Database Vulnerabilities

# Introduction:

When designing our project we must consider any vulnerabilities or weaknesses that could become a threat to us or our users. This makes it important to discuss and implement solutions to these problems.

According to Shulman(2006)”Top 10 database security threats” the 10 most common security threats to a database include: Excessive privilege abuse, Legitimate privilege abuse, Privilege Elevation, database platform vulnerabilities, SQL injection, weak audit trail, denial of service, database communication protocol vulnerabilities, weak authentication, and backup data exposure. In this report I will be discussing all of these topics with the exception of SQL injections and Platform vulnerabilities as SQL injection was covered by Peter in our Vulnerability Document conducted previously and Platform Vulnerabilities was covered under the vulnerable and outdated components covered by me.

# Excessive Privilege abuse:

According to Shulman(2006)”Top 10 database security threats” excessive privilege abuse is “*When users (or applications) are granted database access privileges that exceed the requirements of their job function*.” This is important to consider as a weakness as users could use these permissions for malicious purposes. The example given by Shulman(2006)”Top 10 database security threats” was that “*a university administrator whose job requires only the ability to change student contact information may take advantage of excessive database update privileges to change grades*.” This shows an example of how someone could change data to better reflect their intentions. This is important to us as in our pay roll systems some of this data could relate to wages or hours worked which could lead to someone being paid too little or too much which would be in violation to our LSEPI analysis we conducted, both violating legal and social issues relating to staff. The given solution to this problem is by ensuring that all users only have the minimum level of access required to do there job, no more and no less.

# Legitimate Privilege abuse:

According to Shulman(2006)”Top 10 database security threats” legitimate privilege abuse is *“Users may also abuse legitimate database privileges for unauthorized purposes.”* This is a more difficult problem to excessive privilege abuse as we cannot simply take away the privileges as they are required to function in that role. The solution to this given by Shulman(2006)”Top 10 database security threats” is that in addition the excessive privilege abuse protections we must also apply similar standards to the surrounding context of database access. For example in our database we can prevent this by tracking what times people are accessing the database, for what purposes and what they are accessing we can identify users who are breaking this policy and who may have malicious intent.

# Privilege Elevation:

According to Shulman(2006)”Top 10 database security threats” privilege elevation is when *“Attackers may take advantage of database platform software vulnerabilities to convert access privileges from those of an ordinary user to those of an administrator.”* This could be done by taking advantage of vulnerable functions or SQL statements in our code. A solution to this could be to test our code to find these vulnerabilities so that an attacker may not take advantage of them.

# Weak Audit trail:

According to Shulman(2006)”Top 10 database security threats” the weakness associated with an audit trail are *“Automated recording of all sensitive and/or unusual database transactions should be part of the foundation underlying any database deployment. Weak database audit policy represents a serious organizational risk on many levels.”* This relates to the previous solution to Legitimate privilege abuse as we should be recording all sensitive or unusual activity relating to the database.

# Denial of Service:

A denial of Services attack (or DOS attack) is when access to the network is denied to intended users. Shulman(2006)”Top 10 database security threats” recommends the following action to prevent DOS attacks *“DOS prevention requires protections at multiple levels. Network, application, and database level protections are all necessary.”* These levels include Connection controls, IPS and Protocol validation, Dynamic Profiling and Response timing. This means if our project needs to work over a network we should consider additional research into these topics.

# Backup data exposure:

According to Shulman(2006)”Top 10 database security threats” “*Weak authentication schemes allow attackers to assume the identity of legitimate database users by stealing or otherwise obtaining login credentials. An attacker may employ any number of strategies to obtain credentials.*” There are three main methods described: Brute force (Entering user details until they’re able to login), Social Engineering (Taking advantage of peoples ‘innate trust’ to attempt to steal login credentials) and direct credential theft (an attacker steals login credentials through files or notes). To stop these types of attacks we need further develop our policy to protect against these attacks. For example anyone who has login credentials to our program should have a secure password, for example containing a mixture of letters, capitals, numbers and/or symbols to help prevent brute force attempts. In addition to this we should also teach employees to not inherit trust phone calls or emails and to never given away specific information such as passwords over them.

# References:

* Shulman(2006)”Top 10 database security threats” <https://schell.com/Top_Ten_Database_Threats.pdf>