Hijacking Safari 4 Top Sites with Phish Bombs

Hijacking Safari 4 Top Sites with Phish Bombs - Inferno, securethoughts.com.

- Published: date not stated
- Original: <http://securethoughts.com/2009/08/hijacking-safari-4-top-sites-with-phish-bombs/>
- Current location: <https://securethoughts.com/2009/08/hijacking-safari-4-top-sites-with-phish-bombs/>
- Preserved from: https://securethoughts.com/2009/08/hijacking-safari-4-top-sites-with-phish-bombs/ (live) on 2026-08-09
- Licence: unknown

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.

Hijacking Safari 4 Top Sites with Phish Bombs | SecureThoughts.com

---

Hijacking Safari 4 Top Sites with Phish Bombs

Music: Bomfunk MC's – Super Electric

Well, this one is an interesting issue I found while evaluating Safari 4 Beta (v528.16). This is not your usual XSS or CSRF bug which requires a site vulnerability, but a persistent browser backdoor that impacts all Safari 4 users using versions 4.0.2 and below. I was pretty amazed at some of the new features offered by the latest version of Apple's browser, especially the hyped **Top Sites** and **Cover Flow**. I decided to hack this cool feature. Here is what i found.

========== **SECURETHOUGHTS.COM ADVISORY**

- CVE-ID : CVE-2009-2196
- Release Date : August 11, 2009
- Discovered by : Inferno

==========

I. TITLE ————————- Hijacking Safari 4 Top Sites with Phish Bombs

II. VULNERABLE ————————- Safari 4 all versions < 4.0.3 Platforms affected - Mac OS X v10.4.11, Mac OS X Server v10.4.11, Mac OS X v10.5.7, Mac OS X Server v10.5.7, Windows XP and Vista

III. BACKGROUND ——————————- Safari is a web browser developed by Apple Inc. It is the default browser in Mac OS X v10.3 and higher. Safari for the Microsoft Windows platform first released on 11 June 2007 and currently supports both Windows XP and Windows Vista. The current stable release of the browser is 4.0.3 for Mac OS X and Windows. (Source – Wikipedia).

Safari 4 introduced the Top Sites feature to provide an at-a-glance view of a user's favorite websites. It is the most hyped feature of Safari 4 and widely used by users to quickly jump to their frequently used sites which can include their banks, email accounts, shopping sites, etc.

IV. DESCRIPTION ——————————- It is possible for a malicious website to place arbitrary sites into your Top Sites view through automated actions. The attack technique makes use of javascript windows where in a small window is used to repeatedly browse to different sites that the attacker wants to add in your Top Sites list. This window is completely hidden using the window.blur function and user won't know that is happening in the background. Please note that this attack is not possible using invisible iframes as Safari does not use iframe urls to decide Top Sites content.

Once the attack completes execution, the small window gets closed and the next time you use Safari Top Sites, it will be have the attacker's defined sites replace your existing legitimate sites. To make this decision of which sites to replace with, an attacker can first use the CSS History Hack found by Jeremiah Grossman[[2]](https://jeremiahgrossman.blogspot.com/2006/08/i-know-where-youve-been.html) and then accordingly set fake sites relative to those user's visited websites. Hence, this could easily facilitate a serious phishing attack. The situation is worsened by the Safari's inadequate protection against URL obfuscation attacks as highlighted in [[3]](https://securethoughts.com/2009/06/phishing-with-url-obfuscation-continues-in-safari-4), which makes it almost impossible for a regular user to spot the fake site and differentiate it from a legitimate one.

V. PROOF OF CONCEPT ——————————- http://securethoughts.com/b/q.htm The PoC currently runs in under a minute, which is based on most conservative input parameter values.

The two input parameters in this attack are the number of times the fake website should be visited (n)(default=28) and timeout(t)(default=2 sec) that triggers a switch between two fake websites. It is very simple and adds two fake websites for bankofamerica.com and gmail.com to your top sites. (it does not check your browser history, but that is left as an exercise for the reader [image: :)]). Also, you might have to increase the parameter value of 'n' if you visit your favorite sites very often.

A real-world hacking scenario would look like:

