Post by **Gokul Kurunthasalam**

Peer Response

What do you like about their flowchart?

I appreciate the clear explanation about the SQL injection method in your Flowchat figure 1.1. The types of SQL injection like HHTP attack's, time based attacks, Boolean attacks, error based attacks and union based attacks. It is possible to obtain sensitive data from the database servers via blind SQL Injection. Most likely, the hacker uses the application database to send true or false (1 or 0) queries, then examines the results based on the applications' responses. Figure 1.2 gives detailed explanation about the web interface Boolean SQL Injection.

In what way(s) might it be improved?

I guess few more detailed explanation about the Figure 1.2 an 1.3 needed in this post. Also, it would be good if the following explanation is added to the Figure 1.3, obtaining information about the database itself is frequently important when utilizing SQL injection vulnerabilities. This covers the kind and version of the database software as well as the tables and columns that make up the database's contents.

References:

https://beaglesecurity.com/blog/vulnerability/boolean-based-blind-sql-injection.html. [Accessed on 14 Dec 2022]