extern blog SensePost;

extern blog SensePost; - haroon, sensepost.com.

- Published: date not stated
- Original: <https://www.sensepost.com/blog/1303.html>
- Preserved from: https://www.sensepost.com/blog/1303.html (stored) on 2026-08-09
- Capture timestamp: 20120525021444
- 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.

extern blog SensePost;

|

| [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | | | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | |

| | |

| [image: image] | [image: image] | | | [image: image] | [image: image] | | | [image: Header] | [image: image] | [image: image] | | | [image: image] | | | [image: image] |

Fri, 10 Aug 2007

The slides | tool | paper from BlackHat07/DefCon07 have been posted online for your wget'ing pleasure.

More details on squeeza (the tool) can be found on the squeeza page, but in a nutshell is a sql injection tool that uses Metasploits concept of splitting exploit/payloads/etc with SQL Injection attacks. Current modules are written for MS-SQL server but include functionality for (user defined sql queries, some db schema enumeration, command execution, file-transfer, db_info) and the information is returned (channel selection) via one of (application error messages, DNS, Timing). The modularity'ness means that these all mix and match - I.e. if you write a module to "extract data from all tables that look like username*", the results would be available on any of the available channels.. (Its a pretty neat tool.. and saved our bacon more than once) So check it out, and send feedback to research@sensepost.com

The Paper / Slides (the paper really needs a touch of updating) cover the data exfiltration via DNS/Timing but also goes into a not-so-well-known attack dubbed Cross Site Request Timing. Since page load times (and other page activities) can be timed across the domains it ends up being a nice way to kick the same origin policy in the shins. (we know the world really doesnt need another acronym related to X.S* but couldnt resist!)

If nothing else, in its current guise the attack should let a popular page (one thats been reddit'ed / Slashdotted) make use of its visitors for a distributed brute force attack on web applications that track session-state through the URL/POST body..

Visio pic of the attack in action (courtesy of Nick our Visio Ninja)(click images for full size) [

[image: dxsrt.png]

"](http://www.sensepost.com/blogstatic/2007/08/dxsrt.png)

and the example we demo'd during the talk was a brute force attack on a time-leaky login page:

[

[image: dxsrt1.png]

"](http://www.sensepost.com/blogstatic/2007/08/dxsrt1.png)

Check out the paper / slides* and send us feedback...

(*Sadly in pdf, the slides do not play our embedded hampster .mp4.. so when u get to slide 40 please surf to http://youtube.com/watch?v=a1Y73sPHKxw)

| [image: image] | | | [image: image] | | | [image: image] | | | [image: image] | | | [image: image] | | | [image: image] | | | [image: image] | | | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | |

|

| [[image: Blog]](https://www.sensepost.com/blog/) | [image: image] | | | [image: image] | | | [image: image] | | | [image: image] | | | [[image: Video]](https://www.sensepost.com/videos/) | [image: image] | | | [image: image] | | | [[image: Research]](https://www.sensepost.com/research/) | [image: image] | | | [[image: QotW]](https://www.sensepost.com/qow/) | [image: image] | | | [image: image] | [image: image] | | | [image: image] | | | [image: image] | | | [image: Categories] | [image: image] | [image: image] | | | [image: image] | .ac.za (1) .za (2) about:us (38) analysis (4) auctions (1) auditors (1) b-sides (2) blackhat (17) blog (10) broadview (4) build-it (1) ccdcoe (1) cloud (12) community (19) conferences (73) consulting (1) crypto (4) estonia (1) fail (3) foos (1) footprinting (1) fun (51) goodbye (1) hackrack (2) Hope? (2) howto (10) imsojaded (2) infosec-soapies (25) infrastructure (3) interns (1) ios (1) jobs (1) local (7) mac (15) management (12) materials (3) memcached (2) metricon (2) metrics (3) mindless-politics (4) mindmaps (1) mobile (3) modelling (5) PCI (2) penny (1) pentest (2) phone (1) pickle (4) policy (1) post-it (1) presentations (2) Press (3) privacy (6) product (2) programming (5) public (329) python (5) [qo[w|m|?] (5)](https://www.sensepost.com/blog/?find=qo[w|m|?]) rambling (2) README (1) real-world (16) Release (3) report-info (1) research (52) reversing (10) risk (2) SAP (2) security-fyi (8) security-news (6) silly-yammerings (19) suru (1) tech-toys (3) threat (5) time-waster (6) tin-foil-hat (6) tools (49) training (31) travel (2) tricks (1) UK (2) Uncategorized (3) uncon (2) vendors (7) videos (6) vulnerability (10) wasc (1) webapps (6) web_x.0 (2) windows (1) writing-advice (1) zaprize (2) zen-hacking (6) | [image: image] | | | [image: Archives] | [image: image] | [image: image]

| | | [image: image] | May 2012 (5) April 2012 (1) March 2012 (3) Feburary 2012 (1) December 2011 (3) November 2011 (2) October 2011 (6) September 2011 (3) August 2011 (3) July 2011 (3) June 2011 (2) May 2011 (6) March 2011 (3) Feburary 2011 (3) January 2011 (1) December 2010 (2) November 2010 (4) October 2010 (3) August 2010 (4) July 2010 (1) June 2010 (4) May 2010 (3) April 2010 (3) March 2010 (7) Feburary 2010 (2) January 2010 (3) December 2009 (4) November 2009 (4) October 2009 (3) September 2009 (5) August 2009 (9) July 2009 (1) June 2009 (5) May 2009 (4) April 2009 (10) March 2009 (13) Feburary 2009 (12) January 2009 (11) December 2008 (9) November 2008 (8) October 2008 (5) September 2008 (5) August 2008 (6) July 2008 (6) June 2008 (6) May 2008 (2) April 2008 (3) March 2008 (7) Feburary 2008 (12) January 2008 (9) December 2007 (8) November 2007 (4) October 2007 (9) September 2007 (14) August 2007 (18) July 2007 (13) June 2007 (17) May 2007 (2) July 2006 (1) April 2006 (1) August 2005 (1) June 2005 (1) May 2005 (2) | [image: image] | | | [image: Blogroll] | [image: image] | [image: image] | | | [image: image] | JYeti Dominic Junaid | [image: image] | | | [image: Archives] | [image: image] | [image: image] | | | [image: image] |

rss [[image: Videos RSS Feed]](https://www.sensepost.com/blog/index.rss)

| [image: image] | | | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | |

| | |

| [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | [image: image] | | | [[image: Top of Page]]() | [image: image] | [image: Legal stuff] | [image: image] | [image: image] | |

| |