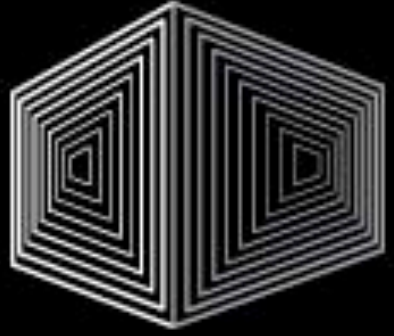


HITB SECCONF 2008
27th - 30th October 2008 MALAYSIA

# Clickjacking

Jeremiah Grossman
Founder & CTO

**Special Thanks:**
**Robert "RSnake" Hansen**
**SecTheory**

10.29.2008



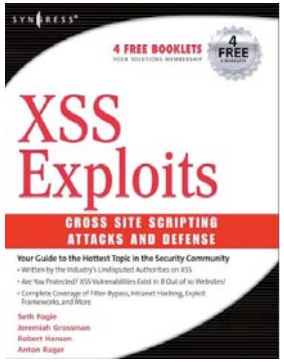
WhiteHat SECURITY

© 2008 WhiteHat, Inc.

# Jeremiah Grossman

- WhiteHat Security Founder & CTO
- Technology R&D and industry evangelist (InfoWorld's CTO Top 25 for 2007)
- Frequent international conference speaker
- Co-founder of the Web Application Security Consortium
- Co-author: Cross-Site Scripting Attacks
- Former Yahoo! information security officer






# Two Parts of Web Security

## Websites

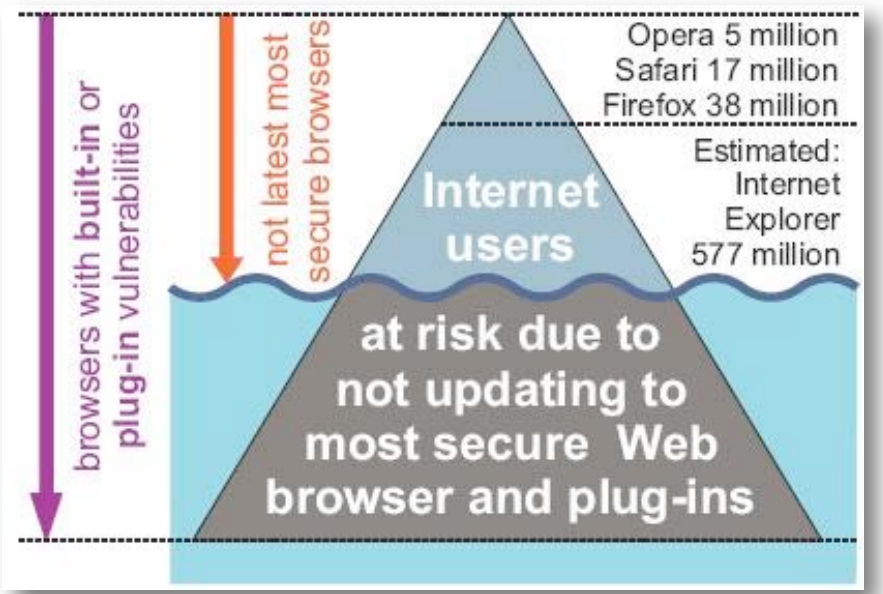

## Web Browsers

MUST be able to protect against HOSTILE WEB USER

MUST be able to protect against HOSTILE WEB PAGE

# The State of Web Browser Security



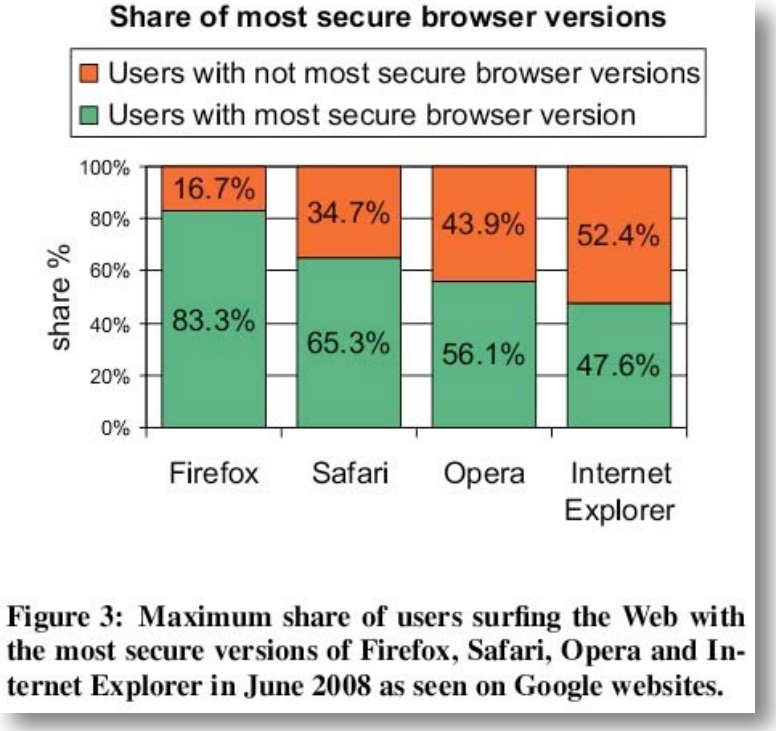




**Figure 3: Maximum share of users surfing the Web with the most secure versions of Firefox, Safari, Opera and Internet Explorer in June 2008 as seen on Google websites.**

The Web browser Insecurity Iceberg represents the number of Internet users at risk because they don't use the latest most secure Web browsers and plug-ins to surf the Web. This paper has quantified the visible portion of the Insecurity Iceberg (above the waterline) using passive evaluation techniques - which amounted to more than 600 million users at risk not running the latest most secure Web browser version in June 2008...

http://www.techzoom.net/publications/insecurity-iceberg/

# What Do the Experts Say/Do?

9. Is the average Web user capable of protecting themselves or their Web browser from being exploited? XSS, CSRF, JavaScript Malware, Browser Exploits, etc.

4. What is your personal approach to Web browser security?

| | Response Percent | Response Count |
|---|---|---|
| Virtualization | 25.2% | 79 |
| **Security add-ons** | **60.2%** | 189 |
| Use multiple-browsers | 51.3% | 161 |
| Disable JavaScript, Flash, JavaScript, etc. | 57.0% | 179 |
| Use Lynx | 9.6% | 30 |
| | comments | 52 |
| | ***answered question*** | **314** |
| | ***skipped question*** | **26** |

