15-SQL Injection

PLEASE use prebuilt labs

Victim Data: direct interaction Need 2-6 computers online that have the services running and vulnerable

Advanced: Build a data file / artifact that is actionable by the contract holder. There are no instructions for this task. You must figure everything out.
Advanced: capture encrypted packets, using decryption process from capture discussion

Attacker Data: Kali/ Parrot

Objective

The objective of this lab is to perform SQL injection attacks and other tasks that include, but are not limited to:

- Understanding when and how web applications connect to a database server in order to access data
- Performing a SQL injection attack on a MSSQL database
- Extracting basic SQL injection flaws and vulnerabilities
- Detecting SQL injection vulnerabilities

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform SQL injection attacks on target web applications. The recommended labs that will assist you in learning various SQL injection techniques include:

1. Perform SQL injection attacks
   1.1. Perform an SQL injection attack on an MSSQL database
   1.2. Perform an SQL injection attack against MSSQL to extract databases using sqlmap*
2. Detect SQL injection vulnerabilities using various SQL injection detection tools
   2.1. Detect SQL injection vulnerabilities using DSSS
   2.2. Detect SQL injection vulnerabilities using OWASP ZAP

***Indicates capture**