

Forum:[Hack Forums](#)

Thread: [How do notorious hackers find vulnerabilities?](#)

your_a_big_tramp - July 3, 2017, 5:42 am

Do they look at the source ? Or do they use a program to scan for SQL, XSS, and other things? If so what program.

SysAdmin - July 3, 2017, 5:43 am

Trial and Error. Usually their own programs.

Prawnster - July 3, 2017, 5:43 am

(Jul 3, 2017 05:42 AM)your_a_big_tramp Wrote: [\[CITE\]](#) Do they look at the source ? Or do they use a program to scan for SQL, XSS, and other things? If so what program.

I swear you ask the same shit every other day with a new thread.

Most people will do their own searching and then maybe use a vulnerability scanner to scan the site to double check.

KelseyM - July 3, 2017, 5:46 am

There is no sure way to find a vulnerability. You have to try a little of everything. I mean, if there was a how to guide, don't you think people would protect against it eventually? Some small websites won't have certain protections, but most have the basic ones covered. Just read and learn, then trial and error. Think of it as a game, something of a puzzle.

RandTheRand - July 3, 2017, 5:46 am

Reverse engineering software/hardware to find holes in security. That's why it is recommended you learn c and assembly as reverse engineering will only show you assembly code

vaiperboy - July 3, 2017, 5:48 am

reverse engineering everything
debugging, testing, etc...

virtualized - July 3, 2017, 5:49 am

There are programs to scan for public vulnerabilities, which website owners may not have noticed or fixed yet.

Other than that, people just search. Years of trial and error.

Biker BoyZ - July 3, 2017, 5:51 am

custom software made by them that can pick this shit in seconds. these types are known to the unknown notorious hackers.

Asdethprime - July 3, 2017, 7:07 am

The basics to finding vulnerability normally revolves around Fuzzing. If you can find a binary of the program, what people would do is use various different fuzzers , alongside their own cases to test the limits of the program. Assumption being, sooner or later you will find a vulnerability.

Finding a vulnerability and creating an exploit are 2 different things. You might not be able to create a exploit for every vulnerability you find.

Normally a debugger is use, for example Olly DBG. The purpose of the debugger is to give the

vulnerability researchers a view into why exactly did the program respond the way in which it responded.

One after that you create proof of exploit through trial and error.

It's not easy, it's never been purported to be easy.

You can get books on it, past research and a lot of differen things, but at the end of the day you would need to know every ins and out of the program, every ins and outs of how the program operates on a very low level (normally around memory) and a significant amount of luck to go with it.

There is a reason big exploits cost as much as they do, which could cross a million dollars for 1 single major remote code execution vulnerability in one of the popular software.

Zixem - *July 3, 2017, 8:42 am*

depends, if you have access to the source code it might be less frustrating. because you see how everything works and can make sure that they implement security right.

if you perform a black-box testing, it'll be based on trial and error.