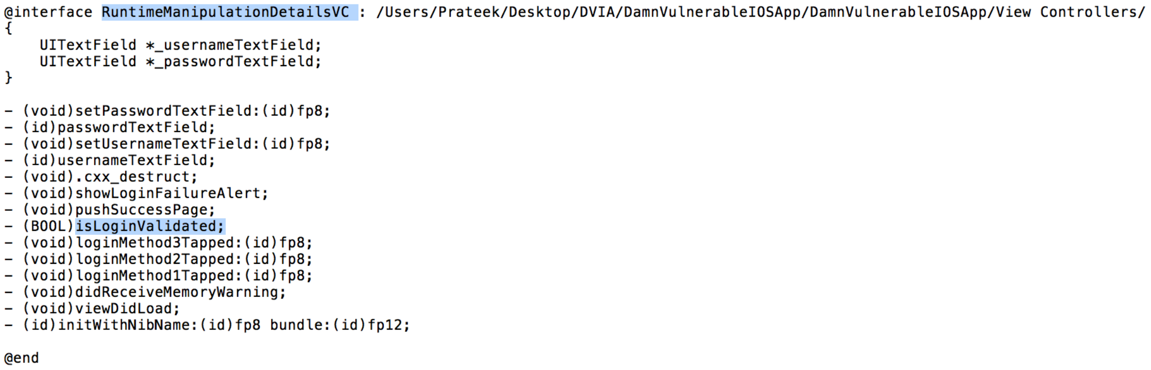
Damn Vulnerable IOS Application Solutions

http://damnvulnerableiosapp.com/

Runtime Manipulation – Login Method 1

This one is pretty straightforward. By looking at the class-dump info for this application, we can see these methods in the view controller *RuntimeManipulationDetailsVC.*



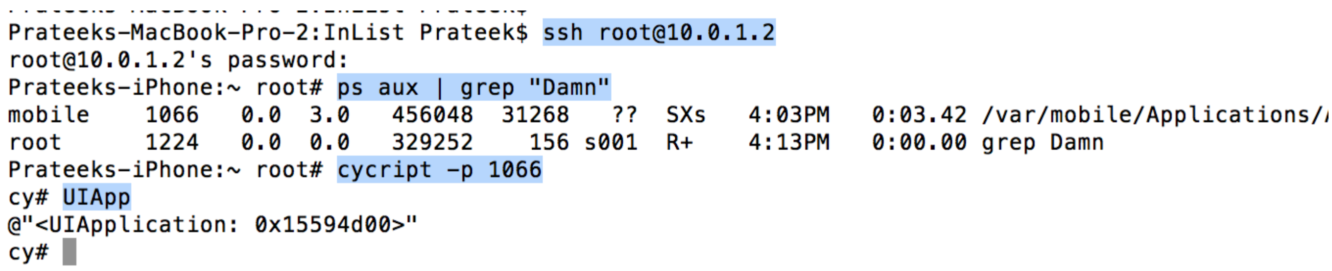
```
@interface RuntimeManipulationDetailsVC : /Users/Prateek/Desktop/DVIA/DamnVulnerableIOSApp/DamnVulnerableIOSApp/View Controllers/
{
    UITextField *_usernameTextField;
    UITextField *_passwordTextField;
}

- (void)setPasswordTextField:(id)fp8;
- (id)passwordTextField;
- (void)setUsernameTextField:(id)fp8;
- (id)usernameTextField;
- (void).cxx_destruct;
- (void)showLoginFailureAlert;
- (void)pushSuccessPage;
- (BOOL)isLoginValidated;
- (void)loginMethod3Tapped:(id)fp8;
- (void)loginMethod2Tapped:(id)fp8;
- (void)loginMethod1Tapped:(id)fp8;
- (void)didReceiveMemoryWarning;
- (void)viewDidLoad;
- (id)initWithNibName:(id)fp8 bundle:(id)fp12;

@end
```

The method of interest is – (BOOL)isLoginValidated . Looks like this method decides whether the user credentials are correct or not and return a YES or NO accordingly. If we can get this method to always return YES, then we may be able to bypass the login.

Let's ssh into our device and hook into our application using cycript.



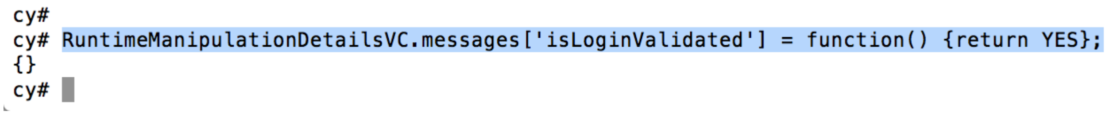
```
Prateeks-MacBook-Pro-2:InList Prateek$ ssh root@10.0.1.2
root@10.0.1.2's password:
Prateeks-iPhone:~ root# ps aux | grep "Damn"
mobile    1066   0.0  3.0   456048  31268   ??  SXs    4:03PM   0:03.42 /var/mobile/Applications/
root      1224   0.0  0.0   329252    156 s001  R+     4:13PM   0:00.00 grep Damn
Prateeks-iPhone:~ root# cycript -p 1066
cy# UIApp
@"<UIApplication: 0x15594d00>"
cy# 
```

Now let's modify the implementation for the method – (BOOL)isLoginValidated to always return YES. If you are not comfortable with cycript, I would recommend you read the following articles.

a) http://highaltitudehacks.com/2013/07/02/ios-aios-appllication-security-part-4-runtime-analysis-using-cycript-yahoo-weather-app
b) http://highaltitudehacks.com/2013/07/02/ios-application-security-part-5-advanced-runtime-analysis-and-manipulation-using-cycript-yahoo-weather-app
c) http://highaltitudehacks.com/2013/07/25/ios-application-security-part-8-method-swizzling-using-cycript

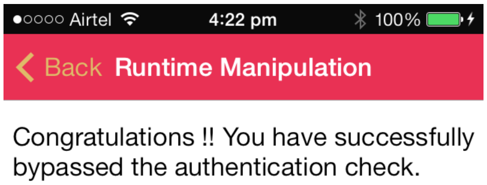
Use the following command in cycript to modify the implementation for this method

```
RuntimeManipulationDetailsVC.messages['isLoginValidated'] = function() {return
YES};
```



```
cy#
cy# RuntimeManipulationDetailsVC.messages['isLoginValidated'] = function() {return YES};
{}
cy#
```

Now tap on Login Method 1 without entering any input in the username and password text field and you will see that you will be taken to the success page. Congratulations, you just bypassed the authentication check for `Login Method 1` using Cycript.



Congratulations !! You have successfully bypassed the authentication check.