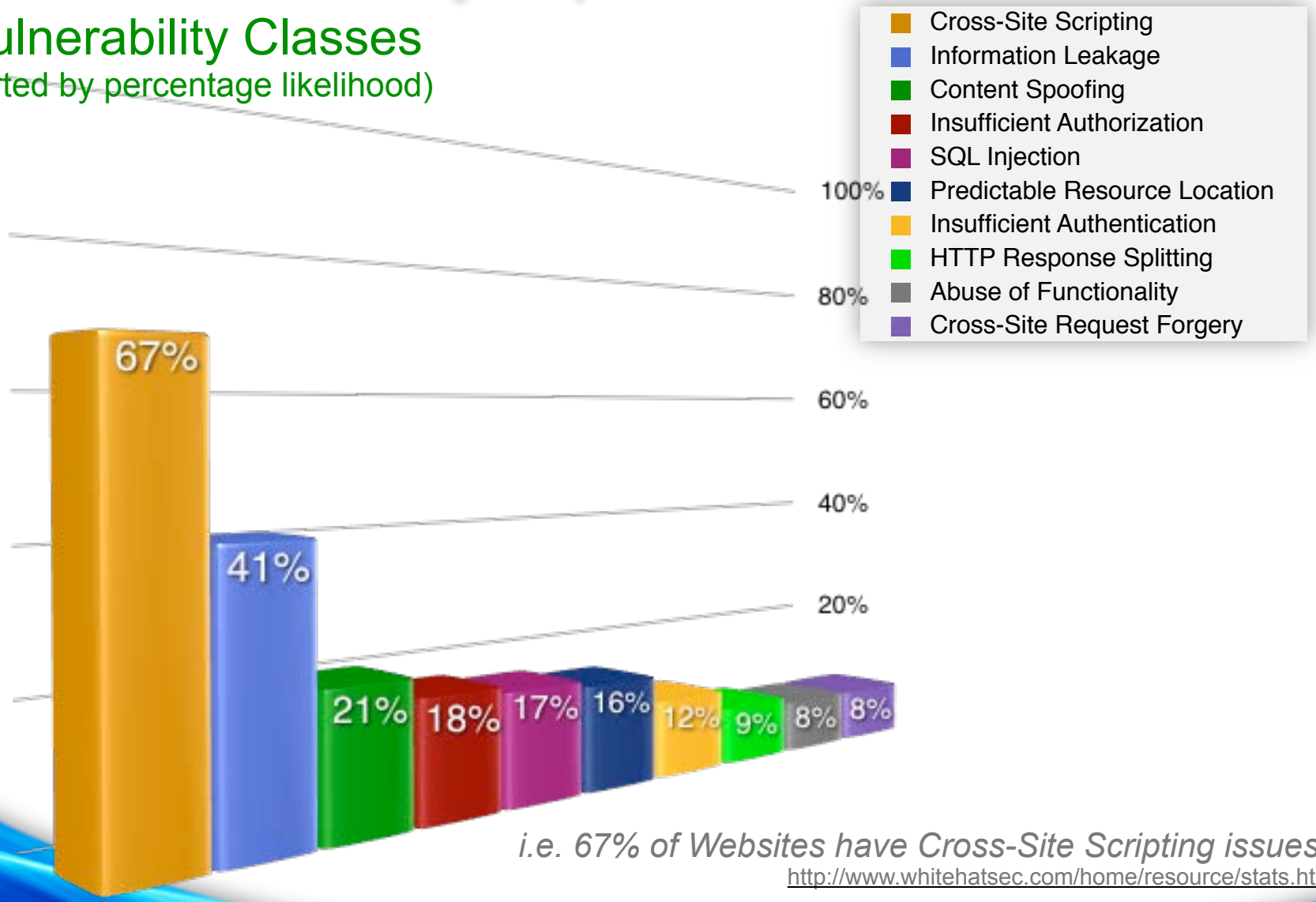
http://jeremiahgrossman.blogspot.com/2008/07/results-web-application-security.html
http://jeremiahgrossman.blogspot.com/2007/10/web-application-security-professionals.html

WhiteHat SECURITY

# WhiteHat Security Top Ten

## Vulnerability Classes

(sorted by percentage likelihood)

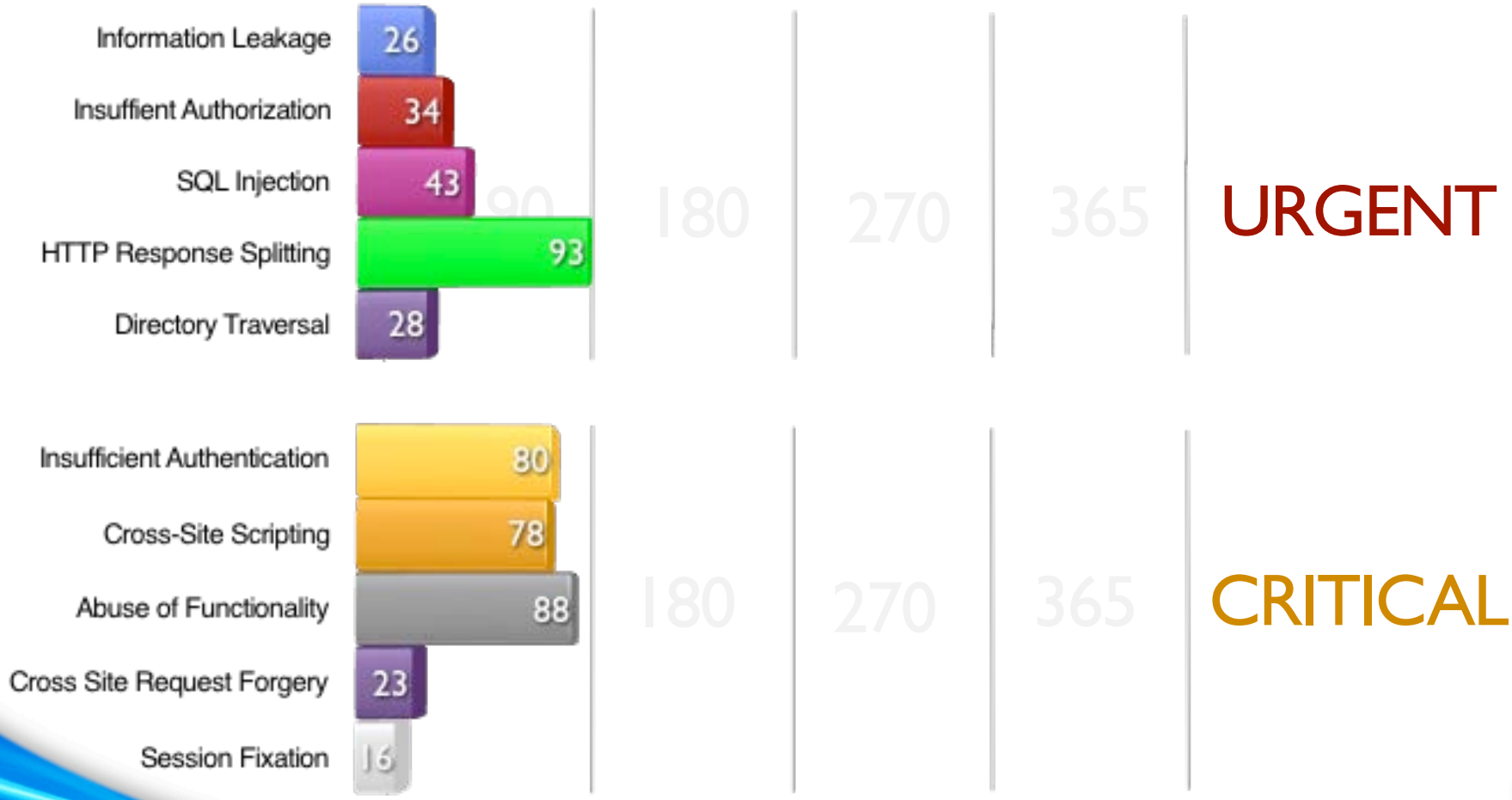



*i.e. 67% of Websites have Cross-Site Scripting issues*

http://www.whitehatsec.com/home/resource/stats.html

WhiteHat SECURITY

# Time-to-Fix (Days)





# Mass SQL Injection / Drive-by-Download

1. Google recon for weak websites (*.asp, *.php)
2. Generic SQL Injection populates databases with malicious JavaScript IFRAMEs.
3. Visitors arrive (U.N., DHS, etc.) and their browser auto-connects to a malware server infecting their machine with trojans.
4. Botnets form with then continue SQL injecting websites


Over **79%** of websites hosting *malicious code* are legitimate (compromised by attackers)

http://blogs.zdnet.com/security/?p=1150
http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html
http://blogs.zdnet.com/security/?p=1122
http://news.zdnet.com/2424-1009_22-198647.html
http://ddanchev.blogspot.com/2008/04/united-nations-serving-malware.html

WhiteHat SECURITY

# Moral of the Story...

Fix your website vulnerabilities and patch your browsers.

