

Forum:[Hack Forums](#)

Thread: [Security Causing Paranoia](#)

3257337207b38fa92bb8527ad - October 20, 2019, 6:36 pm

First rule of security: do not trust user input.

My day job I work as a security researcher / engineer. My job is to stay ahead of the threat curve, stay up-to-date, and mitigate threats both current and future threats.

All day everyday my mind is in the head space of "every request is malicious" and in turn, I notice in my day-to-day I treat every "request" (real human interaction) as malicious.

I am curious as to if this is a common experience amongst engineers. Have you experienced this?

Pawnhub - October 20, 2019, 8:22 pm

You should be able to specify what is valid and invalid requests on your sites and services you are managing, treating all request's as malicious just means you are not upto date with what should be happening vs what is happening or what isn't happening.

3257337207b38fa92bb8527ad - October 21, 2019, 3:41 am

(Oct 20, 2019 08:22 PM)UnknownPawn Wrote: [\[CITE\]](#) You should be able to specify what is valid and invalid requests on your sites and services you are managing, treating all request's as malicious just means you are not upto date with what should be happening vs what is happening or what isn't happening.

I completely disagree.

You should treat all incoming queries as malicious until you are satisfied otherwise. It is entirely possible to discern between malicious traffic and legitimate users, hence how we can operate an application without crippling our users, but you always need that preface.

Cuthbert - October 21, 2019, 6:34 am

I think these are just your inner most insecurities, when you imagine a network being penetrated, you see yourself being penetrated.

It's kind of an irrational phobia to have, and yes, you're paranoid. If you spend your life looking for daggers, you're sure to find them.

SIM-2327840 - October 21, 2019, 7:08 am

It has happened to me as well, with people approaching me tho?

Pawnhub - October 21, 2019, 7:10 am

(Oct 21, 2019 03:41 AM)3257337207b38fa92bb8527ad Wrote: [\[CITE\]](#) I completely disagree.

You should treat all incoming queries as malicious until you are satisfied otherwise. It is entirely possible to discern between malicious traffic and legitimate users, hence how we can operate an application without crippling our users, but you always need that preface.

That just doesn't make sense. Out of let's say 10k people accessing your service maybe a few would possibly know how to exploit your site. You are thinking everyone is a malicious user, you've even posted on here because it's a problem. I mean take the advice or don't but from where I see it if you are banning legitimate traffic under the pretense don't trust any user input. This is not good for any business. If you can't distinguish legitimate traffic vs malicious there's your problem. You should

be analyzing traffic not assuming it's all malicious.