



Firstly, I successfully completed the "Light" lab on the TryHackMe platform, where we aimed to exploit an SQLite-based vulnerability. The initial step involved establishing a connection to the target system using Netcat (**nc**) on port 1337.

The task title indicated the presence of a user named **"smokey"**, which suggested that this account could be a potential entry point. By leveraging this information, I proceeded with further enumeration and exploitation to gain deeper access to the system.



It gave us an error message when we used single quotes. So it could be Union-based SQLi here.

Now, let’s try to find table name in our database:



We got message from system (**Ahh there is a word in there I don’t like :(** )

In SQLite-based systems, **SQL Injection filters** often detect specific keywords written in a consistent uppercase or lowercase format, such as "UNION", "sqlite\_master", or "table". These filters typically use **blacklist-based detection**, flagging queries that match restricted keywords exactly. To bypass such filters, attackers may **alter the case of characters**, use **string concatenation**, or encode keywords in **hexadecimal or Unicode format** to evade detection.

Now, let's attempt to bypass the filter by testing different combinations of uppercase and lowercase characters:



Yes, it is working now. We got table name from target database:

Now we can use our table name for finding username :



We got our username in “**admintable**”. Our username is “**TryHackMeAdmin**”:

We got answer of the first question of task

Now, let’s get the password of **“TryHackMeAdmin”:**

****

We got answer of the second question of the task.

Now, let’s get the last question of task:



Written by Elnur Ahmedov.