But how much does that really help?

JavaScript malware exploitation can STILL lead to history stealing, intranet hacking, login detection, Web worms, phishing w/ superbait, password theft, session hijacking, accessing illegal content, hacking third-party websites, etc.

Research over the last 7 years

WhiteHat SECURITY


## Get Rich or Die Trying

*"Making Money on The Web, The Black Hat Way"*

*Jeremiah Grossman, Trey Ford*

## Encoded, Layered, and Transcoded Attacks:

*"Threading the Needle past Web Application Security Controls"*

*Arian Evans*

## Xploiting Google Gadgets:

*"Gmalware and Beyond"*

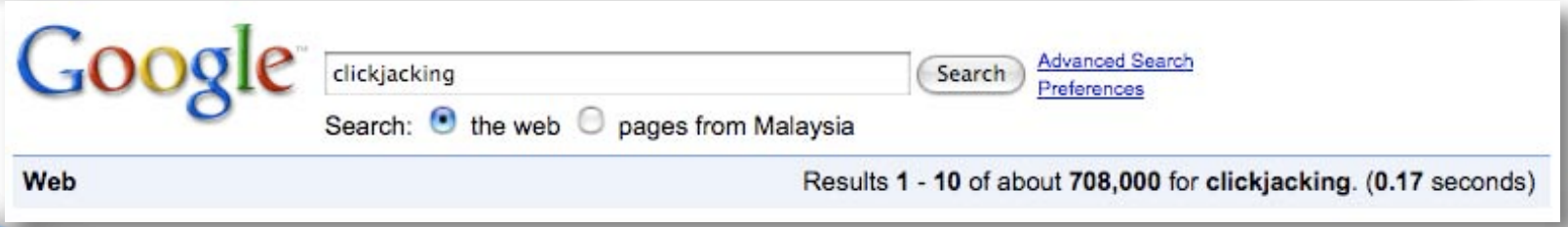
*Robert Hansen, Tom Stracener*

https://www.blackhat.com/html/bh-usa-08/bh-usa-08-schedule.html



# Clickjacking, the New Hotness

# What is Clickjacking?

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.

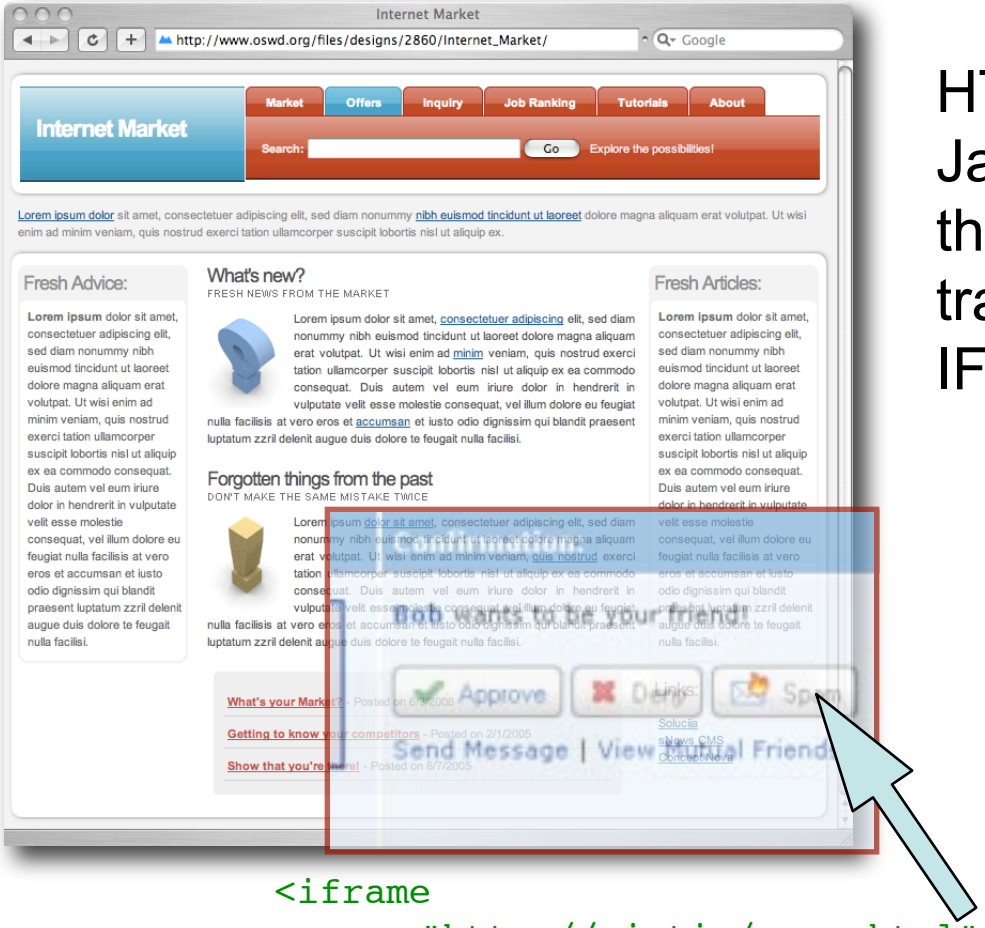
**Next consider that an attacker can invisibly hover these buttons below the user's mouse,** so that when a user clicks on something they visually see, they're actually clicking on something the attacker wants them to.

What could the bad guy do with that ability?

Clickjacking enables other attacks

WhiteHat SECURITY

# Hover Invisible IFRAMEs



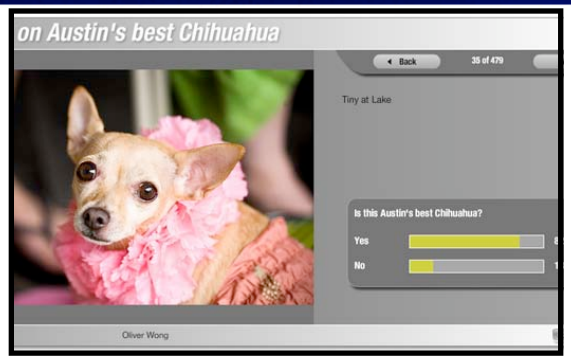

HTML, CSS, and JavaScript may size, follow the mouse and make transparent third-party IFRAME content.

