SQL INJECTION

SAD

2ºASIR
I.E.S. ANTONIO MACHADO
ANA OROZCO ASENSIO

Contenido

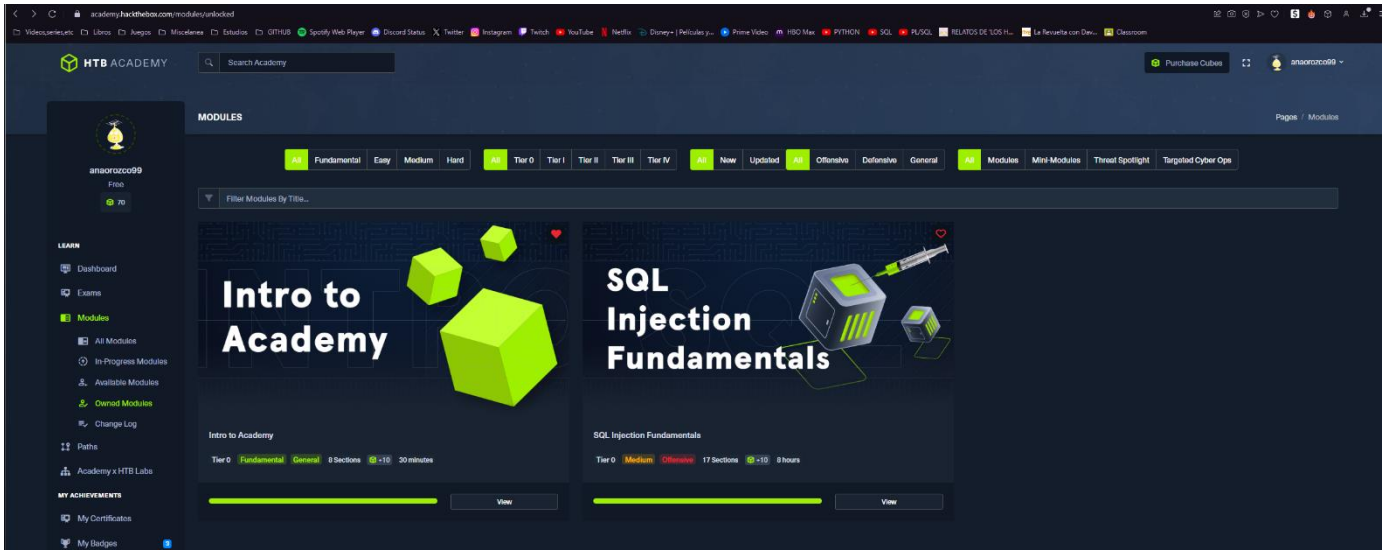
Introducción. 2
HackTheBox..... 2
SQL Injection. 2
Inyección en el login. 3
Inyección en el buscador. 3
Conclusión. 4

Introducción.

En esta práctica realizaremos el módulo de SQL Injection Fundamentals de HackTheBox y documentaremos dos tipos de inyecciones SQL que hemos usado en el curso.

HackTheBox.

En esta captura muestro que he realizado el modulo de SQL Injection Fundamentals de HackTheBox.



SQL Injection.

Una inyección de SQL (hay sitios que lo abrevian como SQLi) es un ataque en el cual se utiliza lenguaje SQL para poder acceder a los datos de una base de datos.

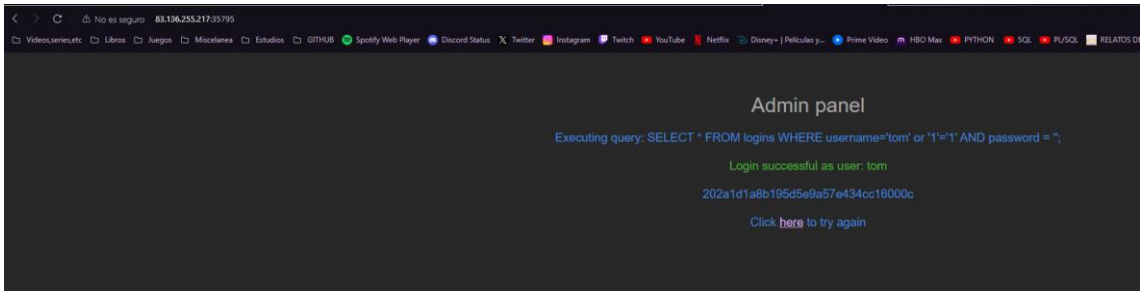
Existen de varios tipos, pero voy a hablar de dos tipos: la inyección en el login y la inyección en un buscador.

Inyección en el login.

Es una técnica que se usa para poder acceder a una web sin usuario ni contraseña, aunque podemos acceder a ciertos usuarios en concreto.

Se usa una comilla simple ‘ después del nombre que queramos buscar para que detecte que esa consulta SQL termina y que nos de un valor o código.

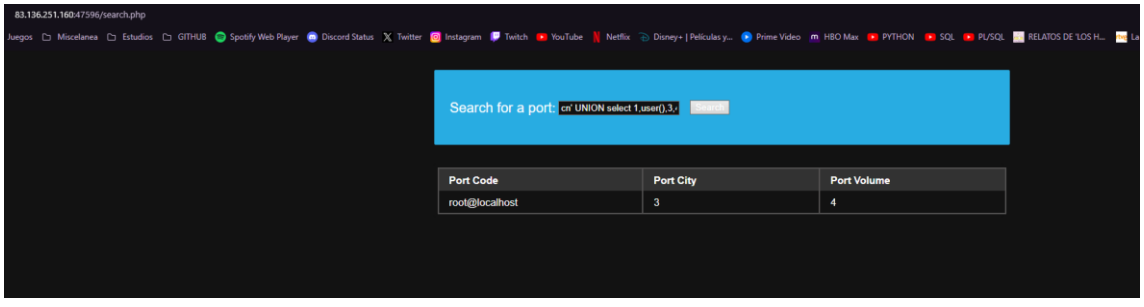
Otro carácter que se utiliza es el doble guion -- que indica el inicio de un comentario haciendo que se ignore el resto de la consulta, lo que es útil para omitir ciertas partes que el atacante no quiere que se ejecuten, por ejemplo la verificación de la contraseña.



En esta práctica teníamos que iniciar como Tom y al hacerlo los sabía la bandera que es el código alfanumérico largo.

Inyección en el buscador.

Es una técnica que se usa en los buscadores en una página web para manipular la consulta que se envía y que nos devuelva alguna información como la versión de la base de datos que utiliza, aunque podemos llegar a hacer updates y deletes a datos.



En esta práctica de la captura caso debíamos usar user() para ver el usuario que accede a la web.

Se puede usar user() como una variable para saber el usuario que está accediendo a la base de datos, también @@version para ver la versión de la base de datos, TABLE_NAME para los nombre de las tables, TABLE_SCHEMA para el esquema de tablas, podemos también cargar archivos como /etc/passwd y un largo etc.

Conclusión.

SQL Injection supone un gran problema sobre todo a páginas y programas que no están preparados para evitarlo, por lo tanto sería interesantes siendo responsables de la seguridad de un servidor que podamos evitar este tipo de ataques tomando algunas medidas como por ejemplo codificar los datos, implementar acceso con menos privilegios, restringir el acceso de los usuarios basándonos en lo que de verdad es necesario que editen (llamado enfoque de confianza cero), etc.