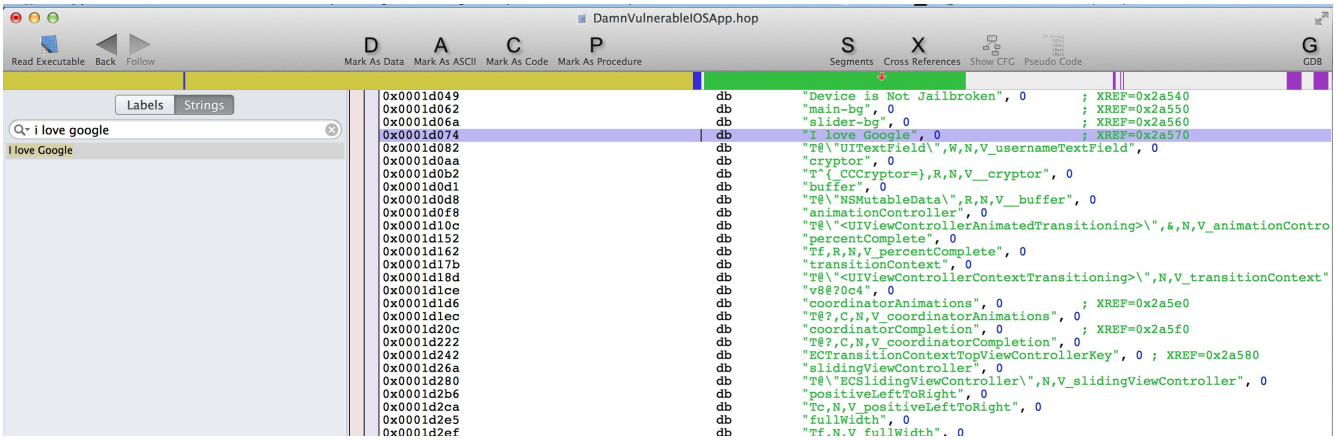
Damn Vulnerable IOS Application Solutions
http://damnvulnerableiosapp.com/

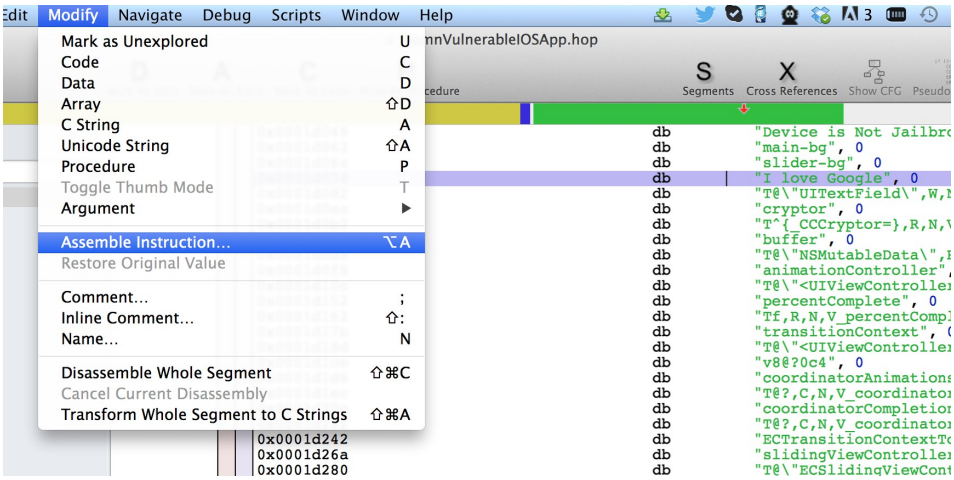
Application Patching – Modifying Alert Text

Open the application binary in Hopper. If you don't know where to find the application binary you can read the solution for the login challenge in this same section (Application Patching). Also make sure to build the application once using Xcode so that the DVIA application is installed in the simulator. Then quit Xcode but keep the simulator application open.

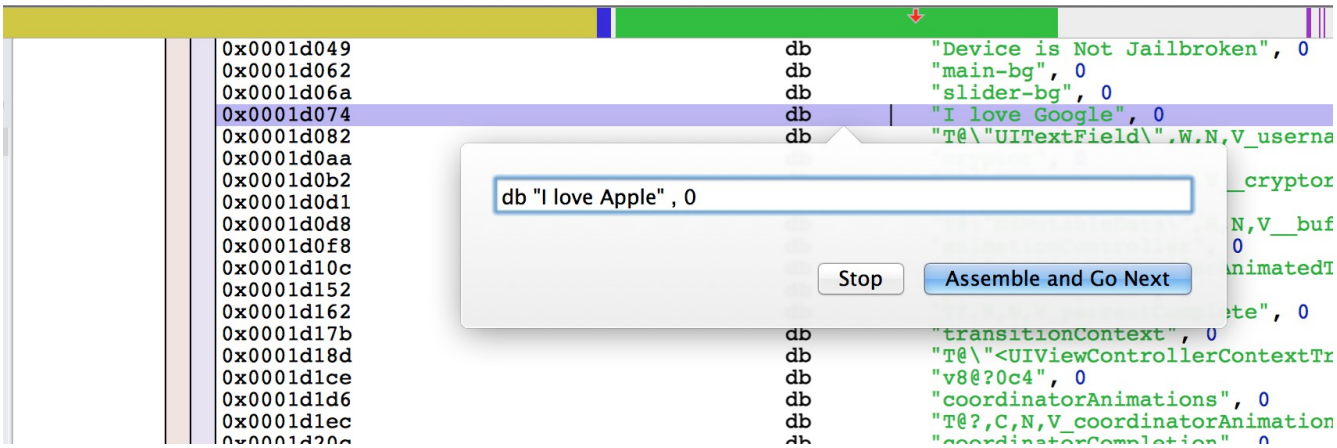
Once you open the application binary in Hopper, you can see the disassembly of the application. Head over to the *Strings* section on the left side and search for the string "I love Google"