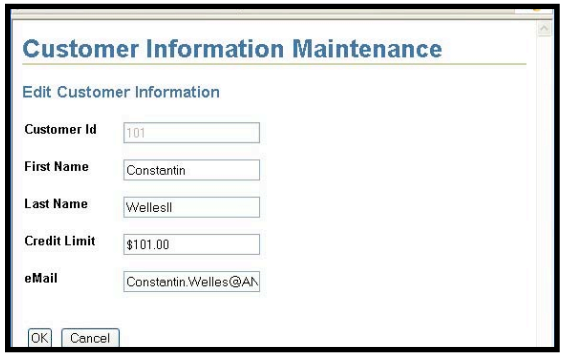
```
<iframe
   src="http://victim/page.html"
   scrolling="no"
   frameborder="0"
   style="opacity:.1;filter: alpha(opacity=.1); -moz-opacity:1.0;">
</iframe>
```

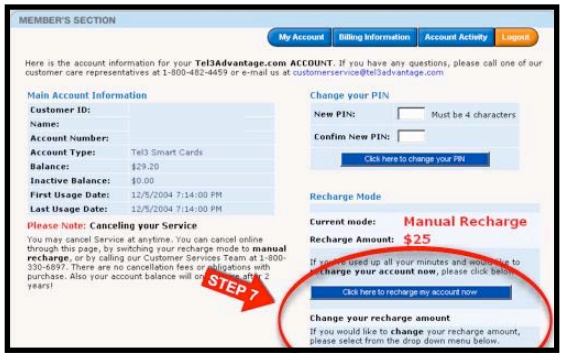

1 x Heritage Grunge Clikit $3.50
- Zip Part 1: Download
Sub-Total: $3.50
Free Shipping: $0.00
Discount Coupons: couponcode : -$3.50
Total: $0.00
Shipping Method: Free Shipping
edit
Payment Method:
edit
Final Step
confirm

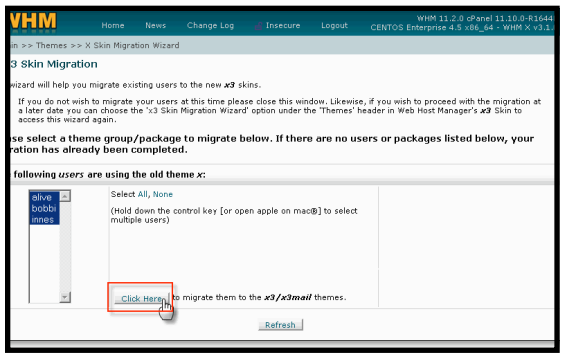

below:
Heritage Grunge Clikit
Your Order Numbe
You can view your order
ng to the My Account
page and by clicking on view
rs.
Please direct any questions you
ve to customer service.
Thanks for shopping with us online!
Download your products here:


on Austin's best Chihuahua
Back
35 of 479
Tiny at Lake
Is this Austin's best Chihuahua?
Yes
No
Oliver Wong

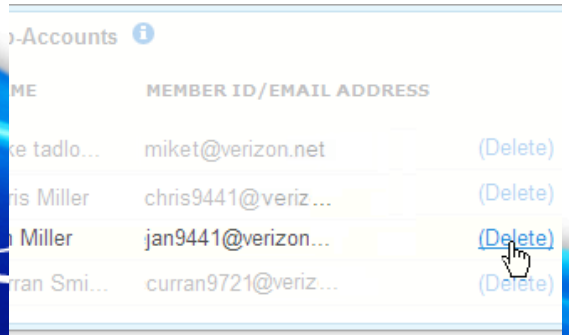

Customer Information Maintenance
Edit Customer Information
Customer Id
101
First Name
Constantin
Last Name
Wellesll
Credit Limit
$101.00
eMail
Constantin.Welles@AN
OK
Cancel

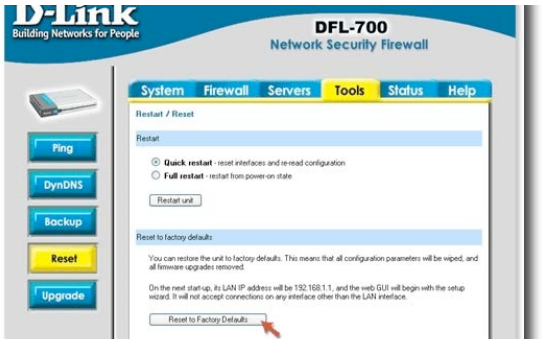

Received Calls
Placed Calls
Cisco Directory - Quick
Cisco Directory - Advanced
Select a directory...
Select
Clear
Exit


MEMBER'S SECTION
My Account
Billing Information
Account Activity
Logout
Main Account Information
Customer ID:
Name:
Account Number:
Account Type:
Balance:
Inactive Balance:
First Usage Date:
Last Usage Date:
Change your PIN
New PIN:
Confirm New PIN:
Click here to change your PIN
Recharge Mode
Current mode:
Manual Recharge
Recharge Amount:
$25
Click here to recharge my account now
Change your recharge amount
STEP 7

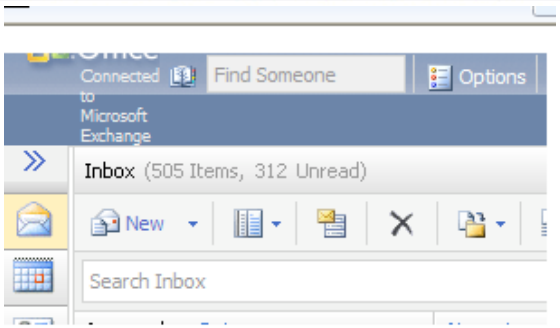

VHM
Home
News
Change Log
Insecure
Logout
3 Skin Migration
Select All, None
Click Here
Refresh

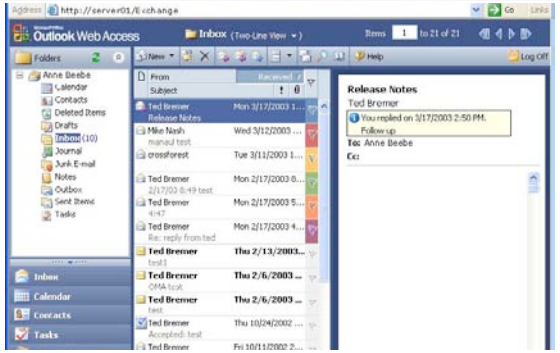

1
digg
digg me

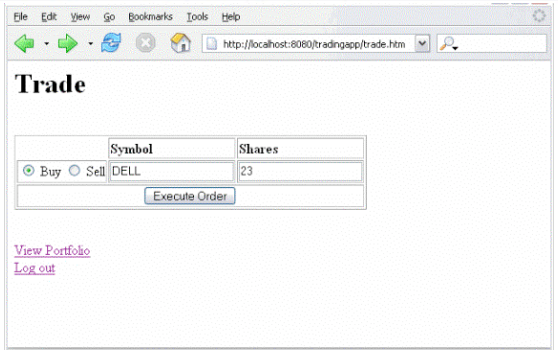

MEMBER ID/EMAIL ADDRESS
miket@verizon.net
(Delete)
chris9441@veriz...
(Delete)
jan9441@verizon...
(Delete)
curran9721@veriz...
(Delete)


D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Firewall
Servers
Tools
Status
Help
Restart / Reset
Ping
DynDNS
Backup
Reset
Upgrade
Reset to factory defaults

