

Forum:[Hack Forums](#)

Thread: [Idea: persistent token separate from session ID to deter scammers](#)

linkinpork - July 9, 2021, 10:26 am

Hi,

Just wanted to share a random (possibly useful) idea I had earlier.

We know that HF uses 2 user-specific tokens: sid and mybbuser cookies. They are given upon authentication, and expire upon logout, password change, and email change.

My idea is that we could get another token -- not user-specific, but browser-specific, and doesn't expire like the typical session token. This could reflect in the trust scan as Matching browser token with other members.

It's not very important, but if the staff have any extra time on their hands this could be something they could look into.

Cheers!

Carrot - July 9, 2021, 11:07 am

Something similar to a google advertising ID? (a device identifier for advertisers that allows them to anonymously track user ad activity on Android devices)

I know of this one, so maybe something similar to:

<https://fingerprintjs.com/>

<https://github.com/fingerprintjs/fingerprintjs>

linkinpork - July 9, 2021, 11:18 am

Hi,

I've never tried those honestly. But it doesn't have to really be a specific API. It's just another randomized token.

If 2 users have the same token, it reflects on their Trust Scan. This would easily reveal multis.

x_x - July 9, 2021, 11:29 am

Idk, I can think of a handful of ways this would be defeated such as; just look at the persons trust scan and change the browser. Am I missing something?

linkinpork - July 9, 2021, 11:38 am

(Jul 9, 2021 11:29 AM)x_x Wrote: [\[CITE\]](#) Idk, I can think of a handful of ways this would be defeated such as; just look at the persons trust scan and change the browser. Am I missing something?

Hi,

That's assuming Trust Scan should be fool-proof. A person could just as well restart their router too.
:P

Or make a new account in fact.

It's not supposed to be unbeatable, just another layer to check for multis.

webdev77 - July 9, 2021, 11:43 am

I don't see a benefit to trying to fingerprint user browsers. It's easily faked or changed and really not a valuable thing to know for a trust scan anyways. There is also the fact that most fingerprints are not completely unique and could be falsely looked as a metric of trust.

linkinpork - July 9, 2021, 11:50 am

(Jul 9, 2021 11:43 AM)webdev77 Wrote: [\[CITE\]](#) There is also the fact that most fingerprints are not completely unique and could be falsely looked as a metric of trust.

Hi,

I was actually thinking maybe it could be in a cookie, a-la session token. But then again I could very well use Burp and blackmail someone by getting their token too :P

Yeah, just realized how this could be weaponized.

Tl;dr don't do it. Bad idea. Closing thread.