

Re: PHP security (or the lack thereof)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-06/msg00660.html>

- *From:* Daniel Hulme <bugtraq@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 24 Jun 2006 09:28:00 +0100
-

The other is to contrive a language that is both sufficient for dynamic web content development, and also **not** Turing-complete. I have no idea what such a language might look like, or even whether the intersection of these two requirements is the null set.

Nice idea, but PHP in its default configuration is **not** Turing-complete. The default configuration causes scripts to time out after 30s of operation, so the halting problem is trivially decidable: all scripts halt on all inputs. Notice that not being Turing-complete doesn't stop people writing insecure code in it. A toy language whose only operation is to change the root password to "password" would also not be Turing-strong, but would make it even easier to shoot yourself in the box.

Something that might have more luck is a system of taint checking like Perl offers. However, making sure programs adhere to a complex specification — and a specification that covered all security holes would be very complex — has been an open research question for some years. Some schools of thought lean towards formal methods and correctness-proving, others towards software engineering techniques, but there is no ideal solution, and the sort of people who are writing the kind of PHP scripts routinely advertised on bugtraq have probably never heard of either. Proof-carrying code might help remedy this, because the server administrator would be able to mandate that any script executed on the server carry a proof with it; however, I believe the amount of programmer-generated annotation required on current implementations would be prohibitive to the largely untrained programmers we are trying to reach.

—

There once was a teacher of great renown, Gather your goods
Whose words were like the tablets of stone, and follow me
Because it's easier to learn than unlearn, Or you will surely die.
Because we've passed the point of no return. Paul Simon, 'The Teacher'