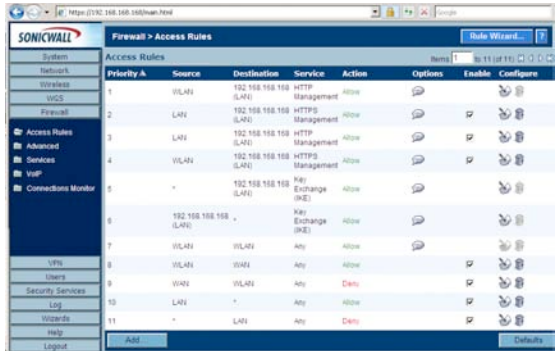

06/06/2007
07:38 AM
Order Status
Preferred ECN
Southern Copper Corporation Com
Bid 78.26 Ask 91.73

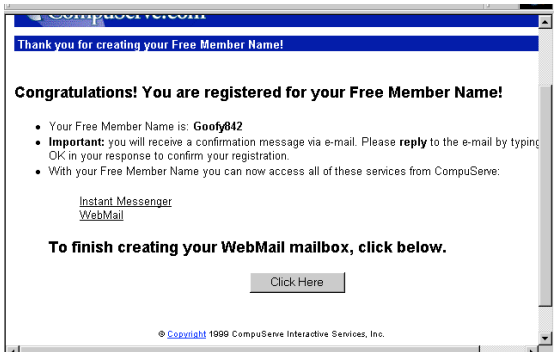

Connected to Microsoft Exchange
Find Someone
Options
Inbox (505 Items, 312 Unread)
New
Search Inbox

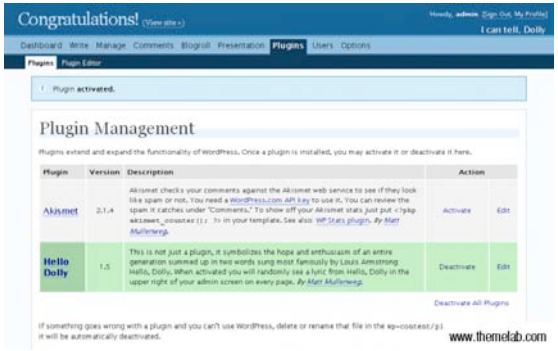

Outlook Web Access
Release Notes
Ted Bremer

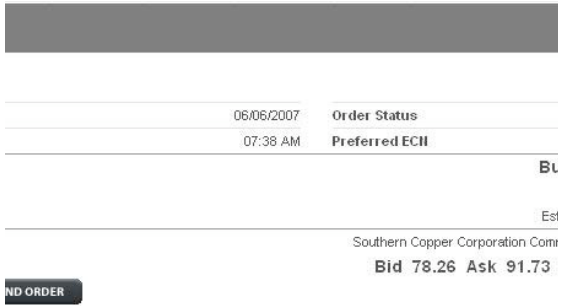

Trade
Symbol
Shares
Buy
Sell
DELL
23
Execute Order
View Portfolio
Log out

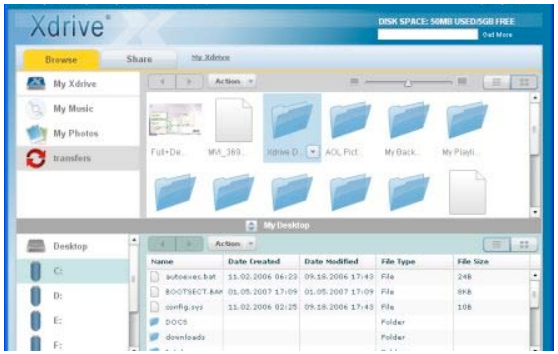

twitter
Name or location
search
jwilkins
Follow
not dead, just got back from burning man this
am, catching up and recoverinh
10 days ago from txt

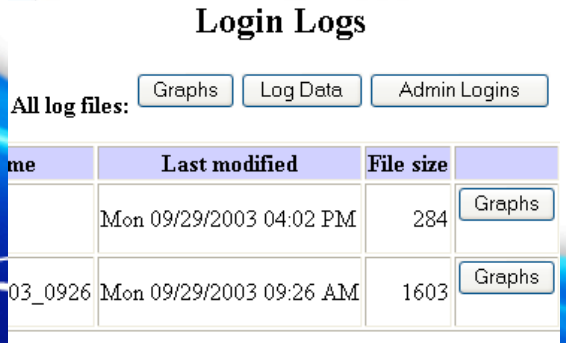

SONICWALL
Firewall > Access Rules
Access Rules


Thank you for creating your Free Member Name!
Congratulations! You are registered for your Free Member Name!
Your Free Member Name is: Goofy642
Instant Messenger
WebMail
To finish creating your WebMail mailbox, click below.
Click Here

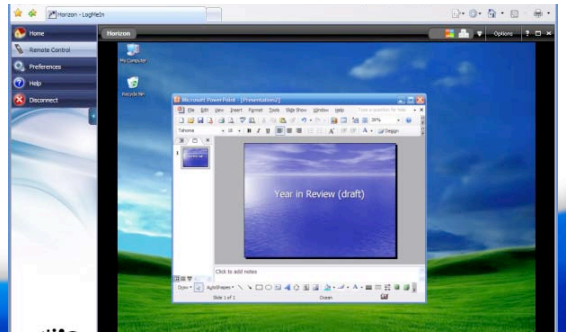

Congratulations!
Plugin Management
Akismet
Hello Dolly
www.themelab.com


06/06/2007
07:38 AM
Order Status
Preferred ECN
Southern Copper Corporation Com
Bid 78.26 Ask 91.73
ND ORDER


Xdrive
My Xdrive
My Music
My Photos
transfers
Desktop


Login Logs
All log files:
Graphs
Log Data
Admin Logins
Last modified
File size
Mon 09/29/2003 04:02 PM
284
Graphs
Mon 09/29/2003 09:26 AM
1603
Graphs


orkut
Friend confirmation
Please make sure that this person is your friend before you confirm
haven't met
acquaintance
friend
good friend
best friend
note: This selection is used to let you categorize your friends list and is o
visible to your friends.
Cancel
Confirm
orkutplus.org


Year in Review (draft)

# Additional PoC Work

Sexy Assassin (Eduardo “Sirdarckcat” Vela, Gareth Heyes, David “ Thornmaker” Lindsay)

http://sirdarckcat.blogspot.com/2008/10/about-css-attacks.html
http://www.thespanner.co.uk/wp-content/uploads/2008/10/the_sexy_assassin2ppt.zip

