is selected, indicated by a blue bar above the tabs. A message at the top states 'Intercept is on'. Below this, there is a table with one row and several columns: Time, Type, Direction, Host, Method, URL, Status code, and Length. A small icon of a mobile phone with a signal is displayed above the table. At the bottom left, there are two buttons: 'Learn more' and 'Open browser'. At the bottom right, it says 'Memory: 185.3MB'.



Pinning SSL



Proxy per la
versione pro. Why
does it work?

Request fail:
Pin verification
failed

Il **pinning SSL** è una tecnica di sicurezza utilizzata per rafforzare la verifica dei certificati durante le connessioni HTTPS.

L'applicazione "pinna" uno specifico certificato o chiave pubblica, **limitando le connessioni solo ai server che presentano il certificato esatto o una chiave specifica.**



Quindi cosa facciamo?

Quindi usiamo uno strumentopolo!

Frida è uno degli strumenti più potenti per il reverse engineering dinamico.

Con Frida, si può **iniettare codice** nell'app in esecuzione e modificare il comportamento del pinning SSL in tempo reale.





How to use Frida?

1. Scarichiamo frida-server
2. Scarichiamo il codice da iniettare*
3. Installiamo frida-server sul telefono e lo avviamo con i giusti permessi

A screenshot of a terminal window titled "/ :adb — Konsole". The window shows a command-line session:

```
x lange@lange-inspiron16plus7620 ~ adb shell
generic_x86:/ $ su root
generic_x86:/ # cd /data/local/tmp
generic_x86:/data/local/tmp # chmod 777 frida-server
generic_x86:/data/local/tmp # ./frida-server &
[1] 8198
generic_x86:/data/local/tmp #
```

The terminal has tabs for "Nuova scheda", "Vista divisa", "frida_rev:zsh", and "7:adb". A blue arrow icon is visible in the top right corner of the terminal window.

* <https://codeshare.frida.re/@pcipolloni/universal-android-ssl-pinning-bypass-with-frida/>

Il piano



MitM Attack with Frida Bypassing SSL Pinning and Burp Intercepting



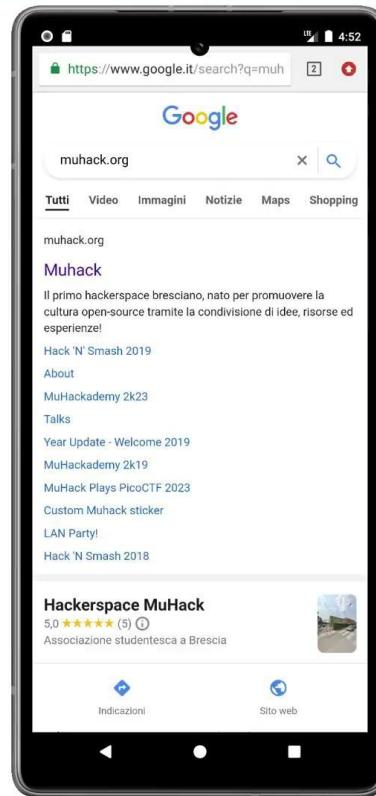
Bypass del
pinning SSL





The screenshot shows the Burp Suite interface. The top navigation bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'View', 'Help', 'Dashboard', 'Target', 'Proxy' (which is underlined), 'Intruder', 'Repeater', 'Collaborator', 'Sequencer', 'Decoder', 'Comparer', 'Logger', 'Organizer', 'Search', and 'Settings'. Below the navigation is a sub-menu with 'Intercept' (which is underlined), 'HTTP history', 'WebSockets history', and 'Proxy settings'. A toolbar below these buttons contains 'Intercept off' (disabled), 'Forward', 'Drop', 'Open browser', and a help icon. The main pane displays a table with columns: Time, Type, Direction, Host, Method, URL, Status code, and Length. A small icon of a shield with a keyhole is centered in the table area. Below the table, a message states 'Intercept is off' with a note: 'If you turn Intercept on, messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.' It includes 'Learn more' and 'Open browser' buttons. At the bottom of the interface is a terminal window titled 'frida_rev : zsh — Konsole' with the command 'lange@lange-inspiron16plus7620 ~/Scrivania/my_stuff/talk/frida_rev'.

Proviamo!





Domande?





Grazie per l'attenzione!

