During training sessions and examinations, the Muse software allows an operator to control the mannequin remotely. This is done by applying preloaded scenarios that represent real life medical situations. The main challenge is that if these preloaded scenarios have been tempered with, they can pose serious risky outcomes which gives the students false results. Software attacks are very common and they subvert data and make it vulnerable. Hackers can access the Muse software and it is important to note that there are so many inhuman hackers who can go to the extent of changing and altering the loaded scenarios to an extent where they do not offer what they were intended to do.

Lyna Griffin, (N.D) states that:

“One of the vulnerabilities that facilitate many injection attacks is when the database is not adequately isolated from the running code. Though isolation may curtail, to some extent, some of these attacks, a better standard security measure is to encode data, making it safe before it is used. Encoded data is transformed into unrecognizable executable statements before being passed to the respective interpreter.”

In this case it becomes of utter most importance to secure the software to avoid injections that can ruin the sessions and examinations.

References

Griffin L, (N.D) Secure Software – Definition and Characteristics. Available from: https://study.com/academy/lesson/secure-software-definition-characteristics.html