Jonathan Disla

Discussion 8.1

Web 340

Prof. Massoud

Security Mindset

Security risks come as fast as new technologies to counteract those risks are released. However, neither the hackers nor those fighting against hacks ever stop reinventing new methods. To have a security mindset is to think like a hacker would. Imagine the security risks an application has or could have given the right situation. Thinking about what can trigger or inject a bug that attacks vulnerabilities in a program. Any small loophole in an application can cause magnificent loss.

Bugs are a very high security risk. While most programs have bugs from time to time, there can be bugs in a program such as inadequate syntax and incorrect or no error handling. It is of extreme importance for a program to throw an error and exit upon catching an error which may be a potential threat to the application. An SSL certicate that is not enforced can cause major issues for the security of users in an application. "If your site has users, you'll want to be responsible and protect them(Hahn, 178)." In SQL there is the term "sequel injection" which is when an input does not escape user input that can pass as a database query. In this case, a user can delete an entire database, very scary. Phishing is a very famous term in the tech world that accounts for a large number of security threats. In mail applications a user may receive a link that inserts a bug to hijack and steal information from a user. A cookie could be left for years without a user knowing while a hacker steals information.

Reference List

Hahn Edward M. "Express in Action." Manning Publications Co. Shelter Island, NY 2016.