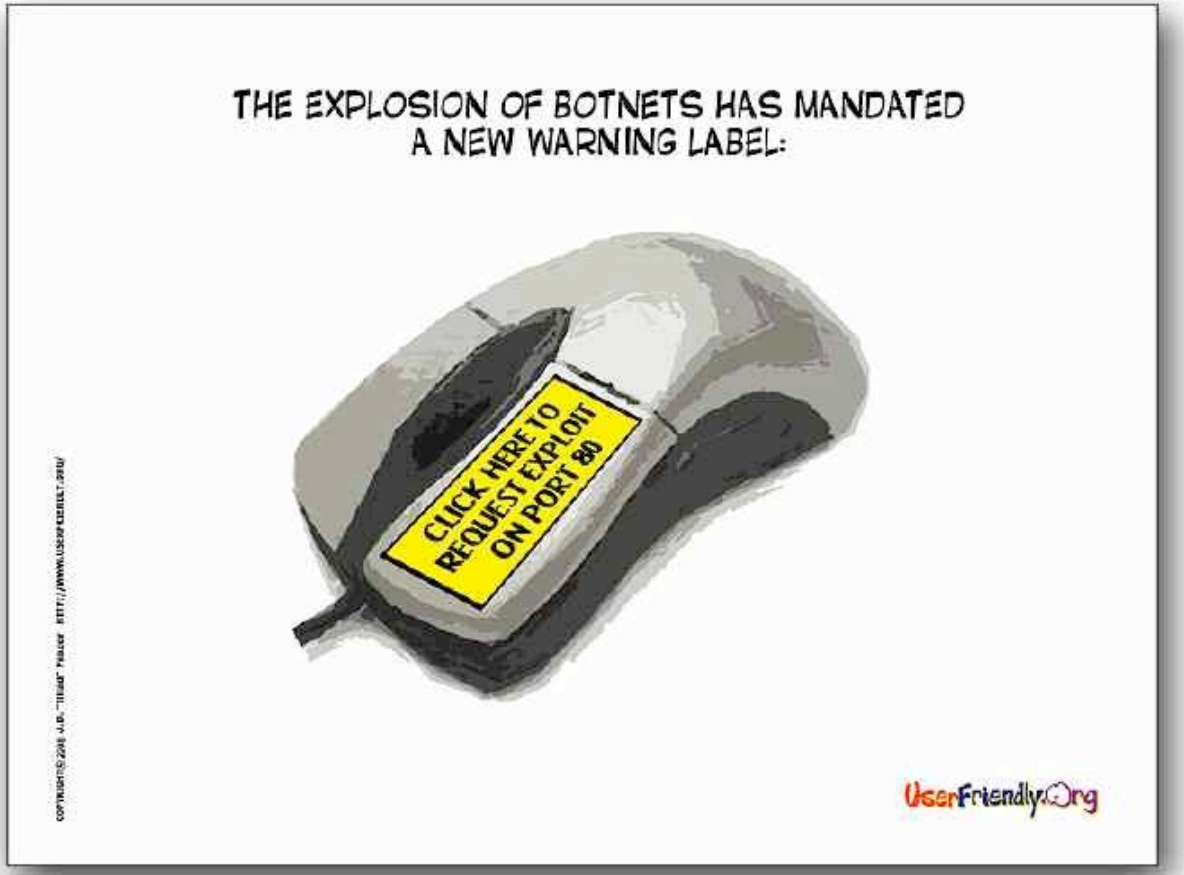
Petko D. (pdp) Petkov

http://lab.gnucitizen.org/projects/ui-redress-attacks
http://www.gnucitizen.org/blog/more-advanced-clickjacking-ui-redress-attacks/
http://www.gnucitizen.org/blog/clickjacking-and-flash/

# Clickjacking Bypasses CSRF Token Protection

The real user clicks on the real button on the real web page.



# Known Since 2002

## Misunderstood, Underestimated, and Long Forgotten

**Bugzilla@Mozilla – Bug 154957** iframe content background defaults to transparent Last modified: 2008-10-11 17:21:00 PDT

Home | New | Search | Find | Reports | Requests | New Account | Help | Log In

*First Last Prev Next No search results available*

**Bug 154957 - iframe content background defaults to transparent** Last Comment

**Status:** RESOLVED INVALID

**Reported:** 2002-06-29 02:06 PDT by Jesse Ruderman
**Modified:** 2008-10-11 17:21 PDT (History)

**Product:** Core
**Component:** Layout: View Rendering
**Version:** Trunk
**Platform:** All All

**Importance:** -- normal with 1 vote (vote)
**Target Milestone:** ---
**Assigned To:** Robert O'Callahan (:roc) (Mozilla Corporation)
**QA Contact:** Chris Petersen

**URL:**
**Whiteboard:** security
**Keywords:**

**Depends on:**
**Blocks:**

Show dependency tree / graph

Compelling, but not enough for a solid presentation or whitepaper...

