Plan de Prácticas
Criptografía y Seguridad 2023-2

Anayanzi Delia Martínez Hernández
anayanzi@ciencias.unam.mx

Ivan Daniel Galindo Perez
ivangalindo@ciencias.unam.mx

Luis Fernando Yang Fong Baeza
fernandofong@ciencias.unam.mx

Marzo 2023

1 Introducción

La inyección de SQL es una de las maneras más comunes de vulnerar alguna aplicación con conexión a alguna base de datos cuyas entradas no estén sanitizadas, en esta práctica se realizarán distintos tipos de inyecciones de SQL en un ambiente seguro con información ficticia utilizando el sitio de:

`https://tryhackme.com/room/sqlinjectionlm`

2 Información previa a la práctica

Supongamos que se tiene una aplicación completamente sencilla, se trata de un login como se muestra en la siguiente figura.

Figure 1: Un login aparentemente sencillo

Que podría ser una apliación cualquiera, sin embargo, ocurre un gran problema, en los cuadros de `input` al final de cuentas, se lleva acabo una interacción

con la base de datos directamente, puesto que se requiere validar que el username sea correcto, que el email también lo sea y obviamente que el password también lo sea, hasta ahí, todo correcto respecto a funcionamiento.

Eso implica que el query que se va a hacer en el login mostrado, debe de ser algo parecido a:

select username, password, email **from** users **where** username = *input* **and** password = **hash_algorithm**(*input*);

O algo asimilable, a esto. El sin embargo, la inyección de SQL, se basa en la vulnerabilidad de NO sanitizar las entradas del usuario y que puedan contenter código de SQL para que sea ejecutable y regrese información sensible o vulnerable, por ejemplo, si en el recuadro de usuario el siguiente fragmento de query: ' **or** 1=1; –, entonces el query se transofrma a:

select username, password, email **from** users **where** username = '' **or** 1=1; – **and** password = **hash_algorithm**(*input*);

Lo cual es completamente ejecutable en alguna consola de SQL (asumiendo que el comentario si se escriba con –).

3 Procedimiento

Para practicar las inyecciones de SQL, apoyándose en la plataforma de TryHackMe, se deberá de resolver el siguiente laboratorio (gratis):

https://tryhackme.com/room/sqlinjectionlm

Que se ve como sigue:
Este laboratorio esta basado en una aplicación didáctica basada en SQLite que es otro tipo de DBMS pero muestra cuál es el query que se está ejecutando en tiempo real (lo que en una aplicación normal no ocurre).

Deberán de obtener todas las banderas hasta terminar el laboratorio.

En caso de que se desee aprender más respecto a las inyecciones de SQL, se les deja el siguiente laboratorio.

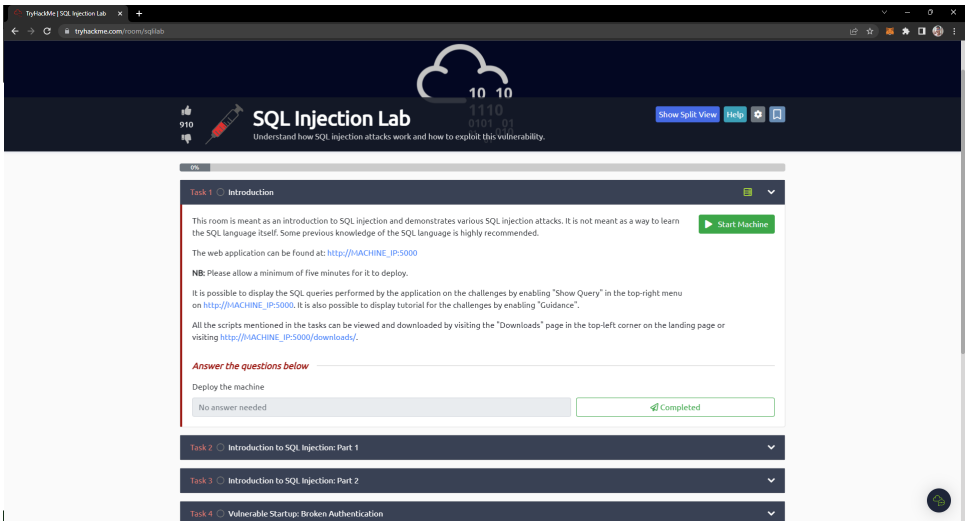

Figure 3: Laboratorio auxiliar

Este lab, es para aprender un poco más o entender mejor el concepto de SQLi, NO ES DE CARACTER OBLIGATORIO.

4 Entregables

Para esta práctica los entregables son:

1. Un archivo .txt / .pdf con todas las banderas de THM.
2. El nombre de la cuenta que haya realizado el laboratorio.
3. Nombres de los integrantes.

Deberán de entregarla a lo más en parejas para el dia 27 de Abril antes de las 23:59:59 via Classroom.

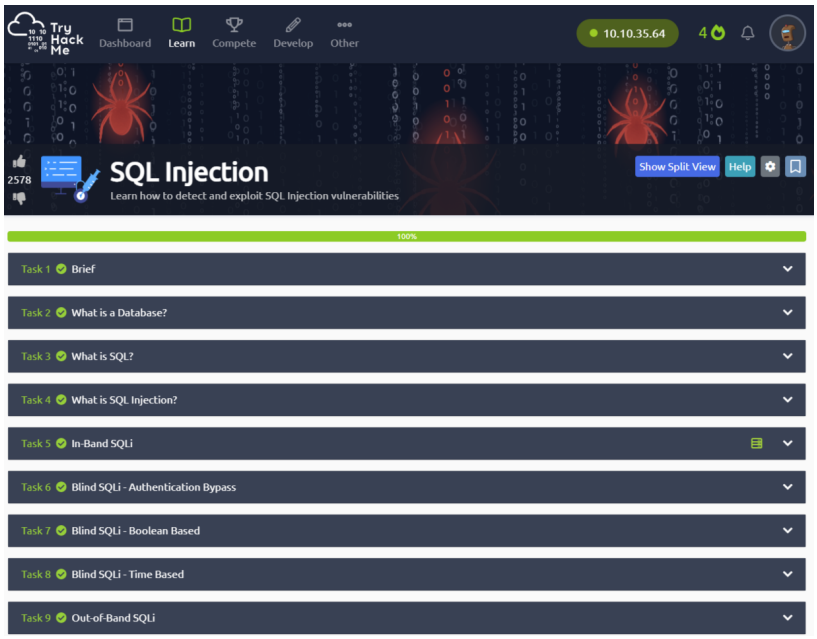

Figure 2: Laboratorio que conscierne a la práctica.