

Clickjacking

Vitaly Shmatikov

Reading Assignment

- ◆ “Next Generation Clickjacking”
- ◆ “Clickjacking: Attacks and Defenses”

Clickjacking (UI Redressing)

[Hansen and Grossman 2008]

- ◆ Attacker overlays multiple transparent or opaque frames to trick a user into clicking on a button or link on another page



- ◆ Clicks meant for the visible page are hijacked and routed to another, invisible page

Clickjacking in the Wild

- ◆ Google search for “clickjacking” returns 624,000 results... this is not a hypothetical threat!
- ◆ Summer 2010: Facebook worm superimposes an invisible iframe over the entire page that links back to the victim's Facebook page
 - If victim is logged in, automatically recommends link to new friends as soon as the page is clicked on
- ◆ Many clickjacking attacks against Twitter
 - Users send out tweets against their will

Clickjacking Meets Spamming

The image is a screenshot of a web browser displaying a BBC News article. The browser's address bar shows the URL www.bbc.co.uk/news/technology-16755434. The page features a navigation menu with categories like Home, US & Canada, Latin America, UK, Africa, Asia, Europe, Mid-East, Business, Health, Sci/Environment, Tech, Entertainment, and Video. The article is dated 27 January 2012 and was last updated at 17:04 ET. The main headline is "Facebook sues alleged clickjacking spammer sparking row". The sub-headline reads: "Facebook is suing a marketing firm, accusing it of 'spreading spam through misleading and deceptive tactics'." The text continues: "Adscend Media is alleged to have carried out 'clickjacking'." and "The practice involves placing posts on the social network which include code that causes the links to appear on the users' homepages as". An inset image shows a close-up of a computer screen displaying a Facebook profile page with a 'GETTY IMAGES' watermark. To the right of the article, there is a "Top stories" section with a photo of a man in a suit and a list of headlines: "Greek PM gives final euro warning NEW", "Syria general 'shot in Damascus'", "Sun 'will continue' says Murdoch", "S Africa to get Mandela banknotes", and "Iran to make nuclear announcement". Below that is a "Features & Analysis" section with a sub-headline "Too revealing".

BBC News - Facebook sues

www.bbc.co.uk/news/technology-16755434

Home US & Canada Latin America UK Africa Asia Europe Mid-East Business Health Sci/Environment Tech Entertainment Video

27 January 2012 Last updated at 17:04 ET

Facebook sues alleged clickjacking spammer sparking row

Facebook is suing a marketing firm, accusing it of "spreading spam through misleading and deceptive tactics".

Adscend Media is alleged to have carried out "clickjacking".

The practice involves placing posts on the social network which include code that causes the links to appear on the users' homepages as

979 Share

Top stories

Greek PM gives final euro warning **NEW**

Syria general 'shot in Damascus'

