Vinci Nicolò

SQL injection

08/10/2021

Security flaw:

The main security flaw in FCCU application regards any input inserted by the user. Indeed, no input is checked or sanitized. For example, the id and password are retrieved from input fields at line 31 and 32 and they are used to build some queries how they are.

Line 31:

```
$id = $PARAM['id'];
```

line 32:

```
$password = $PARAM['password'];
```

An example of dangerous query can be found immediately at line 34:

```
$query = "SELECT * FROM accounts WHERE id = $id AND password = '$password'";
```

Hence, the user can inject any SQL statement that will be inserted in the query and executed.

Fix problem:

A combination of input validation and character escaping has been developed to fix the problem. Now, the field $id can only be a numeric field and the field $password can only be an alphanumeric field. Otherwise, the login page will return an error. These two checks are done with the following if statement:

```
if (is_numeric($PARAM['id']) && ctype_alnum($PARAM['password']))
```

Then, if the two checks are passed, any input parameter will be escaped thanks to the function mysqli_real_escape_string(). For example to escape the field $password:

```
$password = mysqli_real_escape_string($mysqli, $PARAM['password']);
```

Now, even if a user injects some SQL statements, special characters will be escaped with backslashes and they will not be interpreted as SQL language.

Recovery plan:

1. The breach was really serious. Firstly, a malicious user could retrieve any personal information about employees. Secondly, he could transfer any quantity of money to any bank with the right routing number and account number. So, he could perform that operation impersonating an employee through the personal administrative interface. However, he could not gain root access directly to the machine where the PHP program is running.
2. The mitigations described in the previous section should be applied in order to secure the server. Then, a history table may be developed in order to keep tracking of the operations performed on the accounts table. Moreover, a backup of both tables should be developed in a different location in order to retrieve data in case of breach.
3. There are other problems which do not regard the SQL injection. The first regards the variable $amount retrieved from user input and passed to three functions: transfer_funds(), wire_funds() and withdraw_cash(). If the user provides as input a floating number or a string, the FCCU application crashes.

The second regards the function transfer_funds(). Indeed, if the user does not select any person from the drop down menu, the FCC application crashes..