https://bugzilla.mozilla.org/show_bug.cgi?id=154957

# “On the Internet, nobody knows you're a dog”

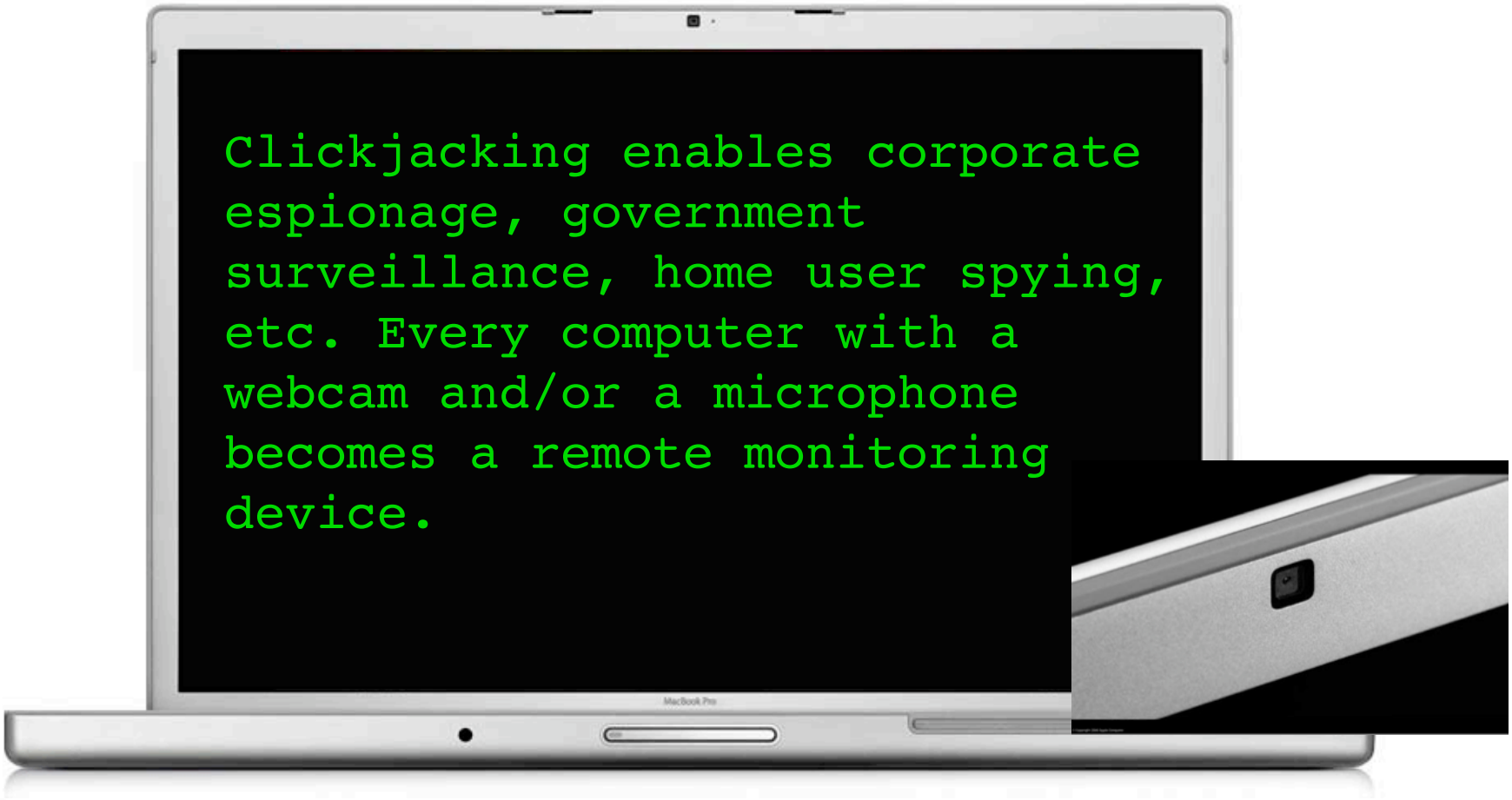
almost


http://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog



# What if a Web page could See and Hear you?




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

# If JavaScript can't do it, Ask Daddy Flash

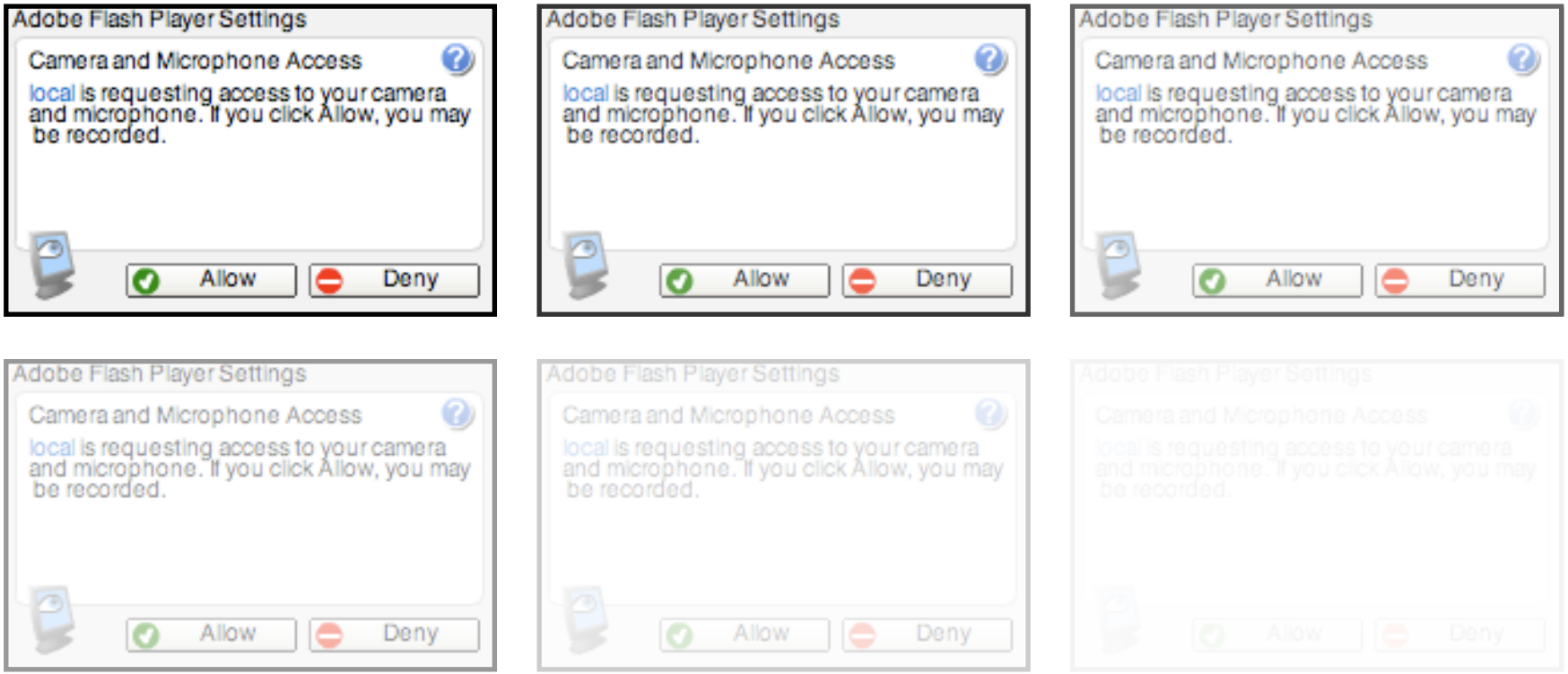
## Adobe Flash Player Version Penetration

Worldwide Ubiquity of Adobe Flash Player by Version — June 2008

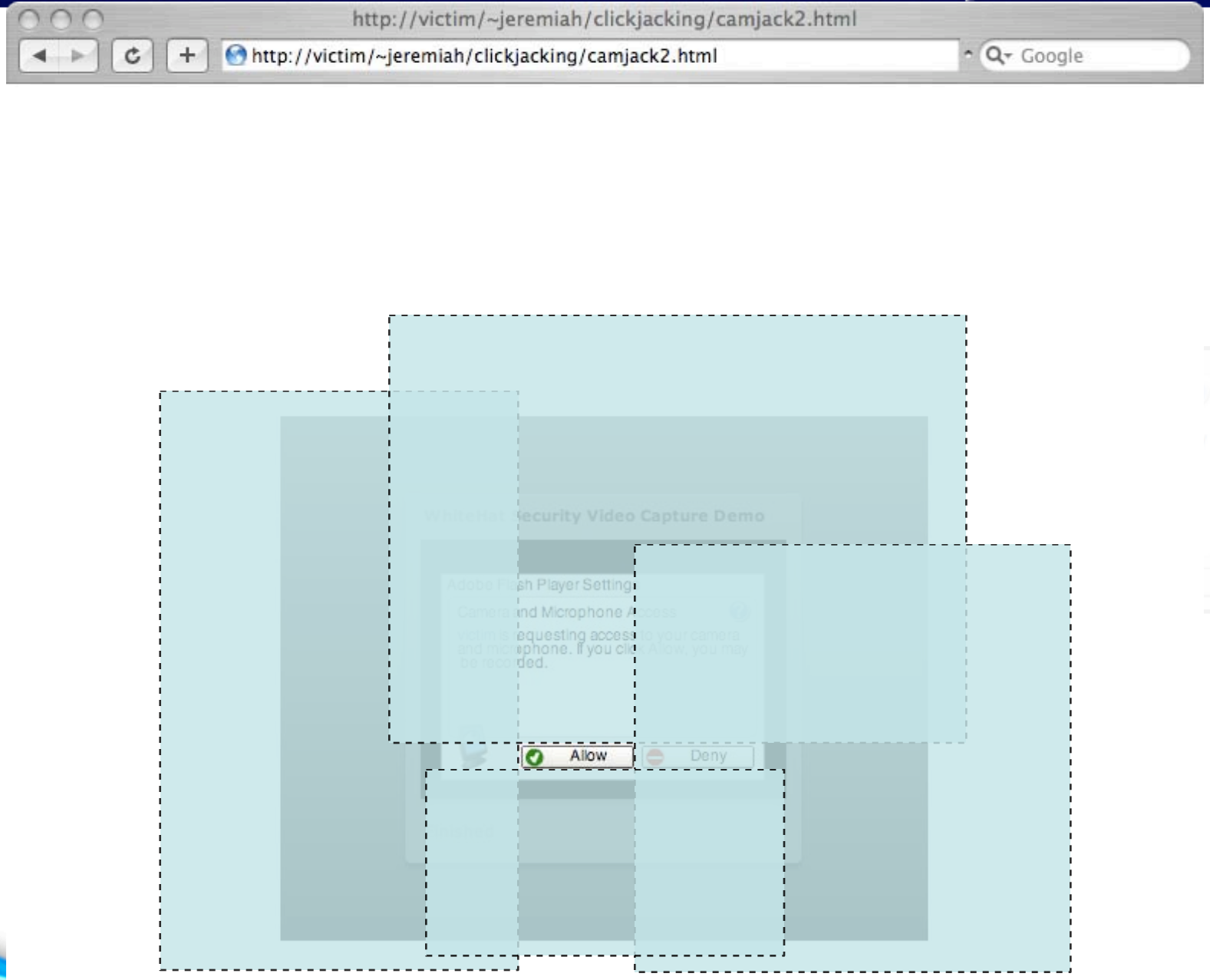
| | Flash Player 6 | Flash Player 7 | Flash Player 8 | Flash Player 9 | Flash Player 9.0.115* |
|---|---|---|---|---|---|
| Mature Markets[1] | No longer surveyed | 99.0% | 98.7% | 97.7% | 81.7% |
| US/Canada | No longer surveyed | 99.1% | 98.9% | 97.8% | 83.3% |
| Europe[2] | No longer surveyed | 98.5% | 97.9% | 96.5% | 78.6% |
| Japan | No longer surveyed | 99.3% | 99.3% | 98.8% | 81.3% |
| Emerging Markets[3] | No longer surveyed | 97.3% | 97.1% | 96.2% | 82.4% |