Sun 'will continue' says Murdoch

S Africa to get Mandela banknotes

Iran to make nuclear announcement

Features & Analysis

Too revealing

GETTY IMAGES

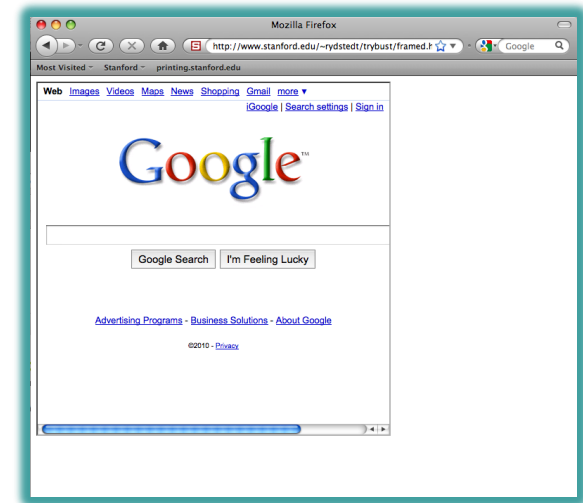
It's All About iFrame

- ◆ Any site can frame any other site

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

- ◆ HTML attributes

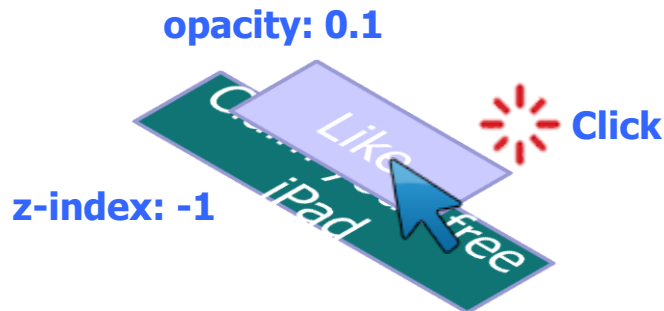
- Style
- Opacity defines visibility percentage of the iframe
 - 1.0: completely visible
 - 0.0: completely invisible



Hiding the Target Element

[“Clickjacking: Attacks and Defenses”]

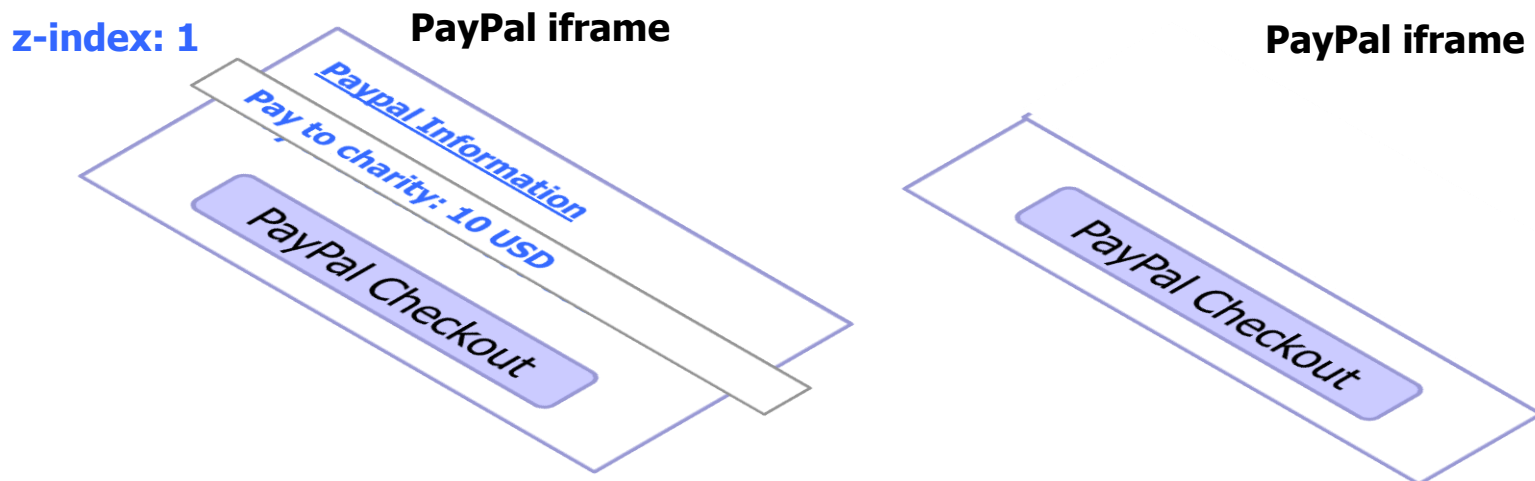
- ◆ Use CSS `opacity` property and `z-index` property to hide target element and make other element float under the target element
- ◆ Using CSS `pointer-events: none` property to cover other element over the target element



Partial Overlays and Cropping

[“Clickjacking: Attacks and Defenses”]

- ◆ Overlay other elements onto an iframe using CSS `z-index` property or Flash Window Mode `wmode=direct` property
- ◆ Wrap target element in a new iframe and choose CSS position offset properties



