**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!**

**Lab 1: 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

**Ataques SQL Injection**

SQL Injection es un ataque básico usado para ganar acceso no autorizado a una base de datos o recibir información directamente de la base de datos. Esto es una fallo que se encuentra en las aplicaciones webs y no en la base de datos o es un problema de la base de datos o del servidor web.

**Tareas de laboratorio**

Una inyección SQL oculta es usada cuando una aplicación web es vulnerable a inyecciones SQL pero el resultado de esa inyección no es visible a los atacantes.

Una inyección SQL a ciega es idéntica a una inyección normal, excepto que cuando un atacante intenta explotar una aplicación, en lugar de ver un mensaje de error útil, se muestra una página genérica personalizada.

En este laboratorio, la máquina hosting (Windows Server 2012) es la máquina víctima y la máquina usada para realizar los ataques será Windows Server 2008.

1. Loguearse en la maquina virtual de Windows Server 2008.
2. Lanzar un buscador web, escribir [**http://www.goodshopping.com**](http://www.goodshopping.com/)y presionar **Enter.**