Network Sniffing

Web pages maintain state using cookies and other session identifiers. Incorrect use of cookies and session identifiers can allow these identifiers to cross over from secure to non-secure networks or vice versa. These unprotected identifiers pose a threat to leave users of the website open to hijacking attacks. Such attacks are especially possible in network café's where all of the users in the café may have access to the wireless traffic of all of the other users.

iBeta uses network sniffing tools to verify that secure sessions aren't leaking their session identifiers to unsecure web sessions. The other tools in our arsenal will occasionally observe some of these vulnerabilities, but generally if they do not, we will examine the traffic to verify that traffic is encrypted and that session identifiers and cookies aren't leaking.