Drag-and-Drop API

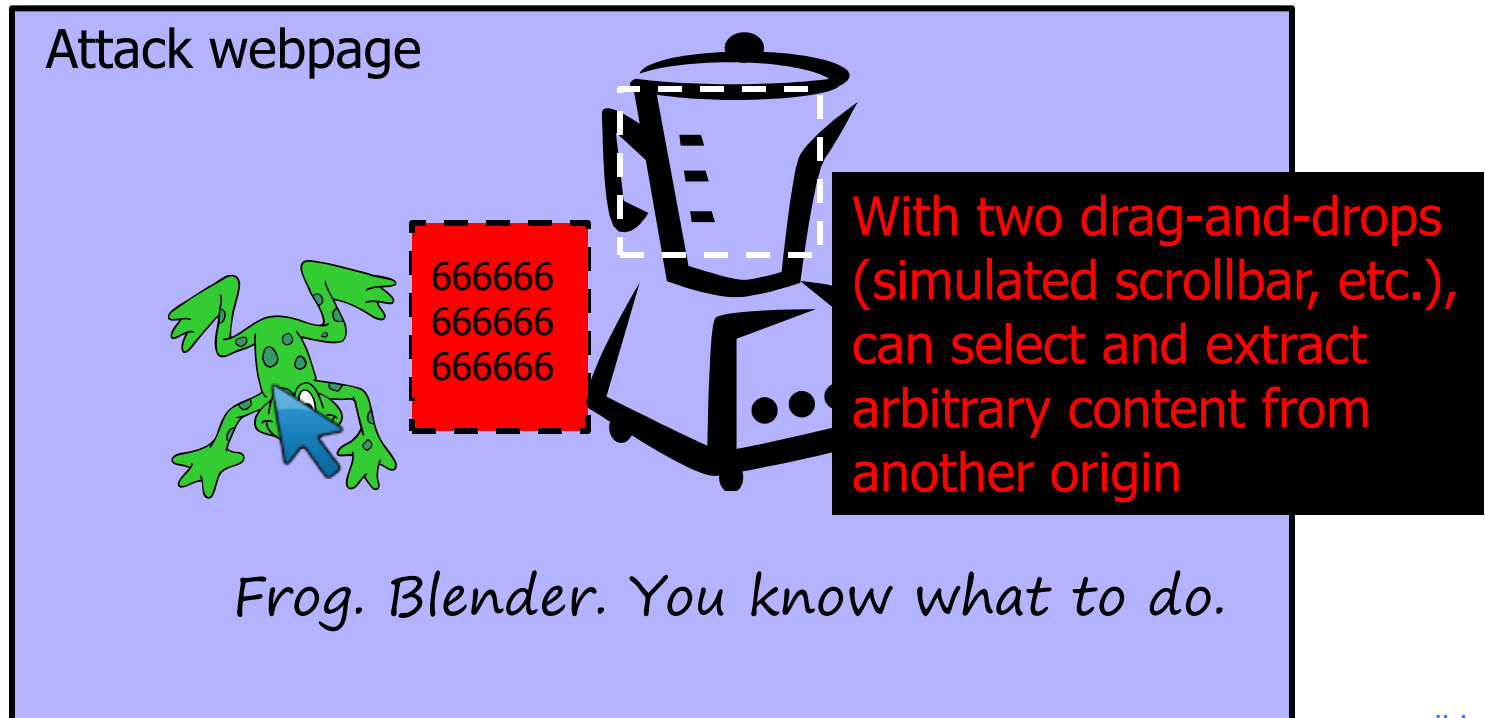
[“Next Generation Clickjacking”]

- ◆ Modern browsers support drag-and-drop API
- ◆ JavaScript can use it to set data being dragged and read it when it's dropped
- ◆ Not restricted by the same origin policy: data from one origin can be dragged to a frame of another origin
 - Reason: drag-and-drop can only be initiated by user's mouse gesture, not by JavaScript on its own

Abusing Drag-and-Drop API

[“Next Generation Clickjacking”]

1. Bait the user to click and start dragging
2. Invisible iframe with attacker’s text field under mouse cursor, use API to set data being dragged
3. Invisible iframe from another origin with a form field



Fake Cursors

[“Clickjacking: Attacks and Defenses”]

- ◆ Use CSS `cursor` property and JavaScript to simulate a fake cursor icon on the screen

Real cursor icon

cursor: none



Fake cursor icon



Keyboard “Strokejacking”

