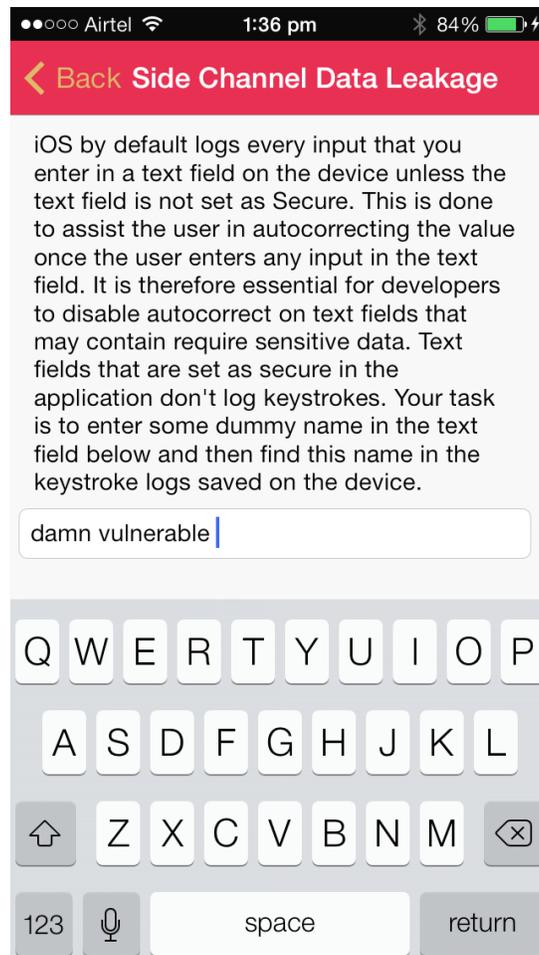


Damn Vulnerable IOS Application Solutions

<http://damnvulnerableiosapp.com/>

Side channel data leakage – Keyboard logs

Enter any dummy data in the text field.



Now ssh to your device and go to the location `/var/mobile/Library/Keyboard/`

```
Prateeks-iPhone:/ root# cd /var/mobile/Library/Keyboard/
Prateeks-iPhone:/var/mobile/Library/Keyboard root# ls
CameraTweak/ CloudUserDictionary.sqlite CoreDataUbiquitySupport/ en_GB-dynamic-text.dat hi-dynamic-text.dat
Prateeks-iPhone:/var/mobile/Library/Keyboard root#
```

Here we can see some files ending with the .dat extension. Choose the .dat file starting with en and try to look at its contents using vim.

```
Prateeks-iPhone:/var/mobile/Library/Keyboard root# vim en_GB-dynamic-text.dat
```

As you can see, this file contains all the keystroke logs that were cached on the device. The image below is just a part of this file, but if you look more into this file, you will notice that the logs are cached for a very long time.

```
^@have^@reached^@by^@now^@am^@cool^@plan^@Elbrus^@then^@might^@go^@for^@scuba^@course^@as^@well^@send^@u^@details^@on^@Fb^@gopro^@almost^@as^@rad^@man^@you^@did^@it^@it^@was |
```