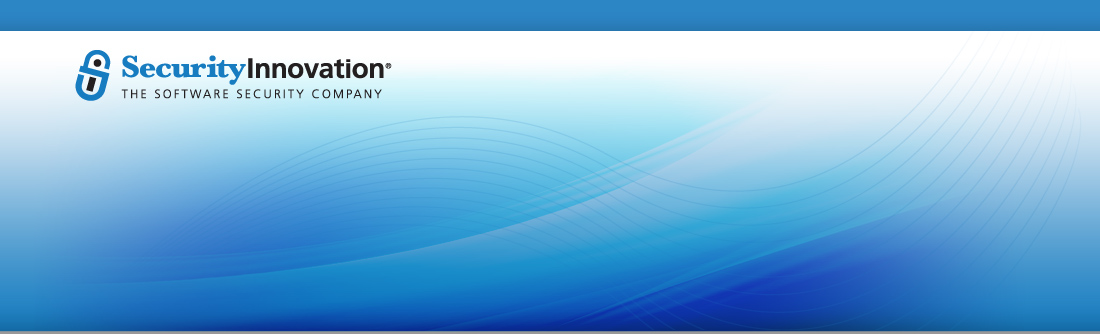


**BOSTON | SEATTLE**

**187 Ballardvale St. Suite A195 ●Wilmington, MA 01887● Ph: +1.978.694.1008**

[**getsecure@securityinnovation.com**](mailto:getsecure@securityinnovation.com)**●** [**www.securityinnovation.com**](http://www.securityinnovation.com)

|  |  |
| --- | --- |
| **Document name:** | Android Debugging using JDWP |
| **Author(s):** | Dinesh Shetty |



Android Debugging using JDWP

# Contact Information

### Technical Contact

Dinesh Shetty

Senior Security Engineer

Email: [dinezh.shetty@gmail.com](mailto:dinezh.shetty@gmail.com)

# Test Configuration

The following is required to verify this issue:

* Download the latest version of the Android-InsecureBankv2 apk from <https://github.com/dineshshetty/Android-InsecureBankv2>
* Download Android SDK from <http://developer.android.com/sdk/index.html>
* A rooted Android device

# Test Steps

1. Copy the InsecureBankv2.apk file to the “platform-tools” folder in the Android SDK and then use the below command to push the downloaded Android-InsecureBankv2 application to the rooted device.

./adb install InsecureBankv2.apk

1. Navigate back to the “platform-tools” folder and enter the below mentioned command:

./adb jdwp

Make a note of all the IDs’ displayed on the screen.

1. Launch the installed InsecureBankv2 application on the rooted device. Log in to the application and notice that the screen displays that the device is “rooted”.
2. Navigate back to the “platform-tools” folder and enter the below mentioned command:

./adb jdwp

Make a note of all the new ID that was not displayed on the screen previously. This is the id for the InsecureBankv2 application.

1. Enter the following command to create a new connection listening on 12345 to which we later connect using jdb.

./adb forward tcp:12345 jdwp:<above id from step 4>

1. Connect to 12345 using jdb.

jdb -attach localhost:12345

1. The list of all the available classes can be viewed using the command “classes”.
2. Methods for a specific class can be found using the below command:

methods com.android.insecurebankv2.PostLogin

1. Set up a breakpoint in the showRootStatus() function using the below command:

stop in com.android.insecurebankv2.PostLogin.showRootStatus()

1. The command “local” can be used to view the current local variables and the “step” command can be used to move to the next instruction.
2. On the device, log in to the application. Notice that the breakpoint it hit.
3. Keep entering “step” till the console shows ‘Step completed: "thread=main", com.android.insecurebankv2.PostLogin.showRootStatus(), line=88 bci=16’ and “local” shows ‘isrooted = false’.
4. Change value of local variable “isrooted” using “set isrooted = false ”.
5. Type “run” to continue the flow of execution.
6. Notice that the device no longer shows up as a rooted device and that the device is now patched.