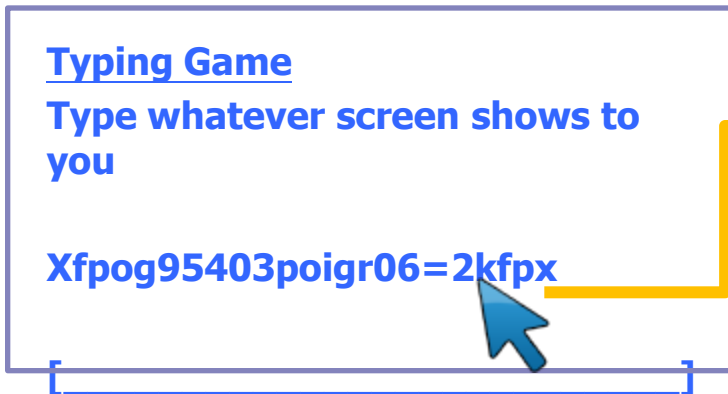
[“Clickjacking: Attacks and Defenses”]

- ◆ Simulate an input field getting focus, but actually the keyboard focus is on target element, forcing user to type some unwanted information into target element

Attacker’s page

Typing Game
Type whatever screen shows to you

Xfpog95403poigr06=2kfpX



Hidden iframe within attacker’s page

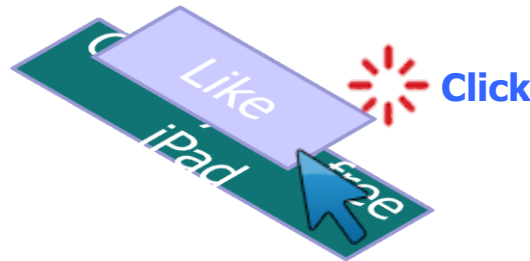
Bank Transfer
Bank Account: 9540
Amount: 3062 USD

Transfer

Compromising Temporal Integrity

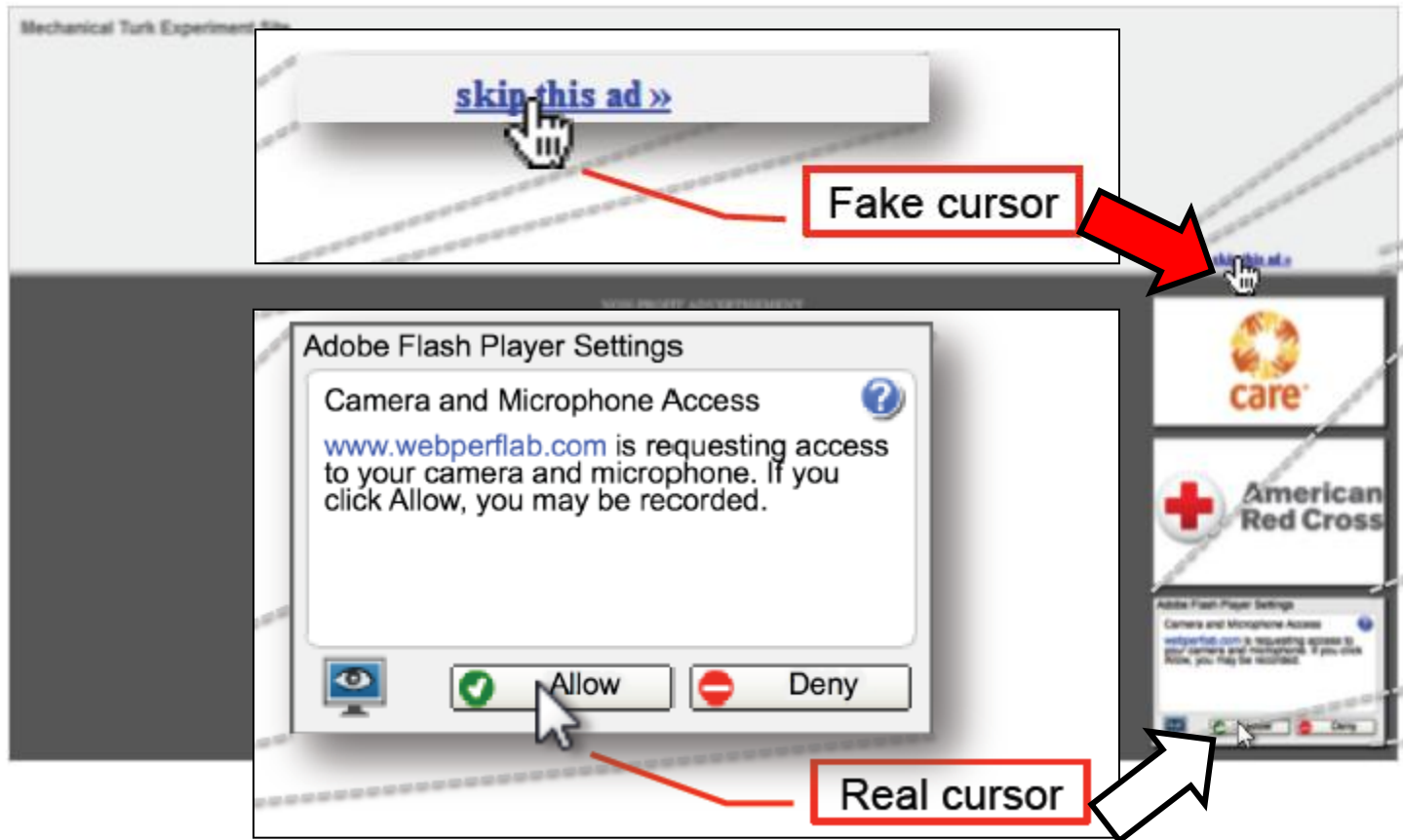
[“Clickjacking: Attacks and Defenses”]

