Android Intent Scheme URLs 攻击

Android 上的 Intent-based 攻击很普遍，这种攻击轻则导致应用程序崩溃，重则可能演变提权漏洞。基于 Android Browser 的攻击手段——Intent Scheme URLs 攻击。这种攻击方式利用了浏览器保护措施的不足，通过浏览器作为桥梁间接实现 Intend-Based 攻击。相比于普通 Intend-Based 攻击，这种方式极具隐蔽性，而且由于恶意代码隐藏 WebPage 中，传统的特征匹配完全不起作用。除此之外，这种攻击还能直接访问跟浏览器自身的组件（无论是公开还是私有）和私有文件，比如 cookie 文件，进而导致用户机密信息的泄露。

Intent scheme URL 的用法：

eg1:

<script>location.href=

“intent:mydata#Intent;action=myaction;type=text/plain;end”</script>

等效于

```
Intent intent = new Intent(“myaction”);
intent.setData(Uri.parse(“mydata”));
intent.setType(“text/plain”);
```

eg2:

intent://foobar/#Intent;action=myaction;type=text/plain;S.xyz=123;i.abc=678;end

等效于

```
Intent intent = new Intent(“myaction”);
intent.setData(Uri.pase(“//foobar/”));
intent.putExtra(“xyz”, “123”);
intent.putExtra(“abc”, 678);
```

其中 S 代表 String 类型的 key-value，i 代表 int 类型的 key-value。

安卓使用 urlschema 打开其他应用 activity

test.html:

```
<html>
<body>
<script >
location.href =
"intent:mydata#Intent;SEL;component=demo.addjavascriptpoc/.MainActivity;action
=android.intent.action.MAIN;end"
</script>
</body>
</html>
```

-参考
https://blog.csdn.net/l173864930/article/details/36951805?spm=a313e.7916648.0.0.11b0b6cXNqLdb