**Project Name: SQL Injection**

**Technology: Kali Linux**

**Market: Security**

**Name / Group: Gagneet S.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Potential Providers:**

Kali Linux

DVWM - Vulnerable Application Environment

**Intended Activities:**

Installation of DVWM in a Kali Linux VM that is installed (persistent).

Exploitation of your own database.

Discussion of your results.

Presentation (to the class) on both your process and your results.

**Design:**

The goal of this lab is to begin to become familiar with one of the common vectors for significant data breach, SQL injection. In order to become familiar, vulnerable practice environments offer opportunity to gain experience and understanding as to how data breaches occur.

**Directions:**

Answer the questions below in preparation for the practical portion of your lab (in Section 2).

**Questions to Answer:**

**Section 0: Lab Basics**

Explain the following terms:

Kali Linux- An Linux distribution used for pen testing

SQL Injection- Using commands to attack a database

DVWM - Vulnerable Application Environment- A database meant for testing sql attacks

**Section 1: Lab Environment**

Describe the process of SQL injection?

* Used to attack sql database by inserting malicious sql statements into a entry field.

What does it offer?

* It allows attackers to bypass application security measures and gain access to sensitive data.

What is the importance of having a DVWM - Vulnerable Application Environment for SQL?

* To test one’s own database to find flaws and patch them before others find them.

What tools are used in exploiting the database?

* SQL commands and Kali Linux could be used to find the vulnerable url for the database

What network technologies allow or disallow access to a database service to the broader network?

* A Firewall

What is one of the leading network issues that contributes to SQL injection?

* Sharing a website server with the SQL Database.

**Section 2: Practical**

Installation of Kali Linux

Installation of DVWM - Vulnerable Application Environment

SQL Injection

Review of Findings in Group

Presentation of Findings to the Class

Develop (and document … and submit) a plan to better deploy a database server so that you mitigate issues BEFORE they occur. Include an image from a network diagramming tool (i.e. Visio, Draw.io, etc.).

Plan to deploy a Safer Database server:

* To start with the physical server, one should have the sever in a safe secure room where authorization is required with monitored surveillance. With the Database server not sharing any hosting with any other application.
* For the Network side of the server, there should be a firewall that has strong rules to deny most traffic. And should have ports only for some applications and never be allowed for direct access. Firewall rules should also be reviewed monthly to keep up to best practice and see any potential issues.
* The database software should be kept up to most date version, with latest patch applied weekly. Unused functions of the database should be turned off, with any default passwords removed or changed. The applications code that run on the server should be reviewed for SQL injection vulnerabilities.
* All logins to the server should be kept in a log for at least 2 years and audit logs be reviewed weekly.
* Backups should also be taken weekly in case of malware encrypting the system, allowing one to roll back to the previous backup without any issues.