- ◆ Manipulate UI elements after the user has decided to click, but before the actual click occurs



Cursor Spoofing

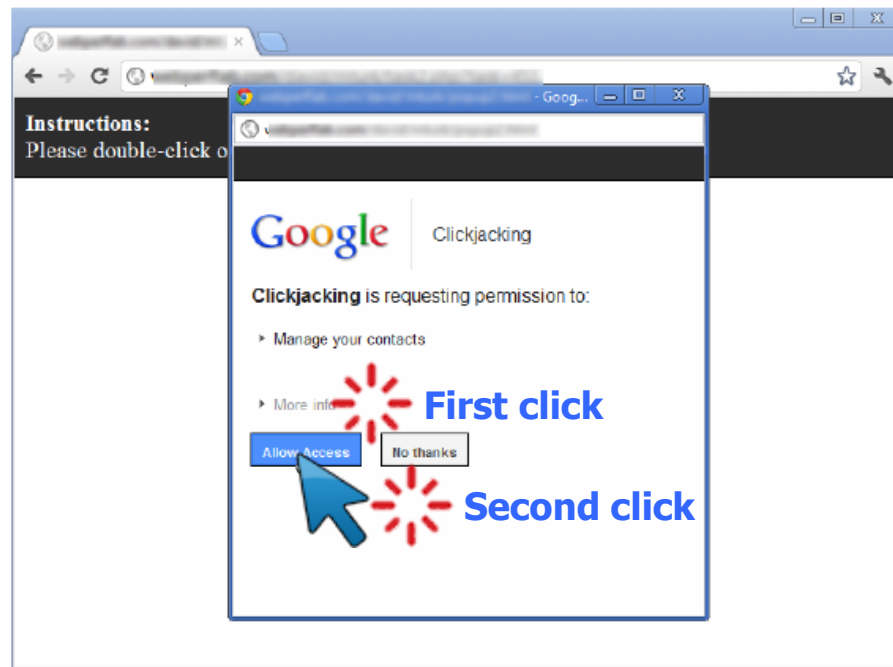
[“Clickjacking: Attacks and Defenses”]



Double-Click Attack

[“Clickjacking: Attacks and Defenses”]

- ◆ Bait the user to perform a double-click, switch focus to a popup window under the cursor right between the two clicks



Whack-A-Mole Attack

[“Clickjacking: Attacks and Defenses”]

- ◆ Ask the user to click as fast as possible, suddenly switch Facebook Like button

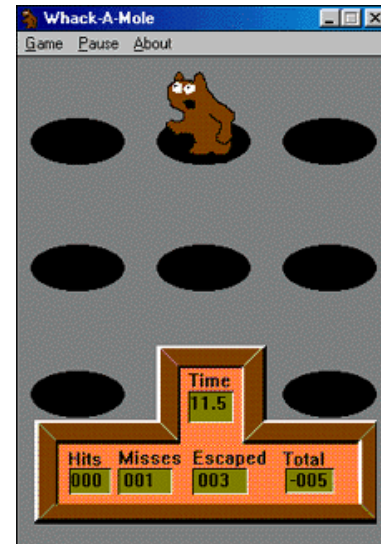
Instructions:

Please click on blue buttons *as fast as possible*. The faster you complete this game, the greater your chances to win a \$100 prize! If you don't click on a button, the game will skip it in 10 seconds.

