Security Bugs

Thomas Zangari

The article talks about how does testing has the ability to generate knowledge about security vulnerabilities. It explains that security bugs are always present because the entire development is focus on what it should do rather on what is should not do and there for it might do more that it should do.

The article explains the security bug testing strategies after analyzing thousands of security reports and answering three questions. What underlying software fault of design decision caused this bug?

What were the symptoms of failure that should have alerted the tester to the presence of the bug? What testing design strategy would have enabled testers to expose the vulnerability before the software was released ?

The study showed that there were four main sources for security vulnerability:

-dependency on shared code libraries: the source of the security bug comes from external source that can became unavailable. Once the sensitive data has been identified we should imagine what is going to be the hackers approach.

- unanticipated user input: unfortunately some inputs can be legitimate but combined can result illegitimate. This is a problem for configuration access option software. Some of these configurations can create security holes. There for testers must ensure good coverage of all various options.

- design vulnerability: Design can produce security holes especially if there are legacy code. The security tester needs to ensure that the functionality of the program don’t causes security holes. Another form, and rare type of design vulnerability is the notes and test planes that are written in the source code by the testers. There for exposing witch test were covered and identifying the holes more easily.

- Implementation vulnerability : Implementation can be done in such a way that it can cause security holes. The best approach is to have security testes while implementing the software.

insecure design, careless implementation. Each of these require different testing strategies.