Talal Jawaid

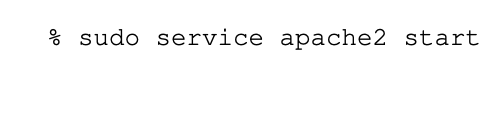
11/24/19

Lab 5

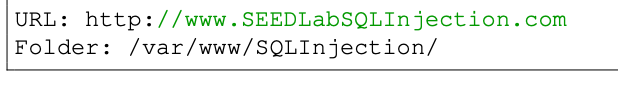
SQL Injection

Sql injection is complicated technique that has been used from the dawn of sql to send custom sql queries to unsanitized inputs to retrieve or manipulate data from databases that are not meant to be accessible.

First step is to launch apache webserver



You then have to modify hosts file to map domain names to web servers ip address.



We then configure sources for website by modifying sources in directory it is hosted in

A screenshot of a cell phone

Description automatically generated

As there are built in countermeasures, we have to disable the PHP mechanism “magic quote.”

A screenshot of a cell phone

Description automatically generated

As the VM we are using does not include the employee management web app for this lab, we have to patch the VM

A screenshot of a cell phone

Description automatically generated

Bootstrap script will patch by adding db called users in the vm, load data into the db, set up virtual host URL, and modifies DNS config.

At this point, the db should host this data. The goal is to access it.

A screenshot of a cell phone

Description automatically generated

As in previous labs, we can just log in to our mySQL

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

This is the web app

A screenshot of a cell phone

Description automatically generated

We then have to access using the SQL injection attack

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

This screen, while innocuous, allows us to submit SQL commands

By using countermeasures, we can prepare against the SQL injection attack

A screenshot of a cell phone

Description automatically generated

I noticed this is very similar to the SQL injection techniques on hackthissite, which was a very valuable resource in understanding SQL injections for this lab.