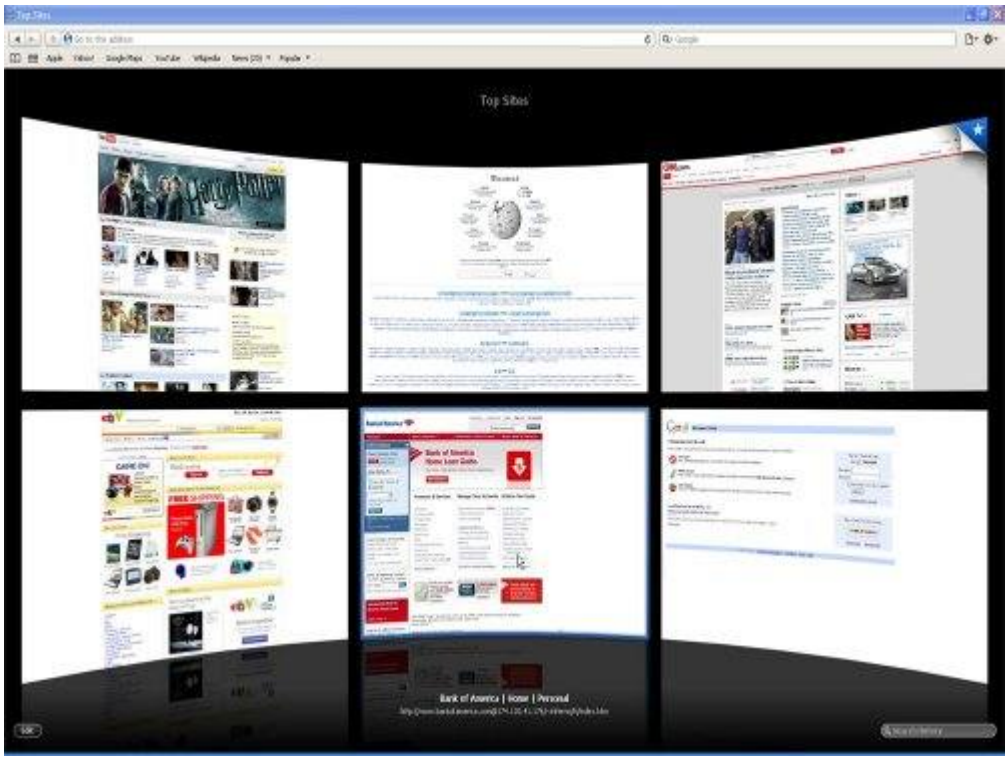
1. Attacker injects malicious javascript on

(a) His or her evil site OR (b) On a legitimate site which allows javascript (e.g. bulletin boards, dashboards, etc).

1. Victim visits the above site.
1. Malicious javascript runs and first checks browser history (using CSS history hack[2]) from a list of Alexa Top 500.
1. Attacker replaces the user's visited sites with fake phishing sites (makes legitimate sounding names with url obfuscation).

1. Every time user opens a phishing site and gets a login page, user's credentials gets stolen. Attacker will present a login error message, asking user to try again later. At the same time, attacker will reset that phishing site back to the legitimate page. This way, user will never know what happened.

1. On another note, attacker can always keep atleast 1 or 2 phishing websites at all times in Top Sites. This will help the attacker to maintain persistent control of a user's session and every time user visits a new site, it will be detected by the attacker and will be replaced by a phishing site in Top Sites.



VI. FIX DESCRIPTION ——————————- This issue is addressed by preventing automated website visits from affecting the Top Sites list. Only websites that are manually entered in the url address bar are considered to be placed in the Top Sites view.

VII. SOLUTION ——————————- Upgrade to Safari 4.0.3.

Apple security updates are available via the Software Update mechanism: http://support.apple.com/kb/HT1338

Apple security updates are also available for manual download via: http://www.apple.com/support/downloads/

VIII. REFERENCES ——————————-

1. Apple Security Updates

http://support.apple.com/kb/HT1222

1. Jeremiah Grossman's CSS History Hack

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

1. Phishing with URL Obfuscation continues in Safari 4

http://securethoughts.com/2009/06/phishing-with-url-obfuscation-continues-in-safari-4/

IX. CREDITS ——————————- This vulnerability is discovered by Inferno (inferno {at} securethoughts {dot} com)

XI. DISCLOSURE TIMELINE ——————————- May 21, 2009: Vulnerability discovered by Inferno. May 21, 2009: Apple contacted. May 21, 2009: Automated response from Apple. May 26, 2009: First response from Apple Security Team. Jun 03, 2009: First Status update provided by Apple. Jun 27, 2009: Second Status update provided by Apple. Jul 24, 2009: Coordinated public release of Advisory with Apple. Aug 11, 2009: Software Update and Public Advisory issued by Apple.

I would like to thank Apple Security Team for their timely responses, understanding the high severity of this issue and releasing a patch in a reasonable time period.

Both Chrome and Opera browsers offer similar features, but are not impacted by this vulnerability. Chrome only allows manually typed urls in the address bar to go into the “Most Visited” start page, whereas Opera requires a user to explicitly add his or her favorite web page as a speed dial entry. IE does not have this feature, so is unaffected by this.

I met several interesting people at BlackHat and Defcon this year from Apple, Microsoft, WhiteHat, SecTheory, McAfee, Paypal, etc. One of the folks i met was Daniel Herrera from SecTheory. He told me some of the research he had been doing, one of which was a similar anomaly in Top Sites. He was very happy to know that Apple is fixing this issue. In the near future, he will share with us his cool ideas. This includes some of the vulnerabilities he is working on for Opera.
