

About CSS Attacks

About CSS Attacks - sirdarckcat, sirdarckcat.blogspot.com.

- Published: date not stated
- Original: <<https://sirdarckcat.blogspot.com/2008/10/about-css-attacks.html>>
- Preserved from: <https://sirdarckcat.blogspot.com/2008/10/about-css-attacks.html> (live) on 2026-08-10
- Licence: unknown

Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

Content

UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Gareth, David and I went to [Microsoft Bluehat v8](#), it was pretty fun meeting everyone.

Gareth described the talk pretty well in here: <http://www.thespanner.co.uk/2008/10/20/bluehat/>, ([slides](#)) anyway I want to show the stuff we didn't showed at Bluehat because of their no-zero-day policy (even if the vendor wasn't willing to patch).

So well we have the following clickjacking PoCs, that show different attack techniques.

Ghost Mirror - GMail PoC

<http://www.sirdarckcat.net/gmailclickjacking.html>

Sends an email when you click [Send] (check your sent mails folder).

This technique works like this:

You get a copy of the generated HTML code of the target webpage, then you simply hide everything, except for the button you want to overlay.. you could draw other things using absolute positioning, but this is enough for most scenarios.

You can checkout the "ghost page" here: <http://www.sirdarckcat.net/dad.html>

This attack has it's pros and it's cons.. the most important pro is that it's the best way of doing cross-browser exploits.. since you don't depend on the sizes, margins, overflow rules etc.. that different browsers use.

This attack (and PoC) was reported to Google Security Team on Sat, Sep 27, 2008 at 11:37 PM, the response was that it won't be fixed (I'm sure they have more serious issues to take care about).

Frame Cropping - Twitter PoC

<http://www.sirdarckcat.net/coconuterror.html>

This one uses another technique, that is usefull for selecting a specific section of a webpage, this specific PoC is Firefox only, not because the technique is not possible on other browsers, but because you have to make a different exploit for each different browser.

The way it works is using 2 iframes with a fixed height/width and position, you only have to positionate the iframe using negative left/top coordinates, once you have that, you crop to the height and width of the button.

If that's not possible due to styling specific issues, then you have to use a second iframe that will have a height/width of the size of the button to be overlayed.

Both iframes must have the CSS properties** overflow:hidden; **and** border: 0** (or their HTML attribute equivalent {like frameborder instead of border}).

This one is sexy :)

We also have the.. javascript ones.

Pixel Window - Adobe Flash Webcam PoC <http://ha.ckers.org/weird/cjdivtest.html>

This one overlays 4 divs leaving a window where the mouse will be clicked.

Update to the latest Adobe Flash Player to be protected against this vulnerability. <http://get.adobe.com/flash/>

Mouse Chase - Adobe Flash Webcam PoC

<http://grack.com/record/>

The same principle of Pixel Window..but now with the overlay chasing the mouse position.

CSS Attribute Reader Source Code

<http://eaea.sirdarckcat.net/cssar/v2/?source>

The first version of the reader wont be released yet, maybe later.. sorry.

This type of attack is relevant, because this could start a new type of attack based on XSS, that could be called Cross Site Styling (since we are not really using a scripting language).

There's another version, made by Wisec that is also pretty cool, based on meta refreshes, it calculates 1 char per second, [he'll be presenting it soon at ruxcon](#).

By the way, I also want to say thanks to the guys that attended [bunkent0r](#) for their feedback on the presentation.

Greetz!!