http://www.adobe.com/products/player_census/flashplayer/version_penetration.html

WhiteHat SECURITY




```
<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>
```


http://victim/~jeremiah/clickjacking/camjack2.html
http://victim/~jeremiah/clickjacking/camjack2.html
Google
Allow
Deny

# Global Security Settings Panel

Adobe Flash Player™ Settings Manager

Global Security Settings

Some websites may access inform
system of security. This is usually
sites could obtain unauthorized inf
website attempts to use the older

Always ask

Always trust files in these location

Adobe Flash Player™ Settings Manager

Website Privacy Settings

For websites you have already visited, view or change the privacy settings for access to your camera and / or microphone.

Always ask

Always allow

Always deny

Delete website | Delete all sites

Visited Websites

| Privacy | Websites | Used | Limit |
|---|---|---|---|
| | grack.com | - | 100 KB |
| | www.flickr.com | - | 100 KB |
| | www.keezmovies.com | - | 100 KB |
| | blip.tv | 1 KB | 100 KB |

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager04.html



# Now We're Ready to Publicly Present...

Submitted a CFP to OWASP AppSec NY 2008

New white paper - www.sectheory.com/clickjacking.htm

Research shared with Mozilla, Microsoft, and Adobe

**Adobe**: Why are you going to zero-day us!?
**Jeremiah/RSnake**: zero-day? What zero-day!? It's a browser problem!
**OWASP Organizer**: We understand if you must pull the talk.
**Media**: Red flags go up, emails start flying, and phone rings constantly
**Curmudgeons**: This is lame, partial disclosure, jerks, it's all hype.
**Browser Vendors**: We'll look closer at clickjacking and see what we can do.
**Researchers**: Is this it? No. Is this it? No. Is this is it? We can neither confirm nor deny.
**Giorgio Maone**: I can fix this. Wait almost, let me try again.
**Dhillon Andrew Kannabhiran**: Want to keynote HiTB with clickjacking?
**Guy Aharonovsky**: Spills the beans complete with PoC code and video. Uh Oh.

http://blogs.adobe.com/psirt/2008/10/clickjacking_security_advisory.html
http://blog.guya.net/2008/10/07/malicious-camera-spying-using-clickjacking/
http://blogs.adobe.com/psirt/2008/10/security_bulletin_for_flash_pl.html

# Website Defenses

Frame-busting code

JavaScript enabled buttons

```
<script>
if(top != self) top.location.href = location.href;
</script>
```

```
<iframe src=" fool.html" security=restricted></iframe>
```

Out-of-Band confirmation

Referer Checks



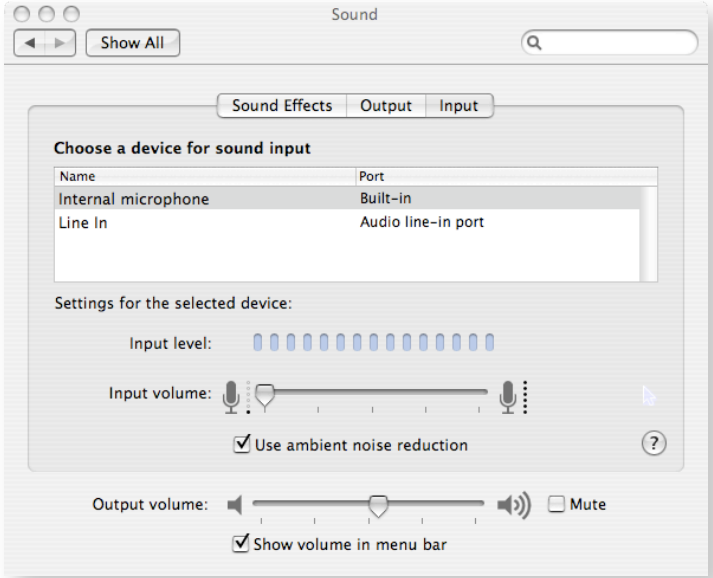
 

# Web Browser Defenses

- Upgrade to Flash Player 10
- NoScript w/ ClearClick
- FlashBlock
- Disable Plug-ins
- Virtualize
- Unplug or tape the webcam
- Disable or mute microphone

Content Security Policy

UI Redressing




http://noscript.net/
http://www.adobe.com/go/getflashplayer/
http://flashblock.mozdev.org/
http://people.mozilla.org/~bsterne/content-security-policy/details.html
http://lists.whatwg.org/pipermail/whatwg-whatwg.org/2008-September/016284.html

# Browser Vendor Conflict of Interest

Mozilla Products | Security

http://www.mozilla.com/en-US/firefox/security/

mozilla | Products | Add-ons | Support | Community | About

## The Safest Web Browser

Firefox keeps your personal info personal and your online interests away from the bad guys.

Products / Firefox

- Features
- Security
- Customization
- 100% Organic Software
- Tips & Tricks
- Release Notes
- Other Systems and Languages

### So How Do We Do It?

What makes Firefox different? Most importantly, we're open. That means anyone around the world (and we have thousands of experts watching our back) is able to look into our code and find any potential weak spots in our armor.

And when we hear about a problem, we roll up our sleeves and get to work fixing it right away. It's in your best interest (and ours) to take care of the issue, even if it means admitting we're a little less than perfect.

### Get Firefox 3

3.0.1, English (US), Mac OS X (17.2MB)

Download Now - Free

Release Notes - Other Systems and Languages



# Questions!?

For more information: http://www.whitehatsec.com/

**Jeremiah Grossman, founder and CTO**
blog: http://jeremiahgrossman.blogspot.com/
jeremiah@whitehatsec.com

Thank you Robert Hansen, Adobe PSIRT, HiTB

WhiteHat SECURITY