

LAB-06

Testing SQL injection error

Mutillidae

Procedure:

1.The LAB-06 Question is to find which php is vulnerable to SQL.

Referring to the user-info page, which PHP file contains the source code vulnerable to SQL injection?

☐ MySQLHandler.php
☐ user-info.php
☐ constants.php
☐ index.php
☐ ddsmoothmenu.js

Submit

Choose the best answer or view Hints and Videos

2.Open the login page and let us test whether the application validates user input.

Password incorrect

Please sign-in

Username

Password

Login

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

Please sign-in

Username

Password

Login

Injecting code: admin' – we can find that this page vulnerable to SQL injection.

Failure is always an option

Line	238
Code	0
File	/var/www/mutillidae/classes/MySQLHandler.php
Message	/var/www/mutillidae/classes/MySQLHandler.php on line 238: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1 Query: SELECT username FROM accounts WHERE username='admin' --'; (1064) [mysqli_sql_exception]
Trace	#0 /var/www/mutillidae/classes/MySQLHandler.php(238): MySQLHandler->doExecuteQuery('SELECT username...') #1 /var/www/mutillidae/classes/MySQLHandler.php(279): MySQLHandler->executeQuery('SELECT username...') #2 /var/www/mutillidae/includes/process-login-attempt.php(57): SQLQueryHandler->accountExists('admin' --'; #3 /var/www/mutillidae/index.php(225): include_once('/var/www/mutillidae...') #4 (main)
Diagnostic Information	Error querying user account

[Click here to reset the DB](#)

OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.10.8 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](#)

Login

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

Hints and Videos

Exception occurred

Please sign-in

Username

Password

Referring to the user-info page, which PHP file contains the source code vulnerable to SQL injection?

☒ MySQLHandler.php
☐ user-info.php
☐ constants.php
☐ index.php
☐ ddsmoothmenu.js

Referring to the user-info page, which PHP file contains the source code vulnerable to SQL injection?

☐ MySQLHandler.php
☐ user-info.php
☐ constants.php
☐ index.php
☐ ddsmoothmenu.js

Correct