**UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA**

**UNAN-León**

****

**Facultad de Ciencias y Tecnología**

**Departamento de Computación**

**Ingeniería en Telemática**

**Componente:** Seguridad de Redes

**Docente:** Aldo Martínez

**Tema:** SQL Injection

**Fecha:** 29-04-2019

**Integrante:** Jonathan Eduardo Ochoa Velasquez 15-01898-0

**¡A la libertad por la Universidad!**

SQL Injection Attacks on an MS SQL Database

SQL injection es una técnica usada para atacar sitios web, y es la vulnerabilidad más común existente en los sitios web.

Escenario del Laboratorio:

Hoy en día, la inyección SQL es uno de los ataques a sitios web más comunes. Estos ataques son realizados a bases de datos que tienen vulnerabilidades, las cuales pueden ser usadas por los atacantes para ejecutar sus propias sentencias SQL con el objetivos de modificar u obtener información de los datos almacenados en dicha base de datos, comprometiendo la seguridad del sitio web y de sus usuarios.

Como un administrador de seguridad experto en pruebas de penetración, necesitas probar aplicaciones web que se ejecutan en la base de datos MS SQL para detectar vulnerabilidades y fallas.

Objetivos del Laboratorio:

El objetivo de este laboratorio es proveer a los estudiantes conocimientos de los ataques SQL Injection y analizar las aplicaciones web para detectar vulnerabilidades.

En este laboratorio vas a aprender como:

* Loguearte con credenciales válidas
* Probar las inyecciones SQL
* Crear tu propia cuenta de usuario
* Crear tu propia base de datos
* Lista de directorios
* Hacer cumplir los ataques de denegación de servicios.

Desarrollo del Laboratorio

Para completar este laboratorio, necesitarás:

* Una computadora corriendo Windows Server 2012 (Máquina víctima)
* Una computadora corriendo Windows Server 208 (Máquina atacante)
* MS SQL Server tiene que estar corriendo con los privilegios del sistema
* Un buscador web con conexión a internet