Buttons clicked: 17/20

Time elapsed: 27.6 sec

CLICK ME



Solution: Frame Busting

- ◆ I am a page owner
- ◆ All I need to do is make sure that my web page is not loaded in an enclosing frame ...

Clickjacking: solved!

- Does not work for FB "Like" buttons and such, but Ok

- ◆ How hard can this be?

```
if (top !== self)
    top.location.href = location.href
```

Frame Busting in the Wild

- ◆ Survey by Gustav Rydstedt, Elie Burzstein, Dan Boneh, Collin Jackson



Following slides shamelessly jacked from Rydstedt

If My Frame Is Not On Top ...

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!=
```

... Move It To Top

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)
```

What About My Own iFrames?

- ◆ Check: **is the enclosing frame one of my own?**
- ◆ How hard can this be?
- ◆ Survey of several hundred top websites ...
... **all** frame busting code is broken!

Courtesy of Walmart

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



Error in Referrer Checking

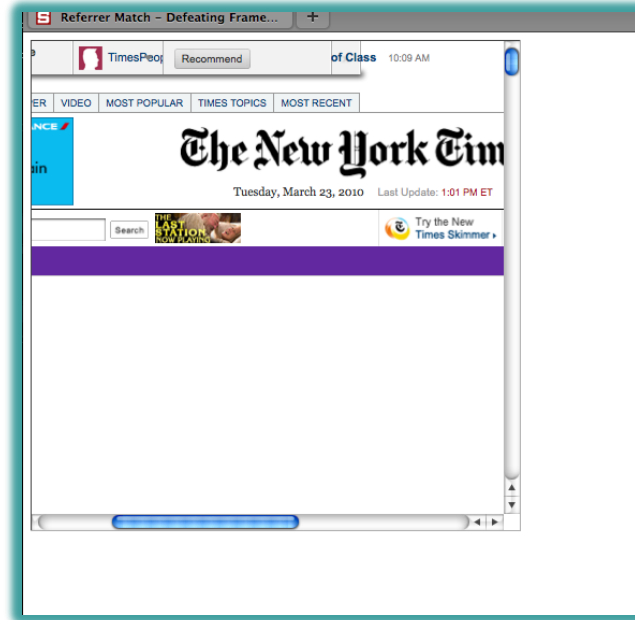


From <http://www.attacker.com/walmart.com.html>
<iframe src="http://www.walmart.com">

Courtesy of *The New York Times*

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


Error in Referrer Checking

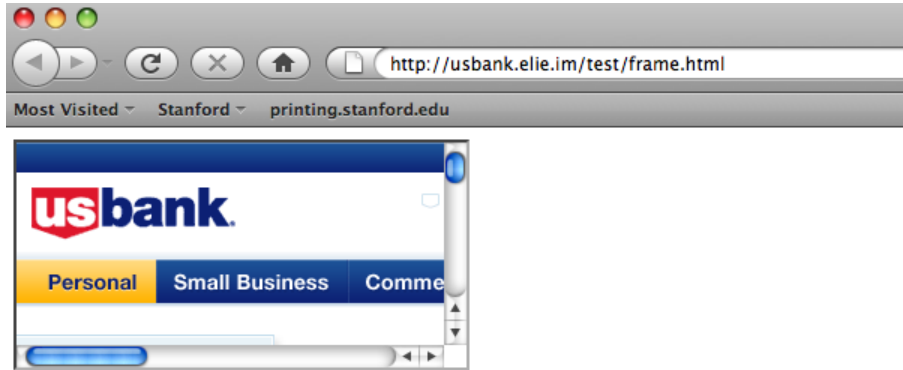


From <http://www.attacker.com/a.html?b=https://www.nytimes.com/>
<iframe src="http://www.nytimes.com">

Courtesy of

```
if (self != top) {  
    var domain = getDomain(document.referrer);  
    var okDomains = /usbank|localhost|usbnet/;  
    var matchDomain = domain.search(okDomains);  
  
    if (matchDomain == -1) {  
        // frame bust  
    }  
}
```

Error in Referer Checking



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

Strategic Relationship?

