SQLi Attack on the Rise (Film at 11:00)

Posted At : August 8, 2008 1:30 PM | Posted By : Mark Kruger
Related Categories: Coldfusion Security

Unless you have had your head in the sand (those of you on your honeymoon are excused) you know that the ColdFusion world has been awash in SQL Injection attacks over the last month. Anecdotally I am seeing a significant increase in attacks this week - about 15 times what they were a few days ago. Michael Dinowitz reports that house of fusion was receiving 4000 attacks in 5 minutes (that's nearly 50 thousand an hour). **Brad Wood** reports no less 90 request per second. The suspicion is that the attack is driven by searching Google for sites with ".cfm" pages. That means the more successful that you are at search engine optimization the more likely you are to be targeted. Conversely if you don't have a good number of pages ranked then you are probably then you will see fewer attacks.

It seems these attacks are orchestrated using infected computers throughout the internet. Some effort is underway to collect IP addresses to see if a pattern emerges. I suspect that approach will not yield fruit, but I still applaud the effort. We (**CF Webtools**) are continuing to assist customers in any way we can - everything from wholesale changes to sites, to blacklist techniques to friendly advice over the phone. As these attacks accelerate they become more like Denial of Service attacks than anything else. Even if you are binding all your variables and you have great controls you will still have to deal with a bombardment of thousands of requests against your CF pages. I recommend that you use one of the many blacklist techniques out there - at least temporarily. Some folks have started out sending emails alerts when these attacks are underway but quickly discovered that the volume of email can be pretty hefty. I recommend just killing the request - abort it at the top of your application prior to the application being instantiated. Then at least you have kept it from filling up your error log. Meanwhile this round of attacks has had the positive affect of causing folks to suddenly pay attention to a great deal of vulnerable code. Here's another silver lining you may not have considered...

The Silver Lining

ColdFusion evangelist and luminary **Ben Forta** did manage to find a silver lining. In a recent CF-Talk post he said (and I quote):

> *" On the plus side, it's nice to see CF finally getting the recognition it deserves, even if it is from parasitic bottom-feeding bots created by despicable scum-sucking feeble-excuse-for-a-carbon-based-life-form repugnant socially-inept basement-dwelling death-penalty-deserving hacker-wannabes."*

I'm pretty sure that Ben speaks for all of us.

If you are just hitting this issue click through the related posts below or just read nearly all the ColdFusion Muse posts since July 18th. There are mitigation techniques and links to tools that can help. In particular check out the post that provides a thorough explanation of the attack. Make sure and read the comments as well for a good list of tips.