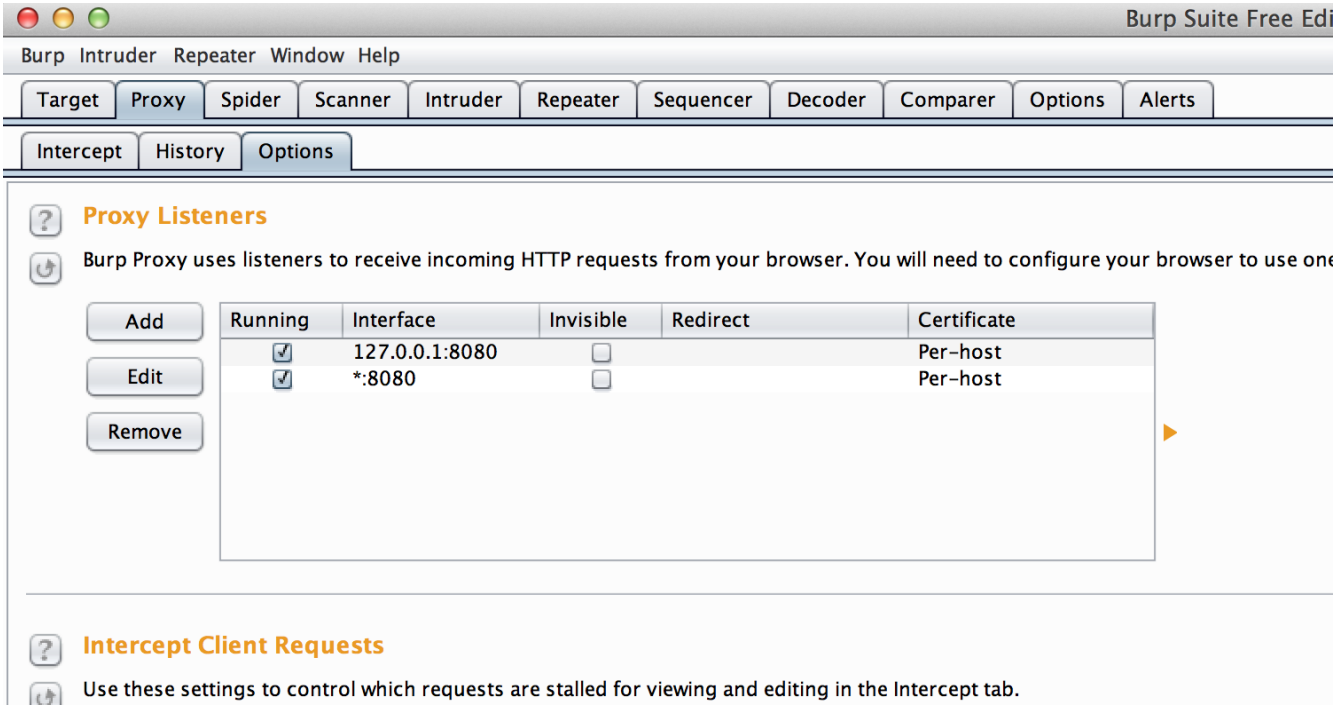
Damn Vulnerable IOS Application Solutions
http://damnvulnerableiosapp.com/

Transport Layer Security – HTTP

To capture the data going to and fro from the application over HTTP, you can use many free applications. Some of the good Ones are Burpsuite and Charles. In this case, we will be using Burpsuite.

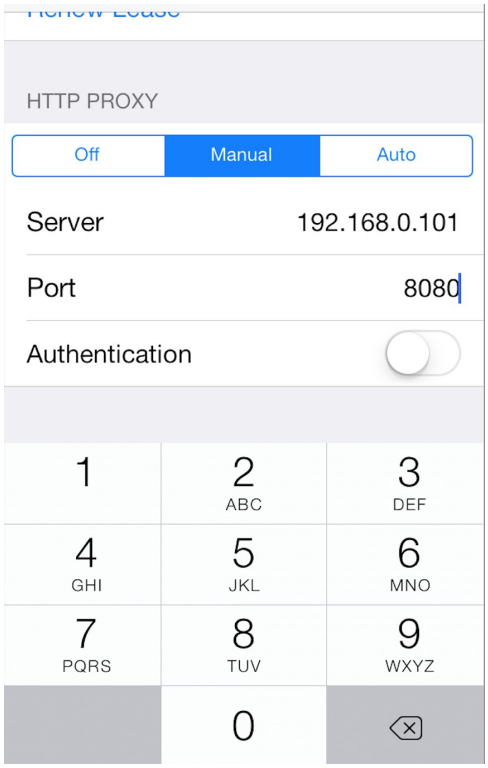
Let's launch Burpsuite and head over to *Proxy - > Options* and make sure the proxy is listening on every interface. To do that, check the option next to *.8080. This indicates that the proxy will listen to every interface on the port 8080.