Norwegian State House Bank

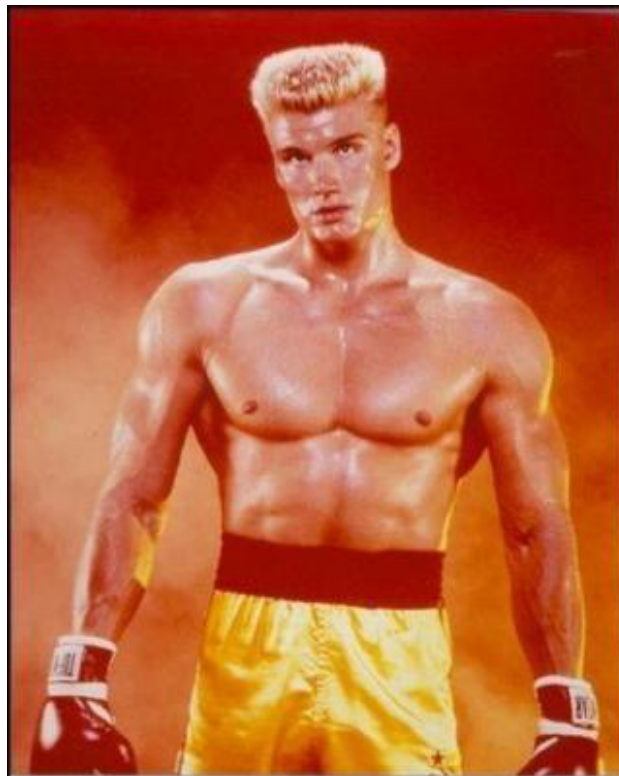
<http://www.husbanken.no>



Strategic Relationship?

Bank of Moscow

<http://www.rusbank.org>



Courtesy of



```
try{
  A=!top.location.href
} catch(B){}
A=A&&
!(document.referrer.match(/^https?:\V\[-az09.]
*\.\google\.(co\.|com\.)? [a-z] +\imgres/i))&&
!(document.referrer.match(/^https?:\V\([^\V]*\.)?
(myspace\.com|
myspace\.cn|
simsidekick\.com|
levisawards\.com|
digg\.com)\//i));

if(A){ // Frame bust }
```

Do Your Trusted Sites Frame Bust?



Google Images does not frame bust

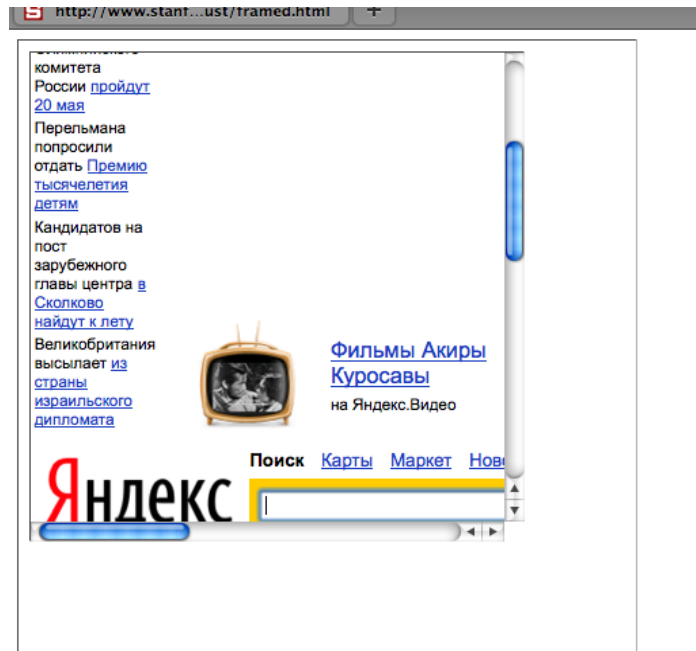
Many Attacks on Referer Header

- ◆ Open redirect referer changer
- ◆ HTTPS->HTTP redirect changes the header
- ◆ Apparently, hard to get regular expression right
- ◆ Trust other sites to frame your pages, but what if those trusted sites can be framed themselves?

