To: William H. Flathead III

From: Claudio Facchinetti

Subject: Security issue: SQL injection attack

Date: October 3, 2021

The objective of this memo is bring to your attention a security issue that has been discovered in software for the Community Credit Union.
As discussed in previous meetings it looks like someone has access to personal information and there is deficit of more than $32,000.
The reason for this is a vulnerability present in the Community Credit Union software, more precisely in the `FCCU`.php file, which is called SQL Injection.
As you know we are saving data on an instance of MySQL, which is a relational database using the SQL to perform operations, regardless of where the code comes from. As a matter of fact the web application `FCCU.php` does not sanitize user inputs in almost all user fields but rather passes it directly to the database as it is.
If the user acts nicely than nothing bad happens, however if the user is a malicious one and attempts to insert some SQL code in the fields than the database will interpret this code and will act accordingly, for example letting the user in without considering the password. What is even worse is that an attacker could also not know any account ID but still login into every single account by exploiting this vulnerability. The worst possibility, however, is that an attacker can login as a specific user and wire funds to another account on another bank by simply exploiting this vulnerability.
A good news, however, is that an attacker can neither create new accounts nor update the existing ones making them having any balance.
I have already proceeded to patch this issue by removing all plain string concatenation with prepared statements: in this way all strings passed get escaped and therefore interpreted correctly by the database manager.
Other than this I also noticed that the user the application is using to perform database operations has all privileges even though it does not need, for example, to perform any insertion or deletion. For this reason I would suggest to redefine the privileges granted to that user so that it has only the strictly necessary ones.
As a final note I would like to remark that this is what has caused the data being accessed by unauthorised parties and the deficit of more than $32,000. From what I saw at the moment there are no logs, therefore we have no idea of where funds went; a suggestion could be employing a robust logging solution so that in such cases we can build some kind of history to at least track funds being moved around.