**Security Issues + Mitigation Strategies**

1. **Using MD5 (salted or unsalted) for password**

This becomes an issue not due to MD5 being cryptographically weak but because it is simply too fast. Hackers are able to try billions of candidate passwords per second on a single GPU. A solution would be to use deliberately use slower generating hash constructions like scrypt.

(<http://security.stackexchange.com/questions/19906/is-md5-considered-insecure>)

1. **WireShark able to analyze packets and read data sent/received from database**

This is a serious issue as the username and password (although MD5 hashed) are being sent over the network unprotected. A hacker is able to pick up and read this data, simply convert the hash back to its plaintext form and attain access to the entire system. One main solution is the use of SSL via HTTPS to encrypt the entire data transfer.

1. **Why it's a bad idea for a system to use the stored procedure created when registering new users in production.**

The stored procedure we have created accepts a plaintext password and performs the md5 conversion prior to inserting it into the database. This process can enable hackers to attain the password prior to it entering the stored procedure. One way to mitigate this would be to perform the hash outside of any stored procedure and simply insert this hashed value into the database.