Typical Frame Busting Code

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

Who Is Your ~~Daddy~~ Parent?



Double framing!!

```
framed1.html
<iframe
src="framed2.html">
```

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

Descendant Navigation Policy

- ◆ A frame can only navigate its descendants

```
framed1.html  
<iframe  
src="framed2.html">
```

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

- ◆ `top.location = self.location` is always okay

Who Is On Top?

```
if (top.location != self.location)
    top.location = self.location
```

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

Location Clobbering

◆ IE 7

```
var location="clobbered";
```

◆ Safari

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

- `top.location` now undefined

User Can Stop Frame Busting

- ◆ User can manually cancel any redirection attempt made by frame busting code
- ◆ Attacker just needs to ask...

```
<script>
```

```
    window.onbeforeunload = function() {  
        return "Do you want to leave PayPal?";  
    }
```

```
</script>
```

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

Ask Nicely

The image shows a web browser window displaying the PayPal homepage. The browser's address bar shows the URL `http://www.stanford.edu/~rydstedt/c`. The browser tabs include "stanford Online - 12..." and "Ask Nicely - Defeating Framebusti...". The PayPal homepage features a navigation menu with "Home", "Personal", "Business", and "Developers" tabs. Below the menu are links for "How PayPal Works", "Pay Online", "Send Money", "Get Paid", and "Products & Services". On the left, there is an "Account login" section with input fields for "Email address" and "PayPal password", a "Go to" dropdown menu set to "My account", and a "Log In" button. Below the login section are links for "Problem with login?" and "New to PayPal? Sign up.". The main content area displays a "WELCOME TO PayPal" banner with the tagline "The world's most-loved way to pay a" and a "PayPal Shopping ALL THE BRAND" banner featuring a couple with shopping bags. A "Confirm" dialog box is overlaid on the right side of the browser window. The dialog has a blue question mark icon and contains the following text: "Confirm", "Are you sure you want to navigate away from this page?", "Do you want to leave PayPal?", and "Press OK to continue, or Cancel to stay on the current page." At the bottom of the dialog are "Cancel" and "OK" buttons.

... Or Don't Even Ask

- ◆ Most browsers let **attacker** 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">
```


X-Frame-Options

- ◆ HTTP header sent with the page
- ◆ Two possible values: **DENY** and **SAMEORIGIN**
- ◆ DENY: page will not render if framed
- ◆ SAMEORIGIN: page will only render if top frame has the same origin

Adoption of X-Frame-Options

- ◆ Good adoption by browsers
- ◆ Poor adoption by sites
- ◆ Limitations
 - Per-page policy
 - No whitelisting of origins
 - Proxy problems

Content Security Policy (Firefox 4)

- ◆ Another HTTP header: **frame-ancestors** directive can specify allowed framers
- ◆ Allows specific restrictions and abilities per site

Best For Now (Still Not Good)

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

These Sites Do Frame Busting

The Facebook logo, consisting of the word "facebook" in white lowercase letters on a dark blue rectangular background.

facebook®

The Twitter logo, featuring the word "twitter" in a light blue, rounded, lowercase font with a white outline.

twitter

The PayPal logo, with "PayPal" in a bold, italicized blue font, where the "P" is significantly larger than the other letters.

PayPal™

Do These?



Frame Busting on Mobile Sites

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
Wells Fargo	https://m.wf.com/	NO
NyTimes	http://m.nytimes.com	Redirect
E-Zine Articles	http://m.ezinearticles.com	Redirect

Tapjacking

- ◆ Zoom buttons in a transparent iframe so that they cover entire screen
- ◆ Hide or fake URL bar
- ◆ Make a page that masquerades as a known application to trick user into clicking

Read more:

<http://seclab.stanford.edu/websec/framebusting/>