

Forum: [Hack Forums](#)

Thread: [Web Application Race Conditions](#)

Kyle1995 - May 25, 2016, 6:59 pm

I was gunna write a tutorial butttt [this does the job perfectly](#)

I don't think I've ever seen it mentioned on this forum, I don't usually post stuff unless I think it's interesting and this is something I would consider interesting. I just realized a large part of a code base I'm working on is incredibly vulnerable so I decided to see what I could find and why it's literally never mentioned here?

Whens the last time you've seen a query locking a table before reading/writing? I'm fairly sure (guessing, correct me if I'm wrong) procedures and transactions are equally vulnerable, even though that's semi rare to see imo too. I can think of a few other workarounds, like rate limiting with one session per user, but the point is this is that it's crazy common.

Just off the top of my head I can think of a social exchange framework that's incredibly vulnerable to this type of attack. Basically most web apps with a virtual currency (not just money) and not some sort of strict protection could get raped pretty hard. Especially if you have the source to it. And even otherwise I can't honestly say it'd be that much harder to blackbox.

MaXoNe - May 26, 2016, 2:12 am

Agreed, most developers forget about race conditions, have had a chance to report some bugs to my clients related to race conditions.

Even facebook has had race conditions vulnerabilities.

Some companies wont bother to fix these since these are not really bugs that script kiddies can find with scanners.

Darkkk - September 3, 2016, 10:03 am

I was planning on doing some research into RC within ruby, php, Django in the next few weeks. I've also seen dozens of cases where shit can really hit the wall. Yet no body wants to talk about it.