Damn Vulnerable IOS Application Solutions

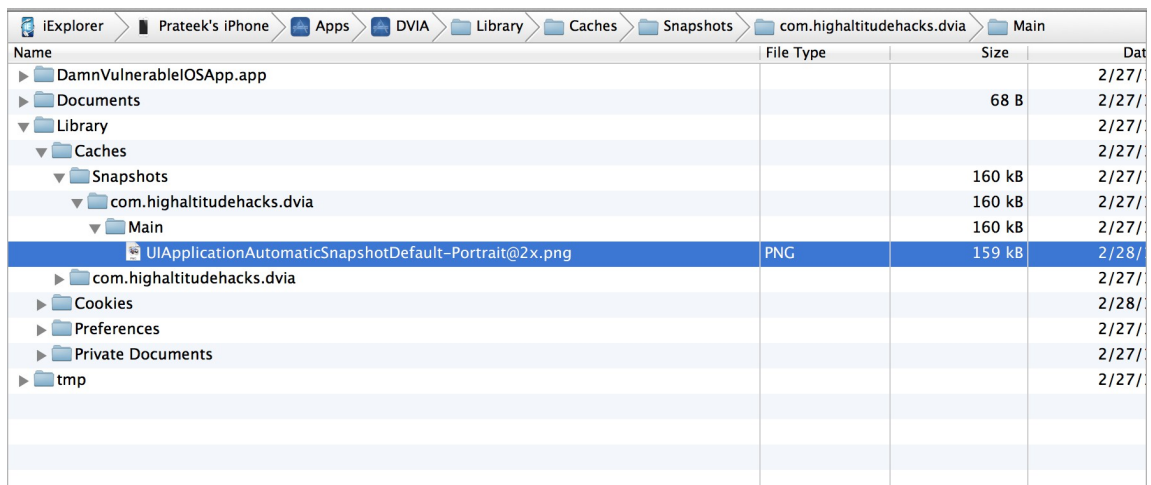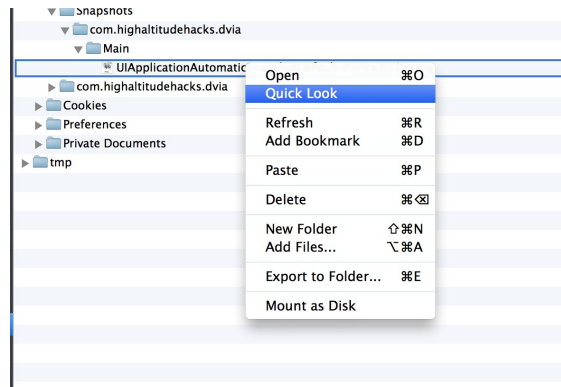## http://damnvulnerableiosapp.com/

Side channel data leakage – App Screenshot

Enter any dummy answer in the security question text field and tap on the home button on your device to take the application in the background. iOS will take a screenshot of the application before it goes in the background. You can find this screenshot in the location as shown below using iExplorer inside the application sandbox.

Right click on it and select the quick look option.

You will find that this screenshot contained the answer to the security question that was cached on the device. In order to prevent this kind of a vulnerability, this text field should have been set with the secure option.

Side Channel Data Leakage

app again to bring it to foreground while the app content is loaded in the background. This is done in order to provide a seamless experience. However, sometimes the screenshot may contain important information and since the screenshot is stored in the applicaton sandbox without proper protection, it can be obtained quite easily. Your task is to fill some data in the text field below, then take the app into the background and find the application screenshot showing the data entered in this text field.

Please answer this security question.

Johnny |

Submit