Let's also find our system's IP address. In this case, it is 192.168.0.101

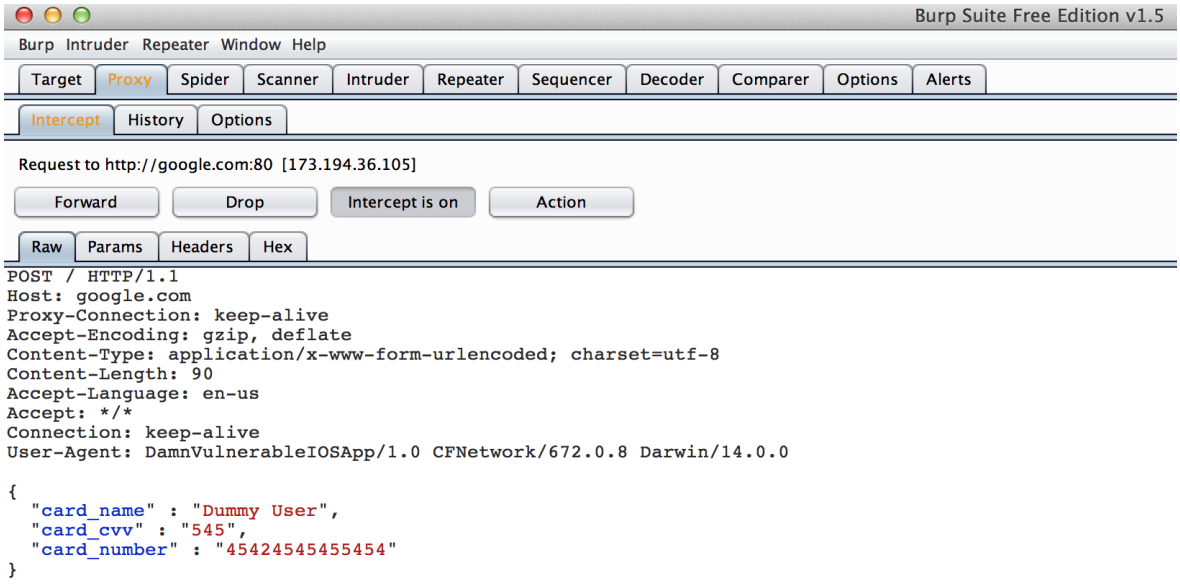
```
Prateeks-MacBook-Pro-2:DVIA Prateek$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet6 ::1 prefixlen 128
        inet 127.0.0.1 netmask 0xff000000
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=1<PERFORMNUD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether c8:e0:eb:15:81:f9
        inet6 fe80::cae0:ebff:fe15:81f9%en0 prefixlen 64 scopeid 0x4
        inet 192.168.0.101 netmask 0xffffff00 broadcast 192.168.0.255
        nd6 options=1<PERFORMNUD>
        media: autoselect
        status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
```

Now lets go to our IOS device, open the Settings applications, go to Wifi and then tap on the info button next to the wifi network we are connected to. If we scroll down, we will see an option to set an HTTP proxy. Let's enter the server address as the address of our computer and the port as 8080.



Now lets quit and restart our Application, go to the section *Transport Layer Security,* enter some dummy credit card information in the fields and tap on *Send Over HTTP.*

Now in Burpsuite go to Proxy->Intercept and you will notice that the data was intercepted.



You can also set Intercept to Off and notice all the traffic going through without actually intercepting the traffic.

Alternatively, you can also intercept the HTTP traffic using a simple sniffer tool like Wireshark.