LAB03B: SQL Injections

Simon X Camilo

Redacted

Redacted

February 16 2021

This server(localhost, used for the website urbank) has vulnerabilities that allow for attackers to get user information by using sql injection. This document displays every vulnerability that I was able to find with the help of online resources I found online.

# SQL Vulnerabilities

1. Exploiting error to get info on the database
2. Getting info on the system used by the web server
3. Get name of database

## Exploiting error to get info on the database

Entering “’ or extractvalue(0x3a,concat(0x3a,(**command**())))#” in the username field appends us to a legitimate field, allowing us to enter any command we want as a syntax error. Extract value provides us with the database printed as an error. Command should be replaced with a mysql command that will give you the info you want to get.

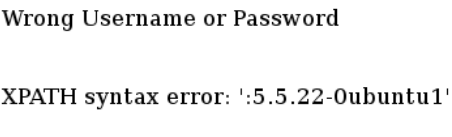
This is what is going to be used to get more information on the system and make changes

## Getting version info on the **system used by the web server**

Identifying the database can be done by entering ' or extractvalue(0x3a,concat(0x3a,(select version())))#

We can ask for what’s the version of the client the web server is using, with “select version”.

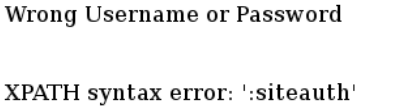
below is the output:



## **Look at the** tables in the database

You can get the name of the database by entering ' or extractvalue(0x3a,concat(0x3a,(select database())))#

We get this output:



# Citations

Kaplarevic, V. (2020, June 01). How to Check mysql Version: 5 easy Commands {UBUNTU, LINUX}. Retrieved February 18, 2021, from https://phoenixnap.com/kb/how-to-check-mysql-version

Mysql commands. (n.d.). Retrieved February 18, 2021, from [http://g2pc1.bu.edu/~qzpeng/manual/MySQL%20Commands.htm](http://g2pc1.bu.edu/~qzpeng/manual/MySQL Commands.htm)