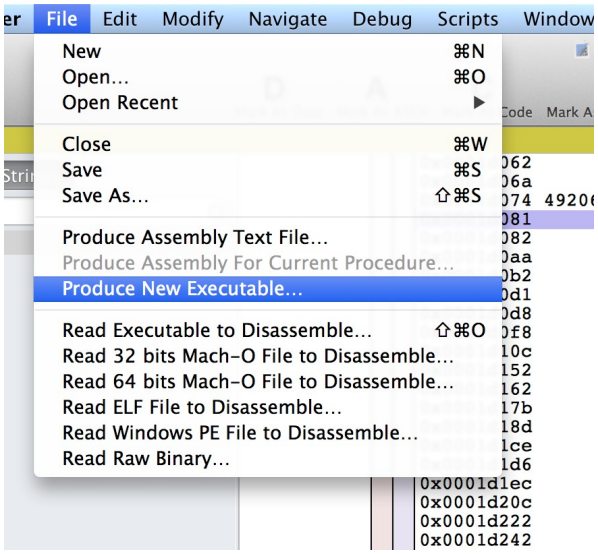
This will show you the location where this string is stored in the application binary. To modify this instruction, make sure this instruction is selected in the disassembly and select *Modify → Assemble Instruction*



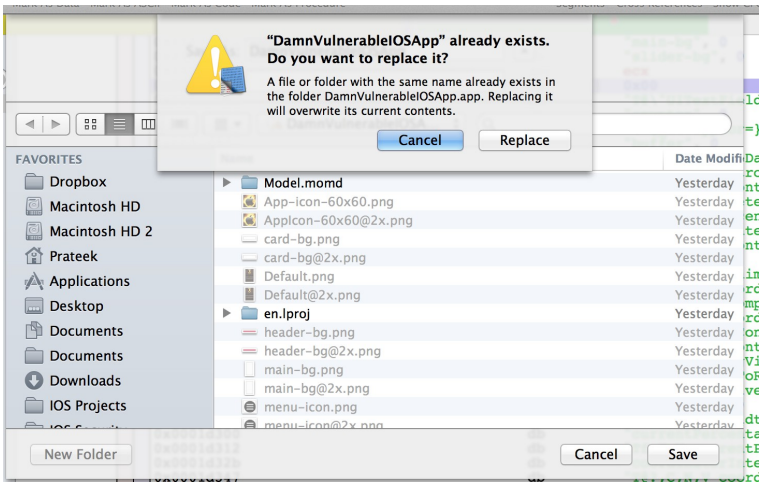
Copy the exact instruction but replace "I love Google" with "I love Apple"



Now save this modified binary by first using the command Cmd+S and then Going to File → Produce New Executable

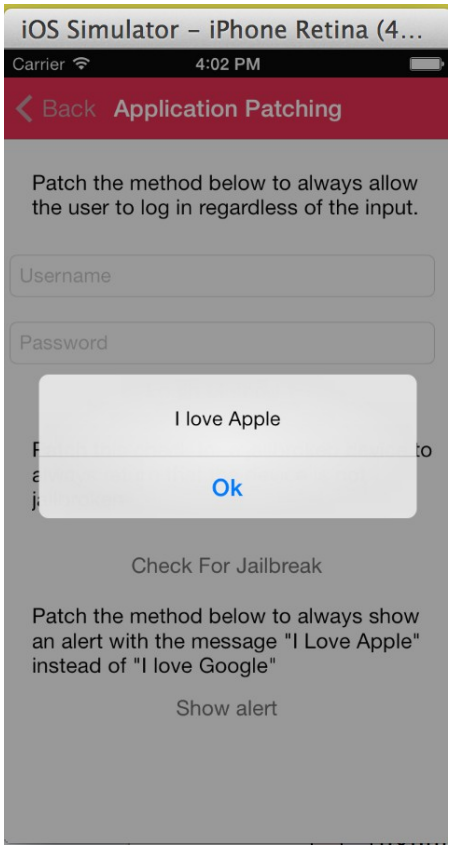


And overwrite the existing binary...



Please note that while modifying instructions, you might be overwriting some other instructions also so be careful when trying to make changes with Hopper.

In the IOS simulator, kill the current running instance of DVIA and restart it. Then head over to the Application patching challenges and tap on *Show Alert*.



As you can see, we have successfully modified the alert text with our own.