HYDRA.AS.UTEXAS.EDU

DB incident on 2022-11-24

On 2022-11-24 at approximately 9 UT, hydra's user database was deleted.

I discovered that all entries contain information on a single user with a fictitious username and other details.

It is impossible to reconstruct the exact scene, however it is most likely that the situation unfolded as follows.

1) The manual creation of a good-looking hydra account. At this level, code on Hydra verifies that the data are reasonably accurate.

At 09:08:54 UT, a new user was made with the DB query.

INSERT into user set username = 'tsSLAueP', password = 'da3f50400551551ea03382ac7c3bfa587f789b68', first name = 'tsSLAueP', last name = 'tsSLAueP', email = 'example@email.tst', institution = 'Georg August Universitat'

2) Utilize scanning software that employs direct links to update information for a newly generated user.

This time, there were many connections per second with a single IP address. It's difficult to determine which were successful, and it's also possible that data entry was performed manually. The update commands I discovered in the DB log were like:

*UPDATE user set username to tsSLAueP9993516, first name to response.write(9564528*9182937), last name to tsSLAueP, email address to sample@email.tst, institution to Georg August Universitat, and user id to 410.*

Unfortunately, the code on hydra was not validating all user information fields.

This has led to the database data loss.

With the assistance of CNS IT, I was able to restore data from 20221114.

Only data for one user was lost. I reached out to him, and he recreated his account.

To avoid such issues in the future, I modified the code on hydra and added string sanitization to prevent incorrect characters in text fields.

For example names cannot contain symbols such as "response.write(9564528*9182937)"

Additionally, I implemented hourly database backups to hydra, nossy, and depot.

Since hydra is the sole computer in our operation queue chain with access to the outside world, its database backups are saved on both hydra and HET.