Ben Wasserman

CPSC 370

October 30th, 2018

SQL Injection Lab

ii.

1. The version of the database server is 5.0.51a-3
2. After some basic research, I was able to find a variety of vulnerabilities in this specific version of software. Below is a list of potential vulnerabilities
   1. Allows for remote authenticated users via unknown vectors
   2. Remote authenticated users can cause denial or service attacks with the GREATEST or LEAST command and a variety of other arguments
   3. There are multiple stack-based buffer overflow errors that allow the user to execute code or cause a denial of service attack
   4. Some string format vulnerabilities allow a remote authenticated user to cause a denial of service attack and affect databases.

iii.

1. This query returns the name of the user and the host name for the connection.
2. This could be very useful in connecting..

iv.

1. This query returns the name of the database
2. This is very useful in determining how we can connect.

v.

1. This returns the name of all the tables
2. This is extremely useful in finding tables to exploit

vi.

1. This returns all the columns in the